Landtag Brandenburg **Drucksache 2/5253**

2. Wahlperiode

Sechster Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Berichtszeitraum: vom 1. April 1997 bis 31. März 1998

Datum des Eingangs: 13.05.1998 / Ausgegeben: 18.05.1998

Inhaltsverzeichnis Seite

1 Datenschutzrechtliche Entwicklung ... 14
1.1 Einleitung ... 14
1.2 Schaffung einzelgesetzlicher Regelungen im Land Brandenburg ... 15
1.3 Umsetzung der EG-Datenschutzrichtlinie in nationales Recht ... 19
1.3.1 Novellierung des Bundesdatenschutzgesetzes ... 19
1.3.2 Angleichungsbedarf des Brandenburgischen Datenschutzgesetzes ... 20
1.4 Technisch-organisatorische Maßnahmen bei der Einhaltung des Datenschutzes ... 22
1.4.1 Landesverwaltungsnetz ... 22
1.4.1.1 Abschottung der lokalen Netze durch Firewalls ... 22
1.4.1.2 Sicherstellung der Vertraulichkeit der im LVN übertragenen personenbezogenen Daten ... 23
1.4.1.3 Anschluß des LVN an das Internet ... 23
1.4.1.4 Protokollierung von Nutzeraktivitäten auf WWW-Servern ... 24
1.4.1.5 Bürokommunikation mit GroupWise ... 24
1.4.1.6 Verfahren Haushalts-, Kassen- und Rechnungswesen ... 25
1.4.2 TeleKommunikationsverbund der obersten Landesbehörden ... 25
1.4.2.1 Neue Software zur Gebührendatenverarbeitung ... 25
1.4.2.2 Praxis der Telefonabrechnung verschiedener Ministerien ... 26
1.4.5 Kryptographie - der Schlüssel für sichere Daten ... 28
1.4.5.1 Folgenminderung bei Einbrüchen in Kommunalverwaltungen ... 28
1.4.5.2 Verschlüsselung der Daten beim Wohngeldverfahren ... 28
1.5 Neue Technologien ... 29
1.5.1 Risiken bei der Nutzung von Handys ... 29
1.5.2 Neue Vorschriften bei Telekommunikations-, Tele- und Mediendiensten ... 30
1.5.3 Sicherheit bei der Telearbeit ... 32
1.5.4 Kryptographie - der Schlüssel für sichere Daten ... 34
2 Allgemeiner Datenschutz ... 35

2.1 Brandenburg - das erste Bundesland mit einem Akteneinsichtsrecht ... 35
2.2 Änderung des Verwaltungsverfahrensgesetzes ... 37
2.3 Staatsverträge ... 39
2.3.1 Festlegungen für soziale Versicherungsträger ... 39
2.3.2 Staatsvertrag über grenzüberschreitende kommunale Zusammenarbeit ... 39
2.4 Verwaltungsvorschrift zum Brandenburgischen Datenschutzgesetz ... 41
2.5 Druck von Lohnsteuerkarten im Auftrag ... 42
2.6 Unseriöse Datenerhebung durch Marketingfirmen ... 43
2.7 Petentenschutz auch für Bedienstete der öffentlichen Verwaltung ... 44
2.8 Altakten - ein unendliches Thema ... 46
2.8.1 Verbleib von Lohn- und Gehaltsunterlagen ehemaliger DDR-Einrichtungen ... 46
2.8.2 Akten liquidierter Betriebe - Verkauf DISOS GmbH ... 47
2.8.3 Verzeichnis von Gefangenenkarteien und Gefangenenakten der früheren DDR ... 47
3 Inneres ... 48
3.1 Melde- und Personenstandswesen ... 48
3.1.1 Novellierung des Brandenburgischen Meldegesetzes ... 48
3.1.2 Neue Verordnung über regelmäßige Datenübermittlungen der Meldebehörden ... 54
3.1.3 Kommunalwahl 1998 ... 55
3.1.3.1 Änderung des Kommunalwahlgesetzes ... 55
3.1.3.2 Kommunalwahlverordnung ... 56
3.1.4 Änderung des Personenstandsgesetzes ... 57
3.1.5 Problematische Datenverarbeitung im Auftrag bei Software-Umstellung ... 58
3.2 Grundstückswesen ... 59
3.2.1 Änderung des Vermessungs- und Liegenschaftsgesetzes ... 59
3.2.2 Pilotprojekt ... 60
3.3 Polizei ... 60
3.3.1 Einsatzleitsystem der Polizei ... 60
3.4 Verfassungsschutz ... 61
3.4.1 Sicherheitsüberprüfungsgesetz ... 61
3.5 Statistik ... 63
3.5.1 Stand beim Statistikregistergesetz ... 63
3.5.2 Stand der Vorbereitung der Volkszählung 2001 ... 64
3.5.3 Statistischer Beirat ... 65
3.5.4 Sonstiges ... 66
3.5.4.1 System repräsentativer Verkehrserhebung (SrV 98) ... 66
3.5.4.2 Heim- und Telearbeit bei der Statistikstelle ... 67
3.5.4.3 Kommunalstatistik ... 69
4 Justiz/Staatsanwaltschaft ... 70
4.1 Gesetze und Rechtsverordnungen ... 70
4.1.1 Ausführungsgesetz zur Insolvenzordnung ... 70
4.1.2 Neufassung MiZi 98 ... 70

4.1.3 Neufassung MiStra ... 71
4.2 Verfahrensfragen ... 72
4.2.1 Automation bei den Staatsanwaltschaften ... 72
4.2.2 Gerichtliche Verfahren, durch die mehrere Personen betroffen sind ... 73
4.2.2.1 Sammeladressierung ... 73
4.2.2.2 Übermittlung von Meldeadressen ... 73
4.3 Eingaben zu Grundbuchangelegenheiten ... 74
4.3.1 Öffentlichmachen personenbezogener Daten durch Grundbuchauszug ... 74
4.3.2 Einsicht in Grundbuchakten durch Berufsgenossenschaft ... 75
4.3.3 Einsichtnahme ins Grundbuch ganz und gar? ... 76
4.4 Forschung ... 76
5 Bildung, Jugend und Sport ... 77
5.1 Gesetze und Verordnungen ... 77
5.1.1 Lehrerbildungsgesetz ... 77
5.1.2 Verwaltungsvorschrift zum Schulbetrieb ... 78
5.1.3 Grundschulverordnung ... 78
5.1.4 Sonderpädagogik-Verordnung ... 79
5.1.5 Berufsfachschulverordnung für kaufmännische Berufe ... 80
5.1.6 Berufsfachschulverordnung ... 81
5.1.7 Berufsfachschulverordnung mit Berufsabschluß gemäß Bundesbildungsgesetz und Handwerksordnung 82
5.1.8 Fachoberschulverordnung ... 82
5.1.9 Berufsfachschulverordnung für sozialpflegerische Berufe ... 83
5.1.10 Verordnung über wissenschaftliche Untersuchungen ... 83
5.1.11 Verwaltungsvorschriften über schulische Zeugnisse ... 84
5.2 Datenschutzrechtliche Einzelangelegenheiten im Schulbereich ... 85
5.2.1 Schulverwaltungsprogramm ... 85
5.2.2 Fotografen in der Schule ... 85
5.2.3 Bundeswehr forscht nach einem ehemaligen Schüler ... 85
5.2.4 Projekt ... 86
5.2.5 Schülerausweise in Scheckkartenformat ... 87
5.3 Jugend ... 87
5.3.1 Kontrollbesuch bei der Zentralen Adoptionsstelle Berlin-Brandenburg ... 87
5.3.1.1 Aufgaben ... 87
5.3.1.2 Ergebnisse der Prüfung ... 88
5.3.2 Teilnehmerlisten für Ferienfreizeiten ... 91
5.3.3 Neue Entgeltsatzung des Kita-Verbundes ... 91
6 Wissenschaft, Forschung und Kultur ... 92
6.1 Wissenschaft ... 92
6.1.1 Spannungsverhältnis von Forschung und Datenschutz - Gespräche mit der Deutschen Forschungsgemeinschaft ... 92
6.2 Archive ... 94

6.2.1 Benutzungsordnung des Brandenburgischen Landeshauptarchives 94
6.2.2 Verwaltungsvorschriften zum Archivgesetz in Sicht 94
6.2.3 Archive und elektronische Datenverarbeitung 95
6.2.4 Archivfachliche Voraussetzungen im Sinne von § 2 Abs. 8 BbgArchivG 97
6.2.5 Ausschreibung von Arbeitsstipendien durch das MWFK 97
6.3 Hochschulen 98
6.3.1 Novellierung des Hochschulgesetzes 98
6.3.2 Meldeverfahren für die Krankenversicherung der Studenten 99
6.3.3 Datenverarbeitende Stelle bei Anfertigung von Diplomarbeiten 100
6.3.4 Einführung von Chipkarten an Hochschulen 100
6.3.5 Telefon- und Vorlesungsverzeichnis im Internet 101
7 Arbeit, Soziales, Gesundheit und Frauen 102
7.1 Soziales 102
7.1.1 Gesetze und Verordnungen 102
7.1.1.1 Sozialhilfedatenabgleichsverordnung gem. § 117 Bundessozialhilfegesetz 102
7.1.2 Aktuelle Fälle 103
7.1.2.1 Leistungssachbearbeitung von Sozialversicherungsträgern für eigene Mitarbeiter 103
7.1.2.2 Umgang mit Hinweisen auf Fahruntauglichkeit von Versicherten bei Sozialversicherungsträgern ... 104
7.1.2.3 Übermittlung von Sozialdaten an die Kriminalpolizei 105
7.1.2.4 Arzneimittel-Budget-Informationen des Apothekenrechenzentrums für die Kassenärztliche Vereinigung Brandenburgs 107
7.1.2.5 Betreiben eines Krankenkassendruckzentrums durch eine Firma 108
7.1.2.6 Auskunftsersuchen einer Krankenkasse an ein Gesundheitsamt wegen Massenerkrankungen 108
7.2 Gesundheit 109
7.2.1 Gesetze, Verordnungen und Erlasse 109
7.2.1.1 Gesetz zur Regelung des Transfusionswesens 109
7.2.1.2 Infektionsschutzgesetz 110
7.2.1.3 Verwaltungsvorschrift zum Umgang mit Impfdateien im Gesundheitsamt 110
7.2.1.4 Brandenburgisches Rettungsdienstgesetz 111
7.2.1.5 Umgang mit personenbezogenen Daten aus Leichenschauscheinen 112
7.2.1.6 Novellierung des Psychisch-Kranken-Gesetzes 112
7.2.2 Aktuelle Fälle 113
7.2.2.1 Prüfung der Datenverarbeitung in einem Krankenhaus 113
7.2.2.2 Umgang mit Dienst- und Privatpost in der zentralen Poststelle einer Landesklinik 118
7.2.2.3 Verpflichtung der Beschäftigten in Krankenhäusern zum Tragen von Namensschildern 119
7.2.2.4 Krankenhauswanderer 120
7.2.2.5 Archivierung von Krankenakten im Archiv des Trägers 121
7.2.2.6 Tumorbasisdokumentation 123
7.2.2.7 Fragebogen für Kita-Untersuchungen 124
8 Ernährung, Landwirtschaft und Forsten 124
8.1 Gesetze und Verordnungen 124

8.1.1 Novellierung des Tierzuchtgesetzes ... 124
8.1.2 Novellierung des Tierschutzgesetzes - endlich ist es soweit ... 125
8.2 Sonstiges ... 127
8.2.1 Informationsanspruch ehemaliger LPG-Mitglieder ... 127
8.2.2 Neues Datenverarbeitungssystem zur Kontrolle der Agrarförderung ... 128
8.2.3 Numerierung von Hundesteuermarken ... 129
9 Umwelt, Raumordnung und Naturschutz ... 130
9.1 Abfall- und Altlastendatenschutzverordnung ... 130
9.2 Anschluß des MUNR an das Landesverwaltungsnetz ... 130
10 Stadtentwicklung, Wohnen und Verkehr ... 133
10.1 Bau- und Wohnungswesen ... 133
10.1.1 Mietspiegel ... 133
10.1.2 Kommunales Vorkaufsrecht - welche Daten braucht die Gemeinde? ... 134
10.1.3 Verwaltungsvorschrift zu Planungsunterlagen für Bauleitpläne u. ä. ... 135
10.1.4 Bereichsspezifische Datenschutzregelung in der Bauordnung ... 136
10.2 Verkehr ... 136
10.2.1 Datenverarbeitung im Vollzug der Landesschiffahrtsverordnung ... 136
10.2.2 Fahrerlaubnisverordnung ... 137
11 Finanzen und Wirtschaft ... 138
11.1 Finanzen ... 138
11.1.1 Gesetze und Verordnungen ... 138
11.1.1.1 Automation in der Steuerverwaltung ... 138
11.1.1.2 Arztgeheimnis contra Steuererhebung ... 138
11.1.2 Sonstiges ... 139
11.1.2.1 Homosexualität - ein erhöhtes Versicherungsrisiko? ... 139
11.1.2.2 Information über wettbewerbsrechtliche Bußgeldbescheide durch die Landeskartellbehörde ... 140
11.1.2.3 Steuernummern von Mitgliedern der Handwerkskammern ... 140
11.1.2.4 Feststellung der Stundungsvoraussetzung bei Realsteuer- und Kommunalabgabenschulden ... 141
11.1.2.5 Geltendmachen von Werbungskosten für Bildungsreisen ... 141
11.1.2.6 Veröffentlichung strafbewehrter Unterlassungserklärungen ... 141
11.2 Wirtschaft ... 142
11.2.1 Einholung von BZR-Auskünften durch Ingenieurkammer über das Wirtschaftsministerium ... 142
12 Kommunale Probleme ... 143
12.1 Kommunalverwaltung um neues Image bemüht - Schaffung von Bürgerbüros ... 143
12.2 Jugendämter ... 145
12.2.1 Unterhaltsrechtsfragen ... 145
12.2.2 Das Umgangsrecht eines Nichtsorgeberechtigten ... 145
12.2.3 Kontrolle der Beratungstätigkeit der freien Träger ... 146
12.2.4 Einsichtnahme in Jugendhilfeakten durch Dritte ... 147
12.2.5 Aktenübergabe vom Jugendamt ans Sozialamt ... 148
12.2.6 Unterhaltsberechnungen bei einem Selbständigen ... 148

12.3 Meldeamt 149
12.3.1 Gezielte Werbung durch Musikschulen 149
12.4 Sozialamt 150
12.4.1 Ermittlungen des Sozialamts - nicht unbedenklich 150
12.4.2 Einsatz von (privaten) Sozialhilfeermittlern 151
12.5 Sonstige Stellen 153
12.5.1 Zweckverbände zur Daseinsfürsorge 153
12.5.1.1 Wasserversorgung in Privathand 153
12.5.1.2 Abfallentsorgung durch eine GmbH 153
12.5.1.3 Selbstauskunft gegenüber Zweckverbänden 155
12.5.2 Aktenübergabe beim Zuständigkeitswechsel des jugendärztlichen Dienstes 156
12.5.3 Bußgeldstelle in friedensstiftender Mission 157
12.6 Sonstiges 159
12.6.1 Gemeindevertretung 159
12.6.1.1 Organisatorische Maßnahmen bei Weitergabe an Gemeindevertretung 159
12.6.1.2 Einsichtnahme von Gemeindevertretern in Unterlagen bei Bürgerbegehren 160
12.6.1.3 Datenweitergabe in Stadtverordnetenversammlung 162
12.6.1.4 Weitergabe eines Protokolls an private Dritte 162
12.6.1.5 Zulässigkeit von Bürgerbefragungen in Kommunen 162
12.6.1.6 Offenbarung personenbezogener Daten in Amtsblatt der Gemeinde 163
12.6.2 Standesamt zu Unrecht verdächtigt 163
12.6.3 Telefonrecherchen durch private Auskunftsunternehmen 164
13 Personaldatenverarbeitung 164
13.1 Verwaltungsvorschriften zur Personalaktenführung 164
13.2 Sonstiges 167
13.2.1 Informations- und Kontrollbesuche bei personalaktenführenden Stellen des Landes 167
13.2.2 Einsichtsrechte des Landesrechnungshofs und der Rechnungsprüfungsämter in Personalakten 174
13.2.3 Personalentwicklungskonzept 177
13.2.4 Einsichtnahme in dienstliche Beurteilung durch die Schwerbehindertenvertretung 179
13.2.5 Einsatz eines Kopiererfassungssystems 179
13.2.6 Personaldatenschutz contra Informationsanspruch der Presse 180
13.2.7 Personalnachrichten in Ministerialblättern und in Hausmitteilungen 182
13.2.8 Negative Bewertung in Dienstbesprechungen und Protokollen 182
13.2.9 PERIS - ein Personalinformationssystem für die Landesverwaltung 184
14 Aus der eigenen Behörde 186

Anlage 1 Rede des Landesbeauftragten für den Datenschutz vor dem Plenum des Landtages Brandenburg am 25. Februar 1998

Anlage 2 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 20. Oktober 1997 zu den Vorschlägen der Arbeitsgruppe der Arbeits- und Sozialministerkonferenz (ASMK)
„ Verbesserter Datenaustausch bei Sozialleistungen“

Anlage 3 Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997 in Bamberg
Novellierung des Bundesdatenschutzgesetzes und Modernisierung des Datenschutzrechts

Anlage 4 Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997 in Bamberg
Informationelle Selbstbestimmung und Bild-Ton-Aufzeichnungen bei Vernehmungen im Strafverfahren

Anlage 5 Entschließung der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997 in Bamberg
Erforderlichkeit datenschutzfreundlicher Technologien

Anlage 6 Thesenpapier der Datenschutzbeauftragten des Bundes und der Länder zum Allgemeinen Informationszugangsrecht und zum Recht auf informationelle Selbstbestimmung

Anlage 7 Bonner Appell gegen den geplanten Großen Lauschangriff

Anlage 8 Entschließung der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 19./20. März 1998 in Wiesbaden
Datenschutz beim digitalen Fernsehen

Anlage 9 Entschließung der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 19./20. März 1998 in Wiesbaden
Datenschutzprobleme der Geldkarte

Anlage 10 Stellungnahme der Datenschutzbeauftragten der Europäischen Union vom 28. Februar 1997 zum

Grünbuch über den Jugendschutz und den Schutz der Menschenwürde in audiovisuellen Diensten und Informationsdiensten (KOM (96) 483 endg.),

zur Mitteilung an das Europäische Parlament, den Rat, den Wissenschafts- und Sozialausschuß und den Ausschuß der Regionen über rechtswidrige und schädliche Inhalte im Internet (KOM (96) 487)

sowie zur Ratsentschließung vom 28. November 1996 über rechtswidrige und schädliche Inhalte im Internet

Anlage 11 Entschließung der Europäischen Konferenz am 19. September 1997 zum Entwurf der Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation (früher: ISDN-Richtlinie)

Anlage 12 Empfehlung der Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten nach Art. 29 der EG-Datenschutzrichtlinie
Empfehlung 1/97 vom 25. Februar 1997 zu Datenschutzrecht und Medien

Anlage 13 Empfehlung der Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten nach Art. 29 der EG-Datenschutzrichtlinie
Erste Leitlinie für die Übermittlung personenbezogener Daten in Drittländer vom 26. Juni 1997

Anlage 14 Gemeinsame Erklärung der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation vom 12. September 1997 zur Kryptographie

Anlage 15 Handys – Komfort nicht ohne Risiko

Anlage 16 Orientierungshilfe des AK Technik
Datenschutzrechtliche Protokollierung beim Betrieb informationstechnischer Systeme (IT-Systeme)

Anlage 17 Arbeitspapier „Datenschutzfreundliche Technologien“

Anlage 18 Arbeitspapier „Datenschutzfreundliche Technologien in der Telekommunikation“

Anlage 19 Stichwortverzeichnis

Anlage 20 Abkürzungsverzeichnis

1 Datenschutzrechtliche Entwicklung

1.1 Einleitung

Mit dem 6. Tätigkeitsbericht, den ich dem Landtag und der Landesregierung vorlege, gebe ich einen Überblick meiner Arbeit im Berichtszeitraum 1997/1998 und weise außerdem auf ausgewählte Probleme hin, die künftig einer stärkeren Beachtung bedürfen. Gleichzeitig komme ich damit auch der Pflicht nach, über die Schaffung einzelgesetzlicher Datenschutzregelungen im Land Brandenburg zu berichten.

Die Adressaten für diesen Bericht sind in erster Linie die Mitglieder des Landtags, darüber hinaus auch die interessierte Öffentlichkeit und nicht zuletzt die Vielzahl der öffentlichen Stellen im Flächenland Brandenburg mit ihren Beschäftigten. Die Informationsansprüche und Erwartungen sind notwendigerweise unterschiedlicher Art und können in einem solchen Bericht jeweils nur begrenzt Berücksichtigung finden. Durch Themenauswahl und Darstellungsweise wird versucht, dem Rechnung zu tragen.

Der Berichtszeitraum zeichnet sich durch eine schwerpunktmäßige Bearbeitung von spezialgesetzlichen Vorschriften im Schulbereich aus (s. unter 5.1 ff.). Die Landesregierung hatte sich das Ziel gesetzt, alle untergesetzlichen Vorschriften an das Brandenburgische Schulgesetz anzupassen und bis zum Beginn des Schuljahres 1997/1998 in Kraft zu setzen. Daher lag es nahe, diese Bemühungen der Landesregierung zu unterstützen und gemeinsam mit dem Ministerium für Bildung, Jugend und Sport zeitgleich eine Informationsbroschüre zum „Datenschutz in den Schulen" herauszugeben, die landesweit - insbesondere den ca. 1200 staatlichen Schulen und Schulämtern - als Arbeitsmaterial zur Verfügung gestellt wurde. Die Informationsbroschüre kann kostenlos bei meiner Behörde abgefordert werden.

Einen weiteren Schwerpunkt stellt der Sozialbereich dar. Auffällig ist inzwischen hier, daß der Bundesgesetzgeber dazu tendiert, aufgrund der zunehmend knapper werdenden öffentlichen Mittel die Befugnis der Sozialämter zur Verhinderung des Sozialmißbrauchs ständig zu erweitern, ohne daß diese ihre bereits bestehenden Möglichkeiten voll ausschöpfen (s. unter 7.1.1.1 und 12.4.2).

Im Berichtszeitraum führte meine Behörde eine Reihe von Prüfungen vor Ort durch. Dabei handelte es sich zum einen um die bereits im 5. Tätigkeitsbericht angekündigten Folge- bzw. Ergänzungsprüfungen von TK-Anlagen der obersten Landesbehörden (s. unter 1.4.2), von Behördenanschlüssen an das Landesverwaltungsnetz (s. unter 1.4.1) sowie von einem Krankenhaus (s. unter 7.2.2.1) und zum anderen um repräsentative Prüfungen im Bereich der Personalaktenführung (s. unter 13.2.1) und die Prüfung der Zentralen Adoptionsstelle Berlin-Brandenburg (s. unter 5.3.1). Vergleichbare Prüfungen im Adoptionsbereich sind mir nicht bekannt. Wegen personeller Engpässe waren zu meinem Bedauern weitere Prüfungen (aber auch die Bearbeitung einiger Sachthemen) nicht möglich.

Die Anzahl der Eingaben und Anfragen an die Behörde hat im Berichtszeitraum erfreulicherweise weiter zugenommen. Auffällig häufig handelte es sich dabei um anonym vorgetragene Anliegen von Bediensteten der öffentlichen Verwaltung (s. unter 2.7). Ich vermute, daß sie Nachteile aufgrund der derzeitigen Arbeitsmarktsituation und ihrer wirtschaftlichen Abhängigkeit befürchten, wenn dies unter Namensnennung geschehen würde.
Wie auch schon früher finden sich im Tätigkeitsbericht ausführliche Darlegungen zu technisch-organisatorischen Fragen sowie neuen Technologien (s. vor allem unter 1.5). Darüber hinaus wird auf grundsätzliche Probleme und Grenzen bei Bemühungen - bislang nur - großer Gemeinden in Brandenburg eingegangen, ihre Verwaltung so umzustrukturieren, daß mit Hilfe der modernen Informationstechnik eine zeitgemäße Verwaltung entsteht (s. unter 12.1). Bereits abzusehen ist,

daß diese Problematik noch viel stärker bei der derzeit in Rede stehenden Gemeindereform im Flächenland Brandenburg große praktische Bedeutung erlangen wird. Schließlich wird erstmals in einem Datenschutzbericht die Frage der Übernahme maschinenlesbarer Datenträger in die Archive angesprochen (s. unter 6.2.3). Auf die damit verbundenen Problemfelder sind die Archive weder durch die personelle noch sachliche Ausstattung eingestellt.

In einer Reihe von Fällen wurden in Verbindung mit Eingaben und Prüfungen (s. unter 5.3.1, 9.2, 12.5.3 und 12.6.1.6) gravierende Mängel festgestellt, die ich gem. § 25 Abs. 1 BbgDSG förmlich beanstandet habe. Von einer solchen habe ich abgesehen, wenn sichergestellt war, daß die beanstandungswürdigen Mängel (s. unter 7.1.2.2 und 12.3.1) gem. § 25 Abs. 2 BbgDSG abgestellt werden.

Auf spezielle Probleme der neuen Bundesländer wird in zweifacher Hinsicht eingegangen. Zum einen werden aufgrund zahlreicher Nachfragen an meine Behörde Hinweise über den Verbleib von Altdaten liquidierter Betriebe und von Gefangenunterlagen gegeben (s. 2.8 ff.). Zum anderen wird auf Unzulänglichkeiten des Grundbuchs bei Rückübertragungen im Zusammenhang mit dem Sachenrechtsbereinigungs- bzw. Schuldrechtsänderungsgesetz eingegangen (s. unter 4.3.3).

Neben vielem, was sonst noch im Berichtszeitraum erreicht wurde, ist das Akteneinsichts- und Informationszugangsgesetz hervorzuheben. Auch wenn Einzelbestimmungen darin hinter den Erwartungen zurückbleiben, so ist doch erstmalig gesetzlich die Möglichkeit geschaffen worden, daß jedermann einen Anspruch auf Verwaltungsinformationen hat. Dem Landesbeauftragten für den Datenschutz ist als weitere Aufgabe die eines Beauftragten für das Recht auf Akteneinsicht zugewiesen worden. Bundesweit wird durch dieses Landesgesetz quasi exemplarisch verdeutlicht, daß auch die Verwaltung einzubeziehen ist, wenn der Gedanke der Demokratie weiter entwickelt werden soll.

Den Kolleginnen und Kollegen in Bund und Ländern danke ich wiederum für die zweckdienliche Zusammenarbeit. Hervorheben möchte ich an dieser Stelle auch die Zusammenarbeit mit der für den privaten Bereich zuständigen Aufsichtsbehörde beim Ministerium des Innern. Der kontinuierliche Informationsaustausch über gemeinsam berührende datenschutzrechtliche Fragestellungen wirkte sich auf die Durchsetzung datenschutzrechtlicher Belange im Land Brandenburg sehr förderlich aus.

Zum Abschluß meiner Amtszeit möchte ich insbesondere meinen Mitarbeiterinnen und Mitarbeitern, die ich immer auch als Mitstreiter in gemeinsamer Sache gesehen habe, ganz herzlich für ihre Einsatzbereitschaft selbst in Zeiten stärkerer Widerstände und Belastungen danken. Ich hoffe, daß auch für sie diese Zeit ein Gewinn war. Meinem Nachfolger wünsche ich, daß er möglichst nahtlos mit seinen Vorstellungen über seine Amtsführung an das Erreichte anknüpfen kann und die Unterstützung, die erforderlich ist, um mit Erfolg dem Wohl der Bürgerinnen und Bürger Brandenburgs dienen zu können.

Als Stichtag für den Tätigkeitsbericht wurde der 31. März 1998 gewählt.

1.2 Schaffung einzelgesetzlicher Regelungen im Land Brandenburg

Fortschritte sowie Entwicklungen des Datenschutzes lassen sich sehr genau an den im Berichtszeitraum in Kraft getretenen oder im Entwurf vorliegenden bereichsspezifischen Datenschutzregelungen ablesen. Das Brandenburgische Datenschutzgesetz (BbgDSG)[1] schreibt deshalb in § 27 vor, daß dies in jedem Tätigkeitsbericht „in einem gesonderten Teil" zu geschehen hat.

Die nachfolgende Auflistung von in Kraft getretenen Gesetzen sowie Verordnungen und Verwaltungsvorschriften entspricht der Gliederung des Tätigkeitsberichtes nach dem Ressortprinzip. Eine Gewichtung erfolgt ausschließlich jeweils in den in der Klammer angegebenen Kapiteln.

Gesetze:

- Gesetz zu dem Mediendienste-Staatsvertrag vom 12. Februar 1997 und zur Durchführung medienrechtlicher Staatsverträge vom 7. Juli 1997, GVBl. I S. 75 (s. unter 1.5.2)

- Akteneinsichts- und Informationszugangsgesetz (AIG) vom 10. März 1998, GVBl. I S. 46 (s. unter 2.1)

- Gesetz zu dem Staatsvertrag zwischen dem Land Brandenburg und dem Land Sachsen-Anhalt über die grenzüberschreitende kommunale Zusammenarbeit in Zweckverbänden und durch Zweckvereinbarungen vom 9. Oktober 1997, GVBl. I S. 108 (s. unter 2.3.2)

- Gesetz zur Änderung des Brandenburgischen Kommunalwahlgesetzes vom 30. März 1998, GVBl. I S. 54 (s. unter 3.1.3.1)

- Gesetz zur Änderung des Vermessungs- und Liegenschaftsgesetzes vom 8. Dezember 1997, GVBl. I S. 116 (s. unter 3.2.1)

- Brandenburgisches Abfallgesetz (BbgAbfG) vom 06. Juni 1997, GVBl. I S. 40 (s. unter 9.1.1)

- Brandenburgisches Architektengesetz (BbgArchG) vom 7. April 1997, GVBl. I S. 20

- Gesetz zur Änderung der Brandenburgischen Bauordnung und anderer Gesetze vom 18. Dezember 1997, GVBl. I S. 124 (s. unter 10.1.4)

Verordnungen und Verwaltungsvorschriften:

- Verordnung über die Einrichtung automatisierter Abrufverfahren und regelmäßiger Datenübermittlung im Liegenschaftskataster (Liegenschaftskataster-Datenübermittlungsverordnung - LiKaDÜV) vom 17. Dezember 1997, GVBl. II 1998 S.13

- Verfahren in Gnadensachen (Gnadenordnung) vom 11. April 1997, JMBl. S. 66

---

[1] Gesetz zum Schutz personenbezogener Daten im Land Brandenburg, i. d. Fass. vom 23. Mai 1996, GVBl. I S. 185, geänd. durch § 27 Abs. 2 Nr. 3 BbgStatG vom 11. Oktober 1996, GVBl. I S. 294

- Verordnung über regelmäßige Datenübermittlungen der Meldebehörden (MeldÜV) vom 7. August 1997, ABl. S. 734

- Verordnung über die Arbeitszeit der Beamten im Land Brandenburg (Arbeitszeitverordnung - AZV Bbg) vom 17. November 1997, GVBl. II S. 842

- Verordnung über Schulversuche, Versuchsschulen, abweichende Organisationsformen und Schulen mit besonderer Prägung (Schulversuchsverordnung - SchVersuchV) vom 23. April 1997, ABl. MBJS S. 339

- Verordnung über den Bildungsgang zum Erwerb eines Berufsabschlusses nach Landesrecht in den Sozialberufen an der Berufsfachschule (Berufsfachschulverordnung für sozialpflegerische Berufe - SozBFSV) vom 24. April 1997, ABl. MBJS S. 634 (s. unter 5.1.9)

- Verordnung über die Bildungsgänge in der Sekundarstufe I (Sekundarstufe I-Verordnung - Sek I-V) vom 5. Mai 1997, GVBl. II S. 374

- Verordnung über den Schutz personenbezogener Daten in Schulen, Schulbehörden sowie nachgeordneten Einrichtungen des für die Schule zuständigen Ministeriums im Land Brandenburg (Datenschutzverordnung Schulwesen - DSV) vom 14. Mai 1997, GVBl. II S.402

- Verwaltungsvorschriften über Akten an Schulen im Land Brandenburg (VV-Schulakten) vom 14. Mai 1997, ABl. MBJS S. 442

- Verordnung über die Bildungsgänge der Fachoberschule (Fachoberschulverordnung - FOSV) vom 24. Mai 1997, GVBl. II S.434 (s. unter 5.1.8)

- Verordnung über den Bildungsgang der Grundschule (Grundschulverordnung - GV) vom 16. Juni 1997, GVBl. II S.473 (s. unter 5.1.3)

- Verordnung über den Bildungsgang der Berufsfachschule zum Erwerb eines Berufsabschlusses in kaufmännischen Berufen nach dem Berufsbildungsgesetz (Berufsfachschulverordnung kaufmännischer Berufe nach BBiG - KaufBFSV) vom 19. Juni 1997, GVBl. II S. 490 (s. unter 5.1.5)

- Verordnung über die Eingliederung von fremdsprachigen Schülerinnen und Schülern in die allgemeinbildenden und beruflichen Schulen (Eingliederungsverordnung - EinglV) vom 19. Juni 1997, GVBl. II S. 533

- Verordnung über den Bildungsgang der Berufsfachschule zur Erlangung eines Berufsabschlusses nach Landesrecht (Berufsfachschulverordnung - BFSV) vom 19. Juni 1997, GVBl. II S. 586 (s. unter 5.1.6)

- Verordnung über Unterricht und Erziehung für junge Menschen mit sonderpädagogischem Förderbedarf (Sonderpädagogik-Verordnung - SopV) vom 24. Juni 1997, GVBl. II S. 524 (s. unter 5.1.4)

- Verordnung über die Ausbildung und Prüfung in der gymnasialen Oberstufe (Gymnasiale-Oberstufe-Verordnung - GOSTV) vom 30. Juni 1997, GVBl. II S. 658

- Verordnung über den Bildungsgang der Berufsfachschule zum Erwerb eines Berufsabschlusses nach dem Berufsbildungsgesetz oder der Handwerksordnung (Berufsfachschulverordnung Berufsabschluß nach BBiG oder HwO - BBHwBFSV) vom 3. Juli 1997, GVBl. II S. 610 (s. unter 5.1.7)

- Verordnung über Prüfung zum nachträglichen Erwerb von Abschlüssen der Sekundarstufe I und der allgemeinen Hochschulreife für Nichtschülerinnen und Nichtschüler im Land Brandenburg (Nichtschülerprüfungsverordnung - NschPV) vom 23. August 1997, GVBl. II S. 762

- Verwaltungsvorschrift über die Organisation der Schulen in inneren und äußeren Schulangelegenheiten (VV-Schulbetrieb - VVSchulB) vom 1. Dezember 1997, ABl. MBJS S. 894 (s. unter 5.1.2)

- Verwaltungsvorschriften über schulische Zeugnisse (VV-Zeugnisse - VVZeu) vom 1. Dezember 1997, ABl. MBJS S. 954 (s. unter 5.1.11)

- Verordnung über die Genehmigung wissenschaftlicher Untersuchungen an Schulen (Wissenschaftliche Untersuchungen Verordnung - WissUV) vom 11. Dezember 1997, GVBl. II 1998, S. 118 (s. unter 5.1.10)

- Verordnung zur Richtlinie 89/48/EWG des Rates vom 21. Dezember 1988 über eine allgemeine Regelung zur Anerkennung der Hochschuldiplome, die eine mindestens dreijährige Berufsausbildung abschließen, für die Lehrämter (EG-Lehramtsanerkennungsverordnung - EGLeV) vom 1. Februar 1998, GVBl. II, S. 128

- Verordnung über die Anerkennung von Bienenbelegstellen (BienBeLV) vom 29. Januar 1998, GVBl. II S. 127

- Verwaltungsvorschrift des Ministeriums für Stadtentwicklung, Wohnen und Verkehr zum Wohnungsbindungsgesetz (VV-WoBindG) vom 5. Mai 1997, ABl. S. 490

- Verwaltungsvorschrift des Ministeriums für Stadtentwicklung, Wohnen und Verkehr zur Prüfung der Einkommensverhältnisse nach den §§ 25 bis 25d des Zweiten Wohnungsbindungsgesetzes (Einkommensprüfungserlaß) vom 5. Mai 1997, ABl. S. 512

- Verwaltungsvorschrift zur Herstellung von Planungsunterlagen für Bauleitpläne, Vorhaben- und Erschließungspläne sowie für Satzungen nach § 34 Abs. 4 Baugesetzbuch vom 3. September 1997, ABl. S. 846 (s. unter 10.1.2 und 10.1.3)

- Allgemeine Verwaltungsvorschrift zu § 34 a der Gewerbeordnung und zur Bewachungsverordnung - BewachVwV vom 22. August 1997, ABl. S. 799

- Rundschreiben des Ministeriums für Stadtentwicklung, Wohnen und Verkehr zum Datenschutz im Verfahren nach § 3 Abs. 2, § 4 und 28 des Baugesetzbuches (BauGB) vom 29. September 1997, ABl. S. 904

1.3 Umsetzung der EG-Datenschutzrichtlinie in nationales Recht

1.3.1 Novellierung des Bundesdatenschutzgesetzes

Im Oktober 1998 läuft der Zeitraum von drei Jahren aus, der zur **Umsetzung der EU-Datenschutzrichtlinie**[2] in nationales Recht vorgesehen ist. Drei Jahre, das schien im Oktober 1995 ein langer und für die Anpassung des deutschen Rechts an die Richtlinie ausreichender zeitlicher Rahmen zu sein, wurde doch von zuständigen Stellen immer wieder betont, daß das (bundes-) deutsche Datenschutzrecht nicht nur altbewährt, sondern gerade für die Erarbeitung der europäischen Datenschutzrichtlinie wegweisend gewesen sei.

In diesen knapp drei Jahren ist zwar durch das Bundesministerium des Innern (BMI) ein **Referentenentwurf** für die Novellierung des Bundesdatenschutzgesetzes erarbeitet worden, und dieser Entwurf hat in den Monaten Dezember 1997 und Januar 1998 allen Datenschutzbeauftragten des Bundes und der Länder zur Stellungnahme vorgelegen - auch in meiner Behörde ist eine ausführliche Ausarbeitung mit Kritik und Vorschlägen erarbeitet worden. Dennoch wird der „Fahrplan" für die Umsetzung der Richtlinie in nationales Recht trotz des weit vorangeschrittenen Erarbeitungsstandes nicht eingehalten werden. Nach Informationen aus Bonn wird das Bundesdatenschutzrecht in dieser Legislaturperiode nicht mehr in das eigentliche Gesetzgebungsverfahren eingebracht werden; nach der Wahl zum Deutschen Bundestag im September 1998 wird sich erst der neugewählte Bundestag mit der Materie Datenschutz zu befassen haben.

Die Gesetzgebungsarbeit in den Bundesländern zur Überarbeitung des **Landesdatenschutzrechts** hat überhaupt erst mit viel Verspätung begonnen. Dies schien zunächst durchaus sinnvoll zu sein, da die Länder die Schrittmacher-Tätigkeit des Bundesgesetzgebers abwarten und auf diese Weise ein möglichst einheitliches deutsches Datenschutzrecht schaffen wollten. Nachdem sich im Herbst 1997 abzeichnete, daß der Bund die Vorgaben der EU-Richtlinie nicht rechtzeitig in nationales Recht umsetzen würde, begann auch in den einzelnen Bundesländern die Formulierungstätigkeit für landesrechtliche Regelungen.

Dem Referentenentwurf des BMI zufolge ist darüber hinaus die Aufgabe, die Datenschutz-Richtlinie umzusetzen, nicht als eine Aufforderung dazu verstanden worden, das deutsche Datenschutzrecht lesbarer zu formulieren, es zu modernisieren, es zu vereinfachen. Statt dessen wurde geradezu kleinlich darauf geachtet, das bisher geltende Datenschutzrecht soweit zu erhalten, wie dies überhaupt möglich ist, und es nur im Sinne der EU-Richtlinie zu modifizieren. Das bedeutet vor allem:

- die EU-Richtlinie enthält keine Trennung zwischen öffentlichen und nicht-öffentlichen Stellen; in dem Referentenentwurf wird die in Deutschland traditionelle Zweiteilung unter Berufung auf ein Zusatzprotokoll zur Richtlinie jedoch weitgehend aufrecht erhalten,

- der Abwehrcharakter gegenüber dem Staat, der dem deutschen Datenschutzrecht eigentümlich ist, wird nicht gemindert; in dem Referentenentwurf wird demgegenüber versucht, vor allem im nicht-öffentlichen Bereich den Datenschutz nicht zu verschärfen, ihn vielmehr eher konturlos erscheinen und Sanktionen bei Datenschutzverletzungen möglichst nicht greifen zu lassen,

- durch die Richtlinie werden die Rechte des Betroffenen deutlich hervorgehoben, vor allem durch Benachrichtigungspflichten und Auskunftsrechte; in der Umsetzung zeigt sich hingegen nicht die Tendenz, derzeitig

[2] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995, ABl. EG Nr. 281/31

geltende Betroffenenrechte zu verstärken oder auszuweiten,

- bei den Kontrollen wird, wie in der Richtlinie vorgesehen, der Anlaßbezug von Kontrollen im nicht-öffentlichen Bereich entfallen; die Forderung nach einer „völligen Unabhängigkeit" der Kontrollstelle wird allerdings bedauerlicherweise durch den Entwurf nicht umgesetzt, an der Kontroll-Zuständigkeitsverteilung bezüglich öffentlicher und nicht-öffentlicher Stellen wird nichts geändert werden; das hat zur Folge, daß auch in dem jeweiligen Landesrecht die Anforderung der Richtlinie kaum Chancen auf Umsetzung hat, desgleichen werden reale Durchsetzungsmöglichkeiten der Datenschutzbeauftragten, die der Richtlinie zufolge durchaus bereitgestellt werden könnten, wohl nicht geschaffen werden,

- der seit der letzten größeren Novellierung des Bundesdatenschutzgesetzes (1990) deutlich veränderten und beschleunigten Entwicklung im Bereich der Informationstechnik wird in dem Entwurf kaum oder nicht Rechnung getragen; auch werden keine neuen rechtlichen Verfahren, wie z. B. das Datenschutzaudit oder eine (dokumentierte) Datenschutz-Folgenabschätzung in das Datenschutzgesetz eingearbeitet.

Nun kann ein Bedauern über die absehbare Verspätung bei der Umsetzung der EU-Richtlinie nach der - eher negativen - Bilanz durchaus auch positiv gewertet werden: Ein neu gewählter Bundestag könnte ja mit viel Elan darangehen, Persönlichkeitsrechte deutlicher herauszuarbeiten und dem Datenschutzrecht den Platz zu verschaffen, den es in der Informationsgesellschaft haben müßte und der ihm von der EU dem Ansatz nach gegeben worden war. Die Hoffnung aber, die sich in der Darstellung in meinem vierten Tätigkeitsbericht[3] wiedergespiegelt hatte, hat bisher getrogen, sie hat sich jedenfalls bisher nicht in ein modernes zukunftgerechtes Datenschutzgesetz umsetzen lassen.

Bei der Diskussion um die Umsetzung der EU-Datenschutzrichtlinie in nationales Recht kann es allerdings nicht nur darum gehen, die Datenschutzgesetze des Bundes und der Länder an die EU-Vorgaben anzupassen. Bei korrekter Sicht der Dinge müßte es den Gesetzgebern ständig bewußt sein, daß **bereichsspezifisches Datenschutzrecht** gleichfalls den EU-Anforderungen entsprechen muß. Dies bedeutet zudem, daß auch bereichsspezifisch der Umsetzungszeitraum für die Anpassung hätte genutzt werden müssen; der insgesamt größere Aufwand könnte wohl dem erweiterten Anpassungsanspruch dienen. Dieser Gedanke ist jedoch kaum präsent, vielmehr sieht sich vor allem der Bundesgesetzgeber immer noch in der Pflicht, die Anforderungen, die das Bundesverfassungsgericht in seinem Volkszählungsurteil aufgestellt hat, in die Fachgesetze einzuarbeiten. Selbst ein so großes und wichtiges Gesetz wie das Strafvollzugsgesetz hat die Novellierung, besser: die Ergänzung in diesem Bereich erst noch vor sich.

1.3.2 Angleichungsbedarf des Brandenburgischen Datenschutzgesetzes

Die Verzögerung, die bei der Anpassung des Bundesdatenschutzgesetzes an die EU-Richtlinie eingetreten ist und die nicht mehr aufgeholt werden kann, hat zur Folge, daß die Länder gefordert sind, die Landesdatenschutzgesetze „europagerecht" zu gestalten. Das ist eine Feststellung, die einfach auszusprechen ist, die aber viele Probleme, die mit der Umsetzung verbunden sind, in sich birgt. Ein föderativer Staatsaufbau hat zwar unbestritten viele Vorteile, bei der Frage des Datenschutzes zeigen sich allerdings gerade in Deutschland Schwierigkeiten, die andere Staaten so nicht haben.

Die Ursache liegt in der in Deutschland tradierten Trennung des Datenschutzes in unterschiedliche Schutzniveaus, je nachdem, ob der Datenschutz im öffentlichen oder im nicht-öffentlichen Bereich anzuwenden ist. Die

[3] s. unter 1. 3.1

EU-Datenschutzrichtlinie, die diese Trennung nicht aufweist und deren Umsetzung demzufolge dazu führen müßte, daß es diese Niveauunterschiede künftig nicht mehr gibt, wird in Deutschland insoweit nicht umgesetzt werden.

Das Schutzniveau bei öffentlichen Stellen der Länder war bis jetzt demjenigen des Bundes sehr weit angepaßt. Da der Bund nun keine - für den Bund selbst - verbindlichen Vorgaben bereitstellen wird, werden die Länder entweder zu separatistisch wirkenden Einzelregelungen kommen oder aber untereinander mit großem Abstimmungsaufwand zu einer gemeinsam zu erarbeitenden Lösung kommen müssen.

Die Landesbeauftragten für den Datenschutz haben sich dafür ausgesprochen, daß eine nun drohende Zersplitterung des Datenschutzrechts verhindert werden muß und haben sich darüber hinaus für eine Harmonisierung des Datenschutzrechts in ganz Europa ausgesprochen. Deshalb haben sie auf der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 24.10.1997 in Bamberg folgende Forderungen in einer Entschließung[4] aufgestellt:

- weitgehende Gleichbehandlung des öffentlichen und des nicht-öffentlichen Bereichs,

- Vermeidung eines Gefälles zwischen dem Anwendungsbereich des Gemeinschaftsrechts und dem Datenschutz in den sonstigen Gebieten,

- Verbesserung der Datenschutzkontrolle durch anlaß-unabhängige Kontrollen und durch ausdrückliche Festlegung der völligen Unabhängigkeit der Aufsichtsbehörden,

- Erweiterung der Eingriffsbefugnisse der Datenschutzbeauftragten des Bundes und der Länder,

- Sonderregelungen für Presse und Rundfunk nur insoweit, als dies zur Sicherung der Meinungsfreiheit notwendig ist; dies bedeutet Einbeziehung aller administrativen Bereiche in die Kontrollmöglichkeiten der Landesbeauftragten für den Datenschutz,

- größere Bürgerfreundlichkeit durch einfachere und verständlichere Formulierungen in den Gesetzen,

- Bestellung weisungsfreier interner Datenschutzbeauftragter in den öffentlichen Stellen,

- Anpassung der gesetzlichen Regelungen an die moderne Informationstechnologie durch Berücksichtigung der bereits erreichten und der demnächst zu erwartenden Technologien, vor allem durch die Forderung nach Datensparsamkeit, Anonymisierungen und Verschlüsselung bereits in den Vorgaben zur Technikanwendung.

Weitere Forderungen, z. B. nach Angleichung von Verfahrensschritten und Begriffen, aber insbesondere solche, die die Weiterentwicklung der Lebenswirklichkeit infolge der fortschreitenden Entwicklung der Technik und der sogenannten Globalisierung aller Lebensbereiche betreffen, beziehen sich nicht in erster Linie auf die Umsetzung der Richtlinie, sondern darauf, daß der Datenschutz und seine gesetzliche Umsetzung einer ständigen Fortschreibung bedürfen.

Ich habe schon im Herbst 1997 darauf gedrungen, mit der Novellierung des Brandenburgischen Datenschutzgesetzes (BbgDSG) zu beginnen. Erste Vorgespräche dazu fanden zwischen dem Berliner Datenschutzbeauftragten und meiner

[4] s. Anlage 3

Behörde sowie dem MI und der Berliner Senatsverwaltung für Inneres statt. Das zuständige Fachreferat im MI vertritt allerdings die gleiche Linie wie das BMI, nämlich die Umsetzung der Richtlinie ist in kleinstem Rahmen vorzunehmen. Soweit diese Tendenz der Einheitlichkeit der Datenschutzgesetze des Bundes und der Länder dient, ist sie - leider - zu akzeptieren. Ein wirklich effektiver Ansatz zur Fortentwicklung des Datenschutzrechts kann nur mit dem Bund und nicht gegen dessen Datenschutzgesetzgebung geplant und umgesetzt werden.

1.4 Technisch-organisatorische Maßnahmen bei der Einhaltung des Datenschutzes

1.4.1 Landesverwaltungsnetz

Bereits im 4. Tätigkeitsbericht[5] bin ich darauf eingegangen, welche Forderungen an einen datenschutzgerechten Zugang öffentlicher Verwaltungen zum Internet zu stellen sind. Im Berichtszeitraum habe ich das Landesverwaltungsnetz (LVN) bei einigen Behörden in bezug auf ausgewählte Einzelaspekte geprüft.

Das LVN in Brandenburg hat sich in den letzten Jahren zu einem unverzichtbaren **Kommunikationsmedium der Behörden** entwickelt. Angeschlossen sind derzeit Landesbehörden sowie kommunale Einrichtungen. Die im Landesverwaltungsnetz angebotenen Dienste sind vielfältig. So ermöglicht z. B. ein zentraler Zugang zum Internet die über eine Firewall gesicherte Verbindung weltweit, und mit Hilfe des Bürokommunikationsprogramms GroupWise können ca. 4500 Bedienstete des Landes und der Kommunen miteinander kommunizieren. Auch der Ausbau des Verwaltungsnetzes befindet sich in vollem Gange. So wird derzeit ein Hochgeschwindigkeitsnetz installiert, mit dessen Hilfe die Kommunikation im Land noch effizienter werden soll. Das zukünftige multimediale Landesverwaltungsnetz wird aus einem sogenannten Kernnetz, welches von der Polizei betreut wird, sowie aus drei darauf aufbauenden Fachnetzen bestehen; dem Fachnetz des Landesamtes für Datenverarbeitung und Statistik (LDS), dem Fachnetz der Polizei und dem Fachnetz der Finanzverwaltung. Der Kernnetz- sowie alle Fachnetzbetreiber haben sich in gemeinsamen Beratungen schon frühzeitig dazu verpflichtet **Sicherheitskonzepte vor Inbetriebnahme** der jeweiligen Netze zu erarbeiten. An der Erstellung des Sicherheitskonzeptes zum Fachnetz LDS waren u. a. ein Vertreter des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie auch meine Behörde beteiligt. In diesem Sicherheitskonzept wurden u. a. auch die grundlegenden Voraussetzungen zum Schutz der über das Landesverwaltungsnetz übertragenen personenbezogenen Daten definiert. Die Sicherheitskonzepte des Kernnetzbetreibers sowie der Fachnetze der Polizei und der Finanzverwaltung sind mir derzeit noch nicht bekannt. Ich gehe aber davon aus, daß auch diese Netzbetreiber ihre Sicherheitskonzepte mit mir abstimmen werden.

1.4.1.1 Abschottung der lokalen Netze durch Firewalls

[5] s. unter 1.4.2

Werden personenbezogene Daten des mittleren Schutzbedarfs (Schutzstufe B des Schutzstufenkonzeptes)[6] oder höher in den Behörden verarbeitet und sind die lokalen Netze der Behörden am Landesverwaltungsnetz angeschlossen, so ist das lokale Netz mit Hilfe einer Firewall zu schützen, da ein unberechtigter Zugriff auf die im lokalen Netz verarbeiteten personenbezogenen Daten sonst nicht ausgeschlossen werden kann. Diese Forderung wird auch im Sicherheitskonzept zum Fachnetz LDS erhoben. Der weitaus größere Teil der am LVN angeschlossenen Behörden haben diese Forderung noch nicht erfüllt.

Das LDS beschäftigt sich schon seit einigen Jahren mit Firewallsystemen und bietet den Behörden auch entsprechende Unterstützung bei der Auswahl und Einführung von Firewallsystemen an. Auf meinen Vorschlag hin werden auch demnächst Schulungen zur Administration und Konfiguration von Firewallsystemen im LDS durchgeführt.

1.4.1.2 Sicherstellung der Vertraulichkeit der im LVN übertragenen personenbezogenen Daten

Kontrollbesuche haben ergeben, daß selbst sensible personenbezogene Daten im LVN teilweise noch unverschlüsselt übertragen werden. Dieser unhaltbare Zustand kann nicht länger hingenommen werden. Bereits in meinem 4. Tätigkeitsbericht[7] habe ich die **Verschlüsselung von personenbezogenen Daten in Weitverkehrsnetzen** gefordert. Ausgehend vom derzeitigen Stand der Technik sind personenbezogene Daten des mittleren und höheren Schutzbedarfs (Schutzstufen B und C)[8] bei der Übertragung im Landesverwaltungsnetz zu verschlüsseln. Eine entsprechende Forderung ist auch im Sicherheitskonzept des Fachnetzes LDS enthalten.

Der Interministerielle Ausschuß für Informationstechnik (IMA-IT) hat auf der 47. Sitzung im Dezember 1996 eine Arbeitsgruppe „Übertragungssicherheit" gebildet, in der auch meine Behörde mitarbeitet. Das Ziel dieser Arbeitsgruppe besteht darin, die Einführung eines einheitlichen Verschlüsselungsverfahrens im Land vorzubereiten.

Auch im LDS werden Überlegungen angestellt, durch Aufbau eines verschlüsselten Kanals zwischen zwei Firewallsystemen eine verschlüsselte Übertragung von Daten im Landesverwaltungsnetz zu ermöglichen. Mit dieser Lösung können personenbezogene Daten des mittleren Schutzbedarfs (bis Schutzstufe B) im Landesverwaltungsnetz übertragen werden. Bei sensibleren Daten (Schutzstufe C) ist eine Verschlüsselung auf Anwendungsebene erforderlich. Im Bereich der Anwendungsverschlüsselung sollte bis zur Einführung eines landesweiten Verschlüsselungsverfahrens auf das Produkt Pretty Good Privacy (PGP) zurückgegriffen werden. Diese Softwarelösung wurde auch schon im Wohngeldverfahren[9] erfolgreich implementiert.

1.4.1.3 Anschluß des LVN an das Internet

Das Landesverwaltungsnetz Brandenburg ist über eine Firewall an das Internet angeschlossen. Hierzu wurde schon frühzeitig vom LDS ein entsprechendes Sicherheitskonzept erstellt, das auch die Forderungen der Orientierungshilfe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu „Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet" berücksichtigt. Eine von mir im Berichtszeitraum durchgeführte Kontrolle des

---

6 s. Broschüre „Technisch-organisatorische Aspekte des Datenschutzes" aus der Informationsreihe „Der Landesbeauftragte für den Datenschutz Brandenburg informiert" unter Pkt. 3.1

7 s. unter 1.4.2

8 s. Fn. 6

9 s. unter 1.4.5.2

Anschlusses des LVN an das Internet hat keine Beanstandungen gem. § 25 BbgDSG ergeben. Die während der Prüfung festgestellten Mängel wird das LDS kurzfristig abstellen. U. a. habe ich gefordert, das Sicherheitskonzept dem aktuellen Stand der Technik anzupassen, die Filtermechanismen der Router restriktiver zu nutzen und einen Bereitschaftsdienst zur ständigen Überwachung der Firewall einzurichten.

1.4.1.4 Protokollierung von Nutzeraktivitäten auf WWW-Servern

Bereits in der Vergangenheit[10] habe ich auf die Problematik der **Protokollierung von Nutzeraktivitäten** auf WWW-Servern (World Wide Web) hingewiesen. Im letzten Berichtszeitraum wurde von mir der datenschutzgerechte Einsatz von WWW-Servern überprüft. Bei allen kontrollierten WWW-Servern mußte ich feststellen, daß Nutzeraktivitäten protokolliert wurden. Nach dem Mediendienste-Staatsvertrag und dem Informations- und Kommunikationsdienstegesetz[11] ist dies allerdings nicht zulässig.

Protokolldateien von WWW-Servern werden häufig auch zur Erstellung von Statistiken herangezogen. So wird z. B. ausgewertet, wie oft auf bestimmte WWW-Seiten zugegriffen wurde. Zur Erstellung dieser Statistiken wird die Internet-Adresse der Benutzer nicht benötigt. Bei einigen WWW-Server-Implementationen besteht die Möglichkeit, die personenbezogenen Internet-Adressen der **Protokolldatei** zu **anonymisieren**, indem die letzte Stelle der Internet-Adresse durch „xxx" ersetzt wird (z. B. 10.219.3.xxx).

Solange die Internet-Adressen der Protokolldateien nicht anonymisiert gespeichert werden, habe ich die **Deaktivierung der Protokolldateien** gefordert.

1.4.1.5 Bürokommunikation mit GroupWise

Das Bürokommunikationssystem GroupWise wird von vielen Behörden des Landes eingesetzt. Mit diesem Programm können u. a. Nachrichten ausgetauscht und Termine abgestimmt werden.

Die Stärke der im Bürokommunikationssystem GroupWise eingesetzten Verschlüsselungsverfahren ist als „niedrig" einzuschätzen, solange die verwendeten **kryptographischen Verfahren** sowie die Schlüsselverwaltung von der Herstellerfirma nicht offengelegt werden oder sich herausstellen sollte, daß die in GroupWise verwendeten Verfahren nicht dem Stand der Technik entsprechen. Auch aufgrund der sehr stringenten amerikanischen Exportbeschränkung für starke kryptographische Verfahren ist derzeit davon auszugehen, daß in GroupWise nur schwache Verschlüsselungsverfahren implementiert sind.

Da aufgrund der Verwendung schwacher kryptographischer Verfahren die Vertraulichkeit der im Landesverwaltungsnetz übertragenen Daten nicht sichergestellt werden kann, dürfen derzeit keine personenbezogenen Daten der Schutzstufen B und C übermittelt werden. Die Übertragung personenbezogener Daten der Stufe A kann für einen gewissen Zeitraum hingenommen werden. Das Ziel muß jedoch sein, zukünftig alle personenbezogenen Daten, die im Landesverwaltungsnetz übertragen werden, mit Hilfe von dem Stand der Technik entsprechenden Verfahren zu verschlüsseln und digital zu signieren.

---

[10] s. 4. Tätigkeitsbericht unter 1.4.2

[11] s. unter 1.5.2

1.4.1.6 Verfahren Haushalts-, Kassen- und Rechnungswesen

Bei der Prüfung einer Landesbehörde stellte ich u. a. fest, daß beim Haushalts-, Kassen- und Rechnungswesen-Verfahren (HKR-Verfahren) Daten unverschlüsselt über das Landesverwaltungsnetz übertragen werden.

Im Sicherheitskonzept zum Fachnetz LDS wurde u. a. festgestellt, daß die im HKR-Verfahren verarbeiteten personenbezogenen Daten der Stufe C unseres Schutzstufenkonzeptes zuzuordnen sind. Daraus resultiert, daß die im Landesverwaltungsnetz übertragenen personenbezogenen **HKR-Daten mit sicheren kryptographischen Verfahren** zu **verschlüsseln** sind[12]. Ich habe daher das für das Fachverfahren zuständige Ministerium der Finanzen gem. § 25 Abs. 2 BbgDSG aufgefordert, folgende technisch-organisatorischen Maßnahmen umzusetzen:

- Verschlüsselung der beim HKR-Verfahren über das Landesverwaltungsnetz per Filetransfer übertragenen personenbezogenen Daten bis spätestens zum Ende des Jahres 1998,

- Verschlüsselung der beim HKR-Verfahren auf den Servern gespeicherten personenbezogenen Daten bis spätestens zum Ende des Jahres 1998,

- Verschlüsselung der beim HKR-Verfahren über das Landesverwaltungsnetz per Terminalemulation übertragenen personenbezogenen Daten bis spätestens zum Ende des Jahres 1999.

Aufgrund der Verarbeitung sensibler personenbezogener Daten ist das **lokale Netz** der HKR-Daten verarbeitenden Behörde **durch eine Firewall** zu schützen.[13]

1.4.2 TeleKommunikationsverbund der obersten Landesbehörden

1.4.2.1 Neue Software zur Gebührendatenverarbeitung

[12] s. 5. Tätigkeitsbericht, Anlage 3 (Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9. Mai 1996)

[13] s. unter 1.4.1.1

In meinem letzten Tätigkeitsbericht[14] beanstandete ich nach einer umfangreichen Kontrolle der zentralen Telekommunikation-Anlage (TK-Anlage) des TK-Verbundes der obersten Landesbehörden die dort genutzte Software zur **Gebührendatenverarbeitung**. In Gesprächen mit der Staatskanzlei als verantwortlichem Betreiber des TK-Verbundes konnte ich erreichen, daß sich die Landesregierung meine Beanstandungen zu eigen gemacht und sich nach Verhandlungen mit Vertretern der Lieferfirma der zentralen TK-Anlage unter Beteiligung meiner Behörde zu einem etappenweisen Austausch der Software für die Gebührendatenverarbeitung entschlossen hat.

Einem von mir angeforderten Zwischenbericht der Staatskanzlei vom Februar 1998 zum aktuellen Stand konnte ich entnehmen, daß die erforderlichen Arbeiten noch im zweiten Quartal 1998 abgeschlossen werden. In diesem Bericht wird zur neuen Software u. a. folgendes gesagt: „Die umfangreichen Datensätze werden bis auf die ausschließlich zur Gebührenberechnung notwendigen Einzeldaten automatisch beim Anfall gelöscht. Durch einen gesonderten Eingabebefehl wird die Löschung dieser Einzelverbindungsdaten nur verhindert, wenn ein schriftlicher Antrag eines Ressorts zur befristeten und stichprobenartigen Überprüfung dienstlicher Telefonate laut Dienstvereinbarung mit den Personalräten vorliegt oder wenn ein Nutzer schriftlich den Einzelausweis privater Telefonate mit der Gebührenabrechnung beantragt hat. ... Es kann abschließend davon ausgegangen werden, daß der vom Datenschutzbeauftragten des Landes auf der Basis seines Prüfberichtes geforderte, bessere Schutz personenbezogener Daten beim Betrieb des TK-Verbundes der obersten Landesbehörden mit der Umrüstung der neuen GDV (Gebührendaten-verarbeitung) auf das Betriebssystem Windows 95 gewährleistet wird. Gleichzeitig wird der **Dienstvereinbarung** mit den Personalräten zur Betreibung des TK-Verbundes vollständig entsprochen."

Ausdrücklich begrüße ich die Entscheidung der Staatskanzlei zum Einsatz der datenschutzfreundlichen Software für die Gebührendatenverarbeitung. Bereits jetzt ist erkennbar, daß auch untergeordnete Landesbehörden dem Beispiel der Staatskanzlei folgen und diese Software, die sich im übrigen auch in mehreren Bundesministerien im Einsatz befindet, nutzen möchten.

1.4.2.2 Praxis der Telefonabrechnung verschiedener Ministerien

In drei ausgewählten Ministerien, die am zentralen TK-Verbund der obersten Landesbehörden teilhaben, überprüfte ich die Vorgehensweise bei der Gebührenabrechnung. Mein Kontrollziel bestand ausschließlich darin, festzustellen, inwieweit in diesen Einrichtungen die in der allgemeinen Verwaltungsvorschrift über die Einrichtung und Benutzung dienstlicher TK-Anlagen für die Verwaltung des Landes Brandenburg (Dienstanschlußvorschrift - **DAV**)[15] und die in der betreffenden Dienstvereinbarung mit dem Personalrat **über die Nutzung der ISDN-Telekommunikationsanlage** des Telekommunikationsverbundes der obersten Landesbehörden des Landes Brandenburg enthaltenen Vereinbarungen zur Abrechnung von Privatgesprächen und zur Überprüfung der Daten von dienstlichen Gesprächen eingehalten werden.

Abrechnung von Privatgesprächen

[14] s. 5. Tätigkeitsbericht unter 1.6.3

[15] vom 30. November 1993, ABl. S. 1775

Die Abrechnung der Privatgespräche erfolgt nach einer Zahlungsliste der zentralen TK-Anlage bei der Staatskanzlei. Zusätzlich hat jeder Beschäftigte die Möglichkeit, einen Einzelgebührennachweis mit der um die letzten drei Ziffern gekürzten Zielrufnummer anzufordern, der ihm im verschlossenen Umschlag direkt zugestellt wird. Um den laufenden Aufwand für den Einzug der Telefongebühren zu reduzieren, wird in einigen Ministerien gegenwärtig von einer monatlichen auf eine vierteljährliche Abrechnung übergegangen. Da von der Staatskanzlei aber weiterhin nur monatliche Listen kommen, erstellt ein Mitarbeiter des Ministeriums daraus eine Quartalsliste, auf deren Grundlage die Einzahlung der Telefongebühren erfolgt. Eine Verlängerung der Speicherfristen der Verbindungsdaten ist mit diesem neuen Abrechnungsverfahren nicht verbunden, da die Einzelverbindungsnachweise für die Privatgespräche weiterhin monatlich an die Beschäftigten versandt werden. Aus Datenschutzgründen wäre auch nichts dagegen einzuwenden, wenn die Speicherfrist entsprechend dem quartalsmäßigen Abrechnungszeitraum angemessen verlängert würde, was allerdings auch eine Anpassung der o. g. Vorschriften erfordert.

Die mit dem Wegfall der Freigrenze von 5,- DM monatlich bei der Bezahlung von Privatgesprächen auftretenden Kuriositäten, wonach z. T. für private Telefongebühren von 0,12 DM monatlich ein unvertretbarer Verwaltungsaufwand zum Gebühreneinzug betrieben wird, können nicht dem Datenschutz angelastet werden. Hier sollte der Glaubwürdigkeit halber ein vernünftiger Kompromiß gesucht werden.

Beim Einzug der Gebühren für die Privatgespräche konnte ich keinerlei Mängel bezüglich des Datenschutzes feststellen.

Überprüfung von Dienstgesprächen

Eine mißbräuchliche Nutzung des dienstlichen Telefonanschlusses liegt u. a. dann vor, wenn ein Mitarbeiter ein Privatgespräch führt, es aber nicht als ein solches kennzeichnet und demzufolge die Kosten dafür seinem Arbeitgeber anlastet. Um dem entgegenzuwirken, ohne eine vollständige Überwachung des Telekommunikationsverhaltens von Beschäftigten zu ermöglichen, wurde in § 7 der Dienstvereinbarung in begrenztem Umfang eine stichprobenartige Kontrolle dienstlicher Gespräche vorgesehen. In diesem Rahmen ist es dann erlaubt, die kompletten Verbindungsdaten einschließlich der vollständigen Rufnummer des angerufenen Teilnehmers zu speichern, auszudrucken und einer geeigneten Überprüfung zu unterziehen. Der organisatorische Ablauf dieser Kontrollen wurde von der Staatskanzlei als verantwortlichem Betreiber des zentralen TK-Verbundes detailliert festgelegt.

Dieses Kontrollinstrumentarium wird in den überprüften Ministerien sehr unterschiedlich genutzt. So lehnte beispielsweise ein Ministerium derartige Kontrollen grundsätzlich ab, da sie ihm ungeeignet erschienen, alle Mißbrauchsmöglichkeiten lückenlos aufzudecken. Statt der regelmäßigen stichprobenartigen Kontrollen schlug das betreffende Ministerium in größeren Zeitabständen eine einmalige gründliche, vollständige und möglichst flächendeckende Kontrolle aller dienstlichen Telefongespräche vor. Ich legte dar, daß der in der DAV und in der Musterdienstvereinbarung festgelegte Kontrollmechanismus für alle am TK-Verbund beteiligten Landesbehörden gilt und von mir als datenschutzgerecht beurteilt wird und daß ich für neue weniger datenschutzgerechte Regelungen mit einzelnen Ressorts keinen Anlaß sehe. In der Antwort auf meinen Prüfbericht teilte das betreffende Ministerium allerdings mit, daß es in Zukunft doch auf die vereinbarten Kontrollen zurückgreifen werde.

Demgegenüber nimmt das Ministerium der Finanzen (MdF) die stichprobenartigen Kontrollen dienstlicher Gespräche im zulässigen Rahmen in vorbildlicher Weise wahr. Durch eine regelmäßige stichprobenartige Überprüfung der Daten dienstlicher Gespräche und einer sachlichen Bearbeitung von Verstößen gegen die Vorschriften zur Nutzung der TK-Anlage, ist es dort gelungen eine Atmosphäre zu schaffen, die die Beschäftigten zur Ehrlichkeit im Umgang mit der

TK-Anlage geradezu anspornt. Damit gibt das MdF auch ein Beispiel dafür, daß mit den mit meiner Behörde abgestimmten datenschutzfreundlichen Regelungen in der DAV und der Musterdienstvereinbarung einer mißbräuchlichen Nutzung der TK-Anlage effektiv entgegengewirkt werden kann.

Insgesamt konnte ich bei der Überprüfung der Daten von dienstlichen Gesprächen keine datenschutzrechtlichen Verstöße feststellen. Dies ist sicher auch darauf zurückzuführen, daß die Staatskanzlei den organisatorischen Umgang mit den zulässigen Kontrollen in sehr detaillierter Form empfohlen hatte.

1.4.5 Kryptographie - der Schlüssel für sichere Daten

1.4.5.1 Folgenminderung bei Einbrüchen in Kommunalverwaltungen

Im Berichtszeitraum traten vermehrt Einbrüche bei brandenburgischen Kommunalverwaltungen auf. In einigen Fällen waren es Mitarbeiter dieser Verwaltungen, die aus diesem Anlaß um eine Beratung vor Ort baten. Ich werte dies als weiter gestiegene Sensibilität in Sachen Datenschutz und als Vertrauensbeweis für meine Behörde. In anderen Fällen entnahm ich Zeitungsmeldungen und Petitionen entsprechende Hinweise.

Ortsbesichtigungen ergaben, daß sowohl **Arbeitsplatz-PC als auch Server** entwendet worden waren. In einer Reihe von ähnlich gelagerten Fällen sind aber auch die Festplatten der Server fachmännisch ausgebaut worden. Darauf werden regelmäßig auch personenbezogene Daten mehrerer Fachämter gespeichert, eigentlich eine an sich sinnvolle Maßnahme im Hinblick auf eine zentrale Datensicherung. Vornehmlich wurden dabei Daten des Meldeamtes, des Sozialamtes, des Gewerbeamtes, der kommunalen Betreuung, der Schulverwaltung sowie Daten über Ordnungswidrigkeiten entwendet. Es ist mir bisher kein Fall bekannt geworden, daß Täter polizeilich ermittelt werden konnten.

Häufig ist die Lage der Dienstgebäude so, daß selbst bei **Raumüberwachung und Aufschaltung zu Wachschutzdiensten oder der Polizei** ein rechtzeitiges Eingreifen wegen der Weiträumigkeit des Flächenlandes Brandenburg nicht möglich ist. Weil also derartige Einbrüche offensichtlich kaum verhindert werden können und andererseits alle genannten Daten von erheblicher Sensibilität sind, habe ich in allen Fällen empfohlen, Verschlüsselungssoftware einzusetzen, die im allgemeinen auch recht preiswert zu erhalten ist. Wenn diese auf anerkannten anspruchsvollen kryptographischen Verfahren beruhen, sind die Daten so gut geschützt, daß sie von dem Täter nicht gelesen werden können. Zwar ist dann der materielle Schaden immer noch erheblich, wenn keine entsprechende Versicherung abgeschlossen wurde, zumindest aber bleibt die Vertraulichkeit der personenbezogenen Daten gesichert. Ich würde es begrüßen, wenn sich die Landesregierung dieses Problems stärker als bisher annähme und zu dessen Lösung geeignete Vorgaben bzw. Empfehlungen gäbe.

1.4.5.2 Verschlüsselung der Daten beim Wohngeldverfahren

Bereits früher[16] hatte ich über die Einführung eines Wohngeldverfahrens im Land berichtet und gefordert, daß alle **personenbezogenen Daten** des Wohngeldverfahrens beim Transport per Diskette - unabhängig von der Versandform - und bei der Übertragung in Netzwerken **in geeigneter Weise** zu **verschlüsseln** sind.

Das LDS hat sich seither intensiv mit geeigneten kryptographischen Verfahren auseinandergesetzt, so daß nach einer Testphase im Oktober 1997 meine Forderung nach Verschlüsselung der personenbezogenen Daten beim

[16] s. 3. Tätigkeitsbericht unter 9.1.3 und 9.1.4

Diskettentransport und beim Filetransfer erfüllt werden konnte. Verwendet wird dabei die kryptographische Software Pretty Good Privacy (PGP). Mit Hilfe dieser Software werden die personenbezogenen Daten verschlüsselt und dann per Diskette oder per Filetransfer von der jeweiligen Wohngeldstelle zum LDS zur weiteren Verarbeitung übermittelt. Die Verschlüsselung der Daten beruht auf asymmetrischen und symmetrischen Verfahren. Als symmetrisches Verfahren wird IDEA und als asymmetrisches wird RSA mit einer Schlüssellänge von 1024 Bit eingesetzt. Die zur Verschlüsselung benötigten öffentlichen Schlüssel werden vom Trust Center des LDS zertifiziert. Ein Wechsel der asymmetrischen Schlüssel erfolgt jährlich.

Die an das Landesverwaltungsnetz angeschlossenen Wohngeldstellen können, mit Hilfe der im Wohngeldverfahren implementierten Terminalemulation, Rechenergebnisse vom Großrechner des LDS abfragen. Die dabei über das Landesverwaltungsnetz übertragenen personenbezogenen Daten werden derzeit noch nicht verschlüsselt.

Die Verschlüsselung der Daten beim File- und Diskettentransfer unter Verwendung sicherer kryptographischer Verfahren ist ein positives Beispiel für die Durchsetzung der Forderungen des Datenschutzes nach **Einsatz datenschutzfreundlicher Technologien**. Mit Hilfe kryptographischer Verfahren kann der Schutz von personenbezogenen Daten bei der Übertragung im Landesverwaltungsnetz auf hohem Niveau sichergestellt werden.

1.5 Neue Technologien

1.5.1 Risiken bei der Nutzung von Handys

Mein 3. Tätigkeitsbericht[17] enthält Ausführungen zur Sicherheit in der **Mobilkommunikation**. Darin habe ich, ausgehend von den bei der Kommunikation anfallenden Daten, Forderungen für den datenschutzgerechten Betrieb der Mobilfunknetze aufgestellt.

Handys sind heute längst zum Massenartikel geworden und aus dem täglichen Leben nicht mehr wegzudenken. Die mobilen Sprach- und Datenübertragungsdienste schaffen - für jeden nachvollziehbar - willkommene Mobilität, Erreichbarkeit an fast jedem beliebigen Ort und Bequemlichkeit. Gerade diese Eigenschaften erlauben aber auch den Mißbrauch von Handys. Damit der Nutzer solchen Gefahren entgegentreten und sein Verhalten darauf einstellen kann, möchte ich hier auf einige Mißbrauchsmöglichkeiten hinweisen:

- Handys bieten durch geschickte Auswahl von Leistungsmerkmalen und den Einsatz handelsüblicher Zusatzgeräte hervorragende Möglichkeiten, Gespräche in ihrem Umfeld meist unbemerkt abzuhören.

- Neue Techniken (sog. IMSI-Catcher) ermöglichen es, über Handys geführte Telefonate gezielt mitzuhören oder aufzuzeichnen; dazu lassen sich vom Netzbetreiber vorgesehene Verschlüsselungsmöglichkeiten für den Nutzer unbemerkbar ausschalten.

- Die Standortinformationen der Kommunikationspartner lassen sich zur Bildung detaillierter Bewegungsprofile mißbrauchen. Die betreffenden Informationen liegen bereits bei einem eingeschalteten Handy vor, das Führen eines Telefongespräches ist dazu nicht erforderlich.

[17] s. unter 1.4.3

Bezüglich weiterer Mißbrauchsmöglichkeiten von Handys verweise ich auf ein gemeinsames Informationsblatt[18] aus Mecklenburg-Vorpommern und Nordrhein-Westfalen mit dem Titel „Handys - Komfort nicht ohne Risiko", das im Auftrag der Konferenz der Datenschutzbeauftragten des Bundes und der Länder konzipiert wurde. Es kann über meine Behörde kostenlos bezogen werden.

1.5.2 Neue Vorschriften bei Telekommunikations-, Tele- und Mediendiensten

Während der Nutzer im einseitigen Kommunikationsprozeß des klassischen Rundfunks und Fernsehens keine Datenspuren hinterläßt, sind diese in Multimediadiensten[19] vielfältig und aussagekräftig, denn bei der **Nutzung der modernen Informations- und Kommunikationstechnologie** fallen große Mengen personenbezogener Daten an. Die Betreiber müssen Stammdaten über die Teilnehmer ihrer Anschlüsse und die von ihnen genutzten Dienste speichern. Für die technische Abwicklung der Verbindung ist die Verarbeitung der Teilnehmernummern und der genutzten Dienste als Verbindungsdaten erforderlich. Als Nutzungsdaten fallen Daten über in Anspruch genommene Angebote, den Zeitpunkt, die Zeitdauer und andere leistungsbezogene Informationen an. Aus Stamm-, Verbindungs- und Nutzungsdaten werden in mehreren Verarbeitungsschritten die Abrechnungsdaten erstellt. Durch solche Datenverarbeitungen können sehr sensible Datensammlungen entstehen und bisher anonym gebliebene Lebenssachverhalte mit ihrer Hilfe individuell zugeordnet werden - wie der Umfang der Mediennutzung, die Beteiligung an Lernprogrammen, das Blättern in Waren- oder Reisekatalogen und Aussagen über die Kreditwürdigkeit oder den Gesundheitszustand des Nutzers. Diese Daten können in vernetzten Systemen aufbereitet, zusammengeführt, abgeglichen, kontrolliert und zu **Interessen- oder Persönlichkeitsprofilen** zusammengestellt werden - der gläserne Medienkonsument wäre damit perfekt. Die drei neuen gesetzlichen Regelungen

- das Telekommunikationsgesetz (**TKG**)[20],
- das Informations- und Kommunikationsdienstegesetz (**IuKDG**)[21] und
- der Mediendienste-Staatsvertrag[22]

enthalten jedoch Regelungen, die geeignet sind, dem entgegen zu wirken.

Die Antwort auf die Frage, welches der drei Gesetze jeweils zur Anwendung kommt, erfordert eine eindeutige Zuordnung der betreffenden Dienste zu Telekommunikationsdienstleistungen, Telediensten oder Mediendiensten. Eine derartige Zuordnung ist bei den neuen Diensten in vielen Fällen nicht möglich, da es zu Überlagerungen kommt. Deshalb muß man feststellen, daß der Gesetzgeber sein ursprüngliches Ziel, einen einheitlichen Rechtsrahmen für die Informations- und Kommunikationstechnik in Deutschland zu schaffen, nicht voll erfüllt hat.

---

18 s. Anlage 15

19 s. 4. Tätigkeitsbericht unter 1.5.1

20 vom 25. Juli 1996, BGBl. I S. 1120

21 vom 22. Juli 1997, BGBl. I S. 1870

22 vom 12. Februar 1997, GVBl. I S. 76

Telekommunikationsgesetz (TKG)

Entsprechend der Begriffsdefinition in § 3 Nr. 6 TKG handelt es sich bei der Telekommunikation um das „Aussenden, Übermitteln und Empfangen von Nachrichten jeglicher Art in Form von Zeichen, Sprache, Bildern oder Tönen mittels Telekommunikationsanlagen". Deshalb geht es hier nicht um die Aufbereitung oder Verwendung von übertragenen Inhalten, sondern um den reinen technischen Vorgang der Übertragung. Dies ist hinsichtlich der Unterscheidung von Telekommunikationsdiensten einerseits und Telediensten sowie Mediendiensten andererseits von wesentlicher Bedeutung, wobei von der Einordnungslogik her außer acht gelassen werden muß, daß sowohl Rundfunk als auch Medien- und Teledienste meist unter Nutzung von Telekommunikationsanlagen erbracht werden.

Neu in das TKG aufgenommen wurde, daß Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbringen, die personenbezogenen Daten ihrer Kunden nur noch dann für Zwecke der Werbung, Kundenberatung oder Marktforschung nutzen dürfen, wenn der Kunde eingewilligt hat. Die Eintragung der Kundendaten in öffentliche gedruckte oder elektronische Verzeichnisse erfolgt nur, soweit der Kunde dies beantragt hat. Die Betroffenen können selbst bestimmen, ob und welche Angaben in den Kundenverzeichnissen veröffentlicht werden sollen. Damit wird es möglich, die entsprechenden Angaben zwar in gedruckten, nicht aber in elektronischen **Verzeichnissen (CD-ROM)**[23] veröffentlichen zu lassen.

Neu ist auch eine Vorschrift, die Anbieter von Telekommunikationsdiensten zur Führung von Kundendateien verpflichtet, auf die Gerichte und Staatsanwaltschaften, die Polizei, die Zollbehörden und die Nachrichtendienste durch ein automatisiertes Abrufverfahren nahezu schrankenlos zugreifen können. Datenschutzrechtlich besonders brisant ist die Tatsache, daß die Diensteanbieter den Zugriff der Sicherheitsbehörden so zu gestalten haben, daß er unbemerkt erfolgen kann. Dies widerspricht allerdings allen bisher in anderen Rechtsbereichen vorgesehenen Sicherheitsvorkehrungen und Kontrollpflichten der datenverarbeitenden Stellen beim Online-Zugriff auf Daten und verhindert, daß befugte Datenzugriffe von unbefugten Zugriffen unterschieden werden können.

Die Vorschriften über die Kontrolle des Datenschutzes im Geltungsbereich des **TKG** wurden insofern verändert, als nunmehr der Bundesbeauftragte für den Datenschutz als zentrale Stelle für die Kontrolle der Einhaltung von Datenschutzbestimmungen zuständig ist. Für das Angebot von Telekommunikationsdienstleistungen durch öffentliche Stellen der Länder bleiben jedoch auch weiterhin die Landesbeauftragten für den Datenschutz zuständig.

Informations- und Kommunikations-Gesetz

Mit dem als Artikelgesetz vorliegenden Informations- und Kommunikations-Gesetz (IuKDG)[24], in der Presse zumeist als „Multimedia-Gesetz" bezeichnet, wurden neben einer Reihe von Änderungen bereits bestehender Gesetze (Anpassung des Strafrechts, Jugendrechts, Verbraucherschutzrechts und des Urheberrechts) drei neue Gesetze geschaffen:

- das Teledienstegesetz (**TDG**),
- das Tledienstedatenschutzgesetz (**TDDSG**) und
- das Signaturgesetz (**SigG**).

---

23 s. 4. Tätigkeitsbericht unter 1.5.5

24 vom 22. Juli 1997, BGBl. I S. 1870

Das Teledienstegesetz gilt für alle elektronischen Informations- und Kommunikationsdienste, die für eine individuelle Nutzung bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt, dazu gehören beispielsweise Dienste wie elektronische Post, Telebanking, Telearbeit, Telemedizin und Fernlernen.

Die Vorschriften des TDDSG sind aus der Sicht des Datenschutzes als sehr fortschrittlich zu bewerten. Darin werden die Diensteanbieter erstmals verpflichtet, die technischen Einrichtungen für Teledienste so zu gestalten, daß keine oder so wenig personenbezogene Daten wie möglich erhoben und verarbeitet werden. Ferner hat der Diensteanbieter dem Nutzer die Inanspruchnahme von Telediensten und ihrer Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Die **Erstellung von Nutzungsprofilen** ist nur bei Verwendung von Pseudonymen zulässig, wobei eine spätere Zusammenführung des Nutzungsprofils mit dem tatsächlichen Nutzer ausdrücklich untersagt wird; damit ist der Erstellung von personenbezogenen Nutzer- und Verhaltensprofilen wirksam vorgebeugt. Mit dem neuen Multimediagesetz übernahm der Gesetzgeber eine gewisse Vorreiterrolle zur weiteren Entwicklung des Datenschutzrechts. Da die gleichen datenschutzrechtlichen Bestimmungen im wesentlichen auch in den auf Länderebene geltenden Mediendienste-Staatsvertrag übernommen wurden, konnte ein einheitlich hohes Datenschutzniveau auch auf diesen Bereich übertragen werden.

1.5.3 Sicherheit bei der Telearbeit

Im Zuge meiner Kontrolltätigkeit stellte ich fest[25], daß im Land Brandenburg erste Pilotprojekte zur Telearbeit realisiert werden. Ich möchte daher im folgenden auf datenschutzrechtliche Aspekte dieser doch relativ neuen Arbeitsform eingehen.

Es sind verschiedene Formen der Telearbeit zu unterscheiden. Während der Mitarbeiter bei der **Teleheimarbeit** ausschließlich zu Hause arbeitet, behält er bei der **alternierenden Telearbeit** seinen behördlichen Arbeitsplatz auch weiterhin. Er wechselt quasi nach Bedarf zwischen seinem Heimarbeitsplatz und seinem Arbeitsplatz in der jeweiligen Dienststelle. Eine weitere Variante ist die **mobile Telearbeit**. Bei dieser Form wird die Verbindung zu IT-Systemen der Dienststelle von wechselnden Standorten aus hergestellt. Anwendungsfälle der mobilen Telearbeit könnten z. B. Schulungsmaßnahmen und Präsentationen sowie Abfragen der persönlichen Mailbox sein.

Bei allen Formen der Telearbeit halte ich besonders folgende technisch-organisatorische Maßnahmen gem. § 10 BbgDSG für erforderlich:

- Es findet **keine Datenverarbeitung im Auftrag** gem. § 11 BbgDSG statt. Der Telearbeiter bleibt weiterhin Bediensteter seiner Behörde. Die betroffene Dienststelle bleibt datenverarbeitende Stelle im Sinne von § 3 Abs. 4 Nr. 1 BbgDSG.

[25] s. unter 3.6.4.2

- Aufgrund der erhöhten Sicherheitsrisiken dürfen **keine sensiblen personenbezogenen Daten** (Schutzstufe C)[26] auf dem Telearbeitsplatzcomputer verarbeitet werden.

- Werden personenbezogene Daten zwischen dem Telearbeitsplatz und der jeweiligen Dienststelle übertragen, sind diese grundsätzlich mit sicheren kryptographischen Verfahren zu verschlüsseln und digital zu signieren.

- In einer **Dienstanweisung** sind die erforderlichen technisch-organisatorischen Maßnahmen festzuschreiben und der Telearbeiter muß sich schriftlich zur Einhaltung dieser geforderten Maßnahmen verpflichten.

- Zum Schutz der zentralen Netzzugänge ist die Erstellung eines Sicherheitskonzeptes unabdingbar.

- Die **Abschottung der zentralen Netzzugänge** ist mit Firewallsystemen sicherzustellen. Die Paßwörter sind über Weitverkehrsnetze grundsätzlich nur verschlüsselt zu übertragen.

- Es dürfen **nur dienstliche Arbeitsplatzcomputer** (APC) eingesetzt werden.

- Der APC darf **nur für dienstliche Aufgaben** genutzt werden.

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

- Leistungs- bzw. Verhaltenskontrollen dürfen nur vorgenommen werden, wenn eine entsprechende Dienstvereinbarung gem. § 65 PersVG[27] zwischen Arbeitgeber und Personalrat dies ausdrücklich zuläßt.

- Es sind nur die unbedingt erforderlichen personenbezogenen Daten im Telearbeitsplatzcomputer zu verarbeiten. Personenbezogene Daten sollten nach Möglichkeit vor der Verarbeitung anonymisiert bzw. pseudonymisiert werden.

Zusätzlich halte ich folgende Maßnahmen bei der Teleheimarbeit für erforderlich:

- Die **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 Telearbeiter kann nur freiwillig in entsprechende Kontrollen einwilligen. Ohne schriftliche Einwilligung des Betroffenen ist die Telearbeit grundsätzlich abzulehnen.

- Gem. § 65 Nr. 4 PersVG ist das **Mitbestimmungsrecht des Personalrats** bei der Einrichtung vom Heimarbeitsplätzen zu berücksichtigen.

---

[26] s. Fn. 6

[27] vom 15. September 1993, GVBl. I S. 358

Abschließend sei angemerkt, daß die Einrichtung von Telearbeitsplätzen aus Sicht des Datenschutzes grundsätzlich als problematisch anzusehen ist. Denn trotz der hier dargestellten zusätzlichen technischen und organisatorischen Maßnahmen ist davon auszugehen, daß eine vergleichbare Sicherheit wie bei Behördenarbeitsplätzen nicht erreicht werden kann und damit ein höheres Restrisiko immer bestehen bleibt. Es ist deshalb schon vor der Einrichtung solcher Telearbeitsplätze genauestens zu prüfen, ob die Erforderlichkeit wirklich gegeben ist.

1.5.4 Kryptographie - der Schlüssel für sichere Daten

Zum Stand der Diskussion um eine gesetzliche Reglementierung des Einsatzes von kryptographischen Verfahren bei der Datenübertragung in Weitverkehrsnetzen hatte ich mich zuletzt in meinem 5. Tätigkeitsbericht[28] geäußert. Im April 1997 fand der 5. Deutsche IT-Sicherheitskongreß des Bundesamtes für Sicherheit in der Informationstechnik (BSI) unter dem etwas doppeldeutigen Motto „Mit Sicherheit in die Informationsgesellschaft" statt. Dort und an anderer Stelle wurde auch über das Für und Wider einer Kryptoregulierung diskutiert. Ein **sog. Kryptogesetz** ist bisher noch nicht vorgelegt worden: Proteste von Unternehmen der Privatwirtschaft, von Datenschutzbeauftragten, von Bundestagsabgeordneten und von vielen engagierten Bürgern, aber auch kritische Töne aus dem Bundeswirtschafts- und dem Bundesjustizministerium haben dies bisher verhindert, weil die angedachten Regelungen insgesamt unausgereift waren.

Inzwischen soll aber das Bundesinnenministerium über das BSI die Firma Siemens mit der Entwicklung eines sog. Krypto-Chips (Codename „Pluto") beauftragt haben[29]. Mit diesem elektronischen Baustein sollen später E-Mails an öffentliche Stellen verschlüsselt werden. Äußerst problematisch ist allerdings, daß die verschlüsselten Daten mittels eines „Nachschlüssels" gelesen werden können. Das Ziel dieses Verfahrens soll langfristig zusätzlich darin bestehen, daß auch die Daten der Bürger und der Privatunternehmen nur mit diesem Chip für die Kommunikation im Internet verschlüsselt werden dürfen. Praktisch würde dies tatsächlich den „Großen Lauschangriff" auf die **Weitverkehrsnetze** darstellen und den Überwachungsstaat durch den Einsatz einer „Internet- oder Datenpolizei" komplettieren.

---

28 s. unter 1.3.3

29 s. „Spiegel" Nr. 8 vom 16.02.1998, S. 22; „Computerwoche" 8/1998, S. 6

Sowohl das BSI als auch Siemens haben dazu erklärt[30], daß nicht beabsichtigt sei, etwaige Hintertüren in den Krypto-Chip einzubauen. Aus Sicherheitsaspekten werden derartige Maßnahmen abgelehnt. Allerdings würde technisch eine solche Regelung genauso leicht unterlaufen werden können wie ein generelles Krypto-Verbot. Denn etwa mit Hilfe der **Steganographie** können Daten durch Verstecken in anderen Daten so verschlüsselt werden, daß ein Dritter dies nicht bemerken kann. Allein durch diese Tatsache der Nichteignung wäre eine solche Überwachungsmöglichkeit bereits verfassungsrechtlich unzulässig, weil sie nicht verhältnismäßig ist. Sie ist auch deshalb unverhältnismäßig, weil hier jedermann einer Strafverfolgungsmaßnahme unterworfen werden könnte, ohne daß ein konkreter Anlaß vorliegt. Sie hätte auch erhebliche Auswirkungen auf Geschäfts- und Betriebsgeheimnisse, die nicht mehr wirkungsvoll geschützt wären. Dies hätte einen deutlichen Wettbewerbsnachteil zur Folge. Deshalb sollten die Verschlüsselungsmöglichkeiten für alle Interessierten völlig frei sein. Eine sichere **Kryptographie ohne Zugriffsmöglichkeit** für Staat oder sonstige Dritte ist der beste Schutz für Bürger, staatliche Verwaltung und Wirtschaft.

2 Allgemeiner Datenschutz

2.1 Brandenburg - das erste Bundesland mit einem Akteneinsichtsrecht

Die Väter und Mütter der Verfassung des Landes Brandenburg haben sich aufgrund ihrer persönlichen Erfahrungen (mehrheitlich ehemalige DDR-Bürger) für die Aufnahme eines Allgemeinen Akteneinsichtsrechts in die Verfassung (Art. 21 Abs. 4) eingesetzt. Sie haben damit einen Schlußstrich unter die jahrzehntelange Diskussion in der alten Bundesrepublik gezogen, ob das Prinzip der Amtsverschwiegenheit noch einem demokratischen Staatswesen entspricht[31]. Zudem hat sich das Bundesverfassungsgericht zu den Grundvoraussetzungen der demokratischen Meinungs- und Willensbildung wie folgt geäußert: „Es gehört zu den elementaren Bedürfnissen des Menschen, sich aus möglichst vielen Quellen zu unterrichten, das eigene Wissen zu erweitern und sich so als Persönlichkeit zu entfalten. Zudem ist in der modernen Industriegesellschaft der Besitz von Informationen von wesentlicher Bedeutung für die soziale Stellung des einzelnen. Das Grundrecht der Informationsfreiheit ist wie das Grundrecht der freien Meinungsäußerung eine der wichtigsten Voraussetzungen der freiheitlichen Demokratie“[32]. „Erst mit seiner Hilfe wird der Bürger in den Stand gesetzt, sich selbst die notwendigen Voraussetzungen zur Ausübung seiner persönlichen und politischen Aufgaben zu verschaffen, um im demokratischen Sinne verantwortlich handeln zu können“[33]. Die 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 23./24. Oktober 1997 in Bamberg setzte sich auf der Grundlage eines unter meiner Federführung erstellten Thesenpapiers[34] mit den Grenzen eines allgemeinen Informationszugangsrechts auseinander.

Bereits im vorigen Tätigkeitsberichten hatte ich mich zum Stand des Gesetzgebungsverfahrens geäußert.[35] Auf beharrliches Drängen des Landtags legte die Landesregierung im Berichtszeitraum einen Gesetzentwurf[36] vor, zu dem der

30 s. Computermagazin c`t 1998, Heft 6, S. 94

31 Lodde, St.: Informationsrechte des Bürgers gegen den Staat, C. Heymanns Verlag KG Köln, 1996

32 BVerfGE 7, 198, 208

33 BVerfGE 27, 71, 81

34 s. Anlage 6 (DuD 1998, S. 32)

35 s. 5. Tätigkeitsbericht unter 2.3.1

36 zu einem Akteneinsichtsrechtsgesetz: LT-Drs. 2/4417 vom 2. September 1997

Innenausschuß des Landtags im Dezember 1997 eine Anhörung durchführte[37]. Neben anderen Fachleuten hatte ich dabei Gelegenheit, mich anhand eines Fragenkatalogs sowohl zum Gesetzentwurf selbst als auch zu allgemeinen Problemen zum Akteneinsichtsrecht, wie z. B. vergleichbare Gesetzesvorhaben in anderen Bundesländern, Erfahrungen mit dem Akteneinsichtsrecht anderer Länder, Verkauf von Informationen der Verwaltung, Entwicklung neuer Wirtschaftszweige, Auswirkungen auf archivrechtliche Bestimmungen, zu äußern. Die parlamentarische Behandlung des Gesetzentwurfs, vor allem die Anhörung, haben dazu geführt, daß das Gesetz vom Landtag mit umfangreichen Änderungen inzwischen als Akteneinsichts- und Informationszugangsgesetz (AIG) in Kraft getreten ist[38].
Trotzdem ist mit dem AIG aus Ängstlichkeit nur eine äußert restriktive Form für ein Akteneinsichts- und Informationszugangsrecht gewählt worden. Dies geht im wesentlichen auf Befürchtungen und Warnungen zurück, das Land Brandenburg werde als Wirtschaftsstandort entwertet und außerdem sei dann die Arbeitsfähigkeit der Kommunalverwaltung nicht mehr garantiert. Ich teile diese Auffassung nicht. Aber selbst die Darstellungen, die von Experten aus Ungarn und der Schweiz gemacht wurden, sowie Hinweise auf andere Länder, in denen Akteneinsicht zum Teil seit langem und auch sehr umfangreich gewährt wird, ohne daß dort diese Befürchtungen zutreffen, haben den Gesetzgeber lediglich darin bestärkt, das Gesetz nun in dieser Form zu verabschieden.

Zu den wesentlichen, den Umfang des Akteneinsichtsrechts bestimmenden §§ 2, 4 und 5 habe ich folgende Einwände erhoben:

- In § 2 wird der Anwendungsbereich des Gesetzes festgelegt. Er ist so geblieben, wie er von der Landesregierung vorgesehen war. Dadurch sind entgegen meinen Empfehlungen Stiftungen und Anstalten des öffentlichen Rechts von der Möglichkeit, Akten einzusehen, völlig ausgenommen.

- Nach § 4 (Schutz überwiegender öffentlicher Interessen) ist ein Antrag auf Akteneinsicht schon dann abzulehnen, wenn z. B. in den Bereichen Wohl des Landes, Strafverfolgung und -vollstreckung, aber auch Gefahrenabwehr bereits die Möglichkeit einer Beeinträchtigung der bezeichneten Schutzgüter eintreten „könnte".

- In § 5 (Schutz überwiegender privater Interessen) übernehmen datenschutzrechtliche Bestimmungen die Aufgabe des wichtigsten Regulativs. So ist es nicht verwunderlich, daß ich mich in diesem besonderen Fall nicht, wie sonst üblich, für eine Verschärfung oder Präzisierung des Datenschutzgedankens einsetzen mußte; denn dies war bereits in umfassendster Weise in den Gesetzentwurf eingearbeitet worden. Ich habe allerdings eine Regelung gefordert, die die Kenntnisnahme von Namen, Titel akademischem Grad, innerdienstlicher Funktionsbezeichnung, dienstlicher Anschrift und Rufnummer in der Regel grundsätzlich zuläßt, es sei denn, der Offenbarung stehen schutzwürdige Belange des Amtsträgers entgegen. Dies ist aufgegriffen worden (§ 5 Abs. 3). Dafür war für mich nicht - wie in der Gesetzesbegründung ausgeführt - entscheidend, daß der Arbeitsaufwand für ein Schwärzen und für ein anschließendes Kopieren der geschwärzten Fassung vermieden wird, sondern daß die Information in Gänze erhalten bleibt. Der Eingriff in das Recht auf informationelle Selbstbestimmung geschieht deshalb im öffentlichen Interesse.

Es waren die Parlamentarier, die das Argument mehrerer Gutachter aufgegriffen haben, daß es einen Informationsbeauftragten geben müsse und daß diese Aufgabe durch den Landesbeauftragten für den Datenschutz wahrgenommen werden solle. Diesen Standpunkt hatte ich von Anfang an vertreten. Dabei habe ich allerdings vorgeschlagen, die Aufgabe dem Landesbeauftragten für den Datenschutz unmittelbar zu übertragen und nicht, wie es nun

[37] LT-Drs.: 2/901-I vom 19. Dezember 1997

[38] vom 10. März 1998, GVBl. I S. 46

in § 11 Abs. 1 vorgesehen ist, über den Umweg eines weiteren Beauftragten - den Beauftragten für das Informationszugangsrecht - zu bestellen, um die Aufgabe letztlich doch beim Landesbeauftragten für den Datenschutz anzusiedeln. Zu meinem Vorschlag hätte es allerdings einer Änderung des BbgDSG bedurft, die das MI mit der Argumentation abgelehnt hat, man müsse zunächst einmal Erfahrungen sammeln. Notfalls müßte das AIG novelliert werden und in diesem Fall wäre es einfacher, nur ein, nicht aber zwei Gesetze zu ändern. Selbst wenn dies lediglich verfahrenstaktisch gemeint wäre, könnte ich mich dieser Argumentation nicht anschließen. Der gesetzgeberische Aufwand ist derselbe, ob nur mittels eines Artikelgesetzes ein Gesetz novelliert und gleichzeitig ein anderes abgeändert wird, oder ob nur ein einziges Gesetz von dem Gesetzgebungsverfahren betroffen ist.

Noch bevor das AIG im Gesetz- und Verordnungsblatt für das Land Brandenburg veröffentlicht wurde, lag mir ein Entwurf für Verwaltungsvorschriften zum AIG zur Stellungnahme vor. Die Tendenz, die sich in diesen verwaltungsinternen Vorschriften widerspiegelt, übertrifft sogar noch das Gesetz in seiner fast schon verfassungsrechtlich bedenklichen Auslegungsenge. Auch durch diese Vorschriften hat die Landesregierung verdeutlicht, daß sie die Verfassungsvorgabe so eingeengt wie irgend möglich realisieren will, obwohl die Abgeordneten in dem Gesetzgebungsverfahren dieser Tendenz partiell entgegensteuerten. Die Bürger werden jedoch, wenn ihnen Akteneinsicht verwehrt werden sollte, sich gegebenfalls gegen eine zu enge Auslegung des Gesetzes und gar der Verfassung zur Wehr setzen.

Der Weg, den „Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht" anzurufen, ist durch das AIG selbst vorgezeichnet. Daneben steht dem Betroffenen, dem Akteneinsicht verwehrt wird, der Verwaltungsrechtsweg offen. Erst durch die Art und Weise und durch den Umfang, in welchem die Bevölkerung das Recht auf Akteneinsicht wahrnimmt und erforderlichenfalls durchsetzt, wird sich zeigen, ob dieses Gesetz ein großer oder nur ein kleiner Schritt in die Informationsgesellschaft darstellt. In jedem Fall geht von ihm eine bundesweite Signalwirkung aus.

2.2 Änderung des Verwaltungsverfahrensgesetzes

Der Bund hatte in seinem Gesetz zur Beschleunigung von Genehmigungsverfahren[39] das Verwaltungsverfahrensgesetz (VwVfG)[40] insofern geändert, als verwaltungsverfahrensvereinfachende und -beschleunigende Regelungen getroffen wurden. Erklärtes Ziel war die Verbesserung der wirtschaftlichen Rahmenbedingungen, um so den Standort Deutschland wettbewerbsfähig zu halten. Die Verwaltungsverfahrensgesetze des Bundes und der Länder sind fast gleichlautend gestaltet. Deswegen ist es sinnvoll, die Änderungen, die am Bundesgesetz vorgenommen worden waren, ganz oder zumindest weitgehend in das Verwaltungsverfahrensgesetz für das Land Brandenburg (VwVfGBbg)[41] zu übernehmen. Dazu liegt bisher allerdings nur ein Referentenentwurf vor.

Aus datenschutzrechtlicher Sicht ist vor allem die vorgesehene Änderung von § 73 VwVfGBbg, der das **Anhörungsverfahren in Planfeststellungsverfahren** betrifft, von Interesse. Die beiden ersten Absätze von § 73 VwVfGBbg sollen erheblich erweitert werden, insofern soll über die vergleichbaren Änderungen des Bundesrechts hinausgegangen werden. In Brandenburg sollen dem Entwurf zufolge künftig die Namen und gegenwärtigen Anschriften der von einem Planverfahren betroffenen Eigentümer in den Plan eingefügt werden.

---

39 vom 12. September 1996, BGBl. I S. 1354

40 vom 25. Mai 1976, BGBl. I S. 1253; zul. geänd. durch Art. 1 Genehmigungsbeschleunigungsgesetz vom 12. September 1996, BGBl. I 1354 (BGBl. III 201-6)

41 vom 26. Februar 1993, GVBl. I S. 26, geänd. durch Art. 3 Ges. zur Änderung d. VwVfG BB u. and. Ges. vom 11. November 1996, GVBl. I 306

Ich habe mich ausdrücklich gegen das Vorhaben ausgesprochen und dafür eingesetzt, daß der im Bundesrecht verwendete Text unverändert übernommen wird. Ich habe damit argumentiert, daß nicht nur jede das Recht anwendende Behörde, sondern auch der Gesetzgeber verpflichtet sei, Eingriffe in das Persönlichkeitsrecht nur dann und nur insoweit vorzunehmen, als dies erforderlich ist.

Zur Entscheidungsfindung ist die **Namensnennung in den Planunterlagen** nicht erforderlich, da es bei Planfeststellungen ausschließlich um Grundstücke und nicht um Personen geht. Betroffen ist immer der jeweilige Eigentümer des Grundstücks. Die Offenbarung von Namen und Adresse des Eigentümers - in ausliegenden Planunterlagen - kann sehr leicht dazu führen, daß auf den Eigentümer durch Dritte Druck ausgeübt wird, sich in einer von diesen näher bestimmten Weise zu verhalten oder, da ja Entschädigungen gezahlt werden müssen, von dem Eigentümer Geld zu verlangen.

Da außerdem die gesetzlich festgelegte Mindestzahl Betroffener, denen im Rahmen eines Massenverfahrens gem. § 74 Abs. 5 VwVfGBbg der Planfeststellungsbeschluß bekanntgemacht werden muß, von bisher 300 auf nur noch 50 Betroffene herabgesetzt werden soll, erhöht sich das Risiko für den einzelnen, daß sein Name den anderen Betroffenen infolge öffentlicher Zustellung bekannt gemacht wird.

Schließlich würde die geplante Änderung von § 73 Abs. 3 VwVfGBbg zur Folge haben, daß nicht nur die Auslegungsfrist verkürzt werden soll, sondern daß darüber hinaus die Möglichkeit, die Betroffenen immer dann direkt über geplante Veränderungen zu informieren, wenn der Kreis der Betroffenen klein ist, entfällt. Nicht zuletzt mit Blick auf die doch wünschenswerte Gleichheit der Verfahren im Bund und in den Ländern ist daher insoweit die bundesrechtliche Lösung vorzugswürdig. Das gilt auch für die datenschutzrechtliche Bewertung.

Im Ergebnis wurde unter Beteiligung meiner Behörde ein **Kompromiß** gefunden, demzufolge die gesetzliche Regelung der **Zulässigkeit von Namensnennungen als eine Ermessensregelung** ausgestaltet wurde: in den Plan können auch Namen und Adressen der betroffenen Grundstückseigentümer aufgenommen werden. Dem Kompromiß zufolge soll dem Text der Begründung des Gesetzentwurfs zu entnehmen sein, unter welchen Voraussetzungen das Ermessen auszuüben ist. Ich bin auf diesen Kompromißvorschlag deshalb eingegangen, weil die Verwaltung überzeugend vorgetragen hatte, daß die Planauslegung vor allem Anstoßwirkung erzeugen soll und daß dabei auch Dritte ihre Interessen wahrnehmen und sich gegebenfalls an dem Planverfahren beteiligen können sollten; Dritte kennen aber die Katasterbezeichnungen in der Regel nicht.

Als Regel-Ausnahme-Verhältnis für Nennung und Nicht-Nennung der Eigentümerdaten wurde in dem Kompromiß die Lage der betroffenen Grundstücke herangezogen: insbesondere in geschlossenen Ortschaften ist Namensnennung entbehrlich und daher zu unterlassen; sind aber weit abgelegene Gegenden betroffen, so wird die Namensnennung in der Regel sinnvoll, weil hilfreich sein. Ich habe allerdings nachdrücklich darauf bestanden, daß das Regel-Ausnahme-Verhältnis zugunsten der Nicht-Nennung der Namen ausgestaltet sein muß, andernfalls würde der Kompromiß den Vorgaben der Verfassung widersprechen, da eine noch so wünschenswerte Anstoßfunktion gegenüber dem Persönlichkeitsrecht keinen Vorrang haben kann.

2.3 Staatsverträge

2.3.1 Festlegungen für soziale Versicherungsträger

In Art. 87 Abs. 2 Satz 2 GG findet sich die Bestimmung, die es den Ländern ermöglicht, für soziale Versicherungsträger selbständig bestimmte Festlegungen zu treffen. Das gilt in diesem Zusammenhang nur für diejenigen Fälle, in denen sich der Zuständigkeitsbereich von Sozialversicherungsträgern über mehr als ein, aber höchstens drei Bundesländer erstreckt. Die Bundesländer können demnach regeln, daß eines der betroffenen Länder zum aufsichtsführenden Land bestimmt wird, mit der Folge, daß dann das betreffende Bundesland und nicht der Bund als zuständig angesehen wird.

Eine derartige Festlegung kann nur staatsvertraglich vorgenommen werden. Die Länder haben sich entschieden, die Lösung durch einen einzigen, alle Länder betreffenden Staatsvertrag herbeizuführen, statt je nach Bedarf mehrere zwei- oder dreiseitige Staatsverträge abschließen zu wollen. In dem allseitigen Staatsvertrag[42] ist festgelegt, daß dasjenige Land aufsichtsführend sein soll, in welchem der Versicherungsträger seinen Sitz hat, wenn ein solcher Fall länderübergreifender Versicherungsträger gegeben ist. Nachdem sämtliche Länderparlamente ihre Zustimmung zu dem Staatsvertrag erteilt hatten, ist dieser am 1. Juni 1997 in Kraft getreten.

Die in § 81 SGB X[43] geregelte **datenschutzrechtliche Kontrolle** wird in dem Staatsvertrag aber nicht erwähnt. Sie ist auch nicht - obwohl das zulässig wäre - bundesgesetzlich und unabhängig von dem Verhalten der Länder geregelt worden. Dies bedeutet, daß eine Regelungslücke vorliegt, die geschlossen werden muß. Sie war Anlaß, unter den Landesbeauftragten für den Datenschutz (LfD) ein Meinungsbild zu erstellen, in dessen Ergebnis es als am sinnvollsten angesehen wird, daß die datenschutzrechtliche Kontrolle der behördlichen Aufsicht unterliegen soll, die für das jeweilige Sitzland des Versicherungsträgers die datenschutzrechtliche Kontrolle ausübt (Sitzlandprinzip).

Diese Meinung habe auch ich vertreten. Aus meiner Sicht ist damit aber nur auf eine pragmatische Hilfskonstruktion abgestellt worden. Die gesetzliche Regelungslücke besteht weiter, da eine die Landesgrenzen überschreitende Kontrolle ebenso wie die Aufsicht staatsvertraglich geregelt werden muß, sofern sie nicht gesetzlich geregelt ist. Damit ist der LfD des Sitzlandes nur befugt, in dem Sitzland selbst durch Kontrollen aktiv zu werden. Soll eine Kontrolle in einem der anderen Länder durchgeführt werden, dann kann er nur den LfD des betreffenden Landes bitten, für ihn - quasi „im Auftrag" - tätig zu werden und ihm als dem Sitzland-LfD die Ergebnisse der Kontrolle mitteilen. Eine Kontrollgarantie ist also nicht gegeben.

Ich habe deswegen im Kreise der Datenschutzbeauftragten angeregt, daß bei Abschluß derartiger Staatsverträge ein Artikel eingearbeitet wird, der die Kontrollkompetenz des LfD festlegt[44].

2.3.2 Staatsvertrag über grenzüberschreitende kommunale Zusammenarbeit

Die Landesregierung hatte im April 1997 den Text eines Staatsvertrages mit dem Land Sachsen-Anhalt über die grenzüberschreitende kommunale Zusammenarbeit in Zweckverbänden und durch Zweckvereinbarungen unterzeichnet. Im August wurde das zur Umsetzung dieses Vertrages erforderliche Zustimmungsgesetz im Landtag behandelt.

---

42 vom 11. Oktober 1996, GVBl. I S. 289 (GVBl. I 1997, S. 101)

43 vom 18. August 1980, BGBl. I S. 1469, ber. S. 2218; zul. geänd. durch SGB III-ÄndG vom 16. Dezember 1997, BGBl. I S. 2970

44 s. auch unter 2.3.2

Bei zweiseitigen Verträgen wird u. a. regelmäßig festgelegt, welches Recht jeweils angewendet werden soll. Im vorliegenden Fall war das Recht des Sitzlandes als anzuwendendes Recht und zur Bestimmung der zuständigen Aufsichtsbehörde festgelegt worden. Datenschutz kann in solchen Fällen ausdrücklich, aber auch ohne die konkrete Nennung dieses Regelungsbereichs - durch geeignete Wortwahl - zum Gegenstand des Vertrages gemacht werden; in dem vorliegenden Fall war der Datenschutz nicht erwähnt worden.

Ich habe Kritik an dem Verfahren geübt, derartige Staatsverträge auszuhandeln, ohne dabei in irgendeiner Weise datenschutzrechtliche Belange zu berücksichtigen. In diesem Zusammenhang habe ich bemängelt, daß ich nicht bereits vor Unterzeichnung des Staatsvertrages zu dieser Frage gehört worden war.

Artikel 2 des Vertrages lautet:

> „Soweit in diesem Staatsvertrag nichts anderes geregelt ist, gilt
>
> 1. für Zweckverbände des Recht der kommunalen Zusammenarbeit des Landes, in dem der Zweckverband seinen Sitz hat oder haben soll,
>
> 2. für Zweckvereinbarungen das Recht der kommunalen Zusammenarbeit des Landes, dem die Körperschaft angehört, der durch die Vereinbarung die Erfüllung oder Durchführung der Aufgabe übertragen worden ist oder werden soll."

Auf meine Kritik hin hat mir das MI mitgeteilt, daß es für eine frühzeitige Heranziehung des LfD keinen Anlaß gesehen habe. Aus dem Vertragstext ergebe sich, daß das Recht des jeweiligen Landes maßgeblich sei. Dies folge aus dem Umkehrschluß zu dem eigentlichen Vertragstext, der nur die jeweils betroffene Einrichtung selbst (Recht der kommunalen Zusammenarbeit) zum Gegenstand habe. Das Territorialprinzip bleibe somit unberührt; „je nach Landeszugehörigkeit des betroffenen Bürgers (sei) entweder brandenburgisches oder sachsen-anhaltinisches Recht anzuwenden". Die Aufsicht über den grenzüberschreitenden Zweckverband oder die Körperschaft, welcher grenzüberschreitende Aufgaben übertragen worden seien, obliege dem Vertragsinhalt zufolge den zuständigen Behörden des Sitzlandes. Ebenso sei die Zuständigkeit des Datenschutzbeauftragten geregelt. Dem LfD des Sitzlandes komme daher die Befugnis zu, die für erforderlich angesehenen Prüfungen durchzuführen. Dabei habe er „je nach Wohnsitz des betroffenen Bürgers die datenschutzrelevanten Maßnahmen anhand des brandenburgischen oder sachsen-anhaltinischen Datenschutzrechts zu überprüfen".

Die Vertragsauslegung durch das MI beinhaltet demnach nicht, daß es auf das Recht des Ortes ankommt, der den Gegenstand einer Anfrage oder Petition betrifft, sondern daß vielmehr das Landesrecht anzuwenden ist, dem der Betroffene seinem Wohnsitz nach unterliegt. Eine solche Rechtsanwendung kann recht willkürlich wirken und schwer nachvollziehbar sein. Verstöße gegen den Datenschutz durch eine öffentliche Stelle können nur an demjenigen Maßstab als Verstöße bewertet werden, der für die „Stelle" gilt, die handelt oder Handlungen unterläßt, Maßstab kann dagegen nicht der zufällig von der Handlung oder Unterlassung betroffene Bürger sein. Etwas anderes könnte allenfalls nur insoweit gelten, als der Ort der Auswirkung einer Handlung oder Unterlassung gemeint sein sollte.

Die datenschutzrechtliche Kontrolle selbst ist in dem Schreiben des MI nicht angesprochen worden. Aus meiner Sicht könnte bei grenzüberschreitender Auswirkung auch eine grenzüberschreitende Kontrolle erforderlich werden. Soweit der

LfD des Sitzlandes für zuständig erklärt wird, müßte er demzufolge in dem Vertragspartnerland kontrollierend tätig sein können. Ich sehe allerdings Probleme auf den LfD zukommen, der sich auf einen Vertrag beruft, in welchem bei dem Begriff „Aufsicht" ausdrücklich das jeweilige Innenministerium genannt ist, und der sich auf eine Erstreckung der Kontrollkompetenz auch bezüglich des Datenschutzes berufen muß, um in einem anderen Land Kontrollbefugnisse wahrnehmen zu können. Eine ausdrückliche und normenklare Regelung hätte ich bevorzugt.

In dem einige Monate später verhandelten Staatsvertrag zwischen Brandenburg und dem Freistaat Sachsen mit dem gleichen Regelungsgegenstand und fast identischem Wortlaut habe ich noch einmal ausdrücklich auf die Problematik der grenzüberschreitenden Kontrolle hingewiesen. Ich habe damit argumentiert, daß zu den Aufsichtsbehörden, die in dem Staatsvertrag benannt sind, der LfD nicht zu rechnen ist, und daß deshalb insoweit eine Regelungslücke vorliegt. Ich habe darauf hingewiesen, daß die Situation anderes zu beurteilen sei, wenn in Art. 2 des Vertrages anstelle von „Recht der kommunalen Zusammenarbeit" schlicht das Wort „Recht" stünde. Dann würde auch das Datenschutzrecht des jeweiligen Sitzlandes von dem Regelungsbereich des Staatsvertrages umfaßt sein.

Als Alternative habe ich vorgeschlagen, Art. 2 um eine Nummer 3 mit folgendem Wortlaut zu ergänzen:

„3. Für den Datenschutz gelten die Nummern 1 und 2 sinngemäß".

Mit Hinweis auf die Regelungs- und Wortgleichheit der beiden Staatsverträge wurde mein Vorschlag abgelehnt. Das MI hat seine oben dargelegte Auffassung noch einmal bekräftigt, daß die Auslegung der beiden Verträge bereits früher schriftlich dargelegt worden sei. Ich werde mich gegebenfalls bei der Ausübung der Kontrollkompetenz auf die vom MI vorgegebene weite Vertragsauslegung berufen müssen.

2.4 Verwaltungsvorschrift zum Brandenburgischen Datenschutzgesetz

Die 1995 in Kraft getretenen Verwaltungsvorschriften zum Brandenburgischen Datenschutzgesetz[45] waren bewußt als „vorläufige" deklariert worden, u. a. weil darin von vornherein verschiedene Fragestellungen ausgespart wurden und demzufolge hierzu keine Ausführungen zu finden waren. Nach einer Erörterung, die sich über zwei Jahre hingezogen hatte, liegen seit Anfang 1998 nunmehr Verwaltungsvorschriften zum Brandenburgischen Datenschutzgesetz[46] vor, die zusätzliche Erläuterungen zu § 9 (Automatisiertes Abrufverfahren und regelmäßige Datenübermittlung) sowie zu den §§ 11 (Verarbeitung personenbezogener Daten im Auftrag) und 11 a (Wartung und Fernwartung) enthalten. Dazu habe ich bereits früher Ausführungen gemacht[47].

Hervorzuheben ist, daß nunmehr in den Verwaltungsvorschriften eine ausführliche Darstellung des Behördenbegriffs zu finden ist. Dies gilt vor allem in Hinblick auf Behörden, auf die nicht das Brandenburgische Datenschutzgesetz, sondern wegen der Verweisung in § 2 Abs. 2 BbgDSG ganz überwiegend das Bundesdatenschutzgesetz anzuwenden ist.

Neu ist die Aufgabenbeschreibung für den Datenschutzverantwortlichen in den Ausführungen zu § 7 BbgDSG (Sicherstellung des Datenschutzes) als „Ersatz" für die sonst übliche Institution eines behördlichen

45 vom 23. Februar 1995, ABl. S. 134

46 vom 17. Dezember 1997, ABl. 1998 S. 94

47 s. 5. Tätigkeitsbericht unter 2.1

Datenschutzbeauftragten. Das MI hat Vorgaben zu dieser für den Datenschutz in der Behörde verantwortlichen Person an der jetzigen Lebenssituation orientiert und ausführlichere Beschreibungen in die Verwaltungsvorschriften eingearbeitet.

Im Zuge der Bearbeitung der Verwaltungsvorschriften sind auch die Anlagen - Formulare einschließlich Ausfüllhinweise als Bestandteil der Verwaltungsvorschriften - überarbeitet und dem novellierten Gesetz angepaßt worden.

2.5 Druck von Lohnsteuerkarten im Auftrag

Nach § 39 des Einkommensteuergesetzes (EStG)[48] ist es Aufgabe der Gemeinden, denjenigen Bürgern, die Arbeitnehmer sind, rechtzeitig für jedes Kalenderjahr unentgeltlich eine Lohnsteuerkarte nach amtlich vorgeschriebenem Muster auszustellen und zu übermitteln. Da den meisten der Gemeinden keine eigene Druckerei zur Verfügung steht, muß jedenfalls der Druck der Karten - als Datenverarbeitung im Auftrag - fremdvergeben werden. Die Gemeinden gehen inzwischen zunehmend dazu über, diese Aufgabe durch private Unternehmen ausführen zu lassen, und nicht selten beauftragen sie die Druckerei auch mit der Kuvertierung und der Verteilung der Karten an die Adressaten.

Durch die Beauftragung privater Stellen, die nicht Beliehene sind, mit einer hoheitlichen Aufgabe ergeben sich besondere Probleme des Datenschutzes. Mit Hilfe von Verträgen, die auf diese Situation möglichst genau zugeschnitten sind, und vor allem mit der besonderen Verpflichtung derjenigen Personen, die konkret mit den Lohnsteuerkarten umzugehen haben, soll diesen Problemen begegnet werden. Die Verpflichtung erfolgt nach § 5 BDSG und nach dem Verpflichtungsgesetz[49] und ist grundsätzlich durch Verantwortliche der Gemeinde, die ja die hoheitliche Aufgabe an eine andere Stelle vergibt, aber Herrin des Verfahrens bleiben muß, i. d. R. selbst vorzunehmen. Hier wird eine Problematik deutlich, die allein schon dadurch auftritt, daß die druckende und kuvertierende Firma meist nicht in der Gemeinde oder in deren enger Nachbarschaft angesiedelt ist, sondern häufig an einem weit entfernten Ort besteht.

Über eine längere Zeit fand wegen dieser Problematik ein reger Meinungsaustausch meiner Behörde mit dem Ministerium der Finanzen statt. Im Ergebnis dieser Diskussion wurde nach Ressortabstimmung dem MI die Federführung bei der erforderlichen weiteren Klärung dieser Grundsatzfrage übertragen. Inzwischen hat sich das MI der Meinung des Bundesministeriums der Justiz angeschlossen, das davon ausgeht, daß jedenfalls die grundsätzliche Zulässigkeit der Beauftragung privater Stellen mit Druck, Kuvertierung und Verteilung bzw. Versendung von Lohnsteuerkarten bejaht werden kann, wenn alle mit der betreffenden Aufgabe befaßten Personen ordnungsgemäß verpflichtet worden sind, so daß ihnen die strafrechtlichen Konsequenzen einer Verletzung von Privat- oder Dienstgeheimnissen bekannt sind.

---

48 i. d. Fass. vom 16. April 1997, BGBl. I S. 821; zul. geänd. durch Ges. vom 19. Dezember 1997, BGBl. I S. 3121

49 Art. 42 des Einführungsgesetzes zum Strafgesetzbuch (EGStGB) vom 2. März 1974, BGBl. I S. 469, ber. S. 547, geänd. durch Ges. vom 15. August 1994, BGBl. I S. 1942

2.6 Unseriöse Datenerhebung durch Marketingfirmen

Im vergangenen Jahr haben Marketingfirmen in Deutschland in großem Umfang Haushaltsumfragen durchgeführt. Ich erhielt deswegen eine Vielzahl von Eingaben und Telefonanrufen. Der Tenor war dabei stets eine Verärgerung, meistens auch eine Verunsicherung der Bürger. Ich hatte deshalb u. a. auch mit einer Presse-Information in allgemeiner Form reagiert und deutlich darauf hingewiesen, daß die Beantwortung der Umfragen völlig freiwillig sei, daß aber die personenbezogenen Daten u. U. weltweit gehandelt und genutzt werden.

Unseriös waren diese Befragungen aus verschiedenen Gründen. Zunächst waren die Firmennamen angelehnt worden an die von seriösen Institutionen: INFAS Lifestyle AG an infas Sozialforschung GmbH bzw. Claritas Deutschland Data + Services GmbH an den Deutschen Caritasverband der katholischen Kirche. Dies sollte offensichtlich der ganzen Sache einen ehrbaren Anstrich geben. Darüber hinaus wurde für die Beantwortung der umfangreichen und äußerst detaillierten Einzelfragen unter Ausschluß des Rechtswegs mit Losgewinnen, Vorabinformationen über Sonderangebote und mit Gutscheinen geworben.

Bei der Benennung der Aufklärungspflichten über die Erhebung gab es weitere Probleme. Claritas Deutschland hatte zwar die Freiwilligkeit der Beantwortung dargestellt und auch auf eine Widerspruchsmöglichkeit bzgl. Datenweitergabe hingewiesen, dies jedoch nicht deutlich aus dem Kontext hervorgehoben. INFAS Lifestyle hatte dagegen eine Erklärung zum Datenschutz vorbereitet, dabei jedoch nicht die Freiwilligkeit der Beantwortung und die Widerspruchsmöglichkeit benannt.

Der Zweck der Umfragen ist in beiden Fällen mißverständlich dargestellt worden. Weder das Konsumverhalten noch die Marktforschung stand im Vordergrund, sondern vielmehr die personenbezogene **Adressengewinnung**, also ausschließlich das Marketing. Unschwer erkennbar sollten Daten über Bankverbindungen, Versicherungen, Kauf- und Lebensgewohnheiten, Gesundheit, Grundeigentum usw. der auskunftgebenden Bürger gesammelt, genutzt sowie damit gehandelt werden. Wäre dies nicht bezweckt gewesen, hätten auch anonyme Erhebungen ausgereicht. So aber liegen bei den Firmen detaillierte Persönlichkeitsprofile mit weit über 100 Erhebungsmerkmalen pro Person, bei INFAS Lifestyle sogar noch über deren Partner und Kinder vor. Die jährlichen staatlichen Befragungen nach dem Mikrozensusgesetz, die ausschließlich statistischen Zwecken dienen, nehmen sich dagegen dem Umfang nach geradezu harmlos aus. Datensammlungen bei privaten Unternehmen können für den Bürger zu einer erheblichen Bedrohungs- und Manipulationsmöglichkeit werden, weil er nicht mehr wissen kann, wer über ihn welche Daten gespeichert hat.

Die häufig an mich gerichtete Bürgerfrage, ob denn derartige Befragungen durch private Unternehmen überhaupt zulässig seien, ist allerdings zu bejahen, weil die Beantwortung derartiger Fragen im Fall einer fehlenden Rechtsvorschrift die Zustimmung des Betroffenen zwingend voraussetzt (§ 4 Abs. 1 BDSG); die freiwillige Zustimmung - durch das Ausfüllen des Fragebogens - ersetzt die fehlende Rechtsgrundlage.

In einer Presse-Information zu dieser Angelegenheit hatte ich deshalb geraten, die Haushaltsbögen dieser Firmen gar nicht erst auszufüllen. Denkbar ist aber auch, die nicht ausgefüllten Erhebungsbögen solcher Umfragen mit dem kostenlosen Rückbrief an den Absender zurückzuschicken, der dann das Rückporto tragen muß.

Obwohl ich auf die Zuständigkeit des MI als zuständige Datenschutzaufsichtsbehörde für den privaten Bereich verwiesen hatte, bin ich wegen meiner Presse-Information insofern kritisiert worden, als ich nur für die öffentlichen Stellen des Landes zuständig sei und mich deshalb Äußerungen zu nicht-öffentlichen Stellen zu enthalten habe. Zweifelsfrei gibt es in

Brandenburg geteilte Zuständigkeiten in Datenschutzangelegenheiten. Jedoch steht es dem Landesbeauftragten für den Datenschutz aufgrund der **Unabhängigkeit seines Amtes** nach § 23 Abs. 2 BbgDSG frei, den Bürgern des Landes allgemeine Empfehlungen zu datenschutzrechtlichen Fragestellungen zu geben. Es ist der in Brandenburg gem. § 38 BDSG zuständigen obersten Kontrollbehörde (MI) freigestellt, sich gleichermaßen im Rahmen ihrer Kompetenz um eine erforderliche öffentliche Aufklärung zu bemühen.

Allgemeine Empfehlungen halte ich noch aus einem weiteren Grund für sehr wichtig: So hatte ich wiederholt auf Anfragen darauf hinweisen müssen, daß auch bei Kommunalstatistiken[50] auf freiwilliger Basis das datenschutzrechtliche Prinzip der Erforderlichkeit gilt. Nur so können sich kommunalstatistische Erhebungen von der Unseriösität solcher Haushaltsbefragungen abheben und damit die erforderlich Akzeptanz bei der betroffenen Bevölkerung und jeweils tatsächlich ein repräsentatives Ergebnis als Grundlage für Selbstverwaltungsaufgaben finden.

2.7 Petentenschutz auch für Bedienstete der öffentlichen Verwaltung

Aus dem Kreis der Mitarbeiter einer Amtsverwaltung wurde beklagt, daß in dem **internen Telefonverzeichnis** des Amtes u. a. nicht nur die Bürgermeister der amtsangehörigen Gemeinden und Mitglieder der Gemeindevertretung, sondern auch Bedienstete des Amtes mit deren Privatanschriften, privaten Telefonverbindungen und auf einer gesonderten Liste auch deren Geburtsdaten und konkreten Altersangaben aufgeführt waren.

[50] s. auch unter 3.5.4.3

In meiner Beurteilung verwies ich gegenüber dem zuständigen Amtsdirektor darauf, daß Form und Umfang dieser Veröffentlichung zumindest bezüglich der Bediensteten des Amtes eine datenschutzrechtliche Besonderheit darstellen, da es sich bei den Angaben zu deren Person um Personaldaten i. S. v. § 29 BbgDSG, die gleichzeitig auch als Personalaktendaten i. S. v. § 57 Abs. 3 Landesbeamtengesetz (LBG)[51] anzusehen seien, handelt. Auch wenn das Telefonverzeichnis „Nur für den Dienstgebrauch" deklariert sei, würden die Informationen, die die Nutzer des Verzeichnisses daraus ziehen können, für die jeweils Betroffenen eine unerlaubte Offenbarung ihrer Daten darstellen, sofern diese zuvor nicht ausdrücklich ihre Zustimmung zu einer Veröffentlichung ihrer über die **dienstlich erforderlichen Angaben** (Namen, Arbeitsbereiche, Apparatnummern des Diensttelefons) hinausgehenden Personaldaten erteilt haben, weil eine materiell-rechtliche Grundlage i. S. v. § 4 Abs.1 Buchst. a BbgDSG, die eine Offenbarung rechtfertigen würde, nicht vorliegt. Hier war ganz offensichtlich die ersatzweise Zustimmung der Betroffenen nicht eingeholt worden und in der erhofften Vollständigkeit wohl auch nachträglich nicht einholbar, so daß der zuständige Amtsdirektor letztlich zusagte, aus allen Telefonverzeichnissen die relevanten Daten innerhalb von zwei bis drei Wochen zu entfernen. Verständnis zeigte er jedoch zunächst nicht dafür, daß der Sachverhalt von einem Bediensteten/einer Bediensteten an meine Behörde herangetragen worden war, ohne daß dieser/diese den Dienstweg eingehalten hätte. Er sah darin insbesondere eine Unterminierung seiner Mittel und Möglichkeiten für eine vertrauensvolle Zusammenarbeit mit seinen Mitarbeitern; gleichzeitig sah er die Gefahr für möglicherweise ungerechtfertigte Verdächtigungen entstehen. Insbesondere wollte er nicht verstehen, daß meine Behörde ihm, dem Leiter der Amtsverwaltung, eine Antwort auf die Frage verweigerte, wer die Eingabe geschrieben hatte, dies könne nicht dazu angetan sein, das Vertrauen für eine gute Zusammenarbeit mit dem LfD aufzubauen. Solche und ähnlich gelagerte Sachverhalte werden mir in letzter Zeit zunehmend vorgetragen.

Der Gesetzgeber hat in § 21 Abs. 1 BbgDSG auch Bediensteten öffentlicher Stellen ausdrücklich das Recht eingeräumt, sich **unmittelbar an den LfD** zu wenden, „**ohne** daß der **Dienstweg** einzuhalten ist". Darüber hinaus ist in Abs. 2 bestimmt: „Niemand darf deswegen benachteiligt oder gemaßregelt werden, weil er sich an den Landesbeauftragten für den Datenschutz wendet". Wenn also ein Bediensteter den direkten Weg zum LfD sucht, ist zu vermuten, daß er diesbezüglich Nachteile befürchtet. Insoweit ist eine Offenbarung der Namen meiner Petenten auszuschließen, es sei denn, sie würden einer solchen ausdrücklich zustimmen.

Auch ich halte es, nicht zuletzt im Interesse besserer Durchsetzbarkeit datenschutzrechtlicher Belange, für begrüßenswert, wenn die dienstliche Situation und das Vertrauensverhältnis zwischen Mitarbeitern und Vorgesetzten so entwickelt ist, daß auch datenschutzrechtliche Probleme intern erörtert, evtl. sogar ausgeräumt werden können, ohne daß Nachteile zu befürchten wären. Ob diese Voraussetzungen immer gegeben sind, vermag ich im einzelnen nicht zu beurteilen. Jedenfalls muß meine Behörde dem **Schutzbedürfnis** ihrer Petenten Rechnung tragen, wollte ich mich nicht selbst einer Pflichtverletzung schuldig machen. Aufgrund dieser Rechtslage kann das Vertrauensverhältnis meiner Behörde zu den datenverarbeitenden Stellen diesbezüglich auch überhaupt nicht zur Disposition gestellt werden.

Meine Aufgabe ist es, einzig den datenschutzrechtlichen Aspekt einer Eingabe zu beurteilen. Dabei spielt für mich der Name des Petenten allenfalls dann eine Rolle, wenn nur mittels dieses Namens eine Aufklärung der Angelegenheit möglich ist. Ansonsten habe ich auf der Grundlage von § 23 i. V. m. § 25 BbgDSG relevanten Hinweisen selbst dann von Amts wegen nachzugehen, wenn diese anonym vorgetragen werden.

---

[51] vom 24. Dezember 1992, GVBl. I S. 506; zul. geänd. durch Ges. vom 17. Dezember 1996, GVBl. I S. 363

2.8 Altakten - ein unendliches Thema

2.8.1 Verbleib von Lohn- und Gehaltsunterlagen ehemaliger DDR-Einrichtungen

Die Frage nach dem Verbleib und Überlegungen zur weiteren Behandlung sowie zur Verwendbarkeit von Altpersonalakten (sog. **Kaderakten**) waren Gegenstand vielfältiger Ausführungen in meinen Tätigkeitsberichten von Beginn meiner Amtszeit an[52]. Daß auch nach über sieben Jahren seit der Vereinigung noch großes Interesse am Verbleib ihrer Personalunterlagen besteht, zeigten auch in diesem Berichtsjahr wieder die vielfältigen, insbesondere fernmündlichen Nachfragen Betroffener in meiner Behörde, die überwiegend darauf ausgerichtet waren, wie sie an ihre früheren Lohn- und Gehaltsunterlagen herankämen. Während meine Dienststelle zumindest bezüglich der zentralen und kommunalen Einrichtungen der DDR, die in den Bereich oberster Landesbehörden oder wiederum in den kommunalen Bereich überführt worden waren, häufig dann weiterhelfen kann, wenn und soweit die Kaderakten nicht bereits einer „Bereinigungsaktion" noch vor der Vereinigung (**„Modrow-Erlaß"**)[53] oder im Zusammenhang mit der Neuanlage der Personalakte bei Übernahme in den öffentlichen Dienst zum Opfer gefallen sind, ist dies bisher im Falle anderer ehemaliger Arbeitgeber aus DDR-Zeiten regelmäßig deshalb nicht möglich gewesen, weil ich über keine ausreichenden Informationen bezüglich deren Rechtsnachfolge verfügte.

Um so mehr bin ich darüber erfreut, aufgrund einer Information des Berliner Datenschutzbeauftragten jetzt darauf hinweisen zu können, daß das Bundesarchiv ein **Verzeichnis über Verbleib und Aufbewahrung von Lohn- und Gehaltsunterlagen von Mitarbeitern zentraler Einrichtungen der DDR** erarbeitet hat. Dieser Liste ist zu entnehmen, daß sowohl öffentliche als auch nicht-öffentliche Stellen diese Daten vorhalten, die insbesondere für die Überführung von Zusatzversorgungsanwartschaften bei der Bundesversicherungsanstalt für Angestellte (BfA) als Versorgungsträger für die Zusatzversorgungssysteme der ehemaligen DDR von Bedeutung sind. Das Bundesarchiv stellt Interessenten auf schriftliche Anforderung eine Kopie dieser Liste zur Verfügung. Darüber hinaus hat die BfA ein sehr umfangreiches **Arbeitgeberverzeichnis** erstellt, mit dem ehemalige Arbeitgeber aus DDR-Zeiten den die Akten verwahrenden Rechtsnachfolgern gegenübergestellt werden. Im Bedarfsfall informieren die BfA-Mitarbeiter Versicherte mit Hilfe dieses Anschriftenverzeichnisses über den möglichen Verbleib von Unterlagen, die für die Bearbeitung ihres dortigen Vorgangs erforderlich sind.

Entsprechende Anfragen können unmittelbar gerichtet werden an:

Bundesarchiv	Bundesversicherungsanstalt für Angestellte
Ref. DDR 1	- Versorgungsträger f. d. Zusatzversorgungssysteme -
Finckensteinallee 63	Hirschberger Str. 4
12205 Berlin	10317 Berlin

[52] s. 1. Tätigkeitsbericht (TB) unter 5.3.4 u. Anlage 1, 2. TB unter 3.2.1, 3.2.2 u. 6.2.3, 4. TB unter 13.2.1 sowie 5. TB unter 13.1.2 u. 13.1.3.4

[53] Verordnung zur Arbeit mit Personalunterlagen vom 22. Februar 1990, GBl. der DDR I S. 84

2.8.2 Akten liquidierter Betriebe - Verkauf DISOS GmbH

Neben vielen anderen Aufgaben verwaltet die Bundesanstalt für vereinigungsbedingte Sonderaufgaben (BVS) als Nachfolgerin der Treuhand auch die **Akten der** ihrer Zuständigkeit unterstehenden **ehemaligen DDR-Betriebe**. Teil dieser Akten sind auch hochsensible personenbezogene Daten früherer Arbeitnehmer. Im Rahmen von Rationalisierungsmaßnahmen hat die BVS diesen Aufgabenbereich ausgelagert und auf das in ihrem alleinigen Besitz befindliche Tochterunternehmen die DV-InformationsSysteme, Organisation und Service GmbH (DISOS) übertragen. Diese verwaltet die in Rede stehenden Akten im Wege der Datenverarbeitung im Auftrag. Eine ausreichende Einflußnahme der BVS war damit gewährleistet und auch notwendig, da es sich hier um Daten handelt, die einer öffentlich-rechtlichen Zweckbindung unterliegen, die aufgrund hoheitlicher Eingriffsbefugnisse erhoben worden sind.

Ende 1997 wurde die DISOS an IBM Deutschland veräußert. Verwalter der Akten ist damit eine private Firma. Zwar kann hier über die fortbestehenden vertraglichen Regelungen ein gewisses Maß an Datenschutz sichergestellt werden, dieser endet jedoch dort, wo auch die Befugnisse des Bundesbeauftragten für den Datenschutz (BfD) enden. Die vormals bestehende öffentlich-rechtliche Bindung besteht nach der Veräußerung an IBM nicht weiter fort. Tatsächlich wurde hier ein hoher vorhandener Schutzstandard, der aufgrund der Brisanz der verwalteten Akten in jeder Hinsicht gerechtfertigt war, aufgegeben und auf ein niedrigeres Niveau zurückgeführt. Das dem privatwirtschaftlichen Handeln immanente Gewinnstreben birgt u. U. eine Vielzahl datenschutzrechtlicher Risiken für den verwalteten Datenbestand bzw. für die betroffenen Bürger mit sich.

Gegenwärtig stellt sich die Situation nun so dar: die (private) DISOS verwaltet den Aktenbestand für die BVS, vertraglich geregelt im Wege der **Datenverarbeitung im Auftrag**. Da es sich beim Auftragnehmer (BVS) um eine Bundesbehörde handelt, obliegt somit die datenschutzrechtliche Kontrollkompetenz in dieser Sache dem BfD.

2.8.3 Verzeichnis von Gefangenenkarteien und Gefangenenakten der früheren DDR

Von der Existenz eines Verzeichnisses von Gefangenenkarteien und Gefangenakten der früheren DDR erhielt ich zufällig Kenntnis. Es wurde in Kooperation der Justizbehörden der neuen Bundesländer und Berlins durch die Senatsverwaltung für Justiz erstellt und liegt mir in Kopie (Stand: August 1995) vor. Es enthält - nach Einrichtungen der DDR-Strafjustiz geordnet - Auskünfte über den jetzigen Standort dieser Unterlagen sowie Hinweise über deren Vollständigkeit (Gefangenenpersonalakten, Gesundheitsakten, Lohnkontenkarten), zu DDR-Zeit vorgenommenen Umlagerungen, Sicherheitsverfilmung, Ausdünnungen, usw.

3 Inneres

3.1 Melde- und Personenstandswesen

3.1.1 Novellierung des Brandenburgischen Meldegesetzes

Ohne daß das Ministerium des Innern (MI) nach meinen Einlassungen im letzten Tätigkeitsbericht zur Novellierung des Brandenburgischen Meldegesetzes[54] zu meiner Behörde den Gesprächsfaden wegen der noch kontrovers diskutierten Punkte aufgenommen hatte, wurde mir erst im Januar 1998 ein überarbeiteter Entwurf dieses Gesetzes mit der Bitte um kurzfristige Stellungnahme zugeleitet. Verkürzt war auf meine letztjährigen Kritikpunkte und Vorschläge fast zeitgleich lediglich indirekt in der Stellungnahme der Landesregierung zum letzten Tätigkeitsbericht (Stellungnahme)[55] und dabei inhaltlich - insbesondere hinsichtlich der Vorschläge und Empfehlungen, die wegen der technologischen und gesellschaftlichen Entwicklungen von grundsätzlicher datenschutzrechtlicher Bedeutung sind - in nicht angemessener Weise eingegangen worden.

Insoweit habe ich in Anbetracht der Wichtigkeit der Angelegenheit den Verfahrensablauf bemängelt. Gleichwohl konnte ich mit Genugtuung feststellen, daß in einigen Regelungen meine Vorstellungen Beachtung gefunden haben. Zu begrüßen ist es, daß die vom MI mit Übersendung des Novellierungsentwurfs (Stand: 09.01.1998) dargestellten Zeitabläufe eine Verabschiedung des neugefaßten Brandenburgischen Meldegesetzes noch im Sommer des Jahres 1998 erwarten lassen. Aus meiner Stellungnahme sind im einzelnen folgende Punkte hervorzuheben[56]:

Kreismeldekarteien

Es ist vorgesehen, daß Unterlagen der Kreismeldekarteien bis zum 31. Dezember 1999 in die kommunalen Archive zu „überführen" sind. Damit wird meiner Forderung, die Kreismeldekarteien der Verwaltung selbst aufgrund einer materiell-rechtlichen Regelung im Brandenburgischen Meldegesetz zu entziehen, zwar Rechnung getragen, es ist jedoch nach dem bisherigen Vorlauf nicht erkennbar, weshalb die Regelung nicht bereits zum Ende 1998 greifen sollte.

Um darüber hinaus eine Gleichbehandlung aller (noch) vorhandenen Datenbestände sicherzustellen, habe ich in Anlehnung an archivrechtliche Bestimmungen folgenden Wortlaut empfohlen: „Sie sind den zuständigen Archiven so frühzeitig gem. § 4 Abs. 1 Brandenburgisches Archivgesetz anzubieten, daß diese sie bis Ende 1998 (spätestens 6 Monate nach Inkrafttreten des Gesetzes) übernehmen können.".

Adreßbuchverlage

---

54 s. 5. Tätigkeitsbericht unter 3.1.1.1 und 12.4.1.2

55 LT-Drs. 2/4768 vom 15. Dezember 1997

56 die hier gewählte Reihenfolge orientiert sich an den behandelten Punkten im 5. Tätigkeitsbericht, vgl. Fn. davor

Mit dem Vorhaben, Adreßbuchverlagen keine Meldedaten mehr zu übermitteln, wird nicht nur vielfältigen, seit langem den Meldebehörden angelasteten Gefahren (Fehlauswertungen, Ausforschungen im Vorfeld krimineller Handlungen über Adreßbücher u. a.), sondern vor allem auch Gefahren, die durch unkontrollierbare Aggregierung, Schaffung bundesweiter Adreßdateien durch Einscannen und kommerziellen Vertrieb über CD-ROM drohen, begegnet. Hierauf bin ich bereits an anderer Stelle[57] eingegangen. Ein weitere datenschutzrechtliche Verbesserung der bisherigen Rechtslage sehe ich darin, daß nicht mehr auf die Widerspruchsmöglichkeit der Meldepflichtigen (in mitunter sehr aufwendigen und nicht besonders rechtssicheren Verfahren) hingewiesen werden muß.

Datenübermittlungen an öffentlich-rechtliche Religionsgemeinschaften

An den Regelungen soll ohne Einschränkung festgehalten werden. Dabei wird in der Stellungnahme zwar zu Recht auf die Rahmenvorschriften in § 19 Abs. 2 Melderechtsrahmengesetz (MRRG)[58] hingewiesen, jedoch wäre mir daran gelegen zu erfahren, wie das MI die datenschutzrechtlichen Hintergründe meiner diesbezüglichen Kritik im letzten Tätigkeitsbericht beurteilt und ob es bereit wäre, die Initiative für eine Änderung der Rahmenvorschriften in dem von mir geäußerten Sinn zu ergreifen oder eine solche Initiative zumindest zu unterstützen.

Automatisierte Datenverarbeitung und Datenverarbeitung im Auftrag

Die Ankündigung in der Stellungnahme zur automatisierten Datenverarbeitung ließen umfassendere Erweiterungen hierzu erwarten. Leider sieht der vorliegende Entwurf aber nur Bestimmungen zur automatisierten Datenverarbeitung, beschränkt auf den Bereich der Datenverarbeitung im Auftrag, vor. Ich bedauere dies sehr, hoffe aber, daß im Zuge einer möglichst vereinheitlichten weiteren **Automatisierung des Meldewesens** in Brandenburg zumindest im Wege von Verwaltungsvorschriften zum Brandenburgischen Meldegesetz alsbald auch allgemeine datenschutzgerechte Regelungen hinsichtlich der automatisierten Datenverarbeitung erlassen werden, in denen u. a. auch meine Forderungen hinsichtlich des - wie Vorkommnisse im Zusammenhang mit Diebstählen von Servern mit Festplatten immer wieder und in letzter Zeit zunehmend zeigen - notwendigen Einsatzes von **Verschlüsselungs-Software** Berücksichtigung finden werden[59].

Hinnehmbar ist zwar die vorgesehene Erweiterung der Möglichkeit **auftragsweiser Datenverarbeitung** auch auf nicht-öffentliche Stellen **innerhalb der Landesgrenzen** Brandenburgs unter dem Aspekt der vorgesehenen Unterwerfungsklausel und dem Trennungsgebot bzw. dem Verbot der Aggregierung mit anderen Daten. Wenn dies allerdings uneingeschränkt auch auf private Datenverarbeiter zutreffen soll, die lediglich als Niederlassungen internationaler Unternehmen agieren, dann bedarf es hierfür spezieller Bestimmungen über Voraussetzungen und Vertragsgestaltung.

Nicht hinnehmbar ist die auf Behörden beschränkte Möglichkeit der Datenverarbeitung im Auftrag **außerhalb der Landesgrenzen** Brandenburgs. Auf meine diesbezüglichen Bedenken im letzten Tätigkeitsbericht muß ich noch einmal ausdrücklich hinweisen. Auch wenn sich diese öffentlichen Stellen den landesgesetzlichen Regelungen unterwerfen, gingen Bindungen an landesgesetzliche Zuständigkeitsregelungen hinsichtlich der Kompetenzen des Brandenburgischen Datenschutzbeauftragen ins Leere, weil dieser in anderen Bundesländern nicht tätig werden kann. Die Kollegen in den anderen Bundesländern können - jedoch mangels einer gleichlautenden materiell-rechtlichen Regelung zu gegenseitigem

---

57 s. 4. Tätigkeitsbericht unter 3.1.1.6

58 i. d. Fass. vom 24. Juni 1994, BGBl. I S. 1430, geänd. durch Ges. vom 12. Juli 1994, BGBl. I S. 1497, 1503

59 s. unter 1.4.5.1

amtshilfegleichem Handeln - nicht zur Kontrolle verpflichtet werden. Ich muß daher die Erweiterung der Möglichkeit auftragsweiser Datenverarbeitung außerhalb der Landesgrenze Brandenburgs ablehnen, die im übrigen auch Datensicherungsprobleme hinsichtlich der Übertragungswege in sich birgt.

Immerhin wird einer meiner Forderungen mit einer Zusatzregelung nachgekommen werden, daß eine im Rahmen des Brandenburgischen Meldegesetzes in auftragsweiser Datenverarbeitung tätige Stelle, sofern sie auch andere Daten verarbeitet, diese getrennt zu führen hat und nicht mit den Meldedaten zusammen führen darf.

Protokollierung

Mein Vorschlag, **Melderegisterauskünfte** durchgängig zu protokollieren, hat keine Berücksichtigung gefunden. Ich bedauere es sehr, daß auch zu diesem Punkt keine inhaltliche Auseinandersetzung mit meiner Behörde stattgefunden hat.

Eine unter Nutzung elektronischer Verfahren erteilte Auskunft muß auch unmittelbar auf diesem Wege erkennbar sein. Dies gilt - entgegen den Äußerungen in der Stellungnahme - auch für Grunddaten. Gerade die vor Ort gesammelten Beobachtungen im letzten Berichtszeitraum zeigen, daß das Verwaltungshandeln regelmäßig nicht durchgängig nachvollziehbar ist. Darüber hinaus dient die von mir vorgeschlagene durchgängige Protokollierung der Transparenz des Verwaltungshandelns und somit auch dem Schutz der Verwaltung (z. B. vor Fehlverdächtigungen) selbst.

Da Protokollierungspflichten auch in anderen Bundesländern durchgängig nur für regelmäßige Datenübermittlungen oder Übermittlungen an Sicherheitsbehörden (dann dort) bestehen, habe ich meine Forderungen an dieser Stelle nicht aufrechterhalten. Dabei erwarte ich jedoch, daß im Zuge einer möglichst vereinheitlichten weiteren Automatisierung des Meldewesens in Brandenburg zumindest im Wege von Verwaltungsvorschriften zum Brandenburgischen Meldegesetz auch umfassende Protokollierungspflichten für automatisierte Verfahren verankert werden.

Aufbewahrungsfristen

Im vorigen Tätigkeitsbericht hatte ich die gesetzliche Festlegung von Aufbewahrungsfristen deshalb gefordert, weil hierzu eine normenklare Regelung erforderlich ist, um u. a. die bei meinen Kontrollbesuchen in verschiedenen Meldestellen des Landes beobachteten Unsicherheiten auszuräumen, wie lange die nach mehreren Jahren sehr umfangreich gewordenen Sammlungen von schriftlichen Dokumentationen, Übermittlungenkontrollnachweisen, Ausdrucken zu Speichereingaben, Auskunftsnotizen usw. aufzubewahren seien.

Diese Forderung ist nicht berücksichtigt worden, hat nicht einmal Erwähnung in der Stellungnahme gefunden. Ich hoffe, daß zumindest vorgesehen ist, im Wege von Verwaltungsvorschriften zum Brandenburgischen Meldegesetz oder im Erlaßwege die Gleichbehandlung der Dokumentationen bei allen Meldebehörden und damit einhergehend Gesichtspunkte der Praktikabilität mit solchen datenschutzgerechten Aufbewahrungserfordernissen in Einklang zu bringen.

Auskunftssperren und Widerspruchsrechte

Zu begrüßen ist die jetzt vorgesehene zusammenfassende Darstellung der Auskunftssperren. Im Rahmen des informationellen Selbstbestimmungsrechts ist es jedoch nicht hinnehmbar, daß es nun auch in das Ermessen der Verwaltung gestellt sein soll, gegen den Willen des Betroffenen Auskünfte zu erteilen, obwohl der Betroffen zuvor in einem

Prüfverfahren (zumal für einen ohnehin nur begrenzten Zeitraum geltend) glaubhaft machen mußte, daß ihm aus einer Auskunft Gefahren für Leben, Gesundheit, persönliche Freiheit oder ähnliche **schutzwürdige Belange** erwachsen könnten. Damit besteht die Gefahr, daß diese „Schutzregelung" zu einer Scheinregelung verkommen könnte. In der praktischen Handhabung dürften darüber hinaus wegen der ggf. nicht absehbaren Rechtsfolgen den Beschäftigten der Meldebehörden kaum vertretbare Verantwortlichkeiten zugewiesen werden. Zudem würden die von mir im fünften Tätigkeitsbericht problematisierten Gefahren für Betroffene nicht nur unberücksichtigt bleiben, sondern sogar noch erweitert werden.

Im übrigen sollte den Meldestellen zur Pflicht gemacht werden, die Betroffenen vorsorglich auf das Auslaufen der Wirksamkeit beantragter Auskunftssperren hinzuweisen.

In der Stellungnahme wird mein sicherlich etwas ungewöhnlicher Vorschlag der **„gesetzlich sanktionierten Lüge"** bei diesbezüglichen Auskunftsersuchen abgelehnt, ohne daß eine argumentative Auseinandersetzung mit der Problematik erkennbar wäre. Mit einer Auskunft „Auskunftssperre nach § 32 Abs. 6 BbgMeldeG"[60] ist dem **Schutzzweck** Betroffener überhaupt nicht Rechnung getragen, weil gerade erst durch eine solche Auskunft der Auskunftssuchende den Hinweis erhält, daß sich eine Nachbarschaftsbefragung in dem Meldebereich „lohnt". Nur mit einer Auskunft „... ist hier nicht gemeldet" könnte der eigentliche Schutzzweck erreicht werden. Zumindest wären Recherchen des Anfragenden nicht mehr auf Auskünfte der Meldebehörden zurückzuführen.

Da auch nach vielfältiger Bestätigung vor Ort die bisher gesetzlich vorgesehene Auskunftsformel in Vergleichsfällen von den Mitarbeitern der Meldebehörden wegen der auch von diesen gesehenen möglichen fatalen Folgen als eine große menschliche Belastung empfunden wird, habe ich das MI noch einmal eindringlich gebeten, hier eine möglicherweise auch von meinen Vorschlägen abweichende, aber problembeseitigende Lösung zu finden.

Dagegen ist es erfreulich, daß in die zusammengefaßten Regelungen zu den Auskunftssperren auch die Unzulässigkeit von Melderegisterauskünften in Fällen der Änderung des Vornamens aufgrund der Vorschriften des **Transsexuellengesetzes** aufgenommen werden soll.

Der vorgelegte Entwurf sieht auch eine Zusammenfassung der Fälle vor, in denen die meldepflichtigen Einwohner einer **Datenweitergabe** (z. B. **an Parteien, Wählergruppen usw. im Zusammenhang mit Wahlen, Volksbegehren, Volksentscheiden sowie Bürgerentscheiden**) widersprechen können. Dabei sollen zukünftig die Betroffenen nicht nur bei der Anmeldung auf ihr **Widerspruchsrecht** hingewiesen werden, sondern mindestens auch einmal jährlich durch öffentliche Bekanntmachung, wobei angemessene Fristen für die Ausübung des Widerspruchsrechts festgesetzt werden sollen.

60 Brandenburgisches Meldegesetz vom 25. Juni 1992, GVBl. I S. 236

Mit diesen Widerspruchsregelungen verknüpft, soll jetzt auch ausdrücklich die Möglichkeit der Übermittlung von **Daten über Alters- und Ehejubiläen zum Zwecke der Veröffentlichung** durch Presse, Rundfunk und andere Medien an die für Veröffentlichungen zuständigen Stellen der Gemeinden gegeben werden. Dies begrüße ich besonders, weil mit dieser materiell-rechtlichen Bestimmung ein meine Behörde seit Jahren beschäftigendes Datenschutzproblem endlich aus der Welt zu schaffen sein dürfte[61].

Unvollständige Angaben

Den melderechtlichen Problemen, die bisher mangels Verfahrensregelungen für die **An- und Abmeldungen von Aussiedlern und Asylbewerbern** durch unvollständige Angaben entstehen konnten, soll jetzt dadurch begegnet werden, daß bei dem Bezug von Erstaufnahmeeinrichtungen und Gemeinschaftsunterkünften für Aussiedler oder Asylbewerber die An- und Abmeldungen durch den Leiter der Einrichtung durchgeführt werden können. Hierzu soll es möglich sein, daß nach vorheriger Abstimmung mit dem für diese Einrichtung zuständigen Ressort vom MI ein verkürztes Verfahren festgelegt wird.

Das gleiche Verfahren ist zwingend auch für Justizvollzugsanstalten oder „ähnliche Einrichtungen" vorgesehen. Ich habe das MI gebeten, den Begriff „ähnliche Einrichtung" - ggf. mit Verweisen innerhalb des Gesetzes - normenklar zu definieren.

Allgemeines

Daten sind nach dem **Ersterhebungsgebot** auch im Meldebereich zunächst immer bei den Betroffenen selbst (also „von den Einwohnern") zu erheben. Die vorgesehene Definition zur Aufgabenstellung der Meldebehörden, daß diese Melderegister führen, die Daten enthalten, die „über die Einwohner erhoben ... werden", impliziert, daß generell auch **am Meldepflichtigen vorbei** dessen Daten erhoben werden dürfen. Eine solche Regelung findet sich zu Recht in keinem der Meldegesetze der anderen Bundesländer, da die Fälle der Vervollständigung bzw. Korrektur der Melderegister ohne Hinzutun der Einwohner bereits durch den Zusatz „..., von Behörden und sonstigen öffentlichen Stellen übermittelt oder den Meldebehörden sonst amtlich bekannt werden" aufgefangen sind. Ich habe dem MI empfohlen, die bisherige Formulierung „die von den Einwohnern erhoben ... werden" beizubehalten.

Mit der Formulierung „die Meldebehörden dürfen personenbezogene Daten, ..., nur nach Maßgabe dieses Gesetzes oder sonstiger Rechtsvorschriften erheben, verarbeiten oder nutzen" waren bisher nicht alle Verarbeitungsvorgänge entsprechend § 3 Abs. 2 BbgDSG erfaßt, so daß eine Neuformulierung erforderlich war. Da jedoch die meldegesetzlichen Bestimmungen dem Brandenburgischen Datenschutzgesetz als Spezialnorm vorangehen, müssen auch die Begriffe innerhalb dieser Spezialnorm für sich verständlich definiert sein. Insoweit wäre die jetzt vorgesehene Reduktion auf den **Begriff „verarbeiten" nicht normenklar**, wenn nicht auch ein Verweis auf die Begriffsbestimmung des § 3 Abs. 2 BbgDSG angebracht würde. Ich habe das MI darauf hingewiesen, daß es jedoch besser wäre, wenn der Begriff „verarbeiten" - wie z. B. im Hamburgischen Meldegesetz - durch den Satz ergänzt würde: „Verarbeiten im Sinne dieses Gesetzes ist das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie Nutzen personenbezogener Daten.".

Es ist weiterhin vorgesehen, daß im Melderegister auch **„frühere Anschriften"** gespeichert werden. Dieser Begriff ist jedoch mißverständlich. Ich habe meine Ansicht an das MI herangetragen, daß hierunter doch wohl nur die unmittelbar vorherige Anschrift oder die unmittelbar vorherigen Anschriften (bei gleichzeitiger Haupt- und Nebenwohnung) und nicht

61 s. 4. Tätigkeitsbericht unter 12.2.1 und 5. Tätigkeitsbericht unter 12.4.2.1

alle bisherigen Anschriften seit erster Meldepflicht fallen können. Insoweit wäre eine erstmalige **begriffliche Klarstellung** erforderlich, zumal sich bei meiner letztjährigen Prüfung von Meldeämtern auch bei dortigen Mitarbeitern diesbezügliche Interpretationsunsicherheiten zeigten.

Die jetzt entsprechend dem Melderechtsrahmengesetz (MRRG)[62] vorgesehene **Verknüpfung der Datensätze** auch Volljähriger bis zum 27. Lebensjahr mit den Eltern ist gesellschaftspolitisch sinnvoll. Aber auch bei anderen - insbesondere allein lebenden - Personen ergeben sich über diese Altersgrenze hinaus nach meinen Erfahrungen häufig Situationen, in denen z. B. in Notfällen, im Falle der Gefahrenabwehr oder im Zusammenhang mit Suchmeldungen eine Verknüpfung zu anderen Personen sowohl zu eigenem Vorteil als auch von gesellschaftspolitischem Wert wären. Wenn auch nach dem MRRG eine solche Möglichkeit nicht vorgegeben ist, könnte jedoch landesrechtlich eine erweiternde Kann-Regelung dergestalt geschaffen werden, daß allen Meldepflichtigen gegen jederzeitigen Widerruf freigestellt wird, in ihren Meldedatensatz auch eine von ihnen genannte Person des Vertrauens mit deren Zustimmung (zusätzlich) eintragen zu lassen.

Aufgrund aktuellerer Rechtsentwicklungen in anderen Bereichen mußte ich in meiner Stellungnahme ergänzend noch auf folgende, für die Novellierung des Brandenburgischen Meldegesetzes relevanten Umstände hinweisen:

Im novellierten Brandenburgischen Kommunalwahlgesetz[63] kommt es - ebenso wie bereits seit 1994 im Brandenburgischen Landeswahlgesetz[64] - künftig für die **Zulassung zum aktiven und passiven Wahlrecht** nicht mehr auf den Hauptwohnsitz, sondern auf den **„ständigen Wohnsitz"** an. Der Hauptwohnsitz ist dann nur noch insoweit maßgeblich, als „der ständige Wohnsitz am Ort der Hauptwohnung vermutet" wird, diese Vermutung ist widerleglich. Der Umstand, daß es wegen dieser Anknüpfung bei Wahlen künftig auch den Begriff des „ständigen Wohnsitzes" im Meldegesetz geben müßte, ist in dem Novellierungsentwurf nicht berücksichtigt worden.

Derzeit werden auch die gemeinsamen bzw. in allen Bundesländern gleichlautenden Verwaltungsvorschriften (hier: MiStra) zum Justizmitteilungsgesetz neugefaßt. Nr. 12 a MiStra[65] bezieht sich auf die Tatsache, daß als Nebenfolge zu bestimmten Verurteilungen Wahlrechtsausschlüsse vorkommen bzw. vorkommen können und daß diese demzufolge den jeweils zuständigen Meldebehörden mitgeteilt werden müßten. Bei den Überlegungen zu den Neuformulierungen der MiStra wird z. Z. nicht davon ausgegangen, daß es bzgl. des Wohnsitzes in Verbindung mit dem Wahlrecht neue Entwicklungen gibt. Insbesondere ist in der bisherigen Konzeption der Neufassung der MiStra nicht berücksichtigt worden, daß der **Wahlrechtsausschluß** in der Regel nur für eine begrenzte Zeit besteht und daß deshalb entweder zusätzlich die **Dauer** oder aber zusätzlich die **Beendigung** des Wahlrechtsausschlusses mitgeteilt werden muß. Aus der Veränderlichkeit des Ausschlusses folgt allerdings, daß der Meldebehörde nicht die Dauer, sondern jeweils Anfang bzw. Ende des Wahlrechtsausschlusses von der bei der Justiz zuständigen Stelle mitgeteilt werden müssen. Dies bedeutet zusammenfassend, daß noch folgende Probleme bzgl. des Brandenburgischen Kommunalwahlgesetzes ohnehin und unmittelbar (a), aber auch bzgl. der Neufassung der MiStra (b) im Brandenburgischen Meldegesetz zu lösen sind:

---

62 i. d. Fass. vom 24. Juni 1994, BGBl. I S. 1430, geänd. durch Art. 3 zur Neuordnung des Erfassungs- und Musterungsverfahrens vom 12. Juli 1994, BGBl. I S. 1497

63 vom 30. März 1998, GVBl. S. 54; s. unter 3.1.3.1

64 vom 2. März 1994, GVBl. I S. 38, geänd. durch Art. 2 d SWG vom 7. Juli 1994, GVBl. I S. 294

65 s. unter 4.1.3

zu a)

- Begriff des ständigen Wohnsitzes in Relation zum Hauptwohnsitz
- Befugnis zur Speicherung der Bestimmung, daß eine Wohnung ständiger Wohnsitz ist
- Befugnis zur Speicherung der Änderung dieser Bestimmung
- Befugnis zur Übermittlung der Bestimmung einer Wohnung zum ständigen Wohnsitz an andere Stellen

zu b)

- Berücksichtigung des Datums der Beendigung des Wahlrechtsausschlusses (die Tatsache des Ausschlusses selbst wird bereits jetzt berücksichtigt und müßte dann „Beginn des Ausschlusses" werden).

Wegen der datenschutzrechtlichen Bedeutung des Gesetzes habe ich es für angemessen erachtet, das MI zu bitten, daß es - ungeachtet des weiteren Gesetzgebungsgangs - im Rahmen unmittelbaren Schriftwechsels auf meine Fragestellungen und Hinweise eingeht und meiner Behörde ggf. die Ablehnung meiner Regelungsvorschläge erläutert.

3.1.2 Neue Verordnung über regelmäßige Datenübermittlungen der Meldebehörden

Noch vor Verabschiedung eines novellierten Brandenburgischen Meldegesetzes[66] hat das MI eine Ablösungsverordnung zur Datenübermittlungsverordnung (MeldDÜV)[67] erlassen. Über die Erforderlichkeit einer möglichst umgehenden inhaltlichen Neufassung hatte ich bereits in meinem vierten Tätigkeitsbericht[68] berichtet. Meine abschließend im letzten Tätigkeitsbericht[69] dargestellten Forderungen und Anregungen sind dabei leider nur z. T. berücksichtigt worden.

So konnte bzgl. der regelmäßigen **Datenübermittlungen an den ORB bzw. an die Gebühreneinzugszentrale (GEZ)** zum Zweck des Gebühreneinzugs dahingehend Einvernehmen erzielt werden, daß eine solche zwar monatlich, aber erst mit einer zeitlichen Verzögerung von mindestens zwei Monaten nach der Anmeldung, Abmeldung oder dem Tod volljähriger Einwohner erfolgen darf. Damit ist der Gefahr begegnet, daß meldepflichtige Personen als potentielle Schwarzhörer und -seher eingestuft werden, noch ehe sie die Chance hatten, sich von sich aus innerhalb einer angemessenen Frist anzumelden. Daß mit der gegenwärtigen und bisherigen (letzten) Anschrift auch jeweils der Rufname mit übermittelt werden soll, ist unter dem Aspekt hinnehmbar, daß die übermittelten Daten nur verwendet werden dürfen, um Beginn und Ende der Gebührenpflicht sowie die zuständige Rundfunkanstalt zu ermitteln und sie nach Erfüllung dieser Aufgaben spätestens innerhalb eines halben Jahres zu löschen sind.

Meine bisherigen Bedenken, **ehrenamtlichen Bürgermeistern** außer Daten von Alters- und Ehejubilaren auch weitere Meldedaten zu übermitteln, sind zumindest insoweit berücksichtigt worden, als jenen die **Grunddaten von Einwohnern ihres Gemeindegebietes** nicht bei An- und Abmeldungen, sondern ausschließlich **bei deren Geburt oder Tod** unter Angabe des betreffenden Tages übermittelt werden dürfen. Dadurch können zumindest keine parallelen Meldedateien aufgebaut werden und der Umfang der zur Verfügung gestellten Daten bleibt auf den Rahmen des aufgabenimmanenten Informationsbedürfnisses ehrenamtlicher Bürgermeister beschränkt. Im übrigen greift auch hier die in der neuen MeldDÜV

---

66 s. unter 3.1.1

67 Verordnung über regelmäßige Datenübermittlungen der Meldebehörden vom 7. August 1997, GVBl. II S. 734

68 s. 4. Tätigkeitsbericht unter 3.1.1

69 s. 5. Tätigkeitsbericht unter 3.1.1.2

für alle Übermittlungsvorgänge geltende Regelung der Zugangs- und Zugriffssicherung sowie der Verpflichtung zur Löschung, sobald die Daten (Anmerkung: konkret und auf den Einzelfall bezogen) zur Aufgabenerfüllung nicht mehr erforderlich sind.

Auch an dieser Stelle muß ich wiederum mit Bedauern zur Kenntnis nehmen, daß meine **Forderungen nach Verschlüsselung** aller regelmäßig zu übermittelnden, elektronisch gespeicherten Daten nicht nur in der MeldDÜV **nicht berücksichtigt** worden sind, das MI sich mit meinen Begründungen zu deren Erforderlichkeit inhaltlich überhaupt nicht auseinandergesetzt hat. Dies wird durch die Stellungnahme der Landesregierung[70] zu meinem letztjährigen Tätigkeitsbericht, in der hierauf inhaltlich ebenfalls nicht eingegangen wird, bestätigt. Ich halte es nach meinen bisherigen Ausführungen in dieser Sache, die ihren Niederschlag insbesondere in meinem vorigen Tätigkeitsbericht[71] gefunden hatten, für völlig unangemessen, dieses Grundsatzproblem mit dem Hinweis abzutun, daß nach den Verfahrensregelungen in § 2 MeldDÜV der Hinweis auf die Beachtung des § 10 BbgDSG (Technische und organisatorische Maßnahmen) darüber hinausgehende Vorschriften zu Datensicherungen (Verschlüsselung von Daten) entbehrlich machten.

In Anbetracht immer stärkerer Vernetzungen - gerade auch der Verwaltungen untereinander - und der damit verbundenen besonderen Gefahren bzgl. der Datensicherung auf den Übertragungswegen wird sich die Landesregierung auf Dauer einer in die Zukunft weisenden Positionierung nicht entziehen können.

3.1.3 Kommunalwahl 1998

3.1.3.1 Änderung des Kommunalwahlgesetzes

Seit April 1998 hat Brandenburg ein geändertes Kommunalwahlrecht. Die Änderung des Brandenburgischen Kommunalwahlgesetzes (BbgKWahlG)[72] betrifft im wesentlichen vier Schwerpunkte: erhöhte Anforderungen an Einleitung und Durchführung der Bürgermeisterabwahl durch Volksbegehren und Volksentscheid, künftige Anknüpfung der Berechtigung für das aktive und das passive Wahlrecht an den ständigen Wohnsitz statt an den Hauptwohnsitz, Wahlrecht für EU-Ausländer bei Kommunalwahlen und eine neue Inkompatibilitätsregelung für leitende Mitarbeiter kommunaler Einrichtungen.

In Brandenburg können Bürgermeister auf zwei verschiedenen Wegen „abgewählt" werden, zum einen durch qualifizierte Mehrheit der Gemeindevertretung und zum anderen durch Votum der Bevölkerung. Für letzteres ist das für Brandenburg geltende reguläre Verfahren von Bürgerbegehren und Bürgerentscheid anzuwenden. Bisher war bereits ein Bürgerbegehren erfolgreich, wenn sich 10 % der kommunalen Wahlberechtigten für die Durchführung eines (dann erforderlich werdenden) Bürgerentscheids aussprachen. Für den Bürgerentscheid waren sodann 25 % der Stimmenanteile das Quorum für eine erfolgreiche Abwahl. Die geringen Anforderungen an das Bürgerbegehren führten in Brandenburg zu einem ausgesprochenem „Bürgermeister-Kegeln".
Um dieser Tendenz einen Riegel vorzuschieben, hatte die Landesregierung bereits in ihrem Entwurf für das BbgKWahlG ein abgewandeltes Verfahren für Bürgerbegehren und Bürgerentscheide konkret für das Ziel der Bürgermeister-Abwahl vorgesehen, die Quoren für das Bürgerbegehren von 10 % auf 25 % und für den Bürgerentscheid von 25 % auf 33 % heraufzusetzen und die Rahmenbedingungen für das Bürgerbegehren in mehreren Punkten zu verschärfen.

---

70 s. unter 3.1.1

71 s. 5. Tätigkeitsbericht unter 3.1.1.2 und 12.4.1.2

72 vom 30. März 1998, GVBl. I S. 54

Da die „Abwahl“ bei einem Bürgerbegehren nicht tatsächlich einer Wahl entspricht, sondern durch das Sammeln von Unterschriften in einem bestimmten Zeitraum eingeleitet werden muß, sah ich mehrere Ansatzpunkte, an denen den datenschutzrechtlichen Belangen Nachdruck verliehen werden mußte. Das entscheidende Problem habe ich allerdings in den neuen Quoren selbst gesehen und habe mich deshalb für eine Verbesserung des Datenschutzes und für eine Senkung der vorgesehenen Quoren mit folgender Argumentation eingesetzt:

Das Bürgerbegehren erfolgt durch das Sammeln von Unterschriften auf Unterschriftenlisten. Die Unterzeichnung ist aber nur dann „gültig“, wenn die unterzeichnenden Personen wahlberechtigt sind, d. h., wenn sie in der Gemeinde wohnen, über 18 Jahre alt und nicht vom Wahlrecht ausgeschlossen sind. Aus diesem Grund müssen auf den Unterschriftenlisten alle diese Angaben von jeder unterzeichnenden Person vollständig aufgeschrieben werden. Anschließend müssen die Angaben durch einen Abgleich mit den Meldedaten bestätigt werden. Daß alle Angaben von den jeweils folgenden Unterzeichnern zur Kenntnis genommen werden können, ist nicht zu vermeiden. Daher muß sichergestellt sein, daß den Unterzeichnern lediglich solche Daten (Name, Vorname, Anschrift und Unterschrift) abgefordert werden, die zu ihrer Identifizierung und zum Abgleich mit dem Melderegister unabdingbar sind. Weitere Daten zu verlangen, ist aus datenschutzrechtlicher Sicht unzulässig.

Erfahrungen aus anderen Bundesländern mit Sammel-Listen haben gezeigt, daß der prozentuale Anteil an Wählerstimmen, je nachdem, ob es sich um kleine, mittlere, mittelgroße oder große Gemeinden handelt, nicht in gleicher Weise erreicht werden kann. Diese Tatsache führt zu dem Ergebnis, daß zwar in einer Gemeinde mit z. B. 1.000 Einwohnern ein Quorum von 25 % fast immer erreicht wird. 25 % in einer Gemeinde mit mehr als 50.000 Einwohnern sind aber nach aller Erfahrung nicht erreichbar; bei einer Großstadt erweist sich ein Quorum von 25 % als unüberwindbares Hindernis. Die Folge ist, daß eine kleine Gemeinde ihren Bürgermeister bereits durch eine größere Zahl von - aus welchen Gründen auch immer - unzufriedenen Wahlberechtigten „los wird“, daß aber in einer Großstadt selbst bei offensichtlichem Mißmanagement der Bürgermeister durch Bürgerbegehren und Bürgerbescheid kaum abzusetzen sein dürfte. Daß eine solche gesetzliche Regelung unzulässig sein muß, weil sich dadurch eine Ungleichheit zwischen Bewohnern (und auch für die Bürgermeister) kleiner und großer Gemeinden ergibt, ist zwar vordergründig keine Frage des Datenschutzes; diese ist aber insoweit tangiert, als bei erkennbar untauglichen Versuchen eine Fülle von nicht verwendungsfähigen Daten gesammelt wird. Ich habe mich deshalb in meiner Stellungnahme gegenüber der Landesregierung und gegenüber dem Landtag dafür eingesetzt, kein einheitliches Quorum vorzugeben, sondern im Gesetz eine Staffelung von Mindestzahlen, die erfahrungsgemäß erreicht werden können festzuschreiben.

Das nun verabschiedete Gesetz enthält Quoren-Stufen von 25, 20 und 15 % für das Bürgerbegehren, je nach dem, ob die Gemeinde weniger als 20.000, weniger als 60.000 oder über 60.000 Einwohner hat. Die Mindeststimmenzahl, die anschließend beim Bürgerentscheid erreicht werden muß, ist mit 25 % gegenüber dem Stand vor der Novellierung des BbgKWahlG unverändert hoch geblieben. Meine weiteren Kritikpunkte aus der Sicht des Datenschutzes wurden weder von der Landesregierung noch vom Landtag aufgegriffen.
Zu den Schwerpunkten „ständiger Wohnsitz“ und Anpassung des Wahlrechts für EU-Bürger werden Ausführungen unter 3.1.1 bzw. unter 4.1.3 gemacht.

3.1.3.2 Kommunalwahlverordnung

Die Landesregierung wird nach der Novellierung des Kommunalwahlgesetzes auch die Kommunalwahlverordnung

(BbgKWahlV)[73] ändern. Der Entwurf der Änderungsverordnung hat mir zur Stellungnahme bereits vorgelegen.

Anders als bei dem BbgKWahlG waren bei der Durchführungsverordnung nur wenige Hinweise auf Verbesserungen zu geben. Ich habe mich insbesondere dafür ausgesprochen, daß die mit der Durchführung der Wahl betrauten Personen deutlich auf ihre Verschwiegenheitspflicht hingewiesen werden, insbesondere auch darauf, daß diese Pflicht nicht mit der Beendigung ihrer Tätigkeit beim Wahlvorhaben endet.

Außerdem habe ich gefordert, daß genauere Bestimmungen über das Verfahren der Vernichtung von Wahlunterlagen in die KWahlV aufgenommen werden. Hierzu gehört vor allem die Pflicht, die Vernichtung nach Zeit und Ort sowie hinsichtlich veranlassender, durchführender und verantwortender Personen zu dokumentieren und darüber hinaus festzulegen, daß die sogenannten „10 Gebote" der technisch-organisatorischen Sicherheit des BbgDSG bei der Unterlagenvernichtung nicht nur eingehalten werden, sondern daß deren Einhaltung ebenfalls zu dokumentieren ist.

3.1.4 Änderung des Personenstandsgesetzes

Der Gesetzgebungsgang bezüglich eines Fünften **Gesetzes zur Änderung des Personenstandsgesetzes (5. PStÄndG)** stagniert. Nach Informationen aus dem zuständigen Referat des Bundesministeriums des Innern (BMI) vom Beginn des Berichtszeitraums müßten zunächst die umfangreichen Stellungnahmen der Länder zum Vorentwurf (Stand: 25. März 1996) ausgewertet werden, bevor eine erneute Besprechung mit den Ländervertretungen im Jahr 1998 stattfinden könne. Daher werde die Erstellung eines offiziellen Referentenentwurfs keinesfalls noch in der 13. Legislaturperiode des Bundestages möglich sein.

Meine gegenüber dem MI geäußerten Anregungen und Empfehlungen zum o. a. Vorentwurf hatte ich in meinem vorigen Tätigkeitsbericht dargestellt[74].

---

[73] vom 31. Juli 1993, GVBl. II S. 412, geänd. durch VO vom 18. Dezember 1995, GVBl. II S. 738

[74] s. 5. Tätigkeitsbericht unter 3.1.2

Der Stellungnahme der Landesregierung zum letzten Tätigkeitsbericht (Stellungnahme)[75] ist zu entnehmen, daß sich das Land Brandenburg zu meiner Forderung, in Anlehnung an § 28 Abs. 1 Satz 2 BbgDSG bei der **Auskunftserteilung zu wissenschaftlichen Zwecken** die Empfänger, die Art der zu übermittelnden personenbezogenen Daten, den Kreis der Betroffenen und den konkreten Forschungszweck im Zustimmungsbescheid der jeweiligen Verwaltungsbehörde zu bezeichnen und diese Zustimmung dem LfD mitzuteilen, in seiner Stellungnahme nicht mehr (rechtzeitig) habe äußern können. Leider findet in der Stellungnahme eine inhaltliche Auseinandersetzung mit meiner „Nachforderung" nicht statt, so daß mir nicht erkennbar ist, ob und inwieweit in diesem Punkt Übereinstimmung mit dem MI besteht. Mir ist im übrigen nicht verständlich, weshalb es gerade bei den Terminabläufen dieses Gesetzgebungsverfahrens nicht möglich sein sollte, ggf. berechtigte Regelungsvorschläge auch noch nach offiziellem Redaktionsschluß für die Stellungnahmen der Länder beim BMI nachzureichen.

Meine letztjährigen Ausführungen, zur Vermeidung diskriminierender Spekulationen einen **fiktiven Todeszeitpunkt** festzulegen, wenn der genaue Todeszeitpunkt nicht feststellbar ist, will das MI aus dort gesehenen Rechtsfolgegründen zwar nicht mittragen, es war dankenswerterweise jedoch bereit, meine an eine entsprechende, bereits vorhandene Regelung bzgl. des Sterbeortes angelehnte Empfehlung an den BMI weiterzuleiten.

Erfreulicherweise wurde meine Forderung, insbesondere im Hinblick auf eine mögliche **elektronische Führung des Zweitbuches** Maßnahmen zur Gewährleistung des Datenschutzes entweder im Personenstandsgesetz selbst zu regeln oder zumindest auf die Anwendbarkeit des § 9 BDSG (bzw. der entsprechenden Bestimmungen in den Landesdatenschutzgesetzen) zu verweisen, in die Stellungnahme des Landes aufgenommen.

Hinnehmbar ist die Auffassung des MI, daß **technische und datenschutzrechtliche Aspekte** nicht im Gesetz selbst geregelt werden müssen, sondern im Rahmen der Ermächtigungsgrundlage für den Bundesminister des Innern auch **in** entsprechenden **Rechtsverordnungen** u. a. zur Führung „elektronischer Zweitbücher" und zur Anwendung technischer Hilfsmittel ausführlicher geregelt werden können. Dabei gehe ich jedoch davon aus, daß sich die dort zu regelnden datenschutzrechtlichen Aspekte auch nur auf den dort zu regelnden ADV-Einsatz beziehen können.

Zwar wird in der Stellungnahme nicht auf meine letztjährigen Ausführungen zu den **Aufbewahrungsfristen für elektronisch geführte Zweitbücher**, die nach meinen Dafürhalten auch für andere Anwendungsgebiete Bedeutung haben, eingegangen, jedoch halte ich meine diesbezüglichen Darstellungen im Rahmen ihrer allgemeinen Bedeutung für zunächst ausreichend; bezogen auf den Bereich des Personenstandsgesetzes wird es darauf ankommen, daß sie zumindest im Wege einer Rechtsverordnung zu den Zweitbüchern Berücksichtigung finden werden.

3.1.5 Problematische Datenverarbeitung im Auftrag bei Software-Umstellung

Eine Amtsverwaltung hatte sich an mich gewandt und nachgefragt, ob es zulässig sei, im Zuge einer Software-Umstellung ganze Datenbestände wie Meldedaten und Daten des Haushalts-, Kassen- und Rechnungswesens (HKR) an eine private Firma zu geben, die für die **Umformatierung der Daten** einige Wochen benötige. Diese Firma hat ihren Sitz außerhalb des Landes Brandenburg.

Im Hinblick auf das Einwohnermeldewesen war dieses Vorhaben deshalb bereits rechtswidrig, weil nach § 35 Abs. 1 BbgMeldeG eine Datenverarbeitung im Auftrag durch eine nicht-öffentliche Stelle der Zustimmung des MI bedarf, die aber

[75] LT-Drs. 2/4768 vom 15. Dezember 1997

nicht vorlag. Denn eine solche Datenverarbeitung im Auftrag außerhalb des Landes Brandenburg ist nach der derzeitigen Rechtslage unzulässig.

Für die Daten des HKR-Verfahrens sind diese strengen Anforderungen zwar nicht gegeben. Allerdings werden hier ebenfalls regelmäßig auch sensible personenbezogene Daten gespeichert, darunter auch solche, die dem Steuergeheimnis unterliegen, so daß ich auch hier von der geplanten Umformatierung am anderen Ort dringend abraten mußte.

Außerdem wäre das Vorhaben der Firma insgesamt nicht nachvollziehbar gewesen, weil die Umformatierung nicht vor Ort unter Kontrolle der Amtsverwaltung stattfinden sollte. Mit einer Kontrolle vor Ort würde der Firma von vornherein die Möglichkeit genommen werden, unzulässige Einsichten in personenbezogene Massendaten oder unzulässige Datenkopien zu erhalten. Für den Fall, daß die Firma zunächst nicht in der Lage gewesen wäre, die erforderlichen Arbeiten mit einem vertretbaren Zeitaufwand in der Amtsverwaltung durchzuführen, habe ich empfohlen, ihr zunächst eine kleinere Menge anonymisierter Daten zu Testzwecken zur Verfügung zu stellen, weil nach § 13 Abs. 3 BbgDSG personenbezogene Daten nicht zu Testzwecken verwendet werden dürfen.

Ich habe zudem darauf hingewiesen, daß selbst bei diesem Verfahren der Abschluß eines Vertrages mit der Firma nach § 11 Abs. 1 BbgDSG erforderlich wäre, weil auch in diesem Fall eine Datenverarbeitung im Auftrag vorliegt und die Firma selbst im Amtsgebäude zumindest in Einzelfällen Einsicht in personenbezogene Daten erhalten könnte.

Erfreulicherweise hat die Amtsverwaltung umgehend reagiert. Der Vertrag sieht jetzt vor, daß die Datenumformatierung nur vor Ort unter Kontrolle stattfindet.

3.2 Grundstückswesen

3.2.1 Änderung des Vermessungs- und Liegenschaftsgesetzes

Im Berichtszeitraum hat die Landesregierung das Vermessungs- und Liegenschaftsgesetz[76] novelliert und zeitgleich eine Liegenschaftskataster-Datenübermittlungsverordnung (LiKaDÜV)[77] erlassen.

Im Rahmen einer bemerkenswert guten und vertrauensvollen Zusammenarbeit mit dem MI sind letztendlich meine datenschutzrechtlichen Bedenken und Forderungen berücksichtigt worden. So wurde u. a. die Vorstellung der Landesregierung, das Liegenschaftskataster uneingeschränkt der Öffentlichkeit zugänglich zu machen, aufgegeben. Durch einen Datenabgleich wäre es ohne jede Schwierigkeit möglich, einen Vermögensabgleich zu allen Personen, die Grundstückseigentümer sind, durchzuführen, wenn die Darlegung eines berechtigten Interesses zur Einsichtnahme in das Liegenschaftskataster entfallen wäre. Ich habe mich gegen eine voraussetzungslose Einsichtnahme ausgesprochen. Es war für mich nicht nachzuvollziehen, weshalb einerseits das Bank- und Steuergeheimnis uneingeschränkt hochgehalten, während andererseits Informationen über das Grundstückseigentum völlig uneingeschränkt zugänglich gemacht werden soll. Ich habe durch entsprechende Eingaben von Petenten die Erfahrung gemacht, daß es gerade die Kataster- und Grundbucheintragungen sind, die als sehr persönlich empfunden und gegen Offenlegung geschützt werden sollten.

---

[76] vom 8. Dezember 1997, GVBl. I S. 116

[77] Verordnung über die Einrichtung automatisierter Abrufverfahren und regelmäßiger Datenübermittlungen im Liegenschaftskataster vom 17. Dezember 1997, GVBl. II 1998, S. 13

3.2.2 Pilotprojekt „Einrichtung eines Abrufsverfahrens im Automatisierten Liegenschaftsbuch (ALB)“

Im Mai 1997 wurde ich über den Plan des Hauptamtes des Landkreises Potsdam-Mittelmark informiert, einen Anschluß an das Automatisierte Liegenschaftsbuch (ALB) durchzuführen. Hier handelte es sich um ein Pilotverfahren für das Land Brandeburg. Als Nutzer kommen vor allem Stellen der Bauplanung und der Bauaufsicht sowie die Straßenverkehrsbehörden, aber auch Stellen, die u. a. mit Angelegenheiten des Umweltschutzes befaßt sind, in Betracht. Meine Behörde wurde gebeten, das Projekt unter datenschutzrechtlichen Aspekten zu begleiten.

Bei dem Projekt ist ein lediglich lesender Zugriff auf die Katasterdaten geplant. Zur Diskussion steht u. a. der Umfang der Informationen aus dem Datenbestand, die den Katasterunterlagen entnommen werden können, sowie das Ausmaß der „Bürgerfreundlichkeit“, d. h., ob vorwiegend Kürzel und Ziffern oder eher vollständige Aussagen angeboten werden sollen. Des weiteren war zu bedenken, welchen Umfang und welche Bereiche jeweils auch für Dritte (Einzelpersonen bzw. nicht-öffentliche Stellen) erkennbar gemacht werden sollten. In bezug auf die Datensicherheit wurden insbesondere Fragen der Zugriffsberechtigung sowie der Protokollierung von Zugriffen erörtert.

Der Probebetrieb wurde gegen Ende des Jahres 1997 aufgenommen.

3.3 Polizei

3.3.1 Einsatzleitsystem der Polizei

Anfang 1996 wurde der Zentraldienst der Polizei für Technik und Beschaffung (ZTB) mit der Anschaffung eines **Einsatzleitsystems für die Brandenburgische Polizei** (ELSBB) beauftragt. Im Berichtszeitraum ist der Pilotbetrieb in der Einsatzleitzentrale des Polizeipräsidiums Oranienburg mit Echtdaten angelaufen. Bis Ende 1998 sollen alle Polizeipräsidien des Landes mit ELSBB ausgestattet werden. Im Herbst 1997 habe ich das Pilotverfahren in Augenschein genommen.

Die in der Zentrale eingehenden Einsatzanforderungen wurden an 10 Arbeitsplätzen abgewickelt, im Endausbau sollen es 30 sein. Den Sachbearbeitern stehen für die Einsatzunterstützung vor Ort folgende Hintergrunddatenbanken zur Verfügung:

- Kfz-Sicherstellung,
- Blutentnahme,
- Kranken-/Leichenwagen,
- Abschleppfirmen,
- Bereitschaftspersonen,
- Schlüsselträger,
- sensible Betriebe (siehe § 30 Abs. 2 Nr. 2 und 3 BbgPolG),
- Gefahrenmeldeanlage in Institutionen,
- Telefonbuch,
- Straßen-, Ort- und Objektdatenbanken.

Noch nicht umgesetzt war die Ortung von Notrufsignalen. Zum Zeitpunkt der Vorführung war der Einsatzsachbearbeiter

noch darauf angewiesen, daß ihm die Ortsangaben vom Notrufenden geliefert werden. Wenn der Anruf von einer ISDN-Anlage abgesetzt worden ist, stellt das System die Telefonnummer automatisch zur Verfügung.

Das System würde auch die Ortung von Polizeifahrzeugen bzw. Sprechfunkgeräten über das sog. **Global Positioning System (GPS)** ermöglichen. Dies ist jedoch noch nicht umgesetzt, weil der Gesamtpersonalrat der Polizei Einwände erhoben hat. Position und Einsatzstatus erfährt der Einsatzsachbearbeiter in der Leitstelle daher über eine Funkmeldung des Einsatzfahrzeugs bzw. des mit Funkgerät ausgestatteten Polizeibeamten.

An einem eigenständigen Arbeitsplatz „Datenpflege" werden die Hintergrunddatenbanken ständig ergänzt bzw. korrigiert. Das System aktualisiert automatisch die an allen Arbeitsplätzen zur Verfügung stehenden Einsatzmittel. Gepflegt wird das ELSBB über einen weiteren abgesetzten Arbeitsplatz. Für beide Arbeitsplätze sind eigene Mitarbeiter der Einsatzleitzentrale abgestellt.

Die Vorführung des Pilotbetriebs ergab keine datenschutzrechtlichen Mängel.

3.4 Verfassungsschutz

3.4.1 Sicherheitsüberprüfungsgesetz

Der im Berichtszeitraum vorgelegte Entwurf eines Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen im Land Brandenburg (Sicherheitsüberprüfungsgesetz - BbgSÜG) ist aus datenschutzrechtlicher Sicht zu begrüßen, weil die Überprüfungen damit eine gesetzliche Grundlage erhalten. Der Entwurf stellt - wie die Gesetze der anderen Bundesländer und des Bundes - auf die Einwilligung der Betroffenen und beteiligten Personen in die Sicherheitsüberprüfung ab. Allerdings muß man dabei auch bedenken, daß die betroffenen Personen einer Sicherheitsüberprüfung mit dem Wissen zustimmen, anderenfalls den Arbeitsplatz nicht zu erhalten oder das berufliche Fortkommen zu gefährden. Sie müssen daher in der Lage sein, das Verfahren nachzuvollziehen und die Tragweite sowie Konsequenzen einzelner Überprüfungsschritte abzuschätzen. Dies stellt hohe Anforderungen an die Normenklarheit der einzelnen Regelungen des Entwurfs. Die Landesregierung hat sich erkennbar bemüht, diesen Anforderungen in Einzelregelungen gerecht zu werden. Es ist ihr dies jedoch nicht durchgängig gelungen.

Wie bereits bei dem bislang auf der Grundlage einer Verwaltungsvorschrift durchgeführten Verfahren ist die Behörde oder sonstige öffentliche Stelle, in der sicherheitsempfindliche Tätigkeiten anfallen, zuständig für die Sicherheitsüberprüfung. Für die organisatorische Abwicklung bestellt sie einen Geheimschutzbeauftragten. **Mitwirkende Behörde an den Sicherheitsüberprüfungen** ist die brandenburgische Verfassungsschutzbehörde, die prüft, ob sicherheitsrelevante Erkenntnisse über die von einer Sicherheitsüberprüfung betroffenen Person vorliegen. Die Art der Sicherheitsüberprüfung, d. h. bis in welche Bereiche der Betroffene eine Überprüfung seiner Privatsphäre hinnehmen muß, richtet sich nach der **Einstufung der Verschlußsachen**, mit denen er bei seiner Tätigkeit in Berührung kommt. Hier sind vier Einstufungen vorgesehen, die von „Nur für den Dienstgebrauch", „VS-Vertraulich", „Geheim" bis „Streng Geheim" reichen. Dementsprechend ist eine **einfache Sicherheitsüberprüfung** für diejenigen vorgesehen, die Zugang zu „VS-Vertraulich" eingestuften Vorgängen haben. Einer **erweiterten Sicherheitsüberprüfung** müssen sich diejenigen unterziehen, die mit geheimen bzw. zu einer großen Anzahl von vertraulichen Verschlußsachen zu tun haben. Zugang zu streng geheimen bzw. einer großen Anzahl von geheimen Unterlagen setzt das Bestehen einer **erweiterten Sicherheitsüberprüfung mit Sicherheitsermittlungen** voraus.

Das Gesetz regelt nicht nur den Geheim- und Sabotageschutz bei öffentlichen, sondern auch bei nicht-öffentlichen Stellen. Aufgrund der Kompetenzzuweisung obliegt die datenschutzrechtliche Kontrolle hier jedoch dem brandenburgischen Innenministerium.

Sicherheitsüberprüfungen stellen einen tiefgreifenden Eingriff in die Persönlichkeitsrechte der betroffenen und beteiligten Personen dar, der nur gerechtfertigt ist, wenn die Kenntnisnahme von Verschlußsachen zur Aufgabenerfüllung durch die betroffene Person unerläßlich ist. Die öffentlichen und nicht öffentlichen Stellen sollten daher verpflichtet werden, Vorkehrungen zu treffen, die einen größtmöglichen Zugangsschutz für Verschlußsachen gewährleisten, damit der Kreis der von einer Sicherheitsüberprüfung betroffenen Person nicht unnötig weit gezogen wird. Bedauerlicherweise fehlt dem vorgelegten Entwurf eine solche Verpflichtung im Gesetzestext selbst oder zumindest ein Hinweis darauf in der Begründung. Dies ist umso bedauerlicher, als bei einer erweiterten Sicherheitsüberprüfung mit Sicherheitsermittlungen festgelegt ist, daß bereits eine Tätigkeit in als Sicherheitsbereich eingestuften Teilen von Behörden oder öffentlichen Stellen eine solche Überprüfung voraussetzt, ohne daß der Betroffene selbst Zugang zu Verschlußsachen hat.

Eine Regelung, die den Kreis der in eine Sicherheitsüberprüfung einbezogenen Personen sehr ausweitet, findet sich in der Vorschrift zur Datenerhebung (§ 13 des Entwurfs). Dort ist die Befragung anderer geeigneter Personen oder Stellen in den Fällen vorgesehen, in denen die Erhebung bei der zu überprüfenden oder bei der einbezogenen Person nicht ausreicht. Der Vorschrift fehlt jedoch eine Definition und damit auch eine Eingrenzung der „geeigneten Personen oder Stellen", so daß für die Betroffenen nicht mehr absehbar ist, welche anderen Personen in die Befragungen mit einbezogen werden können. Der Gesetzgeber setzt der Verfassungsschutzbehörde als mitwirkender Stelle so keine Abgrenzungskriterien des bei einer Sicherheitsüberprüfung zu befragenden Personenkreises.

Weiterhin ist dem Entwurf nicht zu entnehmen, daß die erhobenen Daten in dem **Nachrichtendienstlichen Informationssystem der Verfassungsschutzbehörden (NADIS)** gespeichert und zur Aufgabenerfüllung der Verfassungsschutzbehörden des Bundes und der Länder genutzt werden dürfen. Dieser Umstand ebenso wie die fehlende Abgrenzung der zu befragenden Personen läßt es zweifelhaft erscheinen, ob die Aufklärung der Betroffenen - unerläßlicher Bestandteil der Einwilligung in eine Maßnahme - datenschutzrechtlichen Anforderungen genügt. Bei mangelhafter Aufklärung ist aber die Einwilligung unwirksam. Ich habe daher angeregt, den Kreis der zu befragenden „geeigneten Personen und Stellen" genauer zu definieren sowie festzulegen, daß die Betroffenen schon vor der Datenerhebung darauf hinzuweisen sind, daß personenbezogene Angaben zu ihrer Person in NADIS gespeichert werden.

Auch die Vorschrift über die Maßnahmen, die bei einzelnen Überprüfungsarten durchzuführen sind (§ 14 des Entwurfs), ist nicht ausreichend normenklar geregelt. Auch hier sind wiederum weitere geeignete Auskunftspersonen vorgesehen, ohne daß definiert ist, worin ihre Geeignetheit besteht. Der Betroffene ist damit in der Wahrnehmung seiner Rechte beschränkt, weil u. a. nicht geregelt ist, wie er über solche Personen und ihre Beteiligung Kenntnis erhalten kann. Weiterhin ist es in das Ermessen des Verfassungsschutzes als mitwirkender Behörde gestellt, Einzelmaßnahmen der nächsthöheren Art der Sicherheitsüberprüfung durchzuführen. Die zusätzliche Erhebung muß der betroffenen Person erst mitgeteilt werden, wenn der Zweck der Erhebung dies zuläßt. Damit wird wiederum die Wirksamkeit der Einwilligung der Betroffenen berührt. Es ist nicht nachzuvollziehen, warum in den Fällen, in denen während des Überprüfens sicherheitserhebliche Erkenntnisse angefallen sind, der Betroffene nicht darüber informiert werden kann, daß solche nunmehr vorliegen und daß sie nur ausgeräumt werden können, wenn er einer Erweiterung der Sicherheitsüberprüfung zustimmt.

Die Regelung zur Speicherung, Veränderung und Nutzung personenbezogener Daten (§ 22 des Entwurfs) läuft dem

durchgängigen Prinzip zuwider, daß Sicherheitsüberprüfungen nur mit Zustimmung der Betroffenen durchgeführt werden, die eine umfassende Information über alle Einzelheiten der Maßnahme voraussetzt. Für die betroffenen Personen ist nicht nachvollziehbar, welche nach dem Gesetz erhobenen Daten für die Aufgabenerfüllung der zuständigen - bzw. des Verfassungsschutzes als mitwirkender - Stelle erforderlich sind.

Darüber hinaus stellt die Vorschrift nur auf die erhobenen Daten ab, die in Unterlagen und Dateien gespeichert, verändert und genutzt werden dürfen. Damit bleibt die Frage offen, was mit den Beurteilungen, Schlußfolgerungen und Bewertungen geschieht, die zusammengefaßt das Ergebnis einer Sicherheitsüberprüfung darstellen.

Hier habe ich empfohlen, die zulässige Datenspeicherung der zuständigen Stelle getrennt von der zulässigen Datenspeicherung der mitwirkenden Stelle zu regeln. Dabei sollte die Speicherung in Dateien bei der zuständigen Stelle auf die Identifizierungsdaten (Name, Vorname, Geburtsdatum) beschränkt werden. Eine Datenspeicherung, die über den Umfang eines Aktenhinweissystems hinausgeht, ist für die Aufgabenerfüllung der zuständigen Stelle nicht mehr erforderlich. Dies gilt auch bei der mitwirkenden Stelle.

Auch die Vorschrift zur Übermittlung und Zweckbindung (§ 23 des Entwurfs) ist in datenschutzrechtlicher Hinsicht unbefriedigend. So wird die mitwirkende Stelle befugt, die im Zusammenhang mit einer Sicherheitsüberprüfung gespeicherten personenbezogenen Daten nicht nur zur Aufklärung von sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten für eine fremde Macht zu verarbeiten, sondern auch zur Aufklärung von gewaltbereiten Bestrebungen sowie von Bestrebungen von erheblicher Bedeutung.

Hier können sicherheitsüberprüfte Personen nicht erkennen, ob Bestrebungen, mit denen sie in irgendeiner Weise Kontakt haben, von den Verfassungsschutzbehörden als eine von erheblicher Bedeutung eingestuft wird. Dies gilt in einem gewissen Maß auch für gewaltgeneigte Bestrebungen. Ich habe daher angeregt, die Nutzung der Daten auf die Spionageaufklärung zu beschränken.

3.5 Statistik

3.5.1 Stand beim Statistikregistergesetz

Nach der Verordnung (EWG) Nr. 2186/93 des Rates vom 22.07.1993 über die innergemeinschaftliche Koordinierung des Aufbaus von Unternehmensregistern für statistische Verwendungszwecke[78] ist jedes EU-Mitgliedsland verpflichtet, durch nationales Recht abzusichern, daß statistische Register über Unternehmen aufgebaut und geführt werden.
Seit 1995 hat die Bundesregierung in mehreren Bundesressortentwürfen versucht, ein Statistikregistergesetz zuwege zu bringen. Auskunftspflichtig sind danach Finanzbehörden über Umsatzsteuerpflichtige, die Bundesanstalt für Arbeit über Betriebe mit Arbeitnehmern, Industrie- und Handelskammern, Handwerkskammern und andere Kammern über ihre Kammerzugehörigen sowie Berufsverbände über ihre Mitglieder. Die statistischen Unternehmensregister sollen bei den Statistischen Ämtern von Bund und Ländern geführt werden.

78 ABl. EG Nr. L 196 S. 1

Datenschutzrechtlich besonders brisant war in allen Ressortentwürfen die Befugnis der Statistischen Ämter, der Bundesanstalt für Arbeit (BfA) aktualisierte Einzelangaben über Unternehmen rückübermitteln zu dürfen. Auf diese Weise sollte die dort zu Zwecken des Verwaltungsvollzugs geführte Betriebsdatei ebenfalls auf den jeweils neuesten Stand gebracht werden. Dies hätte allerdings einen erheblichen Verstoß gegen den verfassungsrechtlichen Grundsatz der Trennung von Statistik und Verwaltung bedeutet. Die Datenschutzbeauftragten von Bund und Ländern haben deshalb wiederholt eindringlich auf diese Problematik aufmerksam gemacht. Eine solche Regelung, die den Bruch des Statistikgeheimnisses und die Zweckentfremdung der statistischen Datennutzung beinhaltet, würde vor dem Bundesverfassungsgericht im Falle einer Klage keinen Bestand haben. Erst mit dem letzten Ressortentwurf (Stand: 18.07.1997) konnte hier eine Verbesserung erreicht werden. In dem nun vorliegenden Gesetzentwurf der Bundesregierung[79] ist in Art. 1 (Statistikregistergesetz) darauf abgestellt worden, daß die hier in Rede stehenden Rückübermittlungen „ausschließlich für statistische Zwecke in den abgeschotteten Bereich der Bundesanstalt für Arbeit" erfolgen sollen. Eine umfassendere Definition einer behördlichen Statistikstelle, wie sie etwa in anderen Bundesgesetzen[80] fixiert wird, ist jetzt aber immer noch nicht festgelegt.

3.5.2 Stand der Vorbereitung der Volkszählung 2001

Inzwischen scheint festzustehen, daß die Volkszählung der EU im Jahre 2001 in der Bundesrepublik als Sekundärstatistik durchgeführt werden wird. Sie soll sich im wesentlichen auf die **Melderegister** der Einwohnermeldeämter, aber auch auf Ergebnisse der Beschäftigtenstatistiken und auf die alljährlich durchgeführten 1%igen Stichproben des Mikrozensus, stützen.

Nach wie vor ist die Qualität der Melderegister problematisch, weil bisher nicht erkennbar ist, ob deren Aktualität für eine repräsentative Statistik ausreicht. Um ihre Aussagefähigkeit der Melderegister zu testen, führen die Statistischen Landesämter für ausgewählte Städte und Regionen Erprobungsrechnungen, sog. Haushaltsgenerierungen, durch.

---

79 Entwurf eines Gesetzes zur Durchführung der Verordnung (EWG) Nr. 2186/93 des Rates vom 22. Juli 1993 über die innergemeinschaftliche Koordinierung des Aufbaus von Unternehmensregistern für statistische Verwendungszwecke, BT-Drs. 13/9696 vom 22. Januar 1998

80 s. z. B. § 58 Güterkraftverkehrsgesetz, § 6 Rohstoffstatistikgesetz, § 5 Straßenverkehrsunfallstatistikgesetz, § 7 Gesetz über Steuerstatistiken

Hierzu habe ich festgestellt, daß das von einigen kommunalen Statistikstellen und dem Landesamt für Datenverarbeitung und Statistik (LDS) konzipierte Verfahren zur **Modellrechnung von Haushaltsgenerierungen aus personenbezogenen Einwohnermeldedaten** grundsätzlich zulässig ist, wenn das Prinzip der Geschäftsstatistik gem. § 9 Brandenburgisches Statistikgesetz (BbgStatG)[81] gilt und Meldedaten nach § 28 Abs. 1 BbgMeldeG genutzt werden. Denn das LDS ist gem. § 5 Abs. 2 Ziff. 5, 7 und 8 BbgStatG befugt, Modellrechnungen durchzuführen, öffentliche Stellen auf dem Gebiet der Statistik zu unterstützen und bei der Vorbereitung von Rechtsvorschriften mitzuwirken. Dies trifft auch auf die fachlichen Aspekte der Durchführung von Statistiken der EU zu. Ich gehe davon aus, daß die Ergebnisse der Untersuchungen ausschließlich zu Zwecken der Bewertung der Modellrechnungen genutzt werden und nicht zu kommerziellen Veröffentlichungen. Ansonsten bestünde hier die Gefahr der Zweckentfremdung der Meldedaten, wenn diese ohne den Zusammenhang mit der konkreten Modellrechnung und der Vorbereitung einer gesetzlichen Regelung genutzt werden, nämlich des für die Volkszählung 2001 noch zu erlassenen Gesetzes.

Um die Qualität der Melderegister zu erhöhen, werden von den zuständigen Behörden von Bund und Ländern weitere Überlegungen angestellt. So sollen z. B. alle Behörden, die nach den Meldegesetzen regelmäßig Meldedaten empfangen, ihrerseits den zuständigen Meldebehörden Erkenntnisse über vermutete oder tatsächliche Unrichtigkeit der ihnen zugegangenen Daten übermitteln. Dafür gibt es jedoch keine Rechtsgrundlage. Darüber hinaus verbietet das Amtsgeheimnis (z. B. den Sozial- und Finanzämtern) solche Mitteilungen.

Es ist weiter daran gedacht, aus Anlaß von Wahlen bewußt sog. „negative Wahlberechtigungen" zu versenden, um aus der Reaktion der Einwohner bzw. aus der Unzustellbarkeit der Benachrichtigung Rückschlüsse über unrichtige Melderegisterdaten, etwa über den Wechsel von Haupt- und Nebenwohnung oder den Wegzug, ziehen zu können. Dies kommt einer Zweckentfremdung der bei der Durchführung von Wahlen genutzten personenbezogenen Daten gleich, weil die Bürger über den wahren Zweck der Datengewinnung im unklaren gelassen werden. Inwieweit dies alles aber in eine datenschutzrechtlich einwandfreie Form umgesetzt werden kann, ist derzeit noch nicht absehbar.

3.5.3 Statistischer Beirat

Gemäß § 6 BbgStatG ist beim LDS ein Beirat für Statistik einzurichten, dem der Landesbeauftragte für den Datenschutz als ständiges Mitglied angehört. Dessen Konstituierung fand im Oktober 1997 statt. Nachdem zunächst nach § 6 Abs. 3 BbgStatG eine Geschäftsordnung zu erlassen war, beschäftigt sich der Beirat derzeit mit den technisch-organisatorischen und rechtlichen Voraussetzungen für die Volkszählung 2001.

So ist z. B. die oben geschilderte Modellrechnung[82] zur Vorbereitung der Volkszählung noch insoweit datenschutzrechtlich relevant, als nach deren Abschluß Aussagen darüber geliefert werden können, ob das Verfahren der Einwohnermelderegisternutzung (anstelle einer Primärerhebung) statistisch überhaupt sinnvoll ist. Denn lediglich eine Fehlerquote von höchstens 1 % ist nach fachstatistischer Aussage für „statistiktaugliche Register" noch hinnehmbar. Sollte also das geplante Verfahren für die Volkszählung wegen einer höheren Fehlerquote statistisch nicht haltbar und damit ungeeignet sein, wäre aus datenschutzrechtlicher Sicht auch eine entsprechende Registernutzung zum Zweck der **Volkszählung 2001** nicht geeignet. Entsprechende Eingriffe in das Grundrecht auf informationelle Selbstbestimmung der Bürger entbehrten dann der Verhältnismäßigkeit und wären somit nicht hinnehmbar und datenschutzrechtlich unzulässig.

---

81 vom 11. Oktober 1996, GVBl. I S. 294

82 s. oben unter 3.5.2

Sollten dagegen die Modellrechnungen zu einem positiven Ergebnis führen, wäre für die Durchführung der Volkszählung 2001 eine gesetzliche Vorschrift u. a. aus Gründen der Normenklarheit und der Zweckänderung bei der Nutzung von Verwaltungsdaten zwingend erforderlich. Die Bürger der Bundesrepublik müßten dann vor Beginn der sekundärstatistischen Erhebung etwa durch Postwurfsendungen darüber informiert werden, daß ihre personenbezogenen Daten in den Melderegistern zu Zwecken der Volkszählung genutzt werden.

3.5.4 Sonstiges

3.5.4.1 System repräsentativer Verkehrserhebung (SrV 98)

Kommunale Statistikstellen in den neuen Bundesländern wollen 1998 in Zusammenarbeit mit der Technischen Universität Dresden (TU) Verkehrserhebungen auf freiwilliger Basis durchführen; das Konzept der Erhebung stammt von der TU. Zum Zweck der Bauleitplanung gem. § 1 Baugesetzbuch (BauGB)[83] sollen Verkehrsströme festgestellt werden. Im sog. Haushaltsbogen werden u. a. Daten zur Anzahl der im Haushalt lebenden Personen, zur Fahrzeugausstattung, zur Jahresfahrleistung der Pkw, zur Berufstätigkeit und Ausbildung erhoben. Im sog. Personenfragebogen wird u. a. nach Wegbenutzungen, Zweck des Weges, Verkehrsmittel, Ortsangaben, Entfernungen und Zeitangaben gefragt.

Da im Haushaltsbogen auch nach der Anzahl der Personen im Haushalt, die zu Hause einen Anschluß an das Internet, an Btx oder andere Weitverkehrsnetze nutzen, gefragt werden soll, habe ich darauf aufmerksam gemacht, daß diese Erhebungsmerkmale nicht mit dem Zweck des klassischen Straßenverkehrs in Einklang stehen und deshalb nicht erhoben werden dürfen. Wegen der unseriösen Marketingerhebungen durch verschiedene Firmen[84] in letzter Zeit müßten öffentliche Stellen statistische Vorhaben besonders sorgsam vorbereiten, um neben der Erfüllung der statistikrechtlichen Anforderungen auch die erforderliche Akzeptanz bei der Bevölkerung zu finden. Ich habe schließlich erläutert, daß gegen die Erhebung der strittigen Merkmale zur Nutzung von Weitverkehrsnetzen datenschutzrechtlich nichts einzuwenden ist, wenn die Zweckbestimmung und deren Begründung entsprechend erweitert werden. Denn es ist nachvollziehbar, daß durch die Nutzung von Weitverkehrsnetzen zu Zwecken der persönlichen Information oder der Telearbeit auch der Straßenverkehr beeinflußt werden kann.

Ferner habe ich darauf verwiesen, daß es nach § 17 Abs. 3 BbgStatG möglich sein muß, daß nicht nur Interviewer die Erhebung durchführen, sondern daß auch der freiwillig auskunftgebende Bürger die Beantwortung der Erhebungsfragen schriftlich und selbständig vornehmen kann. Er könnte dann, wie auch bei sonstigen statistischen Erhebungen, die verschlossenen Erhebungsbögen dem Interviewer übergeben oder der kommunalen Statistikstelle zustellen.

Zudem mußte ich darauf hinweisen, daß die Gemeinden oder Gemeindeverbände wohl befugt sind, statistische Arbeiten ganz oder teilweise im Zuge der Auftragsdatenverarbeitung nach § 8 Abs. 1 BbgStatG zu vergeben, daß sie dennoch für die Einhaltung der Rechtsvorschriften, wie etwa die Wahrung der statistischen Geheimhaltung, verantwortlich bleiben. Es kann nicht sein, daß nur der Datenschutzbeauftragte der TU die Schutzmaßnahmen überwacht. Vielmehr muß zusätzlich die Möglichkeit bestehen, daß auch Mitarbeiter der zuständigen kommunalen Statistikstellen im Land Brandenburg sich von der Einhaltung der datenschutzrechtlichen Schutzmaßnahmen in der TU überzeugen können. Die TU hat mir zugesagt, meine Hinweise zu berücksichtigen.

---

83 i. d. Fass. vom 27. August 1997, BGBl. I S. 2141

84 s. unter 2.6

Im übrigen gilt es, daran zu erinnern, daß die geschilderten Erhebungen, die zunächst noch personenbezogen erfolgen, gem. § 11 BbgStatG ausschließlich nur von **kommunalen Statistikstellen** wahrgenommen werden dürfen. Andere Verfahren, bei denen etwa ein Bau- oder Ordnungsamt als Erhebungsstelle fungieren sollte, würden einen schwerwiegenden Verstoß gegen das Prinzip der Trennung von Statistik und Verwaltungsvollzug darstellen.

3.5.4.2 Heim- und Telearbeit bei der Statistikstelle

Neben den allgemein zu beachtenden Grundsätzen der Sicherheit bei der **Telearbeit**[85] gelten für die Gewährleistung des Statistikgeheimnisses und der Zweckbindung statistischer Daten in der **kommunalen Statistikstelle** weitere Einschränkungen. Dazu bedarf es einiger grundsätzlicher Hinweise.

Wenn nämlich nach § 11 Abs. 2 BbgStatG schon für die Statistikstelle innerhalb einer ansonsten überschaubaren und geordneten Behörde besondere organisatorische und technische Maßnahmen der Datensicherung für die Abschottung der Statistik von der Verwaltung gefordert werden, so gelten diese Maßnahmen zur Sicherung des Statistikgeheimnisses natürlich in höherem Maße ebenfalls für die Abschottung von häuslicher Privatheit und unsicheren Weitverkehrsnetzen. Denn beim Teleheimarbeitsplatz fehlt einerseits die gesicherte Büroumgebung; im allgemeinen haben Familienmitglieder und Gäste zum Teleheimarbeitsplatz freien Zugang. Die strengen Zugangsregelungen für eine kommunale Statistikstelle lassen sich hier also normalerweise gar nicht realisieren.

Zudem müßte andererseits wegen der ungeschützten Datenübertragung zwischen Teleheimarbeitsplatz und Server der Statistikstelle zusätzlich ein hoher Sicherheitsaufwand betrieben werden (Einsatz von hochwertiger Verschlüsselungssoftware, Firewallrechner seitens der Statistikstelle und des Teleheimarbeitsplatzes, sichere Identifizierungsmaßnahmen wie z. B. Call-Back-Verfahren und verschlüsselte Paßwortübertragung). Selbst dies dürfte nach dem jetzigen Stand der Technik nicht ausreichen. Deshalb ist dringend zu empfehlen, sie nicht im Telebetrieb zu verarbeiten. **Personenbezogene oder -beziehbare statistische Daten** haben wegen der Wahrung der statistischen Geheimhaltung einen Schutzwert und fallen deshalb in die **Schutzstufe C** des von meiner Behörde entwickelten Schutzstufenkonzepts[86].

Der beabsichtigte Telebetrieb widerspricht sowohl § 11 BbgStatG als auch der Muster-Dienstanweisung für kommunale Statistikstellen[87], die aus Sicherheitsüberlegungen u. a. auf eine Insellösung der automatisierten Datenverarbeitung der Statistikstelle ausdrücklich Wert legt. Wegen der besonderen Brisanz der Wahrung der statistischen Geheimhaltung hätte der Gesetzgeber für den Fall der Teleheimarbeit bei Kommunalstatistiken spezielle Regelungen treffen können oder müssen. Dies hat er aber nicht getan.

Man hat mich auch darauf angesprochen, daß es sich in einigen Fällen einer geplanten statistischen Teleheimarbeit oder anderen Heimarbeit nicht um die Fernverarbeitung sensibler Daten handele, sondern um bereits aggregierte und streng anonymisierte Daten aus Geschäftsstatistiken gem. § 9 BbgStatG. Sofern dies nachprüfbar zutreffen sollte, würde sich die Angelegenheit etwas anders darstellen. Aber auch hier bliebe das Problem, daß eine Telekommunikation mit einem Rechner der Dienststelle derzeit nur als Einzelplatz denkbar ist, weil ansonsten das Behördennetz oder das der Statistikstelle unbefugten Zugriffen ausgesetzt wäre. Auch der direkte Datenträgeraustausch wäre eine mögliche Variante

---

85 s. unter 1.5.3

86 s. Fn. 6

87 Rundschreiben des MI vom 5. August 1996

der Datenübermittlung.

Für einen derartigen Tele- oder sonstigen Heimarbeitsplatz müßte die zuständige öffentliche Stelle allerdings ebenfalls eine besondere Dienstanweisung erstellen, in der gewisse Sicherheitsstandards festgeschrieben werden. Auch müßte sich der Telearbeiter schriftlich verpflichten, sich mit seinem häuslichen Arbeitszimmer der Kontrolle des Landesbeauftragten für den Datenschutz zu unterwerfen, weil überprüfbar sein muß, daß die von ihm verarbeiteten statistischen Daten tatsächlich korrekt anonymisiert sind. Ohne eine solche Verpflichtung, die natürlich einen Eingriff in die durch das Grundgesetz geschützte Privatheit der Wohnung darstellt, sind Telearbeitsplätze aus datenschutzrechtlichen Erwägungen abzulehnen.

In diesem Zusammenhang muß ich auf eine weitere Problematik aufmerksam machen: Gemäß §§ 11 und 8 BbgStatG ist es die **kommunale Statistikstelle** oder eine andere entsprechend ausgestattete und beauftragte Stelle, die Kommunalstatistiken durchführt. Ich beobachte mit Sorge, daß einige große Kommunen sich dieser Verpflichtung entziehen wollen. Man geht dort davon aus, daß aus den Fachämtern keine personenbezogenen statistischen Daten, sondern nur gem. § 9 Abs. 2 BbgStatG streng anonymisierte Daten weitergegeben werden. Diese sollen dann an anderer Stelle in ansprechender Weise zusammengestellt und veröffentlicht werden. Dafür reiche etwa auch ein Sachgebiet Statistik; eine abgeschottete Statistikstelle, wie sie § 11 BbgStatG und die o. g. Muster-Dienstanweisung für kommunale Statistikstellen festschreiben, sei nicht erforderlich.

Zumindest muß klar sein, daß ein solches Sachgebiet keine statistischen Einzeldaten, weder aus den Fachämtern noch vom LDS aus Bundes- oder Landesstatistiken, erhalten kann. Sie dürfen auch keine Primärdaten erheben. So bleibt letztlich nur die Verarbeitung von bereits absolut anonymisierten Daten übrig. Aber selbst dabei ist zu beachten, daß die Zusammenführung solcher Daten nach § 11 Abs. 4 BbgStatG nur der kommunalen Statistikstelle zusteht.

Lediglich durch eine sehr weite Auslegung von § 8 Abs. 1 BbgStatG könnte eine andere Stelle innerhalb der Stadtverwaltung von den Fachämtern beauftragt werden, deren streng anonymisierte Geschäftsstatistiken weiter zu verarbeiten und zu veröffentlichen. Hierbei sind aber insbesondere die Regeln für die Anonymisierung zu beachten, wie sie unter Punkt II, Nr. 5 der o. g. MI-Muster-Dienstanweisung für kommunale Statistikstellen ausgeführt sind. Sobald aber etwa durch die Kleinräumigkeit einer statistischen Darstellung oder durch die Zusammenführung verschiedener Geschäftsstatistiken eine Deanonymisierung möglich oder die für Geschäftsstatistiken erforderliche absolute Anonymisierung nicht mehr erreichbar wäre, läge ein schwerwiegender Verstoß gegen die statistische Geheimhaltung vor. Dieses Problem kann aber grundsätzlich nur durch eine korrekt eingerichtete und abgeschottete Statistikstelle gelöst werden.

Allenfalls für eine relativ knappe Übergangszeit wäre unter den genannten Bedingungen eine solche eingeschränkte statistische Datenverarbeitung durch ein Sachgebiet Statistik innerhalb der Stadtverwaltung einer großen Kommune noch hinnehmbar. Das Ziel, eine Statistikstelle im Sinne des § 11 BbgStatG zu errichten, muß aber nicht zuletzt deshalb angestrebt werden, weil es auch für die Bürger nachvollziehbar sein muß, auf welche Weise Statistiken unter Wahrung des Statistikgeheimnis erstellt werden.
Lediglich kleinen Amtsgemeinden und kleinen Städten kann bei einem solchen Verfahren der gemeinsam veröffentlichten Geschäftsstatistiken durch ein Sachgebiet Statistik ein etwas längerer Übergangszeitraum zugebilligt werden, wenn die strengen Regeln der absoluten Anonymisierung eingehalten werden und keine inhaltliche Zusammenführung der Geschäftsstatistiken erfolgt.

In allen Fällen sollte aber ernsthaft bedacht werden, daß der Gesetzgeber mit § 11 Abs. 6 BbgStatG für alle die Gemeinden und Gemeindeverbände, die die Anforderungen nach § 11 Abs. 1 und 2 nicht erfüllen können oder wollen, die Befugnis zur Errichtung einer gemeinsamen kommunalen Statistikstelle eingeräumt hat, um dadurch den Aufwand an Personal und Kosten zu verringern.

3.5.4.3 Kommunalstatistik

Eine kreisfreie Stadt hatte sich vorgenommen, im Rahmen einer Sozialstudie vor dem Hintergrund einer städtebaulichen Rahmenplanung für einen Stadtteil eine repräsentative ca. 1%ige Stichprobe auf Freiwilligkeitsbasis durchzuführen. Die Erhebung sollte in bereits anonymisierter Form erfolgen. Erhebungsmerkmale sollten Angaben zur Wohn- und Lebenssituation, zu Vorzügen und Mängeln des Wohnumfeldes, zu Wünschen über das zukünftige Stadtteilzentrum und zur Versorgung mit sozialen und kulturellen Einrichtungen sein. Die Vorbereitung, Durchführung und Verarbeitung der Erhebung sollte als Datenverarbeitung im Auftrag durch eine private Stelle erfolgen.

Insgesamt hatte ich keine grundsätzlichen datenschutzrechtlichen Bedenken gegen dieses Vorhaben. Nach § 10 Abs. 1 BbgStatG sind die Kommunen befugt, zur Wahrnehmung ihrer Selbstverwaltungsaufgaben Kommunalstatistiken durchzuführen. Vom LDS konnten keine entsprechenden statistischen Einzelangaben geliefert werden. Da die statistische Erhebung ohne Auskunftspflicht erfolgen sollte, bestand gem. § 10 Abs. 2 BbgStatG keine Satzungspflicht.

Nach § 8 BbgStatG ist die Vergabe statistischer Arbeiten an andere Stellen oder Personen zulässig, sofern sichergestellt ist, daß die einschlägigen datenschutz- und statistikrechtlichen Vorschriften eingehalten werden. Für deren Einhaltung ist bekanntlich der Auftraggeber verantwortlich. Der Auftragnehmer muß sich der Kontrolle des Auftraggebers und des Landesbeauftragten für den Datenschutz unterwerfen.

Folgende Unterlagen, die später auch den zu befragenden Bürgern übergeben wurden, waren mir vorgelegt und z. T. unter meiner Beratung überarbeitet worden: ein Anschreiben der Stadtverwaltung über Sinn und Zweck der Kommunalstatistik, eine Erklärung zum Datenschutz, ein Auszug aus dem Brandenburgischen Statistikgesetz, die Fragebögen zur Sozialstudie für Erwachsene, ein Fragebogen für Kinder und Jugendliche und eine Zusatzkarte mit der Anfrage, ob der Befragte einem vertiefenden Interview zustimmen wolle und Einladungen zu Informationsveranstaltungen über die Weiterentwicklung seines Stadtteils wünsche.

Die mir vorgelegten Unterlagen und die Erläuterung des Verfahrens der Datenerhebung und -verarbeitung erschienen mir nachvollziehbar. Die Anforderungen an die Unterrichtung der zu Befragenden gem. § 20 BbgStatG waren durch das Anschreiben der Stadtverwaltung Potsdam und die Erklärung zum Datenschutz erfüllt.

Die Zusammenarbeit zwischen der Stadtverwaltung Potsdam, dem Auftragnehmer und meiner Behörde hatte sich bei der Vorbereitung dieses Projekts erfreulicherweise auf angenehme Weise als konstruktiv und sachdienlich dargestellt.

4 Justiz/Staatsanwaltschaft

4.1 Gesetze und Rechtsverordnungen

4.1.1 Ausführungsgesetz zur Insolvenzordnung

Im Mai 1997 erhielt ich Gelegenheit, zu einem ersten Entwurf für ein Brandenburgisches Gesetz zur Ausführung der Insolvenzordnung (AGInsO) Stellung zu nehmen. Meine kritischen Ausführungen zu dem Gesetzentwurf betrafen einerseits das Vorhaben, bei dem Verfahren einen „vorgeschriebenen" Vordruck zu verwenden, und andererseits die Bestimmung, daß eine juristische Person des öffentlichen Rechts nicht insolvenzfähig sein solle.

Der erste Entwurf ist inzwischen durch einen stark überarbeiteten Entwurf ersetzt worden. Die beiden von mir kritisierten Punkte sind ersatzlos aufgegeben worden; eine Begründung dafür ist mir nicht bekannt.

Weitere, bis dahin nicht aufgeführte Regelungsteile wurden in den neuen Entwurf für das Ausführungsgesetz aufgenommen. Unter diesen neuen Bestimmungen sind im Zusammenhang mit meinen Aufgaben nur die datenschutzrechtlichen Bestimmungen in § 7 zu nennen; demnach ist nach Maßgabe des Brandenburgischen Datenschutzgesetzes zu verfahren. Bis auf Vorschläge zu redaktionellen Änderungen in bezug auf diese Vorgabe habe ich zu dem neuen Entwurf keine Kritik geäußert.

Das Ausführungsgesetz zur Insolvenzordnung ist dem Landtag bisher noch nicht zugeleitet worden.

4.1.2 Neufassung MiZi 98

Vom 1. Juni 1998 an wird das Justizmitteilungsgesetz (JuMiG)[88] anzuwenden sein. Aller Voraussicht nach wird zu diesem Zeitpunkt auch die auf neuen Stand gebrachte „Anordnung über Mitteilungen in Zivilsachen (MiZi)" in Kraft gesetzt werden. Mitteilungsregelungen dieser Art sind untergesetzliche Folgeregelungen zum Justizmitteilungsgesetz, die den Umgang mit den Entscheidungen der Gerichte betreffen und durch die Mitarbeiter der Geschäftsstellen der Gerichte umzusetzen sind. In der MiZi ist u. a. festgelegt, in welchen Fällen, an welche Stellen und in welchem Umfang z. B. Scheidungsurteile bzw. deren wichtigste Aussagen mitgeteilt werden, wie die Namensfolge infolge des Endes der Ehe geregelt worden ist und ggf., welche Folgen bezüglich der Ehelichkeit und Nichtehelichkeit von Kindern der beendeten Ehe eingetreten sind.

[88] vom 18. Juni 1997, BGBl. I S. 1430

Der hier interessierende Teil des JuMiG, d. h. dessen Art. 1, ist als Zweiter Abschnitt (§§ 12 bis 22) in das Einführungsgesetz zum Gerichtsverfassungsgesetz (EGGVG)[89] eingefügt worden und hat „verfahrensübergreifende Mitteilungen von Amts wegen" zum Gegenstand. Damit gibt es endlich eine gesetzliche Vorschrift für den Umgang mit personenbezogenen Daten für die Weitergabe von Daten durch die Gerichte der ordentlichen Gerichtsbarkeit und der Staatsanwaltschaften.

Für die Umsetzung des Gesetzes in Verwaltungsvorschriften blieb nur ein knappes Jahr Zeit. In diesem Zeitraum mußten die bisher bereits genutzten Verwaltungsvorschriften überarbeitet und ergänzt werden. Trotz des äußerst knappen Zeitrahmens hat die länderübergreifende MiZi-Arbeitsgruppe darin übereingestimmt, daß jeweils der erste Entwurf dieser Vorschriften den Datenschutzbeauftragten des Bundes und der Länder zur Stellungnahme zugeleitet werden sollte. Die Datenschutzbeauftragten hatten daraufhin ihrerseits eine Arbeitsgruppe zusammengestellt, die die Federführung zur Bearbeitung einer Stellungnahme für die MiZi übernehmen sollte. Der Berliner Datenschutzbeauftragte erklärte sich bereit, innerhalb der MiZi-Datenschutzarbeitsgruppe die Koordinierungssaufgaben wahrzunehmen; meine Dienststelle beteiligte sich an der Arbeitsgruppe. Von dieser wurden unter hohem Zeitdruck Textvorschläge erarbeitet und den Datenschutzbeauftragten des Bundes und der Länder zugesandt, mit dem Ziel, den Sachverstand aus den Dienststellen zu nutzen, damit der ministeriellen Arbeitsgruppe ausgereifte Vorschläge zum Datenschutz unterbreitet werden könnten.

Das Ergebnis der so umfassend gestalteten abgestuften Mitwirkung der Datenschutzbehörden des Bundes und der Länder ist aus meiner Sicht sehr erfreulich ausgefallen. Die gemeinsame Stellungnahme und die Verbesserungsvorschläge aus der Sicht des Datenschutzes wurden den zuständigen obersten Justizbehörden (Ministerien und Senatsverwaltungen) Ende Januar 1998 übersandt. Ich habe mich den erarbeiteten Vorschlägen - wie die meisten meiner Kollegen - angeschlossen und dem Ministerium der Justiz und für Bundes- und Europaangelegenheiten (MdJBE) den Text der Stellungnahme unverändert weitergegeben. Das parallele Verfahren zur Erarbeitung der neuen MiStra[90] ist ebenso zu beurteilen.

Die Ministerielle Arbeitsgruppe ist nun gefordert, die Vorgaben des Gesetzes, des Datenschutzes und der gerichtlichen und staatsanwaltlichen Praxisanforderungen aufeinander abzustimmen und rechtzeitig vor dem 01.06.1998 die endgültigen Vorschriften vorzulegen, so daß diese im Bundesanzeiger veröffentlicht und damit anwendbar gemacht werden können.

4.1.3 Neufassung MiStra

Parallel zur Erarbeitung einer gemeinsamen Stellungnahme zu MiZi erfolgte eine entsprechende Durcharbeitung des MiStra-Entwurfes; auch die MiStra soll zum 1. Juni 1998 in Kraft treten.

Die „Anordnung in Mitteilungen in Strafsachen (MiStra)" dient dazu, festzulegen, aus welchem Anlaß, auf welchem Weg und in welcher Art und welchem Umfang Mitteilungen, die Strafsachen betreffen, von Gerichten und Staatsanwaltschaften von Amts wegen an andere Stelle zu übermitteln sind. Die Rechtsgrundlagen, d. h., Regelungen des Justizmitteilungsgesetzes (JuMiG), werden differenziert dargestellt und Folgerungen daraus gezogen, oder aber sie werden direkt übernommen; letzteres trifft z. B. auf die Pflicht der Staatsanwaltschaften zu, die Polizei über das Aktenzeichen und den Ausgang von Strafverfahren zu benachrichtigen (Art. 32 JuMiG; 2. Teil 1. Abschn. Nr. 11 MiStra). Außerdem werden z. B. Mitteilungen zum Wählerverzeichnis durch Anpassung an die Einführung des Kommunalwahlrechts für EU-Bürger in Teil 2, Abschn. 1, Nr. 12a MiStra geregelt.
Im Fall der MiStra konnte eine auch nur annähernde Begleitung durch meine Behörde nicht stattfinden, obgleich es sich

89 vom 27. Januar 1877 (RGBl. S. 77); zul. geänd. durch JuMiG vom 16. Juni 1997, BGBl. I S. 1430, ber. 2779

90 s. unter 4.1.3

auch bei der MiStra um eine datenschutzrelevante Aufgabe gehandelt hat. Ich habe mich den endgültigen MiStra-Vorschlägen der Arbeitsgruppe, die in ganz vergleichbarer Weise wie bei dem MiZi-Verfahren entstanden sind, angeschlossen und auch diese gemeinsame Stellungnahme der Datenschutzbeauftragten unverändert übernommen, um sie sodann dem MdJBE zu übergeben.

4.2 Verfahrensfragen

4.2.1 Automation bei den Staatsanwaltschaften

Seit Ende 1995 betreibt Brandenburg in einem gemeinsamen Entwicklungsprojekt mit den Bundesländern Hamburg, Hessen und Schleswig-Holstein das Verfahren „**Mehrländer-Staatsanwaltschaften-Automation (MESTA)**“[91].

Im Berichtszeitraum hat ein Pilotierungsverfahren bei der Staatsanwaltschaft Neuruppin die Arbeit aufgenommen. Im Verlauf des Jahres 1998 ist die landesweite Inbetriebnahme von MESTA geplant.

Wichtige Problembereiche, wie z. B. der weitere Umgang mit der Zentralen Namenskartei, die Regelung der Zugriffsberechtigungen auf den Datenbestand und die Festlegung von Löschungsfristen, auf deren Klärung ich u. a. immer wieder gedrängt hatte, wurden bis zur Aufnahme des Pilotverfahrens folgendermaßen geregelt:

- Die Zentrale Namenskartei, die bisher den Nachweis der Ermittlungsverfahren sichergestellt hat, wird mit Ausnahme der ab 01.01.1998 noch offenen Verfahren nicht nacherfaßt.

- Die Zugriffsberechtigungen auf MESTA sind vom Generalstaatsanwalt des Landes Brandenburg festgelegt worden. Danach haben jeder leitende Oberstaatsanwalt sowie die Abteilungsleiter zu jeder Zeit auf alle Verfahren Lesezugriff.

- Die Löschungsfristen in MESTA richten sich nach dem Entwurf des Strafverfahrensänderungsgesetzes 1996 (StVÄG 1996)[92].

Im Oktober vergangenen Jahres habe ich mir das Pilotierungsverfahren bei der Staatsanwaltschaft Neuruppin vorführen lassen. Zum Vorführungszeitpunkt konnten verschiedene staatsanwaltschaftliche Ermittlungsverfahren (Js-, OWiG- und UJs-Verfahren) in MESTA registriert werden. Weitere Register waren noch nicht programmiert. Auch die Schnittstelle „Fremddaten“, über die der Datenaustausch mit anderen Behörden, insbesondere mit der Polizei realisiert werden soll, arbeitete noch nicht. Für die Schnittstelle soll ein Speicher zur Verfügung stehen, in dem die von den Fremddatenbanken eingehenden Daten umformatiert und bei Akteneingang in der Staatsanwaltschaft durch MESTA abgerufen werden.

Die Inaugenscheinnahme der technischen Anlagen sowie der Räume, in denen diese untergebracht sind, ergab, daß die gem. § 10 BbgDSG erforderlichen technischen und organisatorischen Maßnahmen noch nicht ausreichend umgesetzt waren. Dazu habe ich einige Änderungen empfohlen und gehe davon aus, daß sie bis zum Abschluß der Pilotierungen umgesetzt werden. Funktionsstörungen oder sonstige datenschutzrechtliche Mängel stellten sich bei der Vorführung nicht heraus. Eine abschließende datenschutzrechtliche Beurteilung des Pilotierungsverfahrens konnte ich bisher noch nicht

91 s. 4. Tätigkeitsbericht unter 4.2

92 s. 5. Tätigkeitsbericht unter 4.1.2

vornehmen, da das MdJBE noch nicht - wie zugesagt - die dazu erforderlichen Listen mit den Zugriffsvergaberechten und die Ausdrucke von Masken übersandt hat.

4.2.2 Gerichtliche Verfahren, durch die mehrere Personen betroffen sind

4.2.2.1 Sammeladressierung

Eine Petentin hatte im Zusammenhang mit einem verwaltungsgerichtlichen Verfahren vorläufigen Rechtsschutz nach § 80 Abs. 5 der Verwaltungsgerichtsordnung (VwGO)[93] gegen eine beabsichtigte Maßnahme eines Zweckverbandes beantragt. Daraufhin erhielt sie von dem Gericht ein Schreiben, das gleichlautend an sie selbst sowie an 29 weitere Antragsteller gerichtet war. Alle Beteiligten waren in dem Schreiben mit Namen und Aktenzeichen ausgewiesen.

Die Zusammenführung der völlig gleichgerichteten Verfahren war durch den Zweckverband vorgenommen worden, der seine Stellungnahme dem Gericht gegenüber in einem einzigen Schriftsatz abgegeben hatte. Die Petentin hatte parallel zu der Petition eine Dienstaufsichtsbeschwerde gegen die für das Verfahren zuständige Kammer des Verwaltungsgerichts erhoben; die Dienstaufsichtsbeschwerde wurde zurückgewiesen, da sich das Gericht rechtskonform verhalten hatte.

Auch ich war in dem Bemühen, den Sachverhalt aufzuklären, an das Gericht herangetreten. Das Oberverwaltungsgericht (OVG) stellte in seiner Antwort zunächst klar, daß keine Verbindung der gleichgerichteten Verfahren zur gemeinsamen Entscheidung vorgenommen worden war; allein die Art und Weise der Stellungnahme des Zweckverbandes hatte die gemeinsame Behandlung in Form einer Sammeladressierung zur Folge gehabt. Das Gericht hatte daraufhin jedem einzelnen Kläger eine Durchschrift der Stellungnahme, auf der jeder Kläger aufgeführt war, zugeschickt.

Für einen datenschutzfreundlichen Umgang mit derartigen Schriftstücken sah das OVG keinen Ansatz, da Gerichte an dem Original der Schriftsätze nichts ändern dürfen. Sie haben insoweit im Verhältnis der beiden Streitparteien zueinander lediglich so etwas wie eine Botenfunktion.

Aus Sorge, daß bei sogenannten **„Parallelverfahren"** die im Einzelfall beteiligten Behörden des Landes nur jeweils in einem einzigen Schriftsatz Stellung nehmen und damit gegen den Datenschutz verstoßen, regte das Gericht aber seinerseits an, daß ich mich aus Anlaß des vorliegenden Falles an die zuständige Rechtsaufsicht für den Verband wenden möge, damit derartige problematische „Sammeladressierungen" von Schriftsätzen künftig vermieden werden. Zusätzlich sollte angeregt werden, daß auf (innen-)ministerieller Ebene ein allgemeiner Erlaß zur Vermeidung solcher Adressierungen und zusammenfassender sachlicher Darstellungen in den Gerichtsverfahren erarbeitet und verbreitet wird.

Dieser Anregung bin ich gefolgt und habe sie sowohl an den Zweckverband als auch an das Ministerium des Innern (MI) als der zuständigen Rechtsaufsichtsbehörde weitergegeben.

4.2.2.2 Übermittlung von Meldeadressen

Ganz entgegengesetzt fiel die Beantwortung der Frage eines Petenten aus, der angefragt hatte, ob es zulässig sein könne, daß in einem Strafverfahren sowohl **Mitangeschuldigte** als auch Zeugen mit vollem Namen und kompletter Adresse in den Schreiben des Gerichts aufgeführt seien.

---

93 i. d. Fass. vom 19. März 1991, BGBl. I S. 17; zul. geänd. durch Ges. vom 22. Dezember 1997, BGBl. I. S. 3224

Zur Eröffnung eines strafrechtlichen Verfahrens ist der Angeschuldigte so genau zu benennen, daß er als anzuklagende Person eindeutig feststeht. Sind bei einer Tat mehrere Personen beteiligt gewesen und handelt es sich dabei um ein Strafverfahren, das gegen mehrere oder alle der beteiligten Personen gerichtet ist, dann sind in der Anklageschrift sämtliche in Frage kommenden Täter oder Teilnehmer näher zu bezeichnen. Einzige andere Möglichkeit wäre insoweit nur eine Trennung der Verfahren durch das Gericht selbst; eine Verfahrenstrennung würde allerdings nur aus prozessualen, nicht aber aus datenschutzrechtlichen Gründen in Betracht kommen können.

Die Anklageschrift ist nach § 201 Strafprozeßordnung (StPO)[94] dem Angeschuldigten mit der Aufforderung zur Erklärung seiner beabsichtigten Haltung bzgl. des Verfahrens mitzuteilen. Dabei müssen ihm alle Tatsachen bekannt gemacht werden, die der Entscheidung des Gerichts zu Grunde gelegt werden. Zu diesen Tatsachen gehören auch die Angaben über die Person von Mitangeschuldigten.

In § 200 Abs. 1 StPO ist bestimmt, daß in der Anklageschrift die Beweismittel anzugeben sind. Zu der „Angabe der Beweismittel" gehören der Rechtsprechung sowie der Literatur zufolge auch die **Anschriften der Zeugen**. Dem Angeschuldigten muß zur Vorbereitung seiner Verteidigung vor Gericht zuvor die Möglichkeit eingeräumt worden sein, Erkundigungen über die benannten Zeugen einzuholen. Dazu ist die volle Kenntnis von Namen und Anschrift eines jeden Zeugen erforderlich.

In besonders gelagerten Fällen kann es allerdings geboten sein, die Gefährdung von Zeugen zu vermeiden. Deshalb ist es inzwischen gesetzlich zulässig, daß gem. § 68 Abs. 2 StPO bei gefährdeten Zeugen statt der Wohnanschrift (nur) eine **ladungsfähige Anschrift** angegeben zu werden braucht. Das Nichtangeben der Wohnanschrift setzt allerdings zwingend eine Abwägung der Grundrechte des Angeschuldigten bzw. Angeklagten auf rechtliches Gehör und ein faires Verfahren einerseits und des Zeugen auf Wahrung des Persönlichkeitsrechts und der körperlichen Unversehrtheit andererseits voraus; eine generelle Anwendung von § 68 Abs. 2 StPO wäre nicht zulässig. Neben gefährdeten Zeugen bietet das Gesetz auch solchen Zeugen, die Wahrnehmungen in amtlicher Eigenschaft gemacht haben, eine Privilegierung an, sie dürfen statt des Wohnortes den Dienstort angeben.

Als Ergebnis habe ich dem Petenten mitgeteilt, daß das von ihm angesprochene Verfahren aus datenschutzrechtlicher Sicht zulässig ist.

4.3 Eingaben zu Grundbuchangelegenheiten

4.3.1 Öffentlichmachen personenbezogener Daten durch Grundbuchauszug

Ein Petent hatte eine Doppelhaushälfte erworben. Nach Abschluß des Kaufvertrages, aber noch vor Eintragung des Verkaufs im Grundbuch, nahm der Käufer einen Kredit auf. Mit Zustimmung des Verkäufers wurde das Grundstück wegen dieses Kredits schon belastet; diese Eintragung erfolgte früher als die über den Eigentumwechsel.

Bei Grundstücksteilungen legt das Grundbuchamt nur für den verkauften Teil ein neues Grundbuchblatt an, während für den Grundstücksteil, der beim abgebenden Verkäufer verbleibt, das bisherige Grundbuchblatt fortgeführt wird. Die Folge ist, daß wegen der Methode der **Darstellung von Löschungen im Grundbuch** (lediglich Streichung) die persönlichen

94 i. d. Fass. vom 7. April 1987, BGBl. I S. 1074, ber. S. 1319; zul. geänd. durch Ges. vom 17. Dezember 1997, BGBl. I S. 3108

Daten der Käufer sowie die Eintragungen der Belastungen des abgespaltenen Grundstücks auch auf dem ursprünglichen Grundbuchblatt weiterhin unabänderlich erkennbar bleiben.

Der Eigentümer des ursprünglich ganzen Grundstücks erhält so mit jedem Grundbuchauszug Daten und Informationen über ein anderes Grundstück, das ihm gar nicht gehört. Wird das Grundstück verkauft, erhält sogar der neue Eigentümer diese Informationen, obwohl ihm der abgetrennte Grundstücksteil nie gehört hat; dieselbe Problematik ergibt sich für den Fall, daß Personen oder Stellen unter Darlegung eines berechtigten Interesses Einsicht in das Grundbuch nehmen. Hierdurch sah sich der Petent in seinen Persönlichkeitsrechten beeinträchtigt.

Leider sieht das Grundbuchrecht in diesen Fällen nicht vor, daß bei einer Teilung von Amts wegen oder auf Antrag nicht nur ein, sondern immer gleich zwei neue Grundbuchblätter anzulegen sind. Grundbuchordnung (GBO)[95] und Grundbuchverfügung (GBV)[96] sind so gestaltet, daß eine **Grundstücksteilung** nicht der Anlaß dafür ist, auch das ursprüngliche Grundbuchblatt durch ein neues zu ersetzen oder es umzuschreiben.

Wegen dieser Angelegenheit habe ich mich an das MdJBE und an den BfD gewandt, um eine Änderung der GBV anzuregen. Es geht um eine Änderung der Grundbuchverfügung dahingehend, daß die Teilung von Grundstücken - oder die Vereinigung oder die Zuschreibung von Grundstücken - neben anderen Gründen zum Anlaß genommen werden kann, das ursprüngliche Grundbuchblatt zu schließen und neue Grundbuchblätter anzulegen, die der jeweiligen aktuellen Situation entsprechen.

4.3.2 Einsicht in Grundbuchakten durch Berufsgenossenschaft

Jeder Eigentümer eines landwirtschaftlichen oder forstwirtschaftlichen Grundstücks ist gem. § 2 SGB VII[97] Mitglied in einer landwirtschaftlichen Berufsgenossenschaft und hat in dieser Eigenschaft Beiträge zur Unfallversicherung zu zahlen. In einem Fall hatte sich die landwirtschaftliche Berufsgenossenschaft über das Grundbuch Kenntnisse darüber verschafft, wie das kleine (brachliegende) Grundstück eines Petenten im Blick auf dessen Pflicht zur Zahlung von Beiträgen zur Unfallversicherung einzustufen sei.
Durch Angaben in dem Bescheidschreiben hatte die Berufsgenossenschaft ihrem potentiellen Mitglied gegenüber dargelegt, daß der Petent als **Eigentümer eines bestimmten Grundstücks Kraft Gesetzes Mitglied in der Unfallversicherung** geworden sei. Die dem Bescheid zugrundeliegenden Informationen, die sich die Berufsgenossenschaft bei der Einsichtnahme in das Grundbuch und die dazugehörigen Grundbuchakten verschafft hatte, waren dem Kaufvertrag entnommen worden. Über den Bescheid und die Vorgehensweise der Berufsgenossenschaft war der Petent ungehalten, weil er sich nicht in der Rolle eines Unternehmers im Sinne der Bestimmungen der Unfallversicherung, durch die er zur Zahlung verpflichtet werden sollte, sah.

Ich habe dem Petenten mitgeteilt, daß aus datenschutzrechtlicher Sicht nichts gegen die Vorgehensweise der Berufsgenossenschaft einzuwenden ist, da dafür sowohl im Bereich des Sozial- als auch des Grundbuchrechts bereichsspezifische Datenschutzregelungen bestehen. Insbesondere die Grundbuchverfügung befugt die Berufsgenossenschaft, gem. § 43 GBV das Grundbuch und darüber hinaus gem. § 46 GBV die Grundakten einzusehen. In der Praxis bedeutet dies, daß von der Berufsgenossenschaft als einer Behörde immer dann, wenn die sonstigen ihr zur

---

95 i. d. Fass. vom 26. Mai 1994, BGBl. I S. 1114

96 vom 24. Januar 1995, BGBl. S. 114

97 vom 7. August 1996, BGBl. I S. 1254; zul. geänd. durch Ges. vom 17. Dezember 1997, BGBl. I S. 3108

Verfügung stehenden Möglichkeiten, sich Sicherheit über die beitragspflichtige Person und über die Beitragshöhe zu verschaffen, nicht ausreichen, die gesamten Unterlagen, die zu einem Grundstück bei dem Grundbuchamt vorliegen, eingesehen werden können.

4.3.3 Einsichtnahme ins Grundbuch ganz und gar?

Einer weiteren Eingabe lag die Angabe zugrunde, daß ein Grundstückspächter gegenüber dem Grundstückseigentümer Kenntnisse vorweisen konnte, die der Pächter u. a. aus dem Erbschein entnommen haben mußte. Das Grundstück war 1993 rückübereignet worden. Etwa ein Jahr später erhielt der weit entfernt lebende neue Eigentümer überraschend Besuch von dem Pächter; dieser trat dem Eigentümer gegenüber „wie eine Amtsperson" auf und konnte auf umfassendes Wissen über Regelungen als Folge des Einigungsvertrages zurückgreifen.

Da sich der Eigentümer unter Druck gesetzt fühlte, wandte er sich mit der Bitte um Klärung an mich, ob der Pächter die Kenntnisse über ihn als den Verpächter zu Recht erhalten habe. Zu meinem Bedauern konnte ich in diesem Fall dem Petenten nicht helfen.

Das Grundbuchrecht läßt die Einsicht in das Grundbuch selbst, aber auch in die Grundbuchakten zu, und zwar immer dann ganz, wenn die Voraussetzungen für die Einsicht vorliegen, oder gar nicht. Die Voraussetzungen liegen vor, wenn ein berechtigtes Interesse dargelegt wird. In dem vorliegenden Fall war einem Pächter, der durch die Rückgabe eines Grundstücks an den (wirklichen) Eigentümer einen neuen Verpächter erhalten hatte, das berechtigte Interesse wohl nicht abzusprechen, auch wenn er über das Grundbuch hinaus auch in die Grundakten hatte Einsicht nehmen wollen.

Insbesondere ein Pächter, der wegen der **Rechte**, die diesem in Situationen zustehen, die **durch das Sachenrechtsbereinigungsgesetz**[98] oder **durch das Schuldrechtsänderungsgesetz**[99] geregelt sind und dessen rechtliche Beziehungen zum Eigentümer von Gesetzes wegen voraussichtlich viele Jahre andauern werden, wird ein Interesse daran haben, sich über seinen Vertragspartner informieren zu können, den er nicht frei gewählt hatte und den er persönlich in sehr vielen Fällen nicht kennen wird; die Fallgestaltung betrifft allerdings nur die neuen Bundesländer. Schon allein an diesem Beispiel wird deutlich, daß das Einsichtsrecht auch im Grundbuch an Erforderlichkeitskriterien nach Art und Umfang gebunden sein müßte.

4.4 Forschung

Auch in diesem Berichtszeitraum bat mich das MdJBE mehrfach um Stellungnahmen zu Forschungsprojekten. Nachfolgend soll nur auf die vom Ministerium für Bildung, Jugend und Sport in Auftrag gegebene Untersuchung über die Ursachen der in den letzten Jahren im Land Brandenburg signifikant zunehmenden Gewalttaten junger Menschen (vorrangig von Jugendlichen) vor allem gegen ausländische und fremd wirkende Bürger, Personen mit Behinderung oder sonstige Minderheiten berichtet werden.

---

98 Art. 1 des Gesetzes zur Änderung sachenrechtlicher Bestimmungen (Sachenrechtsänderungsgesetz - SachenRÄndG) vom 21. September 1994, BGBl. I S. 2457

99 Art. 1 des Gesetzes zur Anpassung schuldrechtlicher Nutzungsverhältnisse an Grundstücken im Beitrittgebiet (Schuldrechtsanpassungsgesetz - SchuldRAnpG) vom 21. September 1994, BGBl. I S. 2538

Die Studie sollte sich in zwei Abschnitte gliedern:

- Herausfilterung von zu untersuchenden Fällen sowie deren Aktenanalyse hinsichtlich Erstellung einer codierten Fallgeschichte unter Berücksichtigung von Tatgeschehen, Familiensituation und Schulbildung,

- Anbahnung und Durchführung eines zweistündigen Interviews durch erfahrene Psychologen unter Vermittlung des Sozialdienstes.

Während für das Aktenstudium von einer nicht zu erhaltenden Einwilligung ausgegangen werden mußte und auf das überwiegende öffentliche Interesse gem. § 28 Abs. 2 Buchst. b BbgDSG abgestellt werden konnte, war die Einwilligung für den zweiten Teil der Studie unabdingbare Voraussetzung.

Die Besonderheit des Forschungsprojektes lag in der **Wirksamkeit der Einwilligung** gem. § 4 Abs. 1 Buchst. b BbgDSG **unter den Bedingungen des laufenden Strafvollzugs**. Einigkeit bestand darin, daß die freie Entscheidung Einsitzender ein schwer zu beurteilendes Problem ist und insoweit empirische Untersuchungen in diesem Bereich nur sehr eingeschränkt möglich sind. Ein Erwartungsdruck bei diesem Personenkreis dürfte nie ganz zu vermeiden sein; abzulehnen wären Interviews - und zwar sowohl aus datenschutzrechtlichen als auch wissenschaftlichen Gründen -, die unter Ausnutzung einer solchen Zwangssituation geführt würden. Deswegen kam der Anbahnung der Gespräche über den Sozialdienst eine besondere Bedeutung zu. Auf zunächst vorgesehene psychologische Tests wurde trotzdem verzichtet.

5 Bildung, Jugend und Sport

5.1 Gesetze und Verordnungen

Im Berichtszeitraum hat das Ministerium für Bildung, Jugend und Sport (MBJS) u. a. die Rechtsverordnungen Datenschutzverordnung Schulwesen [100], Nichtschüler-Prüfungsverordnung [101] sowie die Verwaltungsvorschrift VV-Schulakten [102] rechtzeitig zum Schulbeginn 1997/98 in Kraft gesetzt.[103]

In der von mir im Berichtszeitraum herausgegebenen **Informationsbroschüre „Datenschutz in Schulen“**[104] sind alle für den Schulbereich maßgeblichen datenschutzrechtlichen Gesetze, Verordnungen, Verwaltungsvorschriften sowie speziellen Verträge aufgeführt. Sie kann bei meiner Behörde angefordert werden.

5.1.1 Lehrerbildungsgesetz

Im Berichtszeitraum hat nunmehr das MBJS einen Entwurf für ein Brandenburgisches Lehrerfortbildungsgesetz (BbgLebiG) vorgelegt. Dieser Gesetzentwurf regelt die gesamte Ausbildung in der ersten (Lehramtsstudium) und zweiten Phase (Vorbereitungsdienst) einschließlich der beiden Staatsprüfungen, die Anerkennung von außerhalb des Landes

100 vom 14. Mai 1997, GVBl. II S. 402

101 vom 23. August 1997, GVBl. II S. 762

102 vom 14. Mai 1997, ABl. MBJS S. 442

103 s. 5. Tätigkeitsbericht unter 5.1.1.1 sowie unter 5.1.1.2

104 s. unter III, S. 51 ff.

Brandenburg erworbenen Lehramtsbefähigungen sowie den gesamten Bereich der Lehrerfort- und -weiterbildung.

Als Aufbewahrungsfristen für die dabei erstellten schriftlichen **Prüfungsarbeiten und Aufzeichnungen** habe ich fünf Jahre empfohlen. Anstatt sie nach Fristablauf zu vernichten, können sie dem Betroffenen auch auf Antrag ausgehändigt werden.

Der Gesetzentwurf regelt in § 20 datenschutzgerecht die Verarbeitung personenbezogener Daten. Danach dürfen die **zuständigen Behörden** (u. a. das Landesprüfungsamt und die staatlichen Studienseminare) personenbezogene Daten von Studierenden und von Lehramtskandidaten nur insoweit verarbeiten, als dies für die Zulassung zur ersten Staatsprüfung, deren Durchführung und Abschluß, für die Zulassung zum Vorbereitungsdienst und dessen Durchführung sowie für die Zulassung zur zweiten Staatsprüfung, deren Durchführung und Abschluß erforderlich ist.

5.1.2 Verwaltungsvorschrift zum Schulbetrieb

Die Verwaltungsvorschriften über die Organisation der Schulen in inneren und äußeren Schulangelegenheiten (VVSchulB)[105] fassen Bestimmungen zusammen, die für alle Schulformen und Bildungsgänge gelten sowie die Organisation des täglichen Schulbetriebes von den Unterrichtszeiten bis hin zur Sicherheitsausstattung der Schulen regeln. Dankenswerterweise hat das MBJS hierzu alle meine Anregungen aufgegriffen.

So ist u. a. festgelegt, daß der Schule in denjenigen Fällen, in denen sie begründete Zweifel hat, ob ein Schüler tatsächlich aus gesundheitlichen Gründen dem Unterricht fernbleibt, ein **ärztliches Attest** vorzulegen ist, daß jedoch **keine Angaben über die Erkrankung** enthalten sein darf. Weiterhin ist der Landesbeauftragte für den Datenschutz ausdrücklich in den Personenkreis aufgenommen worden, der ein uneingeschränktes Zutrittsrecht zu allen Diensträumen in Schulen hat.

Erwähnenswert ist auch der auf mein Betreiben hin aufgenommene Hinweis, daß Informationen über gesundheitliche Beeinträchtigungen oder Fehlverhalten einzelner Schüler nicht auszuhängen sind. Die Informationen erfolgen unter Beachtung der datenschutzrechtlichen Bestimmungen, d. h. sie sind den jeweils betreffenden Lehrkräften z. B. in einem verschlossenen Umschlag mitzuteilen.

5.1.3 Grundschulverordnung

[105] vom 1. Dezember 1997, ABl. MBJS S. 894

In der schulärztlichen Stellungnahme zur Aufnahme in den Bildungsgang der Grundschule sollte ursprünglich das Gesundheitsamt für den Fall, daß es Bedenken gegen die **Einschulung** hat, die dafür ausschlaggebenden Gründe in dem Vordruck benennen. Hierbei handelte es sich um das fast identische Formular der Anlage 4 der außer Kraft getretenen Verwaltungsvorschriften über die Aufnahme von Schülerinnen und Schülern in die Grundschule.[106] Dieser alte Vordruck stand im Widerspruch zu § 5 Abs. 3 Verordnung über den Bildungsgang der Grundschule (GV)[107], wonach das Gesundheitsamt der örtlich zuständigen Schule nur das **Ergebnis der schulärztlichen Untersuchung** - also lediglich die gesundheitliche Schulfähigkeit - mitteilen darf. Aus meiner Sicht bestand die Gefahr, daß das Gesundheitsamt in dem Feld „folgende Bedenken" Eintragungen vornimmt, die über eine Ergebnismitteilung hinausgehen und unzulässig medizinische Daten bzw. eine Diagnose enthalten könnten. Das Ministerium teilte diese Befürchtungen und hat sich schließlich in dem Verordnungstext für folgende Formulierung entschieden:

„Aus ärztlicher Sicht ist das Kind:

- ❒ gesundheitlich schulfähig
- ❒ gesundheitlich nicht schulfähig".

Meine Forderung, die Unterlagen eines Förderausschußverfahrens in einem verschlossenen Umschlag aufzubewahren, ist durch einen Zusatz in der Anlage 1 der Datenschutzverordnung Schulwesen (DSV)[108] aufgenommen worden.

Des weiteren hat sich das Ministerium meinem Vorschlag angeschlossen, für die Förderung von Schülern mit erheblichen Lernschwierigkeiten erst dann Fachleute hinzuziehen, wenn die Eltern über das Vorhaben informiert wurden. Damit wird deren in § 46 Abs. 1 BbgSchulG festgelegten Informationsrecht Rechnung getragen.

Wechselseitige **Hospitationen** zwischen Kindertagesstätte, Hort und der Grundschule sind jetzt nur nach vorheriger Einwilligung der Eltern gestattet.

5.1.4 Sonderpädagogik-Verordnung

106 vom 12. Dezember 1994, ABl. MBJS 1995 S. 50

107 vom 16. Juni 1997, GVBl. II S. 473

108 vom 14. Mai 1997, GVBl. I S. 402

§ 31 BbgSchulG enthält eine Ermächtigung, die nähere Ausgestaltung der sonderpädagogischen Förderung durch Rechtsverordnung zu regeln. Die bisherige Sonderpädagogik-Verordnung[109] beruhte noch auf der außer Kraft getretenen Ermächtigungsgrundlage in § 75 des Ersten Schulreformgesetzes[110] und mußte deshalb geändert werden. Die mir zur Stellungnahme vorgelegte Verordnung über Unterricht und Erziehung für junge Menschen mit sonderpädagogischem Bedarf (SopV)[111] bestimmt u. a. die Aufgaben und die Organisation der sonderpädagogischen Förder- und Beratungsstellen sowie die Art und den Umfang der Zusammenarbeit mit diesen Stellen und das Verfahren zur Ermittlung des sonderpädagogischen Förderbedarfs sowie der Entscheidung des staatlichen Schulamtes.

Neben Formulierungsvorschlägen zu einzelnen Regelungen habe ich dem MBJS mitgeteilt, daß der Begriff „Förderausschuß" gesetzlich nicht definiert ist. Das Ministerium hat in der SopV nunmehr festgelegt, daß der **Förderausschuß** weder eine Schulbehörde i. S. d. § 65 Abs. 3 BbgSchulG noch den schulischen Gremien i. S. d. § 74 Abs. 3 BbgSchulG zuzuordnen sei. Deshalb hat es für den Förderausschuß eine eigene Datenverarbeitungsregelung in § 14 SopV aufgenommen. Danach erhebt und verarbeitet der Förderausschuß die zur Feststellung des sonderpädagogischen Förderbedarfs, insbesondere die zur Erstellung einer Bildungsempfehlung nach dem Verfahren der Kind-Umfeld-Diagnostik erforderlichen sonderpädagogischen, medizinischen und psychologischen Daten.

Bisher sah die Sonderpädagogik-Verordnung vor, daß **weitere Fachleute** (z. B. Schularzt, eine Fachkraft des Jugendamtes) in den Förderausschuß berufen werden sollten. Dazu war lediglich eine „Information der Eltern" vorgesehen. Mein Hinweis, daß der erweiterte Personenkreis innerhalb des Förderausschusses Daten über den Schüler ausschließlich auf der Grundlage einer Einwilligung der Eltern erheben und verarbeiten darf, wurde erfreulicherweise in der Rechtsverordnung berücksichtigt.

Auch für die sonderpädagogischen Förder- und Beratungsstellen hat das MBJS auf meinen Vorschlag hin eine Regelung nachträglich eingefügt, wonach personenbezogene Daten dieser Stellen im Rahmen der Bestimmungen gem. § 65 Abs. 3 und 6 BbgSchulG erhoben und verarbeitet werden dürfen.

Schließlich hat das MBJS die gegenseitigen Informationen oder Hospitationen zwischen Förderschulen und Horten zuvor von den Einwilligungen der betroffenen Schüler, bei Nichtvolljährigen der Eltern, abhängig gemacht, sofern diese Informationsflüsse den Austausch personenbezogener Daten umfassen.

5.1.5 Berufsfachschulverordnung für kaufmännische Berufe

Der berufsfachschulbezogene Bildungsgang dauert drei Jahre und teilt sich in einen fachtheoretischen und fachpraktischen Teil, wobei sich der vollzeitschulische Unterricht in einen berufsübergreifenden und einen berufsbezogenen Bereich gliedert. Vorgesehen ist der Bildungsgang Bürokaufmann bzw. Kaufmann für Bürokommunikation.

Um eine unzulässige Datenvorratshaltung zu vermeiden, hat das MBJS in der Verordnung über den Bildungsgang der Berufsfachschule zum Erwerb eines Berufsabschlusses in kaufmännischen Berufen nach dem Berufsbildungsgesetz (KaufBFSV) entsprechend meiner Ausführungen festgelegt, **eingereichte Unterlagen** nach zweimaliger Nichtversetzung

---

109 vom 30. November 1992, GVBl. II S. 748

110 i. d. Fass. vom 1. Juli 1992, GVBl. I S. 258; zul. geänd. durch Art. 2 Ges. z. Änd. besoldungsrechtl. u. Schuldvorschr. vom 27. Juni 1995, GVBl. I S. 138

111 vom 24. Juni 1997, GVBl. II S. 504

den Schülern unverzüglich zurückzugeben. Dies gilt ebenfalls für den Fall, daß der Schüler nach einer Wiederholung erneut zur Prüfung nicht zugelassen wird.

Ferner habe ich empfohlen, in der als Anlage 4 enthaltenen Vereinbarung über das **Praktikum** die Praxisstelle zu verpflichten, die technischen und organisatorischen Maßnahmen zu ergreifen, die zur Umsetzung der Datenschutzbestimmungen erforderlich sind sowie die Schüler auf den Umgang mit personenbezogenen Daten hinzuweisen. Das MBJS wollte diesen Vorschlag in der Rechtsverordnung berücksichtigen. In der Sache hat das Ministerium klargestellt, daß die von den Schülern während des Praktikums wöchentlich anzufertigenden Berichte, Berichtsblätter im Sinne der Anlage 5 der Verordnung sind. In diesen Berichtsblättern sollen neben den Ausbildungsinhalten (Tätigkeiten) anhand von Beispielen auch Bemerkungen eingetragen werden. Dieses offene Feld eröffnet der Praxisstelle Raum für Eintragungen, die nicht nur in unmittelbarem Zusammenhang mit den durchgeführten Tätigkeiten stehen, wie z. B. Informationen über Verhaltensauffälligkeiten von Schülern. Das MBJS signalisierte mir, auf dieses Feld zu verzichten.

Durch ein Versehen im Verfahren der Inkraftsetzung sind jedoch meine Anregungen zur Ergänzung bzw. Veränderung der Anlagen 4 und 5 der KaufBFSV nicht eingearbeitet worden. Aus diesem Grunde hatte das MBJS allen Schulen, die diesen Bildungsgang eingerichtet haben, mitgeteilt, daß die beiden Anlagen aus der inhaltlich identischen Berufsfachschulverordnung (BFSV)[112] auch für den Bildungsgang der KaufBFSV zu verwenden seien. Ein solcher Hinweis auf den Formularaustausch ist aus meiner Sicht lediglich für eine kurze Übergangszeit, nicht jedoch auf Dauer hinnehmbar. Aus Gründen der Normenklarheit und Rechtssicherheit habe ich deshalb angeregt, eine Änderungsverordnung zu erlassen. Das MBJS hat mir mitgeteilt, z. Zt. damit beschäftigt zu sein.

5.1.6 Berufsfachschulverordnung

Das Ziel dieses Bildungsganges, der zum Berufsabschluß nach Landesrecht als kaufmännischer, chemisch-technischer oder biologisch-technischer Assistent führt, besteht in der Vermittlung einer beruflichen Erstausbildung in verschiedenen Berufszweigen.

[112] s. unter 5.1.6

Ich habe hier gefordert, daß der Aufnahmeantrag dem Schulleiter unmittelbar und nicht dem Oberstufenzentrum generell zuzuleiten ist. Diese Empfehlung hat das MBJS zwar geteilt, übernahm diese jedoch wegen einer technischen Panne nicht in den Verordnungstext. Nach Rücksprache mit dem MBJS wird es die Verordnung über den Bildungsgang der Berufsfachschule zur Erlangung eines Berufsabschlusses nach Landesrecht (BFSV)[113] nachträglich ändern. Die zu Anlage 4 und 5 der KaufBFSV[114] gemachten Vorschläge, sind erfreulicherweise in der Vereinbarung über das Praktikum (Anlage 3) und dem Berichtsblatt (Anlage 4) der BFSV berücksichtigt worden.

5.1.7 Berufsfachschulverordnung mit Berufsabschluß gemäß Bundesbildungsgesetz und Handwerksordnung

In dem Bildungsgang der Berufsfachschule zum Erwerb eines Berufsabschlusses nach dem Berufsbildungsgesetz oder der Handwerksordnung werden die für das erfolgreiche Bestehen der Abschlußprüfung vor der zuständigen Stelle erforderlichen fachtheoretischen und fachpraktischen Kenntnisse und Fertigkeiten vermittelt und die Allgemeinbildung erweitert.

Erfreulicherweise sind meine allgemeingültigen Anregungen bezüglich der Rechtsverordnungen der Berufsfachschule (KaufBFSV und BFSV)[115] in der Verordnung über den Bildungsgang der Berufsfachschule zum Erwerb eines Berufsabschlusses nach dem Berufsbildungsgesetz oder der Handwerksordnung Berufsfachschulverordnung[116] ebenfalls berücksichtigt worden. So ist z. B. vorgesehen, daß nach Entlassung aus dem Bildungsgang, die eingereichten Unterlagen den Schülern unverzüglich zurückzugeben sind.

Die Schüler haben nach dieser Verordnung einen **Ausbildungsnachweis** (Berichtshefte) zu führen, mit dem sichergestellt werden soll, daß der zeitliche und sachliche Ablauf der Ausbildung für alle Beteiligten - Auszubildenden, Ausbildungsstätte, Berufsschule und gesetzlichen Vertreter des Auszubildenden - in möglichst einfacher Form (stichwortartige Angaben) nachgewiesen wird. Bei den Berichtsheften handelt es sich um verbindliche Vordrucke für den Ausbildungsnachweis. Sie werden den Schülern von den fachpraktischen Ausbildungsstätten zur Verfügung gestellt und nach der Prüfung Eigentum der Schüler.

5.1.8 Fachoberschulverordnung

Die Fachoberschule vermittelt fachliche Kenntnisse und Fähigkeiten, erweitert die allgemeine Bildung und schließt mit der Fachhochschulreifeprüfung ab. Sie gliedert sich u. a. in die Fachrichtungen

- Technik,
- Wirtschaft und Verwaltung,
- Sozialwesen.

---

113 vom 19. Juni 1997, GVBl. II S. 585

114 s. unter 5.1.5

115 s. unter 5.1.5 und 5.1.6

116 vom 3. Juli 1997, GVBl. II S. 610

Meinen Empfehlungen zu der zugrundeliegenden Verordnung über die Bildungsgänge der Fachoberschule (FOSV)[117] hat das MBJS nur zum Teil übernommen. So erfolgt eine Datenübermittlung von der Praxisstelle hinsichtlich der schriftlichen Beurteilung über die jeweiligen Schüler nach wie vor generell an das **Oberstufenzentrum**, das als berufliche Schule u. a. die Fachoberschule zusammenfaßt. Insbesondere im Hinblick auf diese Bewertungen, die höchstpersönliche Angaben (z. B. über Arbeitsverhalten und Zuverlässigkeit) enthalten, habe ich gefordert, daß zur Vermeidung der Gefahr, einen zu großen Adressatenkreis zu benennen, unmittelbar der Empfänger, d. h. hier die Schulleiter als Adressat des Oberstufenzentrums, bezeichnet werden sollte.

Dagegen hat das MBJS neben der ursprünglich lediglich vorgesehenen **Verschwiegenheitsverpflichtung** der Gäste auch die Mitglieder des Prüfungsausschusses einbezogen. Dementsprechend ist in der Prüfungsniederschrift nun lediglich eine Notiz über die Belehrung zur Verschwiegenheitspflicht vorgesehen, jedoch die Erklärung zur Verschwiegenheit über alle Prüfungsvorgänge seitens der Mitglieder des Prüfungsausschusses nicht Bestandteil der Prüfungsniederschrift geworden.

5.1.9 Berufsfachschulverordnung für sozialpflegerische Berufe

Die zweijährige Ausbildung gemäß der Verordnung über den Bildungsgang zum Erwerb eines Berufsabschlusses nach Landesrecht in den Sozialberufen an der Berufsfachschule (SozBFSV)[118] gliedert sich in einen theoretischen und einen fachpraktischen Teil, der die Arbeitsfelder Altenpflege, Familienpflege und Heilerziehungspflege umfaßt. Dieser Bildungsgang schließt mit dem Erwerb als Sozialpflegeassistent ab.

Erfreulicherweise enthielt der Entwurf bereits datenschutzrechtliche Passagen, so z. B. wird geregelt, daß die Schüler, insbesondere hinsichtlich der Kenntnis über personenbezogene Daten und Umstände von zu betreuenden Personen, Verschwiegenheit zu wahren haben. Daneben wird die **Verschwiegenheitspflicht** der Mitglieder des Prüfungsausschusses und der Gäste über alle Prüfungsvorgänge in der Prüfungsniederschrift festgelegt.

Darüber hinaus ist eine Einsichtnahme in die Prüfungsunterlagen vorgesehen. Der Prüfling kann sich dabei von einer Person begleiten lassen. Ohne Einschränkung sollte dieser Person ebenfalls Einsicht gewährt werden. Im Interesse des Rechts auf informationelle Selbstbestimmung des Prüflings habe ich mit Erfolg gefordert, daß hierfür der Prüfling vorher sein Einverständnis erklären muß. Diese Ergänzung scheint für die Fälle geboten, in denen eine zweite Person lediglich als Begleitperson (z. B. bei gesundheitlichen Beeinträchtigungen) auftritt.

5.1.10 Verordnung über wissenschaftliche Untersuchungen

Bereits in meinem zweiten Tätigkeitsbericht[119] habe ich über die Verwaltungsvorschrift über wissenschaftliche Untersuchungen in Schulen (VV-WissUV)[120] berichtet. Nunmehr ist im Zuge der Anpassung an die neue Rechtslage die Verwaltungsvorschrift in den Rang einer Rechtsverordnung gehoben worden.

Neu ist in der Verordnung über die Genehmigung wissenschaftlicher Untersuchungen an Schulen (WissUV)[121] die

---

117 vom 24. Mai 1997, GVBl. II S. 434

118 vom 24. April 1997, GVBl. II S. 266

119 s. unter 5.1.4

120 vom 1. August 1995, ABl. MBJS S. 408

121 vom 11. Dezember 1997, GVBl. II S. 118

Bestimmung, daß die Durchführung von Untersuchungen oder Erhebungen im Rahmen von wissenschaftlichen Haus- und Prüfungsarbeiten von Studierenden sowie von Lehramtsanwärtern, die als genehmigt gelten, auf der Grundlage des § 66 Abs. 2 Satz 1 BbgSchulG erfolgen. Es ist präzisiert worden, daß diese Untersuchungen keinen Rückschluß auf bestimmbare Schüler, Lehrkräfte oder auf das sonstige Schulpersonal ermöglichen dürfen.

Aus aktuellem Anlaß - und zwar aufgrund zunehmender Anfragen von Parteien, aber auch rechtsradikaler Gruppierungen an Schüler - sind Untersuchungen oder Erhebungen, die Schüler an ihrer oder an einer anderen Schule durchzuführen beabsichtigen, erstmalig geregelt worden. Diese unterliegen nicht der ministeriellen Genehmigungspflicht, sondern bedürfen der **Genehmigung durch die Schulleitung** der Schule, an der die Untersuchung geplant ist. Sofern dort personenbezogene Daten bei Schülern oder anderen an der Schule tätigen Personen erhoben werden sollen, ist die Genehmigung davon abhängig, ob die Einhaltung datenschutzrechtlicher Bestimmungen gewährleistet ist. Das ursprünglich vom MBJS vorgesehene ledigliche Hinwirken der Schule auf den Datenschutz habe ich als nicht ausreichend angesehen.

In dem Katalog der den Anträgen auf Genehmigung einer wissenschaftlichen Untersuchung beizufügenden Unterlagen ist in bezug auf § 4 Abs. 2 BbgDSG ein Muster der widerruflichen Einverständniserklärung der Eltern zur freiwilligen Teilnahme der minderjährigen Kinder an der Befragung sowie ein Muster eines Hinweises an die Schüler, daß die **Teilnahme** an der wissenschaftlichen Untersuchung **freiwillig und jederzeit widerrufbar** ist, aufgenommen worden.

Als Rechtsgrundlage für die wissenschaftlichen Untersuchungen habe ich auf § 66 Abs. 2 BbgSchulG hingewiesen, wobei ergänzend die Bestimmungen des Brandenburgischen Datenschutzgesetzes gelten, so findet z. B. für die Form der **Einwilligungserklärung** § 4 Abs. 2 BbgDSG Anwendung. Soweit die Antragstellenden keine öffentlichen Stellen sind und somit das Brandenburgische Datenschutzgesetz auf sie keine Anwendung findet, ist festgelegt, daß sie entsprechend zu verpflichten sind.

Das Genehmigungsverfahren hat sich insoweit geändert, als die Anträge auf Genehmigung einer wissenschaftlichen Untersuchung spätestens drei Monate vor deren Beginn bei dem für Schule zuständigen Ministerium vollständig eingereicht werden. Zum Zeitpunkt der **Antragstellung** sollen die für die wissenschaftliche Untersuchung vorgesehenen Schulen von dem Antragsteller schriftlich und umfassend über die beabsichtigte Untersuchung informiert werden. Hiermit wird die rechtzeitige Beteiligung der Schulen gem. § 91 Abs. 3 Nr. 9 BbgSchulG gesichert.

Nunmehr entspricht der Entwurf nach intensiven und kooperativen Gesprächen mit dem MBJS meinen Vorstellungen.

5.1.11 Verwaltungsvorschriften über schulische Zeugnisse

Die Verwaltungsvorschrift über schulische Zeugnisse (VV-Zeu)[122] faßt alle vor Inkrafttreten bestehenden Verwaltungsvorschriften über Zeugnisse in den jeweiligen spezifischen Schulformen - beginnend von der Grundschule bis hin zu den doppelqualifizierenden Bildungsgängen - überschaubar zusammen. Für den Anwender stellt es eine erhebliche Erleichterung dar und dient darüber hinaus dem Grundsatz der Normenklarheit. Datenschutzrechtliche Bedenken hatte ich gegen diese Vorschriften nicht.

[122] vom 1. Dezember 1997, ABl. MBJS vom 8. Januar 1998, S. 954

5.2 Datenschutzrechtliche Einzelangelegenheiten im Schulbereich

5.2.1 Schulverwaltungsprogramm

In meinem 5. Tätigkeitsbericht[123] ging ich bereits ausführlich auf die Einführung eines einheitlichen Schulverwaltungsprogramms (WinSchule) ein. Die dort kritisierten Mängel - u. a. die Felder zum Religionsunterricht - hat das MBJS inzwischen abgestellt. In der aktuellen Version wird nur noch nach der Teilnahme am Unterricht Lebensgestaltung, Ethik und Religion (LER) bzw. am Religionsunterricht gefragt. Das Schulverwaltungsprogramm ist damit an die gesetzlichen Rahmenbedingungen gem. § 65 BbgSchulG angepaßt worden.

Laut Aussage des MBJS haben ca. 450 Schulen das Programm angefordert. Meine Behörde wird die Weiterentwicklung auch in Zukunft kritisch begleiten, vor allem wenn Daten über öffentliche Netze ausgetauscht werden sollten.

5.2.2 Fotografen in der Schule

Immer mehr Fotofirmen machen mit ihrem **Serviceangebot „Schülerausweise"** Jagd auf Schüler. Sie holen klassenweise die schriftlichen Einwilligungserklärungen interessierter Schüler ein. In diesen Einwilligungserklärungen wird gleichzeitig bestätigt, daß die Eltern hierüber informiert seien. Einige von ihren Kindern nicht informierte Eltern wandten sich an mich, da sie das Vorgehen der Fotofirma trotz des Hinweises, daß die Fotos dem angegebenen Zweck dienen sollen, für unseriös hielten und die Schule hierfür verantwortlich machen wollten.

Die ausgegebenen „Schülerausweise", die lediglich den Namen, Vornamen, das Geburtsdatum, das Bild der Schüler sowie die Namen der Schule enthalten, stellten aber keine amtlichen Schülerausweise i. S. d. Verwaltungsvorschriften über Schülerausweise (VV-Schülerausweise)[124] dar, denn deren Erstellung war nicht durch die Schule veranlaßt.

Insoweit lag auch keine **Datenverarbeitung im Auftrag** der Schule i. S. v. § 11 BbgDSG vor. Einer vorherigen Einwilligung der Eltern bedurfte es nicht, da die Schule nicht zur Erfüllung schulischer Aufgaben gehandelt hat, sondern nur dem Unternehmen gestattet hatte, auf dem Schulgelände die Aktion durchzuführen. Es handelte sich hier lediglich um das **privatrechtliche Verhältnis** zwischen den Schülern und dem Unternehmen.

Gleichwohl sollten Eltern zumindest über eine solche Aktion schriftlich informiert werden, um Irritationen vorzubeugen. Dabei wäre den Schulen zur Vermeidung eines großen Verwaltungsaufwandes freigestellt, den Unternehmen solche Aktionen nur unter der Voraussetzung zu gestatten, daß diese sich bereit erklären, Informationsschreiben für die Eltern zur Verfügung zu stellen.

5.2.3 Bundeswehr forscht nach einem ehemaligen Schüler

---

123 s. unter 5.2.2

124 vom 30. September 1991, ABl. MBJS S. 272

Ein Schulleiter wandte sich mit der Frage an mich, ob Mitarbeiter der Bundeswehr Auskünfte über einen ehemaligen Schüler von dessen ehemaligem Klassenlehrer erhalten dürfen. Die erbetenen Auskünfte bezogen sich auf Aussagen über die Ehrlichkeit, Sachlichkeit, den Umgang mit Geld, eventuelle homosexuelle Neigungen sowie eventuelle Angehörigkeit während der Schulzeit zu gewalttätigen Gruppen. Der Schulleiter lehnte derartige Auskünfte ab, solange keine Einwilligungserklärung des ehemaligen Schülers vorgelegt würde und keine datenschutzrechtliche Prüfung erfolgt sei.

Daraufhin legten die Mitarbeiter der Bundeswehr persönlich eine **Einwilligungserklärung** des ehemaligen Schülers vor, die die Befragung zu den o. g. Informationen abdeckte. Der ehemalige Schüler war unterdessen im Marinedienst tätig und mit geheimen Operationen beauftragt. Zwar diente - wie dem Schulleiter nachgewiesen wurde - die Befragung einer **Sicherheitsüberprüfung** in diesem dienstlichen Zusammenhang und war durch Sicherheitsvorschriften, wie das Sicherheitsüberprüfungsgesetz (§§ 7, 10 und 11 SÜG)[125] abgedeckt, jedoch war die Reaktion des Schulleiters, sich zunächst zurückhaltend zu zeigen, korrekt. Es entspricht dem Recht auf informationelle Selbstbestimmung, sich in Vergleichsfällen die zutreffenden Rechtsgrundlagen nennen zu lassen und die Vorlage einer Einwilligungserklärung der Betroffenen zu verlangen.

5.2.4 Projekt „Gläserne Schule“

Die Sicherheitskonferenz Potsdam unterrichtete mich über das Projekt „Gläserne Schule“, das von der Koordinationsstelle Schulische Suchtvorbeugung mit Unterstützung der AOK Schleswig-Holstein durchgeführt werden sollte. Kernstück dieses Projektes ist ein **Fragebogen**, der u. a. Auskunft geben soll über den Konsum und Mißbrauch von Zigaretten, Alkohol, illegalen Drogen sowie Medikamenten, zu Eßgewohnheiten, psycho-sozialen Belastungen und Freizeitverhalten der Schüler. Fragebögen sollen in der Schule von den Schülern anonym ausgefüllt werden. Die Eltern werden zuvor schriftlich über dieses Vorhaben informiert und sollen ihr Einverständnis dazu erklären.

Datenschutzrechtlich hatte ich zum einen darauf hingewiesen, daß bei solchen Befragungen gewährleistet sein muß, daß die Lehrer von den Einzelantworten keine Kenntnis erhalten dürfen. Darüber hinaus ist den Eltern und auch den Schülern zu vermitteln, daß es sich hierbei um eine freiwillige Teilnahme handelt.

Zum anderen erwiesen sich auch Hinweise bzgl. der **Einwilligungserklärung** als notwendig. So fehlten darin die Angabe über das die Studie durchführende Institut. Die Lehrer, die die Einwilligungserklärungen einsammeln und Gewähr dafür übernehmen, daß nur Kinder an der Befragung teilnehmen, für die die Einwilligung der Eltern vorliegt, haben die Einverständniserklärungen zwei Wochen nach der Befragung zu vernichten.

Alle meine Vorschläge sind umgesetzt worden; das Projekt findet mittlerweile an mehreren Schulen (Gymnasien, Gesamtschulen) statt. An der Auswertung sind bereits andere Ämter (z. B. Gesundheitsamt) interessiert, wobei jedoch diesen öffentlichen Stellen nur anonymisierte Daten zur Verfügung gestellt werden dürfen. Hierbei hat die Angabe der Schule zu unterbleiben.

[125] vom 20. April 1994, BGBl. I S. 867

5.2.5 Schülerausweise in Scheckkartenformat

Immer öfter werden Schülerausweise im Auftrag von Schulen im Scheckkartenformat erstellt. Dabei handelt es sich um eine **Datenverarbeitung im Auftrag** gem. § 65 Abs. 1 Satz 2 BbgSchulG i. V. m. § 11 BbgDSG. Soweit der Auftragnehmer keine öffentliche Stelle ist, bedarf die Auftragerteilung der Zustimmung des MBJS.

Dem Ministerium, das z. Zt. noch die Verwaltungsvorschriften über Ausweise zum Nachweis der Schülereigenschaft (VV-Schülerausweis) überarbeitet, habe ich empfohlen, darin u. a. vorzusehen, daß die Schule auch Dritte mit der Erstellung der Karte beauftragen kann, sofern der Auftrag eine Zusatzvereinbarung enthält, die als Anlage in der Verwaltungsvorschrift abgedruckt werden soll. Dieser schriftliche Auftrag enthält Weisungen zur Löschung der Schülerdaten, schließt Unterauftragsverhältnisse mit dem Ausland aus, trifft ferner Festlegungen zu inländischen Unterauftragsverhältnissen, zur Unterwerfung der Kontrolle des Landesbeauftragten für den Datenschutz und zur Bestätigung der Meldepflicht des Auftragnehmers gemäß Bundesdatenschutzgesetz.

Unter diesen Voraussetzungen darf die Schule dem Hersteller mit Einwilligung der Eltern zum Zwecke der Herstellung von Schülerausweisen folgende Daten übermitteln:

- Name, Vornamen
- Nationalität
- Geburtsdatum
- Anschrift
- Lichtbild.

Da das Lichtbild von der Schule geliefert wird, handelt es sich hierbei im Gegensatz zu dem unter 5.3.2. geschilderten Fall um eine Datenverarbeitung durch die Schule.

5.3 Jugend

5.3.1 Kontrollbesuch bei der Zentralen Adoptionsstelle Berlin-Brandenburg

Die Zentrale Adoptionsstelle Berlin-Brandenburg (ZABB) ist eine gemeinsame Einrichtung der Länder Berlin und Brandenburg. Nach dem Staatsvertrag über die Errichtung der ZABB[126] ist die ZABB beim Landesjugendamt Brandenburg (LJA) als dessen Bestandteil in Oranienburg eingerichtet worden. Im Berichtszeitraum hat eine gemeinsame Prüfung mit dem Berliner Datenschutzbeauftragten unter meiner Federführung stattgefunden. Dieser Kontrollbesuch diente der Überprüfung der Umsetzung datenschutzrechtlicher Bestimmungen im Bereich der Adoptionsvermittlung (z. B. §§ 67 bis 85 a SGB X[127] und § 35 SGB I[128]) sowie der Einhaltung technischer und organisatorischer Maßnahmen des Datenschutzes.

5.3.1.1 Aufgaben

---

126 vom 13. Januar 1994, GVBl. S. 79

127 vom 18. August 1980, BGBl. I S. 1469, ber. S. 2218; zul. geänd. durch SGB III-ÄndG vom 16. Dezember 1997, BGBl. I S. 2970

128 vom 11. Dezember 1975, BGBl. I S. 3015; zul. geänd. durch SGB III-ÄndG vom 16. Dezember 1997, BGBl. I S. 2970

Hauptaufgabe der ZABB, die ihre Tätigkeit am 1. Dezember 1994 aufnahm, ist der Aufbau einer nichtautomatisierten „Kinderdatei", geordnet nach den „meldepflichtigen" Einrichtungen in Berlin und Brandenburg. Gem. § 47 Abs. 2 Achtes Buch Sozialgesetzbuch (SGB VIII)[129] ist der Träger einer erlaubnispflichtigen Einrichtung (überwiegend **Heime**), in der Kinder dauernd ganztägig betreut werden, gegenüber der ZABB meldepflichtig. Gemeldet werden müssen die betreuten Kinder, deren bisheriger Aufenthalt und die Einweisungsbehörde. Schließlich ist eine Änderungsmeldung darüber zu machen, ob das Kind zur Adoption in Betracht kommt oder bereits eine Adoptionsvermittlung versucht wurde.

Zur Zeit ist die ZABB damit beschäftigt, die „Kinderdatei" auf ein automatisiertes System umzustellen. Die Eingabe der Meldungen aus den Einrichtungen in Berlin ist bereits abgeschlossen, während die Daten der Einrichtungen Brandenburgs erst zur Hälfte auf den Festplattenspeicher übertragen sind. Die Datenbank wird etwa 1500 bis 1800 Datensätze beider Länder enthalten. Gemeldet werden nur Kinder, die unter 10 Jahre alt sind. Eine Meldung ist dagegen entbehrlich, solange sich Kinder gemeinsam mit dem Personensorgeberechtigten (z. B. der Mutter) in der Einrichtung befinden.

Darüber hinaus unterstützt die ZABB die Adoptionsvermittlungsstellen beim Jugendamt gem. § 11 Adoptionsvermittlungsgesetz (AdVermiG)[130] durch fachliche Beratung, wobei keine personenbezogenen Daten erhoben werden. Mitarbeiter der ZABB leisten z. T. Hausbesuche bei Heimkindern. Eine weitere Aufgabe ist die Hilfe gegenüber Eltern bei der Aufklärung der Kinder über ihre Herkunft seitens der Eltern bzw. die Suche nach ihren leiblichen Eltern. Ferner ist die ZABB für internationale Adoptionen bzw. für alle Auslandsdeutschen zuständig.

5.3.1.2 Ergebnisse der Prüfung

Postlauf

Im Rahmen der Prüfung habe ich erfahren, daß die Zuordnung der Post für die ZABB durch die gemeinsame Poststelle erfolgt. Die Eingangstür zur gemeinsamen **Poststelle** ist während der Anwesenheit der zuständigen Sachbearbeiterinnen stets geöffnet. Die Post für die ZABB öffnet die zentrale Poststelle, steckt sie dann in einen gesonderten Umschlag mit mehreren Einschubfächern, der mit einem Klettverschluß versehen ist. Danach legt sie diesen großen Hefter in ein eigenes offenes Fach seitlich der Eingangstür.

Diese Verfahrensweise verstößt gegen § 35 Abs. 1 Satz 2 SGB I. Nach dieser Vorschrift ist der Leistungsträger verpflichtet, auch innerhalb seiner Einrichtung sicherzustellen, daß die Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden. Die ZABB gilt laut Begründung des Staatsvertrages über die Errichtung einer Zentralen Adoptionsstelle Berlin-Brandenburg (ZABB) als unselbständige Behörde, die Bestandteil des Landesjugendamtes ist. Da in den meisten Fällen auf dem Umschlag die ZABB als Adressat genannt wird, ist eine Zuordnung der Post möglich mit der Folge, daß diese Post unmittelbar, d. h. vor allem ungeöffnet an die ZABB weitergeleitet werden muß. Die Mitarbeiterinnen der gemeinsamen Poststelle sind somit als Unbefugte anzusehen, wenn sie trotz der möglichen Zuordnung die an die ZABB adressierten Briefe öffnen. Darüber hinaus ändert die Aufbewahrung der einzelnen an die ZABB gerichteten Schreiben in Heftern mit Klettverschluß nichts an der Tatsache, daß sie frei zugänglich auch für die anderen Mitarbeiter des Landesjugendamtes sind.

Das LJA hat in seiner Stellungnahme ausgeführt, es werde umgehend sichergestellt, daß die unmittelbar an die ZABB

---

[129] i. d. Fass. vom 15. März 1996, BGBl. I S. 447, geänd. durch Ges. vom 23. Juli 1996, BGBl. I S. 1088

[130] i. d. Fass. vom 27. November 1989 (BGBl. III 404-21)

adressierte Post ungeöffnet an die ZABB weitergeleitet wird. In Einzelfällen versehentlich geöffnete Briefe und Schriftstücke werden wieder zurück in die Originalumschläge gegeben und verschlossen über die Dienstpost der ZABB zugeleitet. Das Personal in der Poststelle wird entsprechend angewiesen und die Regelung mit sofortiger Wirkung in Kraft gesetzt.

Veränderungsmeldungen

Die ZABB verwendet das **Formular** „Veränderungsmeldung", in dem Änderungen gegenüber den Angaben im Meldebogen nach § 47 Abs. 2 SGB VIII eingetragen werden sollen. Obwohl die Veränderungsmeldungen nach dieser Vorschrift nicht vorgesehen sind, sind diese nach Aussage des Leiters der ZABB erforderlich, wenn das Kind nach Hause oder aber in ein Heim eines anderen Bundeslandes entlassen wird. Auch die Aufnahme in eine Familienpflegestelle ist für die ZABB von Bedeutung, da sie nach § 47 SGB VIII nicht meldepflichtig ist. Darüber hinaus wird auch die Entlassung in eine nach § 47 SGB VIII meldepflichtige Einrichtung Berlins oder Brandenburgs in die Veränderungsmeldung eingetragen. Eine solche ist meiner Auffassung nach nicht erforderlich, da diese Einrichtungen ihrerseits nach dem Gesetz meldepflichtig sind und Neuzugänge unter den gegebenen Umständen der ZABB mitteilen müssen. Ich habe darauf hingewiesen, daß zukünftig für diesen Fall eine Veränderungsmeldung zu unterbleiben hat. Eine Veränderungsanzeige im Falle der Entlassung eines Kindes aus einer Einrichtung in eine andere meldepflichtige Einrichtung Berlins oder Brandenburgs wird von der ZABB ab sofort nicht mehr verlangt. Der ZABB-Vordruck „Veränderungsmeldung" wird entsprechend geändert.

Datenlöschung

Eine **Löschung** der personenbezogenen Daten der gemeldeten Kinder erfolgt, wenn diese Kinder in die Pflegefamilie kommen oder wenn ein Entlassungsvermerk vorliegt. Diese Meldungen sind in einer Hängeregistratur in abschließbaren Aktenschränken untergebracht. Für jedes Heim gibt es eine Liste, in der alle Namen von Heimkindern aufgeführt werden. Soweit sie aus den Heimen entlassen wurden und keine Vermittlung in Betracht kommt, werden diese Namen z. T. mit einem grünen Stift, z. T. mit einem schwarzen Stift geschwärzt; trotz dieser Schwärzung sind die Namen noch gut lesbar. Die Schwärzungen sind aufgrund dieses Umstandes unzulänglich. Nach § 61 Abs. 1 Satz 1 SGB VIII i. V. m. § 67 Abs. 6 Ziff. 5 SGB X ist Löschen das Unkenntlichmachen gespeicherter Sozialdaten, d. h. in solchen Fällen muß die jeweilige Liste kopiert, die zu löschenden Angaben geschwärzt und erneut kopiert werden.

Die Schwärzungen von Sozialdaten erfolgen nach Ausführungen der ZABB künftig wie von mir vorgeschlagen.

Externe Systemwartung

Der externe Techniker, der das Administratorpaßwort kennt, kann im Rahmen der **Wartung** auf das ganze System des Landesjugendamtes zugreifen. Aus datenschutzrechtlicher Sicht ist diese Zugriffsmöglichkeit unzulässig. Mit der Wartung ist die Möglichkeit der unbefugten Kenntnisnahme von Sozialdaten gegeben. Für diese sog. Datenübermittlung gibt es keine Befugnisnorm. Nach § 61 Abs. 1 Nr. 1 i.V.m. § 67 d Abs. 1 SGB X ist eine Übermittlung von Sozialdaten nur zulässig, soweit eine gesetzliche Übermittlungsbefugnis nach den §§ 68 bis 77 oder nach einer anderen Rechtsvorschrift in diesem Gesetzbuch vorliegt.

Darüber hinaus verpflichtet § 76 SGB X Sozialleistungsträger, Unterlagen mit Daten, die der ärztlichen Schweigepflicht unterliegen, in der gleichen Weise geheim zu halten, wie dies der Arzt oder eine andere schweigepflichtige Person selbst tun muß. In den Hinweisen zum Umgang mit personenbezogenen Daten in der ZABB vom Januar 1995 wird auf § 203

StGB ausdrücklich Bezug genommen. Es wird davon ausgegangen, daß ein zum persönlichen Lebensbereich gehörendes Geheimnis u. a. durch staatlich anerkannte Sozialarbeiter und deren berufliche Helfer - also etwa in der Adoptionsstelle tätige Verwaltungsfachkräfte - der ärztlichen Schweigepflicht unterliegt.

Zur Lösung des Problems bietet das Landesjugendamt an, daß der **externe Techniker** eine persönliche Erklärung abgibt, in der er sich zur Geheimhaltung sämtlicher Daten verpflichtet, die ihm durch seine Servicetätigkeit zur Kenntnis kommen. Meines Erachtens stellt diese Vorgehensweise keine ausreichende datenschutzgerechte Lösung dar. Vielmehr sollte ein Mitarbeiter zum Systemverwalter qualifiziert und entsprechend eingesetzt werden. Das Landesjugendamt wies darauf hin, daß die Personalhoheit für eine solche Entscheidung beim Ministerium für Bildung, Jugend und Sport liege. Es gab zu bedenken, daß aufgrund der äußerst knappen Personalbemessung des Landesjugendamtes eine solche Aufgabenänderung zu wesentlichen Einschränkungen bei der Wahrnehmung gesetzlicher Aufgaben führe. Dennoch werde ich an der Auffassung festhalten, daß aufgrund des besonderen sensiblen Bereiches ein geeigneter Mitarbeiter zum Systemverwalter qualifiziert werden muß.

Technisch-organisatorische Aspekte

Als Problem stellte sich in der ZABB sowie scheinbar auch im gesamten LJA die Systemverwaltung heraus. Das Amt verfügt über keinerlei eigene ADV-Fachkräfte. Das LJA - wie bereits oben erwähnt - vertraut hier auf eine private Firma, die die Software installiert und alle Rechner administriert. Gegenüber dem für diese Personalentscheidung zuständigen MBJS werde ich die Meinung vertreten, daß im Zuge der ständig wachsenden Automatisierung der Verwaltung einen Mitarbeiter als Systemverwalter zu qualifizieren oder einzustellen ist, der zumindest Wartungs- und Administrationsarbeiten externer Firmen beaufsichtigen kann. Dessen Stellungnahme bleibt abzuwarten.

Kurz vor meinem Kontrollbesuch wurde damit begonnen, das LJA einschließlich der ZABB lokal zu vernetzen und einen Anschluß zum Landesverwaltungsnetz (LVN) herzustellen. Das LJA hat dabei kein Sicherheitskonzept zum Schutz der Sozialdaten der ZABB erstellt. Grund für den Anschluß an das LVN war die Einbindung der Behörde in das HKR-Verfahren. Damit mußte ich zum wiederholten Male feststellen, daß Behörden beim Anschluß an das LVN wenig an die Sicherheit ihrer sensiblen personenbezogenen Daten denken und ihr lokales Netz nicht über eine Firewall absichern[131].

Laut einer ersten Stellungnahme des LJA wird die Datenbank der ZABB wieder aus dem lokalen Netz des LJA ausgegliedert und das geforderte Sicherheitskonzept erstellt. Eine abschließende Beurteilung des Kontrollbesuches war bis zum Redaktionsschluß noch nicht möglich.

[131] s. unter 1.4.1

5.3.2 Teilnehmerlisten für Ferienfreizeiten

Der Vertreter vieler freier Träger der Jugendhilfe eines Landkreises hat mich darüber informiert, daß im Rahmen der letzten regionalen Fachtagung mit den Anbietern von Ferienfreizeiten festgestellt worden sei, daß sich zum Teil inhaltlich stark voneinander abweichende Teilnehmerlisten der Zuwendungsgeber im Umlauf befänden und zu großen Problemen führten. Die Träger der Jugendhilfe waren einhellig der Meinung, daß die Verwendung einer einheitlichen Liste von allen Zuwendungsgebern, insbesondere auch vom MBJS, zu einer Problemlösung beitragen würde. Aus diesem Grunde habe ich mich an das MBJS mit der Bitte gewandt, für Ferienfreizeiten, internationale Begegnungen und Bildungsfahrten, unter der Voraussetzung, daß hierfür eine Förderung nach Teilnehmern erfolge, eine Teilnehmerliste mit maximal folgenden Angaben zu gestalten:

- Name,
- Vorname,
- Alter 6 - 13, 14 - 26,
- Leiter/Betreuer,
- Postleitzahl sowie Wohnort.

Das Ministerium räumte daraufhin ein, daß, soweit Veranstaltungen der Jugendarbeit im Wege der Festbetrags- oder Anteilsfinanzierung gefördert werden, seines Erachtens die persönlichen Daten der Teilnehmer grundsätzlich nicht zu erheben seien. In begründeten Einzelfällen dürfte eine eingeschränkte Erhebung in dem von mir vorgeschlagenen Sinne ausreichen. Werden hingegen solche Veranstaltungen mit teilnehmerbezogenen Festbeträgen gefördert, so sind nach Auffassung des MBJS als Verwendungsnachweise lediglich die Teilnehmerlisten, ein Beleg, der die Dauer der Maßnahme nachweist, und ein Sachbericht einzureichen. In solchen Fällen kann auf die vollständigen Angaben der Teilnehmer nicht verzichtet werden, weil eine Rechnungsprüfung dann nicht mehr durchführbar sei. Das Land fördere in den Bereichen, wo Maßnahmen der Jugendarbeit bezuschußt werden, generell im Wege der Festbetragsfinanzierung. Weiterhin wies das MBJS darauf hin, daß ein Jugendamt für besondere Fälle nicht daran gehindert sei, besondere Regelungen zu treffen. Es sei jederzeit möglich, in Ausnahme von bestehenden Richtlinien z. B. die Finanzierungsart und damit die Verwendungsnachweisführung abweichend zu regeln, insbesondere, wenn aus der Natur des Zuwendungsempfängers auf einen bestimmten Teilnehmerkreis geschlossen werden könne, dessen Sozialdaten in besonderer Weise schützenswert seien (wie z. B. bei einem Förderverein für krebskranke oder psychisch kranke Kinder).

Mit Bedauern habe ich zur Kenntnis genommen, daß das MBJS keine Grundlage sehe, den Jugendämtern eine bestimmte Form von Teilnehmerlisten zur Verwendung vorzuschlagen, es vielmehr dem Zuwendungsgeber überlasse, entsprechend den Erfordernissen des Einzelfalles die Teilnehmerlisten zu gestalten. Somit wird es auch in Zukunft weiterhin unterschiedliche Teilnehmerlisten je nach Veranstaltungsart geben, was ich als sehr unbefriedigend ansehe.

5.3.3 Neue Entgeltsatzung des Kita-Verbundes

Auch nach der neuen Rechtslage im Bereich der Kita-Gebührenerhebung[132] wandten sich mehrere Petenten wegen datenschutzrechtlicher Fragen zum Erhebungsbogen und beizubringender Einkommensbescheide an meine Behörde.

Aufgrund der o. g. Änderung des Kita-Gesetzes hatte ein Träger einer Kindertagesstätte seine Satzung über die Höhe der

[132] s. 5.Tätigkeitsbericht unter 5.3.1

Elternentgelte durch eine neue ersetzt. Darüber hat er die Eltern in einem Anschreiben informiert. Die neue Entgelt-Satzung sieht u. a. vor, daß alle im Haushalt lebenden Kinder für die Bemessung der Elternentgelte zu berücksichtigen sind. Des weiteren sind zum Familieneinkommen auch das Kindergeld, BAföG und die Einnahmen der unterhaltsberechtigten Kinder (z. B. Lehrlingsentgelt, BAföG) zu zählen.

Ich habe empfohlen, die Eltern bzw. Erziehungsberechtigten über die Voraussetzungen der Unterhaltsbedürftigkeit ausführlich zu informieren. Da sich die Gestaltung der **Elternbeiträge** zu den Betriebskosten der Kindertagesstätten gem. § 17 Abs. 2 Kita-Gesetz[133] an der Zahl der unterhaltsberechtigten Kinder bemißt, sind nur solche Kinder zu berücksichtigen, die außerstande sind, sich selbst zu unterhalten (siehe § 1602 Abs. 1 BGB). Sofern das Kind seinen Lebensbedarf aus zumutbarer Arbeit oder aus Vermögenseinkünften bzw. sonstigen Einkünften (z. B. Stipendium, BAföG) bestreiten kann, darf es bei der Staffelung nicht berücksichtigt werden. Deshalb sind Angaben zu diesen Familienangehörigen, z. B. über Lehrlingsentgelt, BAföG, nicht erforderlich. Meine Empfehlungen sind vollständig umgesetzt worden. Für die Bemessung der Elternentgelte werden jetzt alle im Haushalt lebenden, unterhaltsberechtigten Kinder berücksichtigt, und zwar alle Kinder, für die ein **Kindergeldanspruch** besteht.

Noch immer stellt die Ablage von Kopien der Einkommensunterlagen in den Akten ein Problem dar. Zurückzuführen ist dieses auf die Entscheidung des **Landesrechnungshofes,** der es nach Maßgabe der auf seine Tätigkeit anzuwendenden Rechtsgrundlagen der Landeshaushaltsordnung und des Brandenburgischen Datenschutzgesetzes für notwendig hält, daß Unterlagen, anhand deren ausgabenrelevante Berechtigungen überprüft werden müssen, mindestens in Kopie zu den Akten genommen werden. Auch hier ist jedoch das Prinzip des geringsten Eingriffs in die Persönlichkeitsrechte zu beachten. Daher kann jeder selbst auf den Kopien die Angaben, die zur Überprüfung der Einkommensverhältnisse nicht benötigt werden (z. B. über die Religionszugehörigkeit, den Arbeitgeber u. ä.), schwärzen und mit den lediglich zum kurzfristigen Vergleich erforderlichen Originalen vorlegen.

6 Wissenschaft, Forschung und Kultur

6.1 Wissenschaft

6.1.1 Spannungsverhältnis von Forschung und Datenschutz - Gespräche mit der Deutschen Forschungsgemeinschaft

[133] vom 10. Juni 1992, GVBl. I S. 178; zul. geänd. durch Ges. vom 17. Dezember 1996, GVBl. I S. 358

Die Deutsche Forschungsgemeinschaft (DFG) hat 1996 eine Denkschrift unter dem Titel „Forschungsfreiheit - Ein Plädoyer für bessere Rahmenbedingungen der Forschung in Deutschland“[134] herausgegeben, die seinerzeit große Beachtung in der Öffentlichkeit gefunden hat, weil darin u. a. dem Datenschutz pauschaliert vorgeworfen wurde, er behindere den Wissenschaftsstandort Deutschland. Dieser Vorwurf - periodisch immer wieder einmal erhoben - ist im Grunde genommen so alt wie das Thema Datenschutz selbst. Die Denkschrift enthielt nichts wesentlich neues, aber mit der Veröffentlichung derselben war das bestehende **Spannungsverhältnis von Persönlichkeitsrecht** einerseits **und Forschungsfreiheit** andererseits bewußt mit Unterstellungen gegen den Datenschutz in den Blickpunkt der Öffentlichkeit gerückt worden. Auf meine Anregung hin hat sich der hiesige Landtagsausschuß für Wissenschaft, Forschung und Kultur mit dieser Problematik befaßt,[135] allerdings ohne daß Wissenschaftler von Forschungseinrichtungen im Land Brandenburg eingeladen worden wären, um aus ihrer Sicht und Erfahrung hierzu Stellung nehmen zu können.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die Angelegenheit für so wichtig erachtet, daß sie ihren Arbeitskreis Wissenschaft beauftragt hat, Kontakte zur DFG aufzunehmen und gesprächsweise offensichtlich bestehende Mißverständnisse auszuräumen. Inzwischen haben bereits mehrere Gesprächsrunden stattgefunden, und nachdem zunächst ein gewisses Mißtrauen überwunden werden mußte, besteht beiderseits Interesse daran, diese mehr oder minder regelmäßig fortzusetzen. Hierbei stellte bislang eine Ausarbeitung der Deutschen Arbeitsgemeinschaft für Epidemiologie zu **„Datenschutz und Epidemiologie“** die Diskussionsgrundlage dar, in dem aus der Sicht dieser Forschungsrichtung einige Standardproblembereiche zusammengestellt worden sind, bei denen die epidemiologische Forschung mit Fragen des Datenschutzes (Zweckbindung erhobener Daten sowie deren Löschung nach Beendigung des Forschungsvorhabens, Weitergabe anonymisierter Daten, Gestaltung von Einverständniserklärungen, Nutzung/Aufbewahrungsfrist von Daten amtlicher Statistiken, Nutzung von Krebsregistern für Fallkontrollstudien, länderübergreifende Studien) in der Vergangenheit konfrontiert war. Bei diesen Punkten konnte in einem gemeinsamen Arbeitspapier weitgehend auf Verfahrensweisen und bereits erprobte Konzepte abgestellt werden, die die Belange beider Sichten voll berücksichtigen können. Darüber hinaus gibt es allerdings keine **Antwort bei weiteren typischen Konfliktfällen**, die regelmäßig bei der epidemiologischen Forschung ohne Einwilligung auftauchen. Beispielsweise zählen dazu die Problemfelder

- Personalüberlassung der forschenden an die speichernde Stelle zum Zweck der Datenerfassung,

- Verhältnis von Ethik-Kommission zu sonstigen verfahrensrechtlich zu beteiligenden Institutionen (u. a. Landesbeauftragten für den Datenschutz, Landesbehörden),
- Pseudonymisierung durch Einwegverschlüsselung und

- Abwägungskriterien (öffentliches Interesse an Forschungsvorhaben versus schutzwürdige Interessen Betroffener) bei fehlender Einwilligung.

Auch insoweit ist es zu begrüßen, daß die 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 19./20. März 1998 in Wiesbaden auf meine Anregung hin beschlossen hat, die Gespräche mit der DFG fortzusetzen und dabei Probleme weiterer Forschungsrichtungen (z. B. auf dem Gebiet der Sozialwissenschaften) zu erörtern.

---

134 VCH Verlagsgesellschaft mbH, Weinheim

135 am 16. Oktober 1996, LT-Drs. 2/561: TOP 5

6.2 Archive

6.2.1 Benutzungsordnung des Brandenburgischen Landeshauptarchives

Damit in dieser längst überfälligen Angelegenheit eine Klärung herbeigeführt wird, hat das Brandenburgische Landeshauptarchiv (LHA) im Berichtszeitraum einen eigenen Entwurf für eine Verordnung über die Benutzung von Archivgut im LHA vorgelegt, in dem erfreulicherweise alle meine Hinweise[136] Berücksichtigung gefunden hatten. Er war im wesentlichen nur noch in bezug auf die Schaffung einer Befugnisnorm für das Führen einer Personendatei zu ergänzen, die von der Benutzung der Archivbestände des LHA aufgrund der in § 8 genannten Tatbestände (z. B. grobe Fahrlässigkeit im Umgang mit Archivgut, Verstöße gegen die Benutzer- und Leseordnung) zeitweise oder auf Dauer ausgeschlossen sind. Das Inkrafttreten der Benutzerordnung ist allerdings bislang daran gescheitert, daß sich das Ministerium für Wissenschaft, Forschung und Kultur (MWFK) nicht entscheiden konnte, ob - wie von mir vertreten - die Benutzerantragsformulare als Anhang Bestandteil derselben selbst werden oder nicht.

6.2.2 Verwaltungsvorschriften zum Archivgesetz in Sicht

Auch in bezug auf die Schaffung der dringend benötigten Verwaltungsvorschriften zum Brandenburgischen Archivgesetz[137] hat das LHA die Initiative ergriffen und im Berichtszeitraum einen eigenen Entwurf vorgelegt. Darin werden in analoger Reihenfolge zum Aufbau des Brandenburgischen Archivgesetzes Erläuterungen zu verschiedenen Einzelbestimmungen der §§ 3 bis 14 BbgArchivG gemacht, die sich bis auf Ziff. 7 auf traditionelles Archivgut beziehen. Hier wird bezüglich **maschinenlesbarer Daten** eingeräumt, daß deren Aufbewahrung aus Gründen der Kostenersparnis einer geeigneten Behörde desselben Rechtsträgers übertragen werden kann. Obwohl an dieser Stelle ausdrücklich auf die dabei auch weiterhin gegebene Zuständigkeit des Archivs hingewiesen wird, könnte dies zum einen nur als zeitlich begrenzte Zwischenlösung akzeptiert werden. Denn damit ist auf Dauer eine vom Gesetz vorgesehene, strikte Trennung von Verwaltung und Archiv nicht zu realisieren. Zum anderen verlangt der heutige EDV-Einsatz in der Verwaltung dringend, daß sowohl für die Anbietung und Übernahme von maschinenlesbaren Datenträgern als auch für die zu ihrer Auswertung, Sicherung und Nutzung erforderlichen Hilfsmittel und Programme eigenständige Regelungen getroffen werden.[138]

Aus datenschutzrechtlicher Sicht liegt die Bedeutung des vorliegenden Entwurfs für eine Verwaltungsvorschrift zum Archivgesetz in der **Untersetzung bzw. Erläuterung von unbestimmten Rechtsbegriffen**, die die Archivare tagtäglich bei den von ihren im Hinblick auf die Gewährung bzw. die Einschränkung oder sogar den Ausschluß der Archivgutnutzung zu treffenden ermessensfehlerfreien Entscheidungen zu interpretieren haben. Im Entwurf geschieht dies umfänglich und verständlich anhand von Fallgruppen, u. a. in bezug auf Begriffe wie personenbezogenes Archivgut, schutzwürdige Belange, öffentliches Interesse, wissenschaftliche Vorhaben sowie Person der Zeitgeschichte. Es ist weiterhin zu begrüßen, daß - entsprechend meiner Forderung - vor der Benutzung jeder Vorgang dahingehend geprüft werden muß, ob darin personenbezogene Daten enthalten sind. Ebenfalls wurde normenklar geregelt, daß, soweit die Geburts- und Todesdaten nicht aus den betreffenden Archivalien hervorgehen, diese vom Archiv zu ermitteln sind.

---

136 s. 5. Tätigkeitsbericht unter 6.4.1

137 s. 5. Tätigkeitsbericht unter 6.4.2

138 s. hierzu unter 6.2.3

Im Hinblick auf das inzwischen in Kraft getretene Akteneinsichts- und Informationszugangsgesetz (AIG)[139] enthält die Verwaltungsvorschrift - im Gegensatz zum Gesetz selbst - eine **Kollisionsklausel**. Mit Bezug auf § 10 Abs. 7 letzter Halbsatz BbgArchivG wird darin darauf abgestellt, daß Unterlagen, die im Rahmen des AIG eingesehen werden konnten, im bisherigen Maße auch während der Sperrfrist einsehbar bleiben. Ich habe in der Konsequenz dessen angeregt, vorzuschreiben, daß die anbietenden Stellen ihre Akten, für die das zutrifft, in allgemeiner Form, z. B. durch einen Stempelaufdruck mit Verweis auf § 1 AIG bzw. Art. 21 Abs. 4 Verfassung des Landes Brandenburg, keinesfalls aber personenbezogen, zu kennzeichnen haben.

Die Verwaltungsvorschrift enthält am Ende die **Empfehlung an die Gemeinden und Gemeindeverbände**, die gem. § 16 BbgArchivG nach Maßgabe des Brandenburgischen Archivgesetzes für ihren Zuständigkeitsbereich Archivangelegenheiten selbst zu regeln haben, sowie sonstigen juristischen Personen des öffentlichen Rechts (im Sinne des § 4 Abs. 4 BbgArchivG), nach den Bestimmungen der Verwaltungsvorschrift zu verfahren. Sofern die genannten Stellen dieser Aufforderung des Verordnungsgebers im vollen Umfang nachkommen, wäre damit eine wichtige Voraussetzung für eine möglichst gleichartige Handhabung archivrechtlicher Bestimmungen im Land Brandenburg sichergestellt.

6.2.3 Archive und elektronische Datenverarbeitung

Mit dem Einzug der EDV als digitalem Informationsträger in die öffentliche Verwaltung war es lediglich eine Frage der Zeit, bis wann schließlich auch die Archive von dieser Entwicklung eingeholt werden und sich ihrerseits auf die neuen Medien ein- bzw. umzustellen hätten. Das relativ junge Brandenburgische Archivgesetz trägt dieser absehbaren Entwicklung Rechnung. Gem. § 2 Abs. 5 BbgArchivG sind neben traditionellem **Archivgut** auch „maschinenlesbare sowie sonstige Informationsträger" den archivwürdigen Unterlagen und - sonst wäre deren Lesbarkeit in Frage gestellt - „die zu ihrer Auswertung, Sicherung und Nutzung erforderlichen Hilfsmittel und Programme" zuzurechnen.

[139] vom 10. März 1998, GVBl. I S. 46

Allerdings ist es damit allein nicht getan. Mit den elektronischen Datenträgern sind Archive mit einer Reihe völlig neuer und ganz unterschiedlicher Probleme konfrontiert, die alle in direkter Beziehung zum Datenträgermedium stehen, und für die es ohne ein engeres Zusammenspiel zwischen Verwaltung einerseits und den jeweils zuständigen Archiven andererseits keine allseits zufriedenstellende Lösung geben wird. Ich habe daher gegenüber dem Minister für Wissenschaft, Forschung und Kultur angeregt, unter Beteiligung seines Hauses, des LHA und anderer Stellen in einer interessierten Kommune hierzu ein Pilotprojekt durchzuführen, um dabei Erfahrungen[140] zu sammeln und die damit in Verbindung stehenden Fragen zu klären.

Nachfolgend sollen nur ausgewählte Problemfelder zur Verdeutlichung dieser Problematik für die Archive als „bleibende Gedächtnisse" angesprochen werden, die sowohl für personenbezogene Daten als auch Informationen, welcher Art auch immer, gleichermaßen zutreffen:

- Es gibt für digitale Informationen kein „originäres" Trägermedium. Bei einer **Urkunde** oder einem Aktenstück herkömmlicher Art gehören Informationen und Informationsträger untrennbar zusammen. Aufgabe der Archive ist es, diese Informationsgesamtheit zu bewahren. Eine digitale Information ist dagegen beliebig zu kopieren oder auf einen anderen Träger umzusetzen, ohne daß ein äußerer und innerer Qualitätsverlust eintritt. Sie liegt aber grundsätzlich nur in maschinenlesbarer (d. h. in elektronische Impulse umgesetzter) Form vor.

- Es gibt insoweit von keiner digitalen Information ein „Authentikum". Entwurf oder Ausfertigung sind oft nicht zu unterscheiden.

- Jede digital gespeicherte Information ist prinzipiell beliebig zu verändern, ohne daß **Spuren der Veränderung** erkennbar bleiben, es sei denn, die Information wird digital signiert. Es besteht deshalb grundsätzlich die Gefahr der unbefugten oder unbeabsichtigten Vervielfältigung, der versehentlichen Veränderung oder gar der beabsichtigten Manipulation. Für die Rechtssicherheit stellen diese technischen Möglichkeiten ein großes Risiko dar.

  Dem trug die Rechtslage bislang insofern Rechnung, als nur die Originalurkunde als gesetzliches Beweismittel gem. §§ 415 ff. ZPO[141] im Rahmen **richterlicher Unabhängigkeit und freier Beweiswürdigung** gem. § 286 ZPO, § 108 VwGO[142] bzw. § 96 FGO[143] anerkannt wird. Wie sich diesbezüglich das inzwischen in Kraft gesetzte Signaturgesetz[144] auswirken wird, bleibt abzuwarten.

Insoweit ist nach wie vor offen, welche praktischen Schlußfolgerungen daraus für die künftige Arbeit in Archiven mit maschinenlesbaren Datenträgern und deren Hilfsmitteln zu ziehen sind. Es wird dabei die Erwartungshaltung der Öffentlichkeit zu berücksichtigen sein, sich eben auch in den Archiven der Methoden und Möglichkeiten moderner Informationstechnik zu bedienen, d. h. mittels elektronischen Findbüchern unter Beachtung von §§ 10 und 11 BbgArchivG recherchieren und auf maschinenlesbare Informationsträger zugreifen zu können.

---

140 s. hierzu auch 3. Tätigkeitsbericht unter 3.5.3.1

141 Zivilprozeßordnung, i. d. Fass. vom 12. September 1950, BGBl. I S. 533 (BGBl. III/FNA 310-4)

142 Verwaltungsgerichtsordnung, i. d. Fass. vom 19. März 1991; zul geänd. durch Art. 2 MagnetschwebebahnplanungG vom 12. November 1994, BGBl. I S. 3486 (BGBl. III 340-1)

143 Finanzgeschäftsordnung, vom 6. Oktober 1965, BGBl. I S. 1477

144 Art. 3 des Informations- und Kommunikationsdienste-Gesetzes - IuKDG - vom 22. Juli 1997, BGBl. I S. 1870

6.2.4 Archivfachliche Voraussetzungen im Sinne von § 2 Abs. 8 BbgArchivG

Wie im 5. Tätigkeitsbericht[145] berichtet, konnte ein Konsens zwischen dem MWFK und meiner Behörde über das Genehmigungsverfahren zur Unterhaltung von Archiven juristischer Personen des öffentlichen Rechts erzielt werden. Auf dieser Basis kündigte mir das Ministerium an, daß die staatlichen Stellen erfaßt werden sollten, die für eine Prüfung archivfachlicher Voraussetzungen in Frage kommen. Über den Stand der Recherchen und die sich daraus ergebenden Verfahren liegen mir bislang die zugesicherten Informationen nicht vor.

6.2.5 Ausschreibung von Arbeitsstipendien durch das MWFK

Es ist dem MWFK ein Anliegen, im Rahmen seiner Möglichkeiten jungen Kunstschaffenden auf den verschiedensten Gebieten eine Förderung durch jährlich stattfindende Ausschreibungen von Stipendien zukommen zu lassen. Im vergangenen Jahr erreichte mich in Verbindung damit eine Petition, in der sich eine Bewerberin für ein Arbeitsstipendium für Schriftsteller darüber beklagte, daß im nachhinein eine Jurorin bezüglich der von ihr verfaßten Texte mit ihr Kontakt aufgenommen und die eingereichten Themen zu den ihren gemacht habe, um damit zu arbeiten und finanzielle Vorteile aus deren Veröffentlichung zu ziehen. Die Petentin verlangte eine Klärung, wer alles Zugang zu den Texten gehabt habe sowie die sofortige Löschung aller sie betreffenden Daten im Ministerium. Ich bin dieser Angelegenheit nachgegangen und habe die Eingabe zum Anlaß genommen, die generelle Handhabung des Ausschreibungs- und Vergabeverfahrens datenschutzrechtlich zu überprüfen.

Im Ergebnis konnte Einvernehmen mit dem Ministerium darüber erzielt werden, wie das Ausschreibungs- und Vergabeverfahren für Arbeitsstipendien künftig datenschutzgerecht zu gestalten ist. So wird beispielsweise nicht mehr die **Angabe der Konto-Nr.** im Antragsformular abverlangt, sondern dieses Datum gleichzeitig mit dem Zuwendungsbescheid ausschließlich an die Begünstigten abgefragt. Die Angaben mit einer sozialen Komponente (wie z. B. Anzahl der zu unterhaltenden Kinder) werden nur dann erhoben, wenn das Vergabeverfahren solche Auswahlkriterien tatsächlich berücksichtigt. Letzteres verlangt aber auch eine entsprechende Konkretisierung dieser Vergabemodalitäten im Ausschreibeverfahren selbst.

Es wurde auch eine Klärung darüber erzielt, welche Unterlagen nach Abschluß der Ausschreibungsverfahren im Ministerium archiviert werden. Das MWFK hatte zunächst die Auffassung vertreten, daß wegen haushaltsrechtlicher Belange die Bewerberunterlagen (ausgenommen Texte bzw. vergleichbare Belege) zum jederzeitigen Nachweis der ordnungsgemäßen Verwendung von Landesmittel noch geraume Zeit in der Registratur des Ministeriums aufzubewahren seien. Soweit die Argumentation die Begünstigten betrifft, ist dem zuzustimmen. Jedoch ist nach der Landeshaushaltsordnung nicht erkennbar, daß auch eine Prüfkompetenz hinsichtlich der Fragen gegeben ist, ob andere Bewerber die Voraussetzungen erfüllt hätten. Insoweit ist eine **Speicherung** von personenbezogenen Daten über diesen Personenkreis - ausgenommen die Tatsache, daß sie sich beworben haben und nicht berücksichtigt worden sind - aus datenschutzrechtlicher Sicht mangels Erforderlichkeit unzulässig. Das Ministerium wird künftig deshalb von diesem Personenkreis nur noch das Bewerberschreiben und den abschlägigen Bescheid in Kopie bis zur Abgabe dieser Vorgänge an das zuständige Archiv aufbewahren.

---

[145] s. unter 6.4.3

6.3 Hochschulen

6.3.1 Novellierung des Hochschulgesetzes

Bereits im Vorfeld der Hochschulrahmengesetz-Reform[146] hatte die Landesregierung pressewirksam angekündigt, diese zum Anlaß nehmen zu wollen, das Brandenburgische Hochschulgesetz (BbgHG)[147] grundlegend unter Berücksichtigung der notwendigen Anpassungen an das Hochschulrahmengesetz zu überarbeiten und möglichst zeitnah mit dessen Verabschiedung in Kraft zu setzen. Das MWFK bat mich im August 1997, zu einem nicht datierten Referentenentwurf aus datenschutzrechtlicher Sicht Stellung zu nehmen. In meiner Stellungnahme habe ich im wesentlichen auf folgende Aspekte hingewiesen:

Der Referentenentwurf enthält **zahlreiche Ermächtigungen** für das MWFK zum Erlaß von Rechtsverordnungen. Diese werden den hierfür maßgeblichen Vorgaben (Art. 80 GG) nicht gerecht, denn danach müssen sowohl Inhalt, Zweck und Ausmaß der erteilten Ermächtigung im Gesetz selbst bestimmt werden. Beispielsweise findet sich in § 3 Abs. 8 des Referentenentwurfs die Ermächtigung, durch Rechtsverordnung den Hochschulen weitere Aufgaben zu übertragen, wenn sie mit den in § 3 Abs. 1 genannten Aufgaben (Forschung, Lehre und Studium) zusammenhängen. In der Begründung zum Entwurf wurde diese unbestimmte Ermächtigung weder erwähnt, noch erläutert.

Begrüßt habe ich hingegen, daß in § 5 BbgHG-E mit Blick auf § 41 Abs. 2 BbgDSG vorgesehen ist, eine umfassende, bereichsspezifische Datenschutzvorschrift aufzunehmen. Diese schließt die Datenverarbeitung an den Hochschulen selbst, die Erstellung von Hochschulstatistiken und die Übermittlung personenbezogener Daten an Dritte ein. Ergänzende Regelungen sind in den §§ 69 und 70 BbgHG-E vorgesehen.

Allerdings mußte ich dem Ministerium gegenüber in Bezug auf die Einzelvorschriften einen Nachbesserungsbedarf anmahnen:

- Bei der **Erhebung personenbezogener Daten im Zusammenhang mit einem Studium** ist primär von einer Verpflichtung der Betroffenen zur Abgabe ihrer Daten auszugehen. Die Befugnis zur Verarbeitung personenbezogener Daten durch die Hochschule bleibt davon unberührt.

- Die **Aufzählung der Befugnisse**, zu welchen Zwecken Hochschulen personenbezogene Daten verarbeiten dürfen, muß abschließend sein.

- Im Gesetz müssen normenklar Vorgaben für Verarbeitung personenbezogener Daten an Hochschulen - und zwar in Bezug auf den Studienablauf, auf Befragungen (auch anonymer Art) der Studenten zu Lehrveranstaltungen, für die Nutzung von Hochschuleinrichtungen sowie Übermittlung an das Studentenwerk - verankert werden.

Der Gesetzentwurf sieht einen speziellen Paragraphen für **Veröffentlichungen** (§ 22 BbgHG-E) vor, der bislang allerdings lediglich eine Stärkung der Rechte von Mitarbeitern in bezug auf ihre Mitautorenschaft beinhaltet. Ich habe angeregt, den Paragraphen durch einen zusätzlichen Absatz hinsichtlich Veröffentlichung personenbezogener Daten in

---

146 BT-Drs. 13/8796 sowie BR-Drs. 724/97: Entwurf eines Vierten Gesetzes zur Änderung des Hochschulrahmengesetzes

147 vom 24. Juni 1991, GVBl. I S. 156; geänd. durch Ges. vom 16. Oktober 1992, GVBl. I S. 422 und durch 2. ÄndG vom 22. Mai 1996, GVBl. I S. 173

wissenschaftlichen und sonstigen Publikationen zu erweitern. Darin wäre ausdrücklich festzuschreiben, daß die Veröffentlichung personenbezogener Daten von Betroffenen nur mit deren schriftlicher Zustimmung erfolgen darf, ansonsten ist dies nur ausreichend anonymisiert möglich.

Das Ministerium hat mir inzwischen mitgeteilt, daß der „vorgesehene § 5 BbgHG-E die Datenströme an den Hochschulen und die schutzwürdigen Interessen der Hochschulmitglieder und -angehörigen hinreichend erfasse". Als Begründung führt es lapidar an, daß die Vorschriften im wesentlichen § 135 Sächsisches Hochschulgesetz vom 04. August 1993 entsprächen. Dies trifft zwar zu, berücksichtigt u. a. aber nicht die Unterschiede in den Landesdatenschutz- und Hochschulgesetzen beider Länder und ist insofern nicht hinnehmbar.

6.3.2 Meldeverfahren für die Krankenversicherung der Studenten

Eine Fachhochschule hat mich bereits im vergangenen Berichtsjahr auf die gemeinsame Verlautbarung der Spitzenverbände der Krankenkassen (KKs) und der Hochschuldirektorenkonferenz (HRK) vom 12. April 1996 angesprochen. Nach § 5 Studentenkrankenversicherungs-Meldeverordnung (SKV-MV)[148] können KKs und HRK vereinbaren, das Meldeverfahren für die Krankenversicherung zwischen Hochschule und Krankenversicherung maschinell abzuwickeln. Dazu hatten sie sich im Vorgriff auf ein maschinelles Verfahren in der genannten Vereinbarung geeinigt, daß über die in den Anlagen zur SKV-MV aufgeführten Daten hinaus, die **Matrikelnummer** der Studierenden und die Betriebsnummer der jeweiligen Hochschule als weiteres Identifizierungsmerkmal übermittelt werden sollte. Die anfragende Hochschule trug mir dazu vor, daß die Matrikelnummer verschlüsselt Auskunft über das Jahr der Immatrikulation und den gewählten Fachbereich gäbe. Sie fände im gesamten Hochschulbereich als internes Ordnungsmerkmal Verwendung[149] und zwar bis hin zu hausinternen Veröffentlichungen, z. B. Prüfungsergebnissen. Insofern würden die Betroffenen in der Weitergabe ihrer Matrikelnummer eine Verletzung des Datengeheimnis sehen.

Da die SKV-MV in die Zuständigkeit des Bundes als Verordnungsgeber fällt, hatte ich mich diesbezüglich an den Bundesbeauftragten für den Datenschutz mit der Bitte gewandt, die Angelegenheit zu klären. Seine Antwort unter Einbeziehung des BMG besagt, daß die Matrikelnummer nicht zwingend übermittelt werden müsse. Der **Identifizierungsdatensatz beim Meldeverfahren** für die Krankenversicherung der Studenten sehe aufgrund der geäußerten Bedenken nunmehr vor, daß das Aktenzeichen der Hochschule, unter dem der Student geführt wird, hierbei anzugeben sei. Als Aktenzeichen sei ein Merkmal zu verwenden, anhand dessen die Hochschule die Studierenden eindeutig identifizieren könne.

Das MWFK habe ich im Rahmen seiner Rechtsaufsicht gegenüber den Hoch- und Fachhochschulen des Landes Brandenburg gebeten, diese darüber in geeigneter Weise in Kenntnis zu setzen. Es hat dies mittels Rundschreiben getan.

---

148 vom 27. März 1996, BGBl. I S. 568

149 s. auch 4. Tätigkeitsbericht unter 6.2.3

6.3.3 Datenverarbeitende Stelle bei Anfertigung von Diplomarbeiten

Im Berichtszeitraum haben sich vielfach Studenten von Hochschulen des Landes Brandenburg an meine Behörde gewandt, und um Beratung zu datenschutzrechtlichen Fragen in Verbindung mit ihrer Diplomarbeit gebeten. Im Rahmen der Möglichkeiten der Behörde ist diesen Bitten in der Regel entsprochen worden. Dabei hat sich mehrfach ein grundsätzliches Mißverständnis herausgestellt. Im eigenen Interesse bestand zwar großes Interesse, in den Unterlagen (Informationsblätter, Fragebogen) zu vermerken, daß die Vorgehensweisen mit dem Brandenburgischen Datenschutzbeauftragten abgesprochen wären. Sie fanden es allerdings abwegig, sich seiner Kontrolle zu unterwerfen, da es sich um eine Privatangelegenheit handele.

Hier ist davon auszugehen, daß die Universität bzw. der Lehrstuhl/das Institut gem. § 2 Abs. 1 i.V.m. §§ 3 Abs. 4 und 10 BbgDSG eine öffentliche Stelle des Landes Brandenburg ist. Damit ist sie auch in bezug auf die anzufertigenden Diplomarbeiten **datenverarbeitende Stelle** und hat alle technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, die Ausführungen der Vorschriften des Brandenburgischen Datenschutzgesetzes zu gewährleisten und unterliegt insoweit der Kontrollkompetenz des Landesbeauftragten für den Datenschutz gem. § 23 Abs. 1 BbgDSG. Ich habe in den mir bekannt gewordenen Fällen regelmäßig vorsorglich die Institutsleiter darauf hingewiesen.

6.3.4 Einführung von Chipkarten an Hochschulen

Auf der gemeinsamen Sitzung der Rektoren und Kanzler der Hochschulen mit dem MWFK am 6. Februar 1998 wurde nunmehr festgelegt, daß an allen Hochschulen des Landes Chipkartensysteme eingeführt werden sollen. Dazu wurde an der Brandenburgischen Technischen Universität Cottbus ein Pilotprojekt initiiert. In der ersten Stufe des Projektes soll mit Hilfe von Chipkarten u. a. die Bibliotheks- und Mensanutzung ermöglicht werden. Weiterhin soll auch die Immatrikulation durch Chipkarten vereinfacht werden. In einer zweiten Stufe ist dann beabsichtigt, die Chipkarte u. a. auch im ÖPNV nutzen zu können.

Im Vorfeld hatte ich bereits die Einführung von Chipkarten an Hochschulen gegenüber dem MWFK mehrfach angesprochen. Dies war dort lange kein Thema, und so war ich überrascht, als Ende 1997 der Minister mich persönlich von diesem Projekt in Kenntnis setzte, mit der Zusage, daß meine Behörde hierbei frühzeitig einbezogen werden würde. Aus datenschutzrechtlicher Sicht sind an das Vorhaben u. a. folgende Forderungen zu stellen:

- Es gibt mit Ausnahme der Krankenversicherungskarte (§ 291 SGB V[150]) noch keine weiteren gesetzlichen Vorschriften zu Chipkartensystemen. Es sind deshalb die Vorschriften des Brandenburgischen Datenschutzgesetzes anzuwenden.

- Die Verarbeitung personenbezogener Daten ist gem. § 4 BbgDSG nur zulässig, wenn eine entsprechende Rechtsvorschrift vorhanden ist oder der Betroffene schriftlich eingewilligt hat. Die obligatorische Einführung einer Chipkarte bedarf deshalb einer ausdrücklichen gesetzlichen Regelung. Da diese derzeit weder im Brandenburgischen Hochschulgesetz noch in anderen Gesetzen existieren, kann die Einführung von Chipkarten nur freiwillig erfolgen. Ein wesentliches Merkmal der Freiwilligkeit ist eine für die Zukunft **wirksame Widerrufbarkeit**.
- Die datenverarbeitende Stelle hat den Umfang der personenbezogenen Datenverarbeitung entsprechend dem allgemeinen **Erforderlichkeitsprinzip** weitestgehend zu reduzieren.

[150] vom 20. Dezember 1988, BGBl. I S. 2477; zul geänd. durch Ges. vom 17. Dezember 1997, BGBl. I S. 3108

- Die **datenverarbeitende Stelle** gem. § 3 Abs. 4 Nr. 1 BbgDSG bleibt weiterhin die Hochschule, das Studentenwerk usw. Diese öffentlichen Stellen müssen daher auch die in § 10 BbgDSG festgelegten technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten treffen.

- Der Studierende muß jederzeit die Möglichkeit haben, sich über die auf der Chipkarte gespeicherten personenbezogenen Daten zu informieren (**Auskunftsanspruch** gem. § 18 BbgDSG).

- Dem Studierenden dürfen keine Nachteile entstehen, wenn er sich aufgrund der **Freiwilligkeit** weiterhin für konventionelle Verfahren entscheidet. Andererseits dürfen natürlich bei der Nutzung von Chipkarten z. B. keine Rabatte eingeräumt werden. Dadurch würde eine Benachteiligung der Nutzer konventioneller Verfahren eintreten und es würde sich hierbei um keine „echte" Freiwilligkeit handeln. Der Betroffene wäre damit einem faktischen Zwang ausgesetzt.

- Die Studierenden sind vor der Einführung eines Chipkartensystems ausreichend zu informieren (**Transparenzgebot**).

- Werden mit der Chipkarte Dienstleistungen angeboten (z. B. Bezahlen im ÖPNV), die auch anonym erbracht werden können, so ist anstelle der personenbezogenen eine **anonyme Form der Nutzung** vorzusehen.

- Die verschiedenen Anwendungen auf der Chipkarte müssen untereinander abgeschottet werden, so daß nur die jeweils Berechtigten die Daten auf der Chipkarte lesen bzw. ändern können (**restriktive Rechtevergabe**).

- Sicherheitskopien dürfen nicht zentral gespeichert, sondern müssen bei den jeweils datenverarbeitenden Stellen vorgehalten werden.

- Vor der Einführung von Chipkartensystemen hat die datenverarbeitende Stelle ein **Pflichtenheft** und eines schlüssiges **Sicherheitskonzep**t zu erstellen.

An der Brandenburgischen Technischen Universität Cottbus sollen i.V.m. der Einführung von Chipkarten an Hochschulen des Landes in regelmäßigen Abständen Workshops durchgeführt werden, bei denen u. a. Vertreter aller Hochschulen, des MWFK und einer Behörde die inhaltliche, organisatorische und einheitliche Vorgehensweise bei der Einführung der Chipkartensysteme im Land Brandenburg abstimmen. Dieses Vorgehen ist zu begrüßen und könnte Schule machen für vergleichbare Projekte im Lande.

6.3.5 Telefon- und Vorlesungsverzeichnis im Internet

Die von der Landesregierung hierzu in ihrer Stellungnahme[151] zu meinem 5. Tätigkeitsbericht[152] vertretene Meinung, daß ein Einstellen von Telefon- und Vorlesungsverzeichnissen im Internet durch § 29 Abs. 1 BbgDSG abgedeckt sei, kann ich nicht nachvollziehen. Auf der einen Seite ist das Telefonverzeichnis einer Behörde nur für den Dienstgebrauch bestimmt, auf der anderen Seite wird von der Landesregierung die Meinung vertreten, daß personenbezogene Daten der Beschäftigten im Internet weltweit zur Verfügung gestellt werden sollen. Dies ist unverhältnismäßig und widerspricht dem datenschutzrechtlichen Erforderlichkeitsgrundsatz. Wozu soll beispielsweise ein Plantagenbesitzer aus Florida auf die personenbezogenen Daten der Beschäftigten eines Sozialamtes im Land Brandenburg zugreifen können? Dem Transparenzgebot wird meiner Meinung nach auch Genüge getan, wenn z. B. das Organigramm einer Behörde[153] ohne entsprechenden Personenbezug im Internet veröffentlicht wird.

Wird von einer öffentlichen Einrichtung beabsichtigt, auch personenbezogene Daten der Beschäftigten ins Internet einzustellen, so ist dies datenschutzrechtlich nur mit der schriftlichen Einwilligung der Beschäftigten zulässig. Die Beschäftigten sind vorher über die mit dem Einstellen ihrer personenbezogenen Daten in das Internet verbundenen Risiken aufzuklären. Ebenfalls als unabdingbar betrachte ich ein jederzeitiges Widerrufsrecht der Betroffenen.

Im Gegensatz zu den Behauptungen der Landesregierung wird diese Meinung auch von den anderen Datenschutzbeauftragten geteilt. So wurde selbstverständlich auch das in der Stellungnahme der Landesregierung erwähnte Organigramm des Berliner Datenschutzbeauftragten erst nach schriftlicher Einwilligung der Beschäftigten in das Internet eingestellt.

Zur baldigen Klärung der Angelegenheit hatte ich mich deshalb erneut an das MWFK gewandt; bislang liegt mir hierzu trotz mehrfachen Erinnerns noch keine Rückantwort vor.

7 Arbeit, Soziales, Gesundheit und Frauen

7.1 Soziales

7.1.1 Gesetze und Verordnungen

7.1.1.1 Sozialhilfedatenabgleichsverordnung gem. § 117 Bundessozialhilfegesetz

Ausweitungen der Übermittlungsbefugnisse und neue Abgleichsmöglichkeiten bei Sozialdaten waren ein bundesweites Thema im Berichtszeitraum.

---

151 LT-Drs. 2/4768 vom 15. Dezember 1997

152 s. unter 6.2

153 s. hierzu Organigramm meiner Behörde: http://www.brandenburg.de/land/lfdbbg/organigr/organigr.htm

Zum Beispiel wurde zur Umsetzung des § 117 Abs. 1 und 2 Bundessozialhilfegesetz (BSHG)[154] die Sozialhilfedatenabgleichsverordnung (SozhiDAV)[155] erlassen. Bis dahin waren nach § 117 Abs. 3 BSHG aufgrund dieser Vorschrift nur Datenabgleiche zu im einzelnen festgelegten Sozialdaten mit kommunalen Stellen möglich gewesen. Nunmehr kann mit verschiedenen Sozialleistungsträgern der jeweilige Leistungsumfang (Zeitraum und Höhe) abgeglichen werden.

Außerdem erarbeitete eine Arbeitsgruppe der Konferenz der Arbeits- und Sozialminister (ASMK) ein umfangreiches Papier mit **Vorschlägen für weitere Übermittlungsmöglichkeiten zur Bekämpfung von Leistungsmißbrauch**. Dabei wurde z. T. den Grundsätzen der Verhältnismäßigkeit und Erforderlichkeit nicht hinreichend Rechnung getragen. Deshalb habe ich mich mit den Kollegen in Bund und Ländern darauf verständigt, diesen Vorschlägen im Vorfeld von Gesetzgebungsvorhaben umgehend durch eine **Entschließung**[156] zu begegnen. Der kurze Zeit nach unserer Entschließung ergangene Beschluß der ASMK äußerte die Bitte an die Bundesregierung, die erforderlichen Schritte zur Realisierung eines verbesserten Datenaustausches in die Wege zu leiten und „dabei unter Einschluß des Gesprächsangebotes der Datenschutzbeauftragten den Bericht der Arbeitsgruppe und die Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 23./24. Oktober 1997 in die Prüfung einzubeziehen".

Eine der Forderungen aus dieser Entschließung möchte ich besonders hervorheben, nämlich die Empfehlung, zugleich mit einem Abgleichsverfahren ein Instrumentarium zu dessen **Erfolgskontrolle** einzuführen, um die Notwendigkeit der gesetzlich vorgesehenen Maßnahmen zu überprüfen. Dieser Gedanke wurde bereits bei der Umsetzung der Sozialhilfedatenabgleichsverordnung realisiert, indem bei Mustersozialämtern eine wissenschaftliche Begleitung zu diesem Zweck stattfinden soll. Ich halte diesen Gesichtspunkt für wesentlich, da mir in der Praxis immer wieder Fälle begegneten, in denen noch nicht einmal von den bereits vorhandenen Möglichkeiten zur Mißbrauchsbekämpfung Gebrauch gemacht wurde[157] und deshalb kritisch hinterfragt werden sollte, welche zusätzlichen Eingriffe in das Recht auf informationelle Selbstbestimmung tatsächlich erforderlich sind.

7.1.2 Aktuelle Fälle

7.1.2.1 Leistungssachbearbeitung von Sozialversicherungsträgern für eigene Mitarbeiter

Die Anfrage eines Sozialversicherungsträgers, was ich bei einer praktischen Umsetzung der Leistungssachbearbeitung für dessen eigene Mitarbeiter für wesentlich halte, habe ich wie folgt beantwortet:

§ 35 Abs. 1 Erstes Buch Sozialgesetzbuch (SGB I)[158] fordert, daß Sozialdaten auch innerhalb eines Leistungsträgers nur den Befugten zugänglich sein dürfen und bestimmt, daß Sozialdaten der Beschäftigten eines Leistungsträgers und ihrer Angehörigen Personen, die Personalentscheidungen treffen oder daran mitwirken können, weder zugänglich sein noch von Zugriffsberechtigten an diese weitergegeben werden dürfen. Als datenschutzgerecht habe ich eine Verfahrensweise angesehen, bei der folgende Kriterien erfüllt sind:

---

154 i. d. Fass. vom 23. März 1994, BGBl. I S. 646, ber. S. 2975; zul. geänd. durch SGB III-ÄndG vom 16. Dezember 1997, BGBl. I S. 2970

155 vom 21. Januar 1998, BGBl. I S. 103

156 s. Anlage 2

157 s. unter 7.1.2.3

158 vom 11. Dezember 1975, BGBl. S. 3015; zul. geänd. durch SGB III-ÄndG vom 16. Dezember 1997, BGBl. I S. 2970

- Es werden so wenig wie möglich Sachbearbeiter einbezogen.

- Deren Zuständigkeiten sind exakt festgelegt.

- Die Auswahl der zuständigen Sachbearbeiter konnte von den Betroffenen mitgestaltet werden.

- Die zuständigen Sachbearbeiter dürfen nicht zu dem Kreis der Personen zählen, die Personalentscheidungen treffen oder daran mitwirken können.

- Die betroffenen Mitarbeiter sollten angewiesen werden, Bescheinigungen, Anträge u. ä. direkt an die zuständigen Leistungssachbearbeiter zu geben. Post, die zu Händen dieser Sachbearbeiter adressiert ist, ist intern ungeöffnet an diese weiterzuleiten.

Auch durch technisch-organisatorische Mittel muß den besonderen Umständen Rechnung getragen werden. Hierzu ist insbesondere folgendes zu fordern:

- eine gesonderte Dokumentation und Archivierung,

- eine räumliche Abschottung der zuständigen Mitarbeiter,

- eine entsprechende Regelung der Zugriffsberechtigung und

- eine Zugriffssicherung durch spezielle Paßwortvergabe.

Insgesamt sollten die oben aufgeführten Verfahrensschritte in einer Dienstanweisung festgeschrieben werden.

Sofern es wegen der verschiedenartigen Aufgaben und unterschiedlichen fachlichen Qualifikationen nicht möglich sein sollte, die Betreuung der oben angesprochenen Fälle allein in einer einzigen Hand durchzuführen, ist dies nicht zu beanstanden. Denn bereits § 1 Abs. 4 Sozialversicherungsrechnungsverordnung (SVRV)[159] läßt grundsätzlich nicht zu, daß Anordnungs- und Feststellungsbefugte an der Abwicklung der Kassengeschäfte zu beteiligen sind. Demgegenüber ist es wiederum zulässig, die sachliche und rechnerische Feststellung durch dieselbe Person treffen zu lassen. Letzteres wäre die datenschutzrechtlich beste Lösung. Es könnte jedoch auch vorgesehen werden, dies auf zwei für diese spezielle Aufgabe ausgewählte Leistungssachbearbeiter zu verteilen, wenn aus gewichtigen Gründen die idealere Lösung nicht umgesetzt werden kann.

Die Anfrage des einen Sozialversicherungsträgers war für mich zugleich Anlaß, mich bei weiteren Sozialversicherungsträgern im Land darüber zu informieren, wie diese mit der angesprochenen Problematik umgehen. Dabei mußte ich feststellen, daß zumindest eine der angefragten Stellen schon den unmittelbar dem Gesetz zu entnehmenden Forderungen des § 35 Abs. 1 Satz 3 SGB I nicht gerecht wurde, weil auch leitende Mitarbeiter an der Sachbearbeitung beteiligt waren. Diese Gestaltung wurde auf meinen Hinweis hin umgehend geändert.

7.1.2.2 Umgang mit Hinweisen auf Fahruntauglichkeit von Versicherten bei Sozialversicherungsträgern

[159] vom 3. August 1998, BGBl. I S. 809

Ein Petent trug vor, seine Krankenversicherung habe aufgrund eines in der Vergangenheit liegenden Vorfalls, aus dem aber die hinzugerufene Polizei keinerlei Konsequenzen gezogen hatte, Bedenken wegen seiner Fahrtauglichkeit gehabt. Sie habe diese dann Monate nach dem Zeitpunkt, zu dem sie anläßlich einer Gerichtsverhandlung in einem ganz anderen Zusammenhang Kenntnis von dem Vorfall erhielt, der Polizei mitgeteilt. Die Polizei habe daraufhin die Fahrerlaubnisbehörde informiert.

In diesem Fall mußte ich feststellen, daß die Krankenkasse zum Teil nicht erforderliche Daten zunächst an eine unzuständige Stelle übermittelt hatte, ohne daß wenigstens die Voraussetzungen des § 34 Strafgesetzbuch (StGB)[160] tatsächlich erfüllt waren. Dies war unabhängig davon festzustellen, wie man die schwierige Frage beantwortet, ob der **Notstandsparagraph** auch im eigentlich abschließend geregelten Sozialgesetzbuch, das derzeit noch keine entsprechende Vorschrift vorsieht, angewendet werden kann.

Ich habe in diesem Fall von einer Beanstandung nur abgesehen, weil die Krankenkasse mir zugesichert hat, daß sie im Rahmen der Schulungsmaßnahmen ihre Mitarbeiter künftig auf die Problematik, ob § 34 StGB überhaupt anwendbar ist und wenn ja, welche Voraussetzungen dann vorliegen müssen, hinweisen wird. Wenn in Zukunft eine solche Übermittlung angedacht wird, ist nach den neuen internen Vorgaben immer auch der Datenschutzbeauftragte dieser Stelle einzubinden. Im übrigen habe ich berücksichtigt, daß der Gesetzgeber seit einiger Zeit darum bemüht ist, eine dem § 34 StGB vergleichbare Regelung in das Zehnte Buch Sozialgesetzbuch (SGB X)[161] einzufügen.

Ein anderer Sozialversicherungsträger war dagegen in einem ähnlich gelagerten Fall vorbildlich vorgegangen. Hier suchte der behördliche Datenschutzbeauftragten rechtzeitig meinen Rat. Im Laufe des Beratungsgesprächs führte er aus, daß dem Mitarbeiter noch nicht einmal sicher bekannt war, ob der betroffene Versicherte von seiner Fahrerlaubnis überhaupt noch Gebrauch macht. Dahingehende **Ermittlungen** hielt der behördliche Datenschutzbeauftragte jedoch ebenso wie ich **nicht** für eine **Aufgabe des Sozialversicherungsträgers**. Er mußte zugeben, daß bisher ebenfalls nicht versucht worden war, die möglicherweise von dem Versicherten ausgehende Gefahr mit **milderen Mitteln** abzuwenden und beispielsweise zunächst ein persönliches Gespräch mit diesem zu suchen, um auf ihn einzuwirken, von seiner Fahrerlaubnis keinen Gebrauch zu machen bzw. sie zurückzugeben. In diesem Fall kam es nicht mehr zu einer - unzulässigen - Sozialdatenoffenbarung.

7.1.2.3 Übermittlung von Sozialdaten an die Kriminalpolizei

[160] vom 15. Mai 1871, RGBl. S 127, i. d. Fass. vom 10. März 1987, BGBl. I S. 945, ber. S. 1160; zul. geänd. durch TPG vom 17. Dezember 1997, BGBl. I S. 3108

[161] vom 18. August 1980, BGBl. I S. 1469, ber. S. 2218; zul. geänd. durch SGB III-ÄndG vom 16. Dezember 1997, BGBl. I S. 2970

Im Berichtszeitraum erreichten mich verstärkt Anfragen von Krankenkassen, Sozialämtern und ähnlichen Stellen[162] zur Frage der Übermittlung von Sozialdaten an die Kriminalpolizei. Hierzu hatte ich mich schon in den vergangenen Tätigkeitsberichten[163] geäußert.

Diesmal ging es um folgende Fälle:

- Eine fast volljährige Person, die sich in laufender ärztlicher Behandlung befand, wurde seit Monaten vermißt. Vieles sprach dafür, daß sie Opfer eines Kapitalverbrechens geworden war, es konnte jedoch auch nicht ausgeschlossen werden, daß sie freiwillig neue Lebensumstände gesucht hatte. Zur Aufklärung der Angelegenheit wandte sich die Kriminalpolizei an eine Stelle i. S. d. § 35 SGB I mit der Bitte um Mitteilung, wo sich die Vermißte in den letzten drei Monaten aufgehalten habe.

  Eine Übermittlung nach § 68 SGB X, der lediglich eine Mitteilung über die derzeitige Anschrift des Betroffenen zur Erfüllung der Aufgaben der Strafermittlungsbehörden zuläßt, schied damit aus. Die Kriminalpolizei, die auch **keine richterliche Anordnung nach § 73 Abs. 3 SGB X** vorzuweisen hatte, begehrte aufgrund einer Einwilligungserklärung eines Elternteils Auskunft über die Sozialdaten. Bei **fast Volljährigen** ist neben einer Einwilligung der gesetzlichen Vertreter in der Regel aber auch eine Erklärung des Betroffenen selbst einzuholen. Problematisch war hier nun, daß dies nicht möglich war. Es war aber auch nicht auszuschließen, daß die Entscheidung der vermißten Person dahin lauten würde, daß sie gerade neue Lebensumstände suche und nicht wolle, daß diese bekannt würden. Der Kriminalpolizei habe ich deshalb geraten, sich um eine richterliche Anordnung nach § 73 SGB X zu bemühen.

- In einem anderen Fall wandte sich die Kriminalpolizei wegen anderweitig bekannt gewordener Abrechnungsbetrügereien an eine Krankenkasse mit der Bitte, ihr zu Abrechnungszwecken von bestimmten Ärzten übersandte patientenbezogene Daten zu übermitteln. Die in der Anfrage genannte Übermittlungsvorschrift - § 69 Abs. 1 Nr. 1 SGB X - erschien der Krankenkasse problematisch.

---

[162] vgl. § 35 Abs. 1 SGB I i. V. m. §§ 18 ff. SGB I vom 11. Dezember 1975, BGBl. I S. 3015; zul. geänd. durch AFRG vom 24. März 1997, BGBl. I S. 594

[163] s. 2. Tätigkeitsbericht unter 7.3.4 und 3. Tätigkeitsbericht unter 7.1.1.3 sowie 7.1.2.3

Ich habe darauf hingewiesen, daß z. B. nach § 12 SGB V[164] u. a. die Krankenkassen für die Wirtschaftlichkeit der Leistungserbringung verantwortlich gemacht werden. Den Hinweisen auf betrügerische Abrechnungen bestimmter Ärzte sollte die Krankenkasse daher im eigenen Hause nachgehen, und falls sie dabei feststellen müßte, daß auch sie betrogen worden ist, könnte sie zur Erfüllung ihrer Aufgaben nach § 69 Abs. 1 Nr. 1 SGB X die für eine Strafverfolgung erforderlichen Sozialdaten an die Kriminalpolizei übermitteln. Zwar schützt § 76 Abs. 1 SGB X Daten, die den Krankenkassen von Ärzten mitgeteilt wurden, besonders und läßt ihre Offenbarung nur unter den Voraussetzungen zu, unter denen der Arzt selbst offenbarungsbefugt wäre, doch steht auch diese Vorschrift der Übermittlung an die Kriminalpolizei nicht zwingend entgegen. Ein Arzt dürfte nach der Berufsordnung nämlich **zum Schutz eines höheren Rechtsguts**, welches das Interesse der Versichertengemeinschaft an ordnungsgemäßen Abrechnungsverhalten im Einzelfall durchaus darstellen könnte, **Patientendaten offenbaren**. Hinzu kommt, daß personenbezogene ärztliche Unterlagen keinem absoluten Beschlagnahmeverbot unterliegen. Ausnahmsweise können solche Unterlagen nämlich beim **beschuldigten Arzt** zu Beweiszwecken sichergestellt werden.

Eine Befugnis zur Offenbarung von Sozialdaten an die Kriminalpolizei kann in solchen Fällen also vorhanden sein; ob auch eine Übermittlungspflicht besteht, ist nach den für die Amtshilfe geltenden Grundsätzen zu beurteilen.

- Ganz ähnlich wie im vorangegangenen Fall war die Anfrage eines Sozialamtes gelagert, das aufgrund gefälschter Unterlagen ein Darlehen ausgezahlt hatte, aber trotzdem Bedenken gegen die Übermittlung von Sozialdaten an die diesen Fall bearbeitende Kriminalpolizei hatte und ausdrücklich erklärte, selbst solche Vorfälle nicht anzuzeigen. Auch hier habe ich auf die Übermittlungsbefugnis nach § 69 Abs. 1 Nr. 1 SGB X aufmerksam gemacht.

Im übrigen möchte ich darauf hinweisen, daß ständig neue Regelungen gegen den Sozialhilfemißbrauch[165] überhaupt nicht erforderlich wären, wenn die Behörden die derzeit schon bestehenden Möglichkeiten auch tatsächlich ausschöpfen würden.

7.1.2.4 Arzneimittel-Budget-Informationen des Apothekenrechenzentrums für die Kassenärztliche Vereinigung Brandenburgs

Durch Datenschutzbeauftragte anderer Bundesländer war ich darauf aufmerksam gemacht worden, daß die Ärzte von den Kassenärztlichen Vereinigungen mittels arztbezogener Abrechnungsdaten, die diese von den Apothekenrechenzentren erhalten, über ihr jeweiliges Arzneimittelbudget informiert werden.

Eine Anfrage bei der Kassenärztlichen Vereinigung Brandenburgs (KVBB) ergab, daß auch hier im Land eine solche Information der Ärzteschaft durchgeführt wurde. Die mir hierzu erteilten Auskünfte waren anfänglich recht oberflächlich, bis sich die beteiligten Stellen dazu entschlossen, dem Verfahren einen schriftlichen Vertrag zugrunde zu legen. Dessen Entwurf wurde mir zur datenschutzrechtlichen Beurteilung vorgelegt. Zunächst bestanden zwischen dem Vertragstext und den Ausführungen in seiner Anlage gewisse Differenzen. So war nicht eindeutig, ob der Datensatz den Abrechnungsmonat oder das Abrechnungsquartal enthalten sollte und ob er einzelrezeptbezogen und damit letztlich patientenbezogen sein sollte oder nicht.

Für mich war entscheidend, daß bei der geplanten Übermittlung im wesentlichen **§ 296 Abs. 3 SGB V**, der eine

---

164 vom 20. Dezember 1988, BGBl. I S. 2477; zul. geänd. durch Ges. vom 17. Dezember 1997, BGBl. I S. 3108

165 s. unter 7.1.1.1

quartalsweise, nicht patientenbezogene Übermittlung vorsieht, **als Maßstab** diente. In der genannten Vorschrift sind diejenigen Daten aufgeführt, die die Krankenkassen u. a. von den Apotheken(rechenzentren) erhalten und an die KVBB weiter übermitteln dürfen. Diese gesetzlich vorgesehene Verfahrensweise funktioniert nach Angaben der KVBB derzeit noch nicht, so daß man dort daran interessiert war, einen parallelen Weg zu finden, um die Informationen zu erhalten, die für die arztbezogene Wirtschaftlichkeitsprüfung gedacht sind. Konkret sollen die Daten im Vorfeld einer solchen Prüfung dazu verwendet werden, Ärzten ihr Verschreibungsverhalten vor Augen zu führen und sie so darin zu unterstützen, das Wirtschaftlichkeitsgebot zu wahren. Wesentlich war für mich daher neben einer Orientierung an § 296 Abs. 3 SGB V auch, daß die Ärzte über das Vorhaben so umfassend wie nur möglich aufgeklärt werden. Diesen beiden Anforderungen hat die KVBB Rechnung getragen.

7.1.2.5 Betreiben eines Krankenkassendruckzentrums durch eine Firma

Im Sommer 1997 informierte mich eine Firma darüber, daß sie zukünftig das Druckzentrum einer Krankenkasse betreiben werde. Die Firma soll neben den Geräten das Wartungs- und Bedienungspersonal zur Verfügung stellen. Die zu behandelnden Daten werden von der Krankenkasse per Leitung angeliefert und vom Druckzentrum in Papierform an diese zurückgegeben. Das Druckerbedienungspersonal ist dabei beispielsweise für das Einlegen des Papiers und für das Unterbringen der mit Sozialdaten bedruckten Schreiben in Behälter, die für den Transport verschlossen werden, zuständig.

Die Tätigkeit der Firma habe ich als Datenverarbeitung im Auftrag nach § 80 SGB X eingestuft. Das Ministerium für Arbeit, Soziales, Gesundheit und Frauen (MASGF), das als zuständige Aufsichtsbehörde über die Planungen informiert war und deren zulässige Ausgestaltung prüfte, stellte zunächst Überlegungen an, ob anstelle einer Datenverarbeitung im Auftrag eine andere Rechtskonstruktion vorliegen könnte. Ihm erschien die Bearbeitung durch die Firma datenschutzrechtlich nicht sehr relevant, da die Schnittstellen sich in der Hand der Krankenkasse befinden sollten.

Auch wenn man für ein rein technisch bedingtes Umspeichern, das die notwendige Voraussetzung für einen Druckvorgang ist, die Überlegungen des Ministeriums teilen kann, stellt das Ausdrucken der Schreiben eine Datenverarbeitung dar. Die datenschutzrechtliche Relevanz ergibt sich dabei aus dem Umstand, daß der Firma die Kenntnisnahme von Sozialdaten ermöglicht wird. Dieser Auffassung hat sich das Ministerium letztlich angeschlossen. Sie wird vom Ministerium des Innern (MI), das nach § 80 Abs. 6 Satz 4 SGB X für die datenschutzrechtliche Kontrolle bei dem nicht-öffentlichen Auftragnehmer zuständig ist, ebenfalls geteilt.

Darüber hinaus wurde zwischen dem MASGF, dem MI und meiner Behörde klargestellt, daß neben dem Ministerium des Innern nach § 80 Abs. 6 Satz 4 SGB X i. V. m. § 23 Abs. 1 und § 11 Abs. 3 Satz 1 BbgDSG auch **meine Behörde für die Kontrolle eines nicht-öffentlichen Auftragnehmers eines Sozialleistungsträgers zuständig** sein kann. Voraussetzung dafür ist, daß dieser sich nach den landesrechtlichen Regelungen meiner Kontrolle unterworfen hat, die in Abstimmung mit dem MI erfolgen wird. Dem Interesse an einer einheitlichen und wirksamen Sozialdatenschutzkontrolle dürfte dadurch, daß meine Behörde nun nicht mehr nur für den Auftraggeber als öffentliche Stelle, sondern auch für dessen im Land Brandenburg tätigen Auftragnehmer zuständig sein kann, wesentlich besser Genüge getan werden als bisher. Im konkreten Fall wird dem nunmehr durch Ergänzung des Vertrages mit dem Auftragsnehmer entsprochen werden.

7.1.2.6 Auskunftsersuchen einer Krankenkasse an ein Gesundheitsamt wegen Massenerkrankungen

Ein Gesundheitsamt bat mich zu einem Auskunftsersuchen einer Krankenkasse um Rat. In dem betreffenden Kreis war bei etwa 200 Personen dieselbe Erkrankung diagnostiziert worden. Das Gesundheitsamt führte über diese Erkrankungsfälle

eine Liste. Genau an dieser Liste, die nicht nur ihre Mitglieder, sondern auch die anderer Krankenkassen enthielt, war die Krankenkasse interessiert. Sie meldete sich deshalb telefonisch beim Gesundheitsamt, bezeichnete ihr Anliegen als dringlich und forderte eine Übersendung der Liste noch am selben Tag.
Ich teilte dem Gesundheitsamt mit, daß die Krankenkassen, sofern ihnen eine ärztliche Arbeitsunfähigkeitsbescheinigungen zugeleitet würden, zugleich auch über die Diagnose informiert würden. Bezüglich dieser Fälle sei daher nicht ersichtlich, wozu dieses Datum nochmals erhoben werden sollte. Überhaupt dürften die Krankenkassen nur zu bestimmten, in § 284 Abs. 1 SGB V genannten Zwecken Daten erheben. Die Voraussetzungen für die Datenerhebungen müßten in jedem einzelnen Fall gesondert geprüft werden. Für die Fälle, die nicht bei der betreffenden Krankenkasse versichert seien, fehle es bereits an einer **Erforderlichkeit** für die Datenerhebung. Im übrigen hatte sich die Krankenkasse nicht näher erklärt. Ich riet dem Gesundheitsamt daher, von der Krankenkasse eine Begründung ihres Auskunftsersuchens und insbesondere eine Mitteilung der Rechtsgrundlage für die Datenerhebung bezüglich ihrer Mitglieder zu fordern.

Das Ergebnis dieser Rückfrage des Gesundheitsamtes war, daß die Krankenkasse ihr Übermittlungsersuchen auf § 71 Abs. 1 Nr. 2 SGB X stützte. Dabei hatte sie zum einen verkannt, daß die betroffene Erkrankung keine Seuche im Sinne des Bundesseuchengesetzes (BSeuchG)[166] war. Zum anderen stellt § 71 Abs. 1 Nr. 2 SGB X eine Befugnis für eine Übermittlung von Sozialleistungsträgern an Gesundheitsämter dar, für den umgekehrten Übermittlungsweg bildet sie jedoch **keine Rechtsgrundlage**. Auch aufgrund des Brandenburgischen Gesundheitsdienstgesetzes (BbgGDG)[167] ließ sich, außer dem Weg über eine Einwilligungserklärung jedes einzelnen Betroffenen, keine Übermittlungsbefugnis herleiten. Dementsprechend wurde die Auskunft letztlich abgelehnt.

7.2 Gesundheit

7.2.1 Gesetze, Verordnungen und Erlasse

7.2.1.1 Gesetz zur Regelung des Transfusionswesens

Im Berichtszeitraum legte mir das MASGF den Entwurf eines Gesetzes zur Regelung des Transfusionswesens (Transfusionsgesetz) vor. Kaum hatte ich dazu Stellung genommen, erhielt ich vom MASGF auch schon einen aktualisierten Referentenentwurf. Meine Stellungnahme hierzu hat das Ministerium dem Bundesministerium für Gesundheit zugeleitet mit der Bitte um Berücksichtigung im weiteren Gesetzgebungsverfahren.

Das Transfusionsgesetz soll der gesicherten Versorgung der Bevölkerung mit Blutprodukten dienen. Wesentliche Gesichtspunkte sind dabei die Qualitätssicherung, Dokumentationen über den Spender und den Empfänger von Blutprodukten, Mitteilungspflichten und Rückverfolgungsmöglichkeiten für die Fälle, in denen an einer Stelle eine Infektion oder auch nur der Verdacht einer solchen auftritt. Der vielfältige Informationsbedarf soll soweit wie möglich anonymisiert stattfinden.

Im ersten mir vorgelegten Entwurf sollten viele Meldungen mit folgenden Angaben zu dem Betroffenen erfolgen: Initialen, Geburtsdatum und die ersten drei Ziffern der Postleitzahl des Wohnortes. Dieses Verfahren stellt nur eine sehr schwache Anonymisierung dar und kann zudem auch Verwechslungen und Doppelnennungen nicht ausschließen. Ich habe mich

166 i. d. Fass. vom 18. Dezember 1979, BGBl. I S. 2262, ber. 1980, BGBl. I S. 151; zul. geänd. durch ErstÄG vom 25. Juli 1996, BGBl. I S. 1118

167 vom 3. Juni 1994, GVBl. S. 178

deshalb dafür eingesetzt, daß alle **Meldungen** im Transfusionswesen auf einem **mehrteiligen Code** basieren, der z. B. die Spendeeinrichtung, Spendenummer, das Spendedatum, die Chargennummer und die Patientenidentitätsnummer je nach Meldezweck enthalten könnte. Der Gesetzgeber hat sich letztlich für die Kriterien Geburtsdatum und Geschlecht entschieden. Damit lassen sich ein stärkerer Anonymisierungsgrad als bei der anfänglichen Regelung erzielen, aber auch Verwechslungen und Mehrfachzählungen weitestgehend vermeiden. Auch wenn ich die von mir vorgeschlagene Lösung nach wie vor für die bessere erachte, kann das Abstellen auf Geburtsdatum und Geschlecht doch auch als akzeptabel angesehen werden.

7.2.1.2 Infektionsschutzgesetz

Mitte 1997 bat mich das MASGF um eine Stellungnahme zu dem Referentenentwurf eines Gesetzes zur Neuordnung seuchenrechtlicher Vorschriften. Durch das geplante Infektionsschutzgesetz (IfSG) werden das Bundes-Seuchengesetz, das Geschlechtskrankheitengesetz und mehrere Verordnungen zu einem einheitlichen, neu strukturierten, dem aktuellen Stand der medizinischen Erkenntnisse entsprechenden Gesetz zusammengefaßt. Die mir inzwischen vorliegende überarbeitete Fassung des Entwurfs trägt gemäß dem Wunsch der Datenschutzbeauftragten dem Zweckbindungsgedanken wesentlich mehr Rechnung als der erste Entwurf. Auch wurden etliche Aufbewahrungsfristen (z. B. für Aufzeichnungen über nosokomiale Infektionen oder Protokolle über Belehrungen des Personals in bestimmten Einrichtungen) zwischenzeitlich geregelt.

Eine noch im vorangegangenen Entwurf enthaltene, aber völlig unzulängliche **spezielle Regelung zum Datenschutz** ist nunmehr aus dem Entwurf **gestrichen**. Dies hat zur Folge, daß, soweit das Infektionsschutzgesetz hierzu keine speziellen Regelungen trifft, die datenschutzrechtlichen Regelungen des Brandenburgischen Gesundheitsdienstgesetzes[168] Anwendung finden. Anläßlich eines Schriftwechsels zu einer Anfrage eines Gesundheitsamtes[169] mußte das MASGF mir zugestehen, daß die datenschutzrechtlichen Vorschriften des Brandenburgischen Gesundheitsdienstgesetzes in etlichen Punkten unzulänglich sind. Angesichts des Umstandes, daß sich der Bundesgesetzgeber nun auch beim Infektionsschutzgesetz zurückzieht, um landesrechtliche Regelungen zur Geltung kommen zu lassen, erachte ich eine **Überarbeitung der datenschutzrechtlichen Vorschriften des Brandenburgischen Gesundheitsdienstgesetzes** für vordringlich. Da auch das Brandenburgische Psychisch-Kranken-Gesetz[170] einer Novellierung bedarf und mir in der Krankenhausdatenschutzverordnung[171] zwischenzeitlich verschiedene Punkte begegnet sind, die verbessert werden müßten, hielt ich es für angezeigt, dem Ministerium zu empfehlen, das vom Landesgesetzgeber in § 28 Abs. 3 Satz 2 Landeskrankenhausgesetz[172] versprochene Gesetz zum Datenschutz im Gesundheitswesen in absehbarer Zeit zu erarbeiten.

7.2.1.3 Verwaltungsvorschrift zum Umgang mit Impfdateien im Gesundheitsamt

---

168 vom 3. Juni 1994, GVBl. S. 178

169 s. unter 12.5.2

170 vom 8. Februar 1996, GVBl. I S. 26; s. unter 7.2.1.6

171 vom 4. Januar 1996, GVBl. II S. 54; s. unter 7.2.2.1

172 vom 11. Mai 1994, GVBl. I S. 106

In Ergänzung des interministeriellen Runderlasses zur Meldung, Aufbewahrung und Nutzung von Patientendaten aus ehemaligen Einrichtungen des Gesundheitswesens[173] hatte das MASGF mir im vergangenen Jahr den Entwurf eines Runderlasses zur Behandlung von Impfdateien in den Gesundheitsämtern[174] vorgelegt. Diesen Entwurf hat es dann grundlegend überarbeitet, um auch aktuelle Impfungen einzubeziehen. Er berücksichtigte schon damals etliche Anregungen aus vorangegangenen Gesprächen. Aus meiner neuen Stellungnahme wurden die wesentlichen Empfehlungen aufgegriffen.

Die namensbezogene Meldung von aktuellen Schutzimpfungen, die niedergelassene Ärzte oder medizinische Einrichtungen vorgenommen haben, an die zuständigen Gesundheitsämter **bedarf einer schriftlichen Einwilligung des Patienten**. Bedenken wegen zu vager oder zu weiter Einwilligungserklärungen im medizinischen Bereich wurden in der Vergangenheit regelmäßig an mich herangetragen. Ebenfalls meinem Wunsch entsprechend wird die Anlage zu der Verwaltungsvorschrift deshalb eine standardisierte Einwilligungserklärung enthalten. Die vom Ministerium vorgeschlagene Einwilligungserklärung berücksichtigt im wesentlichen die Forderungen des § 4 Abs. 2 BbgDSG, vor allem benennt sie den Arzt/die Einrichtung, der/deren Beschäftigte von der ärztlichen Schweigepflicht entbunden werden soll(en), und die Zwecke der Datenverarbeitung. Sie enthält außerdem einen Hinweis darauf, daß die Einwilligung verweigert und jederzeit widerrufen werden kann, ohne daß dem Betroffenen dadurch ein rechtlicher Nachteil entsteht.

Keine Einigung konnte ich dagegen mit dem Ministerium über die in der Einwilligungserklärung vorgesehene Variante erzielen:

„Bei Anfragen von behandelnden Ärzten oder Unfallambulanzen kann das Gesundheitsamt Auskunft über erfolgte Impfungen erteilen."

Ich gehe davon aus, daß in den Standardfällen entweder der Betroffene sein Impfdokument selbst vorlegt oder eine auf den konkreten Fall bezogene **Einwilligung in die Abfrage beim Gesundheitsamt** erteilen kann. Bei Gefahr für Leib und Leben des Betroffenen kommt, wenn dieser weder rechtlich noch tatsächlich in der Lage ist, sich zu dem Auskunftsersuchen zu positionieren, auch eine mutmaßliche Einwilligung in Betracht. Diese Lösung erscheint mir wesentlich besser als die vorgesehene pauschale Einwilligungserklärung. Bedenken gegen diese bestehen auch deshalb, weil der Betroffene derzeit überhaupt nicht wissen kann, welche Stelle in ferner Zukunft einmal eine solche Auskunft benötigen könnte und ob er möchte, daß dieser Stelle die Auskunft überhaupt, nur über bestimmte Impfungen oder tatsächlich ganz pauschal erteilt wird.

7.2.1.4 Brandenburgisches Rettungsdienstgesetz

[173] vom 22. November 1993, ABl. 1993 S. 1725

[174] s. 5. Tätigkeitsbericht unter 7.3.1.5

Wie im 5. Tätigkeitsbericht[175] berichtet, hatte ich mich beim Landesrettungsdienstplan im Hinblick auf eine angekündigte bereichsspezifische gesetzliche Regelung dazu bereiterklärt, den durch fehlende Regelungen beispielsweise zur Dokumentation entstandenen, aus datenschutzrechtlicher Sicht unbefriedigenden Zustand vorübergehend zu tolerieren. Zwischenzeitlich hat mir das MASGF jedoch mitgeteilt, daß es zunächst nur ein Änderungsgesetz zum Brandenburgischen Rettungsdienstgesetz (BbgRettG)[176] geben werde, in dem datenschutzrechtliche Fragen nicht geregelt würden. Die Notwendigkeit weiterer Änderungen, die ich im Laufe des Berichtsjahres für den Bereich des Datenschutzes noch untermauert hatte, sieht das Ministerium zwar, hält es jedoch derzeit für aussichtslos, über solche Fragen Einigkeit herzustellen.

Auch mit dem MI wurde die **Notwendigkeit einer datenschutzrechtlichen Regelung der Dokumentationen der Leitstellen** besprochen. Die nächste Möglichkeit zur Novellierung wird seitens des MI für das Brandschutzgesetz (BschG)[177] gesehen, wofür bereits Vorbereitungen laufen. Würde die Novellierung des Brandschutzgesetzes als Artikelgesetz vorgenommen, so könnten die Vorgaben zur Dokumentation, die in § 8 BbgRettG festzulegen sind, in einem zweiten Artikel mit novelliert werden. Zumindest sollte die Chance einer zeitlich absehbaren Regelung der Dokumentationsfragen im Bereich des Rettungswesens genutzt werden.

7.2.1.5 Umgang mit personenbezogenen Daten aus Leichenschauscheinen

In meinem vorangegangenen Tätigkeitsbericht[178] hatte ich die Hoffnung geäußert, in diesem Jahr darüber berichten zu können, daß zumindest ein Verordnungsentwurf zur Regelung der Fragen des Leichenschauwesens erarbeitet und mit mir abgestimmt würde. Das MASGF ist jedoch mit einem solchen Vorhaben noch nicht an mich herangetreten.

7.2.1.6 Novellierung des Psychisch-Kranken-Gesetzes

Im Rahmen der datenschutzrechtlichen Beratung eines Landkreises wurde ich mit der Frage konfrontiert, welche Datenerhebungsbefugnisse für den Sozialpsychiatrischen Dienst bestehen und mit welchen Übermittlungsbefugnissen sie korrespondieren, wenn ein Betroffener nicht eine solche Gefahrenquelle darstellt, daß Zwangsmaßnahmen gegen ihn oder zu seinem Schutz eingeleitet werden müssen und er freiwillige Hilfen ablehnt, diese aber nach ärztlichem Urteil benötigt. Hier mußte ich Tendenzen zur „aufdrängenden Hilfe" beobachten, die sich weder derzeit noch künftig begründen lassen dürften. Insoweit scheinen jedoch klare Worte des Gesetzgebers notwendig zu sein.

Die durch die Beratung notwendig gewordene nähere Beschäftigung mit den Vorschriften des Brandenburgischen Psychisch-Kranken-Gesetzes (BbgPsychKG)[179] zeigte, daß die Vorschriften in sich z. T. nicht stimmig waren, was besonders kraß bei den ständig wechselnden Begriffen für den Hilfeträger, den Betroffenen und dessen gesetzlichen Vertreter deutlich wurde. Das MASGF, mit dem ich sogleich einzelne Auslegungsschwierigkeiten besprach, hatte auch schon selbst zuvor Schwächen in der Formulierung des Gesetzes festgestellt. Das Ministerium ließ erkennen, daß eine Novellierung um so eher erreicht werden könnte, von desto mehr Seiten die Notwendigkeit dazu plausibel gemacht würde. Ich habe dem MASGF deshalb vor kurzem meine datenschutzrechtlichen Bedenken und Anregungen zum Gesetz

---

175 s. unter 7.3.1.4

176 vom 8. Mai 1992, GVBl. I S. 170; zul. geänd. durch Haushaltsstrukturgesetz vom 17. Dezember 1996, GVBl. I S. 358

177 i. d. Fass. vom 9. März 1994, GVBl. I S. 65; zul. geänd. durch Haushaltsstrukturgesetz vom 17. Dezember 1996, GVBl. I S. 358

178 s. 5. Tätigkeitsbericht unter 7.3.1.7

179 vom 8. Februar 1996, GVBl. I S. 26

vorgetragen.

Dabei habe ich mich zum einen für eine **durchgängige und einheitliche Begriffswahl** eingesetzt, die durch Definitionen noch abgerundet werden könnte. Zum anderen habe ich angeregt, daß der Informationsbedarf zwischen den Stellen, die mit einem psychisch Kranken befaßt sein können, nochmals geklärt werden sollte, um dann die tatsächlich notwendigen Datenübermittlungsbefugnisse normenklarer formulieren zu können. Als Beispiel hierfür soll die Dokumentation in dem Verzeichnis über angeordnete besondere Sicherungsmaßnahmen nach § 20 Abs. 3 Satz 6 BbgPsychKG dienen: Nach der Gesetzesbegründung ist davon auszugehen, daß die sog. **Besuchskommission** davon Kenntnis erlangen soll, denn das Verzeichnis soll ihre Arbeit erleichtern. Dies spricht dafür, daß das Verzeichnis nicht personenbezogen geführt wird, da anderenfalls das Gebot der ärztlichen Schweigepflicht, das nach § 32 Abs. 7 BbgPsychKG gegenüber der Besuchskommission unberührt bleibt, nicht eingehalten werden könnte. Nicht vereinbar mit der Wahrung der ärztlichen Schweigepflicht gegenüber der Besuchskommission schien mir auch § 52 Satz 1 Nr. 9 BbgPsychKG, der eine Übermittlungsbefugnis von der Unterbringungseinrichtung an die Besuchskommission vorsieht. Eine Grundlage für eine solche Übermittlung kann nach § 32 Abs. 1 Satz 3 BbgPsychKG jedoch nur das Vorliegen einer Einwilligungserklärung des Betroffenen bzw. seines gesetzlichen Vertreters sein.

Aufmerksam gemacht habe ich weiter darauf, daß in dem Gesetz, weil insoweit auch ein Rückgriff auf das ebenfalls bereichsspezifische Brandenburgische Gesundheitsdienstgesetz ins Leere läuft, z. B. an ein **Akteneinsichtsrecht** in die Unterlagen des Sozialpsychiatrischen Dienstes, an Regelungen für die **Wartung und Fernwartung** sowie für die Ausübung von Aufsichtsbefugnissen unter Berücksichtigung des § 203 StGB bei dieser Stelle gedacht werden müßte. Nochmals aufgegriffen habe ich meine Anregung aus dem Gesetzgebungsverfahren, die Rechte und Pflichten des Patientenfürsprechers gem. § 31 BbgPsychKG zu konkretisieren[180].

Auf folgende notwendige Klarstellung habe ich das MASGF ebenfalls hingewiesen: Sofern der Betroffene über eine hinreichende **Einsichtsfähigkeit** verfügt, ist beispielsweise auch bei **Minderjährigen** neben der Einwilligung des gesetzlichen Vertreters diejenige des Betroffenen selbst einzuholen.

7.2.2 Aktuelle Fälle

7.2.2.1 Prüfung der Datenverarbeitung in einem Krankenhaus

Im Laufe des letzten Berichtszeitraumes hatte ich eine Prüfung in einem Kreiskrankenhaus durchgeführt und das Ergebnis der Kontrolle - soweit es die datenschutzgerechte Ausgestaltung des Krankenhausinformationssystems betraf - bereits im 5. Tätigkeitsbericht[181] dargestellt. Auf die weiteren Schwerpunkte der Prüfung, die Umsetzung der Krankenhausdatenschutzverordnung (KHDsV)[182], insbesondere die Aufbewahrung von Behandlungsunterlagen, den Zugriff auf diese und die Dokumentation in den Krankenakten wird im folgenden eingegangen.

Patientenaufnahme

Bereits bei der Aufnahme eines Patienten durch die Krankenhausverwaltung werden von ihm vielfältige

---

180 s. 4. Tätigkeitsbericht unter 7.3.1.1

181 s. unter 7.3.2.4

182 vom 4. Januar 1996, GVBl. II S. 54

personenbezogene Daten erfragt und ihm diverse Formulare zur Unterschrift vorgelegt.
Ein datenschutzrechtlicher Hinweis war bei keinem der Formulare des geprüften Klinikums vorgesehen. Eine sehr vage Einwilligungserklärung war mit weiteren Erklärungen, wie etwa der Vereinbarung der Geltung der Allgemeinen Vertragsbedingungen des Krankenhauses unter der Überschrift „Aufnahmevertrag", verknüpft. Ich habe eine Trennung von datenschutzrechtlich relevanten Erklärungen von anderen Erklärungen gefordert.

Auf meinen Hinweis hin wird derzeit eine datenschutzrechtliche Information für die Patienten erarbeitet. Vom Einholen einer generellen Einwilligungserklärung gleich bei der Aufnahme wird das Krankenhaus zukünftig absehen. Eine Verarbeitung von Patientendaten im Krankenhaus ist nach § 4 Abs. 1 KHDsV zulässig, soweit dies im Rahmen des Behandlungsverhältnisses erforderlich ist oder die Krankenhausdatenschutzverordnung bzw. eine andere Rechtsvorschrift es erlaubt. Damit ist das Gros der Datenverarbeitungen abgedeckt. Nur für die Ausnahmefälle, in denen diese Voraussetzungen nicht vorliegen, muß eine Einwilligung des Patienten nach § 4 Abs. 1 Nr. 3 KHDsV für den konkreten Einzelfall eingeholt werden. Dementsprechend will die Klinik künftig verfahren.

Von den Daten, die bei der Aufnahme erhoben wurden, habe ich vor allem die Frage nach Beruf und Arbeitgeber problematisiert. Diese sind allenfalls bei Arbeitsunfällen oder Berufskrankheiten notwendig. Das Krankenhaus nutzte die Frage nach dem Arbeitgeber jedoch dazu, Patienten, deren Adresse sich geändert hatte, auch zu einem späteren Zeitpunkt noch über den Arbeitgeber zu ermitteln. War jemand ohne Beschäftigung wurde sogar das Merkmal „arbeitslos" eingetragen. Ich habe gefordert, daß diese Vorgehensweise geändert wird.

Die von der Aufnahme erhobenen Daten werden in unterschiedlicher Zusammensetzung für das Patientenstammblatt, Etiketten, das Patientenblatt, die Pförtnerliste oder auch Informationen an die Kostenträger zusammengestellt. Zum Teil waren so im Krankenhaus für längere Zeit Patientendaten doppelt oder dreifach vorhanden. Auf meinen entsprechenden Hinweis hat sich das Krankenhaus dafür entschieden, das für die Verwaltung vorgesehene Patientenblatt, dessen Daten auch dauerhaft im Patientenstammblatt in der Krankenakte aufbewahrt werden, frühzeitig zu löschen. Mit den ausgedruckten Etiketten wurde nach Abschluß einer Behandlung unterschiedlich verfahren. Die einen Abteilungen vernichteten die überschüssigen Etiketten, die anderen hefteten sie in der Krankenakte ab. Nach Abschluß der Behandlung werden die überzähligen Etiketten jedoch nicht mehr benötigt, so daß ihre Aufbewahrung nicht erforderlich ist. Das Krankenhaus hat mir dementsprechend zugesagt, künftig die Etiketten nach der Entlassung eines Patienten zu vernichten.

Informationen an der Pforte

Auf der Grundlage der Datenerhebungen der Krankenaufnahme wurde für den Pförtner jeweils eine aktuelle Liste der Patienten gedruckt, die mit einer Auskunft über ihre Anwesenheit an Besucher einverstanden sind. Diese Liste umfaßte über die an sich nur notwendigen Angaben wie Name, Abteilung und Station hinaus das Geburtsdatum, die Adresse, den Aufnahmetag und die Aufnahmenummer des Patienten. Auf mein Einschreiten hin wurden immerhin das Geburtsdatum und die Adresse aus dieser Auskunftsdatei herausgenommen. Meiner Forderung, auch die Aufnahmenummer, die sich für krankenhausinterne Anonymisierungen anbietet, nicht dem Pförtner zur Kenntnis zu geben, ist das Krankenhaus bisher noch nicht nachgekommen.

Datenübermittlung an Krankenkassen

Die vom Krankenhaus erhobenen Patientendaten werden vor allem an gesetzliche Krankenkassen als Kostenträger übermittelt. Dabei schreibt § 301 Abs. 1 SGB V abschließend vor, welche Daten für die Abrechnung übermittelt werden

dürfen. Abweichend von der genannten Vorschrift enthielt z. B. der Kostenübernahmeantrag des Krankenhauses die Angabe des Arbeitgebers. Dies ist zwischenzeitlich geändert worden. Übermittelt wurde bisher auch der Name des einweisenden Arztes. Zukünftig wird § 301 Abs. 1 Nr. 4 SGB V beachtet, wonach bei ärztlicher Verordnung einer Krankenhausbehandlung nur die Arztnummer des einweisenden Arztes anzugeben ist.

Führung von Patientenakten

Das aus den Aufnahmedaten erstellte Patientenstammblatt wird Bestandteil der Krankenakte. Auch diese krankenhausinterne Dokumentation war z. T. zu bemängeln. So verwendeten die meisten Stationen des Krankenhauses keinen wirklichen **Aktendeckel** mit wenigen personenbezogenen Angaben über den Patienten, sondern hüllten die medizinischen Unterlagen des jeweiligen Patienten in seinen Anamnesebogen ein. So waren u. U. auf den ersten Blick heikle medizinische Daten über den Patienten wahrzunehmen. Bereits eine flüchtige Durchsicht des Inhalts einzelner Krankenakten zeigte, daß diese häufig nicht vollständig dokumentiert waren, z. T. Unterlagen doppelt enthielten oder solche, die nicht in die Krankenakte gehörten. Datenschutzrechtlich am bedenklichsten war ein Fall, in dem die **Namen von Mitpatienten** und sogar der Befund einer dieser Personen in einer anderen Behandlungsakte enthalten war. Das Krankenhaus hat zugesagt, dies zu ändern.

Zugriff auf Patientenakten

Zum Zeitpunkt der Prüfung waren noch die einzelnen Stationen für die Aufbewahrung und Archivierung der Krankenakten zuständig. Die Zugriffs- und Schlüsselbefugnisse waren unterschiedlich geregelt. Teilweise waren nur wenige Personen zugriffsberechtigt, teilweise waren die Unterlagen praktisch für jeden Mitarbeiter frei zugänglich. Vertretungsregelungen waren selten angedacht worden. Dies soll künftig durch Dienstanweisungen für die einzelnen Stationen festgelegt werden. Im wesentlichen werden die Akten jedoch im Krankenhausarchiv von einem Archivar betreut.

Der Zugriff auf die Patientenakten erfolgte bisher über **Registerbücher**, die meist über den Namen des Patienten, seine Aufnahmenummer und den Aufenthaltszeitraum hinaus noch weitere Daten enthielten, die von Abteilung zu Abteilung höchst unterschiedlich geführt wurden. Ich habe gefordert, daß folgende Daten künftig nicht mehr erhoben und gespeichert werden und in der Vergangenheit dazu gespeicherte Patientendaten geschwärzt werden:

- Geburtsdatum, da dieses nur von einer Abteilung als erforderlich angesehen worden war,

- Wohnort, da nach den Erfahrungen einer Abteilung darauf verzichtet werden konnte,

- Diagnose, da nicht ersichtlich war, wozu solche heiklen Daten in einem Registerbuch aufgelistet wurden,

- Vermerk „Verstorben", da dies für das Auffinden einer Krankenakte nicht erforderlich ist.

Archivierung von Patientenakten

Anläßlich der Prüfung suchte das Krankenhaus meine Beratung zur Frage der künftigen Archivierung. Vom Krankenhaus ist beabsichtigt, sämtliche Dokumentationen eines Patienten in einer einzigen Krankenakte zusammenzuführen, die im Krankenhausarchiv aufbewahrt werden soll. Bei einer Wiederaufnahme soll den neubehandelnden Ärzten dann die gesamte vorhandene Dokumentation über den Patienten zur Verfügung gestellt werden. Nach Rücksprache mit dem

MASGF habe ich dem Krankenhaus folgende Auskunft erteilt:

Patientendaten sind zu sperren und dann gesondert im Krankenhausarchiv zu speichern, sobald die Behandlung abgeschlossen ist, die damit zusammenhängenden Zahlungsvorgänge abgewickelt sind und das Krankenhaus den Bericht über die Behandlung erstellt hat (§ 8 Abs. 1 Satz 1 KHDsV). Diese Sperrung kann nach § 8 Abs. 4 Nr. 1 KHDsV u. a. aufgehoben werden „für die Durchführung einer Behandlung, mit der die frühere Behandlung in einem **medizinischen Sachzusammenhang** steht". Diese vom Gesetz geforderte Feststellung kann - vor allem im vorhinein - praktisch nicht getroffen werden. Folgendes kann jedoch gefordert werden:

- Es muß ausgeschlossen sein, daß bei einer Wiederaufnahme automatisch bereits vorhandene Krankenunterlagen herangezogen werden.

- Eine im einzelnen Fall notwendig erscheinende Anforderung bereits vorhandener Krankenunterlagen muß von der derzeit behandelnden Abteilung durch einen Arzt schriftlich begründet werden. Sie soll, wenn möglich, auf einzelne Unterlagen aus der Akte beschränkt werden.

- Eine detaillierte schriftliche Begründung kann nach § 8 Abs. 4 letzter Satz KHDsV bei einer gegenwärtigen Gefahr für Leben oder Gesundheit des Patienten auch nachträglich erfolgen.

- Empfohlen wird, für jede Akte ein **Notfalldatenvorblatt** anzulegen, so daß in vielen Fällen auf eine Vorlage der gesamten Akte verzichtet werden könnte, weil sich die wesentlichen Daten bereits auf diesem Vorblatt befinden.

- § 8 Abs. 4 Nr. 1 KHDsV erfordert keine definitive Feststellung eines medizinischen Behandlungszusammenhangs. Es genügt, daß ein solcher nicht auszuschließen ist.

- Bei einer Aktenanforderung aus dem Archiv prüft der Archivar grundsätzlich lediglich, ob das Nutzungsersuchen im einzelnen schriftlich begründet wurde und im Rahmen der Aufgaben der anfordernden Abteilung liegt. Sollten trotzdem einmal begründete Zweifel beim Archivar beispielsweise am medizinischen Sachzusammenhang bestehen, müßten diese z. B. mit dem Abteilungsarzt der anfragenden Abteilung geklärt werden.

Datensicherheit im „Behandlungsalltag"

Bei der Überprüfung der Sicherung der Patientendaten im medizinischen Bereich mußte festgestellt werden, daß hierfür nur in den seltensten Fällen abschließbare Stahlschränke zur Verfügung standen. Das Krankenhaus hat jedoch zugesagt, dies in absehbarer Zukunft zu ändern.

Moniert habe ich auch, daß im weit offenstehenden Zimmer der Pflegekräfte ein patientenbezogener OP-Plan aushing, der von jedem Besucher und jeder Reinigungskraft in Augenschein genommen werden konnte.

Dienstanweisung zum Datenschutz

Die Information der Mitarbeiter über datenschutzrechtliche Probleme war im Krankenhaus bisher deutlich zu kurz gekommen. Zwar gab es ein Formular, das die Beschäftigten auf ihre Schweigepflicht hinwies, dieses beruhte jedoch nicht auf dem aktuellen Recht. Zusätzlich habe ich dem Krankenhaus das Muster einer Verpflichtung auf das Datengeheimnis

überlassen.

Erst die Ankündigung meiner Kontrolle hat das Krankenhaus veranlaßt, sich eine **Dienstanweisung zum Datenschutz** zu geben. Diese war allerdings fast vollständig von der Dienstanweisung des Landkreises abgeschrieben und nur an wenigen Stellen mit Begriffen aus dem Krankenhausbereich „garniert" worden. Inzwischen hat das Krankenhaus eine besondere Dienstanweisung für den Umgang mit Patientendaten entworfen, die allerdings noch der weiteren Überarbeitung vor allem in technisch-organisatorischer Hinsicht bedarf.

Ein wesentlicher in der Dienstanweisung zu regelnder Punkt betrifft den **behördlichen Datenschutzbeauftragten**, seine Aufgaben, Befugnisse und Rechte. Derzeit wird der Datenschutzbeauftragte vom Landkreis gestellt. Die praktische Konsequenz dieser Bestellung war zunächst, daß dieser dort - auch mangels Einblick in mögliche datenschutzrechtliche Probleme eines Klinikums - nicht tätig wurde, u. a. weil das Krankenhaus keine Beratung durch den Datenschutzbeauftragten suchte. Infolge des Kontrollbesuches meiner Behörde hat der zuständige Datenschutzbeauftragte Anhaltspunkte dafür erhalten, worauf er sein Augenmerk im Klinikum richten könnte und dort einen geeigneten Ansprechpartner gefunden. Aufgrund meiner Anfrage zur Beschäftigung von externen Laboren mußte er feststellen, daß diesen nach einem mit dem Krankenhaus getroffenen Vertrag ggf. ganze Krankenakten überlassen wurden und hat es übernommen, insoweit auf eine Änderung des Vertrages hinzuwirken.

Externer Datenschutzbeauftragter

Trotz dieser auf der einen Seite inzwischen erfreulichen Entwicklung bezüglich des Datenschutzbeauftragten bleibt **für mich die Problematik der Datenverarbeitungsbefugnis eines** solchen **externen Datenschutzbeauftragten** bestehen. Eine wirksame datenschutzrechtliche Kontrolle ohne Kenntnisnahme personenbezogener Daten erscheint mir nicht möglich. Da der Gesetzgeber im Land Brandenburg jedoch ausdrücklich darauf verzichtet hat, den behördlichen Datenschutzbeauftragten zu regeln, kann dieser eventuelle Datenverarbeitungsbefugnisse nur von einer leitenden Stelle innerhalb der Einrichtung herleiten. Inwieweit ein Mitarbeiter des Krankenhausträgers beispielsweise dem Verwaltungsdirektor eines Klinikums unterstellt werden könnte, ist bisher nicht geklärt. Was aus Sicht des Kommunalrechts unproblematisch zu sein scheint, nämlich das Tätigwerden eines Mitarbeiters einer Kommune in einem kommunalen Unternehmen, wirft vor dem Hintergrund der ärztlichen Schweigepflicht und der Krankenhausdatenschutzverordnung, die deutlich zwischen klinischem und Verwaltungsbereich unterscheidet und spezielle datenschutzrechtliche Regelungen für das Krankenhaus trifft, rechtliche Probleme auf. Solange der Gesetzgeber hierzu keine Lösung anbietet, setze ich mich dafür ein, daß Datenschutzbeauftragter nur ein Mitarbeiter des Krankenhauses sein kann.

Außer dem Kooperationsvertrag mit seinem kommunalen Träger über den Datenschutzbeauftragten hat das Krankenhaus noch weitere Verträge geschlossen, die entweder eine Datenverarbeitung im Auftrag beinhalten oder doch zumindest die Gefahr des Kontaktes von Patientendaten mit Externen entstehen lassen:

Einsatz von Fremdfirmen

Zum einen wird Reinigungspersonal einer Fremdfirma im Klinikum beschäftigt. Durch eine spezielle Dienstanweisung für die **Zutrittsberechtigung zum Serverraum** war bislang zumindest einer Mitarbeiterin der Reinigungsfirma der Zutritt zu diesem Raum mit einem eigenen Schlüssel ermöglicht. Nach anfänglichem Sträuben des Krankenhauses gegen eine Änderung dieser Verfahrensweise hat es zwischenzeitlich mitgeteilt, die Reinigungsfirma gewechselt zu haben und das Reinigungspersonal in sämtlichen Räumen, in denen personenbezogene Daten aufbewahrt werden, nur noch **unter**

Aufsicht tätig werden zu lassen.

Outsourcing von Teilaufgaben

Die Lohn- und Gehaltsabrechnungen für die Krankenhausmitarbeiter werden durch eine private Firma in einem anderen Bundesland vorgenommen, ohne daß hierfür die verfahrensmäßigen Vorgaben des § 11 BbgDSG beachtet wurden. Ungeachtet meiner grundsätzlichen Bedenken gegen auftragsweise Datenverarbeitung über die Landesgrenzen hinaus[183] wurden im Ergebnis der Kontrolle dann zumindest sowohl die erforderliche Genehmigung für Datenverarbeitung im Auftrag beim MI eingeholt als auch die Meldung hierüber bei der zuständigen obersten Kontrollbehörde des Auftragnehmerlandes erstattet.

Die Entsorgung von Datenträgern mit Patienten- und sonstigen personenbezogenen Daten war bisher eher vernachlässigt worden. Erst nach mehrfachen Vorhaltungen hat sich das Krankenhaus nunmehr entschlossen, ein **Entsorgungskonzept** anzudenken, bei dem wohl auch eine Spezialfirma eingeschaltet werden wird. Ich mußte das Krankenhaus auch diesbezüglich insbesondere auf die formalen Voraussetzungen eines schriftlichen Vertragsschlusses und der Information/Beteiligung von Kontroll- und Aufsichtsbehörden nach § 6 Abs. 3 KHDsV i. V. m. § 11 Abs.1, 3 BbgDSG hinweisen.

Es ist erfreulich, feststellen zu können, daß nunmehr nach anfänglichem Zögern das Krankenhaus bemüht ist, den durch die Kontrolle aufgedeckten vielfältigen datenschutzrechtlichen Mängeln abzuhelfen. Der Träger der Einrichtung hat hierauf entscheidenden Einfluß genommen und ist damit seiner Verpflichtung gem. § 4 Abs. 5 Satz 3 KHDsV gerecht geworden.

7.2.2.2 Umgang mit Dienst- und Privatpost in der zentralen Poststelle einer Landesklinik

Eine Landesklinik wandte sich mit der Bitte um datenschutzrechtliche Beratung wegen Problemen, die durch die **Vermischung von Privat- und Dienstpost** sowie durch Adressierungsfehler in ihrer zentralen Poststelle entstanden waren, an mich.

Ich habe dem Krankenhaus empfohlen, die Weiterleitung jeglicher Privatpost zusammen mit der Dienstpost ganz zu unterbinden und statt dessen beim Krankenhaus einen öffentlichen Briefkasten installieren zu lassen. Privatbriefe, die trotz dieser Regelung in der Dienstpost aufgefunden würden, könnten dann einfach in diesen Briefkasten eingeworfen werden.

Weise dienstlicher Schriftverkehr einen Mangel auf, der eine Zustellung verhindern könnte, so könnte sich dafür folgende Lösung anbieten: Wegen § 4 Abs. 2 KHDsV sind Schreiben mit patientenbezogenen Daten aus dem medizinischen Bereich des Krankenhauses von dem Absendenden zu verschließen, bevor sie an die Poststelle weitergereicht werden. Die verschlossenen Briefe eines Abteilungssekretariats sollten in einer Mappe an die Poststelle gegeben werden, die das jeweilige Sekretariat bezeichnet. Bei einer nicht DIN-gerechten Gestaltung des Briefes kann dann die ungeöffnete Sendung in der Mappe an den zuständigen Bereich zurückgereicht werden, wo der Brief vom zuständigen bzw. wenn sich dieser nicht ermitteln läßt, vom abteilungsleitenden Arzt geöffnet und anschließend korrigiert werden kann. Im Verwaltungsbereich, wozu auch die Poststelle gehören dürfte, dürfen Briefe aus dem klinischen Bereich, bei denen nicht ausgeschlossen werden kann, daß sie Patientendaten enthalten, nämlich soweit dies organisatorisch vermeidbar ist, nicht geöffnet werden.

---

[183] s. 5. Tätigkeitsbericht unter 12.4.1.2

Bestehe ein konkreter Anlaß zu dem Verdacht, daß ein Mitarbeiter seine private Post in die Dienstpost geschmuggelt hat, um durch diesen Täuschungsversuch Porto für seine Postsendung zu sparen, könnte das besagte Postgut dem unmittelbaren Fachvorgesetzten mit der Bitte zugeleitet werden, im Beisein des Absenders den dienstlichen bzw. privaten Inhalt festzustellen. Auf diese Weise hätte der Absender ggf. Gelegenheit, sich zu einem privaten Inhalt zu bekennen, ohne daß die Postsendung geöffnet werden müßte und Dritte hiervon Kenntnis erlangten.

Der Umstand, daß Schreiben aus dem ärztlichen Bereich nicht offen an die Poststelle gegeben werden dürfen, schließe es nicht von vornherein aus, mehrere Briefe an einen Adressaten in ihren eigenen verschlossenen Kuverts in einem zusätzlich zu verwendenden größeren Umschlag zusammen zu versenden, solange der einzelne Brief an die jeweils zuständige Stelle adressiert bleibe.

Zum allgemeinen **Postlauf im Krankenhaus** habe ich nach Inkrafttreten der KHDsV folgende - etwas von der Darstellung im 2. Tätigkeitsbericht[184] abweichende - Ansicht vertreten:

- Post aus dem ärztlichen Bereich ist wegen § 4 Abs. 2 KHDsV verschlossen an die zentrale Poststelle zu leiten.

- Eingehende Postsendungen, die allgemein an das Krankenhaus adressiert sind, dürfen in der Poststelle geöffnet werden.

- Eingehende Briefe, die mit dem Zusatz „zu Händen" eines Arztes oder einer anderen konkret bezeichneten Stelle im medizinischen Bereich des Krankenhauses versehen sind, sind wegen § 4 Abs. 2 KHDsV verschlossen an diesen/den jeweiligen Bereich weiterzuleiten. Da es sich dabei um Dienstpost handelt, darf diese aber bereits von den dafür als zuständig bestimmten Mitarbeitern der genannten Ärzte bzw. des genannten Bereichs geöffnet werden.

- Lautet die Anschrift hingegen „Herrn/Frau ... (persönlich)/(im Krankenhaus)" so ist nicht auszuschließen, daß es sich um Privatpost handelt, die nur von dem Betreffenden selbst geöffnet werden darf. Dies gilt entsprechend, wenn eine Person im Verwaltungsbereich angeschrieben wird. Auch dort muß Post, die erkennbar an eine bestimmte Person/Stelle gerichtet ist, diese ungeöffnet erreichen, weil nur für deren Aufgabenerfüllung die Kenntnisnahme der übersandten Daten erforderlich ist. Vergleichbares gilt für die Ausgangspost.

7.2.2.3 Verpflichtung der Beschäftigten in Krankenhäusern zum Tragen von Namensschildern

Bundesweit in Diskussion stand die Frage, ob Beschäftigte in Krankenhäusern zum Tragen von Namensschildern verpflichtet werden können.

Dabei war zunächst zu prüfen, ob sich öffentlich Bedienstete gegenüber dem Staat auf ihr informationelles Selbstbestimmungsrecht berufen können. Dies kann nach einhelliger Auffassung der Datenschutzbeauftragten nur insoweit zutreffen, als sie diesem als eigenständige Träger von Rechten und Pflichten gegenübertreten. Dies ist z. B. der Fall, wenn etwa bei Beamten das sog. Grundverhältnis berührt ist. Wenn allerdings ein Funktionsträger eine Tätigkeit für den Staat in dessen Aufgabenerfüllung ausübt, ist das informationelle Selbstbestimmungsrecht des Bediensteten bei der

[184] s. unter 7.2.3.5

Verarbeitung seiner personenbezogenen Daten nicht betroffen. Er ist insoweit mit seinem Namen als Funktionsträger deklarationspflichtig, so daß er eine Namensnennung gegenüber Dritten mittels Namensschild ebenso hinnehmen muß wie das Erscheinen seines Namens in bearbeiteten Vorgängen oder in dienstlichen Telefonverzeichnissen.

Gleichwohl bleibt es Aufgabe des Dienstherrn/öffentlichen Arbeitgebers, situationsabhängig soweit wie möglich dem Schutzbedürfnis der Bediensteten Rechnung zu tragen. Erfahrungsgemäß sind Krankenschwestern - und hier insbesondere Schwesternschülerinnen - häufig Belästigungen männlicher Patienten ausgesetzt, die sich möglicherweise sogar in den privaten Bereich verlagern könnten, wenn durch das Tragen von Namensschildern mit dem Nachnamen (vorrangig bei außergewöhnlichen) Wohnanschriften und Telefonnummern der Betroffenen mit Hilfe von Adreß- und Telefonbüchern ausfindig gemacht werden können.

Die **Gefahr für weibliche Beschäftigte**, durch die Verknüpfung der Berufsbezeichnung mit dem Vornamen (z. B. „Schwester Angelika") auf Namensschildern besonderen persönlichen Herabwürdigungen ausgesetzt zu sein, schätze ich weitaus geringer ein als die mit den o. g. Nachforschungsmöglichkeiten einhergehenden Gefahren bis in den privaten Bereich hinein durch die Zurkenntnisgabe (auch) der Nachnamen, zumal davon ausgegangen werden kann, daß der Vorname im täglichen Pflegebetrieb traditionsgemäß ohnehin auch weiterhin inoffiziell geführt würde.

Es ist daher für mich nicht erkennbar, weshalb es - entgegen traditioneller Handhabung - auf den Aufgabenzweck gerichtet zwingend erforderlich sein sollte, daß sich Krankenschwestern mit ihrem Nachnamen zu erkennen geben, mit dem sich im übrigen regelmäßig kaum eine stärkere Identifizierungswirkung für den internen Dienst- bzw. Pflegebetrieb (und nur darauf kann die Offenbarungspflicht im Rahmen ordnungsgemäßer Aufgabenerfüllung ausgerichtet sein) als mit dem Vornamen erzielen lassen dürfte.

Allerdings kann dies nicht zu dem Schluß führen, daß die Leitungen öffentlicher Krankenhäuser nicht alles tun müssen, den Kreis der Betroffenen durch innerorganisatorische Maßnahmen, zumindest durch geeignete Aufklärungshinweise an die Patienten, vor Anzüglichkeiten und Belästigungen zu schützen.

7.2.2.4 Krankenhauswanderer

Bei einem Kontrollbesuch in einem Krankenhaus[185] mußte ich feststellen, daß dort im Archiv noch anderthalb bis zwei Jahre alte Informationen über Krankenhauswanderer im Mitteilungsblatt der Landeskrankenhausgesellschaft Brandenburg aufbewahrt wurden.

Bereits in meinem 2. Tätigkeitsbericht[186] hatte ich dargelegt, daß Krankenhäuser keine **Warnschreiben** übermitteln, speichern oder nutzen dürfen und etwa vorhandene Warnschreiben anderer Stellen über Krankenhauswanderer unverzüglich zu vernichten haben. Für eine diesbezügliche Datenverarbeitung durch das Krankenhaus besteht auch nach der inzwischen in Kraft getretenen KHDsV **keine Rechtsgrundlage**. Die aufgenommenen Patienten müssen ohnehin untersucht und je nach Untersuchungsergebnis behandelt werden, weshalb solche Warnmeldungen allenfalls Anlaß zu einer besonders kritischen Untersuchung geben könnten. Ansonsten handelt es sich bei ihnen um eine grundrechtswidrige Datenverarbeitung auf Vorrat, die das Prinzip der Erforderlichkeit grob mißachtet.

---

185 s. unter 7.2.2.1

186 s. unter 7.2.3.4

Eine der aufgefundenen Informationen stammte von einer brandenburgischen Krankenversicherung. Diese habe ich darauf hingewiesen, daß eine Datenübermittlung nach §§ 67 d, 68 ff. SGB X jeweils einen konkreten Anlaß voraussetzt, der bei einer Streuung der Informationen über die Krankenhäuser im Land nicht angenommen werden kann. Von einer Beanstandung habe ich in diesem Fall nur abgesehen, weil die Krankenkasse einräumte, daß ihre damalige Verfahrensweise, die bereits anderthalb Jahre zurücklag, nicht korrekt gewesen sei und weil sie alle Fachabteilungen über die Unzulässigkeit solcher Warnmeldungen informiert hatte. Die anderen meiner Kontrolle unterliegenden Krankenkassen im Land Brandenburg habe ich vorsorglich nochmals über meine Beurteilung von Warnhinweisen über Krankenhauswanderer informiert. Darüber hinaus habe ich sämtliche meiner Kontrolle unterliegenden Krankenhäuser des Landes aufgefordert, solche Informationen nicht weiter zu verbreiten und von anderen Stellen, insbesondere der Landeskrankenhausgesellschaft, erhaltene diesbezügliche Mitteilungen umgehend zu löschen.

Die Reaktionen der Krankenhäuser waren überwiegend positiv. In wenigen Fällen waren eigene Listen über Krankenhauswanderer angelegt worden, die zu löschen waren. Bei vielen Krankenhäusern wurden die Mitteilungen der Landeskrankenhausgesellschaft erst nach meiner Aufforderung vernichtet. Teilweise waren in den Krankenhäusern überhaupt keine vergleichbaren Informationen mehr vorhanden, teilweise war aber vor der Vernichtung solcher Warnhinweise eine mündliche Information an einzelne Mitarbeiter erfolgt.

Ich habe den beteiligten Stellen empfohlen, den Datenfluß zwischen Krankenhaus und Krankenkasse im gesetzlich vorgesehenen Rahmen zu verbessern. Bei einer sofortigen Übersendung von Kostenübernahmeanträgen vom Krankenhaus und einer umgehenden Bearbeitung durch die Krankenkasse ließen sich insoweit sicher Kosten vermeiden. Ein in Zweifelsfällen als Alternative dazu geführtes Telefonat, bei dem die Vorgaben des § 301 SGB V, der einen Katalog von Daten festlegt, die das Krankenhaus an die Krankenkasse übermitteln darf, einhalten würde, habe ich ebenfalls als akzeptabel angesehen. Die Krankenkasse sehe ich nach § 284 Abs. 1 Nr. 4 SGB V in diesen Fällen als befugt an, Simulanten u. ä. intern zu kennzeichnen.

Nicht zu beanstanden ist es außerdem, daß dann, wenn ein Klinikum einen Krankenhausbetrüger selbst behandelt hatte, dieser unter den sog. „offenen Zahlungsfällen" gespeichert wird. Patientendaten sind nach § 8 Abs. 1 KHDsV nämlich erst zu sperren, sobald die Behandlung abgeschlossen ist und die damit zusammenhängenden Zahlungsvorgänge abgewickelt sind. Auch bei dieser Verfahrensweise ist jedoch der Verhältnismäßigkeitsgrundsatz zu wahren. Insoweit ist beispielsweise beachtlich, ob es sich lediglich um Bagatellbeträge gehandelt hatte. Auch darf diese Speicherung nicht zeitlich unbeschränkt beibehalten werden.

7.2.2.5 Archivierung von Krankenakten im Archiv des Trägers

Ein Krankenhaus war vom zuständigen Archiv seines Trägers dazu aufgefordert worden, seine aktuellen nicht mehr benötigten Krankenakten dorthin abzugeben. Solche nach der **Krankenhausdatenschutzverordnung** (KHDsV) zu sperrenden Patientenunterlagen werden bei Wiederaufnahmen möglicherweise aber auch sehr überraschend und dringend wieder benötigt. Dem Krankenhaus war deshalb daran gelegen, seine Krankenakten solange wie möglich im eigenen Krankenhausarchiv aufzubewahren. Darüber hinaus problematisierte es die ärztliche Schweigepflicht bei einer Abgabe ans zuständige Archiv.

Ich habe dem Krankenhaus folgende Auskunft erteilt:

§ 8 Abs. 1 Satz 1 KHDsV sieht vor, daß Patientenakten, die aktuell nicht mehr benötigt werden, zu sperren und nach Abs. 2

gesondert im Krankenhausarchiv aufzubewahren sind. Wenn die Daten zur Erfüllung der in § 4 Abs. 1 KHDsV genannten Zwecke (z. B. zur Behandlung) nicht mehr erforderlich sind, vorgeschriebene Aufbewahrungsfristen abgelaufen sind und kein Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange der Betroffenen beeinträchtigt werden, muß nach § 8 Abs. 1 Satz 2 KHDsV eine Löschung erfolgen. Vorgeschriebene Aufbewahrungsfristen sind beispielsweise in der **Berufsordnung der Ärzte**[187] (10 Jahre) sowie in der **Röntgenverordnung**[188] (bis zu 30 Jahre) enthalten, aber auch in einer krankenhausinternen Datenschutzanweisung könnte beispielsweise wegen der Verjährungsfrist des § 852 Abs. 1 BGB eine 30-jährige Aufbewahrungsfrist vorgesehen sein. Die Krankenhausdatenschutzverordnung geht davon aus, daß die Voraussetzungen für die Löschungen der Patientenakten spätestens nach Ablauf von 30 Jahren vorliegen, denn nach diesem Zeitraum schreibt § 8 Abs. 1 Satz 3 KHDsV eine Löschung oder Anonymisierung der Patientendaten vor.

187 vom 25. September 1993, ABl. S. 263; zul. geänd. durch 2. Satzungsänderung vom 23. November 1996, Amtl. Anz. S. 625

188 vom 8. Januar 1987, BGBl. I S. 114; zul. geänd. durch VO vom 25. Juli 1996, BGBl. I S. 1172

Demgegenüber fordert § 4 Abs. 1 **Brandenburgisches Archivgesetz** (BbgArchivG)[189], daß Unterlagen dann, wenn sie für die Erfüllung der Aufgaben einer öffentlichen Stelle nicht mehr benötigt werden bzw. spätestens 30 Jahre nach ihrer Entstehung, unverändert dem Archiv anzubieten sind. Auf die ärztliche Schweigepflicht nimmt das Brandenburgische Archivgesetz im Grunde keine Rücksicht, lediglich bei Beratungsstellen gem. § 4 Abs. 2 Ziff. 3 BbgArchivG ist eine anonymisierte Anbietung und Übergabe an das zuständige Archiv vorgesehen. Obwohl die Krankenhausdatenschutzverordnung rangniedriger ist als das Brandenburgische Archivgesetz habe ich die **Regelung in der Krankenhausdatenschutzverordnung** als **spezieller** angesehen und dem Krankenhaus geraten, vorrangig § 8 Abs. 1 Satz 3 KHDsV zu beachten und im Anschluß an die Aufbewahrung im krankenhauseigenen Archiv patientenbezogene Unterlagen, sofern das zuständige Archiv deren Übernahme überhaupt in Erwägung zieht, schon vor der Anbietung bei diesem zu anonymisieren und im übrigen zu vernichten.

Für diese Entscheidung lassen sich aber auch noch weitere Gründe anführen:

So unterliegen beispielsweise nur die im Gewahrsam eines Krankenhauses befindlichen Unterlagen dem Beschlagnahmeverbot nach § 97 Abs. 2 StPO. Zu bedenken ist auch, daß in § 4 Abs. 2 KHDsV deutlich zwischen der Verwaltung und anderen nicht medizinischen Stellen im Krankenhaus und dem ärztlichen Bereich unterschieden wird. Die Verwaltung und nicht medizinische Stellen dürfen Patientendaten nur in ganz konkret genannten Fällen verarbeiten, im übrigen müssen sie sich mit anonymisierten Daten begnügen. Wenn schon die Datenverarbeitung durch die Verwaltung des Krankenhauses selbst solchen Einschränkungen unterliegt, muß dies erst recht für ein öffentliches Archiv gelten.

7.2.2.6 Tumorbasisdokumentation

Nach der Erarbeitung der Meldebögen für die Tumorbasisdokumentation[190] aufgrund des **Krebsregistergesetz**es und des **Staatsvertrages über das gemeinsame Krebsregister der neuen Bundesländer und Berlins**[191] wurde mir vom MASGF ein Formular mit Datenschutzhinweisen für die behandelnden Ärzte vorgelegt, das ich akzeptiert habe. Außerdem erarbeitete das Ministerium eine **Einwilligungserklärung** für die Übermittlung an das Krebsregister. Dabei hat das Ministerium stets die enge Zusammenarbeit mit mir gesucht. Bedauerlicherweise konnten wir uns jedoch letztlich bezüglich einer Frage nicht verständigen. Ich hatte gefordert, daß diejenigen Ärzte und Einrichtungen, die durch die Einwilligungserklärung von ihrer ärztlichen Schweigepflicht entbunden werden, namentlich bezeichnet werden. So kann zum einen dem eventuellen Wunsch des Patienten Rechnung getragen werden, einzelne behandelnde Ärzte aus dem Geschehen herauszuhalten, wesentlicher erschien mir zum anderen jedoch, daß der Betroffene absehen können muß, welche Personen und Stellen Übermittlungen vornehmen dürfen. Die Erklärung, daß auch künftig behandelnde Ärzte/Einrichtungen Übermittlungen vornehmen dürfen, die vom Ministerium akzeptiert wurden, stellt insoweit eine Blanko-Einwilligung dar, die ich nicht für wirksam halte.

Demgegenüber vertritt das Ministerium die Auffassung, daß eine namentliche Nennung der Ärzte nicht sinnvoll sei, da diese vielfach zum Zeitpunkt der Einwilligungserklärung noch nicht für den gesamten Verlauf der Behandlung feststehen könnten, und hält es nicht für praktikabel, im Bedarfsfall eine erneute aktuelle Einwilligungserklärung einzuholen. Die Unterrichtung des Patienten, daß sich die Einwilligung auch auf künftige Behandlungsaktivitäten erstreckt, und der ausdrückliche Hinweis auf sein jederzeitiges Widerrufsrecht sollen dem Schutz seiner Interessen nach Ansicht des

---

189 vom 7. April 1994, GVBl. I S. 94

190 s. 5. Tätigkeitsbericht unter 7.3.2.3

191 s. 4. Tätigkeitsbericht unter 7.3.1.3 und 5. Tätigkeitsbericht unter 7.3.1.1

Ministeriums ausreichend Rechnung tragen. Immerhin geht auch das Ministerium nicht davon aus, daß die Erklärung zeitlich völlig unbegrenzt Geltung haben könnte. Dementsprechend hat es darauf hingewiesen, daß bei Behandlungsverläufen, die über lange Zeiträume unterbrochen werden, eine aktualisierte Einwilligungserklärung einzuholen ist.

Wie oben ausgeführt, genügen mir diese Versuche des Ministeriums, den Charakter der Blanko-Erklärung etwas abzumildern, nicht. Öffentlichen Krankenhäusern, die sich wegen entsprechender Zweifel an mich wenden würden, könnte ich nur raten, für sich eine konkretere Erklärung vom Betroffenen einzuholen.

7.2.2.7 Fragebogen für Kita-Untersuchungen

Eine Petentin machte mich auf den Fragebogen eines Gesundheitsamtes aufmerksam, der bei Kita-Untersuchungen verwendet wurde und viele Daten abfragte, die über die mit dieser Untersuchung verfolgten Zwecke hinausgingen oder in einer Vielzahl von Fällen eine Datenerhebung auf Vorrat dargestellt hätte. Die angesprochenen Fragen bezogen sich u. a. auf die Eltern und Geschwister des betroffenen Kindes sowie seine behandelnden Ärzte. Das zuständige Gesundheitsamt berief sich darauf, daß die Ausfüllung des **Fragebogen**s freiwillig sei und die Petentin ja von ihrem Recht, die Angaben zu verweigern, Gebrauch gemacht habe. Ich teile jedoch die Ansicht der Petentin, daß Behörden auch bei freiwilligen Datenerhebungen nur die für die Durchführung einer bestimmten gesetzlichen Aufgabe und eines bestimmten zu bezeichnenden Zweckes erforderlichen Daten erheben dürfen. Auch war ich bis dahin davon ausgegangen, daß die Dokumentationsbögen der Kinder- und Jugendgesundheitsdienstverordnung (KJGDV)[192] zu verwenden seien. Jedenfalls hielt ich es aber für empfehlenswert, daß ein zwischen mir und dem MASGF abgestimmtes Formular landesweit eingeführt wird.

Das MASGF signalisierte mir, sich ebenfalls für eine **landeseinheitliche Datenerhebung** einsetzen zu wollen. Inzwischen haben sich das Ministerium und die Landkreises darauf verständigt, den in der Anlage zur KJGDV vorgesehenen ärztlichen Dokumentationsbogen auch für die Kita-Untersuchungen zu verwenden, im übrigen aber für diese Fälle einen besonderen Anamnesebogen erarbeiten und mit mir abstimmen zu wollen.

8 Ernährung, Landwirtschaft und Forsten

8.1 Gesetze und Verordnungen

8.1.1 Novellierung des Tierzuchtgesetzes

Das Bundesministerium für Ernährung, Landwirtschaft und Forsten (BML) hat dem Bundesrat im Mai 1997 den Entwurf eines **Zweiten Gesetzes zur Änderung des Tierzuchtgesetzes**[193] vorgelegt. Dieses Gesetz dient insbesondere der Umsetzung der Richtlinie 94/28/EG des Rates vom 23. Juni 1994[194] über die grundsätzlichen tierzüchterischen und genealogischen Bedingungen für die Einfuhr von Tieren, Sperma, Eizellen und Embryonen aus Drittländern.

---

192 vom 25. Februar 1997, GVBl. II S. 96; s. 5. Tätigkeitsbericht unter 7.3.1.3

193 BR-Drs. 365/97

194 ABl. EG Nr. L 178 S. 66

Das Tierzuchtgesetz[195] wird u. a. um die Vorschriften der §§ 15 a und 15 b ergänzt, die das BML in die Lage versetzen, zwingenden Vorschriften des EG-Tierzuchtrechts auf dem Gebiet des innergemeinschaftlichen Verbringens sowie der Ein- und Ausfuhr durch Rechtsverordnung in nationales Recht umzusetzen.

Im Zuge der Umsetzung der o. g. Regelungen ist zu erwarten, daß eine Vielzahl personenbezogener Daten verarbeitet werden muß. Diese dürften vor allem bei der geplanten **Überwachung der Ein- und Ausfuhr von Zuchttieren, Samen, Eizellen und Embryonen** durch die zuständigen Zollstellen auf der Grundlage einer entsprechenden Rechtsverordnung gem. § 15 b Abs. 2 des Entwurfs anfallen.

Das Tierzuchtgesetz enthielt in seiner bisherigen Fassung in den §§ 19 a und b lediglich eine Regelung zur Erteilung von Auskünften bzw. zur Datenübermittlung zwischen den zuständigen Behörden. Eine ergänzende Regelung zum Datenschutz läßt auch das o. g. Änderungsgesetz vermissen, so daß ich das Ministerium für Ernährung, Landwirtschaft und Forsten (MELF) gebeten habe, sich im Bundesrat aus Gründen der Rechtssicherheit und Rechtsklarheit dafür einzusetzen, daß eine **allgemein gefaßte Regelung zum Datenschutz** in das Tierzuchtgesetz aufgenommen wird. Dazu habe ich eine Ergänzung des § 19 um einen weiteren Absatz mit folgendem Wortlaut vorgeschlagen:

> „(5) Personenbezogene Daten dürfen erhoben, verarbeitet oder genutzt werden, soweit dies durch dieses Gesetz vorgesehen oder ihre Kenntnis zur Erfüllung der Aufgaben nach diesem Gesetz oder der nach diesem Gesetz erlassenen Rechtsverordnungen für die datenverarbeitende Stelle erforderlich ist. Das Bundesministerium für Ernährung, Landwirtschaft und Forsten wird ermächtigt, mit Zustimmung des Bundesrates durch Rechtsverordnung die hiernach zu verarbeitenden Daten näher zu bestimmen. Im Falle des § 15 b Absätze 1 und 2 wird das Bundesministerium für Finanzen ermächtigt, im Einvernehmen mit dem Bundesministerium für Ernährung, Landwirtschaft und Forsten durch Rechtsverordnung die zu verarbeitenden Daten näher zu bestimmen. Im übrigen bleiben das Bundesdatenschutzgesetz und die Datenschutzgesetze der Länder unberührt."

Wie mir das MELF im Juni 1997 mitteilte, war es aus Zeitgründen nicht mehr möglich, meinen Vorschlag rechtzeitig einzubringen, so daß der Bundesrat dem Zweiten Gesetz zur Änderung des Tierzuchtgesetzes ohne eine Regelung zur Datenverarbeitung zugestimmt hat. Das MELF sagte mir jedoch zu, daß es meinen Vorschlag bei der nächsten - Anfang 1998 zu erwartenden - Novelle des Tierzuchtgesetzes aufgreifen werde.

8.1.2 Novellierung des Tierschutzgesetzes - endlich ist es soweit

[195] i. d. Fass. vom 22. März 1994, BGBl. I S. 601

Es war ein wahrhaft langwieriges Gesetzgebungsverfahren, bis der Bundesrat schließlich nach Anrufung des Vermittlungsausschusses am 27.03.1998 dem Gesetz zur Änderung des Tierschutzgesetzes zugestimmt hat[196].

[196] BR-Drs. 285/98 (Beschluß)

In der Vergangenheit[197] habe ich wiederholt darauf hingewiesen, daß im Zusammenhang mit der **zentralen Erfassung von Zirkusbetrieben** eine **gesetzliche Grundlage** für die Einrichtung des zentralen Registers und der damit verbundenen Verarbeitung personenbezogener Daten geschaffen werden muß. Nachdem der Gesetzentwurf der Bundesregierung[198] eine diesbezügliche gesetzliche Regelung vermissen ließ, ist es nun um so erfreulicher, daß mit dem § 16 Abs. 5 Satz 2 Nr. 5 Tierschutzgesetz (TierSchG) das Bundesministerium ermächtigt wird, die zentrale Erfassung aller Wanderzirkusse durch Rechtsverordnung zu regeln, um die erforderliche wirkungsvolle länderübergreifende Überwachung sicherzustellen. Dies ist durch jahrelange gemeinsame Bemühungen des MELF und meiner Behörde erreicht worden.

Des weiteren wurde das Tierschutzgesetz um eine **allgemeine datenschutzrechtliche Regelung** erweitert und das Bundesministerium ermächtigt, die Erhebung bei Dritten, Speicherung, Veränderung, Nutzung und Übermittlung personenbezogener Daten, deren Kenntnis zur Erfüllung der Aufgaben nach dem oder aufgrund des Tierschutzgesetzes notwendig ist, durch Rechtsverordnung zu regeln.

8.2 Sonstiges

8.2.1 Informationsanspruch ehemaliger LPG-Mitglieder

Von meinem Kollegen aus Sachsen bin ich auf datenschutzrechtliche Probleme im Zusammenhang mit der Datenübermittlung und Auskunftserteilung im Rahmen eines Prüfverfahrens nach § 70 Abs. 3 Landwirtschaftsanpassungsgesetz (LwAnpG)[199] hingewiesen worden.

Daraufhin habe ich beim MELF zu Verfahren der Übermittlung von Daten an Mitglieder oder ehemalige Mitglieder von Landwirtschaftlichen Produktionsgenossenschaften (LPG) im Rahmen o. g. Prüfverfahren angefragt.

Das im Rahmen des § 70 Abs. 3 LwAnpG praktizierte Verfahren der Weitergabe der Abschlußberichte an die Ämter für Landwirtschaft und die berechtigten Beschwerdeführer sowie der Abgabe der Unterlagen an die zuständige Staatsanwaltschaft bei Vorliegen entsprechender Verdachtsmomente ist aus datenschutzrechtlicher Sicht nicht zu bemängeln.

Sichergestellt werden muß allerdings, daß neben den berechtigten Beschwerdeführern, die ein Verfahren nach § 70 Abs. 3 LwAnpG in Gang gesetzt haben, auch **alle übrigen anspruchsberechtigten Mitglieder oder ehemalige Mitglieder der LPG** über die Ergebnisse einer Prüfung informiert werden bzw. die Möglichkeit erhalten, Unterlagen einzusehen. Nur so läßt sich das vom Gesetzgeber verfolgte Ziel einer effektiven Überwachung der LPGen durch ihre Mitglieder erreichen.

Die Datenübermittlungsbefugnis der obersten Landesbehörde folgt aus § 16 Abs. 1 Buchst. a i. V. m. § 13 Abs. 1 BbgDSG. Die Übermittlung der Daten an Beteiligte ist zur Erfüllung einer Aufgabe des MELF erforderlich und erfolgt für dieselben Zwecke, denen die Erhebung der Daten gedient hat. Dies folgt aus der Auslegung von § 70 Abs. 3 LwAnpG. Danach darf das Prüfungsverfahren nur eingeleitet werden, wenn der Behörde Anhaltspunkte für ein gesetzwidriges Verhalten bei der Geschäftsführung der LPG bzw. deren Nachfolgerin vorliegen. Die somit stattfindende Anlaßkontrolle hat ihren einzigen

---

197 s. 4. Tätigkeitsbericht unter 8.2 sowie 5. Tätigkeitsbericht unter 8.1.1

198 BT-Drs. 13/7015

199 i. d. Fass. vom 3. Juli 1991, BGBl. I S. 1410

Zweck darin, die Grundlagen für Anzeigen bei der Staatsanwaltschaft sowie für Verfahren nach dem Landwirtschaftsanpassungsgesetz zu schaffen, in denen es auf eine gesetzmäßige Geschäftsführung der LPG ankommt. Das Handeln der nach § 70 Abs. 3 LwAnpG tätigen Behörde im Einzelfall kann daher nur in Mitteilungen gegenüber Beteiligten bestehen, durch die diese darüber unterrichtet werden, wie die Behörde die Rechtslage einschätzt. Diese Mitteilungen müssen als Darstellung der Rechtslage auch personenbezogene Tatsachenangaben enthalten. Zweck des Prüfverfahrens nach § 70 Abs. 3 LwAnpG ist daher eine mehr oder weniger umfangreiche, jedenfalls für eine Rechtsverfolgung hinreichend aussagekräftige und damit nützliche Bekanntgabe der gewonnenen - weitgehend personenbezogenen - Informationen an die Beteiligten.

Aus den genannten Gründen habe ich dem MELF vorgeschlagen, daß nach dem Sinn und Zweck der Norm die Ergebnisse einer Überprüfung nach § 70 Abs. 3 LwAnpG allen ehemaligen LPG-Mitgliedern bekannt zu machen sind, und zwar unabhängig davon, ob sie die Mitgliedschaft gekündigt haben oder nicht, damit sie ihre Ansprüche prüfen (lassen) und ggf. durchsetzen können. Als geeignete und kostengünstige Methode der Bekanntmachung sehe ich die Versendung eines Vordrucks an, anhand dessen der Empfänger ersehen kann, daß ein Prüfbericht vorliegt und bei Bedarf Einsicht in diesen gewährt wird.

Das MELF hat meine Auffassung zum vorliegenden Problem nicht uneingeschränkt geteilt und meint, daß gesetzliche Informationspflichten - wie sie § 70 Abs. 3 LwAnpG vorsieht - in bezug auf Betriebs- oder Geschäftsdaten in den Schutzbereich der Eigentumsgarantie eingriffen. Ein Konsens konnte wegen unserer unterschiedlichen Rechtsauffassungen nicht hergestellt werden. Unterdessen hat sich das Problem erledigt, da Überprüfungen, wie sie im Rahmen der Umstrukturierungsphase seitens des Ministeriums auf der Grundlage des § 70 Abs. 3 LwAnpG vorgenommen worden sind, nicht mehr durchgeführt werden.

8.2.2 Neues Datenverarbeitungssystem zur Kontrolle der Agrarförderung

Das MELF ist mit der Bitte an mich herangetreten, ein Datenverarbeitungssystem zur Kontrolle der förderfähigen Obergrenzen im Rahmen der einzelbetrieblichen investiven Förderung nach der Verordnung (EG) Nr. 950/97[200] aus Sicht des Datenschutzes zu bewerten. Das Programm dient zur Verwaltung einzelbetrieblicher und überbetrieblicher Maßnahmen der Agrarförderung der EU durch den Europäischen Ausrichtungs- und Garantiefonds für die Landwirtschaft (EAGFL), Abt. Ausrichtung.

Mittels des Anwendungssystems zur Kontrolle einzelbetrieblicher Investitionsförderung zur Verbesserung der Effizienz der Agrarstruktur (AKIS) sollen die maximale Förderhöhe sowie die maximale Förderhäufigkeit eines einzelnen landwirtschaftlichen Unternehmens innerhalb eines bestimmten Zeitraumes anhand der gesetzlichen Anforderungen o. g. EU-Verordnung überprüft werden. Dies ist im Land Brandenburg auch gerade deshalb notwendig, weil die **Bewilligung der Fördergelder dezentral** durch die Ämter für Landwirtschaft sowie die Investitionsbank des Landes Brandenburg **erfolgt**.

Das Landesamt für Ernährung, Landwirtschaft und Forsten (LELF) als datenverarbeitende Stelle hat mir auf Wunsch die Möglichkeit gegeben, das Programm bezüglich des Umgangs mit den personenbezogenen Daten der Antragsteller in der Testphase vor Ort zu begutachten. Im Ergebnis des Besuchs Anfang Dezember 1997 konnte ich dem MELF mitteilen, daß dem Vorhaben keine datenschutzrechtlichen Belange entgegenstehen. Ich habe insbesondere die Absicht des LELF

[200] vom 20. Mai 1997; ABl. EG Nr. L 142/1

begrüßt, die **Datenerfassungsbelege** per Post und nicht, wie ursprünglich angedacht, per Fax an die jeweiligen Bewilligungsbehörden zu versenden.

8.2.3 Numerierung von Hundesteuermarken

Ein Tierschutzverein hatte angefragt, inwieweit eine Numerierung von **Hundesteuermarken**, die eine Identifizierung des Hundehalters ermöglichen würde, dem Datenschutz zuwider laufen könnte.

Dazu habe ich ausgeführt, daß der Hundehalter schon nach § 1 Abs. 1 Hundehalterverordnung[201] verpflichtet ist, dem Tier ein Halsband mit Namen und Adresse umzulegen, welches die Ermittlung des Eigentümers bei verursachten Schäden oder Gefahren ermöglicht. Diese Vorschrift scheint jedoch vielen Eigentümern offensichtlich nicht bekannt zu sein, so daß tatsächlich in vielen Fällen eine solche Namens- und Adressenangabe fehlt, obwohl ein Halsband mit Steuermarke vorhanden ist. Eine Numerierung der Steuermarken würde die **Identifizierung der Hundehalter** auf die Fälle beschränken, in denen sie erforderlich sind und so dem Gebot der informationellen Sparsamkeit Rechnung tragen.

So wünschenswert eine vereinfachte Handhabung der Hundehalterermittlung wäre, so wenig ist sie nach der momentanen Gesetzeslage ohne weiteres möglich. Ich habe dem Tierschutzverein mitgeteilt, daß die Hundesteuermarke als Beleg für die ordnungsgemäße Anmeldung des Tieres für die Hundesteuer dient. Die bei der zuständigen Stelle erhobenen und gespeicherten Daten haben den **Zweck der Einziehung der Hundesteuer** und sind somit in einem steuerrechtlichen Verfahren i. S. d. § 30 Abgabenordnung (AO)[202] bekannt geworden. Die Ermittlung eines Hundehalters über die Steuermarke würde offenbaren, wer dieses Tier zur Steuer angemeldet hat; dies wäre ein Verstoß gegen das **Steuergeheimnis**. Etwas anderes würde gelten, wenn einer der Rechtfertigungsgründe für eine Offenbarung nach § 30 Abs. 4 AO vorläge. Eine Offenbarung der Daten wäre z. B. nach § 30 Abs. 4 Satz 1 Nr. 3 AO dann zulässig, wenn der Betroffene in diese Zweckänderung eingewilligt hat. Sollte der Hundehalter bei Entrichtung der Hundesteuer bzw. bei Entgegennahme der entsprechenden Marke bereits eingewilligt haben, daß er über eine Nummer auf der Marke bei Auffinden seines Hundes als Eigentümer ermittelt wird, so wäre dies nach § 30 Abs. 4 Satz 1 Nr. 3 AO trotz der darin liegenden Zweckänderung der Datenverarbeitung zulässig. Da eine solche Möglichkeit im Sinne des Hundeeigentümers wäre und dieser sich in der Regel vermutlich damit einverstanden erklären würde, dürfte das ein durchaus gangbarer Weg sein. Dabei muß allerdings gewährleistet sein, daß sich der Eigentümer nicht schon durch die Kennzeichnung auf der Marke selbst ermitteln läßt und so unberechtigte Dritte allein durch Ablesen der "Nummer" den Eigentümer erfahren könnten. Die Entschlüsselung der Nummer durch die Behörde dürfte nur gegenüber Berechtigten, wie z. B. dem Tierheim oder den Ordnungsbehörden, erfolgen.

Schließlich ist nach § 30 Abs. 4 Nr. 2 AO eine Offenbarung möglich, wenn sie durch Gesetz ausdrücklich zugelassen ist. Die Schaffung einer gesetzlichen Regelung, die eine Eigentümerermittlung durch die Nummer auf der Hundemarke ermöglicht, wäre daher der einzige Weg, die rechtmäßige Vorgehensweise der Ermittlung an die tatsächlichen Gegebenheiten, nämlich des Vorhandenseins der Steuermarke als einziges Indiz auf den Eigentümer, anzupassen. Eine **gesetzliche Regelung**, nach der die Eigentümerermittlung lediglich über eine Nummer stattfinden kann, würde ich aus genannten Gründen sehr begrüßen. Der Zwang zur Namensetikettierung des Halsbandes ist unter dem Gesichtspunkt des Datenschutzes dagegen eher problematisch, während eine Pseudonymisierung des Hundehalters durch eine Nummer auf der Steuermarke keinen datenschutzrechtlichen Bedenken begegnen würde.

---

201 vom 22. Februar 1993, GVBl. II S. 110

202 vom 16. März 1976, BGBl. I S. 613, ber. 1977 S. 269

9 Umwelt, Raumordnung und Naturschutz

9.1 Abfall- und Altlastendatenschutzverordnung

Das nunmehr in Kraft getretene **Brandenburgische Abfallgesetz** (BbgAbfG)[203] enthält in § 40 Abs. 2 eine Verordnungsermächtigung zur spezifischen Regelung des Datenschutzes für die Bereiche Abfall, Altlasten und Bodenschutz.

Im Vorfeld der förmlichen Beteiligung gem. § 7 Abs. 2 BbgDSG hat mich das Ministerium für Umwelt, Naturschutz und Raumordnung (MUNR) zur Besprechung eines ersten Arbeitsentwurfes der Verordnung eingeladen. Dabei bestand Einvernehmen darüber, daß der Regelungsansatz und die Struktur des Verordnungsentwurfs im wesentlichen dem Erfordernis der Umsetzung der Verordnungsermächtigung nach § 40 Abs. 2 BbgAbfG entspricht. Ich habe die Gelegenheit zum Anlaß genommen, noch einmal ausdrücklich darauf hinzuweisen, daß es nach wie vor an einer bereichsspezifischen **Löschungs- bzw. Sperrungsregelung** personenbezogener Daten **in Altlasten-Verdachtsflächenkatastern** fehlt. Es muß die Möglichkeit bestehen, im Falle falsch benannter Verdachtsflächen diese aus den Katastern vollständig zu löschen sowie Verdachtsflächen, die aufgrund eines Ermittlungsergebnisses nicht als solche bestätigt werden, im Kataster zu sperren. Das MUNR hat zugesagt, die Umsetzbarkeit dieser Forderungen zu überprüfen.

9.2 Anschluß des MUNR an das Landesverwaltungsnetz

Im Berichtszeitraum führte ich eine datenschutzrechtliche **Kontrolle** gem. § 26 BbgDSG im MUNR durch. Ziel des Kontrollbesuches war, die Einhaltung der Bestimmungen des Brandenburgischen Datenschutzgesetzes beim Anschluß dieses Ministeriums an das Landesverwaltungsnetz[204] zu überprüfen. Das MUNR ist auf drei Standorte verteilt. Die lokalen Netzwerke der Standorte sind am Landesverwaltungsnetz (hier: Datenverbund der Ministerien) angeschlossen. Ein **IT-Sicherheitskonzept** existiert derzeit nur im Entwurf. Die Prüfung hat eine Reihe von beanstandungswürdigen Ergebnissen erbracht. Hervorzuheben ist:

Gebäude- und Raumsicherung

Die Gebäude- und Raumsicherungen genügen teilweise nicht den Anforderungen des Datenschutzes. Weiterhin existierten keine **Zutrittsregelungen zu den Server- und Verteilerräumen**, so daß Behördenfremde, z. B. auch Mitarbeiter des Vermieters, unkontrolliert Zugang zu Technikräumen erhalten. Ich habe u. a. den **Einbau von Sicherheitstüren** und die **Erstellung einer Dienstanweisung** zur Regelung von Zutrittsbefugnissen für alle Technikräume gefordert.
Die meisten Technikräume waren mit einem Schild **„Technikraum, Zutritt nicht gestattet"** gekennzeichnet. Hier habe ich die umgehende Entfernung dieser Hinweisschilder gefordert, da man potentielle Täter nicht auf Räume mit sicherheitsrelevanter Technik hinweisen sollte.

---

203 vom 6. Juni 1997, GVBl. I S. 40; s. 5. Tätigkeitsbericht unter 9.1

204 s. unter 1.4.1

Dateibeschreibungen

Zur Vorbereitung der Kontrolle sind vom MUNR die Dateibeschreibungen gem. § 8 BbgDSG angefordert worden. Folgende Dateibeschreibungen wurden mir übersandt:

- Erfassung der Bewerber bzw. wahrgenommener Aus- und Fortbildungen,

- Überprüfung der Zuverlässigkeit zum Schutz gegen Entwendung oder erheblicher Freisetzung radioaktiver Stoffe nach § 12 b Atomgesetz (AtG)[205],

- Stellenübersicht.

Während der Prüfung stellte sich heraus, daß die Dateibeschreibungen teilweise nicht dem aktuellen Stand entsprachen. Für einige Anwendungen fehlten die Dateibeschreibungen. Ich forderte das MUNR daraufhin auf, die Dateibeschreibungen zu erstellen bzw. zu aktualisieren.

Abschottung der lokalen Netzwerke des MUNR vom Landesverwaltungsnetz

In den lokalen Netzen des MUNR werden teilweise sensible personenbezogene Daten verarbeitet. Aus diesem Grund ist es zwingend erforderlich, die lokalen Netze mit Hilfe von **Firewallsystemen** gegenüber dem Landesverwaltungsnetz abzuschotten, da ein unberechtigter Zugriff auf die Daten der lokalen Netze sonst nicht ausgeschlossen werden kann. Einige Firewall-Systeme bieten auch die Möglichkeit der Verschlüsselung von Daten auf dem Übertragungsweg. Bei Nutzung dieser Funktionalität kann auch ein gewisser Grundschutz beim Datenaustausch zwischen den drei Standorten des MUNR realisiert werden.

Konfiguration und Administration der Router

Die drei lokalen Netzwerke des MUNR werden jeweils über einen Router mit dem Landesverwaltungsnetz verbunden. Bei zwei der drei Routern besteht die Möglichkeit, Datenpakete zu filtern.

Bei den meisten Routern kann mit Hilfe von **Filterregeln** festgelegt werden, welcher Benutzer bzw. welches Netzwerk welchen Netzwerkdienst in welcher Richtung nutzen darf. Der folgende Auszug aus der Konfigurationsdatei eines Routers soll diesen Sachverhalt verdeutlichen:

Nr.	Protokoll	Quelladresse	Zieladresse	Operator	Port
1	TCP	127.219.3.0	127.219.4.10	gleich	80

[205] i. d. Fass. vom 15. Juli 1985, BGBl. I S. 1565; zul. geänd. durch Ges. vom 19. Juli 1996, BGBl. I S. 1019 (BGBl. III 751-1)

Nach diesem Eintrag können alle Rechner des Netzwerkes 127.219.3.0 auf den Rechner mit der IP-Adresse 127.219.4.10 zugreifen und den Dienst am Port 80 (hier: WWW) nutzen[206].

In der Konfigurationsdatei eines Routers waren eine ganze Reihe von Filterregeln definiert. Während der Prüfung konnte die Erforderlichkeit nicht aller Filterregeln geklärt werden. Ich habe deshalb die Erstellung einer Dokumentation gefordert, aus der ersichtlich wird, welche Filterregeln für welchen Zweck genutzt werden.

Weiterhin konnte auch nicht geklärt werden, welche sicherheitsrelevanten Funktionen die Router zur Verfügung stellen. So ermöglichen z. B. einige Router die Protokollierung unberechtigter Zugriffe. Auch hier habe ich gefordert, daß die vorhandenen Sicherheitsmechanismen der Router „erkundet" und - wenn vorhanden - auch genutzt werden.

In einem Standort wurde ein Router ohne Filterfunktionen eingesetzt. Ich habe gefordert, daß dieser Router durch einen neuen ersetzt wird, der eine Filterung von Datenpaketen ermöglicht.

Administration der Netzwerkserver

Die Systemverwalter der drei Standorte vertreten sich gegenseitig. Aus diesem Grund sind ihnen die Paßwörter aller Server bekannt. Allerdings existiert eine Dienstanweisung zur Administration der Server nicht.

Kritisch anzumerken ist dabei, daß im Vertretungsfall eine Anmeldung an einen Server eines anderen Standortes über das Landesverwaltungsnetz hinweg erfolgt. Die **Systemverwalter-Paßwörter** werden dabei unverschlüsselt übertragen und können daher von Unbefugten leicht abgehört werden. Ist ein potentieller Angreifer jedoch im Besitz der Systemverwalterpaßwörter, so hat er auch Zugriff auf alle sensiblen Daten des jeweiligen Servers. Ich habe daher gefordert, daß **Benutzerkennungen und Paßwörter** während der standortübergreifenden Administration nur **verschlüsselt übertragen** werden. Auch hier würde sich der Einsatz einer Firewall anbieten (s. weiter oben). Über einen verschlüsselten Kanal könnten die Daten sicher zwischen den lokalen Netzen der drei Standorte übertragen werden.

Von einem Systemverantwortlichen wurden zusätzlich auch die Server des Landesumweltamtes administriert. Hierzu habe ich gefordert, daß in einer Dienstanweisung die Verantwortlichkeiten bezüglich des Datenschutzes und der Datensicherheit klar geregelt werden.

Protokollierung von Nutzeraktivitäten auf den WWW-Servern

Auf den WWW-Servern[207] des MUNR wurden Aktivitäten der Nutzer in Protokolldateien gespeichert. Die Speicherung dieser personenbezogenen Daten ist unzulässig, da die Mitarbeiter nicht in die Speicherung ihrer personenbezogenen Daten eingewilligt haben.

Solange die Daten in den Protokolldateien nicht anonymisiert gespeichert werden, habe ich die vollständige Deaktivierung der Protokollfunktion auf den WWW-Servern gefordert.

---

206 Hiweis: Die IP-Adressen wurden geändert.

207 s. auch 1.4.1.4

„Atom-PC“

Auf einem Arbeitsplatzcomputer (APC) wurden Daten von Personen verarbeitet, die mit dem Umgang oder der Beförderung von radioaktiven Stoffen gem. § 12 b AtG in Verbindung stehen. Als Sicherheitsmaßnahme wurde der Paßwortschutz beim Booten aktiviert. Dieser Schutz reicht bei der Verarbeitung sensibler personenbezogener Daten nicht aus. Ich habe daher die Nachrüstung des APC mit entsprechender **Sicherheitssoftware** gefordert.

Einsatz von Notebooks

Aus der Grundschutzanalyse des MUNR geht hervor, daß sich derzeit zwei Notebooks im Einsatz befinden. Während der Prüfung konnte nicht abschließend geklärt werden, wo sich diese Geräte befinden und ob ggf. personenbezogene Daten darauf gespeichert werden. Aufgrund der erhöhten Risiken, die beim Einsatz transportabler Rechner entstehen (z. B. Verlust, Diebstahl) sollte man den Verbleib dieser Geräte dokumentieren. Werden auf den Notebooks personenbezogene Daten verarbeitet, sind diese ebenfalls mit entsprechender **Sicherheitssoftware** nachzurüsten.

Keine Fernwartung von ADV-Systemen

Aus Sicherheitsgründen wird im MUNR grundsätzlich auf eine Fernwartung von ADV-Systemen verzichtet. Diese datenschutzfreundliche Haltung unterstütze ich ausdrücklich, da der Schutz von personenbezogenen Daten bei der Fernwartung nur mit sehr großem Aufwand sichergestellt werden kann.

In seiner Stellungnahme hat das MUNR signalisiert, alle angesprochenen Mängel bis spätestens Ende 1998 abzustellen.

10 Stadtentwicklung, Wohnen und Verkehr

10.1 Bau- und Wohnungswesen

10.1.1 Mietspiegel

Zum Ende des Jahres 1997 ist in den neuen Bundesländern mit dem Gesetz zur Regelung der Miethöhe (MHG)[208] das Mietenüberleitungsgesetz[209] außer Kraft getreten. Nach § 2 Abs. 5 MHG sollen Gemeinden, „soweit hierfür ein Bedürfnis besteht und dies mit einem für sie vertretbaren Aufwand möglich ist, Mietspiegel erstellen“. Datenschutzrechtlich zu hinterfragen war, wie die **Mietspiegelerstellung** im Land Brandenburg durchgeführt werden würde, ob hierbei die Verarbeitung von personenbezogenen Daten geplant war und ob an die Beauftragung von Auftragnehmern gedacht sei.

Um mir hierüber ein Bild zu verschaffen, hatte ich Mitte 1997 die **Landkreise und kreisfreien Städte** angeschrieben und sie gebeten, mir hierzu Auskünfte zu geben. Bis auf einen haben mich alle Angesprochenen über den Stand ihrer Vorhaben informiert. Danach ist das Vorgehen in Brandenburg sehr unterschiedlich. Teilweise übernehmen öffentliche Stellen die Aufstellung von Mietspiegeln, häufig von Mieter- und Vermieterverbänden und Wohnungsunternehmen unterstützt. Teilweise findet eine Funktionsübertragung statt, wobei eine private Stelle die gesamte Durchführung in eigener

[208] vom 18. Dezember 1974, BGBl. I S. 3603; zul geänd. durch Änderungsgesetz vom 15. Dezember 1995, BGBl. I S. 1722

[209] vom 6. Juni 1995, BGBl. I S. 748

Verantwortung unter Bindung an einen Werkvertrag übernimmt. Auch an Auftragsdatenverarbeitung war gedacht worden.

Aus den mir zur Verfügung gestellten Unterlagen konnte ich erfreulicherweise feststellen, daß wohl in den meisten Fällen keine personenbezogenen Datenerhebungen vorgenommen werden und außerdem auf eine Auskunftspflicht verzichtet wurde.

Formal stellen sich Mietspiegel wie Kommunalstatistiken dar, die **Bezugsgrößen für Vergleichsmieten** liefern sollen, um eine Übersicht über ortsübliche Mieten erhalten zu können. Im statistik- und datenschutzrechlichen Sinn handelt es sich hierbei aber nicht um Statistiken. Denn Statistiken könnten ebenfalls im örtlichen statistischen Jahrbuch veröffentlicht werden. Bezeichnenderweise findet sich aber der Begriff der Statistik im Miethöhegesetz nicht. Denn Daten, die zu statistischen Zwecken erhoben werden, dürfen auch nur für statistische Zwecke genutzt werden und nicht zu Zwecken des Verwaltungsvollzuges oder zur Abgeltung privater Rechtsansprüche. Auf dieses Nachteilsverbot weist auch das sog. Volkszählungsurteil[210] nachdrücklich hin. Deshalb sind Daten über ortsübliche Mieten, wie sie der Mietspiegel enthält, nicht mehr und nicht weniger als „eine Übersicht über die üblichen Entgelte ... in der Gemeinde oder in einer vergleichbaren Gemeinde, soweit die Übersicht von der Gemeinde oder von Interessenvertretern der Vermieter und der Mieter gemeinsam erstellt oder anerkannt worden ist (Mietspiegel) ..." (§ 2 Abs. 2 MHG).

10.1.2 Kommunales Vorkaufsrecht - welche Daten braucht die Gemeinde?

Gemäß § 28 Abs. 1 Baugesetzbuch (BauGB)[211] ist den Gemeinden der Inhalt eines Grundstückskaufvertrages mitzuteilen, damit die Gemeinden nachprüfen können, ob sie beabsichtigen, ihr **Vorkaufsrecht** für das betreffende Grundstück geltend zu machen. Zu diesem Zweck ist es Praxis, den gesamten Kaufvertrag der Gemeinde zur Verfügung zu stellen und damit neben den Grundstücksdaten - Lage, Größe, Kaufpreis - auch die persönlichen Daten von Käufer und Verkäufer - Name, Anschrift, ggf. Bankverbindung - zu offenbaren, die dann natürlich bei der betreffenden Gemeinde gespeichert werden. Diesem bisherigen Verfahren kann ich aus datenschutzrechtlicher Sicht nicht zustimmen.

Datenschutzgerecht ist es hier, ein **abgestuftes Verfahren** einzuführen, in dem der Gemeinde in der ersten Stufe nur die Grundstücksdaten mitgeteilt werden. Beabsichtigt die Gemeinde daraufhin ihr Vorkaufsrecht auszuüben, sind in einer weiteren Stufe die personenbezogenen Daten von Käufer und Verkäufer mitzuteilen. Erst zu diesem Zeitpunkt würde auch die Frist des § 28 Abs. 2 BauGB zur Ausübung des Vorkaufrechts in Gang gesetzt.

---

210 vom 15. Dezember 1983, BVerfGE 65, 62

211 vom 23. Juni 1960, BGBl. I S. 341, i. d. Fass. vom 27. August 1997, BGBl. I S. 2141

Der § 28 Abs. 1 BauGB ist deshalb nach meiner Ansicht so auszulegen, daß nur das vorgeschlagene, und in verschiedenen anderen Bundesländern bereits langjährig erfolgreich praktizierte, Zweistufenverfahren einen effektiven Grundrechtsschutz gewährleistet. Diese von mir vertretene Auffassung wird auch von der Notarkammer des Landes Brandenburg und dem Ministerium für Stadtentwicklung, Wohnen und Verkehr (MSWV) geteilt. Ich hatte vorgeschlagen, durch ein entsprechendes Rundschreiben des MSWV das Zweistufenverfahren in den Gemeinden einzuführen. Die Umsetzung dieses Vorhabens scheiterte jedoch an der abweichenden Auffassung des Ministeriums des Innern (MI). Dort wird die Ansicht vertreten, daß die bisherige Praxis den geltenden rechtlichen Anforderungen entspreche, es den Gemeinden aber gleichwohl freigestellt sei, sich des Stufenverfahrens zu bedienen. Auch durch mehrmaligen Informationsaustausch mit dem MI konnte eine Übereinstimmung in den Ansichten nicht herbeigeführt werden. In dem zwischenzeitlich veröffentlichten Rundschreiben[212] ist es deshalb bedauerlicherweise den Gemeinden entsprechend der Ansicht des MI freigestellt, ob die Datenerhebung wie bisher einstufig oder entsprechend meines Vorschlages abgestuft erfolgt.

10.1.3 Verwaltungsvorschrift zu Planungsunterlagen für Bauleitpläne u. ä.

Immer wieder wurde ich in der Vergangenheit mit Unsicherheiten der Kommunen konfrontiert, die sich auf die **Übermittlung personenbezogener Daten zwischen Gemeindeverwaltung und Gemeindevertretung** bezogen. Besonders relevant erschien hier der Punkt, ob die Gemeindeverwaltungen personenbezogene Daten, die ihr bei der Entgegennahme von Bedenken und Anregungen zu nach § 3 Abs. 2 BauGB ausgelegten Bauleitplänen bekannt geworden sind, an die Gemeindevertretung weitergeben dürfen. Diese Frage wurde bislang auch im Kreise der Datenschutzbeauftragten der Bundesländer zum Teil kontrovers diskutiert. In Zusammenarbeit zwischen dem MI, dem MSWV und meiner Behörde wurde Einvernehmen zu folgender Problemlösung erzielt:

Bei dem Datenaustausch im oben geschilderten Fall handelt es sich nicht wirklich um eine Datenübermittlung zwischen zwei Parteien. Richtig ist hier, daß der eigentliche Adressat der Anregungen und Bedenken der Bürger die Gemeindevertretung ist[213]. Die **Gemeindeverwaltung** fungiert hier also nur als „Poststelle", die nach Eingang der Bürgermeinungen diese an die Gemeindevertretung weitergibt, wo diese dann beim Abwägungsvorgang berücksichtigt werden. Die **Gemeindevertretung** als Adressat der Anregungen und Bedenken ist dann auch befugt, die darin enthaltenen personenbezogenen Daten zur Kenntnis zu nehmen.

Bei dieser Vorgehensweise werden die datenschutzrechtlichen Belange dadurch gewahrt, daß die Gemeindeverwaltung die nach § 3 Abs. 2 BauGB vorgebrachten Anregungen und Bedenken unter Kennziffern, die aus sich selbst heraus nicht personenbeziehbaren sind, aufbereitet. Der Gemeindevertretung wird dann zusammen mit den entsprechenden Unterlagen eine Liste zugeleitet, die eine Zuordnung der Kennziffern zu bestimmten Personen erlaubt. Vorteil dieser Verfahrensweise ist, daß die Bauplanungsunterlagen anderen Verfahrensbeteiligten ohne weiteren Verwaltungsaufwand in anonymisierter Form (nur mit Kennziffern versehen) zur Verfügung gestellt werden können.

---

212 Rundschreiben des MSWV zum Datenschutz im Verfahren nach § 3 Abs. 2, § 4 und § 28 Baugesetzbuch (BauGB) vom 29. September 1997 (hier: Ziff. III), ABl. S. 904

213 BVerfGE 77, S. 288 ff

Um zukünftig weitere Unsicherheiten und Nachfragen in dieser Sache zu vermeiden, wurde auf meine Anregung hin die geschilderte gemeinsame Auffassung in einem vom MSWV veröffentlichten Rundschreiben[214] an die Kommunen herangetragen.

10.1.4 Bereichsspezifische Datenschutzregelung in der Bauordnung

Die Landesregierung hat im Berichtszeitraum die Novellierung der Landesbauordnung vorbereitet und den erarbeiteten Entwurf dem Landtag zugeleitet, ohne mich zuvor - wie vom Gesetzgeber gem. § 7 Abs. 2 BbgDSG vorgegeben - beteiligt zu haben. Die Änderung der Brandenburgischen Bauordnung (BbgBauO) ist mit Art. 1 des Gesetzes zur Änderung der Brandenburgischen Bauordnung und anderer Gesetze[215] erfolgt und zum 01.01.1998 in Kraft getreten.

Die bereichsspezifische Regelungen zum Datenschutz in § 91 BbgBauO (neu) richten sich in der Wortwahl nicht stets nach dem BbgDSG, sondern auch nach dem BDSG. Es finden sich außerdem zahlreiche Begriffe, die einzufügen nicht erforderlich gewesen wären. Dennoch stellt die Regelung insgesamt eine abgestufte, in der Praxis umsetzbare gesetzliche Bestimmung - mit der ausdrücklichen Ergänzung in Abs. 6 - dar, daß „im übrigen" die Vorschriften des Brandenburgischen Datenschutzgesetzes gelten.

Innerhalb der Datenschutzvorschrift sind nicht nur die Betroffenen (Bauherren), sondern auch „Beteiligte" mit angesprochen, die in §§ 57 bis 62 BbgBauO definiert sind, sowie weitere am Bau beteiligte Personen, wie z. B. Nachbarn und betroffene Grundstückseigentümer. Aus der Sicht des Datenschutzes ist es fraglich, inwieweit dem Landesgesetzgeber die Kompetenz zusteht, Angelegenheiten, die den Datenschutz nicht-öffentlicher Stellen betreffen, zu regeln, es sei denn, daß davon ausgegangen werden kann, daß es sich insoweit nur um Verfahrensfragen handelt, durch die das Vorgehen der beteiligten öffentlichen Stellen vorgegeben wird.

10.2 Verkehr

10.2.1 Datenverarbeitung im Vollzug der Landesschiffahrtsverordnung

Aufgrund der jüngst bundesrechtlich vorgeschriebenen Registrierung von Wasserfahrzeugen können nunmehr auch Verstöße, wie z. B. Nichteinhaltung der zulässigen Höchstgeschwindigkeit, verfolgt werden. Damit stellt sich datenschutzrechtlich die Frage einer Zulässigkeit der Übermittlung von Haltern durch Landkreise und Kommunen an die Polizei.

---

214 Rundschreiben des MSWV zum Datenschutz im Verfahren nach § 3 Abs. 2, § 4 und § 28 Baugesetzbuch (BauGB) vom 29. September 1997 (Ziff. II), ABl. S. 904

215 vom 18. Dezember 1997, GVBl. I S. 124

Gemäß § 23 Nr. 2 Buchst. e Ordnungsbehördengesetz (OBG)[216] i. V. m. § 43 Abs. 3 Nr. 1 Brandenburgisches Polizeigesetz (BbgPolG)[217] dürfen der Wasserschutzpolizei auf Anfrage personenbezogene Daten, wie o. g. Halterdaten, übermittelt werden. Die Auffassung wurde auch vom zuständigen Fachministerium geteilt. Aus Gründen der Rechtsklarheit für den Bürger habe ich jedoch dem MSWV empfohlen, zukünftig eine entsprechende Regelung in der Landesschiffahrtsverordnung (LSchiffV)[218] selbst vorzusehen. An den Bundesbeauftragten für den Datenschutz habe ich mich mit der Bitte gewandt, auch im bundesrechtlichen Bereich auf eine derartige klarstellende Regelung hinzuweisen.

10.2.2 Fahrerlaubnisverordnung

Als Umsetzung der Zweiten EU-Führerscheinrichtlinie[219] und als Ausführungsbestimmung zum Gesetz zur Änderung des Straßenverkehrs und anderer Gesetze[220] beabsichtigt das Bundesministerium für Verkehr eine Fahrerlaubnis-Verordnung (FeV) zu erlasssen.

Bereits in meinem 4. Tätigkeitsbericht[221] habe ich meine grundsätzlichen Bedenken gegen dieses Vorhaben dargestellt. Daran hat sich auch zwischenzeitlich nichts geändert. Nun soll die geplante Verordnung noch in dieser Legislaturperiode erlassen werden. Zu diesem Zweck wurde im März 1998 ein Referentenentwurf vorgelegt, der aus datenschutzrechtlicher Sicht zu bewerten war. Dies geschah angesichts der Zeitvorgabe seitens des Ministeriums in einem gemeinsamen Fachgespräch der Landesbeauftragten und des Bundesbeauftragten für den Datenschutz. Neben den schon in der Vergangenheit geäußerten Bedenken zeigte sich, daß insbesondere bei der Datenabrufmöglichkeit durch die Landesbehörden aus dem neu zu schaffenden **Fahrerlaubnisregister** bzw. dem **Verkehrszentralregister** eine ausreichende Sicherheit auf dem Übermittlungsweg wegen fehlender und auch zukünftig nicht vorgesehener Verschlüsselung der Daten nicht gewährleistet ist. Weiter ist nicht in vollem Umfang die Trennung beider Register durchgeführt worden, so daß „im Bedarfsfall" eine Bezugnahme unaufwendig möglich ist.

---

216 vom 21. August 1996, BGBl. I S. 266

217 vom 19. März 1996, GVBl. I S. 74

218 vom 9. August 1996, GVBl. II S. 619, geänd. durch Erste Verordnung zur Änderung der Landesschiffahrtsverordnung vom 24. November 1997, GVBl. II S. 881

219 Richtlinie 91/439/EWG des Rates vom 29. Juli 1991, EG ABl. L 237 S. 1; zul. geänd. durch RL 97/26/EG vom 2. Juni 1997, EG ABl. L S. 41

220 BR-Drs. 94/97

221 s. unter 10.1 ff.

11 Finanzen und Wirtschaft

11.1 Finanzen

11.1.1 Gesetze und Verordnungen

11.1.1.1 Automation in der Steuerverwaltung

Im Frühjahr 1996 wurde ich vom Ministerium der Finanzen (MdF) über einen vorliegenden Entwurf zur Steueranmeldungs-Datenübermittlungs-Verordnung (StADÜV) informiert. Sinn dieser Verordnung ist es, dem Steuerpflichtigen zu ermöglichen, bestimmte **Steueranmeldungen auf maschinell verwertbaren Datenträgern** oder über Datenfernübertragung zu übermitteln. Problematisch aus datenschutzrechtlicher Sicht ist hier § 13 der Verordnung. Dieser beinhaltet bisher nur die Ankündigungen, die Einzelheiten des technisch zu realisierenden Datenschutzes in einem die Verordnung begleitenden Schreiben des Bundesfinanzministeriums zu regeln. Dieses Schreiben liegt bisher nicht vor. Es liegt jedoch die Versicherung vor, das Schreiben zeitgleich mit Inkrafttreten der Verordnung zu veröffentlichen. Das MdF hat mir zugesagt, sofort nach Erhalt des Schreibens oder eines Entwurfs, dieses bzw. diesen zur Stellungnahme an mich weiterzuleiten.

11.1.1.2 Arztgeheimnis contra Steuererhebung

Ab 1998 soll die Regelung zum Tragen kommen[222], daß **Fahrtenbücher** von Ärzten nur dann als ordnungsgemäß aus Sicht der Steuerbehörden gelten, wenn bei Hausbesuchen Name und Anschrift der aufgesuchten Patienten vermerkt werden. Nach meiner Meinung, die auch nahezu einhellig von den Datenschutzbeauftragten der Länder und des Bundes vertreten wird, ist die Nennung von Patientennamen im Fahrtenbuch der Ärzte nicht mit geltenden Rechtsvorschriften vereinbar. Sie verletzt das **Arztgeheimnis**. Durch die Neuregelung sollen Ärzte nunmehr auf der Grundlage des § 102 Abs. 1 Nr. 3 b Abgabenordnung (AO)[223] zu Angaben verpflichtet werden, zu deren Preisgabe sie nach dem wortgleichen § 53 Abs. 1 Nr. 3 StPO nicht verpflichtet sind[224]. Mit der Offenbarung von Name und Anschrift eines Patienten gerät der Arzt in einen strafrechtlich relevanten Bereich.

Meiner Ansicht will sich das MdF auch nach intensivem Schriftwechsel nicht anschließen. Zwischen den Datenschutzbeauftragten sowie den auf Landes- oder Bundesebene zuständigen Ministerien besteht hier z. Z. weiter ein offener Dissens. Da ein weiterer Meinungsaustausch auf Landesebene hier nicht zu einer Lösung führen kann, bleibt die auch von mir begleitete Lösung des Problems der Bundesebene vorbehalten.

Der Konflikt zwischen Arztgeheimnis auf der einen Seite und dem Bemühen der Finanzverwaltung um effektive Aufgabenerfüllung auf der andern Seite besteht auch in folgendem Fall:

Wenn durch das Finanzamt Außenprüfungen in Arztpraxen vorgenommen werden, so wird dort auch Einsicht in Unterlagen genommen, aus denen u. a. Patientennamen und - anschriften hervorgehen. Nach meiner Ansicht dürfen diese Angaben dem Finanzamt aber nicht offenbart werden, da auch Patientenname und -anschrift in den geschützten Bereich

---

222 Schr. BMF an Bundesärztekammer vom 1. August 1997 - IV B 2 - S 2145 - 80/97 (Fahrtenbuchführung durch Ärzte)

223 vom 16. März 1976, BGBl. I S. 613

224 BGHSt 33, 148, 151

der ärztlichen Schweigepflicht fallen und ihre Offenbarung gem. § 203 Abs. 1 Nr. 2 Strafgesetzbuch (StGB)[225] grundsätzlich strafbewehrt ist. Deshalb ist auch bei der Auslegung des Auskunftsverweigerungsrechts gem. § 102 Abs. 1 AO derselbe Maßstab anzulegen. Dies bedeutet, daß die Offenbarung von Patientennamen und -anschriften auch im Rahmen des Auskunftsverweigerungsrechts abgelehnt werden kann. Eine Berechtigung der Finanzämter zur Einsichtnahme in Dokumente mit **personenbezogenen Patientendaten** ohne vorherige Anonymisierung besteht nicht.

Die Finanzverwaltung steht bundesweit auf dem Standpunkt, daß der § 102 AO die Offenbarung von Patientennamen und -anschriften zuläßt. Ein Konsens ist nicht in Sicht.

11.1.2 Sonstiges

11.1.2.1 Homosexualität - ein erhöhtes Versicherungsrisiko?

Im Rahmen der Zusammenarbeit mit den Datenschutzbeauftragten der anderen Bundesländer wurde ich informiert, daß einige Lebensversicherungsunternehmen bei Abschluß von Versicherungsverträgen die geschlechtliche Orientierung der zukünftigen Versicherungsnehmer erfragen, um dann bei Homosexuellen den Vertragsschluß abzulehnen oder das Versicherungsrisiko wegen möglicher HIV-Infektion höher einzuschätzen.

[225] vom 15. Mai 1871 (RGBl. S. 127), i. d. Fass. vom 10. März 1987, BGBl. I S. 945

Angaben über das Geschlechtsleben sind besonders zu schützende sensible personenbezogene Daten aus dem Intimbereich einer Person. Dies findet auch Ausdruck in Artikel 8 Absatz 1 EU-Datenschutzrichtlinie (EU-DSRL)[226]. Die nach Artikel 8 Abs. 2 - 4 EU-DSRL zugelassenen Ausnahmen vom Erhebungsverbot derartiger Daten sind hier nicht anwendbar. Die Erhebung dieser Daten ist damit in den genannten Fällen rechtswidrig.

Eine Befragung bei den öffentlich-rechtlichen Versicherern in meinem Zuständigkeitsgebiet hat ergeben, daß im Land Brandenburg eine Erhebung solcher Daten beim Abschluß eines Versicherungsvertrages aus o. g. Gründen nicht erfolgt.

11.1.2.2 Information über wettbewerbsrechtliche Bußgeldbescheide durch die Landeskartellbehörde

Durch einen Hinweis des Landesbeauftragten für den Datenschutz Niedersachsen wurde ich darauf aufmerksam gemacht, daß die Landeskartellbehörden andere Behörden über **wettbewerbsrechtliche Bußgeldbescheide** informieren. Dies geschieht z. B., damit diese Informationen in laufenden oder beabsichtigten Ausschreibungen berücksichtigt werden. Auf meine Nachfrage wurde mir vom Ministerium für Wirtschaft, Mittelstand und Technologie (MWMT) mitgeteilt, daß diese Praxis auch im Land Brandenburg grundsätzlich befürwortet wird, es sei aber innerhalb des letzten Jahres nicht zum Erlaß eines wettbewerbsrechtlichen Bußgeldbescheides und damit auch nicht zu einer derartigen Datenübermittlung gekommen.

In meiner datenschutzrechtlichen Bewertung habe ich darauf hingewiesen, daß es derzeit keine Rechtsgrundlage für die Weitergabe der Bußgeldbescheide gibt. Das MWMT teilt diese Ansicht. Dem Mangel wird allerdings mit dem Inkrafttreten des Justizmitteilungsgesetzes[227] am 1. Juni 1998 mit dem neu eingefügten § 49 a Abs. 2 Ordnungswidrigkeitengesetz (OWiG)[228] und § 17 Nr. 3 Einführungsgesetz zum Gerichtsverfahrensgesetz (EGGVG)[229] abgeholfen werden.

11.1.2.3 Steuernummern von Mitgliedern der Handwerkskammern

Bereits in meinen früheren Tätigkeitsberichten[230] habe ich über die Praxis der Industrie- und Handelskammern (IHK) berichtet, zur Festsetzung der Kammerbeiträge bei ihren Mitgliedern die Steuernummer zu erfragen, ohne auf die Freiwilligkeit einer solchen - durchaus sinnvollen - Angabe hinzuweisen.

Seit Januar 1998 stellt sich dieses Problem auch bei den Handwerkskammern des Landes Brandenburg. Ich habe das MWMT darauf hingewiesen, daß hier genauso zu verfahren sei wie im Falle der IHK, da die Parallelität der Steuernummererhebung eine gleiche datenschutzrechtliche Bewertung erfordert. Das MWMT nahm dies zum Anlaß, an die Handwerkskammern heranzutreten und sie zu einer entsprechenden Anpassung der Erhebungsbögen an die von mir dargestellte Rechtslage aufzufordern. Noch Mitte vergangenen Jahres teilte mir das Ministerium mit, daß in den von den Kammern verwendeten Schreiben und Erhebungsbögen zukünftig auf die Freiwilligkeit der erbetenen Angabe zur Steuernummer hingewiesen werde.

---

226 vom 24. Oktober 1995, EU-ABl. Nr. L 281/31

227 vom 18. Juni 1997, BGBl. S. 1430

228 i. d. Fass. vom 19. Februar 1987, BGBl. I S. 602; zul. geänd. durch Art. 2 2. Zwangsvollstreckungsnovelle vom 17. Dezember 1997 (BGBl. III/FNA 454-1)

229 vom 27 Januar 1877, RGBl. S. 77 (BGBl. III 300-1)

230 s. 3. Tätigkeitsbericht unter 10.1 und 4. Tätigkeitsbericht unter 11.2

11.1.2.4 Feststellung der Stundungsvoraussetzung bei Realsteuer- und Kommunalabgabenschulden

Die Eingabe eines Bürgers im Zusammenhang mit der von ihm beantragten Stundung von Grundsteuern machte mich auf die Gestaltung der dafür von den Landkreisen und kreisfreien Städten verwendeten Antragsformulare aufmerksam. Die Antragsteller werden darin zur umfassenden Offenlegung ihrer wirtschaftlichen Verhältnisse aufgefordert, da ansonsten der Stundungsantrag nicht beschieden werden kann. Ich habe festgestellt, daß in den sonst inhaltlich nicht zu beanstandenden Antragsformularen regelmäßig der Hinweis auf § 12 Absatz 3 BbgDSG fehlte. Danach ist der Antragsteller darauf hinzuweisen, daß ohne eine Offenbarung der wirtschaftlichen Verhältnisse über die beantragte Stundung nicht entschieden werden kann.

Daraufhin habe ich alle Landkreise und kreisfreien Städte des Landes Brandenburg aufgefordert, die Formulare nachzubessern. Inzwischen haben mir alle angeschrieben Behörden die geänderten Formulare zur Begutachtung vorgelegt. Meine Prüfung ergab, daß nunmehr den Belangen des Datenschutzes ausreichend Rechnung getragen ist.

11.1.2.5 Geltendmachen von Werbungskosten für Bildungsreisen

Die Finanzämter sind angewiesen, den Steuerpflichtigen aufzufordern, **Mitteilung über Namen und Anschriften der** übrigen **Reiseteilnehmer** zu machen, wenn diese für Auslandsbildungsreisen Werbekosten gem. § 9 Einkommenssteuergesetz (EStG)[231] oder Betriebskostenausgaben gem. § 4 Abs. 4 EStG geltend machen. Nach Meinung der Finanzverwaltung ist diese Anweisung der Oberfinanzdirektion erforderlich, um die Einheitlichkeit in der Besteuerung aller Reiseteilnehmer zu erreichen und um aus der Zusammensetzung der Reiseteilnehmer auf den beruflichen Anlaß der Reise schließen zu können.

Nach meiner Auffassung ist die Erhebung der Daten der Reiseteilnehmer nicht erforderlich. Zum einen existieren in den Richtlinien der Finanzbehörden eine **Vielzahl andere Kriterien, um die Besteuerungsgrundlagen** zu ermitteln. Zum anderen ist für den o. g. Zweck durchaus ausreichend, die Reiseteilnehmer ohne Namens- und Anschriftennennung nur durch Angabe ihrer Berufsgruppen auszuweisen. Die Erhebung personenbezogener Daten würde das Grundrecht der Betroffenen auf informationelle Selbstbestimmung verletzen, da sie für den beabsichtigten Zweck nicht geeignet sind. Dies zeigt sich bereits daran, daß keineswegs jeder Reiseteilnehmer die Ausgaben steuerlich geltend macht. Insoweit ist es auch nicht sicher, daß dessen Daten zur Gewährleistung der allgemeinen Steuergerechtigkeit benötigt werden. Insoweit stellt die Datenspeicherung eine Bevorratung dar, die auch hier als unzulässig angesehen werden muß.

Im übrigen ist es auch für den Steuerpflichtigen kaum möglich, im nachhinein die geforderten Daten bei den anderen Reiseteilnehmern zu erheben.

Wenn in dieser Frage auch der grundlegende Dissens zwischen dem MdF und mir nicht beigelegt werden konnte, erfolgte doch insoweit eine Annäherung der Positionen, als zukünftig die Finanzämter angewiesen werden, die in Rede stehenden Daten direkt bei den Reiseunternehmen zu erheben.

11.1.2.6 Veröffentlichung strafbewehrter Unterlassungserklärungen

Durch eine Petition wurde mir bekannt, daß die Steuerberaterkammern in ihren Mitteilungsblättern Verurteilungen und

---

[231] vom 16. Oktober 1934 (RGBl. I S. 1005), i. d. Fass. vom 16. April 1997, BGBl. I S. 821

strafbewehrte Unterlassungserklärungen unter Nennung des Namens und der Anschrift der Betroffenen veröffentlichen. Dies wurde auf meine Nachfrage auch von der Steuerberaterkammer Brandenburg bestätigt. Begründet wurde dieses Vorgehen mit der Notwendigkeit, eine Kontrollmöglichkeit für die Kammermitglieder in bezug auf mögliche Wiederholungsfälle zu haben.

Hierfür besteht nach meiner Auffassung keine Rechtsgrundlage. Die Veröffentlichung dieser Daten in den Mitteilungsblättern - und zwar die Namen und Anschriften der Betroffenen einschließlich der Tatsache ihrer Verurteilung -, die im übrigen nicht nur den Kammermitgliedern, sondern auch an die Steuerberaterkammern anderer Bundesländer, das MdF, die Oberfinanzdirektion, die IHK und die Wirtschaftsprüferkammern übersandt wurden, ist als die Übermittlung personenbezogener Daten im öffentlichen Bereich gem. § 14 BbgDSG anzusehen. Die vorgesehenen strengen Voraussetzungen sind hier nicht gegeben. Auch die Rechtfertigung der Veröffentlichungen über § 23 Abs. 2 Gesetz gegen den unlauteren Wettbewerb (UWG)[232] ist nicht möglich. Diese Vorschrift erlaubt die Veröffentlichung nur, wenn dies im zuvor ergangenen Urteil durch das erkennende Gericht angeordnet wurde.

Aufgrund dieser Ansicht habe ich die Steuerberaterkammer Brandenburg aufgefordert, die Veröffentlichungen bis zum Vorhandensein einer entsprechenden Rechtsgrundlage einzustellen. Unterdessen hat sie mir angezeigt, daß zukünftig keine derartigen Veröffentlichungen in den Mitteilungsblättern mehr erfolgen werden.

11.2 Wirtschaft

11.2.1 Einholung von BZR-Auskünften durch Ingenieurkammer über das Wirtschaftsministerium

[232] vom 7. Juni 1909 (RGBl. S. 499)

Auf Anfrage des MWMT hatte ich mich mit der Frage zu beschäftigen, ob durch das Ministerium der Brandenburgischen Ingenieurkammer **Auskünfte aus dem Bundeszentralregister** zur Verfügung gestellt werden können, um es dieser zu ermöglichen, die persönlichen Voraussetzungen bei der Bestellung und Vereidigung von Sachverständigen zu überprüfen. Ich habe hierzu festgestellt, daß eine solche Vorgehensweise eine Umgehung der Auskunftsregelungen wäre und deshalb rechtlich nicht zulässig ist. Gemäß § 41 Abs. 1 Bundeszentralregistergesetz (BZRG)[233] darf eine oberste Bundes- oder Landesbehörde unbeschränkt Auskünfte aus dem BZR für ihren eigenen Tätigkeitsbereich grundsätzlich nicht für andere Zwecke anfordern. Wenn z. B. das MWMT die Auskünfte aus dem BZR anfordert, um sie an die Brandenburgische Ingenieurkammer weiterzugeben, wäre dies eine Zweckänderung, die dem § 41 BZRG zuwiderliefe.

Dieser von mir vertretenen Meinung hat sich das MWMT nach Rückversicherung beim Bundesministerium der Justiz (BMJ) angeschlossen. Zu der Übertragung von Daten aus dem BZR durch das MWMT an nachgeordnete Behörden ist es in Brandenburg nicht gekommen.

12 Kommunale Probleme

12.1 Kommunalverwaltung um neues Image bemüht - Schaffung von Bürgerbüros

Seit einigen Jahren werden vor allem in großen Gemeinden Bemühungen erkennbar, die Gemeindeverwaltung so umzustrukturieren, daß mit Hilfe der modernen Informationstechnik eine zeitgemäße Verwaltung entsteht. Bei Gemeindeverwaltungen kommt hinzu, daß gerade mittels schneller und umfassender Informationen eine Öffnung gegenüber Bürgern erreicht werden kann. Das Ziel ist ein Dienstleistungszentrum, durch dessen Aktivitäten deutlich wird, daß die Verwaltung innerhalb eines demokratischen Gemeinwesens für den Bürger bereitzustehen hat und daß der Bürger nicht als Untertan, sondern als Partner der Verwaltung angesehen werden sollte.

Diese eher abstrakten Ansprüche treffen auf ausgeprägte finanzielle Nöte und Engpässe in der Kommunalverwaltung, da größere und zahlreichere, zum Teil mit hohen Kosten belastete Aufgaben bewältigt werden müssen. Ein sehr weitgehend akzeptierter Ausweg aus Aufgabenzuwächsen bei abnehmenden Budgets ist die Einrichtung eines sogenannten „Bürgerbüros“ als bürgerfreundliches Dienstleistungszentrum.

Bisher ist meine Behörde in keinem Fall von Anbeginn an in die Konzeptentwicklung einbezogen worden. Dies geschah erst, als die Planungen zur Umsetzung des Gedankens schon weit fortgeschritten waren, so daß bei datenschutzrechtlich relevanten Sachverhalten nur noch „die Notbremse angezogen“ werden konnte.

Grundsätzlich begrüße ich die Idee, durch die Einrichtung von Dienstleistungszentren die Verwaltung bürgerfreundlicher zu gestalten. Bürgerbüros können, vor allem in großen Städten, gleichsam wie Satelliten der (zentralen) Kommunalverwaltung wirken und helfen, den Bürgern kürzere Wege zur Erledigung von Behördenkontakten anzubieten; auch für den ländlichen Bereich trifft diese Beurteilung der Wirkung zu.

Eine der Gestaltungsvarianten für ein Bürgerbüro ist die, daß es an zentraler Stelle (wie die Fachämter) angesiedelt ist, deren Tätigkeit ersetzt oder ergänzt. Dabei ergibt sich nur insofern eine Besonderheit, als jeweils ein einzelner Sachbearbeiter mehrere Anliegen eines Bürgers erledigen kann. Diese Bearbeitungsform „aus einer Hand“ wird dadurch

233 i. d. Fass. vom 21. September 1984, BGBl. I S. 1229, ber. 1985 S.195 (BGBl. III 312-7)

ermöglicht, daß die Sachbearbeiter auf verschiedene Datenbestände zugreifen können.

Das Zentrum einer derartigen Einrichtung bildet regelmäßig das Melderegister. Über den Zugriff auf das Melderegister wird es dem Sachbearbeiter möglich, den vorstellig werdenden Bürger als „Gemeindebürger" zu erkennen, oder, anders formuliert, seine eigene Zuständigkeit bestätigt zu sehen. Für den Bürger besteht das Angebot, durch einen Bearbeiter mehrere Anliegen erledigen zu lassen, wie z. B. eine neue Wohnung anzumelden und in Verbindung damit sein Kraftfahrzeug an- oder umzumelden, Abgaben zu entrichten oder Berechtigungsscheine zu erhalten. Soweit aus organisatorischen, aber insbesondere aus rechtlichen Gründen (z. B. im Sozial- und Steuerbereich) Aufgaben nicht erledigt werden können, kann der Sachbearbeiter doch zumindest Formulare ausgeben oder verdeckt entgegennehmen und an das zuständige Fachamt weiterleiten.

Bürgerbüros werden regelmäßig in einem Großraumbüro eingerichtet. Datenschutzrechtliche Belange finden dabei kaum Berücksichtigung. Am deutlichsten zeigt sich das an der Raumaufteilung. Die Arbeitsplätze sind zumeist so nah beieinander angeordnet, daß regelmäßig weder eine visuelle noch eine akustische Abschottung hinreichend gewährleistet werden kann. So ist nicht ausgeschlossen, daß ein Bürger mitverfolgen kann, welche Anliegen andere vortragen.

Mitunter kann in Gesprächen mit den Verantwortlichen noch erreicht werden, daß beispielsweise durch eine geänderte Ordnung der Arbeitsplätze in dem Großraumbüro dem Abschottungsgebot Rechnung getragen wird. Dies setzt aber auch Wartezonen und Räume für Einzelgespräche voraus.

Meine Beratungen im Berichtszeitraum bezogen sich schwerpunktmäßig zum einen auf die Zuordnung von Aufgabenbereichen, die aus datenschutzrechtlichen Gründen nicht in einem Bürgerbüro und schon gar nicht in einem Großraumbüro wahrgenommen werden können. Zum anderen ging es darum, bei den in einem Bürgerbüro wahrzunehmenden Aufgaben i. V. m. § 10 BbgDSG sicherzustellen, daß

- der Zugang zu den Terminals nur dazu befugtem Personal ermöglicht wird,
- das Einsichtnehmen auf den Bildschirminhalt durch Dritte durch Abschirmung verhindert wird,
- der Inhalt von Festplatten gegen Überspielen gesichert wird,
- der schreibende Zugriff auf Datenträger auf das Erforderliche begrenzt wird,
- der Raum gegen gewaltsame Eindringlinge geschützt wird und
- der Inhalt der Datenträger gegen unbefugte Kenntnisnahme abgesichert wird.

Dazu ist es erforderlich, in Dienst- und Organisationsanweisungen genau festzuhalten, welche Mitarbeiter des Bürgerbüros und der zuständigen Fachämter für welche Zwecke auf welche personenbezogenen Daten lesenden oder schreibenden Zugriff haben sollen und welche Datenübermittlungen untereinander zulässig sind. Dabei kommt einer revisionssicheren Protokollierung aller Datenzugriffe und -übermittlungen eine besondere Bedeutung zu, um eine strikte aufgabenorientierte und zweckgebundene Datenverarbeitung zu sichern und eine mißbräuchliche Verwendung der im Bürgerbüro bei einer Person zusammenfließenden Daten auszuschließen.

Es wird für meine Behörde eine Aufgabe bleiben, Bürgerbüros beratend zu begleiten und dafür zu sorgen, daß der Gedanke des Datenschutzes zunehmend stärker berücksichtigt wird. Ich hoffe, daß meine Behörde zukünftig früher über diese Vorhaben informiert wird, damit grundsätzliche Forderungen, aber auch Vorstellungen und Anregungen entsprechend den örtlichen Gegebenheiten rechtzeitig aufgegriffen und umgesetzt werden können.

12.2 Jugendämter

12.2.1 Unterhaltsrechtsfragen

Zur Bemessung des Unterhaltes eines nichtsorgeberechtigten Vaters ist mir ein Vordruck des Jugendamtes zugesandt worden, in dem sämtliche Auskünfte ohne Einschränkung auch vom Ehepartner des Unterhaltspflichtigen abgefragt werden. In einem weiteren Fragebogen wird der Arbeitgeber um Auskunft über die **Berufstätigkeit des Ehepartners** und **Name und Anschrift des Arbeitgebers** gebeten.

Nach § 1603 BGB, der die Voraussetzung der Unterhaltsverpflichtung regelt, ist lediglich die Leistungsfähigkeit des Verpflichteten zu prüfen. Für den Ehegatten des Unterhaltspflichtigen besteht keine Unterhaltspflicht gegenüber dem minderjährigen Kind, weshalb keine Verpflichtung zu den genannten Angaben besteht. Vielmehr handelt es sich hier nicht um eine Rechtspflicht, sondern um Angaben, die der Unterhaltspflichtige zu seiner Entlastung machen kann, da bei der ihm zumutbaren Belastung aus dem Unterhalt für das minderjährige Kind seine Unterhaltspflicht gegenüber dem Ehegatten berücksichtigt werden muß, je nach dessen eigenem Verdienst. Angaben hinsichtlich des Ehepartners sind daher zur Aufgabenerfüllung des Jugendamtes nur dann erforderlich, wenn der andere Ehegatte vom Unterhaltspflichtigen unterhalten werden muß, worauf hinzuweisen ist. Lediglich über die persönlichen Verhältnisse, wie Wiederverheiratung, muß der Unterhaltsverpflichtete Auskunft geben, und zwar aus Gründen des steuerlichen Splitting-Vorteils, der auch unterhaltsberechtigten Kindern aus einer früheren Ehe sowie dem früheren Ehegatten zugute kommt.

Das Jugendamt hat daraufhin eine **Einzelanweisung zum Vordruck „Ermittlungsbogen zu Einkommens- und Vermögensverhältnissen"** erarbeitet. Darin werden die Mitarbeiter des Bereiches Vormundschaftswesen angehalten, künftig im Anschreiben an den Auskunftspflichtigen darauf hinzuweisen, daß Angaben zum Einkommen des Ehepartners nur im Zusammenhang mit dessen eigenem Unterhaltsanspruch zu sehen sind.

Für den **Arbeitgeber** besteht somit auch keine Verpflichtung, die Zeile zur Berufstätigkeit des Ehepartners auszufüllen.

12.2.2 Das Umgangsrecht eines Nichtsorgeberechtigten

Darf ein Jugendamt eines anderen Bundeslandes ein Gutachten der Schulpsychologin anfordern? Diese Frage stellte ein nichtsorgeberechtigter Vater im Zusammenhang mit seinem Recht auf Umgang mit seiner Tochter.

Meines Erachtens bestehen hiergegen in dem vorliegenden Fall keine datenschutzrechtlichen Bedenken. Nach § 64 SGB VIII[234] dürfen Sozialdaten nur zu dem Zweck übermittelt oder genutzt werden, zu dem sie erhoben worden sind. Nach Absatz 2 ist eine Übermittlung für die Erfüllung von Aufgaben nach § 69 SGB X[235] abweichend von Absatz 1 nur zulässig,

[234] i. d. Fass. vom 15. März 1996, BGBl. I S. 447, geänd. durch Ges. vom 23. Juli 1996, BGBl. I S. 1088

[235] vom 18. August 1980, BGBl. I S. 1469, ber. S. 2218; zul. geänd. durch SGB III-ÄndG vom 16. Dezember 1997, BGBl. I S. 2970

soweit dadurch der Erfolg einer zu gewährenden Leistung nicht in Frage gestellt wird.
Das Gutachten wurde damals im Zusammenhang mit dem **Umgangsrecht** des Vaters zum Wohle des Kindes erstellt. Um überprüfen zu können, ob die Voraussetzungen für die Aufrechterhaltung dieses Umgangsrechtes bestehen, sollte das Jugendamt entweder dieses psychologische Gutachten anfordern oder aber, soweit dieses keine Gültigkeit mehr hat, ein neues erstellen lassen. Dies gilt jedoch nur für den Fall, daß das Familiengericht die Befugnis zum persönlichen Umgang mit dem Kind nicht gem. § 1634 Abs. 2 Satz 2 BGB ausgeschlossen hat.

Vorsorglich habe ich darauf hingewiesen, daß die Mitarbeiter des Jugendamtes **unbedingte Neutralität im Umgang mit beiden Elternteilen** üben sollen. Dazu gehört z. B., daß die im Verfahrensrecht vorgeschriebenen Stellungnahmen der Jugendämter stets beiden Elternteilen dann zugänglich sein müssen, wenn sie dem Gericht übermittelt werden. In keinem Fall zulässig ist es, gutachterlich tätige Sachverständige einseitig über Schwächen des einen oder anderen Elternteiles zu informieren, ohne daß dies objektiv nachvollziehbar und aktenkundig ist. Der Leiter des Jugendamtes versicherte mir, als neutraler Vermittler zwischen den Beteiligten zu fungieren mit dem Ziel, den Petenten bei seinem berechtigten Anliegen zu unterstützen.

12.2.3 Kontrolle der Beratungstätigkeit der freien Träger

Ein freier Träger, der Hilfen für sexuell mißbrauchte und von Gewalt betroffene Kinder anbietet, sorgte sich um die Gewährleistung der **Anonymität der Betroffenen**. Aufgrund einer Neuregelung sollen die finanziellen Zuwendungen durch den Landkreis an den Leistungserbringer nun nicht mehr pauschal mittels eines Sachberichtes und zahlenmäßigen Nachweises, sondern leistungsbezogen erfolgen. Dies betrifft vor allem Beratungssituationen, die das Leistungskontingent von 20 Beratungsstunden übersteigen und nach Auffassung des Jugendamtes in ein Hilfeplangespräch gem. § 36 SGB VIII übergehen müssen. Hierbei besteht jedoch das Problem, daß die Ratsuchenden in der Regel mit dem Jugendamt nicht zusammenarbeiten und weiterhin anonym beraten werden wollen.

In meiner Stellungnahme gegenüber dem Jugendamt habe ich darauf hingewiesen, daß der öffentliche Jugendträger nicht berechtigt ist, vom freien Träger Informationen zu verlangen, die nach den Übermittlungsvorschriften des SGB nicht zulässig sind oder unter den besonderen Vertrauensschutz des § 65 SGB VIII fallen. Mit § 61 Abs. 4 SGB VIII hat der Gesetzgeber den Trägern der öffentlichen Jugendhilfe den Auftrag erteilt, bei einer Inanspruchnahme von freien Trägern den Datenschutz „sicherzustellen".

Soweit das Jugendamt nun mit der Einrichtung des freien Trägers in eine Rechtsbeziehung tritt, ermöglicht diese ihm, „entsprechenden Datenschutz" zur Bedingung zu machen. Eine Rechtsbeziehung wird hier im Zusammenhang mit einer Finanzierung aus öffentlichen Mitteln hergestellt.

Das Jugendamt hat dann zwar ein entsprechendes **Prüfungsrecht hinsichtlich zweckentsprechender Verwendung bei Inanspruchnahme öffentlicher Mittel**, jedoch beschränken sich solche Nachprüfungen auf das Notwendigste und dürfen vom Grundsatz her nicht den Kernbestand der Aufgabenstellung des freien Trägers angreifen. Eine Einzelabrechnung würde gerade bei Beratungsstellen mit dem Schwerpunkt Kinderschutz zu einer Behinderung der Beratungstätigkeit freier Träger führen. Für den jeweiligen freien Träger ist es nicht möglich, bei garantierter Anonymität einer Beratung die Verwendung der Mittel für den Förderzweck entsprechend den Vorgaben des Bescheides nachzuweisen, wozu die Mittel verwendet wurden. Diese Form der Nachweisführung halte ich für ungeeignet. Nur im Falle des Vorliegens einer Einwilligung der Ratsuchenden kann eine personenbezogene Übermittlung an das Jugendamt erfolgen. Verweigert der Ratsuchende seine Einwilligung, so sind dem Jugendamt lediglich die Beratungsfälle anonym, z. B.

unter Angabe einer Altersgruppe (z. B. Vorschulalter), sowie Angaben des Problems und die Art sowie die Dauer der Tätigkeiten des freien Trägers (z. B. Begleitung des Kindes zur Polizei, Hausbesuche von ... bis ... Uhr) nachzuweisen.

Das Jugendamt hat in seiner Stellungnahme daran festgehalten, die leistungsbezogene Finanzierung zu favorisieren. Es wies u. a. auf mögliche Beratungsabhängigkeiten zwischen freien Trägern und Klienten hin. Eine regelmäßige Reflexion der zu erbringenden Hilfe sei notwendig und vorgeschrieben, d. h. eine Fortschreibung des Hilfeplanes.

Zur einvernehmlichen Lösung dieses Problems beabsichtige ich, ein gemeinsames Gespräch sowohl mit dem Jugendamt als auch dem freien Träger zu führen, worüber zu gegebener Zeit zu berichten sein wird.

12.2.4 Einsichtnahme in Jugendhilfeakten durch Dritte

Im Berichtszeitraum wandten sich sowohl ein Jugendamt als auch in einem anderen Fall eine nichtsorgeberechtigte Mutter an mich, um prüfen zu lassen, unter welchen Voraussetzungen **Akteneinsicht** gewährt werden müsse.

In dem **ersten Fall** hatte das Jugendamt die Eheleute, die ein Kind adoptiert hatten, zu den Kosten der Hilfegewährung herangezogen. Die Eheleute zweifelten die Einschätzung des Jugendamtes an und beauftragten eine Stadtverordnete mit der Akteneinsicht.

§ 67 SGB VIII begründet kein Akteneinsichtsrecht, sondern gewährt lediglich ein **Auskunftsrecht** gegenüber den Betroffenen. Das Recht auf informationelle Selbstbestimmung wird durch § 67 SGB VIII ausreichend insoweit gewährleistet, als es hinsichtlich des Umfanges des Anspruchs auf Auskunft kein Ermessen der Behörde gibt. Alle Sozialdaten i. S. v. § 67 Abs. 1 SGB X müssen den Betroffenen mitgeteilt werden. Die in den Akten enthaltenen Sozialdaten müssen der Wahrheit entsprechen und frei von unzutreffenden Bewertungen sein. Ein generelles Akteneinsichtsrecht der Betroffenen würde die Unbefangenheit in der Aktenführung und die Gewährleistung der inhaltlichen Vollständigkeit erschweren.

Da jedoch die speichernde Stelle gem. § 83 Abs. 1 S. 4 SGB X das Verfahren nach pflichtgemäßem Ermessen bestimmt, insbesondere die Form der Auskunftserteilung, ist diese durch Übersendung einer Abschrift bzw. eines Speicherauszugs oder durch Gewährung der Einsichtnahme in die Unterlagen möglich.

Ein **Akteneinsichtsrecht von Stadtverordneten** gem. § 36 Abs 3 Gemeindeordnung kommt nicht in Betracht, da es sich in dem vorliegenden Fall nicht um eine Kontrolle gegenüber der Exekutive handelte. Ein Akteneinsichtsrecht durch Beteiligte, wozu auch die Stadtverordnete als Bevollmächtigte der Eheleute i. S. d. § 13 SGB X zählen könnte, kann lediglich aus § 25 SGB X hergeleitet werden. Danach hat die Behörde dem Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. Es muß sich also um Verfahrenshandlungen innerhalb eines laufenden Verwaltungsverfahrens handeln. Sofern den Eheleuten vom Jugendamt eine Kostenentscheidung und damit ein Verwaltungsakt zugegangen ist, und dieser bestandskräftig geworden ist, scheidet ein Akteneinsichtsrecht gem. § 25 SGB X aus.

In dem **zweiten Fall** lag die Besonderheit darin, daß eine Mutter vom Jugendamt Auskunft über die **Heimunterbringung ihrer inzwischen volljährigen Kinder** verlangte.

Da es sich um Angaben über die Art einer Beziehung und die Bezeichnung der Beziehungspersonen handelt, haben diese

von vornherein einen **doppelten Personenbezug**. D. h., sowohl die volljährigen Kinder als auch die Petentin sind Betroffene und beide können Auskunft vom Jugendamt verlangen.

12.2.5 Aktenübergabe vom Jugendamt ans Sozialamt

Ein Sozialamt hat die Frage an mich herangetragen, ob die Jugendamtsakte einer Person, die unter Vormundschaft gestanden hatte und bisher vom Jugendamt betreut worden war, inzwischen aber volljährig geworden sei, vom Sozialamt übernommen werden dürfe.

Gemäß § 67 Abs. 9 SGB X handelt es sich beim Sozialamt und Jugendamt einer Gemeinde oder eines Landkreises um zwei voneinander unabhängige speichernde Stellen. Eine Aktenübergabe setzt damit eine **Übermittlungsbefugnis** für die darin enthaltenen Sozialdaten voraus.

Auch wenn die Aufgabenerfüllung des Sozialamts die Kenntnis der **Akte des Amtsvormunds** erfordert, ist dennoch eine Übergabe an das Sozialamt auszuschließen. Nach § 61 Abs. 2 SGB VIII gilt für den Schutz von Sozialdaten bei ihrer Erhebung, Verarbeitung und Nutzung im Rahmen der Tätigkeit des Jugendamtes als Amtsvormund § 68 SGB VIII, der die Datenverarbeitung nur zur Erfüllung von Aufgaben des Amtsvormunds zuläßt. Die Erfüllung von Aufgaben eines anderen Sozialleistungsträgers läßt hingegen eine Übermittlung dieser Akte nicht zu.

Etwas anderes gilt für die normale **Jugendamtsakte**, bei der eine Übermittlung nach § 69 Abs. 1 Nr. 1 SGB X für die Erfüllung einer gesetzlichen Aufgabe eines anderen Sozialleistungsträgers zulässig sein kann. § 64 Abs. 2 SGB VIII knüpft dies an die weitere Voraussetzung, daß dadurch der Erfolg einer im Rahmen der Jugendhilfe zu gewährenden Leistung nicht in Frage gestellt wird. Für einen Jugendamtsmitarbeiter besonders anvertraute Daten verschärft § 65 SGB VIII die Übermittlungsvoraussetzungen allerdings nochmals.

Ungeachtet der grundsätzlichen Übermittlungsmöglichkeit von leistungsbezogenen Jugendhilfeakten nach § 69 Abs. 1 Nr. 1 SGB X i. V. m. § 64 Abs. 2 SGB VIII wies ich darauf hin, daß selbstverständlich auch hier der **Ersterhebungsgrundsatz des § 67 a SGB X** zu beachten ist, die Daten also primär beim Betroffenen selbst zu erheben sind. Datenerhebungen ohne seine Mitwirkung setzen nach § 67 a Abs. 2 Nr. 1 SGB X nämlich nicht nur eine gesetzliche Übermittlungsbefugnis voraus, sondern auch, daß die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, daß überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Diese Voraussetzungen waren von dem Sozialamt noch nicht geprüft worden. Insbesondere war nicht geklärt, welche konkreten Daten das Sozialamt benötigte. Es war jedoch davon auszugehen, daß die gesamte Jugendamtsakte wesentlich mehr an Informationen enthalten würde, als das Sozialamt für seine Aufgabenerfüllung benötigen könnte. Da es dem Sozialamt vorrangig um eine allgemeine Information über den Sozialhilfeempfänger ging, habe ich ausdrücklich darauf hingewiesen, daß es sich einen solchen Überblick über den bisherigen Lebenslauf des Betroffenen nicht mit Hilfe der Jugendamtsakte verschaffen dürfe. Angesichts der verschiedenen Aufgaben des Jugend- und Sozialamtes sprach vieles dafür, daß es einfacher sein dürfte, die für das Sozialamt notwendigen Daten beim Betroffenen selbst zu erheben.

12.2.6 Unterhaltsberechnungen bei einem Selbständigen

Der Vater eines unterhaltsberechtigten Kindes erkundigte sich bei mir darüber, ob er gegenüber dem Jugendamt verpflichtet sei, die Einnahmen- und Überschußrechnungen einschließlich Abschreibungslisten, Einkommenssteuererklärungen sowie die Einkommenssteuerbescheide der letzten drei Jahre vorzulegen.

Auf Nachfrage beim Jugendamt erfuhr ich, daß dieses als Beistand für das nichteheliche Kind in einer Auskunftsangelegenheit gem. § 1605 BGB tätig geworden sei. Dieser Paragraph beinhaltet einen Auskunftsanspruch von Verwandten in gerader Linie. Danach sind diese verpflichtet, auf Verlangen über ihre Einkünfte und ihr Vermögen Auskunft zu erteilen, soweit dies zur Feststellung eines Unterhaltsanspruchs oder einer Unterhaltsverpflichtung erforderlich ist. Gem. § 1605 Abs. 2 BGB kann nach Ablauf von zwei Jahren die Auskunft erneut verlangt werden. Bei Selbständigen erstreckt sich die **Auskunft** in der Regel **über die letzten drei Geschäftsjahre** und auch **über Steuerrückerstattungen**.

Bei der Einkommensermittlung Selbständiger zur Feststellung der Unterhaltshöhe für das minderjährige Kind wird regelmäßig vom steuerrechtlichen Einkommen ausgegangen. Neben dem Einkommensteuerbescheid ist die Vorlage der Einkommenssteuererklärung für das Jugendamt relevant, um den Steuerbescheid inhaltlich vollkommen nachvollziehen zu können.

In dem Verfahren zur Berechnung der Unterhaltshöhe bei dem Petenten konnte ich somit keinen datenschutzrechtlichen Verstoß feststellen. Das Jugendamt hat nur die Einkommens- und Vermögensverhältnisse durch Aufschlüsselung von Einnahmen und Ausgaben ermittelt. Das ist rechtlich zulässig.

12.3 Meldeamt

12.3.1 Gezielte Werbung durch Musikschulen

Eine Mutter, die von einer städtischen Musikschule einen **Werbebrief mit dem Angebot musikalischer Früherziehung** für ihre beiden noch nicht schulpflichtigen Kinder erhielt, fragte verwundert bei mir nach, auf welchem Wege die Musikschule nicht nur die Anschrift, sondern auch das Alter ihrer Kinder in Erfahrung habe bringen können. Obwohl sie zugestand, daß das Angebot an sich zu begrüßen sei, wollte sie doch sichergestellt haben, daß ihre persönlichen Daten und die ihrer Kinder nicht ohne gesetzliche Grundlage weitergegeben werden. Aufgrund ihrer Kenntnis, daß auch andere Eltern mit Kindern der gleichen Altersgruppe die Post erhalten hatten, vermutete sie, daß die Daten von der Stadtverwaltung stammten und von dort aus unkontrollierbar möglicherweise auch noch an andere Stellen weitergeleitet werden könnten.

Es bestätigte sich, daß der Musikschule die Daten von der Meldebehörde im Rahmen der **Datenübermittlungen an Behörden** gem. § 28 Abs. 1 Brandenburgisches Meldegesetz (BbgMeldeG)[236] auf Antrag zur Verfügung gestellt worden waren. Derartige Übermittlungen bedürfen aber des Nachweises, daß die Daten zur Erfüllung der in der Zuständigkeit des Meldeamts oder der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich sind. Das Meldeamt sah die zweite Voraussetzung als gegeben an, weil in der für die Musikschule geltenden Satzung folgender Aufgabenzweck definiert war: „Die städtische Musikschule ... dient der individuellen Heranführung ihrer Schüler aller Altersgruppen an die Musik und einer möglichst früh einsetzenden und umfassenden musikalischen Ausbildung. Dabei wird die Verbindung auch zu anderen Bereichen der musikalischen Bildung und der Kunst angestrebt.“.

In meiner Überprüfung kam ich zu dem Ergebnis, daß mit dieser materiell-rechtlichen Regelung die **Voraussetzungen des § 28 MeldeG** nicht erfüllt waren. Nach gängiger Kommentierung zum inhaltsgleichen § 18 Abs. 1 Melderechtsrahmengesetz (MRRG)[237] ist eine Erforderlichkeit zur Übermittlung von Meldedaten an andere Behörden

---

[236] vom 25. Juni 1992, GVBl. I S. 236

[237] i. d. Fass. vom 24. Juni 1994, BGBl. I S.1430, geänd. durch Ges. vom 12. Juli 1994, BGBl. I S. 1497, 1503

und sonstige öffentliche Stellen nur gegeben, wenn ohne sie der Datenempfänger seine Aufgaben nicht fehlerfrei, nicht vollständig oder nicht in angemessener Zeit erfüllen kann. Nicht eine dieser Voraussetzungen traf auf die Angebotswerbung für eine musikalische Früherziehung durch die städtische Musikschule zu, weil in der Satzung der Musikschule nicht geregelt war, daß Angebote zur musikalischen Bildung gezielt Einzelpersonen, wie z. B. auch Kindern im Vorschulalter oder Personengruppen zu unterbreiten sind. Die Satzung sieht lediglich die „Heranführung" einer unbestimmten Altersgruppe an die Musik usw. als allgemeine Zielsetzung vor.

Auf eine förmliche Beanstandung der bis dahin unzulässigerweise vorgenommenen Datenübermittlungen habe ich allerdings verzichtet, weil mir die Musikschule versicherte, die in den vergangenen Jahren auf diesem Wege erhaltenen Daten datenschutzgerecht entsorgt zu haben, im übrigen den abschließenden Ausführungen der Stadtverwaltung zu entnehmen war, daß bei Datenübermittlungen aus dem Melderegister nach § 28 Abs.1 BbgMeldeG zukünftig meiner Rechtsauslegung gefolgt werde.

12.4 Sozialamt

12.4.1 Ermittlungen des Sozialamts - nicht unbedenklich

Petenten beschwerten sich bei mir u. a. über folgende Verfahrensweisen des für sie zuständigen Sozialamtes:

- Für den **Nachweis von krankheitsbedingtem Mehrbedarf** wegen kostenaufwendiger Ernährung wurde dem Petenten ein Formblatt für den Arzt mitgegeben, aus dem sich durch den Hinweis auf § 23 Abs. 4 Nr. 2 Bundessozialhilfegesetz (BSHG)[238] für diesen ergab, daß der Betreffende Sozialhilfeempfänger ist.

  Das zuständige Sozialamt hat inzwischen mitgeteilt, daß dieser Vordruck in Zukunft keine Verwendung mehr finden wird, sondern vielmehr der Sozialhilfeempfänger gehalten ist, ein Attest vom Arzt zu erbitten, das dann dem Sozialamt vorgelegt wird. So kann der behandelnde Arzt nicht erkennen, wofür die Bescheinigung benötigt wird.

- Das Sozialamt fragte „aus Gründen der Sozialhilfe" beim privaten Vermieter des Petenten an, ob seine **Miete und die Mietkaution** bezahlt seien.

  Das Sozialamt berief sich als Grundlage für seine Datenerhebung auf § 117 Abs. 3 BSHG. Ein Datenabgleich nach dieser Vorschrift darf aber nur bei anderen Stellen der beteiligten Verwaltung, bei deren wirtschaftlichen Unternehmen und bei den Kreisen, Kreisverwaltungsbehörden und Gemeinden stattfinden, nicht jedoch bei Privatpersonen. Außerdem beschränkt § 117 Abs. 3 Satz 4 BSHG den Umfang der Daten, deren Überprüfung zulässig ist. Abgeglichen werden dürfen danach Dauer und Kosten eines Mietverhältnisses von Wohnraum. Die Fragen nach Mietrückständen und der Bezahlung der Kaution sind davon nicht erfaßt.

238 i. d. Fass. vom 23. März 1994, BGBl. I S. 646, ber. S. 2975; zul. geänd. durch SGB III-ÄndG vom 16. Dezember 1997 BGBl. I S. 2970

Die Anfrage beim Vermieter könnte daher allenfalls auf § 67 a Abs. 2 Nr. 2 b SGB X gestützt worden sein. Die Voraussetzungen für diese Datenerhebung sind ziemlich problematisch[239]. Sie waren im vorliegenden Fall außerdem vom Sozialamt nicht geprüft worden. Zu berücksichtigen ist dabei auch, daß nunmehr in § 15 a Abs. 2 BSHG ein Gericht, bei dem eine Räumungsklage im Falle der Kündigung des Mietverhältnisses wegen Zahlungsverzuges eingeht, verpflichtet ist, den örtlichen Träger der Sozialhilfe unverzüglich darüber zu informieren. Der äußerste Notfall „Obdachlosigkeit" kann damit also durch das Sozialamt in jedem Fall vermieden werden.

- Ein Petent unterstützte hin und wieder unentgeltlich einen Familienangehörigen bei dessen selbständiger Tätigkeit. Das Sozialamt befragte nun einen Kunden des Familienangehörigen dazu, welche Arbeiten der Petent dort verrichtete und was ihm dafür bezahlt werde. Der Befragte war auf die Freiwilligkeit seiner Angaben hingewiesen worden. Die Frage zum Arbeitsentgelt beantwortete er nicht.

  Das Sozialamt trug vor, trotz entsprechender Bitten zu diesen Punkten keine Auskunft vom Petenten erhalten zu haben. Sofern der vom Petenten unterstützte Familienangehörige als sein Arbeitgeber angesehen werden könnte, hätte eine Datenerhebungsbefugnis nach § 67 a Abs. 2 Nr. 2 a SGB X i. V. m. § 116 Abs. 2 BSHG bestehen können. Allerdings durfte das Sozialamt von dieser eigentlich vorrangigen Ermittlungsbefugnis wegen des Auskunftsverweigerungsrechts für nahestehende Personen nach § 116 Abs. 3 BSHG absehen. Deshalb kann auch in diesem Fall letztlich nur § 67 a Abs. 2 Nr. 2 b SGB X als Datenerhebungsvorschrift in Betracht kommen.

In den beiden letzten Fällen wird eine grundsätzliche Problematik deutlich: Das Sozialamt erhält keine oder nur unzureichende **Auskünfte von** den **Dritten**, offenbart diesen jedoch, daß jemand Sozialhilfeempfänger ist und daß das Sozialamt eine Überprüfung seiner Angaben für notwendig hält. Durch die Befragung Dritter wird letztlich nur erreicht, daß der Leistungsempfänger und auch Familienangehörige bloßgestellt werden, ohne daß das Sozialamt wesentliche Informationen erhält. Ich stehe diesen Datenerhebungen daher sehr kritisch gegenüber. Die Sozialleistungsträger können bei unberechtigter Auskunftsverweigerung des Betroffenen ggf. mit einer Ablehnung oder Kürzung der Sozialhilfe gem. § 66 SGB I[240] reagieren.

- In einem weiteren Fall stellte sich heraus, daß das Sozialamt aufgrund einer mündlichen Einwilligungserklärung der Ehefrau des Petenten ein Auskunftsersuchen an dessen behandelnden Arzt gerichtet hatte. Eine solche Einwilligungserklärung, mit welcher der Arzt zugleich von seiner ärztlichen Schweigepflicht entbunden werden sollte, muß jedoch vom Patienten persönlich abgegeben werden. Die Mitteilung der Ehefrau kann diese Erklärung nicht ersetzen. Im übrigen bedarf die Erklärung des Betroffenen nach § 100 Abs. 1 Satz 2 SGB X auch grundsätzlich der Schriftform. Zu Recht erhielt das Sozialamt von dem behandelnden Arzt keine Auskunft.

12.4.2 Einsatz von (privaten) Sozialhilfeermittlern

Im Zusammenhang mit den unter 7.1.1.1 dargestellten gesetzgeberischen Intentionen, **Sozialhilfemißbrauch** durch zusätzliche Übermittlungsbefugnisse zu begegnen, ist auch der verstärkte Einsatz von Sozialhilfeermittlern zu sehen.

Der Einsatz von Außendienstmitarbeitern des Sozialamts, die bei **konkreten Anhaltspunkten für einen Mißbrauch** die erforderlichen Daten vor Ort ermitteln sollen, ist unter den Voraussetzungen des § 67 a SGB X zulässig. Zu beachten ist

---

239 s. unter 12.4.2

240 vom 11. Dezember 1975, BGBl. I S. 3015; zul. geänd. durch SGB III-ÄndG vom 16. Dezember 1997, BGBl. I S. 2970

dabei, daß nach § 67 a Abs. 2 Satz 1 SGB X die Datenerhebung grundsätzlich beim Betroffenen selbst zu erfolgen hat. Bei anderen Personen oder anderen Stellen als Sozialleistungsträgern dürfen die „Mißbrauchsermittler" Daten über den Betroffenen nur nach Maßgabe der in § 67 a Abs. 2 Nr. 2 SGB X genannten Voraussetzungen erheben. Die Datenerhebung bei Dritten ist u. a. zulässig, wenn eine Rechtsvorschrift sie zuläßt oder diese Übermittlung an die erhebende Stelle ausdrücklich vorschreibt. Ein Beispiel hierfür ist die Auskunftspflicht des Arbeitgebers von Sozialhilfeempfängern, deren Unterhaltspflichtigen oder deren nicht getrennt lebenden Ehegatten nach § 116 Abs. 2 BSHG. Eine Datenerhebung bei Dritten kann auch zulässig sein, wenn die Aufgaben nach dem Sozialgesetzbuch ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich machen und keine Anhaltspunkte dafür bestehen, daß überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Die erste Voraussetzung dieser Datenerhebungsbefugnis ist so formuliert, daß eine ihrem Wortlaut entsprechende Fallgestaltung nicht denkbar ist. Insoweit kann man vertreten, daß diese Variante mangels Normenklarheit entfällt. Ich tendiere dazu, ihr durch **enge Auslegung** zu einem gewissen Sinn für den Bereich der Sozialhilfe zu verhelfen und z. B. folgende Situationen unter diese Vorschrift fallen zu lassen:

- Der Betroffene selbst kann wegen fehlender Sachkenntnis keine oder keine ausreichenden Angaben machen, und er kann die Angaben auch nicht anderweitig selbst beibringen.

- Die Überprüfung von Auskünften des Betroffenen, die konkrete Zweifel an ihrem Wahrheitsgehalt aufwerfen, kann nur ohne Mitwirkung des Betroffenen durchgeführt werden.

Zusätzlich ist bei diesen beiden Datenerhebungsbefugnissen das schutzwürdige Interesse des Betroffenen mit dem Datenerhebungsinteresse abzuwägen.

- Der Betroffene erhält befristet die Möglichkeit, Auskünfte oder Nachweise selbst beizubringen, zugleich wird ihm mitgeteilt, bei welcher Stelle die Daten erhoben werden sollen, wenn er untätig bleibt. Er wird weiter darüber informiert, daß seine schutzwürdigen Interessen zu berücksichtigen sind und bei einem Widerspruch durch ihn von deren Überwiegen ausgegangen würde, ggf. aber sein Antrag auf Leistung abgelehnt werden müsse, wenn dessen Voraussetzungen zweifelhaft bleiben.

Es ist zu berücksichtigen, daß sich durch eine korrekte Datenerhebung bei Dritten mit den entsprechenden datenschutzrechtlichen Hinweisen sich für die Befragten auch Informationen über den Kontakt des Betroffenen mit dem Sozialamt, möglicherweise sogar über den Mißbrauchsverdacht, ergeben. Sofern den Befragten dann noch die Beantwortung freigestellt ist, muß bedacht werden, daß es nicht vertretbar ist, bei der Befragung Dritter einerseits indirekt Sozialdaten zu offenbaren, aber andererseits möglicherweise keine oder wiederum mit dem betroffenen Sozialhilfeempfänger abgestimmte Informationen zu erhalten. Ich vertrete deshalb die Auffassung, daß von dieser Datenerhebungsbefugnis jedenfalls dann kein Gebrauch gemacht werden sollte, wenn für den Befragten keine Auskunftspflicht besteht, weil hier bei einer Einschätzung im vorhinein nach den voranstehenden Darlegungen nie ausgeschlossen werden kann, daß das Interesse des Betroffenen überwiegt.

Die obigen Überlegungen gelten **im Falle einer verdeckten Beobachtung** in viel stärkerem Maße. Unter Berücksichtigung des Ersterhebungsgrundsatzes und der Mitwirkungspflichten nach den §§ 60 ff. SGB I ergibt sich, daß eine Datenerhebung ohne Wissen des Betroffenen abzulehnen ist.

Zu diesen Fragestellungen hatte ein Landkreis meinen Rat gesucht. Im dortigen Sozialamt überlegte man, ob bei einem konkreten Verdacht von Sozialhilfebetrug auch **private Ermittler** eingeschaltet werden könnten. Zwar sieht das SGB X

derzeit eine Datenerhebung im Auftrag noch nicht vor, im Hinblick auf die anstehende Änderung durch das Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze könnte sie jedoch toleriert werden. Allerdings hat der Landkreis aufgrund des Gesprächs mit mir bereits bei einer oberflächlichen Prüfung der Voraussetzungen des hier einschlägigen § 80 Abs. 5 SGB X festgestellt, daß diese nicht erfüllt sind.

12.5 Sonstige Stellen

12.5.1 Zweckverbände zur Daseinsfürsorge

12.5.1.1 Wasserversorgung in Privathand

Im Rahmen meiner Prüfung von Zweckverbänden habe ich festgestellt, daß es in zunehmendem Maße zu einer **Auslagerung von öffentlichen Aufgaben** (wie z. B. Wasserversorgung und Abwasserentsorgung) in den nichtöffentlichen Bereich kommt; d. h. juristische Personen des Privatrechts werden aus Effizienz - und Kostensenkungsgründen mit der Wahrnehmung öffentlich-rechtlicher Aufgaben der Daseinsvorsorge beauftragt. In diesen Fällen ist es mir nach der derzeitigen Rechtslage nicht möglich, die Privaten auf die Einhaltung datenschutzrechtlicher Vorschriften zu kontrollieren, da dafür § 2 BbgDSG keinen Raum bietet. Sie fallen damit unter den Geltungsbereich des Bundesdatenschutzgesetzes (BDSG), dessen Regelungen derzeit die Einhaltung eines geringeren Datenschutzniveaus als das Brandenburgische Datenschutzgesetz bietet.

Meine Bedenken bezüglich des ungleichen Datenschutzniveaus wären ausgeräumt, wenn die Privaten, soweit sie öffentliche Aufgaben wahrnehmen, bei der Verarbeitung personenbezogener Daten an die Regeln gebunden blieben, die von öffentlichen Stellen zu beachten sind. Eine Angleichung des Datenschutzniveaus bietet die vor dem Hintergrund der **EU-Datenschutzrichtlinie** anstehende **Novellierung des BDSG**[241].

12.5.1.2 Abfallentsorgung durch eine GmbH

Ein Bürger äußerte Bedenken gegen die Beauftragung einer GmbH mit der Abfallentsorgung. Er bezweifelte darüber hinaus die **Rechtmäßigkeit der „Gebührenbescheiderstellung**" dieser privaten Abfallwirtschaftsgesellschaft.

Der Beauftragung einer GmbH mit der Abfallentsorgung stehen keine datenschutzrechtlichen Bedenken entgegen, da nach § 5 Brandenburgischen Abfallgesetz (BbgAbfG)[242] öffentlich-rechtliche Entsorgungsträger **zuverlässige Dritte** mit der Erfüllung ihrer Aufgaben beauftragen können. Der Gesetzgeber hat mit § 40 Abs. 1 BbgAbfG eine spezialgesetzliche Norm geschaffen, die es Dritten (i. S. v. § 5 BbgAbfG) erlaubt, im Rahmen ihrer Aufgabenerfüllung personenbezogene Daten zu erheben, zu speichern, zu löschen und zu übermitteln, wenn sie mit der Erfüllung gesetzlicher Aufgaben beauftragt werden und die damit befaßten Personen auf die Geheimhaltung von Daten verpflichtet werden. In dem der Petition zugrunde liegendem Fall waren beide Voraussetzungen erfüllt.

Die Berechtigung des Landkreises, Abgaben (Gebühren und Beiträge) zu erheben, ergibt sich aus den §§ 1, 2, 4

241 s. unter 1.3.1

242 vom 6. Juni 1997, GVBl. I S. 40

Kommunalabgabengesetz (KAG)[243] i. V. m. § 9 BbgAbfG sowie der entsprechenden Satzungen. Für die Bürger ist allerdings irreführend, wenn hierbei von einer GmbH „Gebührenbescheide" statt „Rechnungen" ausgestellt werden.

Entgegen der gegenwärtigen Meinung der Landesregierung vertrete ich die Auffassung, daß bei solchen Ausgründungen in Form einer GmbH **sowie der Beteiligung an Eigenunternehmen** i. S. v. § 101 Gemeindeordnung (GO)[244] das Brandenburgische Datenschutzgesetz auch Anwendung finden müßte, so daß Eigenunternehmen damit einer öffentlichen Stelle des Landes gleichgestellt werden. Hierfür sprechen gewichtige Gründe:

- Der Gesetzgeber läßt in § 100 GO ausdrücklich eine **wirtschaftliche Betätigung der Gemeinden** zu, so auch die Beteiligung an Gesellschaften i. S. v. § 101 Abs. 3 Nr. 3 GO.

- Im Land Brandenburg ist die sog. Organisationsprivatisierung nur zulässig, wenn die Gemeinde einen **angemessenen Einfluß**, insbesondere im Aufsichtsrat oder in einem entsprechenden Überwachungsorgan des Unternehmens, gem. § 102 GO erhält. Neben der vom Gesetzgeber geforderten Einflußnahme (Vertretung im Vorstand, Aufsichtsrat o. ä.) hat die Gemeinde gem. § 105 GO **Informations- und Prüfungsrechte** i. S. v. § 53 Haushaltsgrundsätzegesetz.

- Legt man bei der Beurteilung des Sachverhalts das Grundrechtsverhältnis Staat-Bürger zugrunde, so ist es eigentlich unerheblich, ob der Staat (Gemeinde) die Leistung (Abfallentsorgung) in den Formen des öffentlichen Rechts (wie z. B. beim Eigenbetrieb) erbringt oder sich privatrechtlicher Formen wie der GmbH bedient. In jedem Fall wird die öffentliche Aufgabe durch die öffentliche Verwaltung wahrgenommen - nur eben in privatrechtlicher Form.

---

243 vom 27. Juni 1991, GVBl. I S. 200

244 vom 15. Oktober 1993, GVBl. I S. 398

Bei der anstehenden Novellierung des Brandenburgischen Datenschutzgesetzes halte ich eine grundlegende Neuregelung deshalb für erforderlich, weil es ansonsten bei einer Ausgründung wegen der drohenden Verschiebung von einer **„völlig unabhängigen Kontrolle“**[245] durch den Landesbeauftragten für den Datenschutz zu einer durch das MI durchgeführten - also in bezug auf eine Gemeinde durchaus abhängigen - Kontrolle kommt. Das Bundesverfassungsgericht[246] hat bereits auf diese von Verfassungs wegen anerkannte wesentliche Schutzvorkehrung abgestellt.

12.5.1.3 Selbstauskunft gegenüber Zweckverbänden

Im Berichtsjahr haben mich Bürger im Zusammenhang mit Selbstauskunftsbogen, die ihnen von Wasser- und Abwasserzweckverbänden zugegangen sind, um Rat gefragt. Dabei ging es ihnen in erster Linie um die **Rechtsgrundlage der Datenerhebung** für die Abwasserentsorgung, wozu ich im einzelnen folgendes ausgeführt habe:

Die Erforderlichkeit der mittels Fragebogen abgefragten Daten begründet sich nach dem **Abwasserabgabengesetz** (AbwAG)[247] des Bundes sowie dem **Brandenburgischen Abwasserabgabengesetz** (BbgAbwAG)[248].

Gemäß §§ 1 und 9 AbwAG ist für das Einleiten von Abwasser von dem Einleiter eine Abgabe zu entrichten. **Abgabepflichtiger** ist nach § 7 Abs. 1 BbgAbwAG die einleitende **Gemeinde** oder der an deren Stelle für die Abwasserentsorgung **zuständige Zweckverband**. Die Abgabe geht an das Land. Weiter regelt die Vorschrift des § 9 Abs. 2 AbwAG, daß bei Einleitungen, die weniger als acht Kubikmeter je Tag betragen, nur eine sog. Kleineinleiterpauschale zu entrichten ist. Dies betrifft vor allem dezentrale häusliche Abwasserentsorgungsanlagen. Wenn der Abgabepflichtige, d. h. der jeweilige Zweckverband, jedoch nachweisen kann, daß das Schmutzwasser in einer Abwasserbehandlungsanlage entsprechend den allgemein anerkannten Regeln der Technik behandelt wird, entfällt die Abgabepflicht gem. §§ 8 Abs. 2 AbwAG und 6 BbgAbwAG.

Damit die **Höhe der Kleineinleiterabgabe** berechnet und die entsprechenden Angaben gegenüber dem Landesumweltamt gemacht werden können, müssen den Zweckverbänden zunächst einmal die Anzahl der Kleineinleiter bekannt sein, und sie müssen nachweisen können, für wieviele Kleineinleitungen sie eine Abgabenbefreiung beanspruchen können. Aus diesem Grunde ist der Kleineinleiter gem. § 11 Abs. 2 AbwAG auch verpflichtet, dem Abgabepflichtigen die notwendigen Daten und Unterlagen zu überlassen. Ein Verstoß gegen diese Erklärungspflicht stellt gem. § 15 Abs. 2 Nr. 2 AbwAG eine Ordnungswidrigkeit dar, die mit einer Geldbuße geahndet werden kann. Außerdem kann der Kleineinleiter gem. § 12 AbwAG dann selbst zu einer Abgabe, die durch Schätzung ermittelt wird, herangezogen werden.

Ich konnte den Betreffenden mitteilen, daß insoweit keine datenschutzrechtlichen Bedenken gegen das Ausfüllen der entsprechenden Fragebögen bestehen.

---

245 im Sinne von Art. 28 Abs. 1 Satz 2 der Richtlinie 95/46/EG vom 24. Oktober 1995, ABl. EG L 281/31

246 BVerfGE 65, 1 ff.

247 i. d. Fass. vom 5. März 1987, BGBl. I S. 880

248 vom 8. Februar 1996, GVBl. I S. 14

Bei der Prüfung o. g. Eingaben habe ich jedoch wieder feststellen müssen, daß bei der **Gestaltung von Fragebögen** noch immer große Defizite vorhanden sind und die Maßstäbe der §§ 12 und 14 BbgDSG nur teilweise oder gar nicht beachtet werden. Unter Bezugnahme auf frühere Darlegungen hierzu[249] habe ich die jeweiligen Zweckverbände über die Gestaltung von Fragebögen umfassend aufgeklärt.

12.5.2 Aktenübergabe beim Zuständigkeitswechsel des jugendärztlichen Dienstes

Im Berichtszeitraum wurde mir folgender Sachverhalt zur ärztlichen Schweigepflicht vorgelegt. Der jugendärztliche Dienst eines Landkreises forderte die Untersuchungsunterlagen einschließlich Impfkartei eines zugezogenen Kindes von dem Gesundheitsamt der Wegzugsgemeinde an. Für die Anforderung wurde ein Formular verwendet, auf dem der Zweck der Übermittlung sowie eine nicht einschlägige Rechtsgrundlage vermerkt war. Das Gesundheitsamt hielt es für einen **Verstoß gegen die ärztliche Schweigepflicht**, wenn es einer solchen Anforderung ohne Einwilligung des Betroffenen bzw. seiner gesetzlichen Vertreter nachkäme. Die vom Gesundheitsamt geltend gemachten Bedenken teile ich:

Aus der Angabe des Zweckes auf dem Anforderungsformular („Zur weiterführenden Dokumentation"...) geht nicht hervor, welche Einzelangaben für den jugendärztlichen Dienst tatsächlich erforderlich sind. Bei einem gesunden Kind dürfte die Kenntnis des Inhalts früherer Untersuchungen grundsätzlich nicht notwendig sein.

Des weiteren wird nicht deutlich, inwieweit dem **Ersterhebungsgrundsatz**, der über § 28 Abs. 6 Brandenburgisches Gesundheitsdienstgesetz (BbgGDG)[250] gem. § 12 Abs. 2 Satz 1 BbgDSG gilt, Rechnung getragen wird, demgemäß Daten grundsätzlich beim Betroffenen mit dessen Kenntnis zu erheben sind. Meines Wissens werden Schüler beispielsweise aufgefordert, ihren Impfausweis zu Reihenuntersuchungen mitzubringen. Sofern diese Aufforderung befolgt wird, bedarf es der Impfkartei beim früheren Gesundheitsamt nicht.

Unabhängig von diesen an Einzelfragen dargestellten Bedenken halte ich eine **Datenübermittlung nach § 28 Abs. 6 BbgGDG** i. V. m. § 14 BbgDSG für unzulässig, da dieser Rückgriff beispielsweise durch die §§ 28 Abs. 3 und 4 BbgGDG ausgeschlossen ist. Die angesprochenen speziellen Regelungen lassen eine Offenbarung der beim Gesundheitsamt bekanntgewordenen Daten nur unter Berücksichtigung von § 203 StGB (ärztliche Schweigepflicht) zu. Nach § 28 Abs. 1 BbgGDG dürfen Einrichtungen des öffentlichen Gesundheitsdienstes personenbezogene Daten übermitteln, soweit ihre Kenntnis zur Erfüllung ihrer Aufgaben nach diesem Gesetz erforderlich ist. Für die Aufgabenerfüllung des ursprünglich zuständigen Gesundheitsamtes ist die Datenübermittlung jedoch nicht erforderlich.

---

249 s. 4. Tätigkeitsbericht unter 2.3

250 vom 3. Juni 1994, GVBl. S. 178

Das von mir über meine vorstehend ausgeführten Bedenken informierte Ministerium für Arbeit, Soziales, Gesundheit und Frauen (MASGF) hält in dem konkreten Fall § 28 Abs. 1 BbgGDG für einschlägig. Es interpretiert diese Vorschrift so, daß danach Einrichtungen des öffentlichen Gesundheitsdienstes personenbezogene Daten immer übermitteln dürfen, soweit die empfangende Stelle diese zur Erfüllung der ihr zugewiesenen Aufgaben bedarf. Speziell beim Kinder- und Jugendgesundheitsdienst lägen Daten vor, die nach § 1 Abs. 1 der Kinder- und Jugendgesundheitsdienstverordnung (KJGDV)[251] gerade zu dem Zweck erhoben würden, die kindliche Entwicklung zu verfolgen, um bei Störungen möglichst frühzeitig eine Korrektur zum Wohle des Kindes herbeizuführen. Dabei werde als Ergebnis der Reihenuntersuchung eine **Befundkette** angelegt, die im Falle eines Wohnungswechsels in einem anderen Landkreis unterbrochen wäre, wenn die bereits erhobenen Daten nicht übermittelt würden. Dies könne nicht im Interesse des betroffenen Kindes sein.

Ich halte die Entscheidung des Gesundheitsamtes, eine Datenübermittlung grundsätzlich nur mit **Einwilligung** des Betroffenen bzw. seiner gesetzlichen Vertreter zuzulassen, für richtig und stimme dem MASGF nicht zu, die Übermittlungsbefugnis in § 28 Abs. 1 BbgGDG so auszulegen, daß sich daraus eine Offenbarungsbefugnis für Daten ergibt, die einem Arzt anvertraut wurden.

12.5.3 Bußgeldstelle in friedensstiftender Mission

Ein Petent hatte sich an mich gewandt, weil die Bußgeldstelle der Stadt Falkensee der Mieterin seines Grundstücks die Halterdaten eines dort abgestellten Fahrzeugs mitgeteilt hatte. Er gab an, dem Fahrzeughalter zuvor erlaubt zu haben, seinen Pkw auf dem vom Mietvertrag nicht erfaßten Teil des Grundstücks abzustellen. Die Mieterin habe ihm angekündigt, daß sie den Fahrzeughalter ermitteln und das Fahrzeug abschleppen lassen werde. Sie habe sich auch tatsächlich an die örtliche Bußgeldstelle gewandt, um über diese den Halter des in einer anderen Gemeinde zugelassenen Fahrzeugs feststellen zu lassen. Dies habe die Bußgeldstelle auch getan. Die Vermutung des Petenten, daß sie die Halterdaten erhoben und übermittelt habe, weil es sich bei der in Rede stehenden Mieterin um eine Mitarbeiterin der Stadtverwaltung handele, scheint mir, nachdem die Stadtverwaltung zu dem Vorfall Stellung genommen hat, nicht ganz abwegig zu sein. Nachdem die Bußgeldstelle der Mieterin die gewünschte Auskunft erteilt hatte, wurde der Halter des Fahrzeugs angerufen und aufgefordert, sein Fahrzeug vom Grundstück zu entfernen, da es anderenfalls abgeschleppt würde. Dem Petenten war auf seine Beschwerde vom Ordnungsamt mitgeteilt worden, daß die Bußgeldstelle rechtmäßig gehandelt habe.

Da die Rechtmäßigkeit der Erhebung und Übermittlung nicht so eindeutig gegeben war, habe ich die Stadtverwaltung mit Verweis auf die hier einschlägige Rechtsvorschrift in § 39 Abs. 1 Straßenverkehrsgesetz (StVG)[252] um Stellungnahme gebeten. Gemäß der Vorschrift ist die Übermittlung von Halterdaten an Privatpersonen grundsätzlich zulässig, wenn der auskunftserteilenden Stelle dargelegt worden ist, daß die Halterdaten zur Durchsetzung von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt werden.

Die Stadtverwaltung hat den von dem Petenten geschilderten Sachverhalt bestätigt und ausgeführt, daß die Bußgeldstelle der Mieterin mit der Mitteilung der Halterdaten Hilfestellung zu einer späteren zivilrechtlichen Auseinandersetzung geben wollte. Rechtsgrundlage für die „friedensstiftende Mission" sei nicht das Straßenverkehrsgesetz, sondern § 16 Abs. 1 Buchst. c BbgDSG, demgemäß die Übermittlung personenbezogener Daten an Privatpersonen zulässig ist, wenn der Auskunftsbegehrende ein rechtliches Interesse an den Daten glaubhaft macht und das Geheimhaltungsinteresse des

---

[251] vom 25. Februar 1997, GVBl. II S. 96

[252] vom 19. Dezember 1952 (BGBl. III / FNA 9231-1)

Betroffenen nicht überwiegt. Den Ausführungen war ein Vermerk der Bußgeldstelle beigelegt, aus dem zu entnehmen war, daß diese die rechtlichen Hindernisse an einer Datenübermittlung sehr wohl gesehen hatte, aber dennoch die Halterdaten in der Zulassungsgemeinde abgefragt hatte, um zur „Vermeidung einer evtl. gerichtlichen Auseinandersetzung zwischen den beiden Parteien und den damit verbundenen Kosten sowie um zu einer gütlichen Einigung beizutragen". Da die Rechtsauffassung und das Vorgehen der Bußgeldstelle trotz und gerade wegen der Begründung nicht hinnehmbar waren, habe ich die unzulässige Datenerhebung und -übermittlung durch das Ordnungsamt gem. § 25 Abs. 1 Nr. 2 BbgDSG gegenüber dem Bürgermeister der Gemeinde beanstandet.

In seiner Stellungnahme machte der Bürgermeister längere Ausführungen über die Rechte eines Mieters gemäß den einschlägigen Vorschriften des Bürgerlichen Gesetzbuches. Er stellte aber auch selbst fest, daß „der vorliegende Fall dem Ordnungsamt keinen Anlaß zum Einschreiten" geboten hatte und damit die Zuständigkeit der Ordnungsbehörde nicht betroffen gewesen war. Anstatt daraus nun aber den Schluß zu ziehen, daß eine nicht zuständige Stelle eben keine Daten erheben und übermitteln darf, hielt der Bürgermeister mit Verweis auf § 16 Abs. 1 Buchst. c BbgDSG die o. g. friedensstiftende Mission der Bußgeldstelle für rechtmäßig. Demgemäß war die einzige Konsequenz, die die Gemeinde aus meiner förmlichen Beanstandung ziehen will, die Anweisung, daß künftig die Bußgeldstelle nur noch schriftliche Anträge auf Halterauskünfte, denen das rechtliche Interesse des Antragstellers an der Auskunft zu entnehmen ist, bescheidet.

Da weder aufgrund der rechtlichen Ausführungen noch aufgrund der in Gang gesetzten praktischen Verfahrensänderungen sichergestellt war, daß das Ordnungsamt bzw. die Bußgeldstelle der Gemeinde in Zukunft den datenschutzrechtlichen Bestimmungen Rechnung tragen würde, habe ich die Stellungnahme zurückgewiesen.

Der Verstoß gegen das Recht des Halters auf informationelle Selbstbestimmung ist vor allem auf die Nichtbeachtung der Zuständigkeit zurückzuführen. Dieser Mangel war auch nicht dadurch behoben, daß die Mieterin ein berechtigtes Interesse an den Halterdaten glaubhaft machte. Es gehört nicht zu den Aufgaben des Ordnungsamtes bzw. der Bußgeldstelle, private Rechtsansprüche durchzusetzen bzw. dazu Hilfestellung zu leisten. § 1 Ordnungsbehördengesetz (OBG)[253] beschränkt die Aufgabenzuständigkeit der Ordnungsbehörde ausdrücklich auf die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung. Jedes Tätigwerden des Ordnungsamtes ist an die Voraussetzung geknüpft, daß ein Tatbestand gem. § 13 OBG vorliegt, der die öffentliche Sicherheit oder Ordnung bedroht. Diese Voraussetzung war hier aber nicht gegeben, da das in Rede stehende Fahrzeug auf einem Privatgrundstück abgestellt war. Der Schutz bzw. die Durchsetzung privater Rechte und damit auch der Ansprüche, die die Mieterin des Grundstücks, auf dem das Fahrzeug abgestellt war, aus dem Mietvertrag ableitet, obliegt gem. § 1 Abs. 2 Brandenburgisches Polizeigesetz (BbgPolG)[254] allein der Polizei.

Das Ordnungsamt bzw. die Bußgeldstelle kann die Zuständigkeit auch nicht aus der allgemeinen Befugnisnorm des § 16 Abs. 1 Buchst. c BbgDSG herleiten. Hiernach ist die Datenübermittlung nur zulässig, wenn die übermittelnde Stelle die Maßnahme im Rahmen ihrer Aufgabenzuständigkeit durchführt. Datenerhebung (im vorliegenden Fall bei der Zulassungsstelle der anderen Gemeinde) und Datenübermittlung kann die Bußgeldstelle nur betreiben, soweit sie erforderlich sind für die Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben. Im vorliegenden Fall hat die Bußgeldstelle außerhalb ihrer Zuständigkeit gehandelt, somit ist die Datenverarbeitung ein rechtswidriger Eingriff in das Recht auf informationelle Selbstbestimmung des Fahrzeughalters.

---

253 Gesetz über Aufbau und Befugnisse der Ordnungsbehörden vom 13. Dezember 1991, GVBl. S. 636

254 vom 19. März 1996, GVBl. I S. 74

Meiner Aufforderung, erneut Stellung zu nehmen, ist die Stadt Falkensee bisher noch nicht nachgekommen.

12.6 Sonstiges

12.6.1 Gemeindevertretung

In der zurückliegenden Zeit war immer wieder die Frage aufgeworfen worden, was und wieviel die Gemeindevertretung oder einzelne Mitglieder von Gemeindevertretungen aus bestimmten Verwaltungsvorgängen erfahren dürfen. Derartige Fragen wurden auch von Gemeindeverwaltungen gestellt. Sie spiegelten dann recht deutlich die Befindlichkeiten und Befürchtungen der Bürger wider, denen es nicht recht ist, daß Bekannte oder Nachbarn, die in einer Gemeindevertretung sitzen, so aus ihren persönlichen Lebensbereichen erfahren können. Die Abgrenzung zwischen dem, was Gemeindevertreter wissen dürfen, weil sie dies zur Wahrnehmung ihres Mandats wissen müssen, und dem, was hierzu unerheblich ist, ist deshalb von großer Relevanz.

Einerseits gibt die Gemeindeordnung (GO) insgesamt nur grobe Vorgaben, sie enthält andererseits **keine ausdrücklichen Regelungen zum Datenschutz**. Aber auch grobe Regelungen sind, wenn bereichsspezifisch, mit Vorrang zu beachten. Meine Behörde sieht sich deshalb immer wieder veranlaßt, Überlegungen anzustellen, auf welche Weise Vorgaben der GO und Datenschutzkriterien in Übereinstimmung zu bringen sind. Bedauerlicherweise waren wiederholte Versuche, Zweifelsfragen im Zusammenwirken mit dem MI zu lösen, nicht erfolgreich.

12.6.1.1 Organisatorische Maßnahmen bei Weitergabe an Gemeindevertretung

Einer Amtsverwaltung ging es darum, generell und grundsätzlich zu klären, ob und in welchem Umfang eine Gemeindeverwaltung Kopien von Grundstückskaufverträgen an die einzelnen Gemeindevertreter übersenden dürfe. Die Mitglieder der Gemeindevertretung hatten darauf bestanden, sich nicht mit einer Einsichtnahme im Amt oder die Entgegennahme von Tischvorlagen begnügen zu müssen. Ich war - ebenso wie die anfragende Gemeindeverwaltung - der Meinung, daß es einerseits nicht erforderlich sei, Gemeindevertretern derart umfassende Daten in deren Wohnungen überlassen zu sollen. Die Möglichkeit, daß unbefugte Dritte dort von den Vorgängen Kenntnis erhalten können, ist sehr groß. Dritte, z. B. Personen, die im Haushalt des Gemeindevertreters leben, sind gerade in kleineren Gemeinden oft sehr daran interessiert, Einzelheiten zu derartigen Vorgängen zu erfahren. Andererseits sind Kontrollen zur Einhaltung der Vorgaben von § 10 BbgDSG für die versendende Gemeindeverwaltung grundsätzlich nicht möglich.

Das MI hat sich meiner Sicht der Dinge nicht angeschlossen. Es hat dem umfassenden Informationsrecht der Gemeindevertreter den Vorrang gegeben und dargelegt, daß die Verpflichtung zur Nichtweitergabe von Informationen dem befürchteten Mißbrauch entgegenwirke. Es sah sich nicht einmal dazu veranlaßt, dem Gesichtspunkt zuzustimmen, daß - einen grundsätzlichen Vorrang des Informationsrechts vorausgesetzt - dann doch in jedem Einzelfall eine Erforderlichkeitsprüfung erfolgen müsse, bevor eine Versendung in die Wohnung der Gemeindevertreter erfolge.

Schließlich hat es das MI auch abgelehnt, eine Rückgabepflicht für solche Unterlagen an die Gemeindeverwaltung vorzugeben. Auch insoweit meint das MI, die Verschwiegenheitspflicht der Gemeindevertreter sei völlig ausreichend. Zu dieser Pflicht gehöre es auch, überlassene Unterlagen ordnungsgemäß aufzubewahren und je nach Wertung zu behalten oder zu vernichten.

Das kann schon deshalb nicht hingenommen werden, weil es nicht einsehbar ist, weshalb Gemeindevertreter, weil sie zum Schweigen verpflichtet sind, beim Einhalten solcher Pflichten zuverlässiger sein sollten als andere Funktionsträger. In jedem anderen Fall würde das Einhalten bestimmter Voraussetzungen, z. B. technisch-organisatorischer Art, als zwingend vorgeschrieben, damit sensible Informationsströme überhaupt fließen dürfen. Meine Darlegung, daß deshalb eine bereichsspezifische Regelung geschaffen werden müsse, mit der Kriterien dafür festgelegt werden, wann und in welchem Umfang sensible Informationsströme überhaupt fließen dürfen, ist nicht aufgegriffen worden.

12.6.1.2 Einsichtnahme von Gemeindevertretern in Unterlagen bei Bürgerbegehren

In einem Fall wollten Gemeindevertreter die **Unterschriftenlisten**, die zur Vorbereitung der **Abwahl des Bürgermeisters** gesammelt worden waren, sehen und überprüfen. Hier handelte es sich vor allem um solche Gemeindevertreter, die der Partei des abwahlbedrohten Bürgermeisters angehörten. Mir wurde berichtet, es habe gegenüber Unterzeichnern und Unterschriftensammlern Drohungen gegeben; einige Unterzeichner hätten sogar wirtschaftliche Nachteile dadurch erlitten, daß sie bei der Vergabe öffentlicher Aufträge durch die Gemeinde, die ja durch den Bürgermeister handelt, nicht (mehr) berücksichtigt worden seien. Vorhandene Unterlagen seien (nachträglich) verändert worden.

Ausgehend von der Grundsatzentscheidung des Gesetzgebers, daß gem. § 36 GO Gemeindevertretern ein umfassendes Informationsrecht zustehen muß, weil dies der Vorbereitung der Entscheidungen des Gremiums und zur Kontrolle der Verwaltung erforderlich ist, war hier die Kernfrage, ob bei derartigen Bürgerbegehren überhaupt eine solche Aufgabenlage gegeben ist. Wahlen gehören nämlich nicht zu den Aufgaben, die durch die Gemeindevertretung wahrzunehmen sind. **In Wahlunterlagen dürfen Gemeindevertreter** - im Gegensatz zu anderen Unterlagen - **grundsätzlich nicht Einsicht nehmen**, es sei denn, es wäre eine Wahlprüfung vorzunehmen und es würde nach den gesetzlich vorgegebenen Verfahren vorgegangen.

Auch wenn ein Bürgerbegehren nicht einem Wahlvorgang im engeren Sinne gleichzusetzen ist, führt das hierbei praktizierte Verfahren, sein Votum in einer bei der Unterzeichnung offen einsehbaren Liste abgeben zu müssen, bei wahlähnlichen Vorgängen nicht dazu, daß der demokratische Grundsatz, Wahlen geheim durchzuführen, überhaupt nicht gilt. Das Votum eines Unterzeichners gehört zu dessen persönlichem Entscheidungsbereich und muß nicht von ihm begründet werden. Darüber muß er keine Rechenschaft ablegen. Die Entscheidung muß auch ohne Angst vor Repressalien getroffen werden können.

Die Folgerung hieraus ist, daß der Kreis derjenigen Personen, die, damit ein in der Verfassung des Landes Brandenburg verankertes Recht (Art. 22 Abs. 1) verfahrensmäßig korrekt durchgeführt werden kann, unumgänglich mit den Listen befaßt sein muß, so klein wie möglich gehalten werden muß. Daher prüfen in jedem Fall die Mitarbeiter des Meldeamtes und der Wahlleiter die Unterlagen; erst wenn es Anzeichen von Unregelmäßigkeiten geben sollte, die durch diesen Personenkreis nicht ausgeräumt werden können, ist so etwas wie eine Wahlprüfung, d. h. die Befassung durch die Gemeindevertreter oder einer dafür zusammengestellten Gruppe von Gemeindevertretern, zulässig, weil erforderlich.

In bezug auf diese grundsätzliche Frage nach der Einsichtsberechtigung und Aushändigung solcher Listen hat sich das MI dafür ausgesprochen, daß für die Gemeindevertreter eine Einsichtnahme in die Unterlagen unbeschränkt zulässig sei. Das ergebe sich aus § 20 Abs. 2 Satz 1 der GO und aus § 81 Abs. 2 Brandenburgisches Kommunalwahlgesetzes (BbgKWahlG a. F.).[255] Der Datenabgleich zwischen Melderegister und Unterschriftenlisten wird vom MI als „Vorprüfung" bezeichnet; die

[255] vom 22. April 1993, GVBl. I S. 110, geänd. durch Art. 2 Ges. z. Änd. d. BbgKWahlG vom 14. Dezember 1995, GVBl. I S. 274

eigentliche Prüfung des Vorliegens der Voraussetzung für einen Bürgerentscheid - ein erfolgreiches Bürgerbegehren - liege im Entscheidungsbereich der Gemeindevertretung, daher dürfe sie zur Vorbereitung ihrer Entscheidung vollständige Einsicht in die Unterlagen erhalten.

Tatsächlich hat die Gemeindevertretung aber nach dem Wortlaut von § 81 Abs. 2 BbgKWahlG (a. F.) nicht eine Entscheidung, sondern eine **Feststellung** zu treffen; die Vorschrift lautet(e): „(2) Die Vertretung stellt die Zulässigkeit des Bürgerentscheids fest". Weitere Aussagen enthielt die frühere Fassung des KWahlG nicht. Eine solche „Feststellung" ist allerdings erforderlich, damit auf einer solcherart verbindlichen Basis (d. h. des erfolgreichen Bürgerbegehrens) der nächste vom Gesetz vorgesehene Schritt, der Bürgerentscheid, folgen kann.

Der Sicht des MI bezüglich dieser Angelegenheit schließe ich mich nicht an. Eine nachträgliche und opportunistisch (positive) Beurteilung eines tatsächlichen Vorgangs mit der bedauerlichen Folge, daß ein solches Gutheißen Folgewirkungen bei anderen ähnlichen Vorkommnissen nach sich ziehen könnte, kann aus meiner Sicht auch nicht dazu führen, eine schief gelaufene Angelegenheit mit Schweigen zu übergehen.

Eine neue Beurteilung derartiger Angelegenheiten ergibt sich aber aus der neuen Gesetzeslage. Die kürzlich gerade in bezug auf die Bürgermeisterabwahl neu gefaßte Regelung im BbgKWahlG[256] enthält etwas genauere Ausführungen zum Verfahren beim Bürgerbegehren. § 81 Abs. 6 lautet:

> „(6) Der Wahlleiter ermittelt unverzüglich das Ergebnis des Bürgerbegehrens. Die Vertretung stellt in öffentlicher Sitzung nach Anhörung des Wahlleiters fest, ob das Bürgerbegehren zustande gekommen ist; sie ist an die Ergebnisermittlung des Wahlleiters nicht gebunden."

Im Gesetz ist damit eindeutig festgelegt worden, wer bzw. welche Einrichtung das Ergebnis des Verfahrens zu ermitteln hat - hierzu ist der Wahlleiter bestimmt worden. Die Gemeindevertretung nimmt hierauf aufbauend die (amtliche) Feststellung vor, ob das soeben beendete Bürgerbegehren erfolgreich verlaufen war oder nicht und gibt mit der Feststellung, daß das Bürgerbegehren erfolgreich verlaufen sei, den Weg frei für den nächsten Verfahrensschritt, den Bürgerentscheid. Die Gemeindevertretung ist allerdings dem Gesetzestext zufolge an die Ergebnisermittlung nicht gebunden. Dies trägt der Souveränität der Gemeindevertretung Rechnung; sie muß sich zwar an die Ermittlungen des Wahlleiters halten, sofern sie keine konkreten Argumente gegen das ermittelte Ergebnis hat. Aus rechtlichen Erwägungen heraus soll es nicht der Wahlleiter, sondern die gewählte Gemeindevertretung sein, die eine derart gewichtige Feststellung verbindlich zu treffen hat.

256 s. unter 3.1.3.1

12.6.1.3 Datenweitergabe in Stadtverordnetenversammlung

In dem folgenden Fall hatten sich mehrere Petenten an mich gewandt, weil sie es nicht hatten hinnehmen wollen, daß ihre ganz persönlichen Fälle in der Stadtverordnetenversammlung in **öffentlicher Sitzung** thematisiert worden waren. Die betreffende Stadt hatte den Petenten mittels Einzelentscheiden Förderungsbeträge zur Herrichtung ihrer Häuser zukommen lassen. Das Verfahren selbst ist weder bezüglich des Ablaufs noch hinsichtlich der Höhe der ausgereichten Gelder angegriffen worden. Einige Monate nach **Vornahme der Förderungsverfahren** legte die Stadt förmlich ein städtebauliches Sanierungsgebiet fest. Sie bezog die Grundstücke der Petenten - nachträglich - in das Sanierungsareal ein. Hiergegen wehrten sich die Betroffenen durch förmlichen Widerspruch und trugen dazu vor, zwischen ihrer Förderung und der Festlegung des Sanierungsgebiets gebe es keinen zeitlichen und sachlichen Zusammenhang.

Das Verfahren zur Gewährung der Fördermittel war korrekterweise unter Ausschluß der Öffentlichkeit durchgeführt worden. Das nachträgliche Öffentlichmachen habe ich als ein Unterlaufen der die Nicht-Öffentlichkeit regelnden Vorschriften der GO angesehen und gegenüber der städtischen Verwaltung kritisiert. Die Gemeindevertretung hätte zur Behandlung des betreffenden Vorgangs vor Beginn der Beratung dieses Punktes ohne weiteres die Öffentlichkeit ausschließen können; leider muß man hier annehmen, daß es tagespolitische Gründe waren, die dazu geführt hatten, die Angelegenheit an die Öffentlichkeit zu bringen.

12.6.1.4 Weitergabe eines Protokolls an private Dritte

Im Zuge einer Sanierungsmaßnahme, die u. a. auch gärtnerische Maßnahmen umfaßte, war dem damit betrauten Gartenbauunternehmen statt eines regulären Auftrags oder einer Vertragsausfertigung die Kopie eines Gesprächsprotokolls der Geschäftsstelle des Umlegungsausschusses ausgehändigt worden. Dem Gesprächsprotokoll waren allerdings nicht nur die genauen vorzunehmenden Aktionen an dem Grundstück des Betroffenen - d. h. das, was die Auftragnehmerin wissen mußte -, sondern daneben auch die vereinbarten Zahlungen und Entschädigungen an den Betroffenen zu entnehmen gewesen.

Dadurch, daß ordnungsgemäß ermittelte und ausgereichte Entschädigungsbeträge in der Öffentlichkeit bekannt wurden, hatte der Betroffene Nachteile erlitten; hiergegen hatte er sich gewehrt. Ich habe dem zuständigen Oberbürgermeister gegenüber zum Ausdruck gebracht, daß der Vorgang für ihn Anlaß sein sollte, durch geeignete Maßnahmen derartige Verfahrensweisen in seinem Zuständigkeitsbereich künftig zu unterbinden.

12.6.1.5 Zulässigkeit von Bürgerbefragungen in Kommunen

Ein Petent fragte an, ob die Stadtverwaltung befugt sei, eine Bürgerbefragung zur Frage der Trassierung einer Stadterschließungs- und Entlastungsstraße durchzuführen. Es ging darum, zu erfahren, ob die Bevölkerung eher die mögliche nördliche oder die gleichfalls mögliche südliche Trassenführung akzeptieren wollte. Die Befragungsergebnisse sollten dazu dienen, der Gemeindevertretung bei der Entscheidungsfindung zu helfen.

In diesem Fall habe ich bestätigt, daß die Stadt eine derartige Befragung durchführen kann. Dabei ist allerdings unverzichtbar, daß den Bürgern verdeutlicht wird, daß jede Antwort freiwillig gegeben wird und auch unvollständige Beantwortungen zulässig sind.

Die Stadt habe ich auf die Vorschriften hingewiesen, die für den Umgang mit so erhobenen Daten - insbesondere der

Aufbewahrung und der Löschung - bestehen und um die genaue Einhaltung der Vorgaben gebeten. Der dafür verantwortliche Bürgermeister hat mir zugesagt, sich an die Vorgaben halten zu wollen.

12.6.1.6 Offenbarung personenbezogener Daten in Amtsblatt der Gemeinde

Im Amtsblatt einer Gemeinde stand ein Artikel mit dem Titel: „Überprüfungsergebnisse der „Gauck-Behörde" für die Mitglieder der Gemeindevertretung liegen vor". Der Artikel ist mit dem Namen und der Amtsbezeichnung des Vorsitzenden der Gemeindevertretung unterzeichnet und betrifft zwei Gemeinderatsmitglieder; die mit vollem Namen und mit ihrer Parteizugehörigkeit genannt sind.

Durch eine Petition wurde ich auf diese für jeden Leser erkennbare Verletzung des Datenschutzes aufmerksam gemacht. Gegenüber dem Bürgermeister als dem für die Veröffentlichungen im Amtsblatt der Gemeinde Verantwortlichen habe ich diesen Umgang mit personenbezogenen Daten förmlich beanstandet. Dabei habe ich darauf hingewiesen, daß in einem solchen Fall nicht etwa darauf abgestellt werden kann, daß die Gemeindevertretung oder deren Vorsitzender eine derartige Veröffentlichung eines Überprüfungsergebnisses gebilligt oder gefordert hatte.

Personenbezogene Daten hätten nur unter den Voraussetzungen von § 16 BbgDSG weitergegeben werden dürfen oder wenn die Betroffenen der Veröffentlichung zugestimmt hätten. Für den Bürgermeister - und für den unterzeichnenden Vorsitzenden der Gemeindevertretung - war ohne weiteres erkennbar, daß keine der beiden Voraussetzungen gegeben war. Die Veröffentlichung war deshalb widerrechtlich vorgenommen worden.

12.6.2 Standesamt zu Unrecht verdächtigt

Die Beobachtung, daß insbesondere ein bestimmtes Versicherungsunternehmen über aktuelle Daten Neugeborener einer kreisfreien Stadt verfügte und auf diese Weise unmittelbar mit günstigen Angeboten zur Familienversicherung an die Mütter herantreten konnte, ließ den Verdacht aufkommen, daß die Daten unzulässigerweise von Bediensteten des Standesamts oder des städtischen Klinikums übermittelt würden.

Aufgrund meiner Nachforschungen konnte ich beide Möglichkeiten mit ziemlicher Sicherheit ausschließen. Allerdings war zu ermitteln, daß im gynäkologischen Bereich des Klinikums diverse Gutscheine und Teilnahmescheine für Gewinnspiele ausliegen, die insbesondere werdende Eltern ansprechen. Dabei bieten die jeweiligen Firmen insbesondere Kindernahrung, Baby-Bekleidung, aber auch direkt oder über die Teilnahmescheine indirekt Versicherungsschutz für Babys oder junge Familien an. Datenschutzrechtlich sind derartige Angebote unbedenklich, da das jeweilige Unternehmen Anschriften und nähere familiäre Umstände nur über die Eltern selbst erfährt, wenn diese das Angebot annehmen und sich insoweit mit dem Unternehmen freiwillig in Verbindung setzen.

Obwohl ein datenschutzrechtlicher Mangel nicht feststellbar war, sind meine Ermittlungen vorsorglich zum Anlaß genommen worden, im Mitarbeiterkreis der Klinik und des Standesamts der Stadtverwaltung nochmals auf die strikte Einhaltung der Datenschutzbestimmungen hinzuweisen. Nicht zuletzt wurde in diesem Zusammenhang auch festgelegt, daß zukünftig im Amtsblatt der Stadt nicht mehr die vollständigen Wohnanschriften bei Geburten und Sterbefällen veröffentlicht werden.

12.6.3 Telefonrecherchen durch private Auskunftsunternehmen

Aufgrund eines Pressebericht war ich im Sommer 1997 darauf aufmerksam gemacht worden, daß sich in Berlin ein privates Wirtschaftsunternehmen über Jahre hinweg im Wege von Telefonrecherchen illegal eine Vielzahl personenbezogener Daten einzelner Bürger bei öffentlichen Stellen beschafft hatte. Das Unternehmen erschlich sich die Auskunft durch das Vorspiegeln falscher Tatsachen und falscher Amtsbezeichnungen und Titel: beispielsweise durch Auftreten als Polizeibeamter oder Richter.

Ungeachtet einer möglichen Strafwürdigkeit solchen Vorgehens ist es doch vor allem nicht möglich, dem geschädigten Bürger nachträglich den erforderlichen Schutz zukommen zu lassen. Die erschlichenen Daten werden längst wirtschaftlich verwertet oder an Dritte weiterveräußert.

Ich habe deshalb allen Landkreisen und kreisfreien Städte des Landes schriftlich mitgeteilt, daß die Mitarbeiter in den Verwaltungen anzuweisen sind, daß an Dritte keine **personenbezogenen Auskünfte am Telefon** gegeben werden. Im **Regelfall** solle der jeweilige Gesprächspartner unter Hinweis auf die datenschutzrechtlichen Vorschriften aufgefordert werden, seine Anfrage schriftlich zu stellen. In **Eilfällen** besteht die Möglichkeit, daß der Gesprächspartner zurückgerufen wird. Hierbei ist jedoch zu prüfen und strikt darauf zu achten, daß es sich bei der von dem jeweiligen Gesprächspartner angegebenen Nummer tatsächlich um die Rufnummer der entsprechenden öffentlichen Stelle oder des entsprechenden Amtes handelt. In Zweifelsfällen empfiehlt es sich, die Rufnummer des Amtes zu ermitteln und sich über die Telefonzentrale zu dem Gesprächspartner vermitteln zu lassen.

Die Beschaffung und Veräußerung personenbezogener Daten ist angesichts der **wirtschaftlichen Verwertbarkeit** solcher Daten ein einträgliches Geschäft, so daß ich davon ausgehen muß, daß der geschilderte Fall kein Einzelfall ist bzw. daß er Nachahmer finden wird. Da die öffentlichen Stellen in besonderem Maße dazu verpflichtet sind, das vom Grundgesetz gewährleistete Recht des Bürgers auf informationelle Selbstbestimmung zu wahren und zu schützen, dürfte der mit den geschilderten Maßnahmen verbundene Mehraufwand für die öffentliche Verwaltung mehr als gerechtfertigt sein.

13 Personaldatenverarbeitung

13.1 Verwaltungsvorschriften zur Personalaktenführung

Über die Erforderlichkeit umfassender Regelungen zur Personalaktenführung sowie zu deren inhaltlicher Ausgestaltung, aber auch über die Gründe, die eine praktische Umsetzung noch verhindern, habe ich mich ausführlich in meinem letzten Tätigkeitsbericht befaßt[257]. Leider konnte vom Ministerium des Innern (MI) bis dato auf Landesebene noch keine einheitliche Position zur Schaffung einer für die obersten Landesbehörden und deren nachgeordneten Behörden allgemein verbindlichen, für die Kommunen zumindest zur Anwendung empfohlenen Verwaltungsvorschrift über die Führung von Personalakten der Dienstkräfte des Landes Brandenburg (PersaktVV) gefunden werden, weil die einzelnen Ministerien in ihrem Meinungsspektrum im Detail noch zu weit auseinanderliegen. Auch Abstimmungen mit den Spitzenorganisationen der Gewerkschaften und zusätzlich mit dem Ministerium der Finanzen (MdF), das seit kurzem für alle tarifrechtlichen Grundsatzangelegenheiten zuständig ist, stehen noch aus. Zudem scheint gerade der Grundsatzmangel an einer geeigneten materiell-technischen Regelungsgrundlage auch für nichtbeamtete Dienstkräfte, den ich - selbst nach Meinung des MI - zu Recht hervorheben mußte, einer untergesetzlichen Regelung nicht gerade förderlich zu sein. Ich kann mit meinen Kolleginnen und Kollegen in den anderen Bundesländern nur immer wieder dringend die Forderung nach einer allgemeinverbindlichen spezialgesetzlichen Ausgestaltung des **Arbeitnehmerdatenschutzrecht**s an alle Funktionsträger und Gremien, die hier gesetzesinitiativ werden können, herantragen.

Im Detail sind die Auseinandersetzungen des MI mit meinen im letzten Tätigkeitsbericht erhobenen Forderungen und vorgetragenen Anregungen und Empfehlungen[258] wiederum ausschließlich der Stellungnahme der Landesregierung (Stellungnahme)[259] hierzu zu entnehmen. Dabei wird übereinstimmend mit mir bestätigt, daß bis auf wenige Punkte einvernehmliche Lösungen gefunden wurden. In der in meinem letztjährigen Tätigkeitsbericht gewählten Reihenfolge gehe ich noch einmal auf den letzten Stand bezüglich der Punkte ein, die noch mit dem MI zu verhandeln waren:

Zugriffsrecht des Geheimschutzbeauftragten

Meiner Kritik, daß Geheimschutzbeauftragte unmittelbar Einblick in Personalakten sollen nehmen können, setzte das MI entgegen, daß nach der Gesetzesbegründung zu dem mit § 57 Abs. 3 Landesbeamtengesetz (LBG)[260] inhaltsgleichen § 90 Abs. 3 Bundesbeamtengesetz (BBG)[261] im Zusammenhang mit dessen Novellierung[262] im Rahmen ihrer Aufgaben nach den Sicherheitsrichtlinien auch Geheimschutzbeauftragte zu den allgemeinen mit Personalangelegenheiten befaßten Beschäftigten gehören. Stichhaltig scheint mir auch das Argument zu sein, daß der Eingriff in die Persönlichkeitsrechte ungleich größer ist, wenn eine Auskunftserteilung aus der Personalakte an den Geheimschutzbeauftragten den originär zugangsberechtigten Dienstkräften vorbehalten wäre, weil diese wiederum im Zusammenhang mit der Anfrage unzulässige Rückschlüsse auf den Kenntnisstand des Geheimschutzbeauftragten ziehen könnten.

---

257 s. 5. Tätigkeitsbericht unter 13.1

258 vgl. unter 3.1.1 und 3.1.4

259 LT-Drs. 2/4768 vom 15. Dezember 1997

260 vom 24. Dezember 1992, GVBl. I S. 506; zul. geänd. durch Art. 1 d. 2. HaushaltsstrukturG 1997 vom 17. Dezember 1996, GVBl. I S. 363

261 i. d. Fass. vom 27. Februar 1985. BGBl. I S. 479; zul. geänd. durch Art. 12 Abs. 7 PostneuordnungsG vom 14. September 1994 (BGBl. 2030-2)

262 BT-Drs. 12/544, S. 17

Meine Kritik bezog sich allerdings überwiegend auf den formalrechtlichen Aspekt, daß für ein unmittelbares Einsichtsrecht des Geheimschutzbeauftragten eine materiell-rechtliche Grundlage fehle. Dieser Umstand wird mit der in absehbarer Zeit zu erwartenden Verabschiedung eines Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen in Brandenburg bereinigt sein. Einem ersten Entwurf eines Sicherheitsüberprüfungsgesetzes (Stand: 16. Dezember 1997)[263] ist zu entnehmen, daß mit den Regelungen in § 15 eine hinreichende Rechtsgrundlage gegeben sein wird, die die zuständige Stelle (den Geheimschutzbeauftragten) berechtigt, bei einer erforderlichen Sicherheitsüberprüfung im Zusammenhang mit einer sicherheitsempfindlichen Tätigkeit die Personalakten der zu überprüfenden Person einsehen zu können.

Kopierrechte Betroffener an Berichten des BStU

Die Landesregierung wird in diesem Punkt meinen Rechtsausführungen[264] nicht folgen. Ich stelle in Aussicht, daß meine Dienststelle bei diesbezüglichen Anfragen von Behörden auf den bisherigen Argumentationsaustausch mit dem MI verweisen und bei Anfragen Betroffener zusätzlich anheimstellen wird, den Rechtsweg zu beschreiten.

Einsichtsrechte - vom Beschäftigungsverhältnis abhängig?

Ich begrüße die in dem direkten Gespräch mit dem MI erhaltene Zusage, bezüglich meiner Forderung nach einer gleichbehandelnden Regelung für Beamte und Arbeitnehmer zu den Einsichtsrechten in Personalakten[265] eine „möglichst einvernehmliche Formulierung" zu finden.

Behandlung der Vorakten - eher ein Problem der Praxis

In ihrer Stellungnahme geht die Landesregierung leider nicht auf meine Forderung nach einer materiell-rechtlichen Grundlage für die (weitere) Behandlung und Aufbewahrung der Vorakten (Kaderakten)[266] ein. Deren Erforderlichkeit wird - ungeachtet rechtlicher Überlegungen - bereits dadurch erkennbar, daß bis dato selbst für eine zufriedenstellende verwaltungspragmatische Lösung nicht einmal innerhalb der Landesverwaltung Konsens hergestellt werden konnte.

Bis dahin wird meine Behörde allerdings - auf der Basis des bisher gefundenen Einvernehmens mit dem MI - von allen Beschäftigungsbehörden zumindest fordern, daß die nicht (mehr) unmittelbar zur fortlaufenden Bearbeitung benötigten Teile der Vorakten bis auf weiteres im Zugriffsbereich der Personalstellen - allerdings getrennt von der Personalakte, verschlossen sowie als im datenschutzrechtlichen Sinne gesperrt - belassen werden.

Anläßlich einer Reihe von Kontrollbesuchen bei Personalstellen mehrerer unmittelbarer und mittelbarer Landesbehörden sowie Kommunalverwaltungen[267] fielen mir die unterschiedlichsten Handhabungen auf. Soweit ich feststellen konnte, daß Altvorgänge nicht (mehr) unmittelbar für die Führung der aktuellen Personalakten benötigt werden, habe ich jeweils dringend empfohlen, erforderlichenfalls anlaßbedingt (im Zusammenhang mit jedem nächsten Bearbeitungsvorgang an der Personalakte), im übrigen bei Behörden mit hohen Beschäftigungszahlen zumindest sukzessive innerhalb eines

263 s. unter 3.4.1

264 s. 4. Tätigkeitsbericht unter 13.2.4 und 5. Tätigkeitsbericht unter 13.1.3.2

265 s. 5. Tätigkeitsbericht unter 13.1.3.3

266 s. 5. Tätigkeitsbericht unter 13.1.3.4

267 s. unter 13.2.1

Zeitraumes von etwa zwei Jahren, also bis zum Ende des Jahres 1999, eine Bereinigung in der o. a. Weise durchzuführen.

13.2 Sonstiges

13.2.1 Informations- und Kontrollbesuche bei personalaktenführenden Stellen des Landes

Vor dem Hintergrund meiner bisherigen Beobachtungen, daß mangels einheitlich bindender materiell-rechtlicher Regelungen zum Arbeitnehmerdatenschutz bei der Personalaktenführung weder inhaltlich eine Gleichbehandlung zwischen Beamten und Arbeitnehmern noch aus grundsätzlichen organisationsrechtlichen Gründen eine einheitliche Umsetzung datenschutzrechtlicher Erfordernisse bei Personalstellen der unmittelbaren und mittelbaren Landesverwaltungen bzw. im Kommunalbereich garantiert ist[268], habe ich den Versuch unternommen, mir vor Ort einen Überblick über derzeitige Gegebenheiten und Handhabungen zu verschaffen.

Dazu war es auch erforderlich zu erfahren, ob Informationen, Empfehlungen, Dienstanweisungen einschließlich DV-Regelungen u. ä. intern und/oder (ggf.) im Aufsichtswege zu praktischen, rechtlichen und technisch-organisatorischen Problemen bei der Behandlung von Personal(akten)daten vorhanden sind. Hierbei war für mich von besonderem Interesse, in welcher Weise speziellen Aufbewahrungserfordernissen sowohl in der inhaltlichen Behandlung als auch bzgl. der räumlichen Unterbringung Rechnung getragen ist (z. B. bei Vorakten, „Gauck-Bescheiden").

Unter dem Aspekt der mißlichen Rechtslage sah ich als Hauptziele meiner nach dem Zufallsprinzip ausgewählten, exemplarischen Kontrollbesuche bei zwei Ministerien, zwei Schulämtern, drei Kreisverwaltungen, drei Gemeinden (kreisfreie Stadt, amtsfreie Gemeinde, Amtsgemeinde) sowie drei Körperschaften des öffentlichen Rechts:

- Verwertung der Prüfungsergebnisse zur sachlichen und argumentativen Unterstützung des MI bei der Durchsetzung einheitlicher Personalaktenverwaltungsvorschriften (PersaktVV)[269] unter hinreichender Berücksichtigung relevanter Datenschutzaspekte, die bezüglich des Kommunalbereichs zumindest empfehlenden Charakter hätten,

- in jedem Fall die Schaffung einer internen Grundlage für spätere anlaßbedingte Überprüfungen und für Bewertungen rechtlicher und technisch-organisatorischer Probleme im Personaldatenbereich,

- im übrigen die Sachstandsfeststellung zum Zweck der Erweiterung meines Kenntnisstandes bei der datenschutzrechtlichen Begleitung neuer technischer Entwicklungen im Bereich der automatisierten Verarbeitung von Personaldaten.

Dazu war vor Ort insbesondere durch Inaugenscheinnahme der örtlichen Gegebenheiten, stichprobenartige Akteneinsichtnahme, ggf. Programmaufrufe, sowie Gesprächsführung mit Verantwortlichen festzustellen,

- inwieweit inhaltlich, formal und hinsichtlich der Behandlung und Verwahrung sowie des Zugriffsschutzes Personaldaten/Personalaktendaten entsprechend den bisher von mir entwickelten und vorgestellten Anforderungen an den Datenschutz bzw. den von mir mitgetragenen Anordnungen und Empfehlungen des MI behandelt werden,

---

[268] s. 5. Tätigkeitsbericht unter 13.1.1

[269] s. unter 13.1

- auf welchem Stand mit welchen evtl. Problemen sich die automatisierte Personaldatenverarbeitung bezüglich eigener Verarbeitung, Datenverarbeitung im Auftrag, evtl. Funktionsübertragungen und bei Einsatz in Netzen, hierbei speziell im Einsatz von PERIS (bei Landesverwaltungen) und APSIS (im Bereich der staatlichen Schulämter), befindet.

Zu den Gesprächen hatte ich die verantwortlichen Leiter der personalaktenführenden Stelle oder deren Vertreter, zugriffsberechtigte Mitarbeiter, die EDV-Verantwortlichen bzw. Systemverwalter und die behördlichen Datenschutzbeauftragten als Gesprächspartner hinzugebeten.

Selbst wenn wegen der Anzahl der besuchten Personalstellen keine repräsentativen Aussagen gemacht werden können, lassen sich im Ergebnis doch einige interessante Feststellungen treffen bzw. wichtige Rückschlüsse ziehen:

- Der Standard der **Datensicherungsmaßnahmen im Zusammenhang mit der Unterbringung** der manuell geführten Personalgrundakten und der dazugehörenden Teilakten scheint durchgängig recht hoch zu sein. Allerdings habe ich vereinzelt bemängeln müssen, daß ausgesonderte Vorgänge oder listenförmige Ausdrucke wie Gehalts- und Lohnlisten, nicht zugriffssicher untergebracht waren. Da auch bei ordnungsgemäßer Unterbringungsmöglichkeit nicht immer gewährleistet werden kann, daß bei Büroschluß alle in Bearbeitung befindlichen Personalaktenvorgänge weggeräumt und verschlossen werden, habe ich empfohlen bzw. mir bestätigen lassen, daß Reinigungskräfte im gesamten Personalaktenbereich ausschließlich während der Dienstzeit und somit unter Beobachtung der verantwortlichen Bediensteten ihre Arbeiten verrichten. Bei den zugriffsberechtigten Beschäftigten war allgemein eine hohe Sensibilität hinsichtlich der persönlichen Behandlung der Personalvorgänge, insbesondere bezüglich der zu beachtenden Geheimhaltungsgebote im Zusammenhang mit Akteneinsichtnahmen oder der Herausgabe von Informationen, festzustellen.

- **Interne Dienstanweisungen** o.ä. zur Personalaktenführung waren bis auf drei Ausnahmen (zwei Körperschaften des öffentlichen Rechts und eine Amtsgemeinde) in unterschiedlicher Qualität und mit sehr unterschiedlichen Regelungsinhalten zumindest hinsichtlich des Aufbaus und der Gestaltung der Personalgrund- und Personalteilakten vorhanden, wobei die staatlichen Schulämter die Führung ihrer Personalakten und sonstigen Personalunterlagen nach einheitlichen Regelungen[270] ausrichten, die zumindest in den eingeschränkt vorhandenen Teilen weitgehend den beabsichtigten PersaktVV entsprechen, mit diesen aber wohl noch in Übereinstimmung gebracht werden müßten.

  Bedauerlich ist, daß der Entwurf der PersaktVV bisher offensichtlich nur den obersten Landesbehörden bekannt gegeben worden ist, dessen Existenz nach meinen Feststellungen bislang nicht einmal auf Kreisebene bekannt war. Ich meine, daß insbesondere auch das Umfeld der personellen, räumlichen und finanziellen Möglichkeiten in den Kommunen bei den Lösungen für eine möglichst umgehende Umsetzung der PersaktVV berücksichtigt werden muß. Immerhin waren bei allen Stellen - mit Ausnahme der bislang insoweit wohl ziemlich auf sich allein gestellten Körperschaften des öffentlichen Rechts - zumindest bisherige Anweisungen und Empfehlungen des MI bezüglich der Personalaktenführung bekannt oder sind von diesen dort angebotene Seminare in Anspruch genommen worden.

- Die inhaltliche Gestaltung, der Aufbau sowie die Aufteilung der Personalakten zeigte sich in unterschiedlichster Weise. So waren teilweise überhaupt keine **Aktenvorblätter** vorhanden, damit verbunden fanden sich auch keine Hinweise auf Anzahl, Bearbeitungsort und sachlichen Inhalt evtl. vorhandener Teilakten. In diesen Fällen habe ich empfohlen, bis

[270] Rundschreiben Nr. 110/93 des MBJS vom 8. November 1993

zum Erlaß der PersaktVV wenigstens auf der Umschlagsseite der **Personalgrundakte** innen diesbezügliche nachvollziehbare Hinweise anzubringen. In anderen Fällen besteht überhaupt keine Personalgrundakte, die Vorgänge sind hier nicht chronologisch, sondern einzelnen Bearbeitungsschritten (z. B. Einstellung, Bewährungsaufstieg, Genehmigung von Sonderurlaub, Dienstreisen) zugeordnet, ohne daß dies den in dem Entwurf der PersaktVV vorgesehenen Kriterien für das Anlegen von **Teilakten** entsprechen würde. Korrekt waren jedoch stets die Beihilfevorgänge völlig von den übrigen Personalakten getrennt, Kindergeldvorgänge allenfalls zusammen mit den Vorgängen der Gehalts- und Lohnzahlung geführt.

Beachtlich ist das mir entgegengehaltene Argument, daß durch den auf dem Aktenvorblatt der Personalgrundakte dokumentierten Hinweis auf Teilakten (z. B. Disziplinarakten), die wegen Fristablaufs schon vernichtet werden mußten z. B. bei erforderlicher Weitergabe der Personalakten an eine andere Dienstbehörde, möglicherweise mehr Schaden für den Betroffenen entstehen könnte, als wenn auf die Hinweispflicht verzichtet würde. Hier könnte ein System weiterentwickelt werden, das von einer der aufgesuchten Körperschaften des öffentlichen Rechts praktiziert wird. Danach würden aus einem in jeder Personalakte auf die Deckelinnenseite eingeklebten Inhaltsverzeichnis sämtliche möglichen Teilakten, deren mögliche Bestandteile und deren Standort ersichtlich sein. Erst bei Einsichtnahme in eine der in Betracht zu ziehenden Teilakten wäre anhand des dort vorangestellten konkreten Aktenvorblatts festzustellen, ob (noch) Vorgänge vorhanden sind. Im Falle des obigen Beispiels würde der Teilakte Disziplinarakten nach Vernichtung lediglich wieder ein leeres Aktenvorblatt vorangeheftet werden müssen, um jeden Hinweis auf den früheren Vorgang zu verhindern. Meine Behörde wird dieses vermutlich noch zu modifizierende Verfahren in den vorgesehenen weiteren Gesprächen mit dem MI in der Hoffnung vortragen, daß es in den PersaktVV noch Berücksichtigung finden wird.

Ein großes Problem stellt die Tatsache dar, daß ganz offensichtlich bislang nur wenige Dienststellen die Personalakten fortlaufend numerieren. Dadurch ist es unmöglich, die Vollständigkeit der Vorgänge sowohl in den Grund- als auch in den Teilakten nachzuweisen. Betroffene können aber die mit ihrem Akteneinsichtsrecht verbundenen Schutzziele nur angemessen nutzen, wenn sie auf die **Vollständigkeit der Akteninformationen** vertrauen können. Ich habe den betreffenden Personalstellen noch vor Ort geraten, die Personalaktenteile zumindest anlaßbedingt, d. h. bei jedem aktuellen Bearbeitungsvorgang, sukzessive nachzupaginieren, soweit die Teilakten auch heute bereits den Zuordnungskriterien des Entwurfs der PersaktVV entsprechen. Den Grundsätzen der Vollständigkeit von Personalakten einerseits und der Wahrung schutzwürdiger Interessen der Betroffenen andererseits wird bei Bereinigung einzelner Aktenteile letztlich nur angemessen nachgekommen werden können, wenn ersatzweise ein von der Personalstelle und dem Betroffenen unterzeichnetes Protokoll mit Angabe der entfernten Seitenzahlen und ausschließlich dem Hinweis eingeheftet wird, daß diese Seiten in gegenseitigem Einverständnis entfernt wurden.

- Die unterschiedlichsten Gegebenheiten und Verfahrensweisen fand ich bezüglich der **Vorakten und deren Behandlung bzw. Nutzung**[271]. So war selbst bei einem der aufgesuchten zwei Ministerien bisher keine Bereinigung vorgenommen worden, hier waren die Vorakten unverschlossen in den aktuellen Personalgrundakten vorangeheftet, in dem anderen Fall waren die Vorakten bereits bereinigt worden, indem die für die Fortführung des Beschäftigungsverhältnisses erforderlichen Dokumente in die aktuellen Personalgrundakten aufgenommen wurden und die restlichen Voraktenteile hiervon auch räumlich getrennt bis zu weiteren allgemeinverbindlichen Bestimmungen verschlossen aufbewahrt werden. In einigen Fällen waren die Voraktendokumente völlig ungefiltert zum aktuellen Aktenbestandteil gemacht worden oder unbereinigt, aber ebenfalls zusammenhängend und unverschlossen in den Personalgrundakten

[271] s. auch unter 13.1 und 2.8.3

voran- oder nachgeheftet. In anderen Fällen waren aufgrund der auf den sog. „Modrow-Erlaß“[272] zurückzuführenden Bereinigungsaktion überhaupt keine oder nur noch vereinzelt Vorakten vorhanden. Andere Personalstellen hatten darüber hinaus oder ausschließlich eine Bereinigung im Einvernehmen mit den Betroffenen durchgeführt und dies aktenkundig dokumentiert. Bei wieder anderen Stellen war dies - nicht mehr nachvollziehbar - ohne Dokumentation geschehen. In letzteren Fällen befanden sich tatsächlich ordnungsgemäß nur noch solche Voraktenteile in den Personalakten, die auch für die aktuelle Personalsachbearbeitung benötigt werden. Dieser Wirrwarr macht deutlich, daß eine Gleichbehandlung, die i. ü. auch ein Kriterium für die Erforderlichkeit im datenschutzrechtlichen Sinne ist, nur erreicht werden kann, wenn ungeachtet des Erfordernisses einer materiell-rechtlichen Regelung bezüglich der (noch) vorhandenen Voraktenbestände zumindest ein **Kriterienkatalog über die Dokumente** erstellt wird, die zweifelsfrei zur laufenden Personalsachbearbeitung herangezogen werden dürfen, sowie über solche Dokumente, die aus anderen wichtigen Gründen vorsorglich noch verschlossen und getrennt von den laufenden Personalvorgängen aufgehoben werden sollen. Aufgrund der allgemein bestehenden Behandlungsunsicherheiten ist vor Ort wiederholt die Hoffnung geäußert worden, daß alsbald eine diesbezügliche Orientierungshilfe zur Verfügung stehen wird.

272 s. unter 2.8.1

- Leider werden noch immer nicht bei allen Personalstellen die Grundsätze der Landesregierung für die **Überprüfung von Bediensteten des Landes Brandenburg hinsichtlich einer Tätigkeit für das ehemalige Ministerium für Staatssicherheit/Amt für Nationale Sicherheit (MfS/AfNS)**[273] berücksichtigt, ja teilweise waren diese noch nicht einmal bekannt. Dies führt in einigen Fällen dazu, daß die mit den Überprüfungen im Zusammenhang stehenden Vorgänge, wenngleich sie verschlossen sind, so doch wegen ihres geringen oder erweiterten Umfangs jederzeit ohne Erfordernis - insbesondere bei Weitergabe der Personalakte - unzulässige Rückschlüsse auf den Inhalt zulassen. In anderen Fällen waren die Vorgänge sogar offen, zusammen mit den Zusatzfragebögen zum Personalfragebogen betr. evtl. hauptamtlicher oder informeller Mitarbeiterschaft für das MfS, in der Personalgrundakte abgeheftet. In einem Fall waren die sog. „Gauck-Bescheide" zwar ordnungsgemäß getrennt von der Personalgrundakte in einer verschlossenen Teilakte geführt, dafür waren aber die Zusatzfragebögen zusammen mit den Krankmeldungen in einer sog. Teilakte geführt worden. Meine Beobachtungen lassen den Schluß zu, daß bezüglich der ordnungsgemäßen Behandlung dieser Vorgänge ein Informationsdefizit gerade bei Teilen der mittelbaren Landesverwaltung bestehen könnte. In den meisten anderen Fällen wird jedoch offensichtlich ordnungsgemäß nach den genannten Grundsätzen verfahren, zumindest war bei meinen Besuchen vor Ort dann auch festzustellen, daß selbst die räumliche Unterbringung und Zugriffssicherheit vorbildlich gelöst waren. Soweit ich Mängel feststellen mußte, habe ich auf unverzügliche Abhilfe gedrungen und hierzu auszugsweise die besonders klaren einschlägigen Ausführungen im Entwurf der PersaktVV zur Verfügung gestellt.

- Durchgehend bestätigt fand ich, daß bereits in der Praxis den Arbeitnehmern wie den Beamten gleiche **Akteneinsichtsrechte** während und nach dem Beschäftigungsverhältnis eingeräumt werden. Auf meine frühere Forderung[274] hin, dies auch in den PersaktVV so festzulegen, hat die Landesregierung in ihrer Stellungnahme die Prüfung einer möglichst einvernehmlichen Formulierung zugesagt.

Insgesamt fand ich durch meine Erkenntnisse vor Ort bestätigt, daß es unabdingbar ist, bei allen personalaktenführenden Stellen meines Zuständigkeitsbereichs alsbald einheitliche Handhabungen in der Behandlung von Personalaktenvorgängen sicherzustellen. Dies dürfte nicht nur einer rechtssichereren Bearbeitungsweise zugute kommen, sondern auch dem **Gleichbehandlungsgrundsatz** aller Betroffenen in Bezug auf deren individuelle Ansprüche im Rahmen des Rechts auf informationelle Selbstbestimmung. Darüber hinaus könnten aus bisher unterschiedlichen Verfahrensweisen die jeweils praktikabelsten herausgefunden werden, womit vielerorts nach einer Phase partieller Umstrukturierungen auch eine deutliche Verwaltungsvereinfachung erreicht werden dürfte. Jedenfalls war von Mitarbeitern und Verantwortlichen vor Ort ohne Ausnahme in Erfahrung zu bringen, daß vereinheitlichende Verwaltungsvorschriften sehr begrüßt würden.

Im übrigen wurden weitere Problemfelder offensichtlich, die allerdings in näherer Zeit noch gesonderten Überprüfungen und Bewertungen unterzogen werden müssen:

Externe Beihilfenbearbeitung

In diesem Zusammenhang sind datenschutzrechtliche Gefahren darin erkennbar, daß die Beihilfenbearbeitung zweckmäßigerweise durch die Stellen wahrgenommen wird, die bereits (im Rahmen auftragsweiser Datenverarbeitung) Gehalts- und Lohnabrechnungen sowie -zahlungen vornehmen. Mit der damit zwangsläufig verbundenen

---

273 vom 10. Oktober 1995, ABl. S. 914; s. 4. Tätigkeitsbericht unter 13.2.3

274 s. 5. Tätigkeitsbericht unter 13.1.3.3

Verselbständigung von den eigentlichen Beschäftigungsbehörden entsteht die Situation, daß Betroffene gehalten sind, ihre Ansprüche überhaupt nicht mehr gegenüber der Stelle geltend zu machen, die im Rahmen ihrer Fürsorgepflicht zur Gewährung der Beihilfe verpflichtet ist. Diese Situation wird noch prekärer, wenn - anders als bei der unmittelbaren und mittelbaren Landesverwaltung - die Beihilfe nicht bei der Zentralen Bezügestelle der Oberfinanzdirektion Cottbus (ZBB), sondern - wie ich vereinzelt feststellen konnte - sogar bei privaten Krankenkassen bearbeitet wird.

Gehaltspfändungen durch die ZBB

Auf ein weiteres Problem der Verselbständigung machte mich eines der geprüften Ministerien aufmerksam, indem es beklagte, daß die ZBB ohne Rücksprache mit der zuständigen Personalstelle beantragte Gehaltspfändungen durchführe, so daß dort keine Möglichkeit der Bewertung und Prüfung oder des Gesprächs mit den Betroffenen im Rahmen der Fürsorgepflicht (mehr) gegeben sei.

Gehalts- und Lohndaten online

Zunehmend lassen öffentliche Beschäftigungsstellen die Löhne und Gehälter ihrer Beschäftigten im Rahmen auftragsweiser Datenverarbeitung an anderer Stelle berechnen. Ungeachtet der bis zu einer gesonderten Überprüfung bestehenden Zweifel, ob in jedem Fall dabei den datenschutzrechtlichen Erfordernissen von § 11 BbgDSG Rechnung getragen ist, stellt sich die Tatsache als Problem dar, daß dabei regelmäßig die zur Berechnung erforderlichen Grunddaten bzw. Berechnungsergebnisse online übermittelt werden, ohne daß eine Verschlüsselungssoftware eingesetzt wurde. In diesem Zusammenhang verweise ich vergleichend auf meine diesbezüglichen Forderungen im Meldebereich[275]. Die datenschutzrechtlichen Gefahren verstärken sich, wenn zudem die rechnergestützte Personaldatenverarbeitung bei der Personalstelle (auch) gegenüber dem Auftragnehmer nicht abgeschottet ist, oder - wie in einem Fall von mir festgestellt wurde - zwecks dortiger Berechnung hier auszuzahlender Gehälter und Löhne sogar eine online-Verbindung zur Partnergemeinde in einem anderen Bundesland besteht.

Zuständigkeiten im Schulbereich

Einer besonderen Beurteilung muß noch die Personalaktenbearbeitung im schulischen Bereich unterzogen werden. Hier scheint mir trotz des recht guten Regelungswerks hinsichtlich der Führung von Personalakten und sonstigen Personalunterlagen[276] ein deutlicher Mangel an normenklaren materiell-rechtlichen Zuständigkeitsregelungen vorzuliegen. Zwar ist gem. § 131 Abs. 3 Brandenburgisches Schulgesetz (BbgSchulG)[277] das für die Schule zuständige Ministerium ermächtigt, den staatlichen Schulämtern eine Geschäftsordnung zu geben, jedoch haben diese dabei § 132 Abs. 2 Satz 3 Rechnung zu tragen, wonach die Leiter der staatlichen Schulämter (die Kreis- oder Stadtschulräte) Dienstvorgesetzte der Schulleiter, der Schulpsychologen, der Lehrkräfte sowie des sonstigen pädagogischen Personals der Schulen sind. Insoweit handeln die staatlichen Schulämter zunächst selbständig auch im Personalbereich. Da das BbgSchulG selbst keine diesbezügliche spezielle Vorbehaltsregelung enthält, dürfte das Ministerium auch nur im konkreten Einzelfall der Dienst- und Fachaufsicht gem. § 131 Abs. 1 BbgSchulG Bearbeitungsteile an sich ziehen.

---

275 s. 5. Tätigkeitsbericht unter 3.1.1.2 und 12.4.1.2

276 Rundschreiben Nr. 110/93 des MBJS vom 8. November 1993

277 vom 12. April 1996, GVBl. S. 102

Dessenungeachtet ist aufgrund der derzeit geltenden Geschäftsordnung mit ihren Anlagen[278] z. B. vorgesehen, daß Bewerberzulassungen bei Einstellungen und Beförderungen dem Vorbehalt der Qualifizierungsbestätigung durch das Ministerium für Bildung, Jugend und Sport (MBJS) unterliegen. In beiden aufgesuchten staatlichen Schulämtern ist hierzu mit Befremden auch bemerkt worden, daß man nach über sieben Jahren seit der Vereinigung durchaus in der Lage sei, Qualifikationsvoraussetzungen selbst beurteilen zu können. Hier scheinen mir mangels spezialgesetzlicher Befugnisnorm zumindest Zweifel an der Erforderlichkeit für eine regelmäßige Offenbarung gegenüber dem MBJS außerhalb des Anwendungsbereiches von § 71 des Ersten Schulreformgesetzes[279] i.V.m. § 149 Abs. 2 Nr. 1BbgSchulG im Rahmen der Voraussetzungen nach § 29 BbgDSG berechtigt zu sein.

Als ein weiteres Problem für eine ordnungsgemäße Personaldatenverarbeitung stellt im Schulbereich die Regelung dar, daß im Falle einer erforderlichen **Rechtsvertretung** die achtzehn staatlichen Schulämter gehalten sind, die Rechtsstellen von drei jeweils zugewiesenen Schulämtern einzuschalten. Nach § 131 Abs. 3 Satz 1 BbgSchulG ist das MBJS zwar berechtigt, in der Geschäftsordnung festzulegen, daß die staatlichen Schulämter das Land im Rahmen ihrer jeweiligen Zuständigkeit in allen Rechtsangelegenheiten selbst vertreten, jedoch bedarf es dazu gem. § 131 Abs. 4 BbgSchulG einer Rechtsverordnung, wenn das MBJS einzelnen staatlichen Schulämtern z. B. Aufgaben anderer staatlicher Schulämter übertragen will. Eine solche materiell-rechtliche Grundlage i.V.m. § 149 Abs. 2 Nr. 1 BbgSchulG liegt meines Wissens aber für die Rechtsvertretung im Personaldatenbereich nicht vor. Es muß deshalb rechtlich von auch insoweit selbständigen staatlichen Schulämtern mit der Konsequenz ausgegangen werden, daß es sich im Einzelfall um unerlaubte Datenübermittlungen handelt, es sei denn, daß die staatlichen Schulämter sich in Ermangelung eigener Möglichkeiten - dann aber nach eigener Auswahl und in eigener Verantwortung - der Rechtsstelle anderer staatlicher Schulämter oder der Rechtsstelle des/der jeweiligen Landkreises/kreisfreien Stadt im Rahmen auftragsweiser Datenverarbeitung gem. § 11 BbgDSG bedienen.

---

278 Geschäftsordnung-Schulamt vom 21. Dezember 1993, geänd. am 30. Juli 1997

279 i. d. Fass. vom 1. Juli 1992, GVBl. I S. 258; zul. geänd. durch Art. 2 Ges. z. Änd. besoldungsrechtl. u. schuldrechtl. Vorschr. vom 27 Juni 1995, GVBl. I S. 138

Während ich dem gegenwärtigen Stand der technischen Entwicklungen im Bereich der automatisierten Verarbeitung von Personaldaten im Einsatz bei den allgemeinen Landesverwaltungen (PERIS) einen gesonderten Abschnitt dieses Berichts widme[280], stelle ich zum Abschluß meiner Prüfungsergebnisse im folgenden die besondere Situation im Schulbereich dar:

Mit Rundschreiben vom 6. September 1996 hatte das MBJS[281] eine Dienstvereinbarung zur **automatisierten Personaldatenverarbeitung und Stellenbewirtschaftung in den Staatlichen Schulämtern (APSIS)** veröffentlicht. Gegen das Personalinformationssystem APSIS hatte ich keine grundsätzlichen datenschutzrechtlichen Bedenken geäußert. Im Rahmen meiner Kontrollbesuche lag mir besonders daran zu erfahren, wie der praktische Einsatz des Programms in den Schulämtern vonstatten geht. Dabei war insbesondere der Einsatz im Computernetz unter Berücksichtigung der vorhandenen Verschlüsselungssoftware zu überprüfen.

Die ausgewählten zwei staatlichen Schulämter nutzen APSIS in eigenen lokalen Netzen mit eigenem Server. In einem Fall besteht allerdings über eine Schnittstelle ein Anschluß an das Kreisverwaltungsnetz, um die E-Mail-Funktion behördenintern nutzen zu können. Das Kreisverwaltungsnetz besitzt seinerseits zwar keinen Anschluß an das Internet, wird jedoch als Behördenstadtnetz betrieben.

Da die Online-Verschlüsselung von APSIS lediglich durch eine programmeigene Lösung realisiert wird, die den Ansprüchen an ein öffentlich anerkanntes kryptographisches Verfahren nicht genügen kann und auch kein variables Schlüsselmanagement zuläßt, stellt sich die Sicherheitssoftware als sog. **schwache Verschlüsselung** dar, vergleichbar mit der hauseigenen Lösung von PERIS. Weil aber an Personalinformationssysteme öffentlicher Stellen des Landes sowohl wegen der datenschutzrechtlichen Anforderungen als auch aus Gleichbehandlungsgründen der gleiche Qualitätsmaßstab anzulegen ist, kann für die Nutzung von APSIS deshalb auch nur die Einsatzmöglichkeit nach Szenarium 1 von PERIS zur Anwendung kommen. Dies bedeutet u. a., daß APSIS lediglich als kleines lokales, physikalisch eigenständiges Netz nur für die Rechner der Personalabteilung und mit eigenem Server betrieben werden darf. Ein Anschluß an andere lokale oder weite Netze ist nicht zulässig, da erfolgreiche Angriffe auf die Personaldaten nach dem heutigen Stand der Technik nicht ausgeschlossen werden können. Aus diesem Grunde muß die in einem Fall vorgefundene Schnittstelle des APSIS-Netzes zum allgemeinen Behördennetz noch umgehend deaktiviert und nach einer anderen Möglichkeit für eine behördeninterne Kommunikation gesucht werden.

Wegen der schwachen Verschlüsselung müssen bei APSIS generell auch alle zusätzlichen Schutzmaßnahmen wie Raumsicherung, Zutritt von Reinigungskräften nur unter Aufsicht eines befugten Mitarbeiters der Personalabteilung, Nutzung von Data-Safe für den Server u. ä. vorgesehen werden.

13.2.2 Einsichtsrechte des Landesrechnungshofs und der Rechnungsprüfungsämter in Personalakten

[280] s. unter 13.2.9

[281] s. Rundschreiben 80/96 vom 21. November 1996, ABl. MBJS Nr. 13 S. 671

Unter Verweis auf § 95 Abs. 1 Bundeshaushaltsordnung (BHO)[282] hatte das Bundesministerium der Finanzen im Einvernehmen mit dem Bundesministerium des Innern und dem Bundesrechnungshof bereits mit Rundschreiben vom 12. Dezember 1980 darauf hingewiesen, daß dieser aufgrund seines verfassungsmäßigen Prüfungsauftrags verlangen könne, seinen Beauftragten die vollständigen Personalakten vorzulegen. Dabei entscheide er in auf der Grundlage von Art. 114 Abs. 2 GG i. V. m. § 88 BHO unter den sich aus dem Gesichtspunkt des Persönlichkeitsschutzes ergebenden verfassungsrechtlichen Grenzen entsprechend dem Grundsatz der Verhältnismäßigkeit in eigener Verantwortung, welche Vorgänge, insbesondere solche besonders vertraulicher Art (z. B. Gesundheitszeugnisse, Beurteilungen usw.), zur Erfüllung seiner Aufgaben gebraucht würden.

Noch immer steht in der Diskussion, ob und inwieweit vorhandene bundes- und landesrechtliche Vorschriften tatsächlich als ausreichende Rechtsgrundlagen für eine derart umfangreiche und in das jeweilige Befinden gestellte **Prüfkompetenz** (auch) **der Landesrechnungshöfe** angesehen werden können.

Da ein uneingeschränktes Einsichtsrecht in Personalakten unter dem Gesichtspunkt des Persönlichkeitsschutzes ohnehin nur grundsätzlich bejaht werden kann, soweit finanzwirksame Vorgänge zu prüfen sind, teile ich die vom MI und MdF vertretene Auffassung, daß insoweit für Regelungen im Beamtenrechtsrahmengesetz kein Anlaß besteht und aus diesen Gründen auch eine Ergänzung des Landesbeamtengesetzes nicht geboten ist. Zu fragen bleibt allerdings, ob in den haushaltsrechtlichen Bestimmungen eine geeignete Rechtsgrundlage zu finden ist. Mit § 95 Landeshaushaltsordnung (LHO)[283] ist wie mit § 95 BHO dem Rechnungshof ein sehr weitgehendes, aber hinsichtlich der Abgrenzungen zu den genannten Schutzrechten Betroffener nicht normenklares Einsichts- und Auskunftsrecht eingeräumt. Die an sich richtige Feststellung, daß diese weit gefaßte Regelung dem Verfassungsgebot einer lückenlosen Finanzkontrolle durch die Rechnungshöfe dienen soll, darf daher nicht zu dem Schluß führen, daß auch eine Änderung des § 95 LHO nicht in Betracht kommt.

---

282 vom 19. August 1969, BGBl. S. 1284

283 vom 7. Mai 1991, GVBl. S. 46

Da aber derzeit eine bundesweit einheitliche Bewertung in dieser Richtung nicht erreichbar ist, nehme ich es unter dem Aspekt des weitgehenden Auftrags an die Rechnungshöfe und aufgrund der Tatsache, daß die Verfassung des Landes Brandenburg[284] in Art. 107 den Mitgliedern des Landesrechnungshofs (LRH) richterliche Unabhängigkeit zuspricht - vorbehaltlich weiterer rechtlicher Erörterungen insbesondere der bislang nichtbeteiligten Ministerien - vorläufig hin, daß der Landesrechnungshof seine Prüfungen im Personalaktenbereich bis auf weiteres nach den Kriterien eines Rundschreibens des MdF[285] im Wege der **Selbstrestriktion** wahrnimmt. Hieraus sind folgende Punkte zusammengefaßt hervorzuheben:

- Der LRH kann im Rahmen von § 95 Abs. 1 LHO allein nach eigener Entscheidung die **Vorlage vollständiger Personalakten** verlangen.

- Bei **Vorgängen besonders vertraulicher Art** (z. B. Gesundheitszeugnissen, Beurteilungen und dgl .), die durch das von der Verfassung gewährleistete Persönlichkeitsrecht geschützt sind, beschränkt der LRH seine Einsichtnahme - dem Grundsatz der Verhältnismäßigkeit folgend - auf das unbedingt Erforderliche.

- Auch wenn bei Prüfung von Personalausgaben im allgemeinen eine Einsichtnahme in Personalakten erforderlich sein dürfte, soll die zu prüfende Verwaltung davon ausgehen können, daß der LRH regelmäßig auf Einsichtnahme in Teilakten, die der Vertraulichkeit unterliegen (z. B. Disziplinarsachen, Beurteilungen, Gesundheitszeugnisse usw.), verzichtet, ansonsten eine solche nur nach Abwägung in obigem Sinne verlangen wird.

- In den Prüfungsankündigungen wird der LRH so konkret wie möglich mitteilen, welche Unterlagen er benötigt. Sollte sich bei der Prüfung herausstellen, daß darüber hinausgehend Unterlagen benötigt werden, wird der LRH auf Verlangen die Verantwortung für die Erforderlichkeit durch ein Bestätigungsschreiben übernehmen.

- Der LRH wird in geeigneter Form, z. B. auf Listen, bestätigen, welche Personalakten durch welchen Prüfungsbeauftragten eingesehen wurden. Sofern ausnahmsweise vertrauliche Vorgänge eingesehen werden sollen, wird der LRH dies besonders für den jeweiligen Vorgang bestätigen.

- Im übrigen wird (auch) der LRH - soweit das Prüfungserfordernis dies zuläßt - seine Prüfungsergebnisse in einer Form, die dem Persönlichkeitsschutz Rechnung trägt, aufzeichnen (z. B. anonymisiert) und übermitteln (z. B. durch unmittelbare Adressierung an die befugten Verwaltungsstellen).

Ganz anders stellt sich die **Sachlage für kommunale Rechnungsprüfungsämter** (RPA) dar. Im Gegensatz zum Landesrechnungshof ist diesen kein Verfassungsrang, umso weniger den dortigen Funktionsträgern richterliche Unabhängigkeit, ja noch nicht einmal eine eigenständige Aufgabenstellung eingeräumt.

---

284 vom 20. August 1992, GVBl. I S. 298; zul. geänd. durch ÄndG vom 10. März 1997, GVBl. I S. 4

285 Rundschreiben des Ministeriums der Finanzen zum Einsichtsrecht des Landesrechnungshofes in Personalakten gemäß § 95 Landeshaushaltsordnung (LHO) - 17-O 1340-5/95 - vom 16. Oktober 1997, ABl. S. 951

Zwar sind in § 113 Abs. 1 Gemeindeordnung für das Land Brandenburg (GO)[286] Aufgaben des Rechnungsprüfungsamts, die es auf jeden Fall wahrzunehmen hat, konkret festgelegt. Jedoch wird dieser Aufgabenkatalog in Abs. 2 durch Aufgabenbeispiele ergänzt, deren Wahrnehmung davon abhängig gemacht wird, daß sie dem RPA durch die Gemeindevertretung übertragen werden. Auch wird der Mangel an Unabhängigkeit aus den Vorgaben des § 112 Abs.1 Satz 2 GO deutlich. Danach haben die „Gemeindevertretung, der Hauptausschuß und der hauptamtliche Bürgermeister oder der Amtsdirektor ... das Recht, dem RPA Aufträge zur Prüfung der Verwaltung zu erteilen.". Selbst wenn in Satz 3 klargestellt wird, daß das RPA „bei der sachlichen Beurteilung der Prüfungsvorgänge unabhängig und insoweit an Weisungen nicht gebunden" ist, wird doch deutlich, daß die Prüfkompetenz der Rechnungsprüfungsämter nicht in deren eigenes Befinden gestellt ist, sie allenfalls einen Ausführungsspielraum haben, der aber nicht im Wege der Selbstrestriktion ausgefüllt werden kann. Sofern sie bei ihren Prüfungen auch konkret und personenbezogen in Personalakten einsehen wollen, müssen mangels verfassungsrechtlicher Sonderstellung die bereichsspezifischen beamten- bzw. tarifrechtlichen Bestimmungen, die eine solche „personalbearbeitungsfremde Offenbarung" ohne Zustimmung Betroffener nicht zulassen, entgegengehalten werden.

Dadurch, daß wegen des Gleichbehandlungsgrundsatzes zugunsten Betroffener im Rahmen ihres Rechts auf informationelle Selbstbestimmung nur die stringenteren Bestimmungen von § 57 Abs. 3 LBG für alle Beschäftigten des öffentlichen Dienstes gelten können, dürfen „Zugang zur Personalakte (einschließlich evtl. Teil- und Nebenakten) nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist; dies gilt auch für den Zugang im automatisierten Abrufverfahren". Da es sich bei Mitarbeitern des RPA auch nicht um „Beauftragte des Dienstherrn, die zur Wahrnehmung besonderer Belange an Personalentscheidungen zu beteiligen sind", handelt, kann selbst dahingestellt bleiben, ob im Einzelfall eine Einsichtnahme aus haushaltsrechtlichen oder Gründen der Wirtschaftlichkeitsprüfung erforderlich sein könnte. Die Rechnungsprüfungsämter müssen sich auf jeden Fall mit von den Personalstellen **aufbereiteten Materialien** ohne Personenbezug zufrieden geben. Sofern es z. B. im Rahmen einer Wirtschaftlichkeitsprüfung gerade auf konkrete Einzelangaben ankommt, müssen die zu prüfenden Unterlagen von den Personalstellen hinreichend anonymisiert werden, indem etwa Kopien zur Verfügung gestellt werden, auf denen zuvor soweit wie irgend möglich die personenbeziehbaren Angaben geschwärzt wurden. Die notwendige Beziehbarkeit für die weiteren Verwaltungsabläufe könnte z. B. dadurch gewährleistet werden, daß die Personalstelle für die Prüfvorgänge eine Liste mit Ordnungszahlen erstellt, anhand derer sich erforderlichenfalls der Bezug zur jeweiligen Personalakte herstellen ließe.

13.2.3 Personalentwicklungskonzept

Einer Anregung aus Niedersachsen folgend, plante eine oberste Landesbehörde im Benehmen mit dem dortigen Personalrat, daß die Referatsleiter mit „interessierten Beschäftigten" ihres jeweiligen Referats **Gespräche zur Personalentwicklung** mit dem Ziel führen, die persönliche Seite der Zusammenarbeit zwischen Mitarbeitern und Vorgesetzten zu erörtern, wechselseitige Erwartungen zu klären, gegenseitiges Mißtrauen abzubauen, Mißverständnisse und Konflikte in der Zusammenarbeit zu klären, Vertrauen und Zusammenarbeit zu fördern sowie die Bedürfnisse und Wünsche der Mitarbeiter hinsichtlich der beruflichen Entwicklung und Qualifikation kennenzulernen, um diese im Rahmen der Möglichkeiten unterstützen und fördern zu können.

Hierzu war daran gedacht, daß vorbereitend das Personalreferat den Referatsleitern für deren jeweilige Mitarbeiter einen

[286] vom 15. Oktober 1993, GVBl. I S. 398; geänd. durch Art. 3 1. BbgFRG vom 30. Juni 1994, GVBl. I S. 230

als „vertrauliche Personalangelegenheit“ gekennzeichneten Bogen zur persönlichen Entwicklung der Mitarbeiterin/des Mitarbeiters mit dienstbezogenen Angaben zur Person (z. B. welche Beschäftigungszeiten in welchen Bereichen der Behörde in welchen Funktionen) und Hinweisen auf bisherige Tätigkeiten überhaupt, bisherige Weiterbildungsmaßnahmen, bisher angemeldeten Weiterbildungsbedarf u.a. zur Verfügung stellt. Dieser Bogen sollte um den jeweiligen, von beiden Gesprächspartnern unterschriebenen Gesprächsvermerk über das „Mitarbeitergespräch im Rahmen der Personalentwicklung“, für den die Teile „Individuelle Arbeitsziele für die Zukunft“ und „Anregungen zur Förderung und Entwicklung der Mitarbeiterin/des Mitarbeiters (Schwerpunkte)“ vorgesehen waren, ergänzt werden.

Der Personalrat der Behörde fragte nach, ob der praktischen Umsetzung datenschutzrechtliche Gründe entgegenständen.

Für sich genommen war der Teil „Persönliche Entwicklung des Mitarbeiterin/des Mitarbeiters“ unproblematisch, soweit die Angaben unmittelbar aus der Personalakte genommen werden sollten. Das eigentliche Problem war in den Festlegungen zum „Mitarbeitergespräch im Rahmen der Personalentwicklung“ zu sehen:

Auch wenn davon auszugehen war, daß hier Informationen eingeholt werden sollten, die regelmäßig keine Personalaktendaten darstellen, waren diese doch als Personaldaten i. S. v. § 29 BbgDSG zu werten, da sie in unmittelbarem Zusammenhang mit dem Dienst- oder Arbeitsverhältnis erhoben werden und u. a. organisatorischen Maßnahmen bzw. Zwecken der Personalplanung und des Personaleinsatzes dienen sollten. Voraussetzung für eine solche Datenerhebung ist allerdings, daß die zu erhebenden Daten hierzu erforderlich sind bzw. eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung die Erhebung vorsehen. Eine diesbezüglich greifende materiell-rechtliche Grundlage, die die Erhebung allgemeiner, nicht konkretisierter Daten rechtfertigen würde, ist jedoch nicht erkennbar; eine Erforderlichkeit hätte sich allenfalls nachweisen lassen können, wenn ein Fragenkatalog mit konkreten, auf die o. g. Erhebungsziele ausgerichteten Kriterien hätte verwendet werden sollen. Die allgemeinen Fragestellungen wurden diesen Anforderungen nicht gerecht. Der spezialgesetzlich verankerte **Individualschutz** des einzelnen **verbietet** auch eine **ersatzweise Rechtfertigung** etwa **durch eine Dienstvereinbarung** zwischen der Dienststelle und dem Personalrat.

Zu prüfen war letztlich noch, ob die vorgesehene Erhebung auf der Basis der Freiwilligkeit gem. § 4 Abs. 1 Buchst. b BbgDSG hätte durchgeführt werden können. Da aber nicht abzusehen war, ob sich überhaupt, und wenn schon, wieviele Beschäftigte an dem Projekt beteiligen würden, war schon von vornherein zweifelhaft, ob das Auswertungsergebnis für den vorgesehenen Zweck geeignet wäre. Daten, die zur Erfüllung des Aufgabenzwecks nicht geeignet sind, sind aber folgerichtig auch nicht erforderlich. Im übrigen mußte ich auch in diesem Zusammenhang wieder darauf hinweisen, daß gerade im Personaldatenbereich nicht auf die gesetzliche Einwilligungslösung abgestellt werden kann, da die Betroffenen in ihrer sozialen Abhängigkeit für sich Nachteile für den Fall befürchten könnten, daß sie sich nicht beteiligen und insoweit eine echte Freiwilligkeit nicht gegeben ist. Ergänzend sei zu dem geschilderten Einzelfall noch die Gefahr genannt, daß auch bei einer (personenbezogenen) Teilnahme an der Befragungsaktion aufgrund der (möglicherweise sehr kritischen) Angaben Nachteile zu befürchten waren (z. B. Stigmatisierung als „Querulant“ u. ä.).

Im Ergebnis mußte ich feststellen, daß ein zumindest allgemein interessierendes und verwertbares Auswertungsergebnis erzielt werden könne, wenn auf jeden Personenbezug verzichtet würde, so auch auf die gesprächsweise Befragung. Als datenschutzrechtlich unproblematische Lösungsmöglichkeit empfahl ich, die Bitte um Äußerungen zu „Individuellen Arbeitszielen für die Zukunft“ und zu „Anregungen zur Förderung und Entwicklung der Mitarbeiterin/des Mitarbeiters“ an alle Beschäftigten zu verteilen und ihnen freizustellen, ob sie sich überhaupt äußern wollen oder dann Gelegenheit zu geben, ihre Antworten ohne weitere Möglichkeiten der Personenbeziehbarkeit referatsweise und verdeckt zurückreichen.

13.2.4 Einsichtnahme in dienstliche Beurteilung durch die Schwerbehindertenvertretung

Nach Nr. 18.4 der Schwerbehindertenrichtlinien[287] ist die Schwerbehindertenvertretung rechtzeitig und umfassend über den beabsichtigten Inhalt einer **dienstlichen Beurteilung** zu unterrichten; ihr ist Gelegenheit zur Stellungnahme zu geben, sofern der Schwerbehinderte dies nicht ausdrücklich ablehnt. Demgegenüber ist in Nr. 18.5 geregelt, daß die Schwerbehindertenvertretung nur auf ausdrückliches Verlangen der Betroffenen bei der Durchführung eines Beurteilungsgesprächs hinzuzuziehen ist bzw. bei der Eröffnung einer Beurteilung teilnehmen kann.

Zu Recht hatte der behördliche Datenschutzbeauftragte der AOK Brandenburg seine Bedenken gegen diese Diskrepanz an mich herangetragen. In meiner datenschutzrechtlichen Bewertung gegenüber dem MI war auf folgendes hinzuweisen:

Die auf § 25 Abs. 2 Schwerbehindertengesetz (SchwbG)[288] zurückzuführenden Rechte der Schwerbehindertenvertretung müssen im Lichte des Rechts auf informationelle Selbstbestimmung der betroffenen Schwerbehinderten gesehen werden. Dem ist zwar in Nr. 18.5, nicht aber auch in Nr. 18.4 der Schwerbehindertenrichtlinien Rechnung getragen worden, obwohl hier - durch Offenlegung von Beurteilungsinhalten - der Eingriff in die Persönlichkeitsrechte viel intensiver ist. Im übrigen sind dienstliche Beurteilungen Teile der Personalakten, deren Einsichtnahme durch die Schwerbehindertenvertretung gem. § 25 Abs. 3 SchwbG davon abhängig gemacht ist, daß diese von dem Schwerbehinderten hinzugezogen wird. Dem öffentlichen Arbeitgeber ist es zwar freigestellt, die Einhaltung seiner in § 14 SchwbG genannten Pflichten gegenüber Schwerbehinderten im Erlaßwege sicherzustellen. Die an sich begrüßenswerten Regelungen dürfen jedoch hinsichtlich der gesetzlich fixierten Rechte Betroffener nicht interpretatorisch einschränkend wirken.

Das MI folgt dieser Auslegung und wird im Zusammenhang mit einer ohnehin vorgesehenen **Überarbeitung der Schwerbehindertenrichtlinien**, bei der die bisherigen Erfahrungen mit dem Schwerbehindertengesetz und aktuellere Rechtsprechung des Bundessozialgerichts berücksichtigt werden sollen, entsprechend der Abstimmung mit mir unter der Nr. 18.4 etwa folgende Formulierung einarbeiten:

„Die Schwerbehindertenvertretung ist rechtzeitig über die beabsichtigte Erstellung einer dienstlichen Beurteilung zu unterrichten. Auf Wunsch des Schwerbehinderten ist der Schwerbehindertenvertretung Gelegenheit zur Stellungnahme zum Inhalt des Entwurfs der dienstlichen Beurteilung zu geben. Die Beteiligung der Schwerbehindertenvertretung und die Berücksichtigung eines geminderten Leistungspensums sind in der Beurteilung zu vermerken."

13.2.5 Einsatz eines Kopiererfassungssystems

Von einem Petenten wurde ich darüber informiert, daß eine Fachhochschule des Landes beabsichtigt, ein sogenanntes Kopiererfassungssystem (KES) einzuführen. Diese Information nahm ich zum Anlaß, mir das System vor Ort näher anzuschauen. Als Ergebnis ist folgendes festzuhalten:

Durch Nutzung des Kopiererfassungssystems beabsichtigt die Fachhochschule, den **kostenbewußten Umgang der Mitarbeiter beim Anfertigen von Kopien** zu fördern. Unter Verwendung eines TouchKeys (Freischalteinrichtung) erfolgt der Zugriff zum jeweiligen Kopierer, der dazu mit einem sogenannten Controller ausgerüstet wird. In diesem Controller werden die Benutzernummern und die dazugehörigen Summen der angefertigten Kopien gespeichert. Die Daten des

---

287 Runderlaß des Ministeriums des Innern - Z/2 60-08 - vom 6. November 1996, ABl. S. 1058

288 i. d. Fass. vom 26. August 1986, BGBl. I S. 1421/1550

Controllers können mit Hilfe eines Laptops ausgelesen werden. Auf dem Laptop erfolgt dann die Zuordnung der Benutzernummer zu einem bestimmten Benutzer.

Der Anwender erhält von der ADV-Abteilung einen sog. „TouchKey-Button" (kleiner Schlüsselanhänger), auf dem u. a. eine der Person zuordenbare Nummer, die Summe der angefertigten Kopien sowie ein Maximalwert der anzufertigenden Kopien abgelegt werden. Der Benutzer berührt mit dem TouchKey den am Kopierer befindlichen Controller, wodurch das Kopiergerät freigeschaltet wird. Nach dem Anfertigen von Kopien muß der Benutzer erneut den TouchKey verwenden, um den Kopiervorgang zu beenden. Dabei wird die Anzahl der angefertigten Kopien im Controller und im TouchKey abgebucht.

Es ist geplant, daß die Daten des Controllers monatlich in einen Laptop übertragen werden. Auf dem Laptop ist ein Auswertungsprogramm installiert, mit dessen Hilfe die monatlichen Kopien dem jeweiligen Nutzer zugeordnet werden. Auf dem Laptop werden u. a. Name, Vorname, Organisationseinheit, Anzahl der monatlich angefertigten Kopien und das Kopierlimit gespeichert. Das Kopierlimit wird durch die jeweilige Organisationseinheit festgelegt.

Am Monatsende wird den Organisationseinheiten nur deren Gesamtsumme mitgeteilt. Auf Wunsch der Organisationseinheit kann eine Einzelabrechnung der Nutzer angefordert werden. In dieser Einzelabrechnung ist die Summe der monatlich angefertigten Kopien der Nutzer enthalten.

Da es sich bei den Abrechnungsdaten um personenbezogene Daten der Mitarbeiter handelt, aus denen sowohl positive als auch negative Rückschlüsse auf die Verwendung von Arbeitszeiten und auf die Praktikabilität von Arbeitsmethoden gezogen werden können, halte ich es für erforderlich, daß vor Inbetriebnahme des Kopiererfassungssystems der Personalrat gem. § 65 Landespersonalvertretungsgesetz (PersVG) [289] beteiligt und eine **Dienstvereinbarung** abgeschlossen wird. Dadurch wird auch das gesamte Verfahren für den Benutzer transparent. Jedoch sollte in dieser Dienstvereinbarung festgeschrieben werden, daß die mißbräuchliche Nutzung der erhobenen personenbezogenen Daten zur Leistungs- und Verhaltenskontrolle unzulässig ist. Eine Stellungnahme der Fachhochschule, der ich meine Vorstellungen ebenfalls zugeleitet habe, steht noch aus.

13.2.6 Personaldatenschutz contra Informationsanspruch der Presse

Im Rahmen der Kommunalaufsicht hatte das MI einen Tarifexperten der nordrhein-westfälischen Landesverwaltung damit beauftragt, bei der Verwaltung einer kreisfreien Stadt gutachterlich festzustellen, ob und in welchem Umfang dort eine **ordnungsgemäße und angemessene tarifliche Eingruppierung** der kommunalen Angestellten vorgenommen worden war.

Aus den Äußerungen des Gutachters in einem Rundfunkinterview konnte geschlossen werden, daß beispielsweise alle Mitarbeiter einer bestimmten Dienststelle eine Vergütungsgruppe zu hoch eingestuft seien. Diese Dienststelle, zu deren Aufgaben auch intensiver Publikumverkehr gehört, wurde in dem Interview konkret benannt. Aus dem MI selbst wurde an die Presse gegeben, daß beispielsweise eine bestimmte Amtsleiterin mit 600 Mark monatlich überbewertet sei. Auch sie hat, bedingt durch ihre Funktion, besonders viel Kontakt mit Bürgern. Hierdurch sahen sich die Betroffenen in ihren Persönlichkeitsrechten verletzt und wandten sich in getrennten Petitionen an mich.

[289] vom 15. September 1993, GVBl. I S. 358

In seiner Stellungnahme verwies das MI insbesondere darauf, daß es gem. § 5 Brandenburgischem Pressegesetz (BbgPG)[290] grundsätzlich berechtigt sei, die Presse über die Prüfung solcher Angelegenheiten zu unterrichten. Hiernach seien alle Behörden des Landes Brandenburg verpflichtet und berechtigt, Vertretern der Presse die der Erfüllung ihrer öffentlichen Aufgaben dienenden Auskünfte zu erteilen. Dies sei eben auch im Rahmen der Vorstellung des Berichts über die beanstandenswerte Eingruppierungspraxis der Stadtverwaltung erfolgt. Bezweifelt wurde, ob z. B. im Falle der Amtsleiterin die Auskunft gem. § 5 Abs. 2 Nr. 3 BbgPG hätte verweigert werden können, weil damit ein „schutzwürdiges privates Interesse verletzt" worden wäre. Schließlich ständen Amtsträger in leitenden Funktionen oder Funktionen mit Außenwirkung dergestalt in der Öffentlichkeit, daß eine allgemeine Aussage zu der Vergütung nach der tariflichen Eingruppierung fast schon als offenkundig anzusehen sei. So seien Informationsmöglichkeiten für die Öffentlichkeit zur üblichen Eingruppierung bereits durch frei erhältliche Fachliteratur gegeben, einen groben Überblick über konkrete Eingruppierungen böten auch Haushaltspläne. Im übrigen seien Gegenstand der Erklärungen nicht die Personen, sondern die Bewertung der Stellen gewesen, die unabhängig von den sie bekleidenden Personen beurteilt worden seien. Daß hierbei auch auf die entsprechenden Personen zurückgeschlossen werden könne, ließe sich nicht vermeiden. Da im übrigen keine altersbedingten, familiären oder sonstigen persönlichen Umstände weitergegeben worden seien, dürften überwiegende schutzwürdige private Interessen nicht verletzt worden sein.

Demgegenüber bin ich in meiner datenschutzrechtlichen Bewertung zu dem Ergebnis gekommen, daß es durch die Vorgehensweise in beiden Fällen tatsächlich und eindeutig zu einer **Verletzung der Persönlichkeitsrechte** gekommen war:

Zunächst war von mir zu prüfen, ob es sich bei den Informationen lediglich um solche allgemein zugänglicher Art oder um zu schützende Personaldaten handelte und ob hierfür ggf. eine Offenbarungsbefugnis nach § 29 BbgDSG vorlag. Überein stimme ich mit dem MI dahingehend, daß es im Rahmen der Kommunalaufsicht berechtigt ist, selbst oder durch beauftragte Gutachter Unterlagen der Stellenwirtschaft, erforderlichenfalls auch Einzelpersonalvorgänge, einzusehen bzw. einsehen zu lassen, um die Angemessenheit von Eingruppierungen prüfen zu können. Dies halte ich für vereinbar mit den in § 29 BbgDSG genannten Voraussetzungen.

Anders zu beurteilen ist die **Offenbarung** der insoweit erlangten Daten **gegenüber Dritten**. Eine unmittelbare Berechtigung ohne Zustimmung Betroffener oder gar eine Verpflichtung hierzu könnte aus § 29 Abs. 1 BbgDSG nur im Rahmen einer Erforderlichkeit für die dort genannten Aufgabenzwecke abgeleitet werden, ansonsten nur in einer anderweitigen materiell-rechtlichen Befugnisnorm begründet sein. Da ein möglicherweise dienstliches Interesse kein Erfordernis im datenschutzrechtlichen Sinne darstellt, auch weder die unmittelbaren noch die mittelbaren Informationsempfänger ein rechtliches Interesse für die Informationen hätten darlegen können, konnte allenfalls auf eine berechtigende oder verpflichtende Befugnisnorm abgestellt werden. Zu prüfen war, ob eine solche Befugnisnorm in § 5 BbgPG gesehen werden kann.

Zwar ist mit § 5 Abs. 1 BbgPG ein Informationsanspruch der Presse gegenüber Behörden begründet, jedoch ist in Abs. 2 Nr. 3 eben ausdrücklich geregelt, daß u. a. Auskünfte verweigert werden können, „wenn und soweit ... ein ... schutzwürdiges privates Interesse verletzt würde". Insoweit ist auch ein diesbezügliches **rechtliches Interesse der Presse** an konkreten Informationen im Rahmen ihrer öffentlichen Aufgabe gem. § 3 BbgPG einschränkend definiert. Zu Recht konnten sich die Betroffenen nicht nur in ihren **schutzwürdigen privaten Interessen**, sondern sogar in ihrem Recht auf informationelle Selbstbestimmung verletzt fühlen, weil allein mit einer allgemeinen Auskunft z. B. „über einzelne zu hohe Einstufungen bei

[290] vom 13. Mai 1993, GVBl. S. 162

den Amtsleitern bzw. diesen oder jenen Bereichen mit finanziellen Auswirkungen bis zu ... DM bezogen auf die gesamte Stadtverwaltung" dem Informationsrecht der Presse, aber auch der Öffentlichkeit insgesamt hätte nachgekommen werden können, jene daher nicht mit einer Rückschlußmöglichkeit auf ihre Person haben rechnen müssen. Auch der Auslegung, es habe sich bei den Informationen nicht um schutzwürdige Belange gehandelt, weil sie für jedermann durch Einsichtnahme in den Haushaltsplan einsehbar seien, kann nicht gefolgt werden. Zwar kann aus einem Haushaltsplan - bei Spitzenpositionen nicht immer vermeidbar - mitunter ein Personenbezug hinsichtlich der jeweiligen besoldungs- bzw. vergütungsmäßigen Zuordnung hergestellt werden. Damit ist aber gleichzeitig weder feststellbar, ob die angegebene Besoldungs- bzw. Vergütungshöhe in konkreten Einzelfällen auch leistungsangemessen oder aufgabengerecht ist, noch ob sie in dieser Höhe überhaupt in Anspruch genommen wird. Die Tatsache, daß sich die Petenten nach eigenen Angaben nach den Veröffentlichungen nicht nur im privaten Bereich, sondern auch bei der Ausübung ihrer dienstlichen Tätigkeit im Rahmen des Publikumkontaktes Beschimpfungen und abwertenden Bemerkungen ausgesetzt sahen, ist eine Bestätigung dafür, daß mit der Weitergabe der Informationen wegen deren Personenbeziehbarkeit nicht nur potentiell, sondern auch tatsächlich bis in den Persönlichkeitsbereich hinein eine Beeinträchtigung ihrer schutzwürdigen Interessen verbunden war.

Daher wäre vom MI bzw. seinem Beauftragten bezüglich der zuletzt genannten Informationen zu prüfen gewesen, ob auch deren Weitergabe durch § 5 BbgPG gerechtfertigt sein würde. Entgegen der Ansicht des MI ist in beiden behandelten Fällen der falsche Schluß gezogen worden. Der Hinweis des MI, zukünftig in entsprechenden Fragen unbeschadet dortiger Rechtsauffassung größtmögliche Zurückhaltung üben zu wollen, läßt zwar einen deutlichen Vorbehalt gegen meine rechtlichen Beurteilung erkennen; jedoch gehe ich davon aus, daß dies für die tatsächliche Behandlung zukünftiger Vergleichsfälle keine Bedeutung haben wird.

13.2.7 Personalnachrichten in Ministerialblättern und in Hausmitteilungen

Auch wenn meine Ausführungen im letzten Tätigkeitsbericht[291] zur Veröffentlichung von Beförderungen in den „Hausmitteilungen" der Ministerien erkennbar auf Beamte beschränkt waren, weise ich der Klarheit halber noch einmal ausdrücklich darauf hin, daß im Unterschied zu den nach beamtenrechtlichen Gesichtspunkten ausgerichteten Verfahrensmöglichkeiten vor der beabsichtigten Veröffentlichung von Höhergruppierungen zumindest bei nichtbeamteten Beschäftigten unbedingt die Einwilligung der Betroffenen eingeholt werden muß.

13.2.8 Negative Bewertung in Dienstbesprechungen und Protokollen

Immer wieder sind Probleme im Zusammenhang mit der Weitergabe **negativer Bewertungen** über einzelne Mitarbeiter **in Dienstbesprechungen und Personalversammlungen**, deren Dokumentation in den diesbezüglichen Protokollen sowie den Rechten der Einsichtnahme in solche Protokolle Gegenstand von Anfragen an meine Behörde. Häufig wollen die Petenten dabei nicht, daß ich unmittelbar bei den betreffenden Behörden recherchiere, weil sie aus der Situation heraus (zusätzliche) Nachteile befürchten. Gleichwohl lassen sich - auch ohne Kenntnis näherer Umstände - einige grundsätzliche Aussagen zu den datenschutzrechtlichen Aspekten treffen:

Zunächst einmal ist festzustellen, daß es bei Protokollen über Personalversammlungen und interne Dienstbesprechungen nur von nachrangiger Bedeutung ist, ob diese als offiziell oder inoffiziell bezeichnet werden bzw. zur Veröffentlichung bestimmt sind. Entscheidend ist vielmehr, ob sie im Sinne von § 3 Abs. 4 Nr. 4 BbgDSG **Aktenbestandteile** sind bzw. werden sollen oder lediglich **Vorentwürfe oder private Notizen** einzelner Vorgesetzter oder Mitarbeiter darstellen. Auf

[291] s. 5. Tätigkeitsbericht unter 13.2

letztere erstrecken sich die Bestimmungen des Brandenburgischen Datenschutzgesetzes zwar grundsätzlich nicht, jedoch müßte auch bei diesen davon ausgegangen werden, daß es sich um solche, den dortigen Bestimmungen unterworfene Aktenbestandteile handelt, sofern sie personenbezogene Informationen enthalten, die Teil eines amtlichen oder dienstlichen Vorgangs werden sollen bzw. nur werden sollten, ohne alsbald vernichtet worden zu sein. Um personenbezogene Aktenteile in diesem Sinne dürfte es sich bei den beschriebenen Protokollen auf jeden Fall immer dann handeln, wenn sie dienstliche Verwendung gefunden haben, z. B. aus ihnen zitiert wird.

Daraus ergibt sich ein Einsichtsrecht nach § 5 i. V. m. § 18 BbgDSG in jede Art von Protokollen, auch in solche, die nicht zur Veröffentlichung bestimmt sind, für diejenigen, deren personenbezogene Daten festgehalten sind. Dabei ist die Akteneinsicht grundsätzlich jedoch auf jeweils die Teile beschränkt, die die eigenen personenbezogenen Daten enthalten. Hiermit soll dem Individualschutz eines jeden Betroffenen Rechnung getragen werden. **Leistungs- und Bewertungsdaten** haben, sofern sie gem. § 29 BbgDSG im Zusammenhang mit dem Dienst- oder Arbeitsverhältnis stehen, den Charakter von Personalaktendaten. Sofern solche Daten Eingang in Protokolle finden, haben Betroffene ein unmittelbares Recht auf Einsichtnahme nach den bereichsspezifischen Bestimmungen zur Akteneinsicht in **Personalakten** (§ 13 BAT-O, § 60 LBG). Dies trifft auch zu, wenn diese Protokolle ansonsten besonderen Geheimhaltungsvorschriften unterliegen. Für diesen Fall sind dem Betroffenen zumindest die ihn betreffenden Teile des Protokolls offenzulegen.

Weitergehende Einsichtsrechte hat der Landesbeauftragte für den Datenschutz im Rahmen seiner Kontrollbefugnisse nach § 26 BbgDSG von Amts wegen, aber auch, wenn sich ein Petent gem. § 21 BbgDSG an ihn wendet. Er kann ohne Einschränkungen u. a. auch feststellen, ob es sich - ungeachtet der Angaben der betreffenden Verwaltung - bei den Aufzeichnungen tatsächlich nur um vorübergehende Notizen mit ausschließlicher Nutzung durch den Aufzeichnenden handelt.

Die personenbezogene Bekanntgabe schlechter Bewertungen im dienstlichen Zusammenhang bzw. eine personenbeziehbare Diskussion über mangelnde dienstliche Leistungen und negative Verhaltensweisen einzelner Mitarbeiter durch Dienst- oder Fachvorgesetzte in Mitarbeiterbesprechungen kann auf der Grundlage von § 29 BbgDSG allenfalls in dem Umfang und in der Ausführlichkeit gerechtfertigt sein, als dies ein geeignetes Mittel wäre, um einem (zumindest vermuteten) Arbeitsmangel oder sonstigen Mangel im innerbetrieblichen Ablauf begegnen zu können. Zunächst muß aber in jedem Fall geprüft werden, ob nicht bereits eine **anonymisierte Darstellung** ausreicht. Bei jedem Personenbezug müssen die Informationen in Art und Umfang für einen der in § 29 BbgDSG genannten Aufgabenzwecke, z. B. der Personalplanung oder des Personaleinsatzes erforderlich sein, wobei die Angaben in Art und Umfang so reduziert sein müssen, daß sie den **geringsten Eingriff in die Interessen des Betroffenen**, mit dem der Aufgabenzweck noch erfüllt werden kann, bedeuten. Dabei muß insbesondere bedacht werden, daß eine Erforderlichkeit nur gegeben sein kann, wenn Art und Umstände der Offenbarung auch geeignet sind, den vorgesehenen Zweck zu erfüllen. Soweit dieses Ziel nur über den Betroffenen selbst erreichbar ist, dürfen die für erforderlich gehaltenen Informationen auch nur weitergegeben und entsprechende Diskussionen mit Dritten nur geführt werden, wenn dieser auch selbst anwesend ist.

Vor diesem Hintergrund lassen sich zur personenbezogenen Bekanntgabe dienstlicher Bewertungen durch Dienst- oder Fachvorgesetzte in Mitarbeiterbesprechungen folgende Punkte zusammenfassen:

- Datenschutzrechtlich irrelevant ist jede abstrakt vergleichende Darstellung ohne Namensnennung.

- Datenschutzrechtlich noch zulässig ist es, wenn dabei Leistungs- bzw. Eignungskriterien unabdingbar diskutiert werden müßten, ohne daß aus der Situation heraus trotz aller möglichen Zurückhaltung eine Personenbeziehbarkeit

ausgeschlossen werden könnte. Dies dürfte insbesondere in internen Dienstbesprechungen hinzunehmen sein.

- Konkret, also mit vollem Personenbezug, dürfen selbstverständlich offenkundige Informa-tionen (insbesondere wenn der Betroffene selbst darüber im Kreis der Informanden spricht) ausgetauscht werden.

- Sofern Leistungs- und Verhaltensdefizite Gegenstand arbeitsrechtlicher Maßnahmen (z. B. Abmahnung) sind, dürfen diese und die Tatsache selbst ohne Billigung des Betroffenen nicht weitergegeben werden.

- Eine Weitergabe an Mitarbeiter ist zwar grundsätzlich ebenfalls möglich im Rahmen der Erforderlichkeit für organisatorische Maßnahmen, insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes. Dies trifft jedoch nur insoweit zu, als nicht bereits eine anonymisierte Darstellung ausreicht, ansonsten das Gebot des geringsten Eingriffs in die Persönlichkeitsrechte des Betroffenen beachtet wird und Art und Umstände der Offenbarung auch geeignet sind, den vorgesehenen Zweck zu erfüllen.

Ansonsten beinhalten mißbilligende Äußerungen gegenüber Dritten die Offenbarung von Leistungs- und Verhaltensdaten und sind insoweit als eine Offenbarung unmittelbar das Arbeitsverhältnis betreffender Äußerungen zu werten. Eine solche Offenbarung ist jedoch bei Arbeitnehmern nur dann möglich, wenn eine der Voraussetzungen des § 29 BbgDSG (bei Beamten § 61 LBG) erfüllt ist. So wäre z. B. eine Weitergabe solcher Informationen in dem unabdingbar erforderlichen Umfang an zuständige Kontrollorgane und Aufsichtsbehörden möglich.

13.2.9 PERIS - ein Personalinformationssystem für die Landesverwaltung

Die AG Personalinformationssystem beim IMA-IT, die sich mit der Vorbereitung des Einsatzes des Personalinformationssystems PERIS beschäftigte und an der auch meine Behörde beteiligt war[292], hat im November des vergangenen Jahres ihre Aufgabe abgeschlossen und deshalb ihre Tätigkeit eingestellt. Zuletzt war es insbesondere um technisch-organisatorische Schutzmaßnahmen gegangen, die das System vor unbefugten Zugriffen auf die personenbezogenen Daten der Beschäftigten schützen sollen.

Hierzu hatte ich nachfolgende vier **Szenarien** entwickelt, die auch für andere Personalinformationssysteme[293] analog gelten können:

Szenarium I - **Kleines lokales Netz** nur für Rechner der Personalstelle

Kleines lokales, physikalisch eigenständiges Netz mit eigenem Server für PERIS, kein Anschluß an andere lokale oder weite Netze, Diensträume überschaubar zusammenliegend, Raumsicherung vorhanden, spezielle Schutzmaßnahmen für den Personaldatenbestand auf dem Server (Data-Safe, wechselbare Festplatte o.ä.):

Unter diesen Bedingungen dürfte das schwache Verschlüsselungsverfahren von PERIS noch ausreichend sein.

---

[292] s. 4. Tätigkeitsbericht unter 13.1

[293] s. unter 13.2.1

Szenarium II - **Großes lokales Behördennetz** mit verschiedenen Anwendungen **und eigenem Server** für PERIS

Großes lokales Netz, physikalisch nicht eigenständig, mit eigenem Server für PERIS (mit eigenem Systemverwalter und eigener Raumsicherung), kein Anschluß an Weitverkehrsnetze:

Für den Datentransport im Netz reicht die Verschlüsselung von PERIS nicht aus, da aufgrund der bekannten Struktur der Personaldatensätze und dem Wechsel von verschlüsselten und nicht verschlüsselten Datenfeldern eine Dechiffrierung relativ leicht durchführbar ist. Hier sind starke Verfahren (Triple-DES, IDEA, RSA o.ä.) wenigstens für die Leitungsübertragung erforderlich.

Szenarium III - **Großes lokales Behördennetz** mit verschiedenen Anwendungen **ohne eigenen Server** für PERIS

Netzbeschreibung wie unter 2, jedoch ohne eigenen Server für PERIS:

Hier ist sowohl für die Leitungsübertragung als auch für die Datenspeicherung auf dem Server ein starkes Verschlüsselungsverfahren (s. Szenarium II) erforderlich, da der/die allgemeine/n Systemverwalter sonst Zugriff auf den Datenbestand erlangen könnte/n.

Szenarium IV - Für alle **lokalen Netze, die eine Schnittstelle zu Weitverkehrsnetzen** haben

Hier ist generell der Einsatz starker Verschlüsselungsverfahren (s. Szenarium II) erforderlich, da durch Fax-Karten, E-Mail und andere Dienste eine grundsätzliche Gefährdung der Vertraulichkeit von Seiten der Weitverkehrsnetze besteht, die nicht einmal eine Firewall ganz abwehren kann.

Da einerseits die derzeitige Software von PERIS zunächst nur über eine schwache Verschlüsselung verfügte, andererseits aber für dessen Einsatz auch die Szenarien II bis IV gewünscht war, mußte die Frage der Verschlüsselung und des Schlüsselmanagements geklärt werden. Dies war zumindest für das Software-System insofern relativ einfach, als dafür besondere Schnittstellen bestehen. Zu unterscheiden ist dabei zwischen der Netzverschlüsselung und der Datenbankverschlüsselung, die unabhängig voneinander funktionieren.

Für die **Netzverschlüsselung** generiert der Systemverwalter auf dem Server beliebig viele RSA-Schlüsselpaare. Auf Anforderung eines Client (Anwenderarbeitsplatz) sendet der Server den öffentlichen Schlüssel eines beliebigen RSA-Paares an den Arbeitsplatz. Im Arbeitsplatz-PC des Anwenders wird dann ein sog. DES3-Sitzungsschlüssel mittels Zufallsgenerator erzeugt, der dem Server, mit dessen öffentlichem Schlüssel verschlüsselt, zurückgeschickt wird. Der eigentliche Nutzdatentransport erfolgt dann mit der DES3-Verschlüsselung des Anwenders, weil der Server nun dessen DES3-Schlüssel kennt und bei sich verschlüsselt abgespeichert hat. Auch bei einem solchen Verfahren ist die Rechengeschwindigkeit noch ausreichend hoch. Bei jeder neuen Sitzung eines Anwenders werden neue Schlüssel ausgetauscht. Die Datei der RSA-Paare auf dem Server ist ebenfalls verschlüsselt.

Für die besagten RSA-Schlüsselpaare des Servers ist von Bedeutung, wie lang deren öffentliche Schlüssel sind. Als sicher gilt nach dem jetzigen Stand der Technik eine Schlüssellänge von 1024 Bit. Solange die PERIS-Software nur eine Schlüssellänge von 512 Bit realisieren kann, kann sie verantwortungsvoll auch nur nach dem Szenarium I eingesetzt werden. Zukünftig soll es allerdings auch eine Schlüssellänge von 2048 Bit geben.

Die **Serverdatenbankverschlüsselung** ist derzeit noch nicht änderbar. Dies ist für eine Übergangszeit noch hinnehmbar, weil die verantwortliche Firma zugesagt hat, in absehbarer Zeit hier eine Änderungsmöglichkeit für diesen Schlüssel zu programmieren. Der aktuelle Schlüssel für die Serverdaten wird zukünftig wie die o. g. RSA-Schlüsselpaare in der kennwortgeschützten Datei auf dem Server ablegbar sein, die ebenfalls verschlüsselt ist.

Nach meinem jetzigen Kenntnisstand hebe ich gegen die Sicherheitslösungen von PERIS mittels der vorgesehenen Verschlüsselung keine grundsätzlichen datenschutzrechtlichen Bedenken, wenn die dargestellten Schwächen zukünftig abgestellt werden. Allerdings weise ich ausdrücklich und zum wiederholten Male darauf hin,[294] daß PERIS bei einer RSA-Schlüssellänge unter 1024 Bit nur als sog. Insellösung betrieben werden kann.

14 Aus der eigenen Behörde

In den sechs Jahren meiner Amtsführung ist die Dienststelle von einem quasi „Ein-Mann-Betrieb" zu einer leistungsfähigen Bürger- und Verwaltungsbehörde aufgebaut worden, die in der ihr zukommenden gesamtgesellschaftlichen Funktion und Bedeutung sowohl von den Bürgern, dem Landtag, der Landesregierung als auch den zahlreichen öffentlichen Stellen des Landes als unabhängige Kontroll- und Beratungsinstanz angenommen wird, unterdessen anerkannt ist und darüber hinaus bundesweit Beachtung findet.

Die Unterbringung der Behörde 1992 in Kleinmachnow ist der Situation geschuldet. Meine Hoffnung auf einen alsbaldigen Umzug meiner Behörde nach Potsdam hat sich leider nicht erfüllt. Ich halte es nach wie vor für unabdingbar, daß der Datenschutzbeauftragte aber dort erreichbar ist, wo ihn der Bürger auch vermutet - nämlich in der Landeshauptstadt -, wo die obersten Landesbehörden und der Landtag ihren Sitz haben. Nicht zuletzt auch wegen der mit diesen Institutionen zu pflegenden Kontakte haben die Landesbeauftragten für den Datenschutz aller anderen Länder ihren Sitz in der jeweiligen Landeshauptstadt. An meiner Auffassung hat sich auch dadurch nichts geändert, daß die Dienststelle seit geraumer Zeit direkt über die Autobahn zu erreichen ist.

Eine besondere und sehr zeitgemäße Form der Erreichbarkeit meiner Behörde ist durch eine eigene Adresse im Internet (http://www.brandenburg.de/land/lfdbbg/) gegeben. So kann auf diesem Weg insbesondere das unterdessen recht umfangreiche Informationsangebot, das im letzten Berichtszeitraum kontinuierlich um datenschutzrelevante Inhalte erweitert wurde, abgefordert werden. Insgesamt stehen unterdessen meine sämtlichen bisherigen Tätigkeitsberichte, Informationsbroschüren und Presseerklärungen ebenso zum Abruf zur Verfügung wie die aktuellen Entschließungen und Orientierungshilfen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.

Leider mußte ich seit Mitte des Berichtszeitraums wegen einer unumgänglichen Abordnung faktisch den Verlust einer Referentenstelle hinnehmen. Ein weiterer Engpaß wegen der vorübergehend verkürzten Arbeitszeit zweier Mitarbeiter im selben Arbeitsbereich konnte durch die befristete Einstellung eines Juristen in Teilzeitbeschäftigung, der sich dankenswerterweise schnell in die sensible Problematik des Datenschutzes eingefunden hat, weitgehend ausgeglichen werden.

Zunehmend problematisch ist es, die wachsende Fülle der wahrzunehmenden Aufgaben eigenständig und unter Einhaltung der Terminzwänge zu erfüllen. Dies hat dazu geführt, daß im Kreis der Kollegen zunehmend Überlegungen über

[294] s. 3. Tätigkeitsbericht unter 1.3.5 und 4. Tätigkeitsbericht unter 1.4.2

arbeitsteilige Verfahren angestellt werden.

Der Ausstrahlung insgesamt und den vielfältigen Anregungen zu datenschutzrechtlichen Einzelproblemen, die in den letzten Jahren von der Behörde ausgegangen sind, ist es wohl auch mit zuzuschreiben, daß seit März d. J. ihr mit Inkrafttreten des AIG eine zusätzliche Aufgabenstellung zugewiesen wurde und sie seitdem die Amts- und Funktionsbezeichnung „Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht" trägt. Mit dem Akteneinsichts- und Informationszugangsrecht der Bürger steht die Behörde vor einer Herausforderung; sie muß Neuland betreten, um der in sie gesetzten Erwartung zu genügen, bei der praktischen Umsetzung dieses Rechts zwischen Verwaltung und Bürgern zu vermitteln.

Kleinmachnow, den 12. Mai 1998 Dr. sc. Dietmar Bleyl

Der Landesbeauftragte für den Datenschutz

Rede des Landesbeauftragten für den Datenschutz vor dem Plenum des Landtages Brandenburg am 25. Februar 1998

Herr Präsident! Sehr geehrte Damen und Herren Abgeordnete! Der Fünfte Tätigkeitsbericht meiner Behörde war bereits Gegenstand einer Erörterung im Innenausschuß dieses Hohen Hauses. Ich möchte die Gelegenheit nicht nutzen, um die von mir dort angesprochenen Punkte hier noch einmal auszuführen, sondern ich möchte den Tätigkeitsbericht als Ausgangspunkt für weitere Überlegungen nehmen, die anzustellen sind. Der Datenschutzbeauftragte hat auch Vordenker auf seinem speziellen Gebiet zu sein.

Ich möchte aber nicht versäumen, die Zusammenarbeit mit dem Landtag, den Fraktionen und der Landesregierung im Berichtszeitraum als erfreulich und konstruktiv zu bezeichnen. Ich würde mich sehr freuen, wenn dies auch in Zukunft so bliebe.

Nun zu drei Problemen: Was uns beschäftigen muß, ist der Wandel von Werten in der Gesellschaft und damit der Umgang mit Grundrechten, darunter dem Recht auf informationelle Selbstbestimmung. Es gilt, neue Grundsätze hierfür zu entwickeln. Das ist Aufgabe der Datenschutzbeauftragten. Insofern verweise ich auf die schon von Herrn Innenminister Ziel erwähnte Beanstandung des Betreibens der Telekommunikationsanlage aller obersten Landesbehörden. Es war für mich erfreulich, daß die Landesregierung dies zum Anlaß genommen hat, die neuen Datenschutzgrundsätze „Datenvermeidung“ und „Einsatz von datenschutzfreundlichen Technologien“ aufzugreifen und eine diesbezügliche Umrüstung der Anlage zu veranlassen. Die erforderlichen Arbeiten sollen bis zum II. Quartal dieses Jahres abgeschlossen sein.

Dies ist für mich insoweit ein Meilenstein für das Datenschutzrecht in Brandenburg, als Datenschutzrecht hierzulande bislang als Technikfolgenrecht im Sinne von Grundsätzen, die in den Jahren ab 1970 in der alten Bundesrepublik entwickelt worden sind, nämlich der Grundsätze der „Erforderlichkeit“ und „Verhältnismäßigkeit“. „Datenvermeidung“ und „datenschutzfreundliche Technik“ sind hingegen geeignete Prinzipien, dem ungezügelten Informationshunger einer Informationsgesellschaft wirksam Grenzen zu setzen, wird doch damit von vornherein vermieden, daß überhaupt Datenspuren entstehen und Daten weiterverarbeitet werden können.

Diese neuen Datenschutzgrundsätze umzusetzen, wo immer dies im Flächenland Brandenburg möglich ist, sollte unser aller Ziel sein, wobei ich mir vorstellen kann, daß die öffentliche Verwaltung insgesamt hierbei in Verbindung mit Pilotprojekten eine Vorbildfunktion für die Gesellschaft übernehmen könnte. Auch wäre es denkbar, daß die Landesregierung über die Innovation der Entwicklung solcher Technik im Lande unter dem Aspekt nachdenken könnte: Datenschutzfreundliche Technik - ein Qualitätsmerkmal.

Zweitens: Die im Tätigkeitsbericht angesprochene Angleichung der Datenschutzgesetze an die EU-Datenschutzrichtlinie, wodurch europaweit ein gleiches Datenschutzniveau erreicht werden soll, ist von der Landesregierung in ihrer Stellungnahme nicht aufgegriffen worden. Vor der Verabschiedung der EU-Datenschutzrichtlinie war verschiedentlich davon die Rede, daß das bewährte deutsche Datenschutzrecht ein „Exportschlager“ sei und daß insoweit mit Inkrafttreten der EU-Datenschutzrichtlinie so gut wie keine Änderungen im eigenen Land anstünden. Dies hat sich nicht bestätig. Der Bund und alle Bundesländer müssen bis Oktober dieses Jahres Datenschutzbestimmungen in einem sehr umfänglichen Bereich nachrüsten. Ich nenne hier beispielsweise nur die Technikfolgenabschätzung durch sogenannte Vorabkontrollen bei Einführung von neuen Datenverarbeitungssystemen, das Verbot automatisierter Einzelentscheidungen, die Regelungen

über Datenschutzstandards bei Übermittlung in Drittländer - damit sind die Nichtmitgliedsländer gemeint -, die Festschreibung des Prinzips der Datensparsamkeit, die Pflicht zur Bestellung eines behördlichen Datenschutzbeauftragten - letzteres Thema ist in diesem Hohen Hause schon sehr kontrovers diskutiert worden.

Der Bund ist bedauerlicherweise bislang der zu Recht von ihm erwarteten Vorreiterrolle nicht gerecht geworden. Es ist sogar noch offen, ob er überhaupt in der Lage sein wird, termingerecht seiner eigenen diesbezüglichen Verpflichtung nachzukommen.

Damit in Brandenburg diese Schwierigkeit nicht ebenfalls auftritt, hatte ich bereitsEnde letzten Jahres Gespräche initiiert, sowohl unter Beteiligung des Innenministeriums als auch der entsprechenden parallelen Stellen in Berlin. Dieser bewußt so groß gewählte Teilnehmerkreis ist vor dem Hintergrund zu sehen, daß es nach meiner Ansicht mehr und mehr darum gehen muß, zu länderübergreifenden vergleichbaren Datenschutzregelungen zu kommen. Unabhängig davon, welche Änderung des Brandenburgischen Datenschutzgesetzes das Innenministerium als Resümee dieser Gespräche vorschlagen wird, sollte bei der unumgänglichen Novellierung des Brandenburgischen Datenschutzgesetzes in jedem Fall auch der rasanten Technikentwicklung Rechnung getragen werden.

Dabei denke ich beispielsweise an Chipkarten, die demnächst auch in Brandenburg zur Wahrnehmung hoheitlicher Aufgaben zum Einsatz kommen werden, z. B. im Hochschulbereich und im Kurbereich.

Dies sollte nicht ohne bindende Vorgaben an technische Standards im Landesdatenschutzgesetz geschehen, nicht zuletzt, weil davon auch die Akzeptanz solcher und anderer moderner Techniken bei den Betroffen abhängt und der Umfang der damit bezweckten Entlastung der jeweiligen Verwaltung mitbestimmt wird.

Da nicht bei jeder neuen Entwicklung der Technik das Gesetz geändert werden kann, ist es weiterhin vordringlich, die technisch-organisatorischen Maßnahmen der Datenverarbeitung an allgemein verbindlichen Zielvorstellungen auszurichten - ich nenne beispielsweise die Integrität der Daten, die Authentifizierung der Nutzer, die Verwendung von Pseudonymen - und nicht wie bisher im Brandenburgischen Datenschutzgesetz § 10 nur an konkrete Maßnahmen, die ursprünglich für Großrechner erstellt wurden, die in der öffentlichen Verwaltung des Landes kaum Verwendung finden.

Drittens möchte ich auch ganz kurz das Problem des Anspruchs der Verwaltung, bürgernah zu sein, hier ansprechen. Die Verwaltungen, die dem Druck zur Verschlankung und Effektivierung ausgesetzt sind, finden zunehmend die Lösung in der Einrichtung von Bürgerbüros. In solchen Bürgerbüros werden die Außenkontakte zur Verwaltung von Gemeinden, Ämtern und mit Sicherheit demnächst auch von Landkreisen in einer Weise angeboten, daß der Bürger seine Anliegen mit einem Mal und an einer Stelle erledigt bekommt.

Wie dieses durchaus nachvollziehbare Verwaltungsanliegen datenschutzgerecht gestaltet werden kann, das ist durchaus problematisch. Denn jeder Mitbürger kann so unter Umständen alles miterleben, was derjenige, der vor ihm oder neben ihm bedient wird, will, braucht, soll, kann, nicht darf, zu bezahlen hat usw. Dies darf nicht so sein.
Neben diesem technisch lösbaren Datenschutzproblem sind die eigentlichen Probleme von Bürgerbüros eher allerdings im Grundsätzlichen zu sehen, nämlich einerseits in der Zuständigkeit und Verantwortlichkeit für die Daten, auf die die Mitarbeiter dieser vorgelagerten Verwaltungseinheiten zugreifen dürfen, den sogenannten parallelen Zuständigkeiten, andererseits in der Einhaltung der der kommunalen Selbstverwaltung vom Gesetzgeber auferlegten Schranken, insbesondere gegenüber dem Steuer- und Sozialgeheimnis. Dies wird im Augenblick bei den mir bekannt gewordenen Bürgerbüros übersehen und ist bereits bei der Konzeption solcher Bürgerbüros zu beachten.

Sehr geehrte Damen und Herren Abgeordnete! Diese eher kritischen Ausführungen sollten Ihnen nicht den Blick dafür versperren, daß in den letzten Jahren in Brandenburg für jedermann ganz offenkundig insbesondere durch meine Behörde sehr viel für die Durchsetzung des Rechts auf informationelle Selbstbestimmung im öffentlichen Bereich erreicht wurde. Es liegt zum einen aber an der Materie selbst und zum anderen an den eingangs erwähnten, sich ständig ändernden gesellschaftlichen Rahmenbedingungen, unter denen das Recht auf informationelle Selbstbestimmung ausgeübt bzw. gewährt wird, daß Datenschutz immer neue Fragen und Probleme aufwirft. Datenschutz stellt deshalb eine latente Herausforderung an uns alle dar, der ich mich als Leiter der hierfür zuständigen Behörde gern mit Engagement weiterhin stellen möchte. - Herzlichen Dank für Ihr Interesse.

Entschließung
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 20. Oktober 1997

zu den Vorschlägen der Arbeitsgruppe der Arbeits- und Sozialministerkonferenz (ASMK)

„Verbesserter Datenaustausch bei Sozialleistungen"

Mit dem von der ASMK-Arbeitsgruppe vorgeschlagenen erweiterten Datenaustausch bei Sozialleistungen wird die Bekämpfung von Leistungsmißbräuchen angestrebt. Soweit dieses Ziel der Arbeitsgruppe mit einer Veränderung der Strukturen der Verarbeitung personenbezogener Daten im Sozialleistungsbereich - insbesondere mit veränderten Verfahren der Datenerhebung - erreicht werden soll, muß der verfassungsrechtlich gewährleistete Grundsatz der Verhältnismäßigkeit beachtet werden.

Die gegenwärtigen Regelungen der Datenerhebung im Sozialleistungsbereich sehen unterschiedliche Verfahren der Datenerhebung vor, vor allem

- Datenerhebungen beim Betroffenen selbst

- Datenerhebungen bei Dritten mit Mitwirkung des Betroffenen

- Datenerhebungen bei Dritten ohne Mitwirkung des Betroffenen aus konkretem Anlaß

- Datenerhebungen bei Dritten ohne Mitwirkung des Betroffenen ohne konkreten Anlaß (Stichproben/Datenabgleich).

Diese Verfahren der Datenerhebung sind mit jeweils unterschiedlich schwerwiegenden Eingriffen in das Persönlichkeitsrecht der Betroffenen verbunden. So weiß z. B. bei einer Datenerhebung beim Betroffenen dieser, wer wann welche Daten zu welchem Zweck über ihn erhebt und Dritte erhalten keine Kenntnis von diesen Datenerhebungen.

Im Gegensatz dazu wird bei einer Datenerhebung bei Dritten ohne Mitwirkung des Betroffenen dieser darüber im unklaren gelassen, wer wann welche Daten zu welchem Zweck über ihn erhebt und Dritten werden Daten über den Betroffenen zur Kenntnis gegeben (z. B. der Bank die Tatsache, daß der Betroffene Sozialhilfeempfänger ist).

Dieses System der Differenzierung des Verfahrens der Datenerhebung entspricht dem Grundsatz der Verhältnismäßigkeit. Ferner ist zu differenzieren, ob Daten aus dem Bereich der Sozialleistungsträger oder Daten außerhalb dieses Bereichs erhoben werden.

In dem Bericht der Arbeitsgruppe wird dieses System zum Teil aufgegeben. Es werden Verfahren der Datenerhebung vorgesehen, die schwerwiegend in die Rechte der Betroffenen eingreifen, ohne daß hinreichend geprüft und dargelegt wird, ob minder schwere Eingriffe in das Persönlichkeitsrecht zum Erfolg führen können. Die Datenschutzbeauftragten wenden sich nicht um jeden Preis gegen Erweiterungen des Datenaustauschs, gehen aber davon aus, daß pauschale und undifferenzierte Änderungen des gegenwärtigen Systems unterbleiben.

Datenabgleichsverfahren sollen nur in Frage kommen bei Anhaltspunkten für Mißbrauchsfälle in nennenswertem Umfang. Deshalb müssen etwaige neue Datenabgleichsverfahren hinsichtlich ihrer Wirkungen bewertet werden. Daher ist parallel zu ihrer Einführung die Implementierung einer Erfolgskontrolle für das jeweilige Abgleichsverfahren vorzusehen, die auch präventive Wirkungen erfaßt. Dies ermöglicht, Aufwand und Nutzen zueinander in das verfassungsmäßig gebotene Verhältnis zu setzen.

Soweit unter Beachtung dieser Prinzipien neue Kontrollinstrumente gegen den Leistungsmißbrauch tatsächlich erforderlich sind, muß für den Bürger die Transparenz der Datenflüsse sichergestellt werden. Diese Transparenz soll gewährleisten, daß der Bürger nicht zum bloßen Objekt von Datenerhebungen wird.

Bezugnehmend auf die bisherigen Äußerungen des BfD und von LfD bestehen gegen folgende Vorschläge im Bericht gravierende Bedenken:

1. **Mitwirkung bei der Ahndung des Mißbrauchs (für alle Leistungsträger) und Verbesserungen für die Leistungsempfänger** (zu D.II.10.1 und B.I) (S. 30 u. S. 2)

   Die vorgeschlagenen Möglichkeiten von anlaßunabhängigen Mißbrauchskontrollen beinhalten keine Klarstellung der gegebenen Rechtslage, sondern stellen erhebliche Änderungen des bisherigen abgestuften Systems der Datenerhebung dar.

   Die mit der Datenerhebung verbundene Offenlegung des Kontaktes bzw. einer Leistungsbeziehung zu einem Sozialleistungsträger stellt einen erheblichen Eingriff für den Betroffenen dar, u. a. da sie geeignet ist, seine Stellung in der Öffentlichkeit, z. B. seine Kreditwürdigkeit, wesentlich zu beeinträchtigen. Anfragen bei Dritten ohne Kenntnis des Betroffenen lassen diesen im unklaren, welche Daten wann an wen übermittelt wurden.

   Derartige Datenerhebungen werden vom geltenden Recht deshalb mit Rücksicht auf das verfassungsrechtliche Verhältnismäßigkeitsprinzip nur in begrenzten und konkretisierten Ausnahmefällen zugelassen. Von dieser verfassungsrechtlich gebotenen Systematik würde die vorgeschlagene Neuregelung grundlegend abweichen. Die Datenschutzbeauftragten betonen bei dieser Gelegenheit den allgemeinen Grundsatz, daß Datenerhebungen, die sowohl pauschal und undifferenziert sind, als auch ohne Anlaß erfolgen, abzulehnen sind.

   Die Datenschutzbeauftragten weisen schließlich darauf hin, daß gegen eine Ausnutzung der technischen Datenverarbeitungsmöglichkeiten zugunsten des Betroffenen (B.I des Berichts) nichts spricht, solange die Betroffenen davon informiert sind und soweit sie dem Verfahren zugestimmt haben.

2. **Nachfrage beim Wohnsitzfinanzamt des Hilfesuchenden zu Schenkungen und Erbschaften** (zu D.I.1.1) (S. 6)

   Die Datenschutzbeauftragten teilen nicht die Auffassung, daß Stichproben nach der geltenden Rechtslage zu § 21 Abs 4 SGB X möglich sind. § 21 Abs 4 SGB X ist eine Auskunftsvorschrift für die Finanzbehörden, die über die Datenerhebungsbefugnis der Sozialleistungsträger nichts aussagt. Die Leistungsträger dürfen diese Auskünfte bei den Finanzbehörden als Dritten nur nach Maßgabe des § 67a SGB X einholen, soweit das erforderlich ist: Diese Erforderlichkeit setzt Anhaltspunkte für Leistungsmißbrauch im Einzelfall voraus.
3. **Auskunftspflicht der Banken und Lebensversicherungen** (zu D.II.1.6) (S. 13)

Die Datenerhebung im Sozialbereich ist von einer möglichst weitgehenden Einbeziehung des Betroffenen gekennzeichnet. Der Vorschlag zur Einführung einer Auskunftspflicht geht auf dieses differenzierte System der Datenerhebungen im Sozialbereich überhaupt nicht ein.

Die Annahme in der Begründung des Vorschlags, ohne eine derartige Auskunftspflicht bestünden keine sachgerechten Ermittlungsmöglichkeiten, trifft nicht zu. Der Betroffene ist verpflichtet, Nachweise zu erbringen; dazu können auch Bankauskünfte gehören. Allerdings ist dem Betroffenen vorrangig Gelegenheit zu geben, solche Auskünfte selbst und ohne Angabe ihres Verwendungszwecks beizubringen. Nur soweit dennoch erforderlich, ist der Betroffene im Rahmen seiner Mitwirkungspflicht gehalten, sein Einverständnis in die Erteilung von Bankauskünften zu geben.

Die vorgeschlagene pauschale Auskunftsverpflichtung birgt deshalb die Gefahr in sich, daß dann generell ohne Mitwirkung des Betroffenen und ohne sein Einverständnis sofort an die Bank/Lebensversicherung herangetreten wird mit der Wirkung, daß der Betroffene desavouiert wird.

Die Datenschutzbeauftragten halten deshalb eine Klarstellung für dringend erforderlich, daß derartige unmittelbare Anfragen und Auskünfte erst in Betracht kommen, wenn die Ermittlungen unter Mitwirkung des Betroffenen zu keinem ausreichenden Ergebnis führen und Anhaltspunkte dafür bestehen, daß bei der fraglichen Bank/Lebensversicherung nicht angegebenes Vermögen vorhanden ist.

4. Akzeptanz des Datenaustausches (zu E.IV) (S. 36)

Datenabgleiche beinhalten eine Verarbeitung personenbezogener Daten, die nicht beliebig durchgeführt werden darf und anerkanntermaßen einer gesetzlichen Grundlage bedarf. Die im Papier der Arbeitsgruppe unter E.IV vertretene These, daß anlaßunabhängige Datenabgleiche keiner speziellen gesetzlichen Grundlage bedürften, trifft deshalb nicht zu.

Die Datenschutzbeauftragten wenden sich nicht gegen einzelne Veränderungen der Datenverarbeitung im Sozialleistungsbereich, soweit sie tatsächlich erforderlich und verhältnismäßig sind und die zuvor aufgezeigten Grundsätze beachtet werden. Die Datenschutzbeauftragten sind dazu gesprächsbereit.

Entschließung
der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 23./24. Oktober 1997 in Bamberg

Novellierung des Bundesdatenschutzgesetzes und
Modernisierung des Datenschutzrechts

Die fristgerechte Harmonisierung des Datenschutzes entsprechend den Vorgaben der europäischen Datenschutzrichtlinie vom 24. Oktober 1995 droht zu scheitern. Die von dieser Richtlinie gesetzte Dreijahresfrist wird heute in einem Jahr ablaufen. Eine gründliche Beratung im Deutschen Bundestag wird durch den baldigen Ablauf der Legislaturperiode in Frage gestellt.

Noch immer gibt es keinen Kabinettsbeschluß; die Bundesregierung hat bisher noch nicht einmal einen abgestimmten Referentenentwurf vorgelegt. Sie gefährdet dadurch die rechtzeitige Umsetzung der Richtlinie und riskiert ein Vertragsverletzungsverfahren vor dem Europäischen Gerichtshof.

Für die Entwicklung des Datenschutzes ist diese Lage höchst nachteilig:

- Verbesserungen des Datenschutzes der Bürger, z. B. durch genauere Information über die Verarbeitung ihrer Daten, verzögern sich;

- dem Datenschutzrecht droht Zersplitterung, weil den Ländern eine Orientierung für die Anpassung der Landesdatenschutzgesetze fehlt.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an die Bundesregierung, für eine fristgerechte Umsetzung der Richtlinie Sorge zu tragen.

Zur Harmonisierung des europäischen Datenschutzrechts empfehlen die Datenschutzbeauftragten der Bundesregierung und dem Gesetzgeber folgende Grundsatzentscheidungen:

- weitgehende Gleichbehandlung des öffentlichen und des privaten Bereichs bei gleichzeitiger Verbesserung der Datenschutzkontrolle, insbesondere durch generell anlaßunabhängige Kontrolle und durch die ausdrückliche Festlegung der völligen Unabhängigkeit der Aufsichtsbehörden und die Erweiterung ihrer Eingriffsbefugnisse;

- Bestellung weisungsfreier Datenschutzbeauftragter auch bei öffentlichen Stellen mit dem Recht, sich jederzeit an den Bundes- oder Landesbeauftragten für den Datenschutz zu wenden;

- Bürgerfreundlichkeit durch einfache und verständliche Formulierung des BDSG, z. B. durch einen einheitlichen Begriff der Verarbeitung personenbezogener Daten entsprechend der Richtlinie;

- Gewährleistung eines einheitlichen, hohen Datenschutzniveaus durch Beibehaltung der Funktion des BDSG und der Landesdatenschutzgesetze als Querschnittsgesetze sowie durch Vermeidung eines Gefälles zwischen den Bereichen, die der EG-Datenschutzrichtlinie unterfallen, und den übrigen Gebieten, deren Datenschutzregelungen nicht verschlechtert werden dürfen

- Sonderregelungen für Presse und Rundfunk nur, soweit zur Sicherung der Meinungsfreiheit notwendig.

Als ebenso vordringlich betrachten die Datenschutzbeauftragten eine Anpassung der noch von der Großrechnertechnologie der siebziger Jahre bestimmten gesetzlichen Regelungen an die heutige Informationstechnologie und an die Verhältnisse der modernen Informationsgesellschaft. Dazu gehören insbesondere folgende Punkte:

- Verbindliche Grundsätze für die datenschutzfreundliche Gestaltung von Informationssystemen und -techniken, so zur Datensparsamkeit, zur Anonymisierung und Pseudonymisierung, zur Verschlüsselung und zur Risikoanalyse;

- mehr Transparenz für die Verbraucher und mehr Eigenständigkeit für die Anbieter durch Einführung eines Datenschutzaudits;

- Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen, Regelung der Video-Überwachung;

- Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren;

- Einführung einer Vorabkontrolle für besonders risikoreiche Datenverarbeitung, namentlich bei Verarbeitung sensitiver Daten;

- Regelungen für Chipkarten-Anwendungen;

- Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing, unter anderem auch mindestens durch die Festlegung von Hinweispflichten hinsichtlich der Möglichkeit des Widerspruchs; vorzuziehen ist in jedem Fall eine Einwilligungsregelung;

- Verstärkung des Schutzes gegenüber der Einholung von Selbstauskünften vor Abschluß von Miet-, Arbeits- und ähnlich existenzwichtigen Verträgen;

- Datenexport nach Inlandsgrundsätzen nur bei angemessenem Schutzniveau im Empfängerstaat; Festlegung, unter welchen Voraussetzungen ein Mitgliedstaat Daten, die er im Anwendungsbereich der Richtlinie (also nach Inlandsgrundsätzen) erhalten hat, außerhalb ihres Anwendungsbereichs verwenden darf;

- möglichst weitgehende Ersetzung der Anmeldung von Dateien bei der Aufsichtsbehörde durch Bestellung weisungsfreier Datenschutzbeauftragter; Beibehaltung des internen Datenschutzbeauftragten auch bei Sicherheitsbehörden;

- Stärkung der Kontrollrechte des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz durch uneingeschränkte Kontrollbefugnis bei der Verarbeitung personenbezogener Daten in Akten einschließlich solcher über Sicherheitsüberprüfungen.

Die Konferenz weist ferner auf die Rechtspflicht der Länder hin, ihr Datenschutzrecht ebenfalls der EG-Richtlinie fristgerecht anzupassen.

Entschließung
der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 23./24. Oktober 1997 in Bamberg

Informationelle Selbstbestimmung und Bild-Ton-Aufzeichnungen bei Vernehmungen im Strafverfahren

Überlegungen des Gesetzgebers und eine beginnende öffentliche Diskussion, moderne Dokumentationstechnik der Wahrheitsfindung und dem Zeugenschutz in gerichtlichen Verfahren nutzbar zu machen, liegen auch im Interesse des Datenschutzes. Dabei ist allerdings zu beachten, daß Bild-Ton-Aufzeichnungen von Vernehmungen im Strafverfahren einen erheblichen Eingriff in das Persönlichkeitsrecht darstellen. Sie spiegeln die unmittelbare Betroffenheit der Beschuldigten oder Zeugen in Mimik und Gestik umfassend wider. Zweck und Erforderlichkeit dieses Eingriffs bedürfen einer sorgfältigen Begründung durch den Gesetzgeber. Sie bildet den Maßstab, der über Möglichkeiten, Grenzen und Verfahren der Videotechnologie im Strafprozeß entscheidet. Erkennbar und nachvollziehbar sollte sein, daß der Gesetzgeber die Risiken des Einsatzes dieser Technologie, insbesondere die Verfügbarkeit der Aufzeichnungen nach den allgemeinen Vorschriften über die Beweisaufnahme bedacht und bewertet hat. Ferner sollte erkennbar und nachvollziehbar sein, daß Alternativen zur Videotechnologie, namentlich die Verwendung von Tonaufzeichnungen, in die Erwägungen des Gesetzgebers aufgenommen wurden.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder sollten die vorliegenden Gesetzentwürfe des Bundesrates (BT-Drs. 13/4983 vom 19.06.1996) sowie der Fraktionen der CDU/CSU und F.D.P. (BT-Drs. 13/7165 vom 11.03.1997) in einem umfassenderen Bedeutungs- und Funktionszusammenhang diskutiert werden. Zunehmend tritt das Anliegen der Praxis hervor, Bild-Ton-Aufzeichnungen auch mit anderer Zielsetzung zu verwerten:

Bild-Ton-Aufzeichnungen ermöglichen eine vollständige und authentische Dokumentation nicht nur des Inhalts, sondern auch der Entstehung und Begleitumstände einer Aussage. Die Beurteilung ihres Beweiswerts wird dadurch deutlich verbessert. Zugleich dient eine nur einmalige Vernehmung, die möglichst zeitnah zum Tatgeschehen durchgeführt und aufgezeichnet wird, der Wahrheitsfindung und erhöht die Qualität der gerichtsverwertbaren Daten („Vermeidung kognitiver Dissonanzen"). Ausgehend von diesen Überlegungen, hat der Gesetzgeber unter Einbeziehung von Erkenntnissen der Vernehmungspsychologie zu prüfen, ob und inwieweit eine wortgetreue Abfassung von Vernehmungsniederschriften ausreicht und eine Aufzeichnung der Aussage nur im Wort auf Tonband für die Zwecke des Strafverfahrens in ihrer Beweisqualität der Videotechnologie sogar überlegen ist.

Für Videoaufzeichnungen des Betroffenen, die zu seinem Schutz gefertigt werden sollen, ist dessen Einwilligung unverzichtbare Voraussetzung für die Zulässigkeit einer Bild-Ton-Aufzeichnung im Strafverfahren. Sofern der Betroffene nicht in der Lage ist, die Bedeutung und Tragweite einer Bild-Ton-Aufzeichnung und ihrer Verwendungsmöglichkeiten hinreichend zu beurteilen, hat der Gesetzgeber festzulegen, wer anstelle des Betroffenen die Einwilligung erteilen darf. Vor Abgabe der Einwilligungserklärung ist der Betroffene umfassend aufzuklären, insbesondere auch über alle zulässigen Arten der weiteren Verwertung und über die Möglichkeit des Widerrufs der Einwilligung für die Zukunft. Die Aufklärung ist zuverlässig zu dokumentieren. Entsprechendes gilt für die Herausgabe von Videoaufzeichnungen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern wirksame Vorkehrungen zum Schutz des Persönlichkeitsrechts bei Verwendung von Bild-Ton-Aufzeichnungen im Strafverfahren. Unabhängig von der Frage, welche Zielsetzung mit Bild-Ton-Aufzeichnungen im Strafverfahren verfolgt werden soll, sind hierbei insbesondere folgende

Gesichtspunkte von Bedeutung:

1. Es ist sicherzustellen, daß der Eindruck des Aussagegeschehens z. B. durch Zeitlupe, Zeitraffer, Einzelbildabfolge, Standbild und Zoom nicht gezielt verfremdet oder verzerrt wird.

2. Einsatz und Verwertung von Bild-Ton-Aufzeichnungen sind so zu regeln, daß gesetzliche Zeugnisverweigerungsrechte gewahrt bleiben. Insbesondere ist eine weitere Nutzung der Aufnahme, auch zum Zwecke des Vorhalts, ausgeschlossen, wenn sich ein Zeuge auf sein Zeugnisverweigerungsrecht beruft.

3. Vorbehaltlich des o. g. Einwilligungserfordernisses darf eine Übermittlung von Videoaufzeichnungen an Stellen außerhalb der Justiz, wenn überhaupt, nur in Ausnahmefällen erlaubt sein, da nur so ein wirksamer Schutz vor Mißbrauch, etwa durch kommerzielle Verwertung, gewährleistet werden kann. Soweit der Gesetzgeber aus Gründen eines fairen, rechtsstaatlichen Strafverfahrens die Weitergabe von Videokopien an Verfahrensbeteiligte zuläßt, müssen jedenfalls wirksame Vorkehrungen gegen Mißbrauch gewährleistet sein, z. B. sichtbare Signierung und strafbewehrte Regelungen über Zweckbindungen und Löschungsfristen.

4. Eine Verwertung der Aufzeichnungen im Rahmen eines anderen Strafverfahrens ist nur zulässig, soweit sie auch für die Zwecke dieses anderen Verfahrens hätten angefertigt werden dürfen.

5. Soweit eine Verwertung in einem anderen gerichtlichen Verfahren - etwa zur Vermeidung erneuter Anhörung kindlicher Zeugen vor dem Familien- oder Vormundschaftsgericht - zugelassen werden sollte, sind in entsprechenden Ausnahmeregelungen präzise Voraussetzungen hierfür abschließend zu bestimmen und enge Verwendungsregelungen zu treffen.

6. Spätestens mit dem rechtskräftigen Abschluß des Strafverfahrens sind grundsätzlich die Aufzeichnungen unter Aufsicht der Staatsanwaltschaft zu vernichten. Der Betroffene ist davon zu benachrichtigen. Soweit der Gesetzgeber ausnahmsweise zur Wahrung vorrangiger Rechtsgüter eine längere Aufbewahrung der Aufzeichnungen zuläßt, müssen Voraussetzungen, Umfang und Fristen der weiteren Aufbewahrung klar und eng geregelt werden.

Entschließung
der 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 23./24. Oktober 1997 in Bamberg

Erforderlichkeit datenschutzfreundlicher Technologien

Moderne Informations- und Telekommunikationstechnik (IuK-Technik) gewinnt in allen Lebensbereichen zunehmende Bedeutung. Die Nutzer wenden diese Technik z. B. in Computernetzen, Chipkartensystemen oder elektronischen Medien in vielfältiger Weise an und hinterlassen dabei zumeist umfangreiche elektronische Spuren. Dabei fällt in der Regel eine Fülle von Einzeldaten an, die geeignet sind, persönliche Verhaltensprofile zu bilden.

Den Erfordernissen des Datenschutzes wird nicht in ausreichendem Maße Rechnung getragen, wenn sich der Schutz der Privatheit des einzelnen lediglich auf eine Beschränkung des Zugangs zu bereits erhobenen, gespeicherten und verarbeiteten personenbezogenen Daten reduziert. Daher ist es erforderlich, bereits vor der Erhebung und Speicherung die zu speichernde Datenmenge wesentlich zu reduzieren.

Datensparsamkeit bis hin zur Datenvermeidung, z. B. durch Nutzung von Anonymisierung und Pseudonymisierung personenbezogener Daten, spielen in den unterschiedlichen Anwendungsbereichen der IuK-Technik, wie elektronischen Zahlungsverfahren, Gesundheits- oder Verkehrswesen, bisher noch eine untergeordnete Rolle. Eine datenschutzfreundliche Technologie läßt sich aber nur dann wirksam realisieren, wenn das Bemühen um Datensparsamkeit die Entwicklung und den Betrieb von IuK-Systemen ebenso stark beeinflußt wie die Forderung nach Datensicherheit.

Die Datenschutzbeauftragten des Bundes und der Länder wollen in Zusammenarbeit mit Herstellern und Anbietern auf datenschutzgerechte Lösungen hinarbeiten. Die dafür erforderlichen Techniken stehen weitgehend schon zur Verfügung. Moderne kryptographische Verfahren zur Verschlüsselung und Signatur ermöglichen die Anonymisierung oder Pseudonymisierung in vielen Fällen, ohne daß die Verbindlichkeit und Ordnungsmäßigkeit der Datenverarbeitung beeinträchtigt werden. Diese Möglichkeiten der modernen Datenschutztechnologie, die mit dem Begriff „Privacy enhancing technology (PET)“ eine Philosophie der Datensparsamkeit beschreibt und ein ganzes System technischer Maßnahmen umfaßt, sollten genutzt werden.

Vom Gesetzgeber erwarten die Datenschutzbeauftragten des Bundes und der Länder, daß er die Verwendung datenschutzfreundlicher Technologien durch Schaffung rechtlicher Rahmenbedingungen forciert. Sie begrüßen, daß sowohl der Mediendienste-Staatsvertrag der Länder als auch das Teledienstedatenschutzgesetz des Bundes bereits den Grundsatz der Datenvermeidung normieren. Der in den Datenschutzgesetzen des Bundes und der Länder festgeschriebene Grundsatz der Erforderlichkeit läßt sich in Zukunft insbesondere durch Berücksichtigung des Prinzips der Datensparsamkeit und der Verpflichtung zur Bereitstellung anonymer Nutzungsformen verwirklichen. Die Datenschutzbeauftragten des Bundes und der Länder bitten darüber hinaus die Bundesregierung, sich im europäischen Bereich dafür einzusetzen, daß die Förderung datenschutzfreundlicher Technologien entsprechend dem Vorschlag der Kommission in das 5. Rahmenprogramm „Forschung und Entwicklung“ aufgenommen wird.

Neben Anbietern von Tele- und Mediendiensten sollten auch die Hersteller und Anbieter von IuK-Technik bei der Ausgestaltung und Auswahl technischer Einrichtungen dafür gewonnen werden, sich am Grundsatz der Datenvermeidung zu orientieren und auf eine konsequente Minimierung gespeicherter personenbezogener Daten achten.

Thesenpapier der Datenschutzbeauftragten des Bundes und der Länder zum Allgemeinen Informationszugangsrecht und zum Recht auf informationelle Selbstbestimmung

Bei dem vorliegendem Papier handelt es sich um die überarbeitete Fassung des Thesenpapiers, das von der 54. Konferenz am 24.10.1997 mit großer Mehrheit (bei wenigen Gegenstimmen) zustimmend zu Kenntnis genommen wurde.

Allgemeines Informationszugangsrecht und Recht auf informationelle Selbstbestimmung

Die Datenschutzbeauftragten des Bundes und der Länder sehen sich zunehmend mit der Frage konfrontiert, in welchem Verhältnis das Grundrecht auf informationelle Selbstbestimmung zur Forderung nach Schaffung eines allgemeinen Informationszugangsrechtes der einzelnen Bürgerinnen und Bürger gegenüber dem Staat steht. Die Verfassung des Landes Brandenburg sieht ein Recht auf Einsicht in Akten und sonstige amtliche Unterlagen der Behörden und Verwaltungseinrichtungen ausdrücklich vor und macht eine Gesetzgebung notwendig. Im Bund und in einigen anderen Ländern diskutiert ein Teil der Parteien ebenfalls über die Gewährung solcher Rechte. In anderen Staaten gehören Informationszugangsrechte zur Rechtstradition (Schweden), oder sie wurden in den letzten Jahrzehnten eingeführt (z. B. USA, Frankreich, Kanada). Die Europäische Union hat für ihre Institutionen in den Amsterdamer Verträgen ein Akteneinsichtsrecht geschaffen. International hat sich der Begriff „Informationsfreiheit" eingebürgert, der damit über den Begriff der Informationsfreiheit im Grundgesetz hinausgeht.

Es spricht viel dafür, daß die Datenschutzbeauftragten nicht nur die Schranken eines allgemeinen Informationszugangsrechts im Hinblick auf die informationelle Selbstbestimmung aufzeigen, sondern sich auch die Forderung nach einem Informationszugangsrecht selbst zu eigen machen. Ein Teil der Datenschutzbeauftragten hat dies auch in der Vergangenheit bereits getan. Das Recht auf informationelle Selbstbestimmung und auf demokratische Teilhabe können so zu einem ausgewogenen Konzept gebracht werden, bei dessen Durchsetzung die Datenschutzbeauftragten durchaus eine aktive Rolle übernehmen können.

I. Informationsgesellschaft und Informationszugang

Anders als die eher dem Prinzip der Öffentlichkeit verpflichteten Bereiche der Legislative und der Judikative, ist das Verwaltungshandeln in der Bundesrepublik Deutschland traditionell geprägt vom Grundsatz des Amtsgeheimnisses. Das geltende Recht räumt den einzelnen Bürgerinnen und Bürgern in der Regel nur Informationsrechte zur Wahrung ihrer individuellen Rechte gegenüber dem Staat ein. Informationsmöglichkeiten bestehen insoweit wegen einer Betroffenheit in eigenen Rechten. Demgegenüber gewinnt in der Informationsgesellschaft die Frage eines darüber hinausgehenden Informationszugangs und somit die Schaffung und Verwirklichung eines allgemeinen Informationszugangsrechts auch unabhängig von einer individuellen Betroffenheit zunehmend an Bedeutung. Wesensbestimmend hierfür sind individuelle und demokratische Komponenten.

Die Freiheit, sich aus allgemein zugänglichen Quellen zu informieren, zählt für das Bundesverfassungsgericht ebenso zu den Grundvoraussetzungen des demokratischen Meinungs- und Willenbildungsprozesses wie zu den Bedingungen verantwortlichen, individuellen Handelns: „Es gehört zu den elementaren Bedürfnissen des Menschen, sich aus möglichst vielen Quellen zu unterrichten, das eigene Wissen zu erweitern und sich so als Persönlichkeit zu entfalten. Zudem ist in der modernen Industriegesellschaft der Besitz von Informationen von wesentlicher Bedeutung für die soziale Stellung des einzelnen. Das Grundrecht der Informationsfreiheit ist wie das Grundrecht der freien Meinungsäußerung eine der wichtigsten Voraussetzungen der freiheitlichen Demokratie" (vgl. BVerfGE 7, 198 [208]). „Erst mit seiner Hilfe wird der

Bürger in den Stand gesetzt, sich selbst die notwendigen Voraussetzungen zur Ausübung seiner persönlichen und politischen Aufgaben zu verschaffen, um im demokratischen Sinne verantwortlich handeln zu können“ (BVerfGE 27, 71 [81 f.]).

Im Hinblick auf die Entwicklung der Informationsgesellschaft und auf die Vielzahl der allein bei der Verwaltung vorhandenen Informationen, kann die bloße Möglichkeit, sich aus allgemein zugänglichen Quellen zu unterrichten, nicht mehr genügen. Ein Kennzeichen der Informationsgesellschaft ist, daß die einzelnen Bürgerinnen und Bürger in zunehmendem Maße vom Zugang zu Informationen abhängig werden. Selbst zur Durchsetzung eigener Rechte sind sie vielfach auf bisher nicht veröffentlichte Informationen angewiesen, auch wenn sie sich nicht unmittelbar auf sie beziehen, aber als Grundlage für ihre schutzwürdigen Interessen wichtig sind. Je intensiver sich Verwaltung und Bürger/-innen der Informationstechnik bedienen und deren erschließbare Informationsressourcen nutzen, um so enger müssen der Zugang zu den Daten und der Schutz der informationellen Selbstbestimmung miteinander verflochten werden. Um die Rechte der einzelnen Bürgerinnen und Bürger dabei zu gewährleisten, ist die Herstellung von Transparenz eine besonders wichtige Zielsetzung bei der humanen Gestaltung der Informationsgesellschaft.

Neben der individuellen Komponente ist Öffentlichkeit für den demokratischen Staat von zentraler Bedeutung. Der Grundsatz der Öffentlichkeit von Parlamentssitzungen und Gerichtsverhandlungen gehört zum Grundbestand unserer Rechtsordnung; ebenso unumstritten ist die Pflicht zur Veröffentlichung von Gesetzen oder von Gerichtsentscheidungen mit grundsätzlicher Bedeutung. Lediglich der Bereich der vollziehenden Gewalt ist vom Öffentlichkeitsgrundsatz bislang weitgehend ausgenommen geblieben.

Dies ist jedoch unter informationstechnischen Bedingungen, die Verwaltungshandeln zunehmend prägen, nicht mehr zeitgemäß. Vielmehr ist Transparenz der Verwaltung für die Wahrnehmung der Teilhabe unerläßlich. Hierfür kann es auf individuelle Betroffenheit oder (was auf das gleiche hinausläuft) berechtigte Interessen der Einzelnen nicht ankommen.

II. Entwicklung der Informationsrechte in Deutschland

Der Entwicklung rechtsstaatlicher Grundsätze ist es vorrangig zu verdanken, daß schon früh den Beteiligten an Gerichtsverfahren Informationsrechte zugestanden wurden, um Ihnen die Möglichkeit zu geben, ihre rechtlichen Interessen wirkungsvoll verfolgen zu können. Für die verwaltungsrechtlichen Streitigkeiten zwischen Bürger/-innen und Staat brachte dies zwangsläufig auch Informationsrechte am vorangehenden Verwaltungsverfahren der Beteiligten mit sich. Der Informationszugang unterliegt in diesem Bereich allerdings nach wie vor der Voraussetzung, am Verfahren beteiligt zu sein, also in aller Regel in irgendeiner Form in eigenen Rechten betroffen zu sein.

Für eine Vielzahl von Planungsentscheidungen ist mittlerweise anerkannt, daß der Kreis der Betroffenen nicht schon im vorhinein festgelegt werden kann. Aus Gründen staatlicher Informationspflichten - z. B. bei der Bauleitplanung - wurden Instrumente geschaffen, um auch potentiell Betroffene zu informieren. In diesen Verfahren sind Planungsgrundlagen öffentlich bekanntzumachen. Einwände kann aber auch in Planungsverfahren nur geltend machen, wer individuell betroffen ist und damit zum Kreis der Beteiligten an diesem Verfahren im weitesten Sinne gehört.
In den siebziger Jahren setzte sich im Zuge der Datenschutzdebatte endgültig die Einsicht durch, daß auch außerhalb förmlicher Verfahren Auskunfts- und Einsichtsrechte der Betroffenen zu schaffen sind. Der datenschutzrechtliche Auskunftsanspruch besteht unabhängig von der Beteiligung an einem förmlichen Verfahren, bezieht sich gleichwohl jedoch nur auf die Daten zu eigenen Person.

Betroffenen- und verfahrensunabhängige Transparenz der Datenverarbeitung schaffen die bei den Datenschutzbeauftragten zu führenden Dateienregister; auch die Zugangsmöglichkeiten für alle zu staatlichem Archivgut wurden erweitert.

Mit dem Umweltinformationsgesetz hat der Gesetzgeber für einen ganzen Bereich die Regel durchbrochen, daß Informationsrechte in Form von Einsichts- und Auskunftsrechten nur Betroffenen oder Beteiligten zustehen. Dies sollte nicht nur als Angleichung an europäisches Recht im Prozeß der europäischen Integration verstanden werden. Vielmehr muß es als Teil einer die Bürgerrechte stärkenden generellen Rechtsentwicklung eingeordnet werden. Umweltveränderungen betreffen in besonderem Maße potentiell alle Bürgerinnen und Bürger. Die Zusammenhänge können infolge der Langzeitwirkung oft nur schwer nachvollzogen werden, und dies setzt auch genaue Kenntnisse der Umweltsituation und der Umweltfaktoren voraus. Würde die Darlegung der Betroffenheit als Voraussetzung für die Erteilung von Auskünften und Informationen verlangt werden, würde dies häufig den Informationszugang unmöglich machen.

Diese Entwicklungslinie sollte konsequenterweise zu einer Öffnung aller Verwaltungsbereiche für den Informationsanspruch der Bürgerinnen und Bürger führen.

III. Grenzen eines allgemeinen Informationszugangsrechts

Ein schrankenloses allgemeines Informationszugangsrecht würde jeder Bürgerin und jedem Bürger die Möglichkeit eröffnen, Einsicht in alle Verwaltungsakten zu nehmen oder Auskunft darüber zu erhalten. Es steht außer Frage, daß ein derart schrankenloses Recht mit dem Grundrecht auf informationelle Selbstbestimmung - aber auch z. B. in die Forschungsfreiheit - unvereinbar sein würde. Grundsätzlich macht jedes personenbezogene Datum in einem Vorgang eine Abwägung mit diesem Grundrecht erforderlich.

Ein Großteil der für den Informationszugang relevanten Unterlagen enthält jedoch einen solchen Personenbezug nicht. Soweit das Zugangsrecht ausschließlich die Grundlagen des grundsätzlichen Verwaltungshandelns (z. B. Erlasse, Rundschreiben und andere Verwaltungsvorschriften, Dienstanweisungen und Grundsatzakten) betrifft, dürfte demzufolge einem solchen Anliegen aus der Sicht des Datenschutzes nichts entgegenstehen. Auch die weiteren Bereiche sachbezogenen Verwaltungshandelns (z. B. Haushaltswesen, Straßenbau, Bildungswesen) werfen keine datenschutzrechtlichen Fragen auf. Selbst wenn solche Unterlagen einzelne personenbezogene Daten enthalten, lassen sie sich nach Anwendung bekannter und bewährter Verfahren (Schwärzung, Kodierung, Pseudonymisierung) zugänglich machen.

Beziehen sich Verwaltungsvorgänge im wesentlichen auf personenbezogene Daten von Betroffenen, bedarf die Offenbarung der Daten im Hinblick auf das Grundrecht auf informationelle Selbstbestimmung einer ausdrücklichen normenklaren Rechtsgrundlage, soweit nicht ebenfalls eine Anonymisierung in Betracht kommt. Derartige Rechtsgrundlagen auf Bundes- und Landesebene liegen in Spezialgesetzen bereits vor oder sind gegebenenfalls zur Ausweitung des Informationszugangesrechts noch zu schaffen. Für Trivialdaten oder andere Daten, bei denen schutzwürdige Interessen der Betroffenen nicht berührt sein können (z. B. weil der oder die Betroffene - wie beim Telefonbuch - selbst der Verbreitung zugestimmt hat), ermöglichen die Datenschutzgesetze in der Regel bereits jetzt die Offenbarung.

Denkbar wäre außerdem, daß der Gesetzgeber im Gesetz über den freien Informationszugang selbst einen Katalog typisierender Beispiele festlegt, in welchen Fällen darüber hinaus das Recht auf informationelle Selbstbestimmung hinter

dem Informationszugangsrecht zurücktritt und - in Umkehrung des normalerweise geltenden Verhältnisses - der Zugang nur bei besonderer Schutzwürdigkeit der personenbezogenen Daten verweigert werden kann. In einen solchen Katalog könnten beispielsweise mit dem Vorgang befaßte Personen, also Amtsträgerinnen und Amtsträger oder beauftragte Beschäftigte, aber auch Sachverständige, die Beiträge bei oder zu der Bearbeitung der Angelegenheit geleistet haben, aufgeführt werden. Die Offenlegung von Verantwortlichkeiten für Verwaltungsentscheidungen oder für Sachbearbeitung gehört zu einer transparenten Verwaltung und dient den überwiegenden Interessen der Öffentlichkeit. Einer besonders sorgfältigen Abwägung bedarf die Frage, ob und in welchen Fällen der freie Zugang zu Identdaten von an Verwaltungsverfahren beteiligten Personen und möglicherweise zu solchen personenbezogenen Daten zu gewährleisten ist, zu deren Bekanntgabe, Auskunft oder Mitteilung betroffene Personen gegenüber einer Behörde verpflichtet waren.

Generell wäre auch daran zu denken, im Einzelfall eine Einwilligung der Betroffenen in die Offenbarung ihrer Daten einzuholen und sie damit zugleich über das Vorliegen eines Informationsbegehrens zu unterrichten. Wird die Einwilligung nicht innerhalb einer bestimmten Frist erteilt, wäre von Amts wegen zu prüfen, ob dem Begehren der oder des Informationssuchenden durch die Mitteilung der Geheimhaltungsverpflichtung und der lediglich sachbezogenen Auskunftserteilung, durch Schwärzung der Daten für die Akteneinsicht oder durch Abtrennung von Aktenteilen nachgekommen werden kann. Jedenfalls würde eine vom Gesetzgeber in dieser Weise zum Ausdruck gebrachte Festlegung für die Öffentlichkeit erhöhte Anforderungen an die behördliche Begründung einer endgültigen Informationsverweigerung zur Folge haben.

Gegen die Gewährung eines Informationszuganges können darüber hinaus im Einzelfall Aspekte sprechen, die sich aus staatlichen Sicherheitsinteressen ergeben oder auch aus dem Interesse an einer effizienten Erfüllung der öffentlichen Aufgaben der Verwaltung. Diesen Aspekten kann im Rahmen eines Informationszugangsgesetzes Rechnung getragen werden. Dabei ist jedoch auch hier zu beachten, daß Abweichungen vom Grundsatz des allgemeinen Informationszugangs im Gesetz hinreichend konkret und bestimmt zu fassen sind. Um die Gefahr zu vermeiden, daß ein Katalog von Ausnahmetatbeständen den Grundsatz des Informationszugangs letztlich doch wieder in sein Gegenteil verkehrt, müßten auch diese Ausnahmetatbestände (z. B. Wohl des Bundes oder eines Landes, Beeinträchtigung der Strafverfolgung und Vollstreckung der Gefahrenabwehr oder andere Belange der inneren Sicherheit sowie Offenbarung von Akten zur Durchführung eines Gerichtsverfahrens) selbst eng ausgelegt werden. Dasselbe gilt für Aktenvorgänge, die bei der laufenden Verwaltungsarbeit anfallen, insbesondere wenn es sich um personenbezogene Daten handelt.

Eine weitere explizite Einschränkung erfährt das Informationszugangsrecht dort, wo gesetzliche Vorschriften ausdrücklich die Geheimhaltung bestimmter Umstände fordern. Daneben hat ein Informationszugangsgesetz in seinen Ausnahmetatbeständen beispielsweise Betriebs- und Geschäftsgeheimnisse zu berücksichtigen; ein ausgewogener Ausgleich zwischen Informationszugang und den durch die Geheimhaltung geschützten Interessen ist zu schaffen.

IV. Abwehr und Durchsetzung des Informationszugangs

Grundsätzlich sollten vor der Erfüllung eines Informationsanspruchs, der mit der Preisgabe personenbezogener Daten verbunden wäre, Betroffene von dem Informationsbegehren unterrichtet werden, um Einwände geltend machen zu können. Wird ihren Einwänden nicht stattgegeben, und kann der Informationsanspruch nicht ohne Eingriff in ihr Recht auf informationelle Selbstbestimmung erfüllt werden, so müssen sie Gelegenheit haben, Abwehrrechte gerichtlich prüfen zu lassen und gegebenenfalls durchsetzen zu können. Auch dann, wenn ein Informationsanspruch verweigert wird, müssen die Anspruchsteller die Möglichkeit haben, den Anspruch mit gerichtlicher Hilfe durchzusetzen und zumindest prüfen zu lassen.

Zusätzlich zum Rechtsweg bietet es sich an, den Bürgerinnen und Bürgern die Möglichkeit zu eröffnen, sich mit ihrem Anliegen an eine unabhängige Stelle zu wenden (Beauftragter oder Beauftragte für Informationsfreiheit). Umfangreiche positive Erfahrungen aus anderen europäischen und aus außereuropäischen Ländern lassen erwarten, daß eine solche unabhängige Stelle die Mehrheit der Fälle klären könnte. Für die unabhängige Stelle bietet sich eine rechtliche Konstruktion an, die derjenigen der Datenschutzbeauftragten des Bundes und der Länder vergleichbar ist. Ihre Tätigkeit hat gezeigt, daß eine unabhängige Stelle auch dann, wenn sie keine Sanktionen verhängt, sondern lediglich über das Instrument der Beanstandung verfügt, dennoch befriedend und ausgleichend wirken kann. Übertragbar wäre beispielsweise das kanadische Modell, bei dem Datenschutz- und Informationszugangskontrolle unter einem Dach vereint sind.

Das Verhältnis zwischen unabhängiger Verwaltungskontrolle und Verwaltungsgerichtsbarkeit könnte durch eine geeignete Regelung des Vorverfahrens und der zu wahrenden Fristen geklärt werden. Das nach der derzeitigen Rechtslage bestehende Problem, daß das Anliegen der Verwaltung an einer Verweigerung der Akteneinsicht mit der Klage faktisch unterlaufen würde, ließe sich beispielsweise nach amerikanischem Vorbild mit der Einführung eines in-camera-Verfahrens lösen, bei dem der streitbefangene Aktenvorgang nur dem Gericht zur Kenntnis zu bringen wäre.

V. Fazit

Unserem Rechtssystem widerspricht es nicht, den einzelnen Bürgerinnen und Bürgern Rechte einzuräumen, die bei staatlichen Stellen den Zugang zu vorhandenen Informationen ohne den Nachweis der Betroffenheit in eigenen Rechten eröffnen. Das moderne Staatsverständnis geht von mündigen und informierten Bürgerinnen und Bürgern aus. Eine Erweiterung der Informationszugangsrechte ist dafür eine der Voraussetzungen, wobei dem verfassungsrechtlichen Rang des Rechts auf informationelle Selbstbestimmung Rechnung getragen werden muß.

Anlage: Informationszugangsrechte in anderen Ländern

Die Informationszugangsrechte sind in anderen Ländern in unterschiedlicher Weise geregelt:

- Dänemark (kein Verfassungsanspruch, Gesetz über die Öffentlichkeit in der Verwaltung vom 19.12.1985),
- England (kein Verfassungsanspruch, jedoch Absichtserklärungen in dem Regierungsprogramm der britischen Labour Party vom 14.05.1997)
- Frankreich (kein Verfassungsanspruch, durch Gesetz vom 17.07.1978),
- Niederlande (Art. 110 Niederländische Verfassung von 1983, Openness of Administration Act von 1978),
- Österreich (Art. 20 Abs. 4 Österreichische Verfassung vom 15.05.1987, Bundesgrundsatzgesetz vom 15.05.1987),
- Portugal (Art. 268 Portugiesische Verfassung von 1976, einfachgesetzliche Zugangsansprüche),
- Spanien (Art.105 Spanische Verfassung, einfachgesetzliche Ansprüche nur in speziellen Bereichen)

- Schweden (seit 1766 mit Verfassungsrang im Grundsatz, Einschränkungen durch Act on Secrecy von 1980)

- Ungarn (Verfassungsanspruch, Act on Protection of Personal Data and Disclosure of Data of Public Interest von 1992)

- Kanada (kein Verfassungsrang, sowohl auf Bundesebene durch Informationszugangsgesetz vom 28.06.1982 als auch in einzelnen Bundesstaaten wie Ontario, Quebec und British Columbia Informationszugangsgesetze)

- USA (keine verfassungsrechtliche Gewährleistung, Freedom of Information Act von 1966)

- Recht für jeden Unionsbürger auf freien Zugang zu Informationen bei den Organen der EU (Art. 191a EGV als Bestandteil der „Maastrichter Verträge“ vom 16./17.Juni 1997)

Bonner Appell gegen den geplanten Großen Lauschangriff

Die Sicherheit jedes einzelnen Bürgers, sich in einen privaten, vom Staat unbeobachteten Raum zurückziehen, sich darin ausleben und regenerieren zu können, ist für die Verwirklichung seines Grundrechtes auf freie Entfaltung der Persönlichkeit unverzichtbar. Wesentliche Grundbedingungen unserer Gesellschaft gerieten in Gefahr, wenn die Unantastbarkeit des Vertrauensverhältnisses eines Bürgers zu seinem Arzt, Rechtsanwalt, Drogenberater, Seelsorger, aber auch zu seinem Ehepartner aufgegeben würde und wenn die Pressefreiheit dadurch eingeschränkt würde, daß Journalisten ihren Informanten nicht mehr Diskretion zusichern könnten. Die Vertraulichkeit des privaten Gesprächs mit Ärzten, mit Anwälten auch außerhalb einer Strafverteidigung, mit Drogen- oder Schwangerschaftsberatern, mit Journalisten, aber auch die Kommunikation zwischen Ehepartnern und innerhalb der engsten Familie ist genauso schützenswert wie das Verhältnis zu Seelsorgern oder die Arbeit von Abgeordneten. Es kann dem Einzelnen nicht zugemutet werden, diese vertraulichen, oft sogar intimen Gespräche in dem Bewußtsein führen zu müssen, daß Dritte später anhand des aufgezeichneten Inhalts entscheiden, ob und zu welchen strafprozessualen Zwecken die Informationen verwertet werden können. Deshalb richten Ärzte, Datenschützer, Journalisten, Anwälte, Richter und Staatsanwälte vor der Entscheidung des Bundestages und des Bundesrates über eine Einführung des Großen Lauschangriffs den dringenden Appell an alle Politiker, den Gesetzesvorlagen nicht zuzustimmen. Die Absicht, dafür zu sorgen, daß es vor der staatlichen Strafverfolgung keine „kontrollfreien Räume" mehr gibt, ist abzulehnen. Die Bekämpfung der Organisierten Kriminalität ist ein wichtiges Ziel. Dies darf aber nicht um jeden Preis, nämlich durch Opferung der letzten Refugien von Privatheit der Bürger, geschehen. Es geht nicht um „Gangsterwohnungen", sondern um Privatwohnungen, Arztpraxen und Anwaltskanzleien.

Jeder kann betroffen sein.

Entschließung
der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Ländervom 19./20. März 1998 in Wiesbaden

Datenschutz beim digitalen Fernsehen

Die Datenschutzbeauftragten des Bundes und der Länder machen darauf aufmerksam, daß bei elektronischen Diensten immer umfangreichere Datenspuren über das Verhalten der Einzelnen entstehen. Mit der Digitalisierung der Fernseh- und Hörfunkübertragung entsteht die technische Infrastruktur dafür, daß erstmals auch das individuelle Mediennutzungsverhalten registriert werden kann. Sie bekräftigen deshalb ihre Forderung, daß auch bei der Vermittlung und Abrechnung digitaler Fernsehsendungen eine flächendeckende Registrierung des individuellen Fernsehkonsums vermieden wird. Im digitalen Fernsehen („Free TV" und „Pay TV") muß die unbeobachtete Nutzung des Mediums ohne Nachteile möglich bleiben.

Die Datenschutzbeauftragten begrüßen es deshalb, daß die Staats- und Senatskanzleien Vorschläge für die Änderung des Rundfunkstaatsvertrags vorgelegt haben, mit denen Belangen des Datenschutzes Rechnung getragen werden soll. Besonders hervorzuheben sind folgende Punkte:

- Die Gestaltung technischer Einrichtungen muß sich an dem Ziel ausrichten, daß so wenige personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden;

- die Rundfunkveranstalter müssen die Nutzung und Bezahlung von Rundfunkangeboten anonym oder unter Pseudonym ermöglichen, soweit dies technisch möglich und zumutbar ist;

- personenbezogene Daten über die Inanspruchnahme einzelner Sendungen dürfen für Abrechnungszwecke nur gespeichert werden, wenn ein Einzelnachweis verlangt wird;

- wie bereits im Mediendienstestaatsvertrag enthält auch der Entwurf des Rundfunkstaatsvertrags eine Vorschrift zum Datenschutzaudit, d. h. Veranstalter können ihr Datenschutzkonzept und ihre technischen Einrichtungen von unabhängigen Gutachtern prüfen und das Prüfungsergebnis veröffentlichen lassen.

Die Datenschutzbeauftragten halten diese Grundsätze für geeignet, eine datenschutzgerechte Nutzung digitaler Fernsehangebote zu ermöglichen. Die technischen Möglichkeiten, diesen datenschutzrechtlichen Vorgaben zu entsprechen, sind gegeben. Die Datenschutzbeauftragten konnten sich bereits 1996 hiervon praktisch überzeugen. Die Systementscheidung von Veranstaltern für einen Decodertyp, der möglicherweise weniger geeignet ist, die Datenschutzanforderungen zu erfüllen, kann kein Maßstab für die Angemessenheit dieser Anforderungen sein, wenn zugleich andere Geräte Ihnen ohne Probleme genügen.

Der Forderung von Inhabern von Verwertungsrechten, einen Nachweis über die Inanspruchnahme von pay-per-view-Angeboten vorzulegen, kann ohne Personenbezug - etwa durch zertifizierte Zähleinrichtungen oder den Einsatz von Pseudonymen - entsprochen werden.

Die Datenschutzbeauftragten bitten deshalb die Ministerpräsidentin und die Ministerpräsidenten der Länder, an den datenschutzrechtlichen Regelungen des Entwurfs festzuhalten. Damit würden das bisherige Datenschutzniveau für die Fernsehnutzung im digitalen Zeitalter abgesichert und zugleich die Vorschriften für den Bereich des Rundfunks und der

Mediendienste harmonisiert.
Die Datenschutzbeauftragten fordern die Rundfunkveranstalter und Hersteller auf, den Datenschutz bei der Gestaltung von digitalen Angeboten schon jetzt zu berücksichtigen.

Entschließungder 55. Konferenz der Datenschutzbeauftragten des Bundes und der Ländervom 19./20. März 1998 in Wiesbaden

Datenschutzprobleme der Geldkarte

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wiederholt ihre Forderung aus ihrer Entschließung vom 13.10.1995 nach einem anonymen elektronischen Zahlungsverfahren bei elektronischen Geldbörsen. Dies gilt insbesondere für die Geldkarte des deutschen Kreditwesens, bei der in kartenbezogenen „Schattenkonten" der Evidenzzentralen nicht nur der Kaufbetrag und ein identifizierbarer Händlerschlüssel, sondern auch der Kaufzeitpunkt gespeichert werden. Mit diesen Daten können sämtliche mit der Geldkarte getätigten Kaufvorgänge jahrelang nachvollzogen werden, wenn die Daten mit den persönlichen Kundendaten zusammengeführt werden. Diese Geldkarte erfüllt nicht die Forderungen der Datenschutzbeauftragten.

Außerdem werden die Kundinnen und Kunden über diese „Schattenkonten" noch nicht einmal informiert. Die Herausgeber solcher Karten bzw. die Kreditinstitute haben aber die Pflicht, ihre Kundinnen und Kunden über Art und Umfang der im Hintergrund laufenden Verarbeitungsvorgänge zu informieren.

Unabhängig davon müssen bei der Geldkarte des deutschen Kreditwesens sämtliche Umsatzdaten in den Evidenzzentralen und auch bei den Händlern nach Abschluß der Verrechnung (Clearing) gelöscht oder zumindest anonymisiert werden.

Die Datenschutzbeauftragten fordern die Kartenherausgeber und die Kreditwirtschaft erneut dazu auf, vorzugsweise kartengestützte Zahlungssysteme ohne personenbezogene Daten - sog. White Cards - anzubieten. Die Anwendung ist so zu gestalten, daß ein karten- und damit personenbezogenes Clearing nicht erfolgt.

Der Gesetzgeber bleibt aufgerufen sicherzustellen, daß auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher bei Bargeldzahlung anonym zu bleiben.

Stellungnahme der Datenschutzbeauftragten der Europäischen Union vom 28. Februar 1997 zum

Grünbuch über den Jugendschutz und den Schutz der Menschenwürde in audiovisuellen Diensten und Informationsdiensten (KOM (96) 483 endg.),

zur Mitteilung an das Europäische Parlament, den Rat, den Wissenschafts- und Sozialausschuß und den Ausschuß der Regionen über rechtswidrige und schädliche Inhalte im Internet (KOM (96) 487)

sowie zur Ratsentschließung vom 28. November 1996 über rechtswidrige und schädliche Inhalte im Internet

- Übersetzung -

Die Datenschutzbeauftragten der Europäischen Union erkennen die Notwendigkeit, Maßnahmen zum Jugendschutz und zum Schutz der Menschenwürde in bezug auf die neuen audiovisuellen und Informationsdienste in Erwägung zu ziehen. Sie weisen auf die Tatsache hin, daß Art. 1 Abs. 1 der EU-Datenschutzrichtlinie (95/46/EC) die Mitgliedstaaten verpflichtet, die Grundrechte und -freiheiten natürlicher Personen und insbesondere ihr Recht auf Schutz der Privatsphäre in bezug auf die Verarbeitung persönlicher Daten zu schützen.

Das Recht auf Datenschutz ist Teil der Menschenwürde. In diesem Zusammenhang bringen die Datenschutzbeauftragten ein besonderes Interesse am Grünbuch zum Jugendschutz und zum Schutz der menschlichen Würde in audiovisuellen und Informationsdiensten zum Ausdruck. In ihrer Stellungnahme zum Grünbuch berücksichtigen die Datenschutzbeauftragten die Mitteilung der Kommission zu rechtswidrigen und schädlichen Inhalten im Internet (KOM (96) 487), die gleichzeitig veröffentlicht wurde, und die Entschließung des Telekommunikations-Ministerrates vom 28. November 1996 zu rechtswidrigen und schädlichen Inhalten im Internet.

Die Datenschutzbeauftragten messen der richtigen Abwägung zwischen dem Datenschutz (einschließlich der Möglichkeit für Nutzer, ihre Anonymität in den Netzen beizubehalten) und der Notwendigkeit, die Haftung für rechtswidriges Verhalten durchzusetzen (Frage 3 des Grünbuchs), erhebliche Bedeutung bei. Im herkömmlichen Massenmedium Fernsehen verbleibt die Verantwortung für rechtswidrige Inhalte eindeutig beim Anbieter der Information. Fernsehen war für den Zuschauer immer spurlos möglich. Das Grünbuch weist zu Recht darauf hin, daß Online-Dienste zu einem neuen Modell der interaktiven Kommunikation führen: Jeder Nutzer wird zu einem potentiellen Anbieter von Informationen. Aber die Verantwortung für rechtswidrige Inhalte sollte auch im Zusammenhang mit den neuen Online-Diensten beim Urheber verbleiben. Sie sollte nicht auf den Nutzer verlagert oder erstreckt werden. Die Tatsache, daß das Internet oder andere Netze in gewissem Umfang dazu genutzt werden, um illegale Inhalte anzubieten, sollte nicht dazu führen, daß das Internet in ein nahtloses Netz der Überwachung verwandelt wird, in dem der gesamte Netzverkehr beobachtet wird, um rechtswidrige Verhaltensweisen aufzuspüren.

Im Kapitel I, Abschnitt 3 des Grünbuchs („ Umfang der Probleme je nach Art der Dienste“) findet sich die Aussage, daß es praktisch unmöglich ist, zufällig auf unerwünschtes Material im Netz zu stoßen. Da diese Annahme Auswirkungen darauf haben wird, wie die Rechtsordnung Personen behandelt, die auf solches Material zugegriffen haben, kann dieser Satz nicht unwidersprochen bleiben. Es muß betont werden, daß der bloße Zugriff auf kontroverses Material

nicht automatisch als vorsätzlich rechtswidriges Handeln verstanden werden darf, weil

- in dem Maße, in dem das Bewußtsein über kontroverse Inhalte wächst, die Prediger der Gewalt und des Rassismus sicherlich raffinierter vorgehen und Websites anbieten werden, die harmloses und kontroverses Material miteinander vermengen oder die gerade zu dem Zweck gestaltet worden sind, um verborgene Haßpropaganda zu verbreiten, während sie bewußt nützliches und unschädliches Material anbieten, um Besucher anzuziehen,

- Internet-Suchmaschinen werden oft Links (Verknüpfungen) zu kontroversem Material vermischt mit Links zu harmlosem Inhalt liefern. Der Nutzer kann dem Link nachgehen und die Daten überprüfen, ob sie für ihn relevant sind, es sei denn, schon der Name der Website (den die Suchmaschine dem Nutzer anzeigt) ist klar genug. Ein Nutzer, der Informationen zu Themen sucht, die auch extremistische Gruppen interessieren (z. B. bestimmte Abschnitte der Zeitgeschichte) muß unter Umständen zahllose extremistische Websites sichten, die auch nicht durch sorgfältige Wahl der Suchbegriffe ausgeschlossen werden können,

- Offline Navigations-Software (Browser), die ganze Websites auf die lokale Festplatte kopiert und den Nutzer das Material nach Belieben überprüfen läßt, wodurch Netzkosten gespart werden, wird zunehmend populär. Mit dieser Software kann der Nutzer dem Programm mitteilen, welche Angebote kopiert werden sollen, ohne daß er deren Inhalt zuvor gesehen hat, so daß in erheblichem Umfang kontroverses Material unter dem Namen dieses Nutzers aus dem Netz heruntergeladen werden kann, ohne daß er dies weiß, geschweige denn, damit einverstanden ist.

Die Mitteilung der Kommission über illegale und schädliche Inhalte im Internet spricht von einem „ Rechtsgrundsatz der Aufspürbarkeit“. Die Datenschutzbeauftragten halten eine Klarstellung für wünschenswert, was dieser Grundsatz bedeuten soll. Während die Urheber von Inhalten aufspürbar sein sollten, führt die Frage, in welchem Umfang andere Nutzer verfolgbar sein sollten, zu komplexen Problemen und erfordert weitere Untersuchungen. Die Datenschutzbeauftragten schließen aber nicht aus, daß sie sich auf den Standpunkt stellen werden, daß die Privatsphäre der Einzelnen nur dann angemessen geschützt werden kann, wenn ihr Recht auf Anonymität in diesen anderen Fällen gewährleistet ist. Die gegenwärtige Praxis der automatischen und heimlichen Registrierung von Nutzern, die lediglich in den Netzangeboten blättern, lesen oder Informationen aus dem World Wide Web herunterladen, sollte unterbunden werden. Probleme der Usenet Newsgroups müssen unabhängig davon untersucht werden. In jedem Fall ist größere Transparenz hinsichtlich der Sammlung personenbezogener Daten in den Netzen nicht nur entscheidend für den Schutz der Privatsphäre der Nutzer, sondern kann auch ein wichtiges Element der Medienerziehung für Erwachsene und Minderjährige in dem Sinne sein, der im Grünbuch (Kapitel II, Abschnitt 2.3) erwähnt wird.

Die Datenschutzbeauftragten begrüßen die Entschließung des Telekommunikations-Ministerrates vom 28. November 1996, die die Europäische Kommission auffordert, „ die Erforschung von technischen Verfahren zu unterstützen, insbesondere der Filter-Software, der Bewertung, der

Aufspürung und der datenschutzfreundlichen Gestaltung ...". Allerdings würden die Datenschutzbeauftragten es begrüßen, wenn datenschutzfreundliche Technologien in diesem Zusammenhang besonders betont würden. Verfahren der Bewertung sollten in diesem Bereich entwickelt werden, um datenschutzfreundliche Online-Dienste zu fördern. Die Gestaltung und der Einsatz von datenschutzfreundlichen Techniken sollten als wichtige Kriterien in das fünfte Rahmenprogramm für Forschung und technische Entwicklung aufgenommen werden.

Die Datenschutzbeauftragten regen an, daß erwogen werden sollte, einen Vertreter der Datenschutzbeauftragten in eine mögliche Arbeitsgruppe einzubeziehen, die diese Fragen im Zusammenhang mit dem Datenschutz und dem Schutz der Privatsphäre erörtern könnte.

Entschließung der Europäischen Konferenz am 19. September 1997

zum Entwurf der Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation (früher: ISDN-Richtlinie)

- Übersetzung -

Die Europäischen Datenschutzbeauftragten haben bei ihrer Konferenz in Brüssel am 19. September 1997 den gegenwärtigen Stand des Vermittlungsverfahrens zum Entwurf einer Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in öffentlichen digitalen Mobilfunknetzen erörtert.

Die Datenschutzbeauftragten stellen mit Besorgnis fest, daß das Vermittlungsverfahren aufgrund von Kontroversen hinsichtlich gewisser Detailfragen (z. B. Fernmeldegeheimnis; Schutz juristischer Personen; kostenloser Nichteintrag in öffentlichen Teilnehmerverzeichnissen) noch immer nicht abgeschlossen worden ist.

Die Europäischen Datenschutzbeauftragten vertreten mit Nachdruck die Auffassung, daß die Annahme des Richtlinienentwurfs eine notwendige bereichsspezifische Maßnahme für den Datenschutz im Binnenmarkt ist. Mit der vollen Liberalisierung des Telekommunikationsmarktes im Januar 1998 ist ein spezieller Mindeststandard des Datenschutzes in diesem Bereich von entscheidender Bedeutung.

Nach Auffassung der Datenschutzbeauftragten ist die Vertraulichkeit von Daten, die aus der Kommunikation stammen, für den Schutz der Privatsphäre wesentlich, wie dies im Gemeinsamen Standpunkt mit den Änderungen des Europäischen Parlaments zum Ausdruck gekommen ist.

Es ist in höchstem Maße wünschenswert, daß die Richtlinie unter Berücksichtigung dieser Gesichtspunkte in naher Zukunft verabschiedet wird, da die Umsetzungsfrist im Oktober 1998 abläuft. Jede weitere Verzögerung würde die Möglichkeiten einer rechtzeitigen Umsetzung in das Recht der Mitgliedstaaten reduzieren.

Empfehlung der Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten nach Art. 29 der EG-Datenschutzrichtlinie

Empfehlung 1/97

Datenschutzrecht und Medien

angenommen von der Arbeitsgruppe am 25. Februar 1997

Inhalt

1 Einführung

2 Allgemeines
2.1 Freie Meinungsäußerung und Schutz der Privatsphäre
2.2 Rechtlicher Hintergrund des Artikels 9 der Richtlinie
2.3 Überblick über die Rechtslage in den Mitgliedstaaten

3 Ergebnis

Die Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995,

gestützt auf Artikel 29 und Artikel 30 Absatz 3 der Richtlinie,

gestützt auf ihre Geschäftsordnung, insbesondere auf die Artikel 12 und 14

empfiehlt:

1 Einführung

Artikel 9 der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr („Richtlinie") bestimmt folgendes:

„Die Mitgliedstaaten sehen für die Verarbeitung personenbezogener Daten, die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt, Abweichungen und Ausnahmen von diesem Kapitel sowie von den Kapiteln IV und VI nur insofern vor, als sich dies als notwendig erweist, um das Recht auf Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen."

Entsprechend der ihr nach Artikel 30 Absatz 1 Buchstabe a der Richtlinie übertragenen Aufgabe nahm die Datenschutzgruppe in ihrer erster Sitzung die Beratung über die Umsetzung von Artikel 9 auf. Die britische und die deutsche Delegation legten hierzu Arbeitsunterlagen vor. In den Beratungen stellte sich heraus, daß die Anwendung der

Datenschutzbestimmungen im Bereich der Medien in den Mitgliedstaaten derzeit unterschiedlich geregelt ist.

Es wurde festgestellt, daß die Gruppe nützliche Hinweise zur Auslegung von Artikel 9 geben könnte. Zur Vorbereitung sollte das Sekretariat einen Bericht über die gegenwärtige Rechtslage unter Berücksichtigung des Berichts über Datenschutz und Medien des Europarats von 1991 erstellen.

Am 21. Februar 1997 wurde ein von der Gruppe ausgearbeiteter Fragebogen verteilt.

Die Gruppe diskutierte in ihrer dritten Sitzung ein Arbeitspapier und gelangte dabei zu einer Reihe von Schlußfolgerungen, die in der darauf folgenden Sitzung eingehend erörtert wurden. Im Zuge dieser Beratungen wurde vereinbart, das Arbeitspapier in Form einer Empfehlung nach Artikel 30 Absatz 3 der Richtlinie anzunehmen. Die Empfehlung wurde von der Datenschutzgruppe am 25. Februar 1997 angenommen.

Im folgenden wird auf einige allgemeine Aspekte der Anwendung der Datenschutzgesetze in den Medien eingegangen und der rechtliche Hintergrund von Artikel 9 erläutert. In Kapitel 3 wird ein Überblick über die gegenwärtige Rechtslage in den Mitgliedstaaten gegeben. Kapitel 4 enthält die Schlußfolgerungen der Gruppe aus ihren Beratungen über die Anwendung der Datenschutzbestimmungen in den Medien.

Artikel 9 der Richtlinie bestimmt, daß für die Verarbeitung personenbezogener Daten zu journalistischen, künstlerischen oder literarischen Zwecken in bezug auf bestimmte Richtlinienbestimmungen Beschränkungen und Ausnahmen gelten. Die vorliegende Empfehlung konzentriert sich daher auf Ausnahmen und Freistellungen für die Verarbeitung von Daten zu journalistischen Zwecken.

2 Allgemeines

2.1 Freie Meinungsäußerung und Schutz der Privatsphäre

Artikel 10 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) bestimmt in Absatz 1:

„Jeder hat Anspruch auf freie Meinungsäußerung. Dieses Recht schließt die Freiheit zum Empfang und zur Mitteilung von Nachrichten oder Ideen ohne Eingriffe öffentlicher Behörden und ohne Rücksicht auf Landesgrenzen ein."

Dieses Recht gehört zu den wesentlichen Grundrechten, die aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten abgeleitet sind, und ist einer der Wesenszüge des rechtlichen Erbes demokratisch verfaßter Gesellschaften. Historisch gesehen ist das Recht auf freie Meinungsäußerung eines der ersten eingeforderten Menschenrechte, das gesetzlich verankert wurde. Vor allem die Presse erhielt besondere gesetzliche und verfassungsrechtliche Garantien, insbesondere gegen die Vorzensur.

Das Recht auf Privatsphäre wird durch Artikel 8 EMRK gewährleistet. Der in diesem Artikel gewährte Schutz des Privatlebens umfaßt auch den Datenschutz. Ausnahmen von Grundsätzen des Datenschutzes und von Artikel 8 EMRK müssen rechtmäßig und verhältnismäßig sein. Gleiches gilt für Beschränkungen der Meinungsfreiheit, die sich aus der Anwendung datenschutzrechtlicher Grundsätze ergeben können.

Diese beiden Grundrechte dürfen jedoch nicht von vornherein als Kollisionsrechte angesehen werden. Ohne einen ausreichenden Schutz der Privatsphäre würden viele ihre Meinung nicht ohne weiteres zum Ausdruck bringen. Ebenso dürfte die Identifizierung und Klassifizierung von Lesern und Nutzern von Informationsdiensten die Bereitschaft des einzelnen verringern, Informationen entgegenzunehmen und mitzuteilen.

2.2 Rechtlicher Hintergrund des Artikels 9 der Richtlinie

Nach Artikel F Absatz 2 des Vertrags über die Europäische Union hat die Union die Grundrechte zu achten, wie sie durch die EMRK und die gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten gewährleistet sind.

Der Gemeinschaftsgesetzgeber hat die Medien als Sonderfall anerkannt und die Notwendigkeit gesehen, einen Ausgleich zwischen dem Schutz der Privatsphäre und dem Schutz der freien Meinungsäußerung zu schaffen.

Artikel 19 des ursprünglichen Kommissionsvorschlags sah vor, daß die Mitgliedstaaten die Presse und die audiovisuellen Medien von einigen Richtlinienbestimmungen ausnehmen konnten. Aus der Begründung wird deutlich, daß Kernbestimmung dieses Artikels die Pflicht ist, einen Ausgleich zwischen den beteiligten Interessen herzustellen und daß dabei andere verfügbare Hilfsmittel wie das Recht auf Gegendarstellung, ein beruflicher Ehrenkodex, die Schranken der EMRK und allgemeine Rechtsgrundsätze berücksichtigt werden sollten.

In Artikel 9 des geänderten Kommissionsvorschlags wurden dann Ausnahmeregelungen für Medien verbindlich vorgeschrieben. Der Text wurde anschließend erneut geändert, um auch journalistische Tätigkeiten einzubeziehen und die Ausnahmeregelung auf diese Aktivitäten zu beschränken.

Eine weitere Änderung, durch die der Artikel seine jetzige Fassung erhielt, präzisierte die zulässigen Ausnahmen dahingehend, daß sie nicht unterschiedslos für alle Datenschutzbestimmungen gelten sollten. In der jetzigen Fassung sind Ausnahmen zwar verbindlich vorgeschrieben, doch „nur insofern ..., als sich dies als notwendig erweist", um einen Ausgleich zwischen dem Recht auf Privatsphäre und dem Recht auf freie Meinungsäußerung herzustellen. Diese Ausnahmebestimmungen sind zudem beschränkt auf die allgemeinen Bedingungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten, die Übermittlung personenbezogener Daten in Drittländer und Verhaltensregeln für die Kontrollstellen. Ausnahmen von Sicherheitsbestimmungen sind nach Erwägungsgrund 37 nicht zulässig. Außerdem, so heißt es in diesem Erwägungsgrund, sollten die in diesem Bereich zuständigen Kontrollstellen mindestens bestimmte ex post-Zuständigkeiten erhalten, beispielsweise zur regelmäßigen Veröffentlichung eines Berichts oder zur Befassung der Justizbehörden.

2.3 Überblick über die gegenwärtige Rechtslage in den Mitgliedstaaten

In den Rechtsordnungen der Mitgliedstaaten werden gegenwärtig folgende Ansätze verfolgt:

a) In einigen Fällen enthalten Datenschutzbestimmungen keine ausdrückliche Ausnahme für den Bereich der Medien. Dies gilt für Belgien, Spanien, Portugal, Schweden und das Vereinigte Königreich.

b) In Deutschland, Frankreich, den Niederlanden, Österreich und Finnland sind Medien von bestimmten Datenschutzbestimmungen ausgenommen. Ähnliche Ausnahmeregelungen sind in einem italienischen Gesetzentwurf vorgesehen.

c) In anderen Ländern sind Medien von den allgemeinen Datenschutzvorschriften freigestellt und unterliegen Sonderregeln. In Dänemark gilt dies für alle Medien, in Deutschland nur für die öffentlichen Rundfunkanstalten, die nicht den Datenschutzgesetzen der Länder oder des Bundes unterliegen, sondern besonderen Bestimmungen in den von den Ländern geschlossenen Staatsverträgen.

Die Unterschiede zwischen diesen drei Modellen sollten allerdings nicht überbewertet werden. In den meisten Fällen werden Datenschutzbestimmungen - unabhängig davon, ob es ausdrückliche Ausnahmeregelungen gibt - schon wegen des in der Verfassung verankerten Rechts auf freie Meinungsäußerung und Pressefreiheit auf Medien nicht in vollem Umfang angewandt. Diese Grundrechte bilden de facto eine Schranke für die Anwendung des materiellen Datenschutzrechts oder zumindest für dessen Durchsetzung.

Der normale Datenschutz gilt allerdings im allgemeinen für alle Medien-Aktivitäten. Hiervon ausgenommen sind nur die Print-Medien.

Die für den Datenschutz zuständigen Kontrollstellen tragen bei der Anwendung des Datenschutzrechts der Besonderheit der einzelnen Medien Rechnung, unabhängig davon, ob Sonderregelungen bestehen oder nicht.

Die tatsächliche Reichweite der Ausnahmeregelungen läßt sich nicht abstrakt bestimmen, sondern hängt von der Gesamtstruktur des Datenschutzrechts in jedem einzelnen Land ab. In welchem Umfang Ausnahmen erforderlich sind, bestimmt sich danach, wie weit sich das materielle Datenschutzrecht effektiv auf die Aktivitäten der Medien auswirkt.

Die Unterschiede in der Anwendung des Datenschutzrechts in bezug auf die einzelnen Medien lassen sich auch aus einer anderen Perspektive erklären, nämlich ausgehend von der Funktion des Datenschutzrechts und der Verwendung der Informationstechnologie durch die Medien. In den Anfängen des Datenschutzes konzentrierte sich die Aufmerksamkeit auf große zentrale Datenbanken. Medien schienen damals von solchen Bestimmungen kaum betroffen zu sein, so daß Ausnahmeregelungen auch nicht notwendig erschienen. Die Verlagerung des Schwerpunkts im Datenschutzrecht auf den Begriff der Datenverarbeitung und die umfassende Nutzung der Informationstechnologie durch die Medien haben die Situation grundlegend verändert.

Die in den Mitgliedstaaten geltenden Regelungen weisen übereinstimmend eine wichtige Bestimmung auf, der zufolge die Medien - oder zumindest die Presse - gewisse Vorschriften beachten müssen, die zwar nicht zum Datenschutz im eigentlichen Sinne gehören, aber zum Schutz der Privatsphäre des einzelnen beitragen. Diese Bestimmungen und eine häufig umfassende Rechtsprechung bieten eine besondere Form des Rechtschutzes, der mitunter als Ersatz für den fehlenden präventiven Rechtsschutz im Datenschutzrecht angesehen wird.

Will man beurteilen, wie die Privatsphäre in bezug auf die Medien geschützt wird, so muß man folgende Schutzmechanismen berücksichtigen: das Recht auf Gegendarstellung und die Möglichkeit, falsche Darstellungen zu berichtigen, die Berufspflichten der Journalisten und die damit verbundene Selbstkontrolle sowie die Bestimmungen zum Schutz der Ehre (straf- und zivilrechtliche Regelungen zum Schutz vor Verleumdung usw.).

Die Hinwendung der traditionellen Medien zu elektronischer Veröffentlichung und Online-Diensten gibt weiteren Grund zum Nachdenken. Mit den Online-Diensten gewinnt die Unterscheidung zwischen redaktioneller Tätigkeit und nichtredaktioneller Tätigkeit eine neue Dimension, da sich bei Online-Diensten anders als bei den herkömmlichen Medien

die Identität der Empfänger der Dienste feststellen läßt.

3 Ergebnis

Aus dem Vorstehenden dürfte deutlich geworden sein, daß der Rechtsrahmen in den Mitgliedstaaten für die Anwendung des Datenschutzrechts im Bereich der Medien einer generellen Überprüfung bedarf. Insbesondere muß geprüft werden, in welchem Umfang die Anwendung der einzelnen Bestimmungen in den Kapiteln II, IV und VI der Richtlinie zum Schutz der freien Meinungsäußerung eingeschränkt werden muß.

Dabei ist folgendes zu berücksichtigen:

- Grundsätzlich ist das Datenschutzrecht auf Medien anwendbar. Ausnahmen und Freistellungen können nur in bezug auf Kapitel II über die allgemeinen Bedingungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten, Kapitel IV über die Übermittlung personenbezogener Daten in Drittländer und Kapitel VI über die Befugnisse der Kontrollstellen gewährt werden. Die Sicherheitsbestimmungen sind hiervon ausgenommen. Die Kontrollstellen müssen in jedem Fall gewisse Befugnisse für nachträgliche Kontrollen behalten.

- Ausnahmen und Freistellungen nach Maßgabe von Artikel 9 müssen verhältnismäßig sein. Sie dürfen nur in bezug auf Bestimmungen gewährt werden, die die freie Meinungsäußerung beeinträchtigen könnten, und nur soweit dies für die tatsächliche Ausübung dieses Rechts erforderlich ist; dabei ist das Recht auf Privatsphäre der betroffenen Person angemessen zu wahren.

- Ausnahmen und Freistellungen nach Artikel 9 sind unter Umständen nicht erforderlich, wenn die diversen Richtlinienbestimmungen oder die Ausnahmen auf der Grundlage anderer Spezialvorschriften (die selbstverständlich eng auszulegen sind) hinreichend flexibel sind, um einen zufriedenstellenden Ausgleich zwischen dem Recht auf Privatsphäre und dem Recht auf freie Meinungsäußerung zu gewährleisten.

- Artikel 9 der Richtlinie wahrt das Recht des einzelnen auf freie Meinungsäußerung. Ausnahmen und Freistellungen von Artikel 9 können nicht den Medien oder Journalisten als solchen gewährt werden, sondern nur für die Verarbeitung personenbezogener Daten zu journalistischen Zwecken.

- Ausnahmen und Freistellungen gelten nur für die Verarbeitung personenbezogener Daten zu journalistischen (redaktionellen) Zwecken einschließlich der elektronischen Veröffentlichung. Jede andere Form der Datenverarbeitung durch Journalisten oder Medien unterliegt den allgemeinen Richtlinienbestimmungen. Diese Differenzierung ist vor allem für die elektronische Veröffentlichung relevant. Die Verarbeitung personenbezogener Daten von Abonnenten zu Fakturierungszwecken oder für das Direktmarketing (einschließlich der Verarbeitung von Daten über die Inanspruchnahme der Medien zur Erstellung von Verbraucherprofilen) fällt unter den allgemeinen Datenschutz.

- Die Richtlinie verlangt einen Ausgleich zwischen zwei Grundrechten. Um feststellen zu können, ob die Beschränkungen der Rechte und Pflichten aus der Richtlinie im Verhältnis zu dem angestrebten Schutz der freien Meinungsäußerung stehen, muß den speziellen Garantien, über die der einzelne gegenüber den Medien verfügt, besonders Rechnung getragen werden. Beschränkungen des Rechts auf Zugang zu Informationen und auf Berichtigung vor der Veröffentlichung sind nur dann verhältnismäßig, wenn der einzelne nach der Veröffentlichung zur Gegendarstellung und Richtigstellung falscher Informationen berechtigt ist.

- In jedem Fall hat der einzelne bei Verletzung der ihm zustehenden Rechte Anspruch auf einen angemessenen Rechtsschutz.

- Bei der Prüfung, ob Ausnahmen oder Freistellungen verhältnismäßig sind, sind die bestehenden ethischen und beruflichen Pflichten der Journalisten sowie die vom Berufsstand selbst organisierte Aufsicht zu berücksichtigen.

Geschehen zu Brüssel, den 25. Februar 1997.

Im Namen der Datenschutzgruppe

Der Vorsitzende P.J. Hustinx

Erste Leitlinie für die Übermittlung personenbezogener Daten in Drittländer - Mögliche Ansätze für die Bewertung der Angemessenheit

Von der Arbeitsgruppe am 26. Juni 1997 angenommene Diskussionsgrundlage

Inhalt

1 Einführung

2 Verfahrensfragen
2.1 Weiße Listen
2.2 Risikoanalyse spezifischer Übermittlungen

3 Was bedeutet „angemessener Schutz"
3.1 Inhaltliche Grundsätze
3.2 Verfahrens- und Durchführungsmechanismen

4 Praktische Anwendung in der Theorie
4.1 Länder, die das Übereinkommen Nr.108 des Europarats ratifiziert haben
4.2 Sonstige Fälle

1 Einführung

Mit diesem Dokument wird nicht das Ziel verfolgt, auf alle Fragen einzugehen, die sich aus der Richtlinie im Zusammenhang mit der Übermittlung personenbezogener Daten in Drittländer ergeben; hier steht das Bemühen im Vordergrund, die zentrale Frage der Beurteilung der Angemessenheit im Sinne von Artikel 25 Absätze 1 und 2 zu klären. Ausnahmen vom Erfordernis des „angemessenen Schutzniveaus" nach Artikel 26 Absatz 1 werden hier überhaupt nicht behandelt. Es wird davon ausgegangen, daß diese Ausnahmen recht eng definiert sind und wahrscheinlich viele Fälle nicht in ihren Anwendungsbereich fallen und somit auf die Angemessenheit geprüft werden. Die Arbeitsgruppe wird den konkreten Anwendungsbereich dieser Ausnahmen bei ihren künftigen Arbeiten prüfen.

Es sollte nicht vergessen werden, daß der Begriff *angemessen* auch in Artikel 26 Absatz 2 verwendet wird, der die Möglichkeit von ad-hoc-Lösungen - insbesondere vertraglicher Art - für Situationen vorsieht, in denen kein angemessener Schutz im Sinne von Artikel 25 Absatz 2 gewährleistet ist. Verfahrensrechtlich behandelt die Richtlinie diese Fälle allerdings sehr unterschiedlich. Während die Mitgliedstaaten nach Artikel 25 einander und die Kommission über die Fälle zu unterrichten haben, in denen kein angemessenes Schutzniveau gewährleistet ist und die Übermittlung deshalb blockiert wurde, ist die Situation nach Artikel 26 umgekehrt: Die Mitgliedstaaten sind verpflichtet, die Kommission und die übrigen Mitgliedstaaten über jede erteilte Genehmigung zu unterrichten. Dies spiegelt die Tatsache wider, daß es bei derartigen vertraglichen Lösungen inhärente Probleme gibt, wie die Schwierigkeiten einer betroffenen Person, ihre Rechte aus einem Vertrag, bei dem sie selbst nicht Vertragspartei ist, durchzusetzen, und daß sie deshalb nur in einigen spezifischen und wahrscheinlich relativ seltenen Situationen geeignet sind. Die Arbeitsgruppe wird die Umstände gesondert prüfen, unter denen vertragliche ad-hoc-Lösungen geeignet sein können, und bei den künftigen Arbeiten einige Grundsätze im Hinblick

auf die mögliche Form und den möglichen Inhalt derartiger Lösungen ausarbeiten. Diese Arbeit wird wahrscheinlich weitgehend auf den in diesem Dokument enthaltenen Ideen aufbauen, da eine Prüfung der Angemessenheit sowohl Gegenstand des Artikels 26 Absatz 2 als auch des Artikels 25 Absätze 1 und 2 ist.

2 Verfahrensfragen

Artikel 25 sieht vor, daß die Angemessenheit bei den einzelnen Übermittlungen oder Kategorien von Übermittlungen geprüft wird. Aufgrund der hohen Anzahl von Übermittlungen personenbezogener Daten, die täglich die Gemeinschaft verlassen, und aufgrund der vielen an solchen Übermittlungen beteiligten Wirtschaftskräfte, kann aber natürlich kein Mitgliedstaat - unabhängig von dem System, das er zur Anwendung von Artikel 25 wählt - sicherstellen, daß absolut jeder Fall im Detail geprüft wird. Dies heißt freilich nicht, daß kein Fall detailliert geprüft wird, sondern eher, daß Mechanismen entwickelt werden müssen, um den Beschlußfassungsprozeß für eine ganze Reihe von Fällen zu rationalisieren, die somit Entscheidungen, oder zumindest vorläufige Entscheidungen ohne allzu große Schwierigkeiten oder übermäßige materielle Folgen ermöglichen. Eine derartige Rationalisierung ist unabhängig davon erforderlich, wer die Entscheidung trifft, ob sie bei dem für die Verarbeitung Verantwortlichen, der Kontrollbehörde oder irgendeinem anderen durch das Verfahren des Mitgliedstaats eingesetzten Gremium liegt.

2.1 Weiße Listen

Für eine solche Rationalisierung bietet sich die Ausarbeitung „Weißer Listen" von Drittländern an, von denen angenommen werden kann, daß sie ein angemessenes Schutzniveau gewährleisten. Eine derartige Liste könnte „provisorischen Charakter" haben oder „nur zur Orientierung" dienen und somit Einzelfälle, bei denen es besondere Schwierigkeiten geben könnte, nicht berühren. Nichtsdestoweniger ist es in der Logik des allgemeinen Ansatzes von Artikel 25 wichtig, jede Entscheidung über die Aufnahme eines Landes in eine weiße Liste eher auf Einzelfälle zu stützen als auf eine vereinfachte, abstrakte Beurteilung eines Rechtstextes. Wenn nach der Prüfung einiger repräsentativer Fälle von Übermittlungen in ein Drittland bei jedem dieser Fälle der gebotene Schutz als angemessen angesehen wurde, könnte das betreffende Land in die „weiße Liste" aufgenommen werden.

Ein Problem bei diesem Ansatz besteht darin, daß viele Drittländer keinen einheitlichen Schutz für alle Wirtschaftsbereiche bieten. Beispielsweise gibt es in vielen Ländern Datenschutzgesetze für den öffentlichen Bereich, nicht aber für den Privatsektor. In den Vereinigten Staaten ist die Lage insofern noch komplexer, als spezifische Rechtsvorschriften für bestimmte Einzelbereiche wie Kreditauskunft und Aufzeichnung über den Videoverleih, nicht aber für andere bestehen. Ein zusätzliches Problem gibt es in Ländern mit Bundesverfassungen wie den Vereinigten Staaten und Kanada, in denen oft Schwierigkeiten zwischen den verschiedenen Teilen des Bundes bestehen. Deshalb ist bei dem Beschluß darüber, ob der gewährte Schutz bei einer speziellen Datenübermittlung für das gesamte Land oder lediglich einen einzelnen Sektor oder Staat repräsentativ ist, sehr sorgfältig vorzugehen. Nichts steht einer teilweisen Aufnahme eines Drittlands auf eine weiße Liste entgegen und natürlich wird bei Übermittlungen von Daten aus Spanien nach dem geltenden nationalen Recht zwischen Ländern, die einen Schutz über die Grenzen hinaus gewährleisten, und Ländern unterschieden, die nur im öffentlichen Bereich Schutz gewährleisten.

Ferner stellt sich die Frage, wer über die Aufnahme in eine derartige Liste entscheiden sollte. Dazu ist anzumerken, daß die durch Artikel 29 eingesetzte Gruppe bei der Beschlußfassung über einzelne Datenübermittlungen keine explizite Rolle zu spielen hat. Diese Rolle fällt in erster Linie den Mitgliedstaaten zu und dann der Kommission nach dem in Artikel 31 festgelegten Ausschußverfahren. Wie oben ausgeführt wurde, zielt allerdings jegliche Arbeit der Gruppe darauf ab,

Orientierungen für eine Vielzahl von Fällen zu liefern, und nicht notwendigerweise für die Bestimmung eines Einzelfalls. Es sei auch darauf hingewiesen, daß eine der spezifischen Aufgaben der durch Artikel 29 eingesetzten Gruppe darin besteht, der Kommission eine Stellungnahme über das Schutzniveau in Drittländern zu übermitteln. Somit fällt eine Prüfung der Lage in einzelnen Drittländern im Lichte einiger Einzelfälle und eine vorläufige Stellungnahme zur Angemessenheit des Schutzes sehr wohl in den Aufgabenbereich der durch Artikel 29 eingesetzten Gruppe. Derartige positive Entscheidungen könnten in die geplante weiße Liste einbezogen werden. Diese könnte anschließend breit verteilt und von den für die Datenverarbeitung Verantwortlichen, den Kontrollbehörden und den Mitgliedstaaten als Hilfe für deren eigene Entscheidungen verteilt werden.

Steht ein Land nicht auf einer solchen weißen Liste, so heißt dies nicht notwendigerweise, daß das Land auf eine schwarze Liste gehört, sondern eher, daß es noch keine allgemeinen Leitlinien für dieses Land gibt. Die Erstellung einer expliziten schwarzen Liste von Ländern wäre - auch für Orientierungszwecke - politisch sehr heikel.

2.2 Risikoanalyse spezifischer Übermittlungen

Auch wenn die Erstellung einer vorläufigen weißen Liste von Drittländern eine wertvolle Hilfe für die Entscheidungen bei vielen Datenübermittlungen darstellt, wird das betreffende Drittland immer noch in vielen Fällen nicht auf der weißen Liste aufgeführt sein. Die Mitgliedstaaten können mit diesen Fällen je nach ihrer Umsetzung des Artikels 25 in ihre innerstaatlichen Rechtsvorschriften recht unterschiedlich umgehen. Wenn die Kontrollstelle eine spezifische Rolle bei der vorherigen Genehmigung von Datenübermittlungen oder bei einer nachträglichen Überprüfung spielen soll, dann kann allein schon das Volumen der betroffenen Übermittlungen ein System für die Prioritätensetzung bei den Bemühungen der Kontrollstelle erforderlich machen. Ein solches System wäre in Form eines Pakets vereinbarter Kriterien denkbar, die es ermöglichen würden, eine spezielle Übermittlung oder Kategorie von Übermittlungen als besondere Gefahr für die Privatsphäre einzustufen.

Ein solches System ändert nichts an der Verpflichtung jedes Mitgliedstaats, sicherzustellen, daß nur die Übermittlungen erfolgen, bei denen das Drittland ein angemessenes Schutzniveau gewährleistet. Die Tatsache, daß eine Übermittlung keine besondere Gefahr darstellt, berührt das Grunderfordernis des Artikels 25 im Hinblick auf den sicherzustellenden angemessenen Schutz nicht. Allerdings wird die Bewertung des Risikos für die betroffene Person aufgrund der Übermittlung eine nützliche Unterstützung für die konkrete Bestimmung dessen darstellen, was als „angemessener Schutz" angesehen wird. Das System wird auch als Orientierung für Fälle von Datenübermittlungen dienen, die als „vorrangige Fälle" anzusehen sind und geprüft oder in denen sogar Ermittlungen angestellt werden müssen; damit wird es ermöglichen, daß die für die „Überwachung" des Systems eingesetzten Ressourcen direkt auf die Übermittlungen gerichtet werden, die im Hinblick auf den Schutz der betroffenen Personen zu größter Besorgnis Anlaß geben.

Die Arbeitsgruppe wird ein spezifisches, detailliertes Dokument zu den Kategorien von Übermittlungen erstellen, die ihres Erachtens besondere Gefahren für die Privatsphäre mit sich bringen. Dazu werden wahrscheinlich folgende Kategorien gehören:

- Übermittlungen, die bestimmte sensible Datenkategorien gemäß der Definition von Artikel 8 der Richtlinie betreffen;

- Übermittlungen mit dem Risiko finanzieller Verluste (beispielsweise Kreditkartenzahlungen über Internet);

- Übermittlungen, die eine Gefahr für die persönliche Sicherheit darstellen;

- Übermittlungen zum Zwecke einer Beschlußfassung mit großer Bedeutung für die betroffene Person (wie Einstellungs- oder Beförderungsbeschlüsse, Gewährung von Krediten usw.);

- Übermittlungen, die die Gefahr ernsthafter Schwierigkeiten oder der Beeinträchtigung des Rufs einer natürlichen Person nach sich ziehen;

- Übermittlungen, die zu spezifischen Maßnahmen führen können, die eine bedeutende Einmischung in das Privatleben einer natürlichen Person darstellen, wie ungewünschte Telefonanrufe;

- repetitive Übermittlungen großer Datenmengen (wie über Telekommunikationsnetze, Internet usw. verarbeitete elektronische Daten);

- Übermittlungen, die die Erfassung von Daten in einer besonderen verdeckten oder geheimen Form betreffen (beispielsweise „Internet-cookies", eine Art elektronischer Visitenkarte).

3 Was bedeutet „angemessener Schutz"?

Ziel des Datenschutzes ist es, der natürlichen Person Schutz zu gewähren, deren Daten verarbeitet werden. Dies wird üblicherweise über ein Zusammenspiel der Rechte der betroffenen Person sowie der Pflichten derer erreicht, die Daten verarbeiten oder Kontrolle über eine derartige Verarbeitung ausüben. Die in der Richtlinie 95/46/EG niedergelegten Rechte und Pflichten stützen sich auf die in dem Übereinkommen des Europarats Nr. 108 (1981) enthaltenen Rechte und Pflichten, die sich ihrerseits nicht sehr von den in den OECD-Leitlinien (1980) oder den Leitlinien der Vereinten Nationen (1990) festgelegten unterscheiden. Über den Inhalt der Datenschutzbestimmungen, die für die fünfzehn Staaten der Gemeinschaft gelten, besteht somit ein Konsens.

Die Datenschutzbestimmungen tragen allerdings lediglich zum Schutz natürlicher Personen bei, wenn sie in der Praxis befolgt werden. Deshalb muß nicht nur der Inhalt der Bestimmungen geprüft werden, die für in ein Drittland übertragene personenbezogene Daten gelten, sondern auch die für die Gewährleistung der Wirksamkeit derartiger Vorschriften existierenden Mechanismen. In Europa wurden die Vorschriften für den Datenschutz herkömmlicherweise in Form von Gesetzen verankert, womit eine Sanktionsmöglichkeit bei Nichtbefolgung entstand und natürlichen Personen ein Regreßrecht eingeräumt wurde. Darüber hinaus sahen solche Gesetze im allgemeinen zusätzliche Verfahrensmechanismen vor, wie die Einrichtung von Aufsichtsbehörden mit Überwachungs- und Beschwerdeprüfungsfunktionen. Diese Verfahrensaspekte finden sich in der Richtlinie 95/46/EG mit ihren Bestimmungen für Haftung, Sanktionen, Rechtsbehelfe, Kontrollstellen und Meldung wieder. Außerhalb der Gemeinschaft sind allerdings derartige Verfahrensmittel weniger verbreitet, die sicherstellen sollen, daß die Vorschriften für den Datenschutz erfüllt werden. Die Vertragsparteien des Übereinkommens Nr. 108 sind aufgerufen, die Grundsätze des Datenschutzes in ihre Rechtsvorschriften aufzunehmen, zusätzliche Mechanismen wie eine Kontrollbehörde werden hier aber nicht gefordert. Die OECD-Leitlinien enthalten lediglich das Erfordernis, daß sie in den inländischen Rechtsvorschriften „zu berücksichtigen" sind und garantieren somit auf der Verfahrensebene keineswegs, daß sichergestellt wird, daß die Leitlinien tatsächlich in einen wirksamen Schutz natürlicher Personen münden. Die später festgelegten VN-Leitlinien enthalten allerdings Bestimmungen für Überwachung und Sanktionen, womit das wachsende Bewußtsein der Notwendigkeit deutlich wird, weltweit dafür zu sorgen, daß die Datenschutzvorschriften gebührend durchgesetzt werden.

Vor diesem Hintergrund ist klar, daß jede sinnvolle Analyse eines angemessenen Schutzes zwei Grundelemente umfassen

muß: den Inhalt der anzuwendenden Vorschriften und die Mittel für die Gewährleistung ihrer tatsächlichen Anwendung.

Mit der Richtlinie 95/46/EG als Ausgangspunkt und unter Berücksichtigung der Vorschriften der übrigen internationalen Texte zum Datenschutz sollte es möglich sein, zu einem „festen Kern" „inhaltlicher" Datenschutzgrundsätze und „Verfahrens-/Durchsetzungs"-Erfordernisse zu kommen, dessen Einhaltung als Mindesterfordernis für einen als angemessen anzusehenden Schutz bewertet werden könnte. Eine solche Minimalliste sollte keine starre Liste sein. In einigen Fällen wird es notwendig sein, die Liste zu erweitern, während es in anderen auch möglich sein kann, das Verzeichnis der Erfordernisse zu reduzieren. Das Ausmaß des Risikos einer Übermittlung für die betroffene Person, wird ein bedeutender Faktor für die Bestimmung der konkreten Erfordernisse in einem Einzelfall sein. Trotz dieses Vorbehalts ist die Zusammenstellung einer Basisliste minimaler Voraussetzungen ein nützlicher Ausgangspunkt für jede Analyse.

3.1 Inhaltliche Grundsätze

Die Aufnahme der nachstehenden Grundsätze wird vorgeschlagen:

1. **Der Grundsatz der Beschränkung der Zweckbestimmung** - Daten sind für einen spezifischen Zweck zu verarbeiten und dementsprechend nur insofern zu verwenden oder weiter zu übermitteln, als dies mit der Zweckbestimmung der Übermittlung nicht unvereinbar ist. Die einzigen Ausnahmen von dieser Regel sind die in einer demokratischen Gesellschaft aus einem der in Artikel 13 der Richtlinie aufgeführten Gründe notwendigen Fälle.

2. **Der Grundsatz der Datenqualität und -verhältnismäßigkeit** - Daten müssen sachlich richtig und, wenn nötig auf dem neusten Stand sein. Die Daten müssen angemessen, relevant und im Hinblick auf die Zweckbestimmung, für die sie übertragen oder weiter verarbeitet werden, nicht exzessiv sein.

3. **Der Grundsatz der Transparenz** - Natürliche Personen müssen Informationen über die Zweckbestimmung der Verarbeitung und die Identität des im Drittland für die Verarbeitung Verantwortlichen sowie andere Informationen erhalten, sofern dies aus Billigkeitsgründen erforderlich ist. Ausnahmen sind lediglich im Einklang mit den Artikeln 11 Absatz 2 und 13 der Richtlinie möglich.

4. **Der Grundsatz der Sicherheit** - Der für die Verarbeitung Verantwortliche hat geeignete technische und organisatorische Sicherheitsmaßnahmen für die Risiken der Verarbeitung zu treffen. Alle unter der Verantwortung des für die Verarbeitung Verantwortlichen tätigen Personen, darunter auch Verarbeiter, dürfen Daten nur auf Anweisung des für die Verarbeitung Verantwortlichen verarbeiten.

5. **Die Rechte auf Zugriff, Berichtigung und Widerspruch** - Die betroffene Person muß das Recht haben, eine Kopie aller sie betreffender Daten zu erhalten, die verarbeitet werden, sowie das Recht auf Berichtigung dieser Daten, wenn diese sich als unrichtig erweisen. In bestimmten Situationen muß sie auch Widerspruch gegen die Verarbeitung der sie betreffenden Daten einlegen können. Die einzigen Ausnahmen von diesen Rechten haben mit Artikel 13 der Richtlinie im Einklang zu stehen.

6. **Beschränkungen der Weiterübermittlung an andere Drittländer** - Weitere Übermittlungen personenbezogener Daten vom Bestimmungsdrittland in ein anderes Drittland sind lediglich zulässig, wenn das zweite Drittland ebenfalls ein angemessenes Schutzniveau aufweist. Die einzigen zulässigen Ausnahmen haben mit Artikel 26 der Richtlinie im Einklang zu stehen.

Beispiele weiterer, auf spezifische Arten der Verarbeitung anwendbarer Grundsätze:

1. **Sensible Daten** - Sind „sensible" Kategorien von Daten betroffen (die in Artikel 8 aufgelistet sind), so haben zusätzliche Sicherheitsmaßnahmen wie das Erfordernis zu gelten, daß die betroffene Person ausdrücklich in die Verarbeitung einwilligt.

2. **Direktmarketing** - Werden Daten zum Zwecke des Direktmarketings übermittelt, so muß die betroffene Person die Möglichkeit haben, sich jederzeit gegen die Verwendung ihrer Daten für derartige Zwecke zu verwehren.

3. **Automatisierte Einzelentscheidung** - Erfolgt die Übermittlung mit dem Ziel, eine automatisierte Einzelentscheidung im Sinne von Artikel 15 der Richtlinie zu treffen, so muß die natürliche Person das Recht haben, die dieser Entscheidung zugrunde liegende Logik zu erfahren, und andere Maßnahmen müssen getroffen werden, um die berechtigten Interessen der natürlichen Person zu schützen.

3.2 Verfahrens- / Durchführungsmechanismen

In Europa herrscht breite Übereinstimmung darüber, daß die Datenschutzgrundsätze in Rechtsvorschriften eingebettet werden sollen. Man ist sich auch weitgehend darüber einig, daß ein System „externer Überwachung" in Form einer unabhängigen Behörde ein notwendiges Merkmal eines Datenschutzkontrollsystems darstellt. Es reicht allerdings nicht aus, ohne jede Begründung oder Rechtfertigung lediglich zu erklären, daß diese beiden Merkmale für einen angemessenen Schutz gewissermaßen inhärent erforderlich sind. Dies hieße, lediglich rein formalistische Kriterien für die Beurteilung dieser Frage vorzubringen.

Ein besserer Ausgangspunkt wäre die Identifizierung der Basisziele des verfahrensrechtlichen Systems beim Datenschutz und auf dieser Grundlage die Beurteilung des Spektrums der einzelnen, in Drittländern verwendeten gerichtlichen und außergerichtlichen Verfahrensmechanismen im Hinblick auf ihre Fähigkeit, diese Ziele zu erfüllen.

Ein Datenschutzsystem verfolgt im wesentlichen dreierlei Ziele:

1. **Gute Befolgungsrate** der Bestimmungen. (Kein System kann 100 %ige Einhaltung garantieren, einige sind aber besser als andere). Ein gutes System zeichnet sich im allgemeinen dadurch aus, daß sich die für die Verarbeitung Verantwortlichen ihrer Pflichten und die betroffenen Personen ihrer Rechte und der Mittel für deren Durchsetzung sehr stark bewußt sind. Die Existenz wirksamer, dissuasiver Sanktionen ist wichtig, um die Einhaltung der Bestimmungen sicherzustellen; ebenso wichtig sind natürlich Systeme der direkten Überprüfung durch Behörden, Buchprüfer oder unabhängige Datenschutzbeauftragte.

2. **Unterstützung und Hilfe für einzelne betroffene Personen** bei der Wahrnehmung ihrer Rechte. Jeder Einzelne muß seine Rechte rasch und wirksam ohne zu hohe Kosten durchsetzen können. Dazu muß es einen institutionellen Mechanismus geben, der eine unabhängige Prüfung von Beschwerden ermöglicht.

3. **Angemessene Entschädigung** für die geschädigte Partei, wenn die Bestimmungen nicht eingehalten werden. Für dieses Schlüsselelement muß es ein System unabhängiger Schlichtung geben, das die Zahlung einer Entschädigung und gegebenfalls die Auferlegung von Sanktionen ermöglicht.

4 Praktische Anwendung der Theorie

4.1 Länder, die das Übereinkommen Nr. 108 des Europarats ratifiziert haben

Neben der Richtlinie ist das Übereinkommen Nr. 108 im Datenschutzbereich das einzige existierende Instrument des internationalen Rechts. Die meisten Vertragsparteien des Übereinkommens sind auch Mitgliedstaaten der Europäischen Union (alle 15 haben das Übereinkommen jetzt ratifiziert) oder Länder, wie Norwegen und Island, die aufgrund des Abkommens über den Europäischen Wirtschaftsraum durch die Richtlinie gebunden sind. Allerdings hat auch Slowenien das Übereinkommen ratifiziert, und drei andere Länder, darunter die Schweiz, werden die Ratifizierung möglicherweise in naher Zukunft vornehmen. Deshalb ist nicht nur aus rein akademischem Interesse zu prüfen, ob bei den Ländern, die das Übereinkommen ratifiziert haben, davon auszugehen ist, daß sie ein angemessenes Schutzniveau im Sinne von Artikel 25 der Richtlinie bieten.

Eine solche Prüfung sollte - wie in Abschnitt 2 dieses Dokuments ausgeführt wurde - durch das Betrachten einer Reihe spezifischer Fälle erfolgen. Als Ausgangspunkt ist es allerdings sinnvoll, den Wortlaut des Übereinkommens selbst im Lichte der in dem vorigen Abschnitt dieses Dokuments dargelegten theoretischen Darstellung des „angemessenen Schutzes“ zu prüfen.

Im Hinblick auf den Inhalt der Grundsätze läßt sich sagen, daß das Übereinkommen die ersten fünf der sechs „Minimalbedingungen“ einbezieht. Das Übereinkommen enthält auch das Erfordernis geeigneter Schutzmaßnahmen für sensible Daten, das bei derartigen Daten eine Voraussetzung für die Angemessenheit darstellen sollte.

Beim Inhalt der substantiellen Regeln fehlen in dem Übereinkommen Beschränkungen von Übermittlungen in Länder, die nicht Vertragsparteien des Übereinkommens sind. Damit entsteht die Gefahr, daß ein Mitgliedstaat des Übereinkommens Nr. 108 bei einer Datenübermittlung aus der Gemeinschaft in ein weiteres Drittland mit völlig unzureichendem Schutzniveau als Zwischenstation verwendet wird.

Der zweite Aspekt des „angemessenen Schutzes“ betrifft die vorhandenen Mechanismen, die sicherstellen, daß die Grundsätze Wirkung erhalten. Das Übereinkommen legt fest, daß seine Grundsätze in inländische Rechtsvorschriften aufgenommen und geeignete Sanktionen und Rechtsmittel für Verstöße gegen diese Grundsätze eingeführt werden. Dies sollte ausreichen, um eine angemessene Befolgung der Regeln sowie geeignete Rechtsmittel für die betroffenen Personen zu gewährleisten, wenn die Regeln nicht eingehalten werden (Ziele (1) und (3) eines Datenschutzkontrollsystems). Das Übereinkommen verpflichtet allerdings die Vertragsparteien nicht, institutionelle Mechanismen zu schaffen, die eine unabhängige Prüfung von Beschwerden ermöglichen, obschon in der Praxis die Länder, die das Übereinkommen ratifiziert haben, im allgemeinen derartige Mechanismen eingeführt haben. Dies stellt insofern einen Schwachpunkt dar, als ohne derartige geeignete institutionelle Mechanismen die Unterstützung und Hilfe für einzelne betroffene Personen bei der Wahrnehmung ihrer Rechte (Ziel 2) unter Umständen nicht gewährleistet ist.

Diese Kurzanalyse scheint zu ergeben, daß bei Übermittlungen personenbezogener Daten in Länder, die das Übereinkommen Nr.108 ratifiziert haben, davon ausgegangen werden kann, daß sie unter folgenden Voraussetzungen nach Artikel 25 Absatz 1 der Richtlinie zulässig sind:

- Das betreffende Land verfügt auch über geeignete institutionelle Mechanismen wie eine unabhängige Kontrollstelle

mit entsprechenden Befugnissen; und

- das betreffende Land ist die Endbestimmung der Übermittlung und nicht eine Zwischenstation, über die die Daten weiterübermittelt werden.

Hier handelt es sich natürlich um eine eher vereinfachte, oberflächliche Prüfung des Übereinkommens. Spezifische Fälle der Datenübermittlung in Länder des Übereinkommens können neue, in diesem Dokument nicht betrachtete Probleme aufwerfen.

4.2 Sonstige Fälle

Die große Mehrheit der Datenübermittlungen aus der Europäischen Union erfolgt eindeutig in Drittländer, die das Übereinkommen Nr. 108 nicht ratifiziert haben. In diesen Fällen, in denen kein bindendes Instrument des internationalen Rechts Anwendung findet, gibt es keine Alternative; hier muß auf den Grundansatz dieses Papiers zurückgegriffen werden, d.h. es müssen Schlußfolgerungen über die Angemessenheit des in einem Drittland gebotenen Schutzniveaus auf der Grundlage der Situation in einem oder mehreren spezifischen Fällen gezogen werden. Eine Beurteilung einer spezifischen Datenübermittlung kann bisweilen für breite Kategorien analoger Fälle als richtig angesehen werden. Die Analyse derartiger, in hohem Maße repräsentativer Übermittlungen wird die Erstellung einer vorläufigen weißen Liste von Ländern oder Sektoren innerhalb von Ländern erleichtern.

Drei Arten von Übermittlungen wären nach der Richtlinie möglich:

1. Eine Mitteilung personenbezogener Daten durch einen in der Gemeinschaft niedergelassenen, für die Verarbeitung Verantwortlichen an einen anderen, in einem Drittland niedergelassenen, für die Verarbeitung Verantwortlichen;

2. eine Mitteilung personenbezogener Daten durch einen in der Gemeinschaft niedergelassenen, für die Verarbeitung Verantwortlichen an einen Verarbeiter in einem Drittland, der im Namen des in der Gemeinschaft niedergelassenen, für die Verarbeitung Verantwortlichen tätig ist;

3. eine Mitteilung personenbezogener Daten durch eine in der Gemeinschaft ansässige betroffene Person an einen in einem Drittland niedergelassenen, für die Verarbeitung Verantwortlichen.

Die in Abschnitt 3 dargelegten „Kern"-Grundsätze finden wahrscheinlich in unterschiedlicher Weise auf diese drei verschiedenen Übermittlungsarten Anwendung. So unterscheidet sich beispielsweise die klassische Situation einer Übermittlung durch einen in der Gemeinschaft niedergelassenen, für die Verarbeitung Verantwortlichen an einen einzelnen, für die Verarbeitung Verantwortlichen in einem Drittland sehr von einem Fall, in dem Daten durch einen außerhalb der Gemeinschaft ansässigen, für die Verarbeitung Verantwortlichen unmittelbar von einer einzelnen betroffenen Person in der Gemeinschaft über Telefon oder das Internet erfaßt werden.

Gemeinsame Erklärung der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation vom 12. September 1997 zur Kryptographie[295]

Der Schutz der persönlichen Kommunikation vor willkürlichen Eingriffen ist ein Menschenrecht (Art. 12 Allgemeine Erklärung der Menschenrechte vom 10. Dezember 1948; Art. 17 des Internationalen Paktes über Bürger- und politische Rechte; Art. 8 der Europäischen Menschenrechtskonvention). In der Informationsgesellschaft, in der die Kommunikation überwiegend mit den Mitteln der Telekommunikation stattfindet, bedeutet dieses Recht, daß jeder einen Anspruch darauf hat, daß seine elektronisch übermittelten Mitteilungen vertraulich behandelt werden und kein Unbefugter den Inhalt wahrnehmen kann.

Auf Vorschlag der Internationalen Arbeitsgruppe Telekommunikation und Medien hat die 7. Internationale Konferenz der Datenschutzbeauftragten auf ihrer Sitzung in Luxemburg am 26. September 1985 in einem Beschluß darauf hingewiesen, daß Integration und Digitalisierung die Gefahr des unbefugten Aufzeichnens und Auswertens der übermittelten Informationen erhöhen. Die 11. Internationale Konferenz der Datenschutzbeauftragten hat auf ihrer Sitzung am 30. August 1989 in Berlin gefordert, Maßnahmen zur Datensicherung insbesondere gegen den Zugang nicht autorisierter Personen, die Manipulation, das Mithören und zur Gewährleistung der Authentizität des Senders auf höchstem technischen Niveau und zu akzeptablen Preisen anzubieten.

Das einzige diesen Anforderungen entsprechende Mittel ist die Verschlüsselung der Nachrichten. Das Angebot ausreichender Verschlüsselungsmethoden an die Teilnehmer der Telekommunikation ist damit eine elementare Forderung zur Sicherstellung des Datenschutzes. Es bildet darüber hinaus die Grundlage für datenschutzfreundliche Technologien. Für den Mobilfunk hat die 12. Internationale Konferenz der Datenschutzbeauftragten auf ihrer Sitzung in Paris am 19. September 1990 gefordert, Netzbetreiber sollten verpflichtet sein, den Teilnehmern wirksame Verschlüsselungsverfahren anzubieten. Das Angebot einer end-to-end-Verschlüsselung war eine wesentliche Forderung der Datenschutzbeauftragten bei der Diskussion über den Entwurf einer Richtlinie des Rates der Europäischen Union zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen.

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation bekräftigt ihre Forderung, daß zur Sicherstellung der Vertraulichkeit jedem Teilnehmer elektronischer Telekommunikationsdienste ermöglicht werden muß, seine Nachrichten auf einem von ihm zu frei wählenden Niveau zu verschlüsseln.

Das in einigen Ländern erörterte Verbot der Verschlüsselung von Nachrichten widerspricht diesem Grundsatz. Es behindert die Bürger nicht nur bei der Wahrnehmung ihres Menschenrechts auf unbeobachtbare Kommunikation, sondern fördert den Mißbrauch der Telekommunikation für illegale Zwecke. Es kann von denjenigen, die über entsprechende technische und finanzielle Mittel verfügen, jederzeit umgangen werden, so daß ein Verbot nur den arglosen Bürger trifft.

Auch eine Beschränkung der Möglichkeiten zur Verschlüsselung zum Beispiel durch Lizensierung der erforderlichen Software hätte diesen Effekt. Sie ist aus den genannten Gründen insbesondere nicht geeignet, die organisierte Kriminalität zu bekämpfen.

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation hat Verständnis für die Bedürfnisse der

---

295 Die französischen Mitglieder der Arbeitsgruppe haben an der Verabschiedung dieser Erklärung nicht teilgenommen. Die britische Datenschutzbeauftragte hat Vorbehalte gegen diese Erklärung.

Sicherheitsbehörden, bei der Gefahrenabwehr und der Strafverfolgung auch auf verschlüsselte Nachrichten zugreifen zu können. Die 14. Internationale Konferenz der Datenschutzbeauftragten in Sydney am 29. Oktober 1992 hat einen ausführlichen Bericht der Arbeitsgruppe über die Problematik des Zugriffs von Sicherheitsbehörden auf die Telekommunikation zustimmend zur Kenntnis genommen. Die Konferenz stimmte darin überein, daß die technische und rechtliche Entwicklung im Bereich des Fernmeldegeheimnisses sorgfältig beobachtet werden muß, um die Privatsphäre des Einzelnen vor exzessiver Überwachung zu schützen.

Die Arbeitsgruppe bezweifelt, daß eine Regulierung der Verschlüsselung zugunsten der Sicherheitsbehörden einen angemessenen Beitrag zur Bekämpfung der schweren Kriminalität leisten kann. Für die Bekämpfung von Straftaten geringerer Schwere wäre ein Eingriff in das Telekommunikationsgeheimnis ohnehin unverhältnismäßig. Alle erörterten Modelle (Lizensierung der Software, Ex- und Importbeschränkungen, Schlüsselhinterlegung, hardwareseitige Hintertüren wie „clipper chip") führen zu einem schwächeren Schutz, da diese Lösungen auch unbefugt genutzt werden können. Die Durchsetzung gesetzlicher Verpflichtungen, nur bestimmte, lizenzierte Schlüssel zu benutzen, würde das Verhältnis von genereller Vertraulichkeit und ausnahmsweise gesetzlich erlaubtem Zugriff umkehren. Da alle entsprechenden gesetzlichen Verpflichtungen mit ausreichenden technischen und finanziellen Mitteln (z. B. durch Verbergen der Verschlüsselung - Steganografie) umgangen werden können, würde dies zu einer unverhältnismäßigen und letztendlich nutzlosen Überwachung des Einzelnen führen. Daher gibt es einen Unterschied zwischen Eingriffen in traditionelle Formen der Korrespondenz und deren elektronischer Übertragung: Eingriffe in die erstgenannte Form der Kommunikation können legal sein, wenn es „... in einer demokratischen Gesellschaft zur Bekämpfung von Störungen der öffentlichen Ordnung und Verbrechen notwendig ist ..." (Art. 8 Abs.2 Europäische Menschenrechtskonvention); Eingriffe in die elektronische Kommunikation zur Durchsetzung der Limitierung von kryptografischen Methoden können zur Abschaffung vertraulicher elektronischer Kommunikation insgesamt führen.

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation begrüßt sowohl die OECD-Leitlinien über Kryptographie-Politik vom 27. März 1997 als auch die Gemeinsame Erklärung der Europäischen Ministerkonferenz (Bonn, 6. - 8. Juli 1997), in denen die Bedeutung vertrauenswürdiger kryptographischer Methoden zur Erreichung des Vertrauens der Benutzer in verläßliche Informations- und Kommunikationssysteme betont wird. Die OECD-Leitlinien betonen darüber hinaus das Prinzip, daß die freie Auswahl des Benutzers hinsichtlich kryptographischer Methoden nicht durch neue Gesetzgebung eingeschränkt werden sollte (Prinzip 2 der OECD-Leitlinien). Nationale Gesetzgebung, die einen gesetzmäßigen Zugriff erlaubt, soll dieses Prinzip im größtmöglichen Ausmaß reflektieren (Prinzip 6). Die Arbeitsgruppe mißt den Konsequenzen für den Datenschutz, die durch die Nutzung kryptographischer Methoden zur Sicherung der Integrität von Daten in elektronischen Transaktionen ausgelöst werden, besondere Bedeutung zu (Prinzip 5). Die Speicherung personenbezogener Daten und die Schaffung von Systemen zur persönlichen Identifikation in Verbindung mit der Nutzung solcher Methoden erfordern spezielle Maßnahmen zum Datenschutz.

Handys – Komfort nicht ohne Risiko

Was für die einen lächerlich und albern ist, gehört für die anderen zu den Grundbedingungen ihrer Existenz: Mobiltelefone sind - wie auch immer sie bewertet werden - aus dem täglichen Leben kaum noch wegzudenken. Handys sind klein, leicht und daher problemlos mitnehmbar, so daß eine ständige Erreichbarkeit gegeben ist. Gerade diese Eigenschaften erlauben aber auch ihre mißbräuchliche Nutzung als Wanze. Darüber hinaus ermöglichen neue Abhörtechniken das unbemerkte Mithören von Gesprächen.

Das Handy als Wanze

Das Abhören von Räumen mit Wanzen ist aus vielen Darstellungen hinlänglich bekannt. Vielleicht nicht so bekannt ist, daß Handys durch die geschickte Auswahl von Leistungsmerkmalen und den Einsatz handelsüblicher Zusatzgeräte ähnliche Möglichkeiten bieten.

„Liegenlassen" eines Handys

Im einfachsten Fall wird ein eingeschaltetes Handy, mit dem zuvor eine Gesprächsverbindung aufgebaut wurde, im abzuhörenden Raum liegengelassen. Alle im Raum geführten Gespräche werden, sofern das Mikrofon des Handys sie erfaßt, zu einem Zielgerät übertragen. Natürlich hat ein solches „Abhörgerät" wegen der begrenzten Akkukapazität nur eine kurze Betriebsdauer und der Abhörvorgang kann durch einen Blick auf das Display erkannt werden.

Aktivieren eines Handys von außen

Sind bei einem „liegengelassenen" Handy die Leistungsmerkmale „Automatische Anrufannahme" und „Lautlosbetrieb" aktiviert, kann von außen sogar zu einem beliebigen Zeitpunkt abgehört werden. Erst ein Anruf versetzt das Handy dann in den Gesprächszustand. Zwar schließen sich bei vielen Geräten die Leistungsmerkmale „Automatische Anrufannahme" und „Lautlosbetrieb" gegenseitig aus und das Leistungsmerkmal „Automatische Anrufannahme" kann im allgemeinen nur in Kombination mit einer Freisprecheinrichtung genutzt werden; durch eine geschickte Auswahl von Ruftonoptionen und dem Einsatz externer Sprechgarnituren (Mikrofon und Ohrhörer) kann der beschriebene Effekt trotzdem erreicht werden. Somit ist ein Handy allein durch die Nutzung von Standardmerkmalen und frei verfügbarer Technik schon als recht leistungsfähiges Abhörgerät zu betreiben.

Vornehmen von Gerätemanipulationen

Auch durch Hardwaremanipulationen kann die Existenz einer Freisprecheinrichtung simuliert werden (beispielsweise entsprechende interne Beschaltung der Anschlußbuchse). Wenn durch einen weiteren Eingriff in das Handy zusätzlich das Display und der Ruftongenerator deaktiviert und dann Leistungsmerkmale wie oben beschrieben genutzt werden, ist am Handy nicht mehr erkennbar, ob und wann es als Wanze mißbraucht wird.

Wer über entsprechende Spezialkenntnisse und die dafür erforderlichen Hard- und Softwarekomponenten verfügt, kann sogar die im Handy gespeicherte Systemsoftware so verändern, daß ohne Aktivierung von Leistungsmerkmalen das Abhören zu einem beliebigen Zeitpunkt durch Anruf des Handys möglich ist.

Neue Technik zum Abhören von Mobilfunkgesprächen

Gespräche, die mit Handys geführt werden, sind grundsätzlich abhörbar. Das mag zunächst verwunderlich erscheinen, da die Netzbetreiber und Gerätehersteller lange Zeit gerade mit der Verschlüsselung für diese neue Kommunikationstechnik geworben haben. In diesem Zusammenhang wurde jedoch nicht erwähnt, daß Netzbetreiber durch einen Befehl die Verschlüsselung ausschalten können. Diese Funktion ist notwendig, da in einigen europäischen Ländern nur eine unverschlüsselte Kommunikation möglich ist. Ob verschlüsselt oder unverschlüsselt übertragen wird, wird auf den Handys bislang nicht angezeigt.

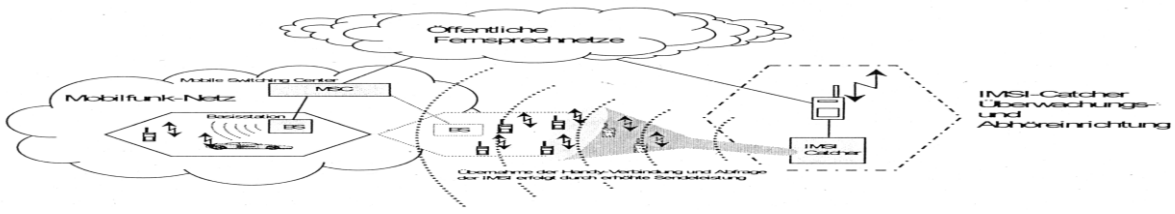
Im Rahmen der Beratungen über ein Begleitgesetz zum Telekommunikationsgesetz wurde erörtert, Nachrichtendiensten und Strafverfolgungsbehörden den Einsatz von Geräten (sog. **IMSI-Catcher**) zu erlauben, die gezielt bei einzelnen Handys die Verschlüsselung ausschalten können und damit das Mithören und Aufzeichnen von Gesprächen ermöglichen. Daneben sollten diese Geräte dazu genutzt werden, die netzinternen Rufnummern von Mobiltelefonen, die sogenannten IMSI (International Mobile Subscriber Identity - netzinterne Teilnehmerkennung) zu ermitteln, um treffsicher auf einzelne Handys zugreifen zu können.

Aufbau des IMSI-Catchers

Das Grundgerät ist nicht größer als ein durchschnittlicher PC. Die Steuerung erfolgt durch ein handelsübliches Laptop. Der IMSI-Catcher kann in zwei Betriebsmodi (fangen, abhören) arbeiten. Geräte zum Fangen und zum Abhören sind identisch; zum Abhören ist zusätzlich lediglich eine Softwareergänzung und ein nachgeschaltetes Handy nötig. IMSI-Catcher können in verschiedenen Funknetzen (D1, D2, E-Plus) eingesetzt werden. Der Betrieb kann aus einem PKW heraus erfolgen. Damit ist ein schneller Ortswechsel unproblematisch.

IMSI-Catcher im Fangmodus

Um gezielt abhören zu können, ist in aller Regel die Kenntnis der Rufnummer erforderlich. Die Abhörgeräte simulieren dafür eine Basisstation, indem sie eine zusätzliche eigene Funkzelle aufbauen, die sich genau wie eine Originalzelle verhält. Weil die Abhörgeräte mit einer etwas stärkeren Leistung arbeiten, melden sich **alle** Geräte in dieser neuen Funkzelle und nicht bei der eigentlichen Basisstation an. Über diese Station laufen dann alle Verbindungsanfragen der Handys. Die Nutzerinnen und Nutzer bemerken von diesem „Fangen" nichts. Von allen in seiner Reichweite befindlichen Handys kann das Abhörgerät neben der IMSI auch die IMEI (International Mobile Station Equipment Identity - Endgerätekennung) abrufen. Technisch bedingt kann während dieser Prozedur niemand mit dem betroffenen Handy Gespräche führen oder empfangen. Selbst Notrufe zu Polizei, Feuerwehr oder ärztlichem Notdienst sind von keinem der in der neuen Funkzelle



eingebuchten Handys möglich.

IMSI-Catcher im Abhörmodus

Im Abhörmodus nutzen IMSI-Catcher die Möglichkeit, die Verschlüsselung auszuschalten. Wenn also die Gespräche eines Handys abgehört werden sollen, wird beim Verbindungsaufbau die Verschlüsselung ausgeschaltet, so daß die Gesprächsinhalte zwar nach wie vor in digitaler Form, jetzt aber unverschlüsselt und mit entsprechender Software abhörbar vorliegen und aufgezeichnet werden können. Solange das Abhörgerät in diesem Modus arbeitet, kann mit keinem gefangenen Handy im Einflußbereich des Abhörgerätes eine Verbindung aufgebaut werden. Lediglich abgehende Gespräche des abgehörten Handys sind möglich.

Die Datenschutzbeauftragten des Bundes und der Länder haben den Einsatz der IMSI-Catcher insbesondere deshalb abgelehnt, weil bei der Feststellung der Rufnummer und beim Abhören der Betroffenen mit einer bisher noch nicht dagewesenen Intensität das Recht auf unbeobachtete Kommunikation unbeteiligter Dritter beeinträchtigt wird.

Selbst wenn diese Abhörgeräte zwar von Nachrichtendiensten und Strafverfolgungsbehörden zunächst nicht eingesetzt werden sollen, bleiben die beschriebenen Risiken für die Nutzerinnen und Nutzer von Handys jedoch bestehen. Einerseits ist nicht auszuschließen, daß dieses Geräte beispielsweise für den Export produziert werden. Andererseits dauert es erfahrungsgemäß nicht lange, bis Bauanleitungen für einzelne Komponenten oder für das gesamte Gerät veröffentlicht werden. Es wäre verwunderlich, wenn das, was erhältlich ist, nicht auch von irgend jemand zum Einsatz gebracht würde.

Es wird deutlich, daß nur ein ausgeschaltetes Handy einen wirklich sicheren Schutz vor mißbräuchlicher Nutzung garantiert. Damit wird aber gerade der Zweck der Handynutzung, der in der ständigen Erreichbarkeit liegt, unterlaufen. Den Nutzerinnen und Nutzern von Handys müssen die hier beschriebenen Risiken jedoch bekannt sein, damit sie für sich selbst bewußt entscheiden können, ob und wie lange sie bei welchen Gelegenheiten ihr Handy einschalten. Schön wäre es, wenn Mobilfunkgeräte so weiterentwickelt und der Netzbetrieb so ausgestaltet würden, daß Mißbrauchsmöglichkeiten von vornherein so weit wie möglich ausgeschlossen sind. Gerätehersteller und Netzbetreiber sind aufgefordert, im Rahmen des geltenden Rechts durch geeignete Maßnahmen dafür zu sorgen, daß ihre Kundinnen und Kunden vertraulich miteinander kommunizieren können. Solange dies nicht sichergestellt ist, bedarf es auch von ihrer Seite der offenen und umfassenden Aufklärung der Kundschaft über die Risiken für die vertrauliche Kommunikation in Mobilfunknetzen.

Herausgeber:

Die Landesbeauftragte für den Datenschutz
Nordrhein-Westfalen
Reichstraße 43
40217 Düsseldorf

Telefon : 0211/38424-0
Telefax : 0211/38424-10
e-mail: mailbox@mail.lfd.nrw.de

Der Landesbeauftragte für den Datenschutz
Mecklenburg Vorpommern
Schloß Schwerin
19053 Schwerin

Telefon: 0385/5252760
Fax: 0385/5252758
e-mail: Datenschutz@mvnet.de

Orientierungshilfe

Datenschutzrechtliche Protokollierung beim Betrieb informationstechnischer Systeme (IT-Systeme)

AK Technik, 1994

1 Begriff

1.1 Unter Protokollierung beim Betrieb von IT-Systemen ist im datenschutzrechtlichen Sinn die Erstellung von manuellen oder automatisierten Aufzeichnungen

- über die tatsächlichen Veränderungen an Hardwarekomponenten (z. B. vorübergehendes Entfernen von Sicherheitselementen wie Diskettenschachtverriegelungen o. ä.) und an der Software (Betriebssystem, systemnahe Software, Anwendungssoftware) sowie

- über die Verarbeitung (Erhebung, Speicherung, Veränderung, Löschung, Sperrung, Übermittlung und sonstigen Nutzung) von personenbezogenen Daten

zu verstehen.

1.2 Elemente einer Protokollierung sind:

- Art des Vorganges,

- Zeitpunkt der Aktivität bzw. des Ereignisses,

- Merkmale der Maßnahme (z. B. Eingabewerte),

- ausführende Person.

Aus den Protokollen muß sich mithin die Frage beantworten lassen: „Wer hat wann mit welchen Mitteln was veranlaßt bzw. worauf zugegriffen?“ Außerdem müssen sich Systemzustände ableiten lassen: „Wer hatte von wann bis wann welche Zugriffsrechte?“

2 Rechtsgrundlagen

2.1 Im Datenschutzrecht des Bundes und der Länder sind die Bestimmungen, die eine Protokollierungspflicht begründen, in der Regel nicht gleichlautend (vgl. z. B. bezüglich der Übermittlungskontrolle Nr. 6 der Anlage zu § 9 BDSG im Verhältnis zu § 10 Abs. 3 Nr. 6 Hessisches Datenschutzgesetz, § 6 Abs. 2 Nr. 6 Bremisches Datenschutzgesetz, § 10 Abs. 2 Nr. 6 BbgDSG). Die Differenzen gehen über rein redaktionelle Unterschiede hinaus, so daß von allgemein gültigen datenschutzrechtlichen Protokollierungsbestimmungen nicht gesprochen werden kann.

2.2 Für eine Reihe von Verwaltungsverfahren gelten zudem bereichsspezifische, vom Datenschutzrecht des Bundes bzw. des betreffenden Landes abweichende Protokollierungsvorschriften. Als Beispiele hierfür sind zu nennen:

Meldegesetze, Polizeigesetze, Verfassungsschutzgesetze, Gesetz über das ZEVIS usw.

2.3 Nur wenige gesetzliche Bestimmungen enthalten explizite Protokollierungsverpflichtungen wie z. B. in Nr. 7 der Anlage zu § 9 BDSG, § 7 Abs. 2 Nr. 6 und § 11 Abs. 2 LDSG SH, § 10 Abs. 2 Nr. 7 BbgDSG. Die meisten Regelungen bedingen (lediglich) eine Protokollierung, um die jeweils geforderte Maßnahme realisieren zu können (vgl. z. B. bezüglich der Speicherkontrolle und der automatischen Abrufverfahren Nr. 3 der Anlage zu § 9 BDSG, § 10 Abs. 2 BDSG, § 20 LDSG-SH, § 9 Abs. 3 und § 10 Abs. 2 Nr. 6 BbgDSG).

2.4 Bevor Art und Umfang von Protokollierungen festgelegt werden, haben die datenverarbeitenden Stellen mithin zu ermitteln, welche gesetzlichen Regelungen für ihren Zuständigkeitsbereich welche Rahmenbedingungen definieren. Der Komplex „Protokollierung" stellt sich mithin nicht als eine Maßnahme im Rahmen des Ermessens dar, sondern als eine Folge aus den jeweils gültigen gesetzlichen Bestimmungen.

2.5 Die nachfolgenden Hinweise können daher nur unter diesem Vorbehalt den Charakter von Mindestanforderungen erfüllen.

3 Gegenstand der Protokollierung

3.1 Differenzierung zwischen der Administration und der Benutzung von IT-Systemen

3.1.1 Beim Betrieb von IT-Systemen sollte zwischen den Funktionen der Administration und der Benutzung unterschieden werden.

3.1.2 Als „Administration" sind die Maßnahmen zur Installation, Modifikation und Konfiguration von Hard- und Software einschließlich der Abarbeitung von Systemnachrichten zu verstehen. Es handelt sich hierbei im wesentlichen um Basisfunktionen, die die fortdauernde Benutzung des Systems überhaupt erst ermöglichen.

3.1.3 Unter „Benutzung" ist die Inanspruchnahme der vom IT-System bereitgestellten Ressourcen anzusehen. In der Praxis stellt sich dies als der Aufruf von Software dar, die entsprechend den in einem Benutzerprofil festgelegten Zugriffsrechten (in der Regel in einem Menü) zur Verfügung gestellt wird.

3.1.4 Die Protokollierung der Administrationsaktivitäten hat daher den Charakter einer Systemüberwachung, während die Protokollierung der Benutzeraktivitäten im wesentlichen der Verfahrensüberwachung dient. Dementsprechend finden sich die Anforderungen an die Art und den Umfang der systemorientierten Protokollierung überwiegend in dem „allgemeinen" Datenschutzrecht, während die verfahrensorientierte Protokollierung weitgehend durch bereichsspezifische „Regelungen" definiert wird (vgl. z. B. Tz 2.2).

3.2 Administration von IT-Systemen
Folgende Aktivitäten sind vollständig zu protokollieren:

3.2.1 Systemgenerierung und Modifikation von Systemparametern

Da auf dieser Ebene in der Regel keine systemgesteuerten Protokolle erzeugt werden, bedarf es entsprechender detaillierter manueller Aufzeichnungen, die mit der Systemdokumentation korrespondieren sollten.

3.2.2 Einrichten von Benutzern

Wem von wann bis wann durch wen das Recht eingeräumt worden ist, das betreffende IT-System zu benutzen, ist vollständig zu protokollieren, dies ergibt sich auch aus der Eingabekontrolle. Für diese Protokolle sollten längerfristige Aufbewahrungszeiträume vorgesehen werden, da sie Grundlage praktisch jeder Revisionsmaßnahme sind.

3.2.3 Verwaltung von Befugnistabellen

Im Rahmen der Protokollierung von Befugniszuweisungen kommt es insbesondere auch darauf an aufzuzeichnen, wer die Anweisung zur Erteilung einer bestimmten Befugnis erteilt hat.

3.2.4 Einspielen und Änderung von Anwendungssoftware

Die Protokolle repräsentieren das Ergebnis der Programm- und Verfahrensfreigaben.

3.2.5 Änderungen an der Dateiorganisation

Im Hinblick auf die vielfältigen Manipulationsmöglichkeiten, die sich bereits bei Benutzung der „Standard-Dateiverwaltungssysteme" ergeben, kommt einer vollständigen Protokollierung eine besondere Bedeutung zu (vgl. z. B. Datenbankmanagement).

3.2.6 Durchführung von Backup-, Restore- und sonstigen Datensicherungsmaßnahmen

Da derartige Maßnahmen mit der Anfertigung von Kopien bzw. dem Überschreiben von Datenbeständen verbunden sind und häufig in „Ausnahmesituationen" durchgeführt werden, besteht eine erhöhte Notwendigkeit zur Protokollierung.

3.2.7 Sonstiger Aufruf von Administrations-Tools

Für praktisch alle IT-Systeme bestehen Tools, die nur in „Ausnahmesituationen" Anwendung finden sollten. Deshalb sollte ihr Einsatz besonders protokolliert werden.

3.3 Benutzung von IT-Systemen

Folgende Aktivitäten sind in Abhängigkeit von der Sensibilität der Verfahren/Daten vollständig bzw. selektiv zu protokollieren:

3.3.1 Versuche unbefugten Einloggens und Überschreitung von Befugnissen

Geht man von einer wirksamen Authentifizierungsprozedur und sachgerechten Befugniszuweisungen aus, kommt der vollständigen Protokollierung aller „auffälligen Abnormalitäten" beim Einloggen und der Benutzung von Hard- und Softwarekomponenten eine zentrale Bedeutung zu. Benutzer in diesem Sinne ist auch der Systemadministrator.

3.3.2 Eingabe von Daten

Die sogenannte Eingabekontrolle erfolgt grundsätzlich verfahrensorientiert (z. B. Protokollierung in Akten, soweit vorhanden, Protokollierung direkt im Datenbestand, sofern keine Akten geführt werden). Auch wenn man davon ausgeht, daß Befugnisüberschreitungen anderweitig protokolliert werden, dürfte eine vollständige Protokol-

lierung von Dateneingaben als Regelfall angesehen werden müssen.

3.3.3 Datenübermittlungen

Nur soweit nicht gesetzlich eine vollständige Protokollierung vorgeschrieben ist (vgl. z. B. § 10 Abs. 2 Nr. 6 DSG NW, § 10 Abs. 2 Nr. 6 BbgDSG), kann eine selektive Protokollierung als ausreichend angesehen werden. In diesem Zusammenhang ist auch die Anfertigung von Dateikopien, Hardcopies usw. relevant. Dabei ist zu beachten, daß der Benutzer die grundsätzliche Befugnis haben muß, derartige Datenübermittlungen zu veranlassen, anderenfalls würde es sich um die Überschreitung von Befugnissen handeln (vgl. Tz. 3.3.1).

3.3.4 Benutzung von automatisierten Abrufverfahren

In der Regel dürfte eine vollständige Protokollierung der Abrufe und der Gründe der Abrufe (Vorgang, Aktenzeichen etc.) erforderlich sein, um unbefugte Kenntnisnahmen im Rahmen der grundsätzlich eingeräumten Zugriffsrechte aufdecken zu können.

3.3.5 Löschung von Daten

Eine vollständige Protokollierung ist insbesondere erforderlich, wenn die Daten ausschließlich in automatisierten Dateien gespeichert sind. In Abhängigkeit vom Gegenstand der Datenverarbeitung ist eine Protokollierung der gelöschten Daten oder lediglich die Tatsache der Löschung angezeigt. Ersteres dürfte „kontraproduktiv" sein, wenn Löschungsansprüche der Betroffenen erfüllt werden.

3.3.6 Aufruf von Programmen

Dies kann erforderlich sein bei besonders „sensiblen" Programmen, die z. B. nur zu bestimmten Zeiten oder Anlässen benutzt werden dürfen. Deshalb ist in diesen Fällen eine vollständige Protokollierung angezeigt. Die Protokollierung dient auch der Entlastung der befugten Benutzer (Nachweis des ausschließlich befugten Aufrufs der Programme).

4 Personenbezug von Protokolldaten

Protokolle, die aus den unter Tz. 3 genannten Gründen erzeugt werden, stellen faktisch alle personenbezogenen Dateien dar. In erster Linie besteht ein Personenbezug zu den „veranlassenden Personen oder Stellen" (vgl. Tz. 1.2). In vielen Fällen lassen Protokolle außerdem Rückschlüsse auf Daten von Betroffenen zu. Soweit in den einzelnen Datenschutzgesetzen nicht Ausnahmeregelungen enthalten sind (vgl. z. B. § 1 Abs. 3 Nr. 1 BDSG, § 8 Abs. 1 Satz 3 LDSG-SH, § 8 Abs. 2 BbgDSG), sind diese Protokolle wie „normale" Dateien zu behandeln.

5 Berücksichtigung der Zweckbindung bei der Nutzung von Protokolldaten

5.1 Protokolldaten unterliegen aufgrund der nahezu übereinstimmenden Regelungen im Datenschutzrecht des Bundes und der Länder einer besonderen engen Zweckbindung (z. B. § 14 Abs. 4 BDSG, § 13 Abs. 5 HDSG). Sie dürfen nur zu den Zwecken genutzt werden, die Anlaß für ihre Speicherung waren.

5.2 Dies sind in der Regel die in einem Sicherheitskonzept festgelegten allgemeinen Kontrollen, die in den meisten Datenschutzgesetzen geforderte „Überwachung der ordnungsgemäßen Anwendung der

Datenverarbeitungsprogramme, mit denen personenbezogene Daten verarbeitet werden" (vgl. § 18 Abs. 2 BDSG, § 8 Abs. 3 LDSG-SH) und die Kontrollen durch interne oder externe Datenschutzbeauftragte. (Näheres hierzu vgl. Schaar, Schläger in CR 7/1993, S. 435).

6 Aufbewahrungsdauer für Protokolle

6.1 Die Aufbewahrungsdauer der Protokolle richtet sich, da es sich um personenbezogene Daten handelt, nach den allgemeinen Löschungsregeln der Datenschutzgesetze. Maßstab ist mithin die „Erforderlichkeit zur Aufgabenerfüllung". Gibt es keinen zwingenden Grund für das weitere Vorhalten von Protokolldateien, besteht eine Löschungspflicht (vgl. z. B. § 20 Abs. 2 BDSG).

6.2 Eine exakte Bestimmung des Zeitraums der Erforderlichkeit für Protokolle, deren Auswertung zeitlich nicht konkretisiert ist (vgl. z. B. die Protokolle im Zusammenhang mit der Administration, Tz. 3.2), ist nicht möglich.
Als Anhaltspunkte können dienen:

- die Wahrscheinlichkeit, daß Unregelmäßigkeiten (noch) offenbar werden können und
- die Möglichkeit, die Gründe von Unregelmäßigkeiten anhand der Protokolle und anderer Unterlagen aufdecken zu können.

Erfahrungsgemäß sollte eine Frist von einem Jahr nicht überschritten werden.

6.3 Soweit Protokolle zum Zwecke gezielter Kontrollen angefertigt werden (vgl. insbesondere Tz. 3.3.1 und 3.3.5), kommen kürzere Speicherungsfristen in Betracht. In der Regel reicht eine Aufbewahrung bis zur tatsächlichen Kontrolle.

6.4 Eine Begrenzung der Speicherungsdauer von Protokolldaten kann auch dadurch erreicht werden, daß durch eine „Ringspeicherung" nur eine maximale Anzahl von Protokolldatensätzen für die Kontrolle vorgehalten wird (z. B. die jeweils letzten „n" Sätze). Andere Möglichkeiten der Reduzierung der Datenmengen bestehen darin, Protokolldatensätze nach einem Zufallsprinzip (feste Prozentsätze o. ä.) zu erzeugen oder die Erstellung durch den Kontrolleur zu initiieren.

7 Technische und organisatorische Rahmenbedingungen

Die Effektivität der Protokollierung und ihre Auswertung im Rahmen von Kontrollen hängt im entscheidenden Maße von den technischen und organisatorischen Rahmenbedingungen ab. In diesem Zusammenhang sollten folgende Aspekte Berücksichtigung finden:

7.1 Es sollte ein Revisionskonzept erstellt werden, das die Zielrichtung der Protokolle und der Kontrollen sowie Schutzmechanismen für die Rechte der Mitarbeiter und der sonstigen betroffenen Personen klar definiert.

7.2 Die Zwangsläufigkeit und damit die Vollständigkeit der Protokolle muß gewährleistet werden.

7.3 Das gleiche gilt für die Manipulationssicherheit der Einträge in Protokolldateien.

7.4 Entsprechend der Zweckbindung der Datenbestände müssen wirksame Zugriffsbeschränkungen realisiert

werden.

7.5 Die Protokolle müssen so gestaltet sein, daß seitens der Revisoren eine effektive Überprüfung möglich ist.

7.6 Die Auswertungsmöglichkeiten sollten vorab mit den Revisoren abgestimmt und festgelegt sein.

7.7 Kontrollen sollten nach dem 4-Augen-Prinzip erfolgen.

7.8 Es sollte vorab definiert werden, welche Konsequenzen sich aus Verstößen ergeben, die durch die Kontrolle von Protokollen aufgedeckt werden.

7.9 Für Routinekontrollen sollten automatisierte Verfahren (z. B. watch dogs) verwendet werden.

7.10 Personalräte und Arbeitnehmervertreter(innen) sollten bei der Erarbeitung des Revisionskonzeptes und bei der Auswertung der Protokolle beteiligt werden.

Arbeitsgruppe „Datenschutzfreundliche Technologien“

des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und der Länder

Arbeitspapier

„Datenschutzfreundliche Technologien“

In der Arbeitsgruppe haben mitgewirkt:
Walter Ernestus (Der Bundesbeauftragte für den Datenschutz), Dieter J. Ermer (Federführung) (Der Bayerische Landesbeauftragte für den Datenschutz), Dr. Martin Hube (Der Niedersächsische Landesbeauftragte für den Datenschutz), Marit Köhntopp (Der Landesbeauftragte für den Datenschutz Schleswig-Holstein), Dr. Michael Knorr (Der Thüringer Landesbeauftragte für den Datenschutz), Dr. Gisela Quiring-Kock (Der Hessische Datenschutzbeauftragte), Dr. Uwe Schläger (Der Hamburgische Datenschutzbeauftragte), Gabriel Schulz (Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern).
Wir danken Frau Sottong-Micas (Europäische Kommission, DG XV) und Herrn Weinand (Bundesamt für Sicherheit in der Informationstechnik) für ihre Mitarbeit.

Stand: 1.10.1997

Inhalt

1. Einleitung

2. Notwendigkeit für Datenschutz durch Technik
2.1 Rechtliche Forderungen und Entwicklungen
2.2 Grundlegende Betrachtung von Informationssystemen

3. Anonymisierung

4. Pseudonymisierung
4.1 Selbstgenerierte Pseudonyme
4.2 Referenz-Pseudonyme
4.3 Einweg-Pseudonyme

5. Realisierungshilfen
5.1 Hashfunktionen
5.2 Digitale Signaturen
5.3 (Signaturschlüssel-)Zertifikat
5.4 Blinde digitale Signatur
5.5 Biometrische Verfahren
5.6 Vertrauensstellen
5.7 Der Identity Protector

7. Zusammenfassung und Handlungsempfehlung

Aus Kostengründen ist wegen des Umfangs auf den vollständigen Abdruck verzichtet worden. Bei Bedarf kann diese Anlage jedoch zusammen mit der Anlage 18 als Broschüre unter der im Impressum angegebenen Adresse ohne weitere Kosten angefordert werden.

Arbeitsgruppe „Datenschutz in der Telekommunikation“

des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ der Datenschutzbeauftragten des Bundes und der Länder

Arbeitspapier

„Datenschutzfreundliche Technologien in der Telekommunikation“

Autoren:
Thomas Jandach (Der Landesbeauftragte für den Datenschutz Baden-Württemberg), Marit Köhntopp (Der Landesbeauftragte für den Datenschutz Schleswig-Holstein), Ursula Meyer zu Natrup (Berliner Datenschutzbeauftragter), Peter Schaar (Der Hamburgische Datenschutzbeauftragte), Wilfried Seiffert (Der Niedersächsische Landesbeauftragte für den Datenschutz), Kurt Urban (Der Landesbeauftragte für den Datenschutz Brandenburg), Andreas Waldenspuhl, René Weichelt (Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern), Holger Weigel (Der Hessische Datenschutzbeauftragte), Franz-Josef Wesener (Federführung), Michael Wilms (Die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen).

Stand: 17.10.1997

Inhalt

1 Einleitung

2 Modelle und Kriterien

2.1 TK-Datenmodell
2.2 Datensparsamkeitsmodell – Elemente anonymer Nutzung
2.3 Bewertungsschema für anonyme Nutzung von TK-Systemen

3 Telekommunikationsdaten in Netzen und Medien

3.1 Zusammenhang von Kontextdaten und Nutzung
3.2 Integrated Services Digital Network (ISDN)
3.3 X.25-Dienste
3.4 Breitbandkommunikation
3.5 ATM
3.6 Zellulare Mobilfunknetze
3.7 Interne Telekommunikationsanlagen
3.8 DECT
3.9 Satellitenkommunikation
3.10 Internet

4 Möglichkeiten der Datenvermeidung und -reduzierung

4.1 Schutz von Sender und Empfänger
4.1.1 Verteilung von Nachrichten
4.1.2 Bedeutungslose Nachrichten: Dummy Traffic
4.1.3 Überlagerndes Senden nach David Chaum: DC-Netz
4.1.4 Mixe
4.1.5 Verhinderung der Peilbarkeit
4.1.6 Änderung des Aufenthaltsmanagements
4.2 Datenminimierung bei der Entgeltabrechnung
4.2.1 Einsatz von Chipkarten für die Bezahlung von Telekommunikationsdienstleistungen
4.2.2 Elektronisches Geld zur Bezahlung von Telekommunikationsdienstleistungen
4.2.3 Möglichkeiten zur Reduzierung oder zur völligen Vermeidung der Speicherung von Verbindungsdaten für Abrechnungszwecke
4.2.4 Möglichkeiten zur Minimierung von Bestandsdaten
4.2.5 Datenminimierung bei Entgeltabrechnungen an Nebenstellenanlagen
4.2.6 Zusammenfassende Bewertung

5 Handlungsempfehlung

Technische Beschreibungen und Beispiel

1 ATM

2 Zellulare Mobilfunknetze

3 DECT

4 Satellitenkommunikation

5 TCP/IP als Grundlage zum Internet

6 Schutz von Nachrichteninhalten

7 Anwendung des Datenmodells für Wähl- und Festverbindungen im digitalen Festnetz

Aus Kostengründen ist wegen des Umfangs auf den vollständigen Abdruck verzichtet worden. Bei Bedarf kann diese Anlage jedoch zusammen mit der Anlage 17 als Broschüre unter der im Impressum angegebenen Adresse ohne weitere Kosten angefordert werden.

Stichwortverzeichnis

(Berichtszeitraum der Jahresberichte: I = März bis Dezember 1992; II = bis März 1994; III = bis März 1995; IV = bis März 1996; V = bis März 1997; VI = bis März 1998 /Seitenangabe)

Abfallbegleitscheinverfahren II/134
Abfallentsorgung II/83; IV/118; VI/147
Abruf V/32
Abschottung III/78, 79, 86; IV/54, 122
Absenderangaben III/154
absolute Anonymisierung III/84
Abwägungsempfehlungen IV/116
Abwasseranschlußgebühr IV/117
Administration VI/125, 126
Adoption VI/83
Adoptionsgeheimnis II/129; III/43
Adreßbuchverlage IV/109; V/30; VI/43
Adreßhandel ..... I/33 ff.; II/94
Adreßmittlung III/110, 156; V/74
Adreßweitergabe II/43; IV/109; V/74
Agrarförderung VI/122
Agrarstatistik V/110
Ahnenforschung V/33
Aktenanforderung IV/124
Aktenbereinigung IV/125; V/147
Aktenbestandteile, unzulässige IV/124
Aktendeckel III/152
Akteneinsicht ..... II/57, 83; IV/76, 81, 87, 124 ff.; V/29, 145; VI/140, 164
Aktenführung III/130; V/124
Aktenvernichtung II/16
Alarmanlage III/17
Allfinanzklausel V/118
Altakten VI/41
Altdaten ..... I/8, 15 ff., 30, 37 (Anlage 1); II/37, 96; III/44, 149; IV/82, 87 ff.; V/124
Altlastenkataster V/111
Altpersonalakten IV/123; VI/41
Amt für offene Vermögensfragen II/81
Amt für Arbeitsschutz und Sicherheitstechnik II/140
amtsärztliche Untersuchung III/160
Amtsermittlung IV/76
Amtsgeheimnisse II/11
Amtshilfe IV/46
Analyse-Dateien V/38
Anerkennungsrichtlinie III/132
Anfangsverdacht IV/40; V/44
Anonymisierung von Prüfungsakten II/89
Anonymisierung V/11; VI/104
Anrufbeantworter II/31
Anrufumleitung II/22

Antragsformulare III/146
Antragsteller III/159
AOK II/120; III/123, 124, 126, 128
Arbeitnehmerdatenschutzrecht V/143; VI/158
Arbeitsamt V/85
Arbeitsbefreiung IV/74
Arbeitsgericht III/91
Arbeitsstipendien VI/92
Arbeitszeitanalyse III/147
Archiv VI/89, 90
Archivierung IV/124; V/146; VI/117
Arzneimittel-Budget VI/102
Arzneimittelgesetz III/138
Arztgeheimnis VI/132
ärztliche Schweigepflicht II/11; III/144; IV/76; VI/85, 118
ärztliches Zeugnis IV/75; VI/143
Aufbewahrung von Personalakten IV/123
Aufbewahrungsfristen V/35
Aufbewahrungspflicht III/89; IV/81, 85; V/125
Aufenthaltserlaubnis IV/50; V/51
Aufklärung III/77, 87
Aufnahmebeleg III/143
Aufschalten II/24
Auftragskontrolle III/15
Ausbildung V/119
Auskunftserteilung III/125, 153; IV/123
Auskunftspflicht III/78, 154; IV/72; VI/145
Auskunftsrecht III/131; IV/45, 76, 82, 87
Auskunftssperre VI/45
Ausländer II/11; III/76; V/50
Ausländerzentralregister II/79
Ausweis mit Magnetstreifen IV/128
Auszeichnungen und Ehrungen IV/25
Autobahnmaut II/29; III/33; IV/107
automatischer Rückruf II/23
automatisierte DV IV/128; V/32; VI/44
automatisierter Datenabgleich V/86
Bankauskunft V/90
Bauaufsichtsämter II/142
Bauleitpläne VI/129
Baustelleninformationsdienst III/148
Bebauungsplan IV/116
Befragung an Schulen IV/65
Begnadigungsverfahren IV/25
Behinderte II/128; V/91
Behördenführungszeugnis II/51, 53; III/137
behördlicher Datenschutzbeauftragter ..... I/42 (Anlage 5); II/18; III/21, 38, 123; IV/25; V/19, 27; VI/112
Beihilfen III/146; IV/123

Beitrags- und Leistungsdaten III/123; IV/117
Beitragsordnung III/135
belangloses Datum III/143
Beliehene IV/25, 97
Benutzerkontrolle III/13
Benutzungsordnung V/83; VI/89
Beratungstätigkeit VI/139
bereichsspezifische Regelungen III/38; IV/82, 85, 87
Bereinigungsanspruch IV/124
Berufsgeheimnis II/11
Berufsgenossenschaft III/126
Berufsordnung für Hebammen II/119; IV/80
Berufsordnung der Ärzte II/118
Bescheide IV/126
Beschlagnahmeverbot III/108, 125; IV/78, 93; VI/118
Bestandsdaten III/30
betrieblicher Gesundheitsbericht IV/75
Betriebslisten II/140
Betriebssystem V/102
Bewachungsunternehmen IV/110
Bewegungsprofile VI/24
Bewerberauswahl V/149
Bildungsreisen VI/134
Blaues Adreßbuch I/44; II/54
Bodenreform V/120
Brandenburgisches Meldegesetz IV/30
Brandenburgisches Abfallgesetz V/111; VI/124, 147
Brandenburgisches Architektengesetz V/113
Brandenburgisches Archivgesetz ..... I/51; II/95; III/118; IV/69; V/83 f.; VI/92, 117
Brandenburgisches Statistikgesetz II/81; III/79; IV/51
Brandenburgisches Sozialberufsgesetz V/86
Brandenburgisches Schulgesetz IV/62; V/67
Brandenburgisches Polizeigesetz IV/37
Brandenburgisches Hochschulgesetz IV/95
Brandenburgisches Datenschutzgesetz ..... I/3 ff., 17, 20, 24, 36; III/37, 39; IV/23
BSI IV/14
BStU-Unterlagen V/143
Bundes-Seuchengesetz VI/105
Bundesausbildungsförderungsgesetz IV/74
Bundesbeauftragter für den Datenschutz ..... I/5, 28, 31, 33 ff.
Bundeskindergeldgesetz I/5; III/43
Bundeskriminalamt II/62, 78
Bundeskriminalamtgesetz II/78; III/63
Bundesseuchengesetz III/138; IV/79; V/96
Bundessozialhilfegesetz II/93; V/85; VI/97
Bundesstatistikgesetz IV/56
Bundesversorgungsgesetz IV/73
Bundeswehr VI/80

Bundeszentralregister ... II/51, 53; VI/135
Bundeszentralregisterauskunft ... IV/109
Bürgerbefragung ... VI/155
Bürgerbegehren ... VI/153
Bürgerkriegsflüchtlinge ... V/49
CD-ROM ... IV/22, 36
CERT ... IV/15
Chipkarten ... II/26; V/14; VI/95
Chipkarten im Zahlungsverkehr ... II/27; IV/21
Chipkarten im Gesundheitswesen ... II/27; IV/78
Chipkarten im öffentlichen Verkehr ... II/28
D-Info ... IV/22
Dateibeschreibung ... V/28; VI/125
Dateienregisterverordnung ... I/54; II/17, 63
Daten mit Doppelbezug ... III/108
Datenabgleich ... VI/98, 144
Datenautobahn ... III/28
Datenerhebung, unerlaubte ... IV/129
Datenerhebung bei Dritten ... VI/146
Datenscheckheft ... III/165
Datenschutz an Schulen ... IV/64, 65
Datenschutzordnung ... IV/25, 27
Datenschutzverordnung Schulwesen ... V/67
Datenspur ... VI/25
Datenträgerkontrolle ... III/13
Datentreuhänder ... III/108; IV/93
Datenverarbeitung im Auftrag II/9, 81, 110, 121; III/43, 141; IV/87; V/27, 120; VI/37, 44, 80, 82, 103, 113
Datenverarbeitungszentrum ... I/27
Datenvermeidung ... V/11
Deanonymisierung ... III/83
Demonstration ... II/73
Detekteien ... IV/35
Diagnose ... IV/74, 80; VI/104
Dienstanschlußvorschriften ... III/42
Dienstanweisung zum Datenschutz ... III/130; V/73
Dienstbesprechung ... VI/175
Dienstgespräche ... II/25; V/11, 24, 93, 117; VI/22
Dienstvereinbarung ... IV/128; V/22; VI/21
Dienstverhältnis ... IV/124
digitale Signatur ... V/105
Diplomarbeit ... VI/95
Diplomarbeiten-Datenbank ... II/98
Direktansprechen ... II/24
direktes Ablesen ... IV/128
Diskettenlaufwerke ... III/18
Drohanrufaufzeichnung ... II/24
Druckzentrum ... VI/103
EG-Umweltinformationsrichtlinie ... I/50 ff.

Ehe- und Jubiläumsdaten ... IV/32, 112; V/32
Ehemalige Einrichtungen ... II/37; V/99
Eigentumsübertragung ... V/36
Eigenunternehmen ... VI/147
Eignungsbedenken ... III/157
Einbürgerungsverfahren ... II/58
Eingabekontrolle ... III/15
Eingangspost ... III/153
Einigungsvertrag ... I/8, 15, 17 ff., 23, 27 f., 31, 33 ff., 38; III/92, 148
Einkommen ... VI/142
Einkommensnachweis ... V/50, 87, 114
Einkommensprüfung ... V/114
Einschulungsuntersuchung ... II/107; III/104; IV/83; VI/74
Einsichtsrecht ... IV/123 f., 126; V/145; VI/70, 71, 175
Einwilligungserklärung ... II/99, 115; III/103, 112, 137, 142, 145; IV/76 f., 86, 94; V/75, 87, 89; VI/79, 81, 106, 109, 118
Einzelverbindungsnachweis ... IV/22, 100; V/24
elektronische Geldbörse ... IV/21
elektronische Telefonverzeichnisse ... IV/22; VI/26
Elternbeiträge ... VI/87
Elternversammlungen ... II/93
Entsorgung von Datenträgern ... IV/16
Erforderlichkeitsprinzip ... IV/123
Erforderlichkeitsprüfung ... IV/46
Erhebungsbeauftragte ... III/77
Erhebungsbögen ... II/93; IV/83, 96, 110; VI/134
Ermessensspielraum ... III/82
Ermittlungsakten ... IV/45
Errichtungsanordnung ... II/75; IV/41
Erschließungsbeiträge ... IV/116
EU-Richtlinie ... IV/10; V/17
Europäische Gemeinschaft ... I/50, 57
EUROPOL ... V/37
Fahrerlaubnis ... VI/100
Fahrerlaubnis, Erst- und Wiedererteilung ... III/156; IV/103
Fahrerlaubnisregister ... VI/131
Fahrerlaubnisverordnung ... V/136
Fahrlehrer- und Fahrschulbestandsdatei ... III/155
faktische Anonymisierung ... III/84
faktischer Zwang ... II/43
Familienanamnese ... III/113; IV/94
Familienarchive ... II/96
Fehlzeiten ... III/147
Fernsehen ... VI/25
Fernwartung ... IV/122; V/95, 103; VI/127
Festnahmelisten ... IV/47
Feststellungsprüfung ... IV/63
Feuermeldeanlage ... III/17
Feuersozietät ... V/118

Finanzämter IV/34
Finanzkontrolle VI/167
Fingerabdruck II/63
Firewall VI/18, 125
Förderausschußverfahren III/101; VI/74, 75
Formulargestaltung IV/28; V/88, 91, 97, 101, 124, 136
Forschung I/48; II/99; III/142; IV/75, 87; V/33, 65, 75, 78; VI/72, 88
Förster IV/100
Fortbildungsveranstaltungen III/166
Fotoaufnahmen II/73
Fragebogen IV/129; V/77, 120
Fraktion II/34
Frauenförderverordnung IV/95
freie Träger VI/139
Freisprecheinrichtung II/22
Freiwilligkeit III/78; IV/78; V/89
Fremdarbeiter II/96
fremdenfeindliche Straftaten II/77
Führerschein IV/103
Führerscheinstellen V/136
Führungszeugnis IV/110
Fusion Berlin/Brandenburg III/38; IV/32
G 10-Gesetz II/59
Gauck-Behörde ..... I/21 ff., 34 f.; II/45
Gebäude- und Wohnungszählung IV/53
Gebäudesicherung III/16; IV/92; V/16; VI/124
Gebührendatenverarbeitung II/144; V/11, 93, 117; VI/20
Geburtsfälle II/106
Gefangene III/96; VI/42
Geheim- und Sabotageschutz V/144; VI/158
Geheimhaltungsregelungen IV/127
Geldwäschegesetz III/89
Gemeindeblatt IV/113
Gemeindeordnung VI/147
Gemeindeunfallversicherungsverband III/127
Gemeindevertretung VI/152
Gemeinsames Krebsregister IV/88, 90; V/96
gerichtliche Verfahrensweisen VI/68
Gerichtsverfassungsgesetz III/91
Gerichtsvollzieher II/88
Geschäftsstatistik IV/52; VI/63
Gesetz über Ordnungwidrigkeiten IV/46
Gesetzgebungsverfahren IV/103
gesetzliche Unfallversicherung IV/72, 73
Gesundheitsamt V/97-99, 120; VI/103, 106, 119, 149
Gesundheitsdienstgesetz II/104; IV/82; VI/105, 149
Gesundheitsfragebogen III/159
Gewahrsam IV/39

Gewalttäter Sport ... II/77
Gewerbeamt ... V/122
Gewerbeanzeige ... IV/108
Gewerbeordnung ... II/140; IV/108
Gewerbetreibende ... II/82
Glaubhaftmachung ... III/133, 145
Gleichstellungsbeauftragte ... II/101; III/44; IV/95
Großer Lauschangriff ... IV/39
GroupWise ... VI/19
Grundbuch ... I/51; III/93; VI/70
Grundgesetz ... I/18, 37, 49 f., 53; III/8, 10, 63, 73
Grundschulgutachten ... III/99, 101
Grundstücksverkehr ... V/36
Gutschein ... V/90
Handwerkskammer ... VI/133
Handy ... VI/24
Hauptausschuß ... II/34
Hausunterricht ... III/100
Hebamme ... III/134; IV/80
Heimarbeit ... VI/62
Hilfsmerkmal ... III/77
Hilfsmittelberatung ... II/121
Hochschuldirektorenkonferenz ... VI/94
Hochschulen ... II/97; VI/95
hoheitliche Aufgabe ... IV/115
Homosexualität ... VI/132
Honorarvertrag ... IV/129
Hotel-Meldeschein ... IV/113
Hundesteuer ... VI/123
Identitätsfeststellung ... IV/38
Identitätsnachweis ... II/57
Identity Protector ... V/10
illegale Beschäftigung ... V/84
Immatrikulation ... IV/69
Immissionsschutz ... II/135; V/112
Immunitätsrichtlinien ... II/34
Impfdateien ... III/137; IV/82, 112; V/98; VI/105, 149
Index Libi-Vorzeigekartei ... V/43
Industrie- und Handelskammer ... IV/110
Infektionsschutzgesetz ... VI/105
informationelle Gewaltenteilung ... III/78
Informationseingriff ... IV/39
Informationssysteme ... IV/20
Inhaltsdaten ... III/31
INPOL ... II/77, 79; IV/43
Insolvenzordnung ... VI/65
interaktives Fernsehen ... IV/17
Internet ... IV/15; VI/19

InVeKoS II/137; III/146; V/111
ISDN-Anlagen II/21; III/42, 164
IT-Grundschutzhandbuch IV/14
IT-Sicherheitshandbuch IV/14
Java IV/16
Jugendamt III/123, 144; IV/74, 96; V/77; VI/75, 83, 138, 141
Jugendhilfe ..... III/122 f.; VI/140
Justizmitteilungsgesetz VI/65
Justizverwaltungsmaßnahme IV/124
Justizvollzugsanstalt III/96; V/58
Kaderakten IV/123; V/143, 146; VI/159
Kaderakten der DDR ..... I/22 ff.
Kartenleser IV/128
Kassenarzt III/136
Katalogstraftaten IV/40
Katastrophenschutz II/81
Kinder- und Jugendhilfegesetz III/144
Kindergeldanspruch II/97; VI/87
Kindergeldzahlungen III/43
Kindertagesstätten-Betriebskostenverordnung IV/96
Kindesmißhandlung III/122
Kirchensteuer I/47
Kita-Elternbeiträge I/45; II/126; III/132; V/78
Kita-Gesetz V/78, 98; VI/87
Klassenlehrer III/104
klinische Arzneimittelprüfung III/138, 145
klinisches Krankheitsregister II/111
Kommunalabgaben IV/116
Kommunalaufsicht VI/173
Kommunale Statistikstellen IV/52; V/52
kommunales Vorkaufsrecht VI/128
Kommunalstatistik IV/52; VI/64
Kommunalverwaltung VI/136
Kommunalwahlen ..... II/50 f.
Konferenzschaltung II/23
Konfliktkommissionen III/92
Kontrollbefugnis des Landesbeauftragten für den Datenschutz IV/115; VI/103
Kontrollbesuch VI/85, 124, 160
Kontrollkompetenz V/115
Kontrollstellen des ökologischen Landbaus IV/97
Kontrollstellen IV/38, 42
Kopien IV/127; V/91
Kopiererfassungssystem VI/172
Korrespondenzen III/153
KpS-Richtlinien II/96
Kraftfahrsachverständigenregister IV/104
Kraftfahrzeughalterdaten II/130
Krankengeschichte II/38

Krankenhaus II/112; III/141; IV/86; V/100, 102; VI/108, 113
Krankenhausarchiv VI/117
Krankenhausgesellschaft III/143
Krankenhausseelsorger III/143
Krankenhauswanderer II/114; VI/116
Krankenkasse V/84, 86, 88; VI/103, 116
Krankenkassenbeitrag V/87
Krankenkassenwechsel V/88
Krankenunterlagen ..... IV/76 f.; V/86
Krankenversichertenkarte II/27; IV/78
Krankheitsregister ..... III/114; IV/90, 92; V/100 f.
Krebsregistergesetz II/123; III/115, 134; IV/88, 90; V/96; VI/118
Kreismeldekartei V/30; VI/43
Kriminalakten ..... II/62, 65 ff.; IV/45
Kriminalität II/78, 80; III/89
Kriminalpolizei II/64; VI/101
kryptographische Verfahren IV/122; VI/23
Kundendaten VI/26
Kündigungsschutzgesetz III/91
Kündigungsschutzprozeß III/91
künftiger Arbeitgeber III/40
Kurabgabe, Berechnung der IV/113
Ladendiebstahl II/66
Landesagentur für Struktur und Arbeit (LASA) II/16
Landesärztekammer II/118; III/135, 142
Landesaufnahmegesetz III/75
Landesbeamtengesetz III/39
Landesbeauftragter für den Datenschutz ..... I/5, 7 ff., 13, 36; IV/89
Landesgesundheitsamt II/107
Landesgleichstellungsgesetz II/100; III/44; IV/95
Landesjugendamt VI/82
Landeskartellbehörde VI/133
Landeskrankenhausgesetz II/109; IV/86
Landeskriminalamt II/60, 62
Landesrechnungshof VI/87, 167
Landesrettungsdienstplan V/98
Landesschiffahrtsverordnung VI/130
Landestierärztekammer IV/99
Landesversicherungsanstalt II/132
Landesverwaltungsnetz VI/17, 124
Landkarte IV/20
Landtag II/32; IV/26; V/19, 29
Landwirtschaftsanpassungsgesetz VI/121
Laptops II/20, 81
Lastenausgleichsämter II/145
Lebensversicherung VI/132
Lehrerbildungsgesetz VI/73
Lehrerfortbildung V/69

Leichenschauschein IV/81, 90, 112; V/99; VI/107
Lichtbilder III/96
Liegenschaftskataster V/35
Lohnsteuerkarte V/119; VI/37
Lokale Netze II/20; VI/18
Löschen III/17; VI/82, 84
Löschungsfristen IV/109
Maastricht II IV/13
Marketingfirmen VI/38
Matrikelnummer IV/71
Mediendienste VI/25
medizinisch-psychologische Gutachten V/136
Medizinischer Dienst der Krankenkassen III/128; IV/77; V/86
Medizinisches Forschungsgeheimnis IV/66
Meldebehörden ..... I/46; II/47, 52 ff., 56
Meldedaten II/40; IV/114
Meldegesetz I/55; II/12, 39, 47, 49, 107; V/30, 82; VI/43
Melderechtsrahmengesetz ..... I/27 f., 33 ff., 38, 44; II/38, 49
Melderegister ..... I/26 ff., 38 f., 56 f. (Anlage 8); II/41, 49 f., 52, 70
Melderegisterauskunft II/49
Meldeschein IV/113
Meldeverfahren VI/94
Meldewesen in der DDR ..... I/26 ff.
Meldewesen ..... I/37 ff., 55; II/38, 46; IV/30
Mietspiegel VI/127
Mikrozensus II/80; IV/56
mildestes Mittel III/136
MiStra VI/66
Mitarbeiter-bezogene Erfassung IV/128
Mitwirkungspflicht III/87, 128
MiZi VI/65
Mobilkommunikation VI/24
Mobiltelefon III/30
Mortalitäts-follow-up III/109
Müllidentifikationssystem IV/118
Musikschule VI/142
Muster-Dienstanweisung V/52; VI/62
Muster-Dienstvereinbarung IV/123; VI/22
Nachermittlungsverpflichtung IV/41
Nachrichtendienste II/79
Nachrichtensammelstelle IV/42
Namensnennung II/82
Namensschilder VI/115
Near Video on Demand IV/18
Neue Bundesländer II/49, 52; IV/87
Nicht-Störer IV/37
Nichtschülerprüfung III/99
Normenklarheit III/76

Notarzteinsatz ... II/122
Notebook ... VI/127
Notenbuch ... V/70
Notenlisten ... III/103
Nutzungsprofile ... VI/27
Observation ... IV/40
Online-Zugriff ... III/123; V/34
Online-Dienste ... IV/19
Ordnungsamt ... IV/46
Organisationskontrolle ... III/16
organisatorische Trennung ... III/85; IV/91
Organisierte Kriminalität ... IV/40; V/40
Organspendeausweis ... IV/84, 89
Ortszuschlag ... V/148
Outsourcing ... V/19; VI/113, 146
Paginierungspflicht ... IV/123
Parallelverfahren ... VI/68
Parlamentsklausel ... IV/25
Parteien ... II/49
Paßwörter ... III/18; V/102; VI/126
Patientenakten ... I/4, 22 ff., 52; II/28; V/99; VI/110
Patientendaten ... III/141; IV/78, 86; V/85
Patientenliste ... III/143
Pay-per-Channel ... IV/18
Pay-per-View ... IV/18
Personalakten ... II/42 f., 102; III/39 f.; IV/122 ff.; V/142
Personalaktenführung ... III/39; V/142; VI/157
Personalausweis ... II/39, 48, 56, 72; IV/105
Personalausweisgesetz ... II/48
Personalentwicklung ... VI/169
Personalienüberprüfung ... IV/38
Personalinformationssystem ... III/40; IV/122; VI/177
Personalnachrichten ... V/147; VI/175
Personalrat ... V/22, 94
Personalratsbüro ... V/149
Personalvertretung ... II/46
Personalvertretungsgesetz ... II/46
Personalverwaltung ... IV/123 f.
Personalwirtschaft ... IV/123
personelle Trennung ... III/85; IV/91
Personendaten ... II/61
Personendatenbank der DDR ... I/26 ff., 37 (Anlage 3)
Personenfahndung ... II/70
Personenkennzahl ... I/26 ff., 33 ff.
Personenstandsgesetz ... VI/52
Personenstandswesen ... IV/68; V/33
Petentenschutz ... VI/39
Petition ... IV/26

Petitionsausschuß ... II/34
Pflanzenschutzsachkundeverordnung ... II/141
Pflegeversicherung ... III/128; IV/73
Planfeststellungsverfahren ... IV/116
Platzverweise ... IV/42
Polizei ... II/38, 59 ff., 70, 73, 77; III/125
polizeiliche Beobachtung ... IV/40
Polizeiliches Informations- und Kommunikationssystem ... IV/44
Postöffnung ... III/131
Postpaid-Verfahren ... II/30
Poststelle ... III/153; VI/83
Prepaid-Verfahren ... II/30
Presse ... VI/173
Pressekonferenz ... II/74
Primärstatistik ... III/79, 83
private Straßenfläche mit öffentlichem Verkehr ... III/161
privater PC ... II/84; III/103; IV/62 f.
Privatgespräche ... V/11, 24, 93, 117; VI/21
Privatpost ... VI/113
Promotion ... IV/70
Protokollierung ... III/89; IV/41, 122; V/104; VI/19, 126
Prüffälle ... IV/49
Prüffristen ... IV/109
Pseudonymisierung ... V/11, 79
Psychisch-Kranken-Gesetz ... II/111; IV/84; VI/107
Rasterfahndung ... IV/40
räumliche Trennung ... IV/126
Raumsicherung ... III/16; VI/124
Recherchen ... IV/122
Rechnungsprüfungsamt ... VI/167
Recht auf informationelle Selbstbestimmung ... I/4, 6 f., 36, 46; III/8 f., 28, 63, 78, 94, 106; VI/81
Rechteverwaltung ... III/18; IV/122; V/102
Rechtsanwalt ... III/87
Rechtsanwaltskammer ... III/87
Rechtsreferendarprüfung ... II/89
Rechtsstreit ... III/145
Registerauskunft ... III/161
Registriernummer ... IV/128
Rehabilitierungsverfahren ... III/93
Religionsgemeinschaften ... VI/44
Religionsgesellschaft ... V/30
Rentenleistungen ... II/132
Rentenversicherung ... IV/72
Restitutionsansprüche ... II/39
Rettungsdienst- und Notarzteinsatzprotokolle ... II/122
Rettungsdienstgesetz ... VI/106
richterliche Unabhängigkeit ... IV/124
Risikofaktoren ... III/16

Router VI/125
Rückmeldeverfahren IV/46
Rückmeldungen III/80
Rücksendepflicht IV/126
Rufnummer VI/21
Rufnummernanzeige II/22
Rundfunk VI/25
Rundfunkgebühreneinzug V/31
Sachenrechtsbereinigungsgesetz VI/71
Sanierungsmaßnahmen IV/114; V/115
Satellitenüberwachung II/137
Scheinehe V/51
Schiedskommissionen III/92
Schleuser II/76
Schlüssellösung II/50, 71
Schuldnerverzeichnis III/88; IV/58
Schuldrechtsänderungsgesetz VI/71
Schülerausweis VI/80, 82
Schülerpraktikum III/102
Schülerunterlagen ..... III/97 f.; V/68, 70, 71
Schulleiter III/105; VI/76
Schulpsychologische Beratung II/91; V/68
Schulreihenuntersuchung V/120
Schulverwaltungsprogramm VI/80
Schulverwaltungssystem V/73
Schutzstufenkonzept III/29; IV/14
Schwangerschaftskonfliktberatung II/127; III/132
Schwerbehindertenvertretung VI/171
SED-Unrechtsbereinigungsgesetz, Zweites III/87
SED-Unrechtsbereinigungsgesetz, Erstes II/88
Sekundärstatistik III/79, 83; IV/58
Selbstangabeformular IV/50
Selbstauskunftsbogen VI/148
Service on Demand IV/18
Set-Top-Box IV/18
Seuchenmeldeverordnung V/96
Sicherheitsempfehlung IV/14
Sicherheitssoftware VI/127
Sicherheitsüberprüfung IV/44; VI/56, 81
Software VI/53
Sorgerecht VI/138, 140
Sozialamt III/133; IV/74; V/89; VI/141, 143, 145
Sozialauswahl III/91
Sozialdaten . . I/(Anlage 7); II/95, 128; III/119 f., 122, 125, 151; IV/73; V/92, 93; VI/84, 98, 103, 141
Sozialgeheimnis II/11; III/120, 129, 151
Sozialhilfeermittler VI/145
Sozialleistungsträger III/154; VI/85
Sozialversicherungsträger VI/98, 100

Speicherkontrolle ... III/13
speichernde Stelle ... II/47; III/103, 105
Speicherung ... III/129
Staatsanwaltschaft ... IV/46; V/60; VI/67
Staatskirchenvertrag ... III/117; V/81
Staatsvertrag ... VI/35
Stammdatensatz ... III/124
Standardsoftwaresysteme ... II/21
Standesamt ... VI/156
Stasi-Unterlagen ... I/21 f., 34 f., 49; II/35, 39, 45; IV/125
Statistik ... II/80; IV/51
Statistikgeheimnis ... II/12; IV/52
Statistikregistergesetz ... VI/58
statistische Fragebogen ... III/77
Statistischer Beirat ... VI/60
Steuergeheimnis ... II/11; IV/117; VI/123
Steuernummer ... IV/110
Störer ... IV/37
Strafprozeßordnung ... V/55
Straftat ... II/66 f., III/122; IV/37
Straftatenkatalog ... IV/40
Strafverfahren ... III/125
Strafverfahrensänderungsgesetz ... II/85
Strafverfolgung ... II/79
Strafvollzug ... III/94
Studentenakten ... I/22, 24 ff.
Stundung ... VI/134
Stundungsantrag ... IV/117
Täter-Opfer-Ausgleich ... V/58, 66
technisch-organisatorische Maßnahmen ... III/39
Teilakten ... IV/123
Teilnehmerlisten ... V/21; VI/86
Telearbeit ... VI/27, 62
Telefax ... II/31; V/15
Telefon, schnurloses ... III/32
Telefonbuchverlage ... IV/109
Telefongebühren ... IV/100; V/11, 22; VI/21
Telefongespräche ... IV/100; V/93
telefonische Auskünfte ... III/152; VI/157
Telefonüberwachungsmaßnahmen ... V/38, 60
Telefonwahlverbindungen ... III/41
Teleheimarbeitsplatz ... VI/62
TELEKOM ... IV/22
Telekommunikation ... II/143; IV/22; V/11; VI/26
TeleKommunikationsverbund ... VI/20
terroristische Vereinigung ... IV/46
Tierschutz ... V/107, 108
Tierschutzgesetz ... VI/120

Tierseuchenkasse ... II/139; III/147
Tierzuchtgesetz ... VI/119
TK-Anlage ... V/11, 22, 93, 117
Totenscheine ... II/105
Transfusionsgesetz ... VI/104
Transplantationsgesetz ... II/124; IV/89
Transportkontrolle ... III/15
Trennungsgebot ... III/77; IV/123
Trust-Center ... V/105; VI/24
Tumorbasisdokumentation ... VI/118
Übermittlung von Sozialdaten ... III/154; IV/75, 77; VI/101
Übermittlungsersuchen ... III/154
Übermittlungskontrolle ... III/14
Überprüfung von Bediensteten ... II/44; IV/125; V/144
Umweltbehörden ... II/133
Umweltinformationsgesetz ... II/133; IV/102
unabhängige Kontrollinstanz ... III/77
Unfallversicherungseinordnungsgesetz ... V/85
unlauterer Wettbewerb ... IV/111
Unschädlichkeitszeugnisse ... V/36
Unterbindungsgewahrsam ... IV/39
Unterhaltspflicht ... II/120; III/122; VI/138, 142
Unternehmensregister ... VI/59
Untersuchungsausschuß ... II/34
Untersuchungshaftvollzugsgesetz ... V/54
Verarbeitungsverbund ... IV/122
Verbindungsdaten ... III/31; IV/100; V/11, 23, 93; VI/21
Verbrechensbekämpfungsgesetz ... II/86; III/62; IV/59
Verdachtsfälle ... IV/49
verdeckte Datenerhebung ... IV/37
verdeckter Ermittler ... IV/39
Verfahrenseinstellung ... IV/46
verfahrensrechtliche Schutzvorkehrungen ... III/91
Verfassung ... V/29
Verfassungsgericht ... V/29
Verfassungsschutz ... II/56, 59
Verfassungsschutzgesetz ... I/52
Verfassungstreue ... I/18 ff.
Verhaltens- und Leistungskontrolle ... V/94
Verhältnismäßigkeit ... III/77, 88
Verkehrserhebung ... VI/61
Verkehrszentralregister ... VI/131
Vermögensfragen ... II/145
Vernichtung ... IV/124
Verpflichtungsgesetz ... IV/98
Versammlungsfreiheit ... II/73
verschlossen kuvertiert ... III/153; IV/77
Verschlüsselung ... IV/42, 80, 91; V/32, 105; VI/23, 29, 177

Vertraulichkeit IV/123; VI/18
Verwaltungsverfahrensgesetz VI/32
Verwaltungsvorschriften zum Ausländergesetz III/75
Video on Demand IV/18
Video-Games IV/18
Videoaufnahmen ..... II/73 f.
Videoüberwachung III/17; IV/25
Vier-Augen-Prinzip III/14
Volkspolizeikreisämter II/38
Volkszählung 2001 ..... V/53
Volkszählung VI/59
Volkszählungsurteil I/6; III/101, 123
Vorakten VI/159
Vorläufige Verwaltungsvorschriften zum Bbg DSG III/39
Vorlesungsverzeichnis V/80
Wachschutzdienste III/17
Wahlen II/49; III/86
Wahlgeheimnis III/81
Wahlrecht II/51, 52
Wald V/109
Wartung und Fernwartung II/11, 110; III/47; IV/24, 87; V/27; VI/84
Wasser- und Abwasserzweckverbände VI/148
Weitverkehrsnetze II/20
Wesensgehaltsgarantie IV/40
Wettbewerbszentrale IV/111
Widerspruchsrecht II/41, 50; IV/94, 113; V/101; VI/45
Wildhandelsüberwachungsverordnung IV/101
Wirtschaftlichkeitsprüfung VI/169
Wirtschaftsklausel II/99
Wohnberechtigungsschein V/135
Wohngeld III/151
Wohngeldstelle III/151
Wohngeldverfahren III/149; VI/23
Wohnungsbauförderung II/141; V/115
Wohnungskartei III/148; V/116
Wohnungsstatistik IV/53
Wohnungsstatistikgesetz II/80; III/76, 79
World Wide Web IV/15
WWW-Server VI/19, 126
ZBB IV/129; V/148
Zeiterfassungssysteme, automatische IV/128
Zentrale Rechnungserfassung II/114
Zentrale Adoptionsstelle VI/82
Zentrale Bußgeldstelle V/40
Zentrales Einwohnerregister ..... I/27 ff., 38 f., 47; II/39; IV/103
Zentrales Fahrerlaubnisregister IV/103
Zentralregister für Zirkusbetriebe V/107; VI/120
Zentralregisterauszug V/125, 136

Zentralstelle für Projektentwicklung ..... I/28 ff.
Zeugen in Strafprozessen VI/69
Zeugen in Untersuchungsausschüssen I/49
Zeugnis III/105; VI/79
Zeugnisverweigerungsrecht III/108, 125
ZIS II/78
Zugangskontrolle III/12
Zugangsrecht IV/123
Zugriffskontrolle III/14
Zugriffssperre III/123; IV/128
Zuordnungsmerkmal III/154
Zusatzfragebogen ..... I/18 ff.
Zuverlässigkeitsüberprüfung II/58; IV/111
Zwangsvollstreckungsverfahren III/88
Zweckbindung II/91; IV/86, 123
Zweckverbände VI/146

Abkürzungsverzeichnis

1. SKWPG	=	Erstes Gesetz zur Umsetzung des Spar-, Konsolidierungs- und Wachstumsprogramms
1. SRG	=	Erstes Schulreformgesetz für das Land Brandenburg
2. MeldDÜÄV	=	Zweite Verordnung zur Änderung der Verordnung über regelmäßige Datenübermittlungen der Meldebehörden
2. SGBÄndG	=	2. Gesetz zur Änderung des Sozialgesetzbuches
a. F.	=	alte Fassung
ABl.	=	Amtsblatt
Abs.	=	Absatz
Abschn.	=	Abschnitt
AbwAG	=	Abwasserabgabengesetz
ADV	=	Automatische Datenverarbeitung
AFIS	=	Automatisiertes Fingerabdruck-Identifizierungssystem
AfNS	=	Amt für Nationale Sicherheit
AG	=	Ausführungsgesetz
AGE	=	Autobahngebührenerfassungssystem
AgrStaG-DVO	=	Verordnung über die Durchführung des Agrarstatistikgesetzes
AGTierSGBbg	=	Gesetz zur Ausführung des Tierseuchengesetzes
AIG	=	Akteneinsichts- und Informationszugangsgesetz
AKIS	=	Investitionsförderung zur Verbesserung der Effizienz der Agrarstruktur
ALK	=	Automatisierte Liegenschaftskarte
AMG	=	Arzneimittelgesetz
Änd.	=	Änderung
Anl.	=	Anlage
AO	=	Abgabenordnung
AO-GS	=	Ausbildungsordnung der Grundschule im Land Brandenburg
AOK	=	Allgemeine Ortskrankenkasse
APOmJD	=	Ausbildungs- und Prüfungsordnung mittlerer Justizdienst
Art.	=	Artikel
Ärzte-ZV	=	Zulassungsordnung für Vertragsärzte
ASMK	=	Arbeits- und Sozialministerkonferenz
ATKIS	=	Amtliches topographisch-kartographisches Informationssystem
Aufl.	=	Auflage
AufnV	=	Verordnung über die Aufnahme in weiterführende Schulen des Landes Brandenburg
AuslG	=	Gesetz über die Einreise und den Aufenthalt von Ausländern im Bundesgebiet
AV	=	Allgemeine Verfügung
AVA	=	Automatisierten Vorgangstagebuchs
AWMF	=	Arbeitsgemeinschaft der Wissenschaftlichen Medizinischen Fachgesellschaften
AZV	=	Abfallzweckverband
BAFI	=	Bundesamt für die Anerkennung ausländischer Flüchtlinge
BAföG	=	Bundesausbildungsförderungsgesetz
BauGB	=	Baugesetzbuch
BbgDSG	=	Brandenburgisches Datenschutzgesetz
Bbg.	=	Brandenburgisch(es)
BbgAbfG	=	Brandenburgisches Abfallgesetz

BbgArchG	=	Brandenburgisches Architektengesetz
BbgArchivG	=	Brandenburgisches Archivgesetz
BbgBO	=	Brandenburgische Bauordnung
BbgGDG	=	Brandenburgisches Gesundheitsdienstgesetz
BbgMeldeG	=	Brandenburgisches Meldegesetz
BbgPAuswG	=	Brandenburgischen Personalausweisgesetz
BbgPolG	=	Brandenburgisches Polizeigesetz
BbgPsychKG	=	Brandenburgisches Psychisch-Kranken-Gesetz
BbgRAVG	=	Brandenburgisches Rechtsanwaltsversorgungsgesetz
BbgRettG	=	Brandenburgisches Rettungsdienstgesetz
BbgSchulG	=	Brandenburgisches Schulgesetz
BbgVerf	=	Brandenburgische Verfassung
BbgVerfSchG	=	Brandenburgisches Verfassungsschutzgesetz
BBiG	=	Berufsbildungsgesetz
BDSG	=	Bundesdatenschutzgesetz
BdVP	=	Bezirksdirektionen der Volkspolizei
BfD	=	Bundesbeauftragter für den Datenschutz
BFSV	=	Berufsfachschulverordnung
BGB	=	Bürgerliches Gesetzbuch
BGBl.	=	Bundesgesetzblatt
BKA	=	Bundeskriminalamt
BKAG	=	Bundeskriminalamtgesetz
BKAG-E	=	Bundeskriminalamtgesetz-Entwurf
BKA-Gesetz	=	Bundeskriminalamtgesetzes
BKGG	=	Bundeskindergeldgesetz
BlnDSG	=	Berliner Datenschutzgesetz
BLVS	=	Landesamt für Verkehr und Straßenbau Brandenburg
BLZpB	=	Brandenburgischen Zentralstelle für politische Bildung
BML	=	Bundesministerium für Ernährung, Landwirtschaft und Forsten
BND	=	Bundesnachrichtendienst
BR-Drs.	=	Bundesrats-Drucksache
BschG	=	Brandschutzgesetz
BSI	=	Bundesamt für Sicherheit in der Informationstechnik
BSS	=	Basisstationen
BSeuchenG	=	Bundesseuchengesetz
BSHG	=	Bundessozialhilfegesetz
BbgSozBerG	=	Brandenburgische Sozialberufsgesetz
BStatG	=	Bundesstatistikgesetz
BStU	=	Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR
BT-Drs.	=	Bundestags-Drucksache
Buchst.	=	Buchstabe
Bundes-SISY	=	bundesweites staatsanwaltschaftliches Informationssystem
BVerfGE	=	Bundesverfassungsgerichtsentscheidung
BZR	=	Bundeszentralregister
BZRG	=	Bundeszentralregistergesetz
bzw.	=	beziehungsweise
ca.	=	circa

CD-ROM	=	Compact Disc - Read Only Memory
CERT	=	Computer Emergency Response Team
DAV	=	Verwaltungsvorschrift über die Errichtung und Benutzung dienstlicher Telekommunikationsanlagen für die Verwaltung des Landes Brandenburg
DBeschrV	=	Verordnung zur Dateibeschreibung
DDR-GBl.	=	DDR-Gesetzblatt
DES	=	Data Encryption Standard
DFG	=	Deutsche Forschungsgemeinschaft
d. h.	=	das heißt
DIN	=	Deutsches Institut für Normung
DORA	=	Dialogorientiertes Recherche- und Auskunftssystem
DSVS	=	Datenschutzverordnung Schulwesen
DV	=	Datenverarbeitung
DVO	=	Durchführungsverordnung
EAGFL	=	Europäischen Ausrichtungs- und Garantiefonds für die Landwirtschaft
ed-Behandlung	=	erkennungsdienstliche Behandlung
EDU	=	European Drug Unit
EG	=	Europäische Gemeinschaft
EGBGB	=	Einführungsgesetz zum Bürgerlichen Gesetzbuch
ELSBB	=	Einsatzleitsystem für die Brandenburgische Polizei
EMRK	=	Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten
EPV	=	Verordnung über die Ergänzungsstudien und Ergänzungsprüfungen für Lehrämter an Schulen (Ergänzungsprüfungsverordnung)
EU	=	Europäische Union
EU-DSRL	=	EU-Datenschutzrichtlinie
EuGH	=	Europäischer Gerichtshof
EUROPOL	=	Europäisches Polizeiamt
EuWG	=	Europawahlgesetz
e. V.	=	eingetragener Verein
FDGB	=	Freier Deutscher Gewerkschaftsbund
FeV	=	Fahrerlaubnis-Verordnung
ff.	=	folgende
FrauFöV	=	Frauenförderungsverordnung
GastVO	=	Verordnung zur Ausführung des Gaststättengesetzes
geänd.	=	geändert
GEK	=	Kohortenstudie „Gesundheit, Ernährung, Krebs“
gem.	=	gemäß
Ges.	=	Gesetz
GewAnzVwV	=	Allgemeine Verwaltungsvorschrift zur Durchführung der Gewerbeordnung
GewO	=	Gewerbeordnung
GEZ	=	Gebühreneinzugszentrale
GG	=	Grundgesetz
GGG	=	Gesetz über die gesellschaftlichen Gerichte der DDR
GIS	=	Geographische Informationssysteme
GKG	=	Gesetz über kommunale Gemeinschaftsarbeit im Land Brandenburg
GKR	=	Gemeinsames Krebsregister
GmbH	=	Gesellschaft mit beschränkter Haftung
GMBl.	=	Gemeinsames Ministerialblatt

GO	=	Gemeindeordnung
GPS	=	Global Positioning System
GUZ	=	Gesetzes über Unschädlichkeitszeugnisse im Grundstücksverkehr
GVBl.	=	Gesetz- und Verordnungsblatt
GWG	=	Geldwäschegesetz
G 10	=	Gesetz zu Artikel 10 Grundgesetz
G 10 AG Bbg	=	Gesetz zur Ausführung des Gesetzes zu Art. 10 Grundgesetz im Land Brandenburg
HebBOBbg	=	Berufsordnung für Hebammen und Entbindungspfleger im Land Brandenburg
HeilBerG	=	Heilberufsgesetz
HKR	=	Haushalt-, Kassen-, Rechnungswesen
HRK	=	Hochschuldirektorenkonferenz
i. d. Fass.	=	in der Fassung
IfSG	=	Infektionsschutzgesetz
IHK	=	Industrie- und Handelskammer
IHK-G	=	IHK-Gesetz
ILB	=	Investitionsbank des Landes Brandenburg
IMEI	=	International Mobile Station Equipment Identity - Endgerätekennung
IMSI	=	International Mobile Subscriber Identity - netzinterne Teilnehmerkennung
INPOL	=	Informationssystem der Polizei
InVeKoS	=	Integriertes Verwaltungs- und Kontrollsystem
ISDN	=	Integrated Services Digital Network (dienste-integrierendes Digitalnetz)
ISO	=	International Organization for Standardization
i. S. v.	=	im Sinne von
ISVB	=	Informationssystem für Verbrechensbekämpfung Berlin
i. V. m.	=	in Verbindung mit
IuK-Technik	=	Informations- und Telekommunikationstechnik
JMBl.	=	Justizministerialblatt
JVA	=	Justizvollzugsanstalt
KA	=	Kriminalakte
KAG	=	Kommunalabgabengesetz
KAN-BB	=	Kriminalaktennachweis Land Brandenburg
Kap.	=	Kapitel
KBA	=	Kraftfahrt-Bundesamt
KHDsV	=	Verordnung zum Schutz von Patientendaten im Krankenhaus
KHIS	=	Krankenhausinformationssystems
KitaBKV	=	Kindertagesstätten-Betriebskostenverordnung
Kita-Gesetz	=	Zweites Gesetz zur Ausführung des Achten Buches des Sozialgesetzbuches - Kinder- und Jugendhilfe - Kindertagesstättengesetz
KJGDV	=	Verordnung über die Aufgaben des Kinder- und Jugend-Gesundheitsdienstes der Gesundheitsämter im Land Brandenburg
KJHG	=	Kinder- und Jugendhilfegesetz
KKO	=	Konfliktkommissionsordnung
KOVVfG	=	Gesetz über das Verwaltungsverfahren der Kriegsopferversorgung
KRG	=	Krebsregistergesetz
KVBB	=	Kassenärztliche Vereinigung Brandenburg
LAG	=	Landesarbeitsgruppe
LAN	=	Local Area Network
LBG	=	Landesbeamtengesetz

LDS	=	Landesamt für Datenverarbeitung und Statistik
LDSG	=	Landesdatenschutzgesetz
LELF	=	Landesamt für Ernährung, Landwirtschaft und Flurneuordnung
LfD	=	Landesbeauftragter für den Datenschutz
LfV	=	Landesamt für Verfassungsschutz
LGG	=	Landesgleichstellungsgesetz
LHA	=	Landeshauptarchiv
LHO	=	Landeshaushaltsordnung
LiKaDÜV	=	Verordnung über die Einrichtung automatisierter Abrufverfahren und regelmäßiger Datenübermittlungen im Liegenschaftskataster
LImschG	=	Vorschaltgesetz zum Immissionsschutz
LJA	=	Landesjugendamt Brandenburg
LKA	=	Landeskriminalamt
LKGBbg	=	Krankenhausgesetz des Landes Brandenburg
LPG	=	Landwirtschaftliche Produktionsgenossenschaft
LSchiffV	=	Landesschiffahrtsverordnung
LSPV	=	Lehrerstellen- und Personalverwaltung
LT-Drs.	=	Landtags-Drucksache
LVK	=	Lichtbildvorzeigekartei
LVN	=	Landesverwaltungsnetz
LwAnpG	=	Landwirtschaftsanpassungsgesetz
MAC	=	Medium Access Control
MASGF	=	Ministerium für Arbeit, Soziales, Gesundheit und Frauen
MBJS	=	Ministerium für Bildung, Jugend und Sport
MdF	=	Ministerium der Finanzen
MdJBE	=	Ministerium der Justiz und für Bundes- und Europaangelegenheiten
MDK	=	Medizinischen Dienst der Krankenkassen
MDS	=	Spitzenverband der medizinischen Dienste der Krankenversicherungen
MeldDÜÄV	=	Änderung der Verordnung über regelmäßige Datenübermittlungen der Meldebehörden
MeldDÜV	=	Verordnung über regelmäßige Datenübermittlungen der Meldebehörden
MELF	=	Ministerium für Ernährung, Landwirtschaft und Forsten
MESTA	=	Mehrländer-Staatsanwaltschaft-Automation
MfS	=	Ministerium für Staatssicherheit
MI	=	Ministerium des Innern
MiStra	=	Anordnung über Mitteilungen in Strafsachen
MOD	=	Magneto-optische Datenträger
MSWV	=	Ministerium für Stadtentwicklung, Wohnen und Verkehr
MUNR	=	Ministerium für Umwelt, Naturschutz und Raumordnung
MWFK	=	Ministerium für Wissenschaft, Forschung und Verkehr
MW	=	Ministerium für Wirtschaft, Mittelstand und Technologie
NADIS	=	Nachrichtendienstliches Informationssystem der Verfassungsschutzbehörden
NASISTE	=	Nachrichtensammelstelle
n. F.	=	neue Fassung
Nr.	=	Nummer
NSIS	=	Nationales Schengener Informationssystem
OEG	=	Opferentschädigungsgesetz
o. g.	=	oben genannte
OP	=	Operation

ÖPNV	=	Öffentlicher Personennahverkehr
ORB	=	Ostdeutscher Rundfunk Brandenburg
OWiG	=	Gesetz über Ordnungswidrigkeiten
PAK	=	Personenarbeitskartei
PaßG	=	Paßgesetz
PAuswG	=	Personalausweisgesetz
pB	=	Polizeiliche Beobachtung
PC	=	Personalcomputer
PersVG	=	Landespersonalvertretungsgesetz
PflRi	=	Pflegebedürftigkeits-Richtlinien
PHW	=	personenbezogener Hinweis
PolG	=	Polizeigesetz
POLIKS BB/BR	=	Polizeiliches Informations- und Kommunikationssystem Brandenburg/Berlin
PO-Nsch	=	Nichtschülerprüfungsordnung
PrüfBerV	=	Prüferberufungsverordnung
PStG	=	Personenstandsgesetz
PTRegG	=	Gesetz über die Regulierung der Telekommunikation und des Postwesens
RAK	=	Referatsarbeitskartei
RSA-Algorithmus	=	nach den Entwicklern Rivest, Shamir und Adleman
RTK	=	Rasterdaten topographischer Karten
RVO	=	Reichsversicherungsordnung
S.	=	Seite
s.	=	siehe
Sachgeb.	=	Sachgebiet
SchG	=	Schiedsstellengesetz
SCHUFA	=	Schutzgemeinschaft für allgemeine Kreditsicherung GmbH
SchuVVO	=	Verordnung über das Schuldnerverzeichnis
SchwbG	=	Schwerbehindertengesetz
SDÜ	=	Schengener Durchführungsübereinkommen
SGB	=	Sozialgesetzbuch
SIS	=	Schengener Informationssystem
SozhiDAV	=	Sozialhilfedatenabgleichsverordnung
SopEPV	=	Verordnung über das Ergänzungsstudium und die Ergänzungsprüfung in Sonderpädagogik (Sonderpädagogik-Ergänzungsprüfungsordnung)
SopV	=	Verordnung über Unterricht und Erziehung für junge Menschen mit sonderpädagogischem Förderbedarf
SozBFSV	=	Verordnung über den Bildungsgang zum Erwerb eines Berufsabschlusses nach Landesrecht in den Sozialberufen an der Berufsfachschule
SrV	=	System repräsentativer Verkehrserhebung
StA	=	Staatsanwaltschaft
StADÜV	=	Steueranmeldungs-Datenübermittlungs-Verordnung
StGB	=	Strafgesetzbuch
StPO	=	Strafprozeßordnung
StUG	=	Stasi-Unterlagen-Gesetz
StVG	=	Straßenverkehrsgesetz
StVollzG	=	Strafvollzugsgesetz
StVZO	=	Straßenverkehrszulassungsordnung
SÜG	=	Sicherheitsüberprüfungsgesetz

SVRV	=	Sozialversicherungsrechnungsverordnung
TB	=	Tätigkeitsbericht
TDSV	=	Telekom-Datenschutzverordnung
TFH	=	Technische Fachhochschule Wildau
TierSchG	=	Tierschutzgesetz
TierSchTrV	=	Tierschutztransportverordnung
TK	=	Telekommunikation
TSK	=	Tierseuchenkasse
TÜ-Maßnahmen	=	Telefonüberwachungsmaßnahmen
u. a.	=	unter anderem
UAG	=	Untersuchungsausschußgesetz
UIG	=	Umweltinformationsgesetz
u. U.	=	unter Umständen
UVEG	=	Unfallversicherungseinordnungsgesetz
UVollzG	=	Untersuchungshaftvollzugsgesetz
UWG	=	Gesetz gegen den unlauteren Wettbewerb
VDMA	=	Verband Deutscher Maschinen- und Anlagenbau e.V.
VermLiegG	=	Vermessungs- und Liegenschaftsgesetz
VersammlG	=	Versammlungsgesetz
VGH	=	Verfassungsgerichtshof
vgl.	=	vergleiche
VGO	=	Vollzugsgeschäftsordnung
VGPolGBbg	=	Vorschaltgesetz zum Polizeigesetz des Landes Brandenburg
VPKÄ	=	Volkspolizeikreisämter
VV	=	Verwaltungsvorschrift
VV-Betriebspraktika	=	Verwaltungsvorschriften über die Durchführung von Schülerbetriebspraktika
VV-Datenschutz/ Statistik	=	Verwaltungsvorschriften über den Schutz personenbezogener Daten in Schulen und über statistische Erhebungen
VV-Hauunt	=	Verwaltungsvorschriften über die Durchführung von Hausunterricht
VV-Schulakten	=	Verwaltungsvorschriften über Akten an Schulen in öffentlicher Trägerschaft
VV-WissU	=	Verwaltungsvorschrift über wissenschaftliche Untersuchungen an Schulen
VwGO	=	Verwaltungsgerichtsordnung
VwVfGBbg	=	Verwaltungsverfahrensgesetz des Landes Brandenburg
VZR	=	Verkehrszentralregister
WildÜV	=	Wildhandelsüberwachungsverordnung
WissUV	=	Verordnung über die Genehmigung wissenschaftlicher Untersuchungen an Schulen
WoBelegG	=	Gesetz über die Gewährleistung von Belegungsrechten im kommunalen und genossenschaftlichen Wohnungswesen
WoBindG	=	Wohnungsbindungsgesetz
WoGG	=	Wohngeldgesetz
WoGSoG	=	Wohngeldsondergesetz
WORM	=	Write Once Read Many
WoStatG	=	Wohnungsstatistikgesetz
WWW	=	World Wide Web
ZABB	=	Zentrale Adoptionsstelle Berlin-Brandenburg
ZBB	=	Zentrale Bezügestelle des Landes Brandenburg
Ziff.	=	Ziffer
ZPO	=	Zivilprozeßordnung

ZTB	=	Zentraldienst der Polizei für Technik und Beschaffung
zul.	=	zuletzt
z. Z.	=	zur Zeit