LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 4/2078**

4. Wahlperiode **23.01.2006**

UNTERRICHTUNG

durch den Landesbeauftragten für den Datenschutz

Siebter Tätigkeitsbericht gemäß § 33 Absatz 1 des Landesdatenschutzgesetzes von Mecklenburg-Vorpommern (DSG M-V)

und

Zweiter Tätigkeitsbericht gemäß § 38 Absatz 1 des Bundesdatenschutzgesetzes (BDSG)

Vorwort

Der vorliegende Siebte Tätigkeitsbericht dokumentiert Kontinuität und Wandel in der Arbeit des Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern in den Jahren 2004 und 2005. Unter Leitung meines Amtsvorgängers, Herrn Dr. Werner Kessel, hat sich die Behörde zu einer leistungsstarken und über das Land hinaus akzeptierten Datenschutzinstanz entwickelt. Fast zeitgleich mit dem Amtswechsel wurde mir die Zuständigkeit für den nicht-öffentlichen Bereich übertragen. Damit berate und kontrolliere ich in nahezu allen Bereichen des gesellschaftlichen Lebens (mit Ausnahme der Bundesbehörden sowie Kernbereichen der Kirchen und des öffentlich-rechtlichen Rundfunks) in Mecklenburg-Vorpommern. Dieser Aufgabe versuche ich durch effektiven Einsatz meiner Mitarbeiterinnen und Mitarbeiter und durch zweckmäßige Verwendung der finanziellen Ressourcen meines Amtes, aber auch durch eine teilweise Neuausrichtung der Tätigkeit gerecht zu werden.

Diese Aspekte spiegeln sich im vorliegenden Tätigkeitsbericht wider. In Anlehnung an die Zuständigkeitsverteilung innerhalb des Landtages und der Landesregierung habe ich den Bericht neu gegliedert. Die Darstellung von Einzelfällen wurde in der Regel um generelle Empfehlungen ergänzt, die sich an den Landtag und die Landesregierung mit dem Ziel wenden, zu einer nachhaltigen Verbesserung des Schutzes des verfassungsmäßigen Rechtes auf informationelle Selbstbestimmung der Bürgerinnen und Bürger in Mecklenburg-Vorpommern beizutragen.

Die Darstellung der einzelnen Sachverhalte in anonymisierter Form dient nicht nur dem Schutz personenbezogener Daten, sondern soll vor allem deutlich machen, dass es mit der Vorlage des Tätigkeitsberichtes nicht um eine Wiederholung abgeschlossener Beratungen und Prüfungen geht, sondern vielmehr darum, anhand des Einzelfalles auf generelle Probleme hinzuweisen und Lösungen anzubieten.

Mit Blick auf die Wahlen zum Landtag Mecklenburg-Vorpommern im September 2006 habe ich den Tätigkeitsbericht früher als üblich fertiggestellt. Ich hoffe, dass dadurch sowohl die Stellungnahme der amtierenden Landesregierung gemäß § 33 Abs. 1 Landesdatenschutzgesetz (DSG M-V) als auch die Beratung des Landtages vor dem Wahltermin möglich ist.

Gleichzeitig veröffentliche ich hiermit den Zweiten Tätigkeitsbericht der Aufsichtsbehörde gemäß § 38 Abs. 1 Satz 6 Bundesdatenschutzgesetz (der erste Bericht wurde auf Drucksache 4/1294 durch die Landesregierung veröffentlicht) in der Annahme, dass der Landtag diesen in seine Beratung einbeziehen wird, auch wenn hierzu keine Stellungnahme der Landesregierung erfolgt. Er umfasst nach Absprache mit der Landesregierung auch den Zeitraum ihrer Zuständigkeit für den nicht-öffentlichen Bereich.

Ich danke meinen Mitarbeiterinnen und Mitarbeitern sowie den Partnern in der öffentlichen Verwaltung als auch in den Unternehmen, die uns bei der Wahrnehmung unseres Auftrages unterstützten, und baue auch weiterhin auf eine vertrauensvolle Zusammenarbeit.

Karsten Neumann
Landesbeauftragter für den Datenschutz
Mecklenburg-Vorpommern

Inhaltsverzeichnis

A SIEBTER TÄTIGKEITSBERICHT GEMÄß § 33 ABSATZ 1 DES LANDESDATENSCHUTZGESETZES VON MECKLENBURG-VORPOMMERN 7

0 Entwicklung der Rahmenbedingungen und Arbeitsschwerpunkte 7

1 Prüfungsfeststellungen und Empfehlungen 15

I Staatskanzlei 15

Neuordnung des Verfahrens der Befreiung von der Rundfunkgebührenpflicht 15

II Innenausschuss und Sonderausschuss „Verwaltungsmodernisierung und Funktionalreform“ / Innenministerium 17

1 Recht, Personal und ressortübergreifende IT-Angelegenheiten 17
1.1 Datenschutz „aus einer Hand“ 17
1.2 Informationsfreiheitsgesetz auch für Mecklenburg-Vorpommern 18
1.3 Datenschutz durch Technik – Gütesiegel für Mecklenburg-Vorpommern 19
1.4 Modernisierung des Meldewesens 21
1.5 Eingliederung des Statistischen Landesamtes in das Landesamt für innere Verwaltung 23
1.6 Auskunftspflicht beim Mikrozensus 24
1.7 Geheimschutzbeauftragter im Innenministerium 25
1.8 Personaldatenweitergabe ungeschützt über den Dienstweg 25
1.9 Die zentrale Firewall des Landes 26
1.10 Internet-Telefonie 27
1.11 Internetportale öffentlicher Stellen 28
1.12 Datenschutzempfehlungen für die Virtuelle Poststelle 30
2 Kommunalangelegenheiten 31
2.1 Videoüberwachung öffentlicher Plätze 31
2.2 Gesetz zur Modernisierung der Verwaltung 33
2.3 Kollegin hört mit 34
2.4 Verdeckte Beobachtung im Auftrag eines Sozialleistungsträgers 35
2.5 Wenn der Sozialleistungsträger an der Tür klingelt 36
2.6 Kontenabfragen durch Sozialbehörden 37
2.7 Dürfen Stadtvertreter wissen, wie viel Geschäftsführer ihrer kommunalen Unternehmen verdienen? 38
2.8 Tonbandmitschnitte in Sitzungen der Gemeindevertretung 39
2.9 Einsicht in Unterschriftenlisten bei Bürgerbegehren 39
2.10 Verbleib der Mitteilungen der Bundesbeauftragten für die Stasi-Unterlagen bei Privatisierungen? 40
2.11 Aktenfund – Eigentümerwechsel mit Folgen 41
2.12 Ausschreibungen von Ausländern zur Einreiseverweigerung im Schengener Informationssystem 42
2.13 Dokumentation erweiterter Melderegisterauskünfte 44
2.14 Parkscheinautomaten ohne Datenschutz 44
2.15 Melderegister vereitelt Wahlrecht 46
2.16 Videoüberwachung von Fahrscheinautomaten 46
2.17 Schutzprofile für Videoanlagen als Hilfsmittel beim Kauf 47
3 Polizei und Verfassungsschutz 48
3.1 Das Akkreditierungsverfahren zur Fußball-Weltmeisterschaft 2006 48
3.2 Zuverlässigkeitsüberprüfung nach Luftsicherheitsgesetz 49
3.3 Biometrie in Ausweisdokumenten 50
3.4 Information über außerdienstliches Verhalten eines kommunalen Mitarbeiters 51

3.5 Papierloses Büro beim Verfassungsschutz ... 52
III Rechts- und Europaausschuss / Justizministerium ... 54
1 Neuregelungen zur DNA-Analyse ... 54
2 Untersuchungshaftvollzugsgesetz überfällig ... 55
3 Spezielle Forschungsklausel in der Strafprozessordnung ... 56
4 Auskünfte an die Presse im Rahmen strafrechtlicher Ermittlungsverfahren ... 57
5 Internet und Online-Banking bei Gerichtsvollziehern ... 57
6 Rahmenbeschluss zur Vorratsdatenspeicherung in der Telekommunikation ... 58
IV Finanzausschuss / Finanzministerium ... 61
1 Data Center Steuern ... 61
2 Bargeldlose Zahlverfahren ... 62
3 Personalkonzepte ... 63
4 Einsichtnahme des Finanzamtes in betriebliche Unterlagen des Notars ... 64
5 Kontoabrufverfahren ... 65
6 Telefonische Befragungen von Sparkassenkunden ... 67
V Wirtschaftsausschuss und Tourismusausschuss / Wirtschaftsministerium 68
1 Terrorbekämpfung im Bereich der Häfen und der internationalen Schifffahrt ... 68
2 Datenübermittlung nach dem Schornsteinfegergesetz ... 68
3 Kurverwaltung als Schrankenwärter ... 69
VI Landwirtschaftsausschuss / Ministerium für Ernährung, Landwirtschaft, Forsten und Fischerei ... 71
1 Auskunft an den Eigentümer einer landwirtschaftlichen Fläche ... 71
2 Cross Compliance in der Landwirtschaft ... 71
VII Bildungsausschuss / Ministerium für Bildung, Wissenschaft und Kultur ... 73
1 Datenerhebungen für Forschungsprojekte ... 73
2 Das Schulberichtssystem ... 73
VIII Bauausschuss /Ministerium für Arbeit, Bau und Landesentwicklung ... 76
1 Höhe des Vermögens bei Wohngeldbeantragung ... 76
2 JobCard-Verfahren ... 76
3 Arbeitslosengeld II ... 78
4 Hochbau-Statistik ... 81
IX Sozialausschuss / Sozialministerium ... 82
1 Neugeborenenscreening ... 82
2 Krankenhausinformationssystem ... 82
3 Biographiebogen in Pflegeheimen ... 83
4 Verarbeitung von Sozialdaten in Vietnam? ... 84
5 Datenaustausch zwischen dem Disease-Management-Programm „Brustkrebs“ und den Krebsregistern ... 85
6 Einsicht in Krankenunterlagen ... 86
7 Einrichtung einer Datenbank über gefälschte Rezepte ... 87
8 Gesetzesänderung zur Gewährleistung von Vorsorgeuntersuchungen ... 88
9 Neue Strukturen bei Sozialleistungsträgern ... 89
10 Beurteilung der Dienstfähigkeit ... 89
11 Erforschung einer Herzkrankheit ... 90
12 Auskunft aus Patientenakten von Verstorbenen ... 91
13 Vergabe neuer Krankenversichertennummern ... 91
14 Krankentransport ... 93
X Umweltausschuss / Umweltministerium ... 94
1 Umweltinformationsgesetz ... 94
2 Erfassung der Abwasserentsorgung in Kleingartenanlagen ... 94
2 Zusammenfassung der Empfehlungen ... 96

B ZWEITER TÄTIGKEITSBERICHT GEMÄß § 38 ABSATZ 1 DES BUNDESDATENSCHUTZGESETZES (BDSG) 104
1 Einführung 104
2 Unabhängigkeit der Datenschutzaufsicht – Vertragsverletzungsverfahren der Europäischen Kommission 106
3 Gesetzesinitiative zur Änderung des Bundesdatenschutzgesetzes 107
4 Handels- und Wirtschaftsauskunfteien 109
5 Kein Profiling ohne Aufklärung 110
6 Anfangsverdacht der rechtswidrigen Verarbeitung von Mandantendaten 111
7 Unzureichend geschützte Lagerung von Personalunterlagen 113
8 Wonach darf der Arbeitgeber fragen? 113
9 Datenschutz bei der Planung von Gästeanfragen im Hotelleriebereich 114
10 Einkauf per EC-Lastschriftverfahren 116
11 Risiken beim Einsatz von Scoring – Verfahren 118
12 Einzugsermächtigung per Postkarte 119
13 Adresshandel und unerwünschte Werbepostsendungen 119
14 Austausch-MDA nicht gelöscht 121

C ANHANG 123

0 Anlagen 123
1 Übermittlung von Flugpassagierdaten an die US-Behörden 123
2 Entschließung zu Radio-Frequency Identification vom 20. November 2003 125
3 Entscheidungen des Bundesverfassungsgerichts vom 3. März 2004 zum Großen Lauschangriff und zur präventiven Telekommunikationsüberwachung 127
4 Automatische Kfz-Kennzeichenerfassung durch die Polizei 128
5 Personennummern 129
6 Einführung eines Forschungsgeheimnisses für medizinische Daten 130
7 Beteiligung der GEZ am Adresshandel (8. Rundfunkänderungsstaatsvertrag) 131
8 Gravierende Datenschutzmängel bei Hartz IV 132
9 Datensparsamkeit bei der Verwaltungsmodernisierung 133
10 Gesetzentwurf der Bundesregierung zur Neuregelung der akustischen Wohnraumüberwachung 134
11 Staatliche Kontrolle muss auf den Prüfstand! 135
12 Keine Gleichsetzung der DNA-Analyse mit dem Fingerabdruck 137
13 Datenschutzbeauftragte plädieren für Eingrenzung der Datenverarbeitung bei der Fußball-Weltmeisterschaft 2006 138
14 Entschließung zur Einführung der elektronischen Gesundheitskarte 139
15 Einführung biometrischer Ausweisdokumente 140
16 Unabhängige Datenschutzkontrolle in Deutschland gewährleisten 142
17 Schutz des Kernbereichs privater Lebensgestaltung bei verdeckten Datenerhebungen der Sicherheitsbehörden 143
18 Telefonieren mit Internettechnologie (Voice over IP - VoIP) 144
19 Telefonbefragungen von Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II datenschutzgerecht gestalten 146
20 Die gravierenden Datenschutzmängel beim Arbeitslosengeld II müssen endlich beseitigt werden 147
21 Keine Vorratsdatenspeicherung in der Telekommunikation 149
22 Appell der Datenschutzbeauftragten des Bundes und der Länder: Eine moderne Informationsgesellschaft braucht mehr Datenschutz 151
23 Sicherheit bei eGovernment durch Nutzung des Standards OSCI 153
24 Erklärung von Montreux 154

25 Resolution zur Verwendung der Biometrie in Pässen, Identitätskarten und Reisedokumenten 158
26 Resolution zur Verwendung von Personendaten für die politische Kommunikation 159
27 Fachtagung: Moderne Verwaltung zwischen Informationsfreiheit und Datenschutz 163
28 Organigramm 201

1 Abkürzungen 202

2 Stichwortverzeichnis 205

3 Publikationen 212

A Siebter Tätigkeitsbericht gemäß § 33 Absatz 1 des Landesdatenschutzgesetzes von Mecklenburg-Vorpommern

0 Entwicklung der Rahmenbedingungen und Arbeitsschwerpunkte

Zur Arbeit der Behörde

Am 11. November 2004 trat die 1. Änderung des Datenschutzgesetzes des Landes Mecklenburg-Vorpommern in Kraft (GVOBl. M-V, S. 505). Mit dieser Änderung erhielt der Landesbeauftragte für den Datenschutz die Aufgabe der Aufsichtsbehörde gemäß § 38 Bundesdatenschutzgesetz und damit die Zuständigkeit für die Überwachung der Durchführung der Datenschutzvorschriften auch im Bereich der Privatwirtschaft.

Mit der Eingliederung dieser neuen Aufgabe in meine Behörde bestand insbesondere die Chance, durch Nutzung des vorhandenen personellen und fachlichen Potentials Synergieeffekte für den Datenschutz im nicht-öffentlichen Bereich zu erzielen. Im Rahmen der Aufgabenübertragung vom bisher zuständigen Innenministerium Mecklenburg-Vorpommern wurde ein Mitarbeiter des höheren Dienstes aus dem Innenministerium in meine Dienststelle versetzt. Da es sich hierbei nicht um den bisherigen Amtsinhaber handelte, musste dieser sich in das Aufgabengebiet jedoch erst einarbeiten.

Unmittelbar nach Übertragung der Aufgabe habe ich den Kontakt zum Kreis der betrieblichen Datenschutzbeauftragten in Mecklenburg-Vorpommern (ERFA-Kreis) gesucht, der durch die Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD) organisiert wird. Bei einem ersten Treffen konnte ich meine Dienststelle vorstellen und über die Beratungsangebote informieren. In diesem neuen Zuständigkeitsbereich konnten wir gemeinsam bereits konkrete Projekte diskutieren.

Die Zusammenarbeit mit dem ERFA-Kreis wird seitdem kontinuierlich fortgesetzt. Die Beratung und Unterstützung der betrieblichen Datenschutzbeauftragten möchte ich jedoch weiter ausbauen. Das Ziel soll eine konstruktive Zusammenarbeit auch zwischen den betrieblichen Datenschutzbeauftragten sein, um die personellen und technischen Voraussetzungen insbesondere für präventiven Datenschutz zu schaffen.

Mit der Einführung eines Datenschutzaudits in Mecklenburg-Vorpommern (Näheres dazu unter A.1.II.1.3) kann ich als Aufsichtsbehörde zusätzlich einen wesentlichen Anreiz zur Entwicklung und Vermarktung datenschutzfreundlicher Produkte leisten. Ich bin sicher, dass die positiven Erfahrungen aus Schleswig-Holstein nach Mecklenburg-Vorpommern übertragen werden können.

Die Zusammenarbeit mit dem Landtag gestaltete sich sehr konstruktiv. Gerne würde ich jedoch den Auftrag des Datenschutzgesetzes Mecklenburg-Vorpommern intensiver wahrnehmen können, den Landtag bei seiner Arbeit zu unterstützen. Von dem Recht des Landtages und seiner Ausschüsse und Fraktionen, mich mit der Erarbeitung von Gutachten und Stellungnahmen zu beauftragen, ist im Berichtszeitraum kaum Gebrauch gemacht worden. Der Landtag Sachsen-Anhalt hatte mich hingegen als Sachverständigen zu einer Anhörung eingeladen, zu der ich ein Gutachten über einen Gesetzentwurf erstellte. Ebenso gestaltet es sich für mich schwierig, den Beratungsauftrag des Gesetzes aus eigener Initiative gegenüber dem Landtag wahrzunehmen, da es an einer korrespondierenden Verfahrensregelung innerhalb der Geschäftsordnung des Landtages fehlt. Dort sind zwar die Zugangs- und Mitwirkungsmöglichkeiten der Landesregierung und ihrer Beauftragten sowie der Bürgerbeauftragten geregelt,

jedoch kein Teilnahme- bzw. Rederecht des Landesbeauftragten für den Datenschutz bei Ausschuss-Sitzungen. Der Verweis auf die Möglichkeit meiner Einbeziehung im Rahmen von förmlichen Sachverständigenanhörungen entspricht meines Erachtens nicht der Intention des Datenschutzgesetzes und erschwert eine zeitnahe und konstruktive Beratungstätigkeit.

1 Ich empfehle dem Landtag, im Rahmen einer Änderung der Geschäftsordnung des Landtages mit Beginn der nächsten Legislaturperiode das Rede- und Zutrittsrecht des Landesbeauftragten für den Datenschutz analog der Rechte der Bürgerbeauftragten zu gestalten, um so die Einbeziehung der Sachkompetenz meiner Behörde in Beratungsgegenstände der Fachausschüsse zu ermöglichen.

Ich bedanke mich ausdrücklich für die gute Zusammenarbeit mit der Landtagsverwaltung im Rahmen der technisch-organisatorischen Unterstützung meiner Behörde. Nur dadurch ist es mir möglich, den administrativen und technischen Aufwand mit dem zur Verfügung stehenden Personal effektiv zu erledigen. Gerne beteilige ich mich auch weiterhin an der Ausbildung von Kaufleuten für Bürokommunikation, weshalb eine weitere Mitarbeiterin meiner Behörde die Ausbilderbefähigung erworben hat. Darüber hinaus würde ich es begrüßen, wenn in Zusammenarbeit mit Landtag und Landesregierung Rechtsreferendaren die Möglichkeit eröffnet würde, eine Station ihrer Ausbildung in meiner Behörde zu absolvieren. Ich werde die Zusammenarbeit mit Universitäten und Fachhochschulen weiter intensivieren, um Studenten von technischen und rechts- oder verwaltungswissenschaftlichen Fachrichtungen Möglichkeiten von Praktika in meiner Behörde zu eröffnen.

Die Zusammenarbeit zwischen der Landesregierung und dem Landesbeauftragten für den Datenschutz hat sich im Berichtszeitraum wesentlich verbessert. Ich wurde bei einer Vielzahl von Gesetzesvorhaben, aber auch bei der Ausgestaltung von technischen und organisatorischen Maßnahmen bei der Verarbeitung personenbezogener Daten innerhalb der Landesverwaltung oft frühzeitig beteiligt. Dadurch konnte ich die Sachkompetenz meiner Behörde umfassend in rechtlichen und technischen Vorhaben einbringen. Hierbei hat sich immer wieder gezeigt, dass die Einbeziehung in einem sehr frühen Stadium geeignet war, Verstöße gegen datenschutzrechtliche Vorschriften zu verhindern und unnötige Ausgaben in erheblichem Umfang zu vermeiden.

Diese frühzeitige Einbeziehung des Datenschutzbeauftragten – wie durch das Datenschutzgesetz Mecklenburg-Vorpommern in § 33 Abs. 2 geregelt – ist jedoch nicht in jedem Falle selbstverständlich. Trotz einer Vereinbarung zwischen den Staatssekretären der Landesregierung im Rahmen eines Beschlusses zur Auslegung der Gemeinsamen Geschäftsordnung II (Amtsblatt M-V, 1996, S. 1228) ist die Beteiligung des Landesbeauftragten für den Datenschutz noch nicht förmlicher Bestandteil derselben und wird sicherlich vor allem deshalb in Einzelfällen nicht beachtet.

2 Ich empfehle daher der Landesregierung, bei einer Überarbeitung der GGO II die förmliche Beteiligung des Landesbeauftragten für den Datenschutz im Stadium des Referentenentwurfes zu Gesetzen und zu Verordnungen mit aufzunehmen.

Auch in diesem Berichtszeitraum habe ich gemeinsam mit meinen Mitarbeiterinnen und Mitarbeitern wieder zahlreiche Schulungs- und Ausbildungsveranstaltungen durchgeführt, um Kenntnisse zu rechtlichen und technischen Datenschutzfragen zu vermitteln. In 60 Veranstaltungen haben wir rund 1.800 Mitarbeiterinnen und Mitarbeiter der öffentlichen Verwaltung, Studierende verschiedener Fachrichtungen und Verantwortliche aus der Wirtschaft erreicht.

So werden durch Mitarbeiter meiner Behörde regelmäßig Kurse an der Fachhochschule für öffentliche Verwaltung und Rechtspflege in Güstrow bestritten und Vorlesungen für Informatiker und Elektrotechniker an der Universität Rostock und an der Hochschule Wismar gehalten. Darüber hinaus habe ich bereits in zwei Polizeidirektionen vor rund 200 Beamten des gehobenen und höheren Polizeivollzugsdienstes, vor der IHK-Hauptversammlung Rostock, vor den Geschäftsführern des Deutschen Roten Kreuzes, auf einer Tagung der Krankenhausdirektoren und bei einer Veranstaltung der Juristischen Studiengesellschaft Vorpommern über aktuelle Datenschutzthemen, über die Arbeit meiner Behörde und über spezielle Datenschutzanforderungen in den jeweiligen Fachbereichen sprechen können. Im Rahmen der Presse- und Öffentlichkeitsarbeit werden Datenschutzthemen bekannt gemacht beziehungsweise in öffentlichen Diskussionen datenschutzrechtliche Standpunkte im Sinne der Wahrung des Selbstbestimmungsrechtes der Bürgerinnen und Bürger vertreten. Deshalb beteilige ich mich an den Tagen der offenen Tür des Landtages, am Mecklenburg-Vorpommern-Tag oder auch an bundesweiten Fachtagungen oder -messen.

Die Zusammenarbeit mit den behördlichen Datenschutzbeauftragten gestaltete sich bisher eher sporadisch. Nachdem die erste Beratung mit den Datenschutzbeauftragten der Polizeidienststellen des Landes Mecklenburg-Vorpommern jedoch sehr erfolgreich verlief und die Datenschutzbeauftragten an mich die dringende Bitte richteten, in einer solchen Form weiterhin beratend und vernetzend tätig zu werden, habe ich mir dies für den nächsten Berichtszeitraum vorgenommen. Zum einen werde ich jährlich zu bereichsspezifischen Beratungen von behördlichen Datenschutzbeauftragten einladen, zum anderen im Rahmen einer Veranstaltungsserie „Datenschutz vor Ort“ in den Landkreisen und kreisfreien Städten Beratungen mit den behördlichen Datenschutzbeauftragten der Ämter, Gemeinden und Städte sowie Bürgersprechstunden, Beratungen mit betrieblichen Datenschutzbeauftragten oder auch Lehrveranstaltungen an den gymnasialen Oberstufen, Fachschulen, Fachoberschulen und Universitäten anbieten. Ich verbinde damit vor allem das Anliegen, die Beratungsleistung meiner Dienststelle, aber auch das Petitionsrecht beim Landesbeauftragten für den Datenschutz breiter in Mecklenburg-Vorpommern bekannt zu machen und die finanziellen und zeitlichen Aufwände für die behördlichen und betrieblichen Datenschutzbeauftragten für eigene Schulung und Beratung sowie für ratsuchende Bürgerinnen und Bürger so gering wie möglich zu halten.

Im Jahr 2005 habe ich die Gelegenheit meines Amtsantrittes genutzt, um innerhalb meiner Dienststelle eine Leitbild-Diskussion zu führen, in der die Arbeitsabläufe und Zuständigkeiten, aber besonders die inhaltlichen Schwerpunktsetzungen in der Arbeit der Behörde diskutiert wurden. Im Ergebnis wurden bereits einige Arbeitsschwerpunkte und Tätigkeitsfelder neu ausgerichtet. Schon die Gestaltung dieses Tätigkeitsberichtes soll dies verdeutlichen. In erster Linie möchte ich mit diesem Bericht dem Landtag und der Landesregierung Empfehlungen aussprechen, die aus meiner Beratungs- und Kontrolltätigkeit resultieren und die über den Einzelfall hinaus Wege aufzeigen, künftig Verstöße gegen das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger des Landes Mecklenburg-Vorpommern zu verhindern. Auf diese Weise soll dazu beigetragen werden, die Arbeit des Datenschutzbeauftragten nachhaltig zu gestalten.

Zur Neuausrichtung gehört auch die Orientierung auf einzelne Projekte, wie die Reihe „Datenschutz vor Ort“, die Neugestaltung des äußeren Erscheinungsbildes der Dienststelle, verknüpft mit der Entwicklung eines Logos, die inhaltliche und gestalterische Überarbeitung der Angebote im Internetauftritt der Dienststelle unter www.datenschutz-mv.de und in den Druckerzeugnissen sowie die jährliche Ausrichtung einer Fachtagung zu einem aktuellen Thema

aus dem Bereich des Datenschutzes. Ich möchte die Außenwirkung und damit die Wirksamkeit der Tätigkeit meiner Behörde verstärken, um so den gesetzgeberischen Auftrag effektiv und nachhaltig umzusetzen. Wir haben uns zum Ziel gesetzt, Petitionen vorrangig zu bearbeiten, unsere Beratungstätigkeit auf einem hohen inhaltlichen Niveau fortzuentwickeln und die Kontakte zu den betrieblichen und behördlichen Datenschutzbeauftragten zur Erhöhung der Effektivität unserer Arbeit zu nutzen. Da wir hierbei an unsere personellen und finanziellen Grenzen stoßen, müssen wir Aktivitäten außerhalb der Prioritäten weitgehend einstellen. Um die hierfür erforderliche Flexibilität beim Einsatz der Mitarbeiterinnen und Mitarbeiter auch weiterhin gewährleisten zu können, habe ich zum 1. Januar 2006 eine diesen Bedingungen angepasste Organisationsstruktur der Dienststelle in Kraft gesetzt (siehe Organigramm in Anlage 28).

Sowohl die technischen als auch die politischen Entwicklungen stellen mich gemeinsam mit meinen Mitarbeiterinnen und Mitarbeitern als zur Wahrung des Rechtes der Bürgerinnen und Bürger bestellte unabhängige Aufsichtsbehörde vor große Herausforderungen. Diese können wir nur dann in angemessener Weise bewältigen, wenn wir uns mit den aktuellen Herausforderungen auseinander setzen und unseren Beitrag dazu leisten, die widerstreitenden Interessen zugunsten der Erhaltung des Rechtes der Bürgerinnen und Bürger auf informationelle Selbstbestimmung auszugleichen. Hierbei können wir jedoch nur unterstützend wirken. Der Ausgleich selbst zwischen beispielsweise den Sicherheitsinteressen und dem Fernmeldegeheimnis oder zwischen den Chancen moderner Kommunikationstechnik und den damit verbundenen Gefahren muss in der gesellschaftlichen Diskussion auf vielen unterschiedlichen Ebenen geschaffen werden; durch das Wirken der politischen Parteien, durch die Gesetzgebung der Parlamente, durch Entscheidungen von Gerichten, aber auch durch mediale Berichterstattung oder durch lokales Handeln von Bürgerinitiativen oder Verwaltungen. Deshalb werde ich unsere beratende und begleitende Kompetenz durch eine engere Zusammenarbeit mit den unterschiedlichen Akteuren stärken und hierfür Partner in der Wirtschaft und deren Verbänden, den Verwaltungen, den Medien und den politischen Parteien suchen.

In zunehmendem Maße arbeiten die europäischen Staaten zusammen und betreiben gemeinsam automatisierte Verfahren zur Verarbeitung personenbezogener Daten. Neben der Zusammenarbeit mit Datenschutzinstitutionen in Deutschland gewinnt daher auch die internationale Zusammenarbeit an Bedeutung. Vor diesem Hintergrund habe ich an der Europäischen Datenschutzkonferenz am 25. und 26. April 2005 in Krakow, Polen, teilgenommen. Die Europäische Datenschutzkonferenz befasste sich vorrangig mit der Entwicklung des internationalen und europäischen Datenschutzrechtes. Die Teilnehmer tauschten Erfahrungen über aktuelle nationale Probleme mit internationalem Bezug aus. Im Mittelpunkt standen die britischen Maßnahmen zur Terrorismusbekämpfung und deren Auswirkungen auf die Datenschutzrechte in Europa. Ebenso diskutiert wurden die europäischen Regelungen zur Übermittlung von Flugpassagierdaten an die USA oder auch die Erfahrungen der Kollegen aus den osteuropäischen Ländern mit der Implementierung des europäischen Datenschutzrechtes in ihrer jeweiligen nationalen Rechtsordnung.

Die Teilnahme an dieser Konferenz gab mir die Möglichkeit zu einem intensiven Erfahrungsaustausch, aber auch zur Kontaktaufnahme mit den Kollegen aus dem deutschsprachigen europäischen Raum. Mein Ziel ist die verstärkte Einbeziehung dieser Dienststellen in die Arbeit des bundesweiten Arbeitskreises „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dem Mecklenburg-Vorpommern vorsteht.

Im November 2005 hatte ich die Gelegenheit zur Teilnahme an der Gründungsveranstaltung der Europäischen Konferenz der Informationsbeauftragten, die bei der Europäischen Akademie für Datenschutz und Informationsfreiheit in Berlin auf Anregung des britischen Informationsfreiheitsbeauftragten stattfand. Ziel dieser Konferenz ist der regelmäßige Meinungsaustausch zwischen den Informationsbeauftragten der europäischen Länder und die Harmonisierung und Weiterentwicklung entsprechender Rechtsvorschriften der Europäischen Union und innerhalb Europas. Insbesondere die Länderberichte über die Ausgestaltung der jeweiligen nationalen Rechtsordnungen zum Thema Informationsfreiheit und Datenschutz haben verdeutlicht, wie wichtig die länderübergreifende Zusammenarbeit ist. So entwickelt sich beispielsweise das Datenschutzrecht in Schweden und in Slowenien im Nachgang zu bereits länger bestehenden Informationsfreiheitsrechten, während sich das Informationsfreiheitsrecht beispielsweise in Deutschland erst entwickelt, hier aber schon auf eine lange Tradition des Datenschutzrechts zurückgegriffen werden kann. Ebenso unterschiedlich sind die nationalen Behörden zur Durchsetzung der entsprechenden Rechte ausgestaltet. Während beispielsweise in Ungarn ein Parlamentarischer Ombudsmann mit einer Behörde die Durchsetzung der Informationsfreiheitsrechte überwacht, so ist dies in Slowenien Aufgabe einer unabhängigen Behörde. Datenschutz und Informationsfreiheit sind die sprichwörtlichen beiden Seiten derselben Medaille. Somit kann das Forum einer europäischen Konferenz der Informationsbeauftragten dem länder- und fachübergreifenden Erfahrungsaustausch ebenso dienen wie gemeinsame Aktivitäten im Rahmen der europäischen Rechtsetzung. Vor dem Hintergrund der geplanten Einführung eines Informationsfreiheitsrechtes in Mecklenburg-Vorpommern habe ich als Datenschutzbeauftragter Mecklenburg-Vorpommerns die Gründungsurkunde mit unterzeichnet und werde die Weiterentwicklung des Informationsrechtes in Europa unterstützen.

Die Internationale Datenschutzkonferenz in Montreux, Schweiz, an der ich aus Kostengründen nicht teilnehmen konnte, befasste sich schwerpunktmäßig mit den Themen der Verwendung der Biometrie für Pässe (Anlage 25) sowie den Datenschutzstandards in der politischen Kommunikation (Anlage 26) und wandte sich mit einem Appell (Anlage 24) unter anderem an den Weltgipfel zur Informationsgesellschaft, der vom 16. bis 18. November 2005 in Tunis unter beachtenswerter medialer Anteilnahme stattfand.

Das wichtigste Forum des Erfahrungsaustausches und der fachlichen Zusammenarbeit ist und bleibt jedoch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Die ständige Konferenz dient der Zusammenarbeit und dem Informationsaustausch über Bund- und Ländergrenzen hinweg. Ziel ist es, den Datenschutz möglichst einheitlich zu verwirklichen. Die wichtigsten Ergebnisse der Arbeit der Konferenz, die überwiegend in bundesweiten Arbeitskreisen der jeweiligen Fachleute geleistet wird, werden in Entschließungen veröffentlicht.

Diese Entschließungen (Anlage 1 bis 23) belegen einerseits die Breite der datenschutzrechtlichen Themen in der aktuellen Bundes- und Landespolitik und andererseits die sehr fortgeschrittene Form der fachlichen Zusammenarbeit zwischen den einzelnen Datenschutzbeauftragten der Länder und dem Bundesbeauftragten für den Datenschutz. An dieser Zusammenarbeit beteiligt sich Mecklenburg-Vorpommern insbesondere durch die Leitung des Arbeitskreises „Technische und organisatorische Datenschutzfragen“. Darüber hinaus beteiligt sich Mecklenburg-Vorpommern, wie alle anderen Landesbeauftragten für den Datenschutz, am Virtuellen Datenschutzbüro, einem Angebot von deutschen und ausländischen Datenschützern im Internet (www.datenschutz.de). Es bietet Informationen rund um den Datenschutz, Diskussionsforen zu aktuellen Datenschutzthemen, und es ist eine Plattform für die Zusam-

menarbeit der Datenschutzbehörden. Diese Einrichtung ist auch für die Datenschutzbeauftragten des öffentlichen und des nicht-öffentlichen Bereiches sowie für die interessierte Öffentlichkeit zu einem wichtigen Arbeits- und Kommunikationsmittel geworden.

Arbeitskreis „Technische und organisatorische Datenschutzfragen“

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wird von verschiedenen, fachspezifisch ausgerichteten Arbeitskreisen beraten und unterstützt. Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (AK Technik) tagt in regelmäßigen Abständen seit 1993 unter der Federführung Mecklenburg-Vorpommerns. Im Berichtszeitraum trafen sich die Mitglieder des Arbeitskreises zu vier turnusmäßigen Sitzungen in Schwerin, Rostock, München und Berlin und einer außerplanmäßigen Sitzung in Berlin.

Zur 42. Sitzung des AK Technik im Februar 2004 in Schwerin waren das erste Mal in der Geschichte des Arbeitskreises Vertreter der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich eingeladen. Die zunehmende Verflechtung von Datenverarbeitungen zwischen Behörden und Unternehmen erfordert eine enge Zusammenarbeit zwischen den jeweiligen Aufsichtsgremien. Hinzu kommt, dass sich die technikrelevanten Datenschutzaspekte in beiden Bereichen ohnehin sehr ähnlich sind, so dass die Empfehlungen des AK Technik sich auch in vielen Gebieten der Datenverarbeitung privater Unternehmen anwenden lassen. Insofern war es folgerichtig, die Mitarbeiter der Aufsichtsbehörden in die Beratungstätigkeit des AK Technik von vornherein einzubeziehen. Es wurde vereinbart, die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich regelmäßig zu den Sitzungen des Arbeitskreises einzuladen.

Ein fachlicher Schwerpunkt dieser Sitzung war das JobCard-Verfahren (siehe Punkt A.1.VIII.2.). Die Entwickler des Verfahrens (Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung GmbH – ITSG GmbH) waren eingeladen, um technische Aspekte des Verfahrens vorzustellen. Ein vom Arbeitskreis vorgelegter Fragenkatalog wurde abgearbeitet. Die Diskussion trug maßgeblich zum besseren Verständnis der Arbeitskreismitglieder für die Abläufe im JobCard-Verfahren bei, brachte aber auch den Verfahrensentwicklern wichtige Erkenntnisse, die dann in die weitere Ausgestaltung des Verfahrens eingeflossen sind.

Zur 43. Sitzung des AK Technik im September 2004 hatte der Fachbereich Informatik der Universität Rostock eingeladen. Schwerpunktthema dieser Sitzung waren die datenschutztechnischen Aspekte verschiedener Formen drahtloser Kommunikation. Die Wissenschaftler informierten über ihre Forschungsergebnisse in den Bereichen WLAN (Wireless Lokal Area Network – kabelloses lokales Netzwerk), Bluetooth (Industriestandard zur drahtlosen Vernetzung von Geräten über kurze Distanzen) und IrDA (Infrared Data Association – Spezifikationen und Protokollstandards für den Austausch von Daten mittels infrarotem Licht). Im Ergebnis wurde eine Arbeitsgruppe beauftragt, entsprechendes Informationsmaterial für Verwaltung, Bürger und Unternehmen zu erstellen.

Die 44. Sitzung des AK Technik fand im Februar 2005 auf Einladung der Firmen Intel und Siemens in München statt. Tagungsort war das von beiden Firmen betriebene RFID Technology Center. Die Sitzungsteilnehmer wollten sich über die technischen Details und Anwen-

dungsmöglichkeiten der neuen RFID-Technologie informieren, um die daraus resultierenden Datenschutzaspekte bewerten zu können.

> **RFID** (Radio Frequency Identification) ist die englische Bezeichnung für Funk-Identifizierung. Daten werden auf einem kleinen Chip (Transponder) berührungslos und in der Regel ohne Sichtkontakt geschrieben und gelesen. Diese Transponder werden an Gegenständen (auch unsichtbar) befestigt, die dann mittels spezieller Lesegeräte kontaktlos über Entfernungen bis zu zehn Metern automatisch identifiziert werden können. So könnten beispielsweise alle Waren eines Supermarkts mit solchen Transpondern ausgestattet und die Preise an der Kasse automatisch ausgelesen werden.

Es wurde beschlossen, eine Informationsbroschüre zu erstellen, in der über die Risiken der RFID-Technologie informiert wird und die Handlungsempfehlungen zum datenschutzgerechten Einsatz von RFID-Systemen geben soll.

Zur Sitzung in München konnte ich erstmals einen Gast aus dem Ausland begrüßen. Ein Mitarbeiter des Eidgenössischen Datenschutzbeauftragten berichtete über das Tätigkeitsfeld der Schweizer Kollegen und zeigte großes Interesse am Ausbau der internationalen Zusammenarbeit. Viele der in Deutschland relevanten Datenschutzthemen sind auch in der Schweiz aktuell, so dass die gemeinsame Bearbeitung sehr sinnvoll erscheint. Es wurde vereinbart, die internationale Zusammenarbeit zu intensivieren und zu den kommenden Sitzungen des AK Technik weitere ausländische Kollegen einzuladen.

Im September 2005 waren die Teilnehmer der 45. Sitzung des AK Technik Gäste in der Vertretung des Landes Mecklenburg-Vorpommern beim Bund in Berlin. Mit Blick auf den nun schon mehr als zehnjährigen Vorsitz Mecklenburg-Vorpommerns im Arbeitskreis hatte der Bevollmächtigte des Landes beim Bund die Mitglieder in seine Dienststelle eingeladen.

Zu dieser Sitzung waren Vertreter des Zentralverbandes Elektrotechnik- und Elektronikindustrie eingeladen, um über den aktuellen Stand moderner Videoanlagen zu berichten. Die Mitglieder des AK Technik berieten mit den Gästen über die Schutzprofile für Videoanlagen, die im Auftrag des Bundesbeauftragten für den Datenschutz entwickelt worden waren (siehe Punkt A.1.II.2.1), und diskutierten über den Nutzen der Schutzprofile und die Auswirkungen auf die Hersteller solcher Anlagen.

Zu dieser Sitzung hatte eine Arbeitsgruppe des AK Technik die Orientierungshilfe zum Datenschutz in drahtlosen Netzen vorgelegt, die im Ergebnis der Beratungen der 43. Sitzung als notwendig erachtet worden war. In diesem Papier werden die Risiken von Funknetzen beschrieben und die aus datenschutzrechtlicher Sicht erforderlichen Schutzziele erläutert. Die Gefährdungen der verschiedenen Funktechnologien werden dargestellt und die daraus resultierenden Sicherheitsmaßnahmen aufgelistet. In einem separaten Kapitel werden datenschutzrechtliche Aspekte beim Einsatz drahtloser Netze betrachtet. Die Orientierungshilfe wurde im Oktober 2005 von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zustimmend zur Kenntnis genommen und kann aus meinem Internetangebot (www.datenschutz-mv.de) heruntergeladen werden.

Zu einer Sondersitzung des AK Technik im Juni 2005 hatte ich Vertreter der Initiative „Deutschland sicher im Netz„ eingeladen, um die Möglichkeiten der Zusammenarbeit zwi-

schen dem AK Technik und der Initiative zu erörtern. In der im Januar 2005 gestarteten bundesweiten Initiative haben sich unter Schirmherrschaft des Bundesministers für Wirtschaft und Arbeit namhafte Partner aus Politik, Wirtschaft und Gesellschaft zusammengeschlossen. Die Initiative will die Sicherheitsrisiken bei der Nutzung des Internet verringern, indem sie für ein sicherheitsbewusstes Verhalten im Umgang mit dem Internet sensibilisiert. Nutzer werden über bekannte Schwachstellen informiert und erhalten sowohl Empfehlungen zu Sicherheitsfragen als auch Softwareprodukte zur Überprüfung von Sicherheitseinstellungen. Auf diese Weise sollen sie in die Lage versetzt werden, die eigene IT-Infrastruktur besser vor den Sicherheitsrisiken des Internet zu schützen und Vertrauen in die Sicherheit ihrer personenbezogenen Daten zu setzen. Mit diesen Inhalten verfolgt die Initiative „Deutschland sicher im Netz“ Ziele, für die sich die Datenschutzbeauftragten des Bundes und der Länder in Wahrnehmung ihrer gesetzlichen Aufgaben seit langem einsetzen.

Der AK Technik hat daher angeboten, die Initiative bei der Formulierung von datenschutzrelevanten Aspekten der geplanten Veröffentlichungen zu unterstützen. Die Vertreter der Initiative sagten zu, wesentliche Teile der zur Veröffentlichung vorgesehenen Informationen vorab dem AK Technik vorzustellen und dessen Kommentare und Hinweise in die Texte einfließen zu lassen.

1 Prüfungsfeststellungen und Empfehlungen

I Staatskanzlei

Neuordnung des Verfahrens der Befreiung von der Rundfunkgebührenpflicht

Seit der Neuregelung des Verfahrens der Befreiung von der Rundfunkgebührenpflicht sind in meinem Zuständigkeitsbereich zunehmend Beschwerden zum Verfahren der Befreiung von Rundfunk- und Fernsehgebühren für sozialbedürftige Personen eingegangen.

Anträge auf Befreiung von der Rundfunkgebührenpflicht werden seit dem 1. April 2005 nicht mehr vom örtlichen Träger der Sozialhilfe, sondern ausschließlich von der örtlich zuständigen Landesrundfunkanstalt entschieden. Die Landesrundfunkanstalten haben die Gebühreneinzugszentrale (GEZ) mit der Bearbeitung der Anträge und der Verarbeitung der in diesem Zusammenhang anfallenden personenbezogenen Daten beauftragt. Dies hat zur Folge, dass Antragsteller verpflichtet sind, die Befreiungsvoraussetzungen durch den Sozialleistungsbescheid im Original oder in beglaubigter Kopie bei der GEZ nachzuweisen (§ 6 Abs. 2 Rundfunkgebührenstaatsvertrag- RGebStV). Die Antragsteller haben daher zusätzliche Kosten durch die Beglaubigungsgebühren zu tragen. Diese Kosten häufen sich dadurch, dass die Bescheide generell nur eine kurze Geltungsdauer haben und deshalb häufig verlängert und wieder neu eingereicht werden müssen. Empfänger des Arbeitslosengeldes II müssen außerdem nach dem Sozialgesetzbuch Zweites Buch (SGB II) bei jedem aktuellen Bescheid einen neuen Befreiungsantrag stellen. Das heißt, die GEZ erhält auch Bescheide, die lediglich Kürzungen der Leistungen festlegen.

Dieses Verfahren entspricht nicht den datenschutzrechtlichen Grundsätzen der Erforderlichkeit und Datensparsamkeit. Ich habe daher gegenüber dem Datenschutzbeauftragten des Norddeutschen Rundfunks sowie gegenüber meinen Länderkollegen angeregt, auf dem Antragsformular die Möglichkeit vorzusehen, dass die für die Befreiung erforderlichen Daten aus den Nachweisen eingetragen und durch die jeweils bewilligende Behörde durch Stempel und Unterschrift bestätigt werden, da dieses Verfahren den gleichen öffentlichen Glauben wie eine beglaubigte Kopie beanspruchen kann. Die Sozialbehörden beziehungsweise kommunalen Verbände unseres Bundeslandes habe ich gebeten, sich dafür einzusetzen, dass die zuständigen Behörden der Landkreise, Städte und Gemeinden an dem vorgeschlagenen Verfahren mitwirken. Allerdings bin ich hier größtenteils auf Ablehnung gestoßen. Die Bundesagentur für Arbeit Nord hat sich mir gegenüber hinsichtlich der Arbeitslosengeld II-Empfänger entschieden gegen ein solches Verfahren bei den nach dem SGB II eingerichteten Arbeitsgemeinschaften geäußert. Grund hierfür seien die zusätzlichen Aufwendungen, die nicht erstattet würden.

Da das geltende Verfahren zur Befreiung von der Rundfunkgebührenpflicht in der Praxis zu erheblichen datenschutzrechtlichen Defiziten führt, haben die Datenschutzbeauftragten des Bundes und der Länder gegenüber der Staatskanzlei Rheinland-Pfalz als federführendes Land in der Arbeitsgruppe der Rundfunkreferenten folgende Änderung von § 6 Abs. 2 RGebStV vorgeschlagen:

> „(2) Der Antragsteller hat die Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht durch die Vorlage einer Bestätigung des Leistungsträgers über die Gewäh-

rung einer Leistung nach Absatz 1 oder das Vorliegen der Befreiungsvoraussetzungen sowie über die Gültigkeitsdauer des zugrunde liegenden Bescheides nachzuweisen."

Die Rundfunkreferenten der Länder halten diesen Vorschlag zwar für die beste Lösung, aber nicht für eine Alternative zur gegenwärtigen Rechtslage, da sie der Argumentation folgen, dass die Verwaltungskosten der Kommunen von den Ländern nicht erstattet werden bzw. die Kommunen einen Ausgleich ihrer Verwaltungskosten von den Ländern fordern könnten, dies jedoch nicht zu realisieren sei.

3 Ich empfehle der Landesregierung, beim Verfahren zur Befreiung von der Rundfunkgebührenpflicht den Gesetzesvorschlag der Datenschutzbeauftragten des Bundes und der Länder zu befürworten und damit ein datenschutzgerechtes Verfahren zu unterstützen.

II Innenausschuss und Sonderausschuss „Verwaltungsmodernisierung und Funktionalreform“ / Innenministerium

1 Recht, Personal und ressortübergreifende IT-Angelegenheiten

1.1 Datenschutz „aus einer Hand“

Seit dem 11. November 2004 ist der Landesbeauftragte für den Datenschutz die zuständige Datenschutz-Aufsichtsbehörde für die nicht-öffentlichen Stellen.

> **Nicht-öffentliche Stellen** sind nach § 2 Abs. 4 Bundesdatenschutzgesetz natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht öffentliche Stellen sind. Darunter fallen vor allem private Einzel- und Gesellschaftsunternehmen aller Branchen, beispielsweise Handel, Versandhandel, Banken, Versicherungen, Auskunfteien, Markt- und Meinungsforschung, Werbung, Adress- und Telefonbuchverlage, Vermietung, Reisebüros, aber auch Angehörige der so genannten freien Berufe wie Steuerberater, Rechtsanwälte, Ärzte oder Apotheker.

Zuvor war das Innenministerium für den nicht-öffentlichen Bereich zuständig. Mit der Aufgabenübertragung auf den Landesbeauftragten für den Datenschutz durch das Erste Gesetz zur Änderung des Landesdatenschutzgesetzes vom 29. Oktober 2004 wird vielen wichtigen Aspekten Rechnung getragen.

Die Bürgerinnen und Bürger erhalten mit der Zusammenlegung eine einzige Anlaufstelle bei Datenschutzfragen mit Stellen in unserem Land. Dies dient auch der Verwaltungseffizienz, da die doppelte Arbeit durch zwei Stellen bei vielen gleichgelagerten Problemen im öffentlichen und nicht-öffentlichen Bereich beendet wird. Damit ist gleichzeitig eine einheitliche Anwendung des sowohl für den öffentlichen als auch für den nicht-öffentlichen Bereich geltenden Rechts gewährleistet.

Die verschiedenen Formen des Outsourcings, die stark zunehmende vernetzte Datenverarbeitung und insbesondere die in den nächsten Jahren sprunghaft steigende Nutzung des Internet erschweren es zunehmend, die Kontrollräume korrekt zu trennen. Die Übertragung der Datenschutzkontrolle auf den Landesbeauftragten für den Datenschutz lässt diese Trennung weitgehend entbehrlich werden und macht die technische Kompetenz des Landesbeauftragten für den Datenschutz für den privaten Bereich nutzbar.

Die internationale Zusammenarbeit wird erleichtert, da in keinem anderen europäischen oder außereuropäischen Staat, in dem der Datenschutz geregelt ist, eine derartige Trennung existiert, wie sie bisher in Deutschland mehrheitlich üblich ist. Zudem wird die von der EU-Datenschutzrichtlinie geforderte Unabhängigkeit der Datenschutz-Kontrollstellen gewährleistet (siehe Punkt B.2.).

Schließlich sind die bisherigen Erfahrungen in den Bundesländern, in denen die Landesbeauftragten für den Datenschutz auch den privaten Bereich kontrollieren, ausnahmslos gut.

1.2 Informationsfreiheitsgesetz auch für Mecklenburg-Vorpommern

Am 1. Juni 2005 habe ich eine Fachtagung zum Thema „Moderne Verwaltung: Zwischen Informationsfreiheit und Datenschutz“ durchgeführt. Ein halbes Jahr nach meiner Amtseinführung war es mir ein großes Anliegen, den Gedanken des freien Informationszugangs der Bürgerinnen und Bürger bei Behörden unseres Landes zu befördern und die Arbeit meines Vorgängers fortzuführen. Sowohl die Informationsfreiheit als auch der Datenschutz basieren auf dem Recht auf informationelle Selbstbestimmung. Die Möglichkeit, über seine persönlichen Daten verfügen zu können, setzt das Recht auf Teilhabe an öffentlich verfügbaren Informationen voraus. Nur wer ausreichend informiert ist, kann auch von seinen Rechten Gebrauch machen und am demokratischen Willensprozess teilhaben.

Im Verlauf der Fachtagung wurden Pro- und Kontraargumente ausführlich diskutiert und die Erfahrungen anderer Bundesländer ausgewertet. Aufgrund der bevorstehenden In-Kraft-Setzung des Bundesgesetzes und der Diskussion eines Landesgesetzes stellt die im September veröffentlichte Tagungsdokumentation (siehe Anlage 27) ein aktuelles Nachschlagewerk dar. Sowohl die Reaktionen der Presse als auch die Resonanz bei Vereinen und Verbänden haben das Interesse unterschiedlicher Gruppen eindrucksvoll deutlich gemacht.

Ein generelles Informationszugangsrecht ergänzt spezialgesetzliche Informationsrechte, wie sie zum Beispiel im Umweltbereich bestehen (Näheres hierzu unter X.).

Mit dem nun vorliegenden Gesetz zur Regelung des Zugangs zu Informationen des Bundes vollzieht nach vier Bundesländern nunmehr auch der Bund den Wandel vom Prinzip der Amtsverschwiegenheit hin zu transparenten Verwaltungsstrukturen mit einem Recht für jedermann auf freien Informationszugang bei Behörden. Selbstverständlich gilt auch dieses Recht nicht schrankenlos. Das Gesetz regelt den Zugang zu Informationen dort in besonderer Weise, wo personenbezogene Daten Dritter betroffen sind. Des Weiteren regelt es auch den Schutz des Betriebs- und Geschäftsgeheimnisses von Unternehmen. So ist dort genau festgelegt, inwieweit ein Zugang gewährt werden kann, ohne die wirtschaftlichen Interessen der betroffenen Unternehmer zu beeinträchtigen. Restriktiv ist der Gesetzentwurf auch insofern, als „öffentliche Belange“ berührt sind. Das ist zum Beispiel der Fall, wenn das Bekanntwerden der Information dem Wohl des Bundes schwerwiegende Nachteile bereiten würde, wenn dadurch der Ablauf eines anhängigen Gerichtsverfahrens erheblich beeinträchtigt würde oder wenn der innerbehördliche Entscheidungsprozess berührt ist. Damit sind Fälle gemeint, in denen Entwürfe und Beschlüsse, die vorzeitig bekannt werden, dem gesamten Projekt schaden oder es zur Erfolglosigkeit verdammen würden.

Das Gesetz sieht vor – ähnlich wie dies bereits für die Länder Berlin, Brandenburg, Nordrhein-Westfalen und Schleswig-Holstein geregelt ist – dass sich die Bürgerinnen und Bürger an den Beauftragten für den Datenschutz wenden können, wenn sie der Auffassung sind, dass ihr Informationsersuchen zu Unrecht abgelehnt oder nicht beachtet worden ist oder dass sie von einer Behörde eine unzulängliche Antwort erhalten haben.

Nachdem das Bundesgesetz zum 1. Januar 2006 in Kraft treten wird, ist es auch für Mecklenburg-Vorpommern unumgänglich, den freien Zugang zu Informationen auf Landes- und Kommunalebene zu regeln.

4 Ich empfehle daher dem Landtag, die Ankündigung der Landesregierung und der Koalitionsfraktionen, noch vor Ende dieser Legislaturperiode ein Informationsfreiheitsgesetz für Mecklenburg-Vorpommern zu beschließen, umgehend umzusetzen.

1.3 Datenschutz durch Technik – Gütesiegel für Mecklenburg-Vorpommern

Unser Landesdatenschutzgesetz (DSG M-V) hat die Voraussetzungen dafür geschaffen, dass Hersteller und Vertriebsfirmen ihre IT-Produkte (Hardware, Software und Verfahren), die für den Einsatz in der öffentlichen Verwaltung geeignet sind, auf ihre Datenschutzfreundlichkeit prüfen und im Erfolgsfalle mit einem Gütesiegel versehen lassen können. Dieses Datenschutzaudit-Verfahren muss durch eine Rechtsverordnung geregelt werden.

§ 5 Abs. 2 DSG M- V

Informationstechnische Produkte, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem Prüfverfahren festgestellt wurde, sollen vorrangig eingesetzt werden. Die Landesregierung regelt durch Rechtsverordnung Inhalt, Ausgestaltung und die Berechtigung zur Durchführung des Verfahrens.

Der Erlass einer solchen Verordnung würde nicht nur einen entscheidenden Qualitätsschritt für den präventiven Datenschutz im IT-Sektor bedeuten. Für die im Lande entwickelten IT-Produkte würde diese formelle Qualitätsbestätigung durch Auditierung zugleich auch einen nicht unbeträchtlichen Marketing- und Absatzfaktor darstellen.

Hersteller und Vertriebsfirmen von IT-Produkten im Land hätten bei einer Auditierung in Mecklenburg-Vorpommern Standortvorteile, denn nach § 5 Abs. 2 Satz 1 DSG M-V sind öffentliche Stellen des Landes grundsätzlich verpflichtet, vorrangig auditierte Produkte einzusetzen. Dementsprechend wäre die gesamte Landes- und Kommunalverwaltung gehalten, bei Ausschreibungen zunehmend das Kriterium der Auditierung in die Anforderungskataloge aufzunehmen. Das Datenschutz-Gütesiegel wirkt im Ausschreibungsverfahren dann als Nachweis der datenschutzrechtlichen Zulässigkeit des Produktes. Es entlastet Verwaltung und Unternehmen von der ansonsten bei jeder Ausschreibung erforderlichen Einzelfallprüfung der Geeignetheit des Produktes für den geplanten Einsatz.

Neben den Wettbewerbsvorteilen im Bereich der öffentlichen Verwaltung würde sich die Auditierung auch in der Privatwirtschaft positiv auf die Vermarktung des Produktes auswirken. Hersteller und Vertriebsfirmen könnten die Qualität ihres Produktes durch das Zertifikat in Werbung und Marketing absatzsteigernd hervorheben. Privaten Kaufinteressenten würde ein Produkt angeboten, das sich durch ein amtliches, datensicherheitstechnisch und datenschutzrechtlich relevantes „Prüfsiegel“ gegenüber Konkurrenzprodukten positiv abhebt. Kunden und Abnehmer könnten diese Datenschutzeigenschaften – gerade beim IT-Einsatz in sensiblen Bereichen – in ihre Kaufentscheidung einbeziehen.

In der öffentlichen Verwaltung würde die Einführung eines Datenschutzaudits gleichzeitig die Arbeit der Vergabestellen entlasten, weil wesentliche technische Komponenten, deren Daten-

schutzniveau der Anwender oft nur schwer beurteilen kann, bereits vorab sachverständig geprüft sind. Die Prüfung der technischen Sicherheit des Produktes würde entfallen, die hinsichtlich der datenschutzrechtlichen Zulässigkeit der konkreten Anwendungen erleichtert. Das Prüfverfahren im Rahmen der Vergabe würde beschleunigt und qualitativ gesteigert.

Eine Auditierung trägt zu Rechtsklarheit in Verwaltung und Wirtschaft bei, da sie gleichzeitig ein einheitlich anzuwendender Verfahrensmaßstab nach transparenten, nachprüfbaren Kriterien ist. Dies kann den Unternehmen bereits im Entwicklungsstadium von Produkten helfen.

Die Anhebung des Datensicherheitsniveaus wirkt sich darüber hinaus auf die Betriebssicherheit der eingesetzten Systeme aus. Fehlerhafte und redundante Anwendungen werden verringert beziehungsweise ausgeschlossen. Bearbeitungszeiten werden verkürzt – die Gesamtkosten reduziert.

Mangels Erlasses der Rechtsverordnung läuft § 5 Abs. 2 DSG M-V bisher allerdings leer, so dass die genannten Effekte nicht zum Tragen kommen können.

Angesichts der beschriebenen Vorteile des Audits für die Wirtschaft wurde in Mecklenburg-Vorpommern bereits von vielen Seiten, beispielsweise von Industrie- und Handelskammern, der IT-Initiative Mecklenburg-Vorpommern, des Fraunhofer Instituts für graphische Datenverarbeitung Rostock und der Gesellschaft für Datenschutz und Datensicherung e. V. – einer Selbstorganisation der Wirtschaft – deutliches Interesse geäußert. Dieses Interesse resultiert nicht zuletzt aus den guten Erfahrungen in Schleswig-Holstein, dem einzigen Bundesland, in dem bisher ein Produktaudit existiert.

Das Produktaudit in Schleswig-Holstein („Datenschutz-Gütesiegel“) hat zu einem nicht unerheblichen Standortvorteil für IT-Entwickler in Schleswig-Holstein geführt, wo seit dem Jahre 2002 eine erhebliche Bandbreite von Produkten aus verschiedenen Wirtschaftsbereichen mit dem Datenschutz-Gütesiegel versehen worden ist. Neben dem Effekt der Erhöhung der Marktchancen hatten die Zertifikate in Schleswig-Holstein zugleich Ausstrahlungswirkungen auf das gesamte Marktgeschehen.

Mit den auditierten Produkten existieren bereits heute Vorzeigesysteme, die auch für Neuentwicklungen als Maßstab herangezogen werden. Bei der Auditierung von Firewalls, VNC-Lösungen oder Krypto-Fileserver-Anwendungen wurden Maßstäbe gesetzt, die für die gesamte Branche von Bedeutung sind.

Das Auditierungsverfahren beginnt mit der Prüfung der Produkte anhand des von mir veröffentlichten Kriterienkataloges durch unabhängige, beim Landesbeauftragten für den Datenschutz akkreditierte Sachverständige. Deren Gutachten bilden die Grundlage für die Entscheidung des Landesbeauftragten für den Datenschutz über die Erteilung des Gütesiegels.

Dieses Akkreditierungverfahren wäre ein weiterer Vorteil für die Wirtschaft im Land. Fachleute aus Mecklenburg-Vorpommern könnten so ihre Qualifikation im technischen und/oder rechtlichen Datenschutz quasi „öffentlich beglaubigt“ nachweisen.

Am 6. Dezember 2005 habe ich in Warnemünde einen Workshop „Datenschutz durch Technik“ durchgeführt, auf dem Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein die oben dargestellten Auswirkungen des Datenschutz-Gütesiegels ein-

drucksvoll dargestellt und mit Zahlen belegt haben. Des Weiteren wurden dort die auf der Grundlage von Schleswig-Holstein erstellten Entwürfe für eine Datenschutz-Gütesiegel-Verordnung, der Anforderungskataloge für IT-Produkte und die zu akkreditierenden Sachverständigen sowie die vergaberechtliche Zulässigkeit des Verfahrens für unser Land diskutiert.

Eine zügige Einführung des Auditverfahrens durch Erlass der Rechtsverordnung würde die beschriebenen Vorteile sowohl für die Verwaltung als auch für die IT-Branche in Mecklenburg-Vorpommern mit ihren weit über 10.000 Arbeitnehmern realisieren.

5 Ich empfehle daher der Landesregierung, auf der Grundlage der bisher geleisteten Vorarbeiten umgehend eine Verordnung nach § 5 Abs. 2 Landesdatenschutzgesetz (DSG M-V) zu erlassen.

1.4 Modernisierung des Meldewesens

Bereits im Dezember 2003 hat der Gesetzgeber in das Landesmeldegesetz (LMG) eine Regelung aufgenommen, welche die elektronische Anmeldung bei der Meldebehörde sowie die Erteilung einfacher Melderegisterauskünfte über das Internet ermöglicht (siehe Sechster Tätigkeitsbericht, Punkt 2.16.1). Die elektronische Datenverarbeitung im Meldewesen soll jedoch noch weiter ausgebaut werden. So ist künftig beispielsweise vorgesehen, dass die Datenübermittlung zwischen der Meldebehörde des neuen Wohnortes und der Wegzugsmeldebehörde ausschließlich auf elektronischem Wege erfolgt. Die Landesregierung arbeitet auf der Basis des Melderechtsrahmengesetzes derzeit an einer umfassenden Novellierung des Landesmeldegesetzes.

Die neuen Verfahren sollen im Rahmen des Modellprojekts „E-Government Region Westmecklenburg“ getestet werden. Hier wollen die kommunalen Partner eine umfassende, Ebenen übergreifende gemeinsame E-Government-Struktur aufbauen. Die Dauer des Projektes ist auf zwei Jahre beschränkt. Die Ergebnisse sollen in die E-Government-Planungen des gesamten Landes einfließen.

E-Government-Masterplan: Der E-Government-Masterplan beschreibt die Strategie der Landesregierung zur Modernisierung der öffentlichen Verwaltung. Geplant ist, möglichst viele Verwaltungsleistungen online so bereitzustellen, dass sie der Bürger auch in den Kommunen nutzen kann. Um den Anforderungen insbesondere bei ressortübergreifenden Themen gerecht zu werden, müssen große Teile der Landesverwaltung neu organisiert und der IT-Einsatz neu geregelt werden. Der Masterplan enthält dazu Grundsätze für die Organisation, das IT-Controlling, die Weiterentwicklung der IT-Infrastruktur, die Standardisierung, die Planung und die Mittelbewirtschaftung (siehe auch Sechster Tätigkeitsbericht, Punkt 2.16.4).

Im ersten Teilprojekt werden die Verfahren entwickelt und erprobt, die für die einfache elektronische Melderegisterauskunft nach § 34 Abs. 1a LMG erforderlich sind. Privatpersonen, Unternehmen und Behörden sollen künftig über das Internet Daten eines einzelnen bestimmten Einwohners abrufen können.

Für diesen Zweck werden so genannte Informationsregister eingerichtet, die nur die für die Abrufe erforderlichen Daten enthalten und getrennt vom Meldedatenbestand zu führen sind. Die Informationsregister könnten grundsätzlich von den Meldebehörden mit der dort verwendeten Software vorgehalten werden. So wäre es beispielsweise sehr einfach, den Auskunftsdatenbestand aktuell zu halten. Auch aus datenschutzrechtlicher Sicht wäre dies eine empfehlenswerte Konstellation, weil die Daten beim jeweiligen Meldeamt und somit in der Verfügungsgewalt der zuständigen kommunalen Stelle blieben und ein zentraler Datenbestand, der weitere Begehrlichkeiten wecken kann, vermieden würde.

Die Landesregierung hat jedoch darauf hingewiesen, dass die Informationsregister ständig zum Abruf bereit gehalten werden müssen, also auch außerhalb der üblichen Dienstzeiten und an den Wochenenden. Somit wäre ein hoher administrativer und personeller Aufwand erforderlich, der von den Meldeämtern in der Regel nur schwer zu leisten sei. Vor diesem Hintergrund plant die Landesregierung, ein zentrales Informationsregister aufzubauen. Der Auskunftsdatenbestand aller Meldebehörden des Landes soll in einer so genannten mandantenfähigen Datenbank im Rechenzentrum des Landes bei der DVZ M-V GmbH gespeichert und unter Nutzung einer Vermittlungsstelle zum Abruf bereit gehalten werden. Meinen Bedenken gegenüber einem zentral vorgehaltenen Datenbestand wurde mit der Mandantenfähigkeit der Datenbank Rechnung getragen. Mit dieser technischen Lösung wird erreicht, dass Daten verschiedener Meldebehörden auch weiterhin als logisch getrennte Datenbestände erscheinen. Diese grundlegenden Anforderungen sind im zu novellierenden Landesmeldegesetz, die technischen Details in einer Rechtsverordnung verbindlich festzuschreiben.

Mit der Entscheidung für ein zentral geführtes, mandantenfähiges Informationsregister steht aber auch fest, dass zusätzliche technische Vorkehrungen zu treffen sind, die einerseits die ständige Aktualität des Registers garantieren und andererseits die Datenübertragungen zwischen Meldebehörden und zentraler Datenbank sichern. Der Bundesgesetzgeber hat in der 1. Bundesmeldedatenübermittlungsverordnung (1. BMeldDÜV) das Sicherheitsniveau für die Übermittlung von Meldedaten zwischen Meldebehörden festgelegt. Demnach sind die zu übermittelnden Daten mit einer fortgeschrittenen Signatur nach § 2 Nr. 2 des Signaturgesetzes zu versehen und zu verschlüsseln. Bei Datenübertragungen sind die Satzbeschreibungen OSCI-XMeld (Online Services Computer Interface) und das Übermittlungsprotokoll OSCI-Transport zu Grunde zu legen (§ 2 1. BMeldDÜV).

OSCI-XMeld ist die von der Bundesvereinigung der kommunalen Spitzenverbände herausgegebene Beschreibung des Datensatzes für die Datenübermittlung im Bereich des Meldewesens. **OSCI-Transport** ist der vom Kooperationsausschuss Automatisierte Datenverarbeitung (ADV) Bund/Länder/Gemeinden herausgegebene Standard für ein Datenübermittlungsprotokoll.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt diese Forderung in ihrer Entschließung vom 15. Dezember 2005 (siehe Anlage 23). Sie empfiehlt den flächendeckenden Aufbau einer OSCI-basierten Infrastruktur, um eine durchgehende Sicherheit bei der Datenübermittlung vom Versand bis zum Empfang (Ende-zu-Ende-Sicherheit) zu gewährleisten. Vermittlungsstellen, die nicht der OSCI-Spezifikation entsprechen und somit das Sicherheitsniveau der behördlichen Kommunikationsströme senken, dürfen daher nur Übergangslösungen sein.

Auch für die regelmäßige Aktualisierung des Informationsregisters ist ein Sicherheitsstandard nach OSCI-Vorgaben zu gewährleisten. Mit der vorgesehenen Anschlusspflicht der Meldebehörden an das Corporate Network der Landesverwaltung ist zwar sichergestellt, dass die Aktualisierung ausschließlich über das besonders abgesicherte Landesnetz erfolgt, die in der 1. BMeldDÜV geforderten Vorkehrungen sind gleichwohl erforderlich.

6 Ich empfehle der Landesregierung, für die neuen elektronischen Verfahren im Meldewesen – insbesondere für die elektronische Melderegisterauskunft – angemessene technische und organisatorische Vorkehrungen zu treffen und bei der Novellierung des Landesmeldegesetzes zu normieren.

1.5 Eingliederung des Statistischen Landesamtes in das Landesamt für innere Verwaltung

Im Zuge der Reform der Landesverwaltung hat die Landesregierung beschlossen, am 1. Januar 2006 das „Landesamt für innere Verwaltung“ zu gründen. In dieses Amt wird von Beginn an das Statistische Landesamt Mecklenburg-Vorpommern als „Statistisches Amt„ integriert werden.

Das Gesetz zur Reform der Landesverwaltung ändert in seinem Artikel 19 das Landesstatistikgesetz, um die Eigenverantwortlichkeit des Statistischen Amtes bei der Wahrung des Statistikgeheimnisses zu gewährleisten. Dabei wurde auch die von mir vorgeschlagene Regelung aufgenommen, wonach das Weisungsrecht gegenüber dem Statistischen Amt sich nicht auf die Weitergabe von Einzeldaten erstreckt, die der statistischen Geheimhaltung unterliegen (statistische Einzeldaten).

Nur so kann die erforderliche Abschottung des Statistischen Amtes von der übrigen Verwaltung des Landesamtes für innere Verwaltung gewährleistet werden. Da sich die Aufgaben der Statistik grundlegend von denen des Verwaltungsvollzuges unterscheiden, muss die Statistik gegenüber dem Verwaltungsvollzug abgeschottet sein. Darauf hat schon das Bundesverfassungsgericht in seinem Volkszählungsurteil hingewiesen (BVerfGE 65, 1, 49).

> „Von besonderer Bedeutung für statistische Erhebungen sind wirksame Abschottungsregelungen nach außen. Für den Schutz des Rechts auf informationelle Selbstbestimmung ist – und zwar auch schon für das Erhebungsverfahren – die strikte Geheimhaltung der zu statistischen Zwecken erhobenen Einzelangaben unverzichtbar, solange ein Personenbezug noch besteht oder herstellbar ist (Statistikgeheimnis)...“

Das Gesetz zur Reform der Landesverwaltung sieht in Artikel 19 weiter vor, dass das Innenministerium die für die Durchführung erforderlichen Maßnahmen in einer schriftlichen Dienstanweisung festlegt. Der Entwurf der Dienstanweisung (Stand vom 16. Dezember 2005) ist mit mir abgestimmt worden.

Für die konkrete Umsetzung des Abschottungsgebotes sind organisatorische, technische und bauliche Maßnahmen erforderlich. Von besonderer Bedeutung ist die technische Abschottung des IT-Bereiches des Statistischen Amtes, da der gesamte IT-Bereich des Landesamtes für

innere Verwaltung zu einem gemeinsamen Dezernat IuK-Technik zusammengefasst werden soll. Mir ist zugesichert worden, dass die Mitarbeiter dieses Dezernats grundsätzlich keinen Zugriff zu Einzeldaten der Statistik haben werden. Nach dem Entwurf der Dienstanweisung bedarf es jeweils einer zusätzlichen schriftlichen Weisung des Statistischen Amtes. Ich habe deutlich gemacht, dass die Zugriffsrechte hinsichtlich der statistischen Einzeldaten nicht nur geregelt, sondern durch technische Maßnahmen in der Praxis auch entsprechend umgesetzt werden müssen.

7 Ich empfehle der Landesregierung sicherzustellen, dass die erforderlichen Abschottungsmaßnahmen eingehalten werden. Neben der oben genannten technischen Abschottung sind dies vor allem

- **die personelle Trennung zwischen Mitarbeitern des Statistischen Amtes und denen aus anderen Abteilungen des Landesamtes für innere Verwaltung,**
- **die bauliche Abschottung mit entsprechender Schlüsselverwaltung,**
- **die Verpflichtung der Mitarbeiter des Statistischen Amtes auf Wahrung der statistischen Geheimhaltung auch gegenüber dem Leiter des Landesamtes für innere Verwaltung und**
- **die Verarbeitung statistischer Einzeldaten im Auftrag nur aufgrund einer schriftlichen Verfügung des Leiters des Statistischen Amtes.**

1.6 Auskunftspflicht beim Mikrozensus

Der Mikrozensus ist eine Repräsentativstatistik über die Bevölkerung, den Arbeitsmarkt sowie die Wohnsituation der Haushalte. Für die Betroffenen (1 % der Bevölkerung) besteht eine gesetzliche Auskunftspflicht. Zur Erhebung der Daten setzt das Statistische Landesamt Erhebungsbeauftragte ein und verpflichtet sie auf die Einhaltung des Statistikgeheimnisses. Die Erhebungsbeauftragten werden besonders sorgfältig ausgewählt. So kommen für diese Aufgabe keine Personen infrage, bei denen ein Interessenkonflikt aufgrund ihrer dienstlichen oder beruflichen Tätigkeit denkbar wäre (z. B. Steuerbeamte, Makler). Ebenso wird darauf geachtet, dass der Erhebungsbeauftragte nicht in unmittelbarer Nachbarschaft der jeweiligen Auskunftspflichtigen wohnt.

Dennoch kann nicht ausgeschlossen werden, dass sich einzelne Erhebungsbeauftragte und Auskunftspflichtige kennen, beispielsweise, wenn beide in derselben Firma oder Behörde arbeiten. Deshalb können die Auskunftspflichtigen die Fragebogen auch selbst ausfüllen und entweder dem Erhebungsbeauftragten übergeben oder direkt an das Statistische Landesamt schicken. Aber auch in diesem Fall sind sie verpflichtet, dem Erhebungsbeauftragten gegenüber bestimmte Angaben zu machen, beispielsweise die Zahl der Haushalte in der Wohnung, die Namen des Wohnungsinhabers und der Haushaltsmitglieder.

Es kann jedoch Fälle geben, in denen Auskunftspflichtige aus nachvollziehbaren Gründen dem Erhebungsbeauftragten auch diese Angaben nicht mitteilen möchten. Daher räumt das Statistische Landesamt, nach meiner Anregung aufgrund der Bearbeitung einer Petition, seit der Mikrozensuserhebung 2005 den Auskunftspflichtigen die Möglichkeit ein, ihm sämtliche

Angaben direkt zuzuleiten und den Erhebungsbeauftragten keinerlei Auskunft zu geben. Im Rahmen der Schulungen werden die Erhebungsbeauftragten entsprechend informiert.

1.7 Geheimschutzbeauftragter im Innenministerium

Derzeit werden die Aufgaben des Geheimschutzbeauftragten des Innenministeriums (als zuständige Stelle für die Einleitung und Durchführung der Sicherheitsüberprüfung) und die Aufgaben des stellvertretenden Leiters der Verfassungsschutzbehörde/Referatsleiter für den Bereich Sicherheitsüberprüfungsakten (als mitwirkende Behörde) von einer Person wahrgenommen. Der Gesetzgeber hat jedoch eine ausdrückliche Trennung beider Stellen in § 4 Abs. 1 und § 4 Abs. 3 Sicherheitsüberprüfungsgesetz Mecklenburg-Vorpommern vorgesehen. Intention des Gesetzgebers war es, dass die zuständige Stelle, also diejenige, die ihren Mitarbeiter sicherheitsüberprüfen lassen will, die Sicherheitsüberprüfung durchführt und die Verfassungsschutzbehörde „nur“ mitwirkt. Bei dieser zuständigen Stelle kann es sich auch um Unternehmen handeln, wenn deren Mitarbeiter als Reinigungskräfte oder Fahrer von Gefahrguttransporten eingesetzt werden sollen. Aufgrund der jetzigen Praxis kann nicht sichergestellt werden, dass die Informationen aus den jeweiligen Aufgabenfeldern nur in dem gesetzlich zulässigen Umfang in die Bewertung des zu beurteilenden Sachverhaltes einfließen.

Die Verschluss-Sachenanweisung Mecklenburg-Vorpommern regelt weitere Aufgaben des Geheimschutzbeauftragten. Er trifft beispielsweise Maßnahmen, wenn er erfährt, dass jemand unbefugt von einer Verschlusssache Kenntnis erlangt. Für den Fall (und zwar nur dann), dass nach den ersten Ermittlungen ein nachrichtendienstlicher Hintergrund oder eine Verratstätigkeit anderer Art nicht auszuschließen ist, ist die Verfassungsschutzbehörde zu beteiligen. Insofern besagt die Verwaltungsvorschrift ganz klar, dass es Sachverhalte gibt, die gegebenenfalls Geheimschutzinteressen verletzen, die jedoch nicht automatisch eine Angelegenheit für den Verfassungsschutz darstellen. So dürfte es beispielsweise häufiger Verstöße gegen die Verschluss-Sachenanweisung geben, weil der Umgang mit Verschlusssachen recht kompliziert ausgestaltet ist und Fehler aus Nachlässigkeit, Unwissenheit oder unrichtiger Interpretation der Vorschriften passieren können. In der weitaus geringeren Anzahl der Fälle dürfte der unrechtmäßige Umgang mit Verschlusssachen einen nachrichtendienstlichen Hintergrund haben, welcher die Beteiligung der Verfassungsschutzbehörde erfordern würde. Durch diese nicht klare Trennung der Aufgaben wird das Recht auf informationelle Selbstbestimmung der betroffenen Mitarbeiter des Innenministeriums erheblich verletzt.

8 Ich empfehle dem Landtag, eine Klarstellung dahingehend vorzunehmen, dass auch in diesem Bereich dem Trennungsgebot Rechnung getragen wird.

1.8 Personaldatenweitergabe ungeschützt über den Dienstweg

Ein Mitarbeiter des öffentlichen Dienstes informierte mich darüber, dass ihm sein unmittelbarer Vorgesetzter eine als „vertrauliche Personalangelegenheit“ gekennzeichnete Umlaufmappe mit geöffnetem Siegel übergeben habe. In der Mappe befand sich eine Mitteilung über die Tilgung einer Disziplinarmaßnahme aus seiner Personalakte. Er bat mich, den Sachverhalt zu prüfen.

Der Leiter der Dienststelle bestätigte, dass diese Personalsache auf dem Dienstweg versandt worden ist. Er räumte ebenfalls ein, dass damit gegen die Geschäftsordnung des Amtes, die eine vertrauliche Behandlung von Personalsachen verlangt, verstoßen wurde. Dieser Verstoß gegen datenschutzrechtliche Bestimmungen wurde in der Dienststelle entsprechend ausgewertet.

Darüber hinaus teilte mir der Dienststellenleiter mit, dass der nach § 110 Landesdisziplinarordnung (LDO M-V, seit 14. Juli 2005: § 18 Landesdisziplinargesetz – LDG M-V) zu tilgende Disziplinarvorgang dem Landesarchiv zur Übernahme angeboten wurde. Sofern das Landesarchiv entscheidet, dass die Unterlagen nicht archivwürdig sind, werden sie von der Dienststelle datenschutzgerecht vernichtet. Eine Kopie des Vernichtungszertifikats wird dem Mitarbeiter dann unverzüglich zugesandt.

Diese Vorgehensweise entspricht den datenschutzrechtlichen Anforderungen. Nach den Bestimmungen des Landesarchivgesetzes Mecklenburg-Vorpommern (§ 6 in Verbindung mit § 2 Abs. 2 LArchivG M-V) haben die öffentlichen Stellen des Landes alle Unterlagen, die sie zur Erfüllung ihrer Aufgaben nicht mehr benötigen, dem zuständigen staatlichen Archiv anzubieten. Übernimmt das Archiv die Unterlagen nicht, gibt es diese der anbietenden Stelle zurück.

Über die Stellungnahme des Amtes habe ich den Mitarbeiter informiert und mich für den Hinweis bedankt, der zu einem datenschutzgerechten Umgang mit Personaldaten beigetragen hat.

1.9 Die zentrale Firewall des Landes

Nachdem ich im letzten Berichtszeitraum die Internetzugänge aller Landesministerien kontrolliert hatte (siehe Sechster Tätigkeitsbericht, Punkt 2.17.1), war auch die zentrale Firewall des Landes zu prüfen. Diese wird von der DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH (DVZ) als Bestandteil des Corporate Network (CN) betrieben und sichert die Netze aller Ministerien und weiterer Landesbehörden gegen unbefugte Zugriffe aus anderen Netzen. Das DVZ wird insoweit als Auftragnehmer für die genannten Stellen tätig (§ 4 DSG M-V).

Erneut war festzustellen, dass das DVZ nach hohen Sicherheitsstandards arbeitet. Es waren nur wenige Hinweise zu geben. So wurden die Protokolldaten der Firewall länger gespeichert als erforderlich. Darüber hinaus protokolliert die Firewall bestimmte unwichtige Ereignisse, obwohl dies nicht zur Erkennung und Beseitigung von Störungen erforderlich ist. Die verwendete Software erlaubt es nicht, diese Meldungen zu unterdrücken.

Die Verträge zwischen Land, vertreten durch das Innenministerium, und DVZ entsprachen noch nicht den Vorschriften für die Datenverarbeitung im Auftrag. Ferner existiert bisher die Revisionsarbeitsgruppe aus Vertretern der Auftrag gebenden Behörden nur auf dem Papier. Ihre Aufgabe ist es, über die IT-Sicherheit der Firewall zu wachen. Dazu sollte sie auch Revisionen durch externe Sachverständige einleiten und dafür sorgen, dass deren Ergebnisse auch berücksichtigt werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfahl bereits im Jahr 2000 die Einrichtung dieses Gremiums. Dem habe ich mich damals bereits ausdrücklich angeschlossen.

Mit der Untätigkeit der Revisionsarbeitsgruppe ist es auch zu erklären, dass das Sicherheitskonzept für die Firewall seit seiner Erstellung vor einigen Jahren nicht aktualisiert wurde. Darüber hinaus war festzustellen, dass die Hard- und Softwarebasis des Firewallsystems veraltet, weil die Erneuerung von Hard- und Software sowie die Bereitstellung redundanter Systeme vertraglich nicht berücksichtigt wurde.

Ich habe deshalb dem Innenministerium vor allem empfohlen, die Verträge zwischen DVZ und Land zum CN und zur Firewall anzupassen, das Sicherheitskonzept zu aktualisieren, regelmäßige Revisionen durchzuführen und die Beschaffung von Ersatz-Hardware und -Software zu beauftragen. Dem DVZ habe ich insbesondere geraten, die Speicherdauer der Protokolldaten zu begrenzen und bei der Auswahl neuer Firewallsoftware darauf zu achten, dass sich die Protokollierung auf das notwendige Maß reduzieren lässt.

DVZ und Innenministerium haben zugesagt, dass sie diesen Empfehlungen folgen werden. Das Innenministerium ist außerdem meiner Anregung aus dem letzten Berichtszeitraum (siehe Sechster Tätigkeitsbericht, Punkt 2.17.1) gefolgt und lässt ein IT-Sicherheitsrahmenkonzept für alle Landesministerien erstellen.

9 Ich empfehle der Landesregierung, Datenschutz- und IT-Sicherheitsaspekte der Landesfirewall im IT-Sicherheitsrahmenkonzept angemessen zu berücksichtigen und die hierfür erforderlichen Ressourcen zur Verfügung zu stellen, um das hohe Sicherheitsniveau auch weiterhin gewährleisten zu können.

1.10 Internet-Telefonie

Kostengünstiges Telefonieren über das Internet ist nicht nur bei Privatanwendern zunehmend beliebt. Auch Behörden und Unternehmen wollen Geld sparen, indem sie ihre Netze für Fernsprech- und Datenverbindungen sowohl im Hause als auch bei der Kommunikation zwischen Behörden oder Betriebsteilen zusammenlegen. Für die Übertragung von Sprache über Datennetze wird die Internet-Technologie Voice over IP (VoIP)

> **Voice over IP** ist die Übertragung von Sprache über das Internet. Als Übertragungsnetzwerk eignet sich jedoch auch jedes andere Netzwerk auf der Basis der Internet-Protokolle, zum Beispiel ein firmeninternes lokales Netz. Sprache wird dabei nicht wie im klassischen Telefonnetz mit Leitungen übertragen, die für die Dauer einer Verbindung exklusiv geschaltet werden, sondern in Form von Datenpaketen. VoIP-Datenpakete teilen sich das Netz mit anderen Diensten, wie HTTP-Verbindungen („Surfen“) oder E-Mail.

verwendet. Auch die Landesregierung plant, künftig keine neuen Telefonanlagen zu beschaffen, sondern den Telefondienst in das Landesdatennetz – das Corporate Network (CN) – zu integrieren.

Für den Datenschutz ist diese Technologie eine Herausforderung, weil sich die Datenschutz- und IT-Sicherheitsprobleme aus dem Internet und den lokalen Datennetzen dann auch auf das Telefonieren mit VoIP auswirken. So können beispielsweise unverschlüsselte Verbindungen

abgehört, angezeigte Rufnummern gefälscht und ganze Netze durch Klingelrundrufe blockiert werden. Außerdem enthält auch VoIP-Software wie andere Programme mitunter Fehler, die sich zum Eindringen in fremde Netze missbrauchen lassen.

Mit einer Entschließung hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder daher im Oktober 2005 Hersteller, Anbieter und Nutzer aufgefordert, das Fernmeldegeheimnis auch bei Voice over IP zu wahren (siehe Entschließung der 70. Konferenz, Telefonieren mit Internettechnologie, Anlage 18). Es ist insbesondere erforderlich,

- sichere Verschlüsselungsverfahren einzusetzen,
- Mängel an Protokollen und Software schnell zu beseitigen,
- offene Protokolle und Standards zu nutzen und
- die bestehenden Datenschutzvorschriften ebenso wie in der leitungsgebundenen Telefonie zu beachten.

Als offen werden **Protokolle und Standards** bezeichnet, die frei zugänglich sind und für deren Nutzung keine Gebühren anfallen. Jeder Interessierte kann offene Protokolle und Standards ohne Einschränkungen selbst untersuchen oder analysieren lassen, beispielsweise daraufhin, ob sie Sicherheitslücken enthalten oder ob sie zur Verarbeitung unnötig vieler personenbezogener Daten führen.

Ende 2004 haben mir die Landesregierung und ihr IT-Dienstleister DVZ M-V GmbH den ersten Entwurf des Feinkonzeptes zur Realisierung der IP-Telefonie im Landesdatennetz vorgelegt. Den Unterlagen ist zu entnehmen, dass datenschutzrechtlichen Aspekten ein hoher Stellenwert beigemessen wird. Die sensiblen Sprachdaten sollen beispielsweise besonders geschützt werden, indem die Sprach- und Datenkommunikation zwar über die gleichen physikalischen Leitungen geführt, logisch jedoch durch so genannte virtuelle private Netze (VPN) voneinander getrennt wird. Darüber hinaus sollen Verschlüsselungsmechanismen angeboten werden, die für einen zusätzlichen Schutz der Sprachdaten bei der Übermittlung über das CN sorgen.

In meiner Stellungnahme zum Feinkonzept habe ich unter anderem empfohlen, diese logische Trennung auch bei der Nutzung so genannter Unified Messaging Systeme (UMS, Ergänzung der IP-Telefonie um weitere Kommunikationsmöglichkeiten wie E-Mail, Fax oder Voice-Mail) aufrecht zu erhalten. Der Landtag Mecklenburg-Vorpommern nutzt bereits ein solches System. Ferner habe ich auf die Mitbestimmungsrechte der Personalvertretungen hingewiesen, die sich auch auf den Verzeichnisdienst (das elektronische Telefonbuch des gesamten Systems) sowie die Speicherung und Abrechnung der Gesprächsdaten erstrecken.

10 Ich empfehle der Landesregierung, bereits bei den Planungen zur IP-Telefonie die Empfehlungen der Datenschutzbeauftragten zu berücksichtigen, um künftig auch bei der Nutzung dieser modernen Kommunikationstechnologie das Fernmeldegeheimnis wahren zu können.

1.11 Internetportale öffentlicher Stellen

Im Rahmen des Modellprojekts „E-Government Region Westmecklenburg“ wollen die kommunalen Partner dieser Region eine umfassende, Ebenen übergreifende gemeinsame E-Government-Struktur aufbauen (siehe Punkt A.1.II.2.13). Über die Internetportale der Verwaltung soll der Zugang zu den online angebotenen Dienstleistungen ermöglicht werden. Da bei der Nutzung von Online-Dienstleistungen immer personenbezogene Daten verarbeitet werden, ist die datenschutzgerechte Gestaltung dieser Portale besonders wichtig.

Vor diesem Hintergrund habe ich die Portale einiger Teilnehmer des Modellprojekts kontrolliert. Diese Kontrollen sollten insbesondere zeigen, ob die aus dem Teledienstegesetz (TDG) und dem Teledienstedatenschutzgesetz (TDDSG) resultierenden Informationspflichten berücksichtigt werden, dem Grundsatz der Datenvermeidung in angemessener Weise Rechnung getragen wird und nicht mehr personenbezogene Daten als zulässig veröffentlicht werden.

Informationspflichten

§ 6 TDG: Diensteanbieter haben für geschäftsmäßige Teledienste mindestens folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten:

1. den Namen und die Anschrift, unter der sie niedergelassen sind, bei juristischen Personen zusätzlich den Vertretungsberechtigten,
2. Angaben, die eine schnelle elektronische Kontaktaufnahme und unmittelbare Kommunikation mit ihnen ermöglichen, einschließlich der Adresse der elektronischen Post
3. ...

§ 4 Abs. 1 TDDSG: Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zweck der Erhebung, Verarbeitung und Nutzung personenbezogener Daten ... zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. Bei automatisierten Verfahren, die eine spätere Identifizierung des Nutzers ermöglichen und eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten vorbereiten, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.

§ 4 Abs. 5 TDDSG: Die Weiterleitung zu einem anderen Diensteanbieter ist dem Nutzer anzuzeigen.

Im Ergebnis war festzustellen, dass die Mehrzahl der kontrollierten Portale Mängel aufwies. Folgende Unzulänglichkeiten waren zu kritisieren:

Die von § 6 TDG geforderten Angaben im **Impressum** waren nicht immer vollständig. Insbesondere wurde oft nicht berücksichtigt, dass aus dem Internetportal Angebote verschiedener Diensteanbieter erreichbar sind. Ist beispielsweise ein Dienstleister mit der technischen Abwicklung des Internetangebots beauftragt und bietet insoweit selbst einen Teledienst an (Anbieten eines fremden Teledienstes nach § 3 Nr. 1 TDG), muss dies im Impressum ausdrücklich erwähnt werden. Wenn das Internetportal zudem Inhalte präsentiert, für die eine andere Stelle verantwortlich ist (etwa Informationen zu einer Gemeinde innerhalb des Kreistagsportals), ist dem Nutzer der Wechsel der Verantwortung im Impressum anzuzeigen.

Für die **Weiterleitung zu einem anderen Diensteanbieter** werden so genannte Links verwendet. Die von § 4 Abs. 5 TDDSG geforderte Kennzeichnungspflicht wurde dabei oft nicht ausreichend umgesetzt. Häufig konnte der Nutzer erst nach Betätigung des Links erkennen, dass er weitergeleitet wird.

In einigen Fällen konnten die Nutzer aus Mangel an aussagekräftigen **Datenschutzerklärungen** nicht nachvollziehen, ob Daten über sie gespeichert werden, für welchen Zweck diese gegebenenfalls verwendet werden und wie lange eine Speicherung vorgesehen ist. Mit dem nichtssagenden Hinweis auf die Speicherung für Statistikzwecke werden die Forderungen des § 4 Abs. 1 TDDSG nicht erfüllt. Oft waren die Betreiber der Portale gar nicht in der Lage, die geforderten Angaben bereitzustellen, weil sie den mit der technischen Abwicklung des Portals beauftragten Dienstleister nicht zu diesen Protokollierungsdetails befragt hatten.

Internetportale werden fast immer genutzt, um Informationsmaterial oder Antragsformulare zum Herunterladen bereitzustellen. Um diese Angebote wahrnehmen zu können, ist es in der Regel nicht erforderlich, dass sich der Interessent gegenüber dem Informationsanbieter identifiziert. Dieses Prinzip der **Datenvermeidung** (§ 5 Abs. 1 DSG M-V) wurde von den Portalbetreibern jedoch nicht immer berücksichtigt. Die anonyme Nutzung des Portals war oft nicht möglich. Vielmehr waren in einigen Fällen die Nutzer gezwungen, sich am Portal anzumelden.

Die Verwaltungen nutzen ihre Internetportale auch, um die Behörde vorzustellen und den Bürgern die Ansprechpartner bekannt zu machen. Einige Behördenleiter vertraten die Auffassung, dass alle Mitarbeiter im Internetangebot erscheinen müssten. Ich habe darauf hingewiesen, dass es sich hierbei um eine Übermittlung von **Daten Beschäftigter** an Stellen außerhalb des öffentlichen Bereichs handelt (§ 35 Abs. 2 DSG M-V), die nur für solche Mitarbeiter zulässig ist, zu deren Aufgaben die Wahrnehmung von Außenkontakten gehört.

11 Ich empfehle der Landesregierung, dem Landtag und den weiteren öffentlichen Stellen des Landes, die „Orientierungshilfe zu Datenschutzfragen bei der Präsentation öffentlicher Stellen im Internet“ zu nutzen, um bestehende oder geplante Internetportale zu prüfen (www.datenschutz-mv.de). Bei der Ausgestaltung der Internetportale sind die Prinzipien der Transparenz und der Datenvermeidung in vollem Umfang umzusetzen.

1.12 Datenschutzempfehlungen für die Virtuelle Poststelle

Die Landesregierung arbeitet mit Hochdruck an der schrittweisen Umsetzung des E-Government-Masterplans. Mein ausdrückliches Angebot im Sechsten Tätigkeitsbericht (Punkt 2.16.4), die Modernisierung der Verwaltung datenschutzrechtlich zu begleiten, wurde bei mehreren Projekten aufgegriffen (siehe beispielsweise Punkte A.1.II.1.4 und A.1.IV.2).

Mit der so genannten Virtuellen Poststelle (VPS) wird unter Federführung des Innenministeriums eine Basiskomponente des E-Government-Masterplans entwickelt, die bei fast allen Vorhaben aus diesem Bereich eine zentrale Rolle spielt.

VPS im E-Government-Masterplan

Durch den Aufbau einer virtuellen Poststelle (Datendrehscheibe) zur Verknüpfung von Diensten im Inter- bzw. Intranet mit Fachanwendungen einschließlich der Bereitstellung übergreifender Funktionen (Verschlüsselung, Signatur, Datentransport) in Verbindung mit der Basiskomponente Verschlüsselung/Signatur soll folgender Nutzen erzielt werden:

- standardisierter Zugriff auf im Inter- bzw. Intranet bereitgestellte elektronische Dienste,
- zentralisierte Signatur und Verschlüsselung gemäß organisatorischer Anforderungen,
- Sicherstellung eines interoperablen Datenaustausches,
- Vermeidung von Parallelentwicklungen,
- Kostenvorteile (erhöhen sich durch Zahl der unterstützten Anwendungen).

Eine VPS unterstützt die Abwicklung einer sicheren, nachvollziehbaren und vertraulichen Kommunikation innerhalb von Behörden sowie zwischen Behörden und externen Stellen. Als Basiskomponente für Kommunikationssicherheit ist sie somit von entscheidender Bedeutung für den datenschutzgerechten Betrieb einer Vielzahl von E-Government-Projekten.

Die Datenschutzbeauftragten des Bundes und der Länder haben zugesagt, Entwicklungen im Bereich des E-Government konstruktiv zu begleiten (siehe Sechster Tätigkeitsbericht, Punkt 2.16.2). Unter Federführung meines niedersächsischen Kollegen erarbeiteten daher Mitarbeiter aus verschiedenen Datenschutz-Dienststellen gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und weiteren Fachleuten aus Industrie und Verwaltung Empfehlungen zur datenschutzgerechten Ausgestaltung dieser zentralen E-Government-Komponente. In der Broschüre „Die virtuelle Poststelle im datenschutzgerechten Einsatz“ (abrufbar unter www.datenschutz-mv.de) werden rechtliche Datenschutzaspekte der VPS erläutert, Sicherheitsziele und -mechanismen beschrieben und vor allem ganz konkrete Handlungsempfehlungen gegeben.

12 Ich empfehle der Landesregierung, bei der Planung und beim Betrieb der landeseigenen Virtuellen Poststelle die Hinweise der Broschüre „Die virtuelle Poststelle im datenschutzgerechten Einsatz“ zu berücksichtigen. Für die datenschutzgerechte Ausgestaltung dieser zentralen E-Government-Komponente sind die Handlungsempfehlungen der Kapitel 8 und 9 besonders hilfreich.

2 Kommunalangelegenheiten

2.1 Videoüberwachung öffentlicher Plätze

Die Anfragen zur Videoüberwachung im Land haben in meiner Dienststelle in den letzten Jahren stetig zugenommen. Häufig fragen Bürger oder behördliche Datenschutzbeauftragte der Kommunen an, unter welchen Voraussetzungen der Einsatz von Videotechnik zulässig ist.

So ließ ein Bürgermeister die neu eingeweihte Tunnelunterführung per Videoaufzeichnung überwachen. Die Vertreter der Stadt trugen vor, sie hätten sich bei der Entscheidung für den Einsatz von Kameras vom Präventionsgedanken leiten lassen. So wollte man auf Wunsch der Einwohner schon im Vorfeld verhindern, dass der Tunnel mit Graffitis besprüht wird beziehungsweise dort Straftaten anderer Art begangen werden.

Nach einem Informationsbesuch und nach Besichtigung der Anlage stellte ich klar, dass hier weder die Voraussetzungen nach dem Sicherheits- und Ordnungsgesetz (SOG M-V) noch die des Landesdatenschutzgesetzes (DSG M-V) vorlagen und die Maßnahme mithin rechtswidrig ist. Bildaufzeichnungen sind nach dem SOG M-V nur zulässig, wenn im Einzelfall tatsächliche Anhaltspunkte für die Begehung von Straftaten von erheblicher Bedeutung vorliegen. Dazu zählen alle Verbrechen und bestimmte Vergehen, wie gefährliche Körperverletzung, Bandendiebstahl und weitere Delikte, die im Straftatenkatalog des § 49 SOG M-V abschließend aufgezählt sind. Zu der neu eingeweihten Tunnelunterführung gab es keine Erkenntnisse – weder Straftaten noch sonstige Anhaltspunkte –, welche einen Videoeinsatz hätten rechtfertigen können. Vielmehr handelt es sich um einen sicherheitstechnisch äußerst gelungenen und vorbildlichen Neubau. Ebenso wenig konnten sich die Stadtvertreter auf die Ausübung ihres „Hausrechts“ berufen, da es sich um einen öffentlichen Weg handelt. Das Bundesverfassungsgericht hat im so genannten Volkszählungsurteil grundsätzlich gefordert, dass Bürgerinnen und Bürger sich frei von staatlicher Beobachtung auf öffentlichen Straßen und Plätzen bewegen können müssen. Nur so seien sie in der Lage, ihre sonstigen Grundrechte selbstbestimmt in Anspruch zu nehmen.

Die Videoüberwachung im öffentlichen Raum betrifft überwiegend unverdächtige Personen und setzt diese der Gefahr der Ausforschung von Lebensgewohnheiten und einem ständig wachsenden Anpassungsdruck aus, ohne dass dem ein adäquater Sicherheitsgewinn gegenübersteht (siehe hierzu auch die Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28.10.2005 in Lübeck, Anlage 22).

Auch die Landesregierung hat in Beantwortung einer Kleinen Anfrage bereits im Jahr 2000 (Drucksache 3/1474 vom 22.08.2000) darauf hingewiesen, dass stationäre Überwachungstechnik wegen des Eingriffs in das allgemeine Persönlichkeitsrecht, aus Gründen der Verhältnismäßigkeit sowie der Notwendigkeit, Personal- und Sachmittel effektiv einzusetzen, nur an kriminalgeografisch bedeutsamen Orten eingesetzt werden darf. Unbestritten ist, dass es sich bei der genannten Tunnelunterführung nicht um einen solchen Kriminalitätsschwerpunkt handelt.

Der Bürgermeister hat nach längerem Schriftwechsel und erst nach Tätigwerden der Kommunalaufsicht der Landesregierung die Konsequenz gezogen und die Videoaufzeichnungsfunktion abgeschaltet.

13 Ich empfehle der Landesregierung, gegebenenfalls zu überprüfen, ob sich an der aktuellen Sicherheitslage in Mecklenburg-Vorpommern seit dem Jahre 2000 etwas geändert hat. Ansonsten ist gegenüber den kommunalen Behörden klarzustellen, dass Videoüberwachungsanlagen auf öffentlichen Straßen und Plätzen nur bei

Vorliegen der gesetzlichen Voraussetzungen zulässig sind. Bei entsprechenden Planungen sind die behördlichen Datenschutzbeauftragten frühzeitig einzubeziehen.

2.2 Gesetz zur Modernisierung der Verwaltung

Für unser Bundesland steht in naher Zukunft eine umfassende Verwaltungsreform an. Die Landesregierung hat hierzu den Entwurf eines Gesetzes zur Modernisierung der Verwaltung des Landes Mecklenburg-Vorpommern in den Landtag eingebracht (LT-Drs. 4/1710). Das Vorhaben berührt auch eine Reihe datenschutzrechtlicher Aspekte. Das Landesdatenschutzgesetz (DSG M-V) enthält für diese Sonderkonstellation zum Teil keine hinreichenden Regelungen, so dass Nachteile für das Recht auf informationelle Selbstbestimmung zu befürchten sind, wenn in diesem Bereich keine Rechtssicherheit geschaffen wird.

Gegenüber dem Sonderausschuss „Verwaltungsmodernisierung und Funktionalreform“ des Landtages habe ich deshalb unter anderem empfohlen, folgende Punkte normenklar zu regeln:

- Der Aufbaustab sollte dafür Sorge tragen, dass die Organisation der künftigen Datenverarbeitung den Anforderungen an Datenschutz und Datensicherheit Rechnung trägt und die notwendigen Maßnahmen unter Beteiligung der behördlichen Datenschutzbeauftragten der öffentlichen Stellen getroffen werden. Der Vorsitzende des Aufbausstabes sollte für die Freigabe von Verfahren nach § 19 DSG M-V verantwortlich sein.
- Da sich die Verarbeitung personenbezogener Daten bei den Anlaufstellen für Verwaltungsangelegenheiten nach Artikel 1 § 97 des Gesetzentwurfs aus datenschutzrechtlicher Sicht nicht zweifelsfrei einordnen lässt, sollte klargestellt werden, dass das Landesdatenschutzgesetz zur Anwendung kommt, soweit besondere Rechtsvorschriften keine Regelungen zur Verarbeitung personenbezogener Daten enthalten.
- Mitarbeiter, die eine unterstützende Tätigkeit gegenüber den Einwohnern in der Anlaufstelle wahrnehmen, erhalten umfassend Kenntnis von deren personenbezogenen Daten, wenn diese mit den verschiedenen Verwaltungen kommunizieren. Dadurch droht das bisherige Schutzkonzept der auch internen Abschottung unterschiedlicher Verwaltungseinheiten für die Personen ins Leere zu laufen, die nicht über einen eigenen Internetanschluss und die hierfür erforderliche Kompetenz verfügen. Zum besonderen Schutz der Betroffenen und zur Sicherung der Zweckbindung der Daten sollten deshalb hierfür vom Leiter der Behörde nur besonders ermächtigte Mitarbeiter eingesetzt werden, die hierdurch keinem Interessenkonflikt mit ihren sonstigen dienstlichen Aufgaben ausgesetzt sind. Darüber hinaus sollte auch eine besondere Zweckbindung für die hierbei zur Kenntnis gelangten Daten vorgesehen werden.
- Nach Artikel 1 § 96 des Entwurfs sind noch nicht abgeschlossene Verwaltungsvorgänge dem neuen Aufgabenträger zur Fortsetzung der Aufgabenwahrnehmung zu übergeben. Hinsichtlich des Verbleibs der übrigen Unterlagen sollte geregelt werden, dass diese, soweit sie nicht nach § 6 Landesarchivgesetz dem zuständigen staatlichen Archiv anzubieten sind, ebenfalls dem neuen Aufgabenträger zu übergeben sind.

Da nicht alle Menschen die technischen Möglichkeiten oder das Interesse dafür haben, mit einer Behörde nur elektronisch zu verkehren, richten die Ämter und amtsfreien Gemeinden **Anlaufstellen** ein. Diese Stellen ermöglichen es den Einwohnern, auf die elektronisch angebotenen Leistungen zuzugreifen, und unterstützen die Einwohner insbesondere dadurch, dass sie

- ihnen bei der Nutzung der elektronischen Kommunikation mit dem Land, den kommunalen Körperschaften und ihren jeweiligen Behörden helfen,
- ihre Anträge entgegennehmen und an die zuständige Stelle weiterleiten,
- die zuständige Stelle benennen und die Einwohner an sie vermitteln können,

die für ihre Verwaltungsangelegenheiten erforderlichen Formulare oder Vordrucke vorhalten oder sie zur Verfügung stellen können.

Im Rahmen meiner Kontrolltätigkeit konnte ich bereits feststellen, dass eine Neuorganisation der Verwaltung auch erhebliche datenschutzrechtliche Auswirkungen für Betroffene haben kann, wenn datenschutzrechtliche Anforderungen nicht umfassend umgesetzt werden.

Diese Fälle haben gezeigt, dass bei der Fusion von Verwaltungen oder im Rahmen von Umstrukturierungen im Vorfeld auch eine Reihe datenschutzrechtlicher und datenschutztechnischer Fragen zu klären sind, um künftig eine ordnungsgemäße Datenverarbeitung zu gewährleisten. Neben der – mittlerweile zum Standard gehörenden – Erstellung von Sicherheitskopien und der Protokollierung der Verfahrensschritte gehören dazu beispielsweise auch die Durchführung von Testläufen, das Erstellen einer aktualisierten Verfahrensbeschreibung, gegebenenfalls eine Vorabkontrolle durch den behördlichen Datenschutzbeauftragten sowie die Freigabe des Verfahrens durch den Leiter der öffentlichen Stelle. Öffentliche Stellen haben daher die hierzu notwendigen Schritte unter Beteiligung ihrer behördlichen Datenschutzbeauftragten rechtzeitig einzuleiten.

14 Ich empfehle dem Landtag, meine Vorschläge zur Sicherstellung ordnungsgemäßer Akten-/Datenübermittlung bei Aufgabenübertragungen und Verwaltungsfusionen im Gesetzgebungsverfahren zu berücksichtigen, um so bei der Verwaltungsmodernisierung die notwendige Rechtssicherheit in Datenschutzfragen zu erhalten.

2.3 Kollegin hört mit

Ein Bürger hat sich mit folgendem Sachverhalt an mich gewandt:

Bei einem Telefongespräch mit einer Mitarbeiterin der Bußgeldstelle habe diese – ohne ihn zuvor hierüber zu informieren – das Telefon nach einigen Minuten auf laut gestellt, so dass eine andere Mitarbeiterin mithören konnte. Zu welchem Zeitpunkt des Gesprächs der Petent hiervon in Kenntnis gesetzt wurde, ließ sich im Nachhinein nicht zweifelsfrei klären. Nach Darstellung der Behörde soll der entsprechende Hinweis in diesem Gespräch bereits unmittelbar nach dem Einschalten des Lautsprechers erfolgt sein.

Ich habe die Verwaltung darauf hingewiesen, dass es nicht genügt, die betroffene Person erst nach dem Einschalten der Mithörtaste darüber zu informieren, da sie durch eine solche Verfahrensweise überrascht beziehungsweise überrollt wird. Vielmehr ist es zum Schutz des Persönlichkeitsrechtes notwendig, vorab das Einverständnis einzuholen.

Die Verwaltung hat den Fall zum Anlass genommen, die Mitarbeiter in einer Hausmitteilung darauf hinzuweisen, dass ein Betätigen der Freisprech- bzw. Lautsprechertaste ohne Einverständnis des Gesprächspartners gegen das Recht auf informationelle Selbstbestimmung und das allgemeine Persönlichkeitsrecht verstößt. Dabei hat sie empfohlen, vorher den Gesprächspartner ausdrücklich darauf hinzuweisen und nach seinem Einverständnis zu fragen.

15 Ich empfehle der Landesregierung sowie allen öffentlichen Stellen des Landes, im Rahmen der regelmäßigen Belehrungen ihre Mitarbeiter darauf hinzuweisen, dass Gesprächsteilnehmer generell vor Betätigen der Freisprechtaste beziehungsweise sonstigen Mithörens durch weitere Personen um ihr Einverständnis zu bitten sind. Diese Verfahrensweise ist verbindlich zu regeln.

2.4 Verdeckte Beobachtung im Auftrag eines Sozialleistungsträgers

Eine Petentin teilte mir mit, dass sie auf dem Weg zur Schule ihrer Kinder von einem Auto verfolgt worden sei. Durch eine Halteranfrage bei der Polizei habe sie erfahren, dass das Fahrzeug auf eine Wach- und Schließgesellschaft zugelassen ist. Sie verdächtigte ihren Sozialleistungsträger, diese Beobachtung angeordnet zu haben, und hat mich gebeten, den Sachverhalt zu prüfen.

Auf meine telefonische Nachfrage beim Landkreis, ob die Beobachtung von dort initiiert worden ist, wurde mir mitgeteilt, dass dies nicht bekannt sei. Dies habe ich der Petentin mitgeteilt und ihr empfohlen, die mit der Überwachung verbundene Datenverarbeitung der Wach- und Schließgesellschaft von der Datenschutzaufsichtsbehörde prüfen zu lassen. Dies war zu diesem Zeitpunkt noch das Innenministerium Mecklenburg-Vorpommern. Von dort habe ich dann später erfahren, dass der Auftrag durch eine öffentliche Stelle erteilt wurde. Näheres wüsste man jedoch nicht.

Daraufhin habe ich mich noch einmal an den Landkreis gewandt. Der Landrat bestätigte nun, dass der Auftrag von dort vergeben wurde, um festzustellen, ob ein Sozialleistungsmissbrauch vorliegen würde. Insbesondere wurde die Wach- und Schließgesellschaft beauftragt, verdeckt zu ermitteln, ob tatsächlich eine zeitweilige Gehbehinderung vorliegt, für die eine Hilfe beantragt wurde, und ob die von der Betroffenen angegebenen zu fahrenden Wegstrecken den Tatsachen entsprechen. Die Petentin hatte dem Landkreis als Sozialleistungsträger diese Angaben mitgeteilt und entsprechende zusätzliche Leistungen beantragt. Der Landkreis sah sich jedoch nicht in der Lage, aus diesen Angaben sowie aus ärztlichen Bescheinigungen den Bedarf an Sozialleistungen abschließend festzustellen. Außerdem begründete er die verdeckte Beobachtung damit, dass die betroffene Person nur begrenzt mitwirken würde.

Mit der verdeckten Beobachtung wurde gegen den Ersterhebungsgrundsatz beim Betroffenen verstoßen (§ 67 a Abs. 2 Satz 1 Sozialgesetzbuch Zehntes Buch – SGB X). Eine Datenerhebung ohne Mitwirkung des Betroffenen ist nur unter den in § 67 a Abs. 2 Satz 2 SGB X ge-

nannten Voraussetzungen zulässig. Diese lagen hier nicht vor. Verdeckte Beobachtungen eines Sozialleistungsempfängers durch private Wach- und Schließgesellschaften sind in jedem Fall unzulässig. Mit einem Auftrag zur verdeckten Beobachtung werden der Wach- und Schließgesellschaft Sozialdaten übermittelt, da der Auftrag Angaben darüber enthalten muss, aus welchem Grund welche Person mit welchem Ziel beobachtet werden soll. Das ist hier in unzulässiger Weise geschehen. Der fragliche Sachverhalt hätte in diesem Fall beispielsweise durch ein amts- oder fachärztliches Gutachten rechtskonform und ohne Verletzung der Privatsphäre geklärt werden können. Nicht zuletzt werden im Rahmen einer „Beschattung“ eine Vielzahl von Daten und sonstigen Erkenntnissen aus der Privatsphäre des Betroffenen bekannt, die mit der beantragten Sozialleistung in keiner Weise zusammenhängen. Deshalb habe ich die verdeckte Beobachtung der Sozialleistungsempfängerin gemäß § 32 Abs. 1 Landesdatenschutzgesetz Mecklenburg-Vorpommern gegenüber dem Landkreis beanstandet.

Der Landrat hat sich meiner datenschutzrechtlichen Bewertung schließlich angeschlossen.

16 Ich empfehle der Landesregierung, im Rahmen der Kommunalaufsicht verstärkt darüber zu wachen, dass verdeckte Beobachtungen von Sozialleistungsempfängern nicht durchgeführt oder angeordnet werden.

2.5 Wenn der Sozialleistungsträger an der Tür klingelt

Mit der Einführung des Arbeitslosengeldes II zum 1. Januar 2005 und durch Hinweise des Bundesministers auf eine verstärkte Bekämpfung angeblichen Leistungsmissbrauches kam erneut die Frage auf, ob und wann Sozialleistungsträger Hausbesuche bei Leistungsempfängern durchführen dürfen.

Sozialleistungsträger haben die gesetzliche Pflicht, den für die beantragte Leistung zugrundeliegenden Sachverhalt zu ermitteln (§ 20 Abs. 1 Sozialgesetzbuch Zehntes Buch – SGB X). Dabei ist jedoch zu berücksichtigen, dass die datenschutzrechtlichen Vorschriften des SGB X den Verwaltungsverfahrensvorschriften vorgehen (§ 37 Satz 3 Sozialgesetzbuch Erstes Buch – SGB I). Somit hat beispielsweise die Datenerhebung bei der betroffenen Person Vorrang gegenüber anderen Ermittlungen.

Hausbesuche sind nur unter besonderen Voraussetzungen ein geeignetes und angemessenes und damit auch datenschutzrechtlich zulässiges Mittel, um im Zweifel die Angaben der Hilfesuchenden zu prüfen (siehe Vierter Tätigkeitsbericht, Punkt 3.10.6). Bei der Durchführung von Hausbesuchen ist aus datenschutzrechtlicher Sicht Folgendes zu beachten:

- Zuerst ist zu klären, ob es andere Möglichkeiten gibt, um den Sachverhalt festzustellen.
- Hausbesuche dürfen nur durchgeführt werden, wenn ein konkreter Grund oder Verdacht vorliegt, zum Beispiel für einen Sozialleistungsmissbrauch. Ob ein Hausbesuch durchgeführt wird, sollte der Leiter der Behörde entscheiden.
- Die Mitarbeiter des Sozialleistungsträgers haben sich gegenüber der betroffenen Person durch den Dienstausweis zu legitimieren.

- Die betroffene Person ist über den Grund des Besuches zu informieren und darüber aufzuklären, dass sie einen späteren Termin vereinbaren oder den Zutritt zur Wohnung verweigern kann. Sofern sie von ihrem Grundrecht auf Unverletzlichkeit der Wohnung (Artikel 13 Grundgesetz) Gebrauch macht, hat sie in anderer Weise an der Klärung des Sachverhaltes mitzuwirken.

17 Ich empfehle der Landesregierung, im Rahmen der Kommunalaufsicht die Hinweise für die Durchführung von Hausbesuchen bei Sozialleistungsempfängern in den Landkreisen und kreisfreien Städten bekannt zu geben.

2.6 Kontenabfragen durch Sozialbehörden

Seit dem 1. April 2005 können aufgrund der neuen Regelungen des § 93 Abs. 7 und 8 Abgabenordnung (AO) über das Bundesamt für Finanzen Kontenabfragen durch Finanzbehörden für steuerliche Zwecke (Abs. 7) und Kontenabfragen durch Finanzbehörden für andere Behörden und Gerichte für bestimmte außersteuerliche Zwecke (Abs. 8) durchgeführt werden. Ich habe mich bei einem Kontroll- und Informationsbesuch über die Durchführung des Verfahrens zu den Kontoabrufen informiert, durch das bisher die meisten Ersuchen gestellt worden sind. Hierbei habe ich keine datenschutzrechtlichen Verstöße festgestellt (Näheres hierzu unter IV.5).

Das Finanzamt hat bisher auch einen Kontenabruf nach § 93 Abs. 8 AO für eine andere Behörde durchgeführt. Im Rahmen eines Kontroll- und Informationsbesuches habe ich mich bei dieser kommunalen Behörde vor Ort ebenfalls über das Verfahren zu diesem Kontenabruf informiert. Das Kontenabrufersuchen wurde dort im Rahmen eines Wohngeldverfahrens gestellt. Die Entscheidung für den Kontenabruf ist jedoch nicht nachvollziehbar dargelegt worden. Zum einen ist der Kontenabruf noch vor der Frist erfolgt, bis zu welcher der Antragsteller die für die Wohngeldberechnung erforderlichen Unterlagen hätte nachreichen können. Zum anderen hält die für die Zulässigkeit des Kontenabrufs erforderliche Prognoseentscheidung den gesetzlichen Anforderungen nicht stand, da sie in erster Linie auf subjektive Kriterien gestützt wurde. Außerdem ist das Ergebnis des Kontenabrufs geöffnet und zu den Akten genommen worden, obwohl zu diesem Zeitpunkt schon ein ablehnender Wohngeldbescheid ergangen war. Der Antragsteller ist zwar vorab über die Möglichkeit, nicht jedoch über die Durchführung des Kontenabrufs informiert worden.

Ich habe darauf hingewiesen, dass die Frist bis zur Einreichung aller Unterlagen in jedem Fall einzuhalten und dass die Prognoseentscheidung anhand objektiver und rechtlich nachvollziehbarer Kriterien zu treffen ist. Weiterhin habe ich empfohlen, das Ergebnis des Kontenabrufs ungeöffnet zu den Akten zu nehmen bzw. datenschutzgerecht zu vernichten, wenn sich der Anlass im laufenden Kontenabrufverfahren erledigt hat, und der Betroffene in jedem Fall über die Durchführung eines Kontenabrufs zu informieren ist.

18 Ich empfehle der Landesregierung, die Ausführungshinweise des Finanzministeriums und die Vollzugshinweise für die Durchführung des Wohngeldgesetzes des Ministeriums für Arbeit, Bau und Landesentwicklung um eine Regelung für den Fall zu ergänzen, wie mit dem Ergebnis des Kontenabrufes verfahren werden soll,

wenn sich der Anlass für einen Kontenabruf im laufenden Verwaltungsverfahren erledigt hat.

2.7 Dürfen Stadtvertreter wissen, wie viel Geschäftsführer ihrer kommunalen Unternehmen verdienen?

Ein Stadtvertreter begehrte vom Bürgermeister Auskunft über die Gehälter in den Unternehmen des privaten Rechts, an denen die Stadt die Mehrheit der Anteile hält. Wenn es sich dabei nur um eine einzelne Stelle handelt, sollte auch die Gehaltsgruppe angegeben werden. Der Bürgermeister sah hier datenschutzrechtliche Belange der Geschäftsführer berührt, weil gerade diese Position in der Regel nur einmal besetzt ist. Deshalb hat er mich um eine Stellungnahme gebeten. Wegen der Grundsätzlichkeit der Angelegenheit habe ich ein umfangreiches Gutachten hierzu erstellt und in meinem Internetangebot veröffentlicht.

Die Kommunalverfassung des Landes (KV M-V) regelt die entsprechenden Informations- und Prüfungsrechte der Gemeinde bei Unternehmen oder Einrichtungen des privaten Rechts, an denen sie unmittelbar oder mittelbar die Mehrheit der Anteile hält (§ 22 Abs. 2 in Verbindung mit § 73 KV M-V). So ist der Gemeindevertretung ein Wirtschaftsplan sowie die Finanzplanung des Unternehmens zur Kenntnis zu geben. Zum Wirtschaftsplan gehört eine Stellenübersicht, welche die organisatorische Gliederung widerspiegeln und nach Besoldungs-, Vergütungs- und Lohngruppen gegliedert sein muss.

Vor diesem rechtlichen Hintergrund und in Anbetracht der Rechte der Gemeinde-/Stadtvertreter halte ich es für zulässig, dass sie einen Stellenplan erhalten – selbst dann, wenn diese Angaben personenbeziehbar sind, weil die Gemeinde-/Stadtvertreter in der Regel die Person kennen, die den Betrieb leitet beziehungsweise ihm vorsteht. Dieses Vorgehen entspräche dem Verfahren der öffentlichen Verwaltung, denn die Besoldungsstufe eines Bürgermeisters oder eines Beigeordneten ergibt sich beispielsweise aus der Kommunalbesoldungsverordnung, die eines leitenden Beamten des Landes aus dem Landesbesoldungsgesetz.

Die Grenze der Auskunftserteilung liegt dort, wo konkret nach dem Einkommen einer einzelnen Person gefragt wird. Wenn also ein Gemeinde-/Stadtvertreter fragt, in welche Gehaltsgruppe ein namentlich genannter Mitarbeiter eines kommunalen Betriebes eingeordnet ist, greift dies in schützenswerte Interessen des Betroffenen ein und unterliegt deshalb nicht der Auskunftspflicht. Abgesehen davon dürfte ein solches Datum bei der Verwaltung nicht vorhanden sein, denn es sind ihr nur Stellenpläne und keine Namenslisten mit Gehaltsgruppen vorzulegen.

Ich habe den Bürgermeister sowie den Städte- und Gemeindetag und den Landkreistag Mecklenburg-Vorpommern über meine Rechtsauffassung informiert.

19 Der Landesregierung empfehle ich, bei der Novellierung der Vorschriften der Kommunalverfassung Mecklenburg-Vorpommern über die Informations- und Prüfungsrechte der Gemeinde bei Unternehmen oder Einrichtungen des privaten Rechts klarstellende Regelungen zur Zulässigkeit der Datenübermittlung an die Gemeindevertreter im Rahmen ihrer Kontrollfunktion aufzunehmen.

2.8 Tonbandmitschnitte in Sitzungen der Gemeindevertretung

Mitglieder einer Gemeindevertretung hatten sich an mich gewandt und zu folgendem Sachverhalt um eine datenschutzrechtliche Bewertung gebeten:

In den Sitzungen der Gemeindevertretung wurden in der Vergangenheit nur kontrovers diskutierte Tagesordnungspunkte auf Tonband aufgezeichnet, was die Anwesenden dann jeweils auch zur Kenntnis nehmen konnten. Dies geschah ohne förmlichen Beschluss im gegenseitigen Einvernehmen. Bei einer Sitzung erfolgte jedoch erstmals eine komplette Aufzeichnung des Sitzungsgeschehens einschließlich der Einwohnerfragestunde, ohne dass hierauf gesondert hingewiesen wurde.

Nach § 29 Abs. 8 Kommunalverfassung Mecklenburg-Vorpommern ist über jede Sitzung der Gemeindevertretung eine Niederschrift zu fertigen. Das Nähere ist durch die Geschäftsordnung zu regeln. Nach der Geschäftsordnung der Gemeinde durften Tonaufzeichnungen unterstützend für das Erstellen des Protokolls gefertigt werden, die dann zur Klärung von Unstimmigkeiten herangezogen werden und nach Genehmigung des Protokolls zu vernichten sind. Insofern waren die Voraussetzungen für einen Mitschnitt der gesamten Sitzung gegeben und es bedurfte keines besonderen Hinweises an die Gemeindevertreter. Da in der Vergangenheit dieses Verfahren nicht einheitlich gehandhabt wurde und Aufzeichnungen nur teilweise erfolgten, habe ich aber aus Gründen der Transparenz empfohlen, die Gemeindevertreter über die Aufzeichnung nochmals zu informieren.

Sofern jedoch Bürger zu Beginn der Sitzung bei der Einwohnerfragestunde auftreten und Fragen stellen oder Vorschläge unterbreiten, halte ich im Hinblick auf deren Persönlichkeitsrechte einen entsprechenden Hinweis durch die Sitzungsleitung immer für erforderlich, da diese die Geschäftsordnung nicht kennen und auch nicht mit einer Aufzeichnung rechnen müssen. Darüber hinaus handeln sie – im Gegensatz zu den Gemeindevertretern – nicht in Ausübung eines öffentlichen Amtes, sondern nehmen als Privatperson ihre Einwohnerrechte wahr. Daher sind sie über die Tatsache der Aufzeichnung und den Zweck sowie den weiteren Umgang hiermit zu informieren.

20 Ich empfehle der Landesregierung, die Gemeindevertretungen darauf hinzuweisen, dass Tonbandmitschnitte zur Protokollerstellung während einer Einwohnerfragestunde nur zulässig sind, wenn die Betroffenen hierüber in geeigneter Weise aufgeklärt wurden.

2.9 Einsicht in Unterschriftenlisten bei Bürgerbegehren

Im Zusammenhang mit einem Bürgerbegehren wurde ich gefragt, wie mit den Unterschriftenlisten umzugehen ist, insbesondere, ob diese der Öffentlichkeit zugänglich gemacht werden dürfen und ob die Mitglieder der Stadtvertretung ein Einsichtsrecht in die Listen beziehungsweise in die „nicht anerkannten“ Unterstützungsunterschriften erhalten können.

Nach § 20 Abs. 6 Kommunalverfassung Mecklenburg-Vorpommern (KV M-V) hat die Stadtvertretung über die Zulässigkeit eines Bürgerbegehrens im Benehmen mit der Rechtsaufsichtsbehörde zu entscheiden. Dabei ist insbesondere von Relevanz, ob die nach der Kommu-

nalverfassung erforderliche Unterschriftenzahl erreicht wurde. Das Bürgerbegehren darf nur durch Personen unterstützt werden, die am Tag des Eingangs des Antrags bei der Gemeinde zu den Gemeindewahlen wahlberechtigt sind. Ob diese Voraussetzung erfüllt ist, prüft die Verwaltung, da ausschließlich sie über die hierfür erforderlichen Informationen verfügt. Auf der Basis des Melderegisters werden die einzelnen Datensätze geprüft und die gültigen sowie ungültigen Stimmen vermerkt. Der Stadtvertretung ist das Ergebnis mitzuteilen, damit sie es in ihrer Entscheidung über die Zulässigkeit des Bürgerbegehrens berücksichtigen kann. Eine Bekanntgabe der in den Listen enthaltenen personenbezogenen Daten an die Öffentlichkeit durch Auslegung oder sonstige Veröffentlichung ist mangels Rechtsgrundlage unzulässig. Im Übrigen ließe sich auch die Notwendigkeit einer solchen Verfahrensweise nicht begründen.

Die Mitglieder der Stadtvertretung müssen für ihre Aufgabenerfüllung nicht wissen, wer im Einzelnen unterschrieben hat. Die Stadtvertretung entscheidet über die Zulässigkeit des Vorhabens insgesamt. Dafür ist es nicht erforderlich, die Gültigkeit der einzelnen Unterstützungsunterschriften zu überprüfen. Insofern ist es auch nicht notwendig, der Stadtvertretung mit dem Beschlussvorschlag die Unterschriftenlisten zur Verfügung zu stellen.

Ungeachtet dessen hat die Stadtvertretung aber die Kontrollmöglichkeit nach § 34 Abs. 4 KV M-V. Auf Antrag eines Viertels der Stadtvertretung oder einer Fraktion ist einzelnen, namentlich benannten Mitgliedern der Stadtvertretung Akteneinsicht zu gewähren, soweit dem nicht schutzwürdige Belange Betroffener oder Dritter oder zu schützende Interessen des Landes oder des Bundes entgegenstehen. Die Entscheidungsbefugnis über die Zulässigkeit des Vorhabens erfordert auch ein Kontrollrecht und damit die Einsichtnahme in die Listen einschließlich der Unterschriften, die für ungültig erklärt wurden. Gleiches muss aber auch für die Einreicher des Bürgerbegehrens gelten, insbesondere wenn das Erreichen des Quorums angezweifelt wird. Die zur Kenntnis genommenen personenbezogenen Daten dürfen aber nur für diesen Zweck genutzt werden. Darüber hinaus sind die Stadtvertreter gemäß § 23 Abs. 6 KV M-V auch zur Verschwiegenheit verpflichtet.

Dem behördlichen Datenschutzbeauftragten der Stadt habe ich meine Auffassung mitgeteilt.

21 Ich empfehle der Landesregierung zu prüfen, ob zum Umgang mit personenbezogenen Daten im Rahmen von Bürgerbegehren Regelungen in die Kommunalverfassung aufgenommen werden sollten, um hier mehr Rechtssicherheit zu erreichen.

2.10 Verbleib der Mitteilungen der Bundesbeauftragten für die Stasi-Unterlagen bei Privatisierungen?

Nach dem Stasi-Unterlagen-Gesetz (StUG) konnten öffentliche Arbeitgeber ihre Beschäftigten auf eine Tätigkeit für das Ministerium für Staatssicherheit/Amt für nationale Sicherheit überprüfen. Im Zusammenhang mit der Privatisierung eines kommunalen Unternehmens wurde ich gefragt, wie mit den Mitteilungen der Bundesbeauftragen für die Stasi-Unterlagen, die Bestandteil der Personalakte sind, nach dem Übergang in ein privat-rechtliches Unternehmen zu verfahren ist.

Ein Betriebsübergang richtet sich nach den Vorschriften des Bürgerlichen Gesetzbuches (BGB). Danach tritt der Rechtsnachfolger in die Rechte und Pflichten aus dem im Zeitpunkt des Übergangs bestehenden Arbeitsverhältnis ein. Mit dem Betriebsübergang geht auch das Eigentum an den Personalunterlagen über. Der vorhergehende Arbeitgeber hat dafür Sorge zu tragen, dass die Personalakten zum Zeitpunkt des Übergangs den aktuellen Maßgaben des Personalaktenrechts entsprechen. Dies bedeutet insbesondere auch, dass er die Personalakten vor der Übergabe an den nachfolgenden Arbeitgeber dahingehend zu prüfen hat, ob sie Daten enthalten, die aufgrund besonderer Vorschriften verarbeitet wurden und damit einem speziellen Schutz unterlagen, der den Regelungen des BGB vorgeht.

Nach dem StUG ist eine generelle Überprüfung nur für Mitarbeiter des öffentlichen Dienstes vorgesehen. Somit dürfen auch nur öffentliche Stellen die Informationen der Bundesbeauftragten für die Stasi-Unterlagen nutzen. Eine Weitergabe dieser Daten an einen privatrechtlich organisierten Eigentümer ist aufgrund dieser strengen Zweckbindung unzulässig.

Da das StUG keine bereichsspezifischen Regelungen enthält, ob und unter welchen Voraussetzungen diese Daten an die Bundesbeauftragte für die Unterlagen der Staatssicherheit zurückzugeben oder zu vernichten sind, sollten sie bei Betriebsübergabe datenschutzgerecht vernichtet werden.

22 Ich empfehle der Landesregierung sowie allen weiteren öffentlichen Stellen, darauf zu achten, dass bei Privatisierungen öffentlicher Unternehmen die von der Bundesbeauftragten für die Unterlagen des Staatssicherdienstes übermittelten Daten vor dem Betriebsübergang datenschutzgerecht vernichtet werden. Im Übrigen dürfen die Unterlagen nur bis Ende des Jahres 2006 für die Überprüfung von Mitarbeitern des öffentlichen Dienstes genutzt werden. Vor diesem Hintergrund ist dafür zu sorgen, dass die in den Personalakten enthaltenen Daten danach durch alle personalbearbeitenden Dienststellen gelöscht werden.

2.11 Aktenfund – Eigentümerwechsel mit Folgen

Bei der Versteigerung eines ehemaligen Kindergartens einer Gemeinde waren Privatpersonen in den Besitz von alten Unterlagen mit personenbezogenen Daten gekommen, die überwiegend noch aus DDR-Zeiten stammen. Darunter befanden sich beispielsweise Lohn- und Personalunterlagen, die Einwohnermeldekartei der Gemeinde, Bauakten, Gemeinderatsprotokolle und Schriftstücke zu „kriminell gefährdeten“ Bürgern, also auch sehr sensible Daten.

Die Akten lagen bereits seit mehreren Jahren im leer stehenden Gebäude. Der genaue Zeitpunkt war nicht mehr feststellbar. Diese – ursprünglich wohl nur zwischengelagerten – Unterlagen wurden seinerzeit schlichtweg vergessen und als „stilles Erbe“ in das 2004 neu gebildete Amt eingebracht. Im Vorfeld der Versteigerung war offensichtlich das Inventar des Gebäudes nicht geprüft worden, so dass die neue Amtsverwaltung von den Unterlagen keine Kenntnis hatte. Nach der Versteigerung wurden die Akten von den Erwerbern des Gebäudes weitergegeben und waren in die Hände eines Bürgers gelangt, der für sich in Anspruch nahm, auch das Eigentum daran erworben zu haben, und deshalb deren Herausgabe gegenüber dem Amt verweigerte.

Durch diesen außerordentlichen Vorfall erhielten unberechtigte Dritte detaillierte Informationen über jetzige und ehemalige Einwohner der Gemeinde. Gegenüber dem Amt als Rechtsnachfolger habe ich deshalb eine Beanstandung gemäß § 32 Abs. 1 Nr. 2 Landesdatenschutzgesetz (DSG M-V) aufgrund folgender Datenschutzverstöße ausgesprochen:

- Es wurden keine Maßnahmen getroffen, um die Vertraulichkeit, die Vollständigkeit sowie die jederzeitige Verfügbarkeit der personenbezogenen Daten gemäß § 21 Abs. 2 Nr. 1, 2 und 3 DSG M-V zu gewährleisten.
- Die alten Meldekarteien, die aufgrund der Einführung des elektronischen Melderegisters nicht mehr zur Aufgabenerfüllung der Meldebehörde benötigt wurden, hätten gemäß § 44 Abs. 3 LMG archiviert werden müssen.
- Die Akten hätten, da sie von der Gemeinde beziehungsweise dem Amt nicht mehr zur Aufgabenerfüllung benötigt wurden, gemäß § 12 Landesarchivgesetz sowie § 13 Abs. 2 und 6 DSG M-V dem zuständigen Archiv angeboten und bei einer Ablehnung der Übernahme vernichtet werden müssen.

Da dieser Vorfall insgesamt erhebliche datenschutzrechtliche Auswirkungen hatte, habe ich der Amtsverwaltung empfohlen, alle Vorkehrungen zu treffen, um die Akten schnellstmöglich wieder in Besitz nehmen zu können.

Die Amtsverwaltung hat umgehend darauf reagiert und alle notwendigen Schritte eingeleitet. Da der Besitzer der Akten – trotz eindringlichen Zuredens der Amtsverwaltung und auch meinerseits – sich hartnäckig weigerte, diese herauszugeben, wurde er im Wege einer einstweiligen gerichtlichen Anordnung verpflichtet, bis zur endgültigen Klärung im Hauptsacheverfahren die Akten vorläufig an das Amtsgericht herauszugeben. Des Weiteren wurde ihm unter Androhung eines Ordnungsgeldes bis zu 100.000 € untersagt, die Unterlagen an einen anderen Ort zu verbringen oder deren Inhalt zu vervielfältigen oder Dritten zugänglich zu machen.

Mittlerweile wurden die Akten beim Amtsgericht hinterlegt. Die Entscheidung des Verwaltungsgerichts in der Hauptsache bleibt abzuwarten. Ich gehe davon aus, dass das Amt die Akten nach Abschluss des verwaltungsgerichtlichen Verfahrens wieder übernehmen wird, so dass dann entsprechend den datenschutz- und archivrechtlichen Vorschriften verfahren werden kann.

23 Ich empfehle der Landesregierung vor dem Hintergrund weiterer Fusionen im kommunalen Bereich, dafür Sorge zu tragen, dass die ordnungsgemäße Übergabe von Aktenbeständen sowie die Verantwortlichkeiten, die Fristen, die Archivierung beziehungsweise die Vernichtung der Unterlagen verbindlich geregelt wird.

2.12 Ausschreibungen von Ausländern zur Einreiseverweigerung im Schengener Informationssystem

Die Gemeinsame Kontrollinstanz für das Schengener Informationssystem (SIS) hat sich darauf verständigt, die Ausschreibungspraxis im Rahmen von Artikel 96 des Schengener Durchführungsübereinkommens (SDÜ) in allen Vertragsstaaten zu prüfen.

Artikel 96 SDÜ sieht Ausschreibungen im Schengener Informationssystem von Drittausländern vor, um diesen Personen die Einreise in das Schengengebiet zu verweigern. Dies betrifft Personen, die insbesondere wegen einer Straftat, die mit mindestens einem Jahr Freiheitsstrafe bedroht ist, verurteilt wurden oder bei denen ein begründeter Verdacht besteht, dass sie schwere Straftaten begangen haben beziehungsweise konkrete Hinweise dafür vorliegen, dass sie solche planen. Ferner können Drittausländer ausgeschrieben werden, die ausgewiesen, zurückgewiesen oder abgeschoben wurden, wobei die Maßnahme nicht aufgeschoben oder aufgehoben worden sein darf, ein Verbot der Einreise oder des Aufenthalts enthalten oder davon begleitet sein muss und auf der Nichtbeachtung des nationalen Rechts über die Einreise oder den Aufenthalt von Ausländern beruhen muss.

Der Bundesbeauftragte für den Datenschutz hat die beim Bundeskriminalamt auf der Basis eines Zufallsgenerators ausgewählten Prüffälle zu diesem Zweck an die Landesbeauftragten für den Datenschutz übersandt. Für unser Bundesland waren sechs Fälle zu prüfen.

Dabei habe ich unter anderem Folgendes festgestellt:

- In allen Fällen handelte es sich um Drittausländer.
- In einem Fall lagen die Voraussetzungen für eine Ausschreibung im SIS nach Artikel 96 SDÜ nicht vor.
- In drei Fällen wurde bei Verlängerung der Speicherung im SIS entsprechend Artikel 112 Abs. 1 SDÜ nicht deren Erforderlichkeit geprüft. Mangels Dokumentation war die Verlängerung der Speicherfrist nicht nachvollziehbar. Ein Fall wurde im Zuge unserer Prüfung gelöscht, da eine weitere Speicherung sich nicht als erforderlich herausstellte.
- Mit der Löschung der Ausschreibung wurden die Unterlagen regelmäßig nicht vernichtet. Die Erforderlichkeit einer weiteren Aufbewahrung muss im Einzelfall aber belegt werden.
- Einige Ausländerbehörden koppelten die Ausschreibungsfrist im SIS an das national unbefristet wirkende Einreiseverbot nach § 8 Abs. 2 Ausländergesetz (neu geregelt in § 11 Abs. 1 Satz 1und 2 Aufenthaltsgesetz 2004), was ich aus datenschutzrechtlicher Sicht für problematisch erachte.

Ich habe den Bundesbeauftragten für den Datenschutz über meine Feststellungen informiert. Er hat die nationalen Ergebnisse an die Gemeinsame Kontrollinstanz (GKI) zur schengenweiten Auswertung weitergeleitet. Die GKI hat im Rahmen dieser Untersuchungen unter anderem herausgefunden, dass die Speicherung in den einzelnen Staaten sehr unterschiedlich ausfällt, und deshalb empfohlen, im gesamten Schengen-Gebiet eine einheitliche Erfassungsdauer vorzusehen.

24 Ich empfehle der Landesregierung, die Ausländerbehörden darauf hinzuweisen, dass das Vorliegen der Voraussetzungen für die Speicherung im Schengener Informationssystem in jedem Einzelfall genau zu prüfen und zu dokumentieren ist.

2.13 Dokumentation erweiterter Melderegisterauskünfte

Die Meldebehörde einer Stadt hatte ihre erweiterten Melderegisterauskünfte mit dem Hinweis versehen, dass die Anfrage nicht aufbewahrt werde. Eine Dokumentation der Anfragen fand nur statt, wenn die betroffene Person, über die Auskunft erteilt wurde, zu benachrichtigen war. Ein Petent hatte Bedenken gegen diese Verfahrensweise und hat mich gebeten, den Sachverhalt zu klären.

Bei einer erweiterten Melderegisterauskunft nach § 34 Abs. 2 Landesmeldegesetz (LMG) erhält der Anfragende von der Meldebehörde neben Namen, Doktorgrad und Anschrift einer bestimmten Person weitere Angaben, zum Beispiel Tag und Ort der Geburt, Staatsangehörigkeiten, verheiratet oder nicht sowie frühere Anschriften. Zuvor muss der Antragsteller jedoch sein berechtigtes Interesse an der Kenntnis dieser Daten glaubhaft gemacht haben. Über die erweiterte Melderegisterauskunft ist die betroffene Person unverzüglich zu unterrichten, es sei denn, der Antragsteller hat ein rechtliches Interesse an der Auskunft, weil er beispielsweise ein Gläubiger ist, der Zahlungsansprüche gegenüber seinem Schuldner hat und für diese Zwecke die entsprechende Auskunft benötigt. Der Empfänger darf gemäß § 34 Abs. 4 LMG die Daten nur für den von ihm gegenüber der Meldebehörde angegebenen Zweck nutzen.

Die fehlende Dokumentation der erweiterten Melderegisterauskünfte habe ich gegenüber der Meldebehörde als Datenschutzverstoß bemängelt. Ohne Dokumentation kann im Nachhinein nicht geklärt werden, ob eine Auskunft zu Recht erteilt wurde. Somit ist weder eine datenschutzrechtliche noch eine verwaltungsgerichtliche Kontrolle möglich. Verwendet ein Antragsteller die ihm erteilte Auskunft für einen anderen Zweck, oder macht er die Daten Dritten ohne Zustimmung der Meldebehörde zugänglich, so ist dies eine Ordnungswidrigkeit, die mit einer Geldbuße geahndet werden kann. Dasselbe gilt für Fälle, in denen der Antragsteller sich die Auskunft durch unrichtige oder unvollständige Angaben erschlichen hat. Ohne eine hinreichende Dokumentation der Vorgänge laufen die datenschutzrechtlichen Bestimmungen jedoch im Streitfall leer, und es ist nicht nachprüfbar, ob die personenbezogenen Daten der Betroffenen entsprechend den gesetzlichen Vorgaben verarbeitet wurden.

Die Meldebehörde hat sich im Ergebnis meiner Auffassung angeschlossen und wird künftig die erweiterten Melderegisterauskünfte nachvollziehbar dokumentieren.

25 Ich empfehle der Landesregierung, die Meldebehörden auf ihre Dokumentationspflichten bei erweiterten Melderegisterauskünften hinzuweisen, deren Einhaltung im Rahmen der Fachaufsicht zu prüfen und bei einer Neugestaltung des Verfahrens die Dokumentationspflichten zu berücksichtigen.

2.14 Parkscheinautomaten ohne Datenschutz

Eine Stadt betreibt Parkscheinautomaten, an denen man sowohl bar als auch mit EC-Karten ohne PIN-Eingabe bezahlen kann. Einem Petenten hatte die Stadt von seinem Konto Parkgebühren für einen Tag im Januar 2005 abgebucht, ohne dass er jemals mit seiner EC-Karte den Automaten benutzt hatte. Er hatte auch nicht an diesem Tag dort geparkt und bat die Stadt um Aufklärung. Diese teilte ihm nach mehreren Monaten Datum, Uhrzeit und den genauen Parkplatz mit, auf dem er geparkt haben sollte. Das Datum lag vier Monate vor dem Buchungsda-

tum. Der Buchungsdatensatz sei erst Anfang Januar vom Automaten weitergeleitet worden. Auf die Technik habe man aber keinen Einfluss. Überdies sei es zur verzögerten Bearbeitung gekommen, weil die Buchungssätze hierzu einzeln manuell durchsucht werden mussten. Da der Petent zu dem genannten Zeitpunkt gar nicht im Lande war, vermutete er einen Missbrauch seiner Daten und wandte sich an mich.

Das zuständige Amt der Stadt teilte mir mit, dass es keine personenbezogenen Daten verarbeite und alle erforderlichen Maßnahmen zur IT-Sicherheit getroffen hätte. Die EC-Karte des Petenten müsse Kontakt mit einem Automaten gehabt haben. Dass die Daten in dem Buchungssatz nicht mit dem Parkdatum übereinstimmen, sei bedauerlich, aber hinzunehmen. Überdies sei zwar ein Dienstleister mit der Wartung der Geräte beauftragt worden, nicht aber mit der Verarbeitung personenbezogener Daten.

Einer datenschutzrechtlichen Prüfung hielten diese Aussagen nicht stand. Bankleitzahl und Kontonummer sind selbstverständlich personenbezogene Daten, denn zumindest die Konto führende Bank kann anhand dieser Zahlen ohne weiteres den oder die Inhaber des Kontos ermitteln. Es kommt nicht darauf an, ob die Stadt dies auch kann.

Das zuständige Amt konnte mir nur sehr lückenhaft beschreiben, welche technischen und organisatorischen Maßnahmen zum Datenschutz getroffen wurden (§ 21 DSG M-V). Die Sicherheitseigenschaften der Automaten und des Datennetzes der Stadt konnte das Amt nicht einmal in Ansätzen darstellen, auch nicht nach einer Befragung des Automatenherstellers. Damit liegt ein Verstoß gegen das Transparenzgebot (§ 21 Abs. 2 Nr. 6 DSG M-V) vor. Zudem fehlt das Sicherheitskonzept (§ 22 Abs. 5 DSG M-V). Weil die Protokolldaten nur unter großen Schwierigkeiten ausgewertet werden konnten, ist auch die Revisionsfähigkeit (§ 21 Abs. 2 Nr. 5 DSG M-V) nicht gegeben.

Die Behauptung des Amtes, dass die EC-Karte des Petenten Kontakt mit dem Automaten gehabt haben müsse, kann so nicht belegt werden. Ein Missbrauch der Daten des Petenten oder ein Systemfehler kann ebenfalls nicht ausgeschlossen werden. Ob unter diesen Umständen die Gebühren überhaupt zu Recht erhoben worden sind, kann letztlich nur gerichtlich geklärt werden.

Überdies hat das Amt auch die Vorschriften zur Datenverarbeitung im Auftrag verletzt (§ 4 DSG M-V). So hat es nicht ausreichend geprüft, ob die technischen und organisatorischen Maßnahmen des Auftragnehmers den Anforderungen des Landesdatenschutzgesetzes entsprechen. Ferner hat das Amt nicht dafür gesorgt, dass sich sein Auftragnehmer meiner Kontrolle unterwirft und mich nicht über die Beauftragung informiert (§ 4 Abs. 3 DSG M-V).

Aufgrund dieser Verstöße habe ich der Stadt eine förmliche Beanstandung ausgesprochen und die Kommunalaufsicht im Innenministerium informiert (§ 32 Abs. 1 DSG M-V). Das Amt hat bisher jegliche Datenschutzverstöße bestritten und keinerlei Schritte zu deren Beseitigung unternommen. Ich habe empfohlen, die EC-Kartenzahlung bis zur Klärung der IT-Sicherheitsfragen außer Betrieb zu nehmen. Eine Stellungnahme der Stadt, in der auch Maßnahmen zur Beseitigung der Missstände aufzuführen sind (§ 32 Abs. 3 DSG M-V), steht noch aus.

2.15 Melderegister vereitelt Wahlrecht

Zur Bundestagswahl im September 2005 hatten zwei Einwohnerinnen einer Gemeinde keine Wahlbenachrichtigungskarten erhalten. Eine der Betroffenen meldete sich noch rechtzeitig vor der Wahl bei der Gemeinde. Die andere hingegen versäumte dies und musste am Wahltag feststellen, dass sie auch nicht im Wählerverzeichnis eingetragen war und deshalb nicht wählen durfte.

Ursache war eine falsche Datenspeicherung im Melderegister, aus dem das Wählerverzeichnis mit den Daten der Wahlberechtigten erstellt worden waren. Das Melderegister ist nicht ein bloßes Registrierungssystem der Einwohner, sondern zugleich wichtige Informations- und Auskunftsquelle für viele öffentliche, aber auch für private Stellen. Daher kann eine fehlerhafte Datenspeicherung im Melderegister, die nicht rechtzeitig bemerkt wird, für Betroffene erhebliche Folgen haben.

Bei der Ämterfusion zu Beginn des Jahres 2005 wurden die drei Melderegister der beteiligten Stellen zusammengeführt. Die Migration der Daten aus drei unterschiedlichen Softwareprogrammen verlief nicht ganz fehlerfrei. So hatten einige Einwohner den Status „verzogen“ erhalten, andere Einwohner hingegen tauchten nunmehr doppelt im Melderegister auf. Die Verantwortlichen hatten vor der Datenübernahme Sicherungskopien gefertigt und nach der Migration ein Fehlerprotokoll erstellen lassen. Auf dieser Basis wurden die meisten der aufgezeigten Fehler berichtigt. Übersehen wurden jedoch die fehlerhaften Datensätze der zwei Einwohnerinnen.

Im Zuge der Bundestagswahl hat die Verwaltung nun auch diese Daten im Melderegister berichtigt und mitgeteilt, dass es sich hierbei um Einzelfälle handelte.

2.16 Videoüberwachung von Fahrscheinautomaten

In den vergangenen Jahren musste ein Nahverkehrsunternehmen mit erheblichem Aufwand die durch Vandalismus entstandenen Schäden an Fahrscheinautomaten beseitigen. Deshalb hatte es sich mit der Frage an mich gewandt, unter welchen Voraussetzungen eine Videoüberwachung der an einigen Haltestellen aufgestellten Fahrscheinautomaten zulässig sei, um so gegen die Täter vorgehen zu können.

Bei den kommunalen Verkehrsunternehmen handelt es sich um öffentliche Stellen des Landes, die als Wettbewerbsunternehmen gemäß § 2 Abs. 5 Landesdatenschutzgesetz (DSG M-V) die materiell-rechtlichen Vorschriften des Bundesdatenschutzgesetzes (BDSG) zu beachten haben. § 6b Abs. 1 BDSG lässt eine Beobachtung öffentlich zugänglicher Räume mit Videoüberwachungstechnik unter anderem zu, wenn es zur Wahrnehmung des Hausrechtes oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Hinsichtlich der Aufzeichnung sind der Erforderlichkeitsaspekt sowie die schutzwürdigen Interessen der Betroffenen nochmals gesondert zu prüfen.

Um die Voraussetzungen des § 6b BDSG zu erfüllen, beabsichtigt das Unternehmen, die Grundstücke, auf denen sich die Wartehäuschen befinden, zu erwerben und die Fahrscheinautomaten in diese zu integrieren. Die Kameras sollen dann so eingestellt werden, dass nur der

Innenbereich überwacht wird. Dies werde für Betroffene, die das Wartehäuschen betreten, deutlich sichtbar gemacht. Hinsichtlich der offenen Seite des Wartehäuschens sei ferner daran gedacht, hier gegebenenfalls eine Markierungslinie vorzusehen, um den überwachten Bereich deutlich zu machen. Die Aufzeichnungen sollen im Schadensfall dazu dienen, zivilrechtliche Ansprüche gegen den Täter geltend zu machen und eine Strafverfolgung zu ermöglichen.

Die Videoüberwachung führt zwangsläufig zur Erfassung einer Vielzahl sich rechtstreu verhaltender Betroffener. Ich halte das Vorhaben deshalb nur in sehr engen Grenzen für zulässig. Dem Unternehmen habe ich daher mitgeteilt, dass ich für seine Überlegungen unter Berücksichtigung der dargelegten Aspekte grundsätzlich Verständnis habe, jedoch mit Blick auf die schutzwürdigen Belange der Betroffenen weitere Punkte zu beachten seien. So ist hinsichtlich der Angemessenheit der Maßnahme festzustellen, dass eine Aufzeichnung rund um die Uhr nicht erforderlich erscheint, da die Schäden an den Automaten in der Regel nur in den Abend- und Nachtstunden entstehen. Ferner müssten die Betroffenen offensiv auf den Umstand der Überwachung hingewiesen werden, damit sie ihr Verhalten darauf einstellen und beispielsweise Fahrscheine im Vorverkauf in anderen Verkaufsstellen erwerben können.

Ich habe empfohlen, diese Punkte in die Prüfung einzubeziehen und, falls die Überlegungen weiterverfolgt werden, mir rechtzeitig ein Datenschutzkonzept zu übersenden, damit ich auch künftig beratend tätig werden kann.

2.17 Schutzprofile für Videoanlagen als Hilfsmittel beim Kauf

Wenn im Einzelfall geklärt ist, dass eine Videoüberwachungsanlage beispielsweise zur Wahrnehmung des Hausrechts generell erforderlich und rechtlich zulässig ist, stellt sich für den potentiellen Nutzer in der öffentlichen Verwaltung immer die Frage, welches am Markt verfügbare Produkt für seinen konkreten Einzelfall geeignet ist. Dazu müssen in einem Pflichtenheft zunächst die technischen Anforderungen definiert werden. In einem recht aufwändigen Beschaffungsverfahren ist dann zu prüfen, welche Produkte diese Anforderungen erfüllen. Oft sind die Mitarbeiter der Beschaffungsstellen überfordert, die vielfältigen Angaben der Herstellerprospekte zu beurteilen und zu bewerten.

Zur Unterstützung dieses Auswahlverfahrens bietet der Bundesbeauftragte für den Datenschutz mit einem so genannten Schutzprofil (Protection Profile) ein Hilfsmittel an. In diesem Schutzprofil sind bereits konkrete, aus datenschutzrechtlichen Vorgaben resultierende Anforderungen an die Funktion und Vertrauenswürdigkeit der zentralen Komponenten einer Videoanlage beschrieben. Beispielsweise wird festgelegt, wie Aufzeichnungsgeräte für Bild-, Protokoll- und Konfigurationsdaten auszugestalten sind und welche Eigenschaften die Bediengeräte für Nutzer, Administratoren und Revisoren einer solchen Anlage haben müssen. Somit können potentielle Käufer die eigenen Anforderungen an die von ihnen gewünschte Anlage schon sehr genau definieren.

Jeder Hersteller von Videoanlagen kann nun sein Produkt so entwickeln, dass die Anforderungen des Schutzprofils erfüllt werden. Da Schutzprofile auf dem Regelwerk der Common Criteria – einem internationalen Standard für die Prüfung und Bewertung der Sicherheit von Informationstechnik – basieren, können die Produkte in einem international anerkannten, förmlichen Verfahren geprüft werden (siehe auch Sechster Tätigkeitsbericht, Punkt 2.18.2). Die Übereinstimmung zwischen den Sicherheitsanforderungen und den im Produkt tatsäch-

lich vorhandenen Sicherheitsfunktionen wird mit einem weltweit gültigen Zertifikat bestätigt. Dieses Zertifikat ermöglicht dem Nutzer, bereits vor dem Kauf einer Videoanlage zu beurteilen, ob seine Anforderungen umgesetzt werden können.

Um den Nutzen der Schutzprofile zu erläutern, hatte ich zur 45. Sitzung des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ im September 2005 Hersteller von Videoanlagen eingeladen (siehe Punkt A.0.). Im Ergebnis der Beratungen wurden folgende Eckpunkte festgehalten:

- Die Schutzprofile helfen dem Anwender bei der Formulierung der Anforderungen an die IT-Sicherheit und an den technischen Datenschutz von Videoüberwachungsanlagen. Zu trennen sind diese Anforderungen von der immer notwendigen Prüfung der rechtlichen Zulässigkeit des Einsatzes von Videoüberwachungsanlagen.
- Die Schutzprofile sind von der Zertifizierung der betreffenden Produkte zu trennen. Schutzprofile ermöglichen es zunächst dem Anwender, seine Anforderungen an ein Produkt konkret zu formulieren. Damit sind sie zwar gleichzeitig eine ideale Voraussetzung, um die so beschriebenen Produkte zertifizieren zu können. Die Existenz eines Schutzprofils zwingt jedoch keinen Hersteller, das darauf basierende Produkt tatsächlich zertifizieren zu lassen.
- Die Zertifizierung von Produkten ist für die Hersteller freiwillig. In welchem Umfang davon Gebrauch gemacht wird, regelt sich durch Marktmechanismen.

26 Ich empfehle den öffentlichen Stellen des Landes, vor der Beschaffung einer Videoüberwachungsanlage den behördlichen Datenschutzbeauftragten zu beteiligen sowie die technischen Anforderungen mit Hilfe des Schutzprofils zu beschreiben. Anbieter sollten bereits im Vergabeverfahren aufgefordert werden, die Kompatibilität ihrer Anlage mit den Anforderungen des Schutzprofils möglichst durch eine Zertifizierung nachzuweisen.

3 Polizei und Verfassungsschutz

3.1 Das Akkreditierungsverfahren zur Fußball-Weltmeisterschaft 2006

Die Durchführung der Fußball-Weltmeisterschaft 2006 erfordert vom Veranstalter zweifellos besondere Sicherheitsmaßnahmen. Aus diesem Grund ist vorgesehen, dass sich Personen, die Zugang zu bestimmten Stadionbereichen erhalten sollen, einem „Akkreditierungsverfahren“ zu unterziehen haben. Zu diesem Personenkreis, der rund 200.000 bis 250.000 Personen umfassen wird, gehören Angehörige der Presse, Mitarbeiter des Fernsehens, Polizeibeamte, Freiwillige und Servicebedienstete aller Sparten, zum Beispiel auch Würstchenverkäufer.

Das Akkreditierungsverfahren sieht vor, dass diese Personen sowohl von den Polizeibehörden als auch von den Verfassungsschutzbehörden der Länder ihres Hauptwohnsitzes hinsichtlich ihrer Unbedenklichkeit überprüft werden sollen. Zu diesem Zweck müssen die Betroffenen eine Einwilligungserklärung abgeben. Aus datenschutzrechtlicher Sicht genügt die Einwilligungserklärung für eine Datenübermittlung durch Polizei- und Verfassungsschutzbehörden nicht, und zwar auch dann nicht, wenn lediglich ein der Akkreditierung zustimmendes oder ablehnendes Votum abgegeben wird. Schon die Freiwilligkeit der Einwilligungserklärung ist zweifelhaft, da daran eine „Arbeitserlaubnis“ geknüpft ist. Betroffen sind durch die Maßnah-

me zahlreiche Arbeitnehmer, die auf Veranlassung ihrer Arbeitgeber Tätigkeiten in den Stadionbereichen vorzunehmen haben. Die Betroffenen werden die Erklärung im Zweifel schon deshalb abgeben, um im Arbeitsverhältnis keine negativen Folgen befürchten zu müssen, die mit der – bei fehlender Einwilligung zwingenden – Ablehnung der Akkreditierung zusammenhängen.

Schon das negative Votum eines einzelnen Landeskriminalamtes oder einer einzelnen Verfassungsschutzbehörde kann dazu führen, dass gegenüber dem Deutschen Fußballbund ein ablehnendes Votum ergeht. Auch die generelle Einbeziehung von beispielsweise Propagandadelikten, ohne dass ein Bezug zu Gewalttaten besteht, ist meines Erachtens im Hinblick auf die Wahrung des Verhältnismäßigkeitsgebotes kritisch zu werten.

Aus all diesen Gründen wäre – auch mit Blick auf die Ausrichtung des G8-Gipfels in Mecklenburg-Vorpommern 2007 – eine spezifische Rechtsgrundlage im Sicherheits- und Ordnungsgesetz sowie im Landesverfassungsschutzgesetz Mecklenburg-Vorpommern erforderlich, welche bei gefährdeten Großveranstaltungen Art und Umfang von Zuverlässigkeitsüberprüfungen regelt. Meine Auffassung habe ich den zuständigen Stellen mitgeteilt. Eine Antwort steht bisher noch aus.

27 Ich empfehle der Landesregierung und dem Landtag, ein Akkreditierungsverfahren bei Großveranstaltungen, die besondere Sicherheitsmaßnahmen erfordern, auf eine generelle gesetzliche Grundlage zu stellen.

3.2 Zuverlässigkeitsüberprüfung nach Luftsicherheitsgesetz

Das Luftsicherheitsgesetz dient dem Schutz vor Angriffen auf die Sicherheit des Luftverkehrs, insbesondere vor Flugzeugentführungen, Sabotageakten und terroristischen Anschlägen. Unbestreitbar kann die Überprüfung der Zuverlässigkeit des Flughafenpersonals einen Beitrag dazu leisten, solche Gefahren zu minimieren. Die Bezirksregierung Düsseldorf als Luftsicherheitsbehörde darf zu diesem Zweck beim Bundeskriminalamt und den Polizeivollzugsbehörden der Länder darüber Auskunft verlangen, ob und gegebenenfalls welche Daten über die betreffende Person in polizeilichen Dateien gespeichert sind.

Ein Petent hatte sich bei der Lufthansa um einen Ausbildungsplatz beworben. Er bekam daraufhin Antwort von der Bezirksregierung Düsseldorf, die besagte, es würden Bedenken hinsichtlich seiner Zuverlässigkeit bestehen. In dem Schreiben der Behörde wird ausgeführt, dass ein Verfahren gegen ihn geführt worden sei wegen Diebstahls mit Waffen/Bandendiebstahls. Als Erkenntnisquelle wird das Landeskriminalamt Mecklenburg-Vorpommern (LKA M-V) aufgeführt. Der junge Mann bestreitet die Tatvorwürfe. Das LKA M-V hatte zurückgemeldet, dass der Petent in einer landesweiten Datei mit der Straftat Diebstahl mit Waffen/Bandendiebstahl gespeichert sei.

Meine Nachforschungen haben ergeben, dass die Staatsanwaltschaft das betreffende Verfahren längst eingestellt hatte. Vom ursprünglichen Tatvorwurf war lediglich ein Verfahren wegen Hausfriedensbruchs übrig geblieben, welches das Amtsgericht nach dem Jugendgerichtsgesetz endgültig eingestellt hatte. Das falsche Datum war in der landesweiten polizeilichen Datei deshalb noch gespeichert, weil die Staatsanwaltschaft den Verfahrensausgang nicht an

das zuständige Kriminalkommissariat zurückgemeldet hatte. Es wurde aufgrund meiner Empfehlung sofort berichtigt.

Für den beruflichen Werdegang des Petenten hätte dieser Fehler fatale Folgen haben können. Erfreulicherweise hat er nach Aufklärung des Sachverhaltes seinen Ausbildungsplatz bei der Lufthansa bekommen.

Aus meiner Tätigkeit ist mir bekannt, dass es kein Einzelfall ist. Oft werden Ausgänge zu staatsanwaltschaftlichen Ermittlungsverfahren nicht an die Polizeidienststellen zurückgemeldet. Das LKA M-V hat daher diese Thematik noch einmal mit den Staatsanwaltschaften grundsätzlich erörtert. Es wurde zugesichert, diese Mitteilungen künftig vorzunehmen.

28 Ich empfehle der Landesregierung, Vorkehrungen zu treffen, damit sowohl die Staatsanwaltschaften als auch die Polizei aktuelle Ausgänge zu Ermittlungsverfahren mitteilen und die sich daran anschließende Korrektur von Eintragungen in Dateien und Verzeichnissen durchgeführt wird. Dies ist den Betroffenen auch in jedem Fall mitzuteilen.

3.3 Biometrie in Ausweisdokumenten

Deutsche Reisepässe, die ab dem 1. November 2005 beantragt werden, enthalten einen elektronischen Speicherchip, in dem neben dem Namen, dem Geburtstag und dem Geschlecht auch biometrische Merkmale des Gesichts des Passinhabers gespeichert werden. Die entsprechende Verordnung des Europäischen Rates verpflichtet die Mitgliedstaaten allerdings erst zur Mitte des Jahres 2006, biometriegestützte Pässe auszugeben. Das hat seinen guten Grund, denn noch immer weisen biometrische Identifikationsverfahren hohe Falscherkennungsraten auf. Die Technik für die Ausweise ist noch nicht ausgereift.

Die Leistungsfähigkeit biometrischer Verfahren wurde in den vergangenen Jahren intensiv untersucht. Im Ergebnis mussten diesen Verfahren noch erhebliche Mängel bescheinigt werden (siehe Sechster Tätigkeitsbericht, Punkt 2.19.1). Das Büro für Technikfolgenabschätzung beim Deutschen Bundestag (TAB) hat Fragen der Biometrie in Ausweisdokumenten erneut untersucht und die Ergebnisse dem Bundestagsausschuss für Bildung, Forschung und Technikfolgenabschätzung vorgelegt (BT-Drs. 15/4000 vom 21. Oktober 2004). Der Bericht stellt zwar fest, dass biometrische Erkennungssysteme ihre Eignung für Verifikationsanwendungen bei Ausweisdokumenten grundsätzlich unter Beweis gestellt haben. Er macht jedoch auch unmissverständlich klar, dass die Leistungsfähigkeit verbesserungswürdig ist und dass angesichts der enormen Komplexität der technischen, administrativen und rechtlichen Umsetzung noch keine ausreichende Wissens- und Erfahrungsbasis für die Einführung vorhanden ist.

Die aktuelle Studie BioP II des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bestätigt die Bedenken des TAB. Der Bericht (www.bsi.de/literat/studien/biop/biop_2.htm) attestiert Gesichtserkennungssystemen zwar eine einfache Bedienbarkeit, kritisiert beispielsweise jedoch die sehr hohen Anforderungen für die Aufnahme des digitalen Fotos. Zudem wird den Systemen bei hohem Sicherheitsniveau eine nicht akzeptable Rückweisungsrate bescheinigt. Besonders bedenklich stimmt die Tatsache, dass die Details zur Überwindungssi-

cherheit nicht veröffentlicht und selbst dem Bundesbeauftragten für den Datenschutz als zuständiger Datenschutzaufsichtsbehörde nicht zur Verfügung gestellt wurden.

In ihrer Entschließung vom Juni 2005 (siehe Anlage 15) kritisiert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die übereilte Einführung biometrischer Ausweisdokumente. Die Datenschutzbeauftragten fordern ein umfassendes Datenschutz- und IT-Sicherheitskonzept, in dem technische und organisatorische Maßnahmen zur Wahrung des Rechts auf informationelle Selbstbestimmung festzulegen sind. Die Konferenz fordert die objektive Bewertung biometrischer Verfahren und die Veröffentlichung der Ergebnisse entsprechender Untersuchungen und Pilotversuche.

Diese Forderungen sind auch deshalb von besonderer Dringlichkeit, weil CDU/CSU und SPD im Koalitionsvertrag angekündigt haben, biometrische Verfahren verstärkt in Pässen, Personalausweisen, Visa und Aufenthaltstiteln einsetzen zu wollen. In Deutschland soll schon im März 2007 damit begonnen werden, digitale Fingerabdrücke in die Pässe aufzunehmen. Darüber hinaus hat das Bundesinnenministerium bereits angekündigt, ab 2007 digitale Personalausweise einzuführen, die ebenfalls biometrische Merkmale enthalten werden.

29 Ich empfehle der Landesregierung, der Novellierung des Pass- und Personalausweisgesetzes im Bundesrat nur zuzustimmen, wenn gewährleistet ist, dass bei der Einführung biometrischer Ausweisdokumente

- **die biometrischen Merkmale ausschließlich von den für die Passkontrollen zuständigen Behörden für hoheitliche Zwecke genutzt werden können,**
- **die in Ausweisen gespeicherten Daten mit den biometrischen Merkmalen nicht als Referenzdaten genutzt werden, um Daten aus unterschiedlichen Systemen und Kontexten zusammenzuführen,**
- **die für die Ausstellung und das Auslesen verwendeten Geräte nach internationalen Standards von einer unabhängigen Stelle zertifiziert werden und**
- **Verfahren festgelegt werden, die einen Datenmissbrauch beim Erfassen der Referenzdaten und im weiteren Verfahren verhindern.**

3.4 Information über außerdienstliches Verhalten eines kommunalen Mitarbeiters

Ein Petent schilderte mir, dass die Polizei aufgrund eines Unfalls einen Straßenbereich in einer Innenstadt mit einem rot-weißen Trassierband abgesperrt hatte. Innerhalb des abgesperrten Bereiches befand sich das Geldinstitut, welches der Petent aufsuchen wollte. Er ignorierte die Absperrung und betrat den Gefahrenbereich. Ein Polizeibeamter forderte ihn daraufhin auf, den Bereich zu verlassen. Dieser Aufforderung kam er nicht nach; deshalb nahm der Polizeibeamte seine Personalien auf. Der Beamte und seine Vorgesetzten kannten den Betroffenen aus früherer gemeinsamer Tätigkeit und wussten, dass er jetzt in der Stadtverwaltung arbeitet. Sie informierten den öffentlichen Arbeitgeber über diesen Vorfall. Daraufhin lud die Personalabteilung den Betroffenen zu einem Personalgespräch ein. Der Petent bat mich zu prüfen, ob die Übermittlung der Daten durch die Polizei an den Arbeitgeber zulässig war.

Eine Übermittlung personenbezogener Daten darf nur erfolgen, wenn dafür eine gesetzliche Grundlage existiert oder der Betroffene eingewilligt hat. Eine Einwilligung lag offensichtlich nicht vor, so dass für die Rechtmäßigkeit der Datenübermittlung eine gesetzliche Grundlage erforderlich gewesen wäre. In bestimmten, spezialgesetzlich geregelten Fällen kann es durchaus zulässig sein, dass die Polizei oder die Staatsanwaltschaft an eine öffentliche Stelle personenbezogene Daten zu personalrechtlichen Zwecken übermittelt. So dürfen beispielsweise die Strafverfolgungsbehörden unter der Voraussetzung des § 125 c Beamtenrechtsrahmengesetz bei Strafverfahren gegen Beamte Daten an den Arbeitgeber übermitteln. Ein Strafverfahren ist hier jedoch nicht eingeleitet worden. Darüber hinaus dürfen unter besonderen Umständen personenbezogene Daten aus Bußgeldverfahren übermittelt werden (§ 49a Abs. 2 Ordnungswidrigkeitengesetz). Bei dem Verhalten des Betroffenen handelte es sich jedoch weder um eine strafbare Handlung noch um eine Ordnungswidrigkeit, so dass die Information des öffentlichen Arbeitgebers nicht durch eine Übermittlungsvorschrift gedeckt war. Sie war somit rechtswidrig. Dies habe ich der Polizei und der Stadtverwaltung mitgeteilt und empfohlen, die Mitarbeiter auf die einschlägigen Rechtsgrundlagen hinzuweisen.

Die Personalabteilung der Stadtverwaltung teilte mir mit, dass über das Gespräch mit dem Betroffenen kein Protokoll angefertigt und das Schreiben der Polizei mit der Information über den Vorfall nicht in die Personalakte aufgenommen wurde.

Dieser Sachverhalt veranlasst mich dennoch, alle personalaktenführenden Dienststellen im Land darauf hinzuweisen, dass nur Unterlagen in die Personalakte aufgenommen werden dürfen, die mit dem Dienstverhältnis in einem unmittelbaren Zusammenhang stehen (§ 100 Abs. 1 Satz 2 Landesbeamtengesetz), beziehungsweise nur die Daten verarbeitet werden, die unter anderem zur Durchführung personeller Maßnahmen erforderlich sind (§ 35 Abs. 1 Landesdatenschutzgesetz).

30 Ich empfehle der Landesregierung, gegenüber den Staatsanwaltschaften und den Polizeidienststellen klarzustellen, dass eine Übermittlung personenbezogener Daten an einen öffentlichen Arbeitgeber nur aufgrund einer normenklaren gesetzlichen Grundlage zulässig ist.

3.5 Papierloses Büro beim Verfassungsschutz

Die Verfassungsschutzbehörde unseres Landes plant, langfristig ein weitgehend papierloses Büro einzuführen, um ihre Arbeit zeitgemäßer und effektiver gestalten zu können. So ist vorgesehen, die elektronische Schriftgutverwaltung, die elektronische Vorgangsbearbeitung und die elektronische Aktenablage in einem System zu vereinen. Gescannte oder selbst am PC erstellte Dokumente sollen künftig das Bearbeitungsoriginal darstellen. Auch weiterhin sollen Nutzer nur über spezifische, für ihre Arbeit erforderliche Zugriffsmöglichkeiten verfügen. Die Führungskräfte der Behörde sollen die Möglichkeit erhalten, sich jederzeit schnell und unabhängig vom Mitarbeiter zu informieren. Das Innenministerium beteiligte mich frühzeitig unter Hinweis darauf, dieses Verfahren schrittweise auch in anderen Bereichen des Innenministeriums einführen zu wollen.

Ich habe die Verfassungsschutzbehörde darauf hingewiesen, dass eine solche Umstellung von papiergebundener auf elektronische Arbeitsweise unbedingt einer gesetzlichen Grundlage

bedarf, welche insbesondere die Wahrung der Rechte der Betroffenen sicherstellt. Das Landesverfassungsschutzgesetz Mecklenburg-Vorpommern unterscheidet zu Recht zwischen der Verarbeitung personenbezogener Daten in Akten und in Dateien und knüpft hieran unterschiedliche Rechtsfolgen. Dem Gesetzgeber war bewusst, dass eine elektronische Verarbeitung von Daten in besonderem Maße in die Persönlichkeitssphäre beziehungsweise in das Recht der Betroffenen auf informationelle Selbstbestimmung eingreift, weil es besondere Gefährdungen aufgrund der technischen Besonderheiten gibt.

31 Ich empfehle dem Landtag und der Landesregierung, für den Übergang zu einem papierlosen Büro bei der Verfassungsschutzbehörde eine gesetzliche Grundlage zu schaffen, wie das beispielsweise beim Verfassungsschutz im Land Brandenburg praktiziert wurde.

III Rechts- und Europaausschuss / Justizministerium

1 Neuregelungen zur DNA-Analyse

Im August 2005 wurde das Gesetz zur Novellierung der forensischen DNA-Analyse als Bundesgesetz verabschiedet.

Forensische DNA-Analyse bedeutet, dass die DNA-Analyse gerichtlich (als Beweismittel) verwertet wird.

Das Gesetz beinhaltet im Wesentlichen die folgenden, erweiterten Anwendungsmöglichkeiten der DNA-Analyse:

- Der Richtervorbehalt für die molekulargenetische Untersuchung von („anonymen“) Spuren wird gestrichen.
- Der Richtervorbehalt für die Entnahme und molekulargenetische Untersuchung vom Beschuldigten bleibt, aber bei Einwilligung des Beschuldigten gibt es keine gerichtliche Entscheidung, sondern nur eine Belehrung durch den Staatsanwalt oder die Polizei über den Zweck der Untersuchung. Ohne Einwilligung kann bei Gefahr im Verzug die Staatsanwaltschaft oder Polizei entscheiden.
- Die Anforderungen, die an Anlasstaten (solche Straftaten, die eine Speicherung in der DNA- Analysedatei zur Verwendung bei etwaigen künftigen Ermittlungsverfahren rechtfertigen) gestellt werden, werden gesenkt. Neu ist, dass neben Sexualstraftaten und „erheblichen“ Straftaten sonstige wiederholt begangene Straftaten, die insgesamt vom Unrechtsgehalt von erheblicher Bedeutung sind, in der DNA-Analysedatei gespeichert werden dürfen. Diese Senkung gilt auch für die Erstellung einer so genannten qualifizierten Negativprognose. Auch hier reicht es aus, wenn prognostiziert wird, dass der Beschuldigte wiederholt Straftaten von nicht erheblicher Bedeutung begeht.
- Die Reihengentests werden erstmalig auf eine gesetzliche Basis gestellt.

Im Mai 2005 hatte ich Gelegenheit, zu dem Referentenentwurf des Bundesjustizministeriums Stellung zu nehmen. Auf folgende Aspekte habe ich besonders hingewiesen:

Gegen den Wegfall des Richtervorbehalts bei „anonymen“ Spuren bestehen keine durchgreifenden datenschutzrechtlichen Bedenken.

Grundsätzliche Bedenken bestehen hingegen, wenn der Richtervorbehalt nach Einwilligung des Betroffenen in die Entnahme und Untersuchung von Körperzellen zum Zweck der Speicherung des Identifizierungsmusters in der DNA-Datei wegfällt. Das Bundesverfassungsgericht hat mehrfach betont, dass die Feststellung, Speicherung sowie die weitere Verwendung des DNA- Identifizierungsmusters in das Grundrecht des Betroffenen auf informationelle Selbstbestimmung eingreift.

Ebenso hat das Bundesverfassungsgericht festgestellt, dass eine Nivellierung von Anlasstaten gegen das Übermaßverbot verstoßen kann. Es hat klar zum Ausdruck gebracht, dass das Grundrecht auf informationelle Selbstbestimmung nur im überwiegenden Interesse der All-

gemeinheit und unter Beachtung des Verhältnismäßigkeitsgrundsatzes eingeschränkt werden darf. Ferner erscheint es kaum möglich, im Rahmen der zu treffenden Negativprognose zu unterscheiden, ob ein Betroffener künftig nur noch einmal oder wiederholt straffällig werden wird. Insofern sehe ich als Datenschutzbeauftragter die Gefahr, dass diese Prognose in Zukunft undifferenziert häufig gestellt werden wird. Eine Evaluierung ist jedoch nach meiner Kenntnis nicht vorgesehen.

Von einem Reihengentest sind überwiegend unverdächtige Personen betroffen. Deshalb hatte ich hier im Hinblick auf die aus dem Rechtsstaatsprinzip herzuleitende Unschuldsvermutung grundsätzliche Bedenken. Wenn es aber doch zu einer gesetzlichen Regelung kommt, sollte dieses Instrument nur dann angewandt werden, wenn andere Möglichkeiten zur Aufklärung der Tat nicht mehr bestehen. Außerdem sollte den Betroffenen nach einer umfassenden schriftlichen Belehrung eine ausreichende Überlegungsfrist eingeräumt werden.

Das Gesetz ist nahezu unverändert in Kraft getreten – ohne die Empfehlungen der Datenschutzbeauftragten aufzugreifen.

32 Ich empfehle der Landesregierung, bei der Überarbeitung der Richtlinie für das DNA-Verfahren der Landespolizei Mecklenburg-Vorpommern und der Richtlinie für die Staatsanwaltschaften des Landes die datenschutzrechtlichen Aspekte zu beachten, mich hieran rechtzeitig zu beteiligen und im Übrigen eine Evaluierung der Neuregelungen vorzunehmen.

2 Untersuchungshaftvollzugsgesetz überfällig

Ein Untersuchungshäftling hat bis zu seiner rechtskräftigen Verurteilung als unschuldig zu gelten. Bisher sind die Bedingungen zur Untersuchungshaft nur unzureichend in einer Generalklausel in Verbindung mit der Untersuchungshaftvollzugsordnung geregelt. Ein bereits im Frühjahr 1999 eingebrachter Gesetzentwurf der Bundesregierung zur Regelung dieser Materie, zu dem ich in meinem Vierten Tätigkeitsbericht unter 3.1.4 Stellung genommen hatte, scheiterte im Bundesrat.

Im September 2004 hat das Bundesministerium der Justiz erneut den Entwurf eines Gesetzes zur Regelung des Vollzugs der Untersuchungshaft vorgelegt. Anliegen des Entwurfes ist es einerseits, das Strafverfolgungs- und Sicherheitsinteresse des Staates im Rahmen des gesetzlichen Zwecks der Untersuchungshaft zu berücksichtigen. Andererseits sind jedoch auch das Persönlichkeitsrecht des Gefangenen sowie die Unschuldsvermutung und der Anspruch auf wirksame Verteidigung im Strafverfahren angemessen zur Geltung zu bringen.

In meiner Stellungnahme habe ich folgende Änderungen beziehungsweise Klarstellungen empfohlen:

Der Referentenentwurf geht davon aus, dass Besuche grundsätzlich überwacht werden, wobei laut Gesetzesbegründung sowohl die optische als auch die akustische Überwachung gemeint ist. Meines Erachtens ist die Art der Überwachung jedoch so entscheidend, dass hierzu eine normenklare Regelung vorzunehmen ist.

Im Entwurf ist weiterhin aufgeführt, dass von der Überwachung des Besuchs- und Schriftverkehrs dann abzusehen ist, wenn eine Gefährdung des Zwecks der Untersuchungshaft oder der Sicherheit oder Ordnung der Anstalt nicht zu befürchten ist. Die Datenschutzbeauftragten des Bundes und der Länder hatten bereits in ihrer Entschließung vom 16. August 1999 darauf hingewiesen, dass diese Maßnahme nur im Fall der Untersuchungshaft wegen Verdunkelungsgefahr unmittelbar und generell durch das Gesetz vorgeschrieben werden sollte. Bei Vorliegen anderer Haftgründe (z. B. Fluchtgefahr) sollte die Überwachung nur im Einzelfall aufgrund richterlicher Anordnung erfolgen dürfen. Der Entwurfstext trägt dem bisher nicht ausreichend Rechnung.

Über das Anhalten von Schreiben sollte in jedem Fall das Gericht entscheiden. Schließlich handelt es sich hierbei um einen schwerwiegenden Eingriff in das Postgeheimnis des Untersuchungsgefangenen, wenn er eine Briefkontrolle hinnehmen muss.

Das Recht auf ungehinderten und unüberwachten telefonischen Kontakt zwischen Verteidigung und Beschuldigtem muss auch in der Untersuchungshaft gewährleistet sein. Mit dem rechtsstaatlichen Gebot einer wirksamen Strafverteidigung wäre es nicht vereinbar, diesen Kontakt von einer besonderen Erlaubnis des Gerichts abhängig zu machen, wie der Entwurf es vorsieht.

Das Auskunfts- und Akteneinsichtsrecht wird für Untersuchungsgefangene teilweise eingeschränkt. Diese Einschränkungen sind nicht hinzunehmen, da dadurch wesentliche Datenschutzrechte in einem besonders sensiblen Bereich beschnitten würden.

33 Ich empfehle der Landesregierung, sich im Rahmen der Länderbeteiligung bei einer erneuten Bundesinitiative für eine datenschutzfreundliche Ausgestaltung der gesetzlichen Regelungen des Vollzugs der Untersuchungshaft einzusetzen, mich frühzeitig hieran zu beteiligen und im Rahmen der eigenen Zuständigkeit für eine Beachtung – auch des Rechtes auf informationelle Selbstbestimmung von Untersuchungsgefangenen – Sorge zu tragen.

3 Spezielle Forschungsklausel in der Strafprozessordnung

Mitunter bekomme ich immer noch Forschungsprojekte von Forschungsinstituten aus den Bereichen Strafsachen oder Strafvollzugsangelegenheiten vorgelegt. Bereits seit der Novellierung der Strafprozessordnung im Jahre 2000 gibt es jedoch eine spezielle Vorschrift zur Übermittlung personenbezogener Daten, welche die Einbeziehung des Landesbeauftragten für den Datenschutz nicht mehr vorsieht. Selbstverständlich bleibt es der Aufsichtsbehörde unbenommen, mich im Vorfeld mit einzubeziehen, wenn der Schutz personenbezogener Daten berührt ist.

Insofern hat sich das Verfahren für Wissenschaftler vereinfacht.

4 Auskünfte an die Presse im Rahmen strafrechtlicher Ermittlungsverfahren

Ein Bürgermeister hat sich bei mir über eine Tageszeitung beschwert, die berichtet hatte, dass die Staatsanwaltschaft die Einleitung eines strafrechtlichen Ermittlungsverfahrens gegen ihn prüfe. Im Bericht wurden die Vorwürfe detailliert dargestellt. Die Staatsanwaltschaft hatte jedoch, wie ich feststellen konnte, nur auf Anfrage und sehr zurückhaltend bestätigt, dass die Einleitung eines Verfahrens geprüft werde. Woher die Zeitung die genauen Informationen hatte, blieb letztendlich ungeklärt. Der Betroffene erfuhr hiervon erst durch die Presse, die ihn um eine Stellungnahme zu den Vorwürfen bat. Ich habe gegenüber dem Generalstaatsanwalt unseres Landes eine fehlende Vorabinformation des Betroffenen kritisiert und meine datenschutzrechtlichen Bedenken deutlich gemacht.

Die Presse hat gegenüber Behörden grundsätzlich ein Auskunftsrecht. Von der Verpflichtung, der Presse die gewünschten Auskünfte zu erteilen, kann nach § 4 Abs. 3 Landespressegesetz unter anderem abgesehen werden, wenn hierdurch ein schutzwürdiges privates Interesse verletzt würde. Auch wenn auf Anfragen der Presse hin die Staatsanwaltschaften zu Einzelfällen nur allgemeine Auskünfte erteilen, so ist damit zwangsläufig – zumindest teilweise – eine Bestätigung der bereits bekannten Sachverhalte verbunden, so in diesem Fall. Insofern erhalten die Informationen dadurch eine neue Qualität.

Aufgrund der Stellung des Petenten in der Öffentlichkeit und der engen Verknüpfung des Tatvorwurfs mit seiner öffentlichen Tätigkeit war eine Auskunft gegenüber der Presse grundsätzlich zulässig. Es war in diesem Fall jedoch zu berücksichtigen, dass der Petent von der Prüfung noch keine Kenntnis hatte und für den Staatsanwalt aufgrund der Anfrage offensichtlich war, dass dieser mit hoher Wahrscheinlichkeit durch die Presse erstmalig hiervon erfahren würde.

Im Hinblick auf ein faires Verfahren und den Schutz des allgemeinen Persönlichkeitsrechts erachte ich es in derartigen Fällen deshalb für notwendig, die Betroffenen zuvor oder zumindest parallel über die Auskünfte an die Presse zu unterrichten.

Die Staatsanwaltschaften sind gehalten, bei Auskunftsersuchen der Presse die schutzwürdigen Interessen der Betroffenen hinreichend zu berücksichtigen. Der Generalstaatsanwalt hat mir mitgeteilt, dass er meiner Rechtsauffassung grundsätzlich beipflichtet und die Problematik auf der nächsten Dienstbesprechung mit den Leitenden Oberstaatsanwälten erörtern wird.

34 Ich empfehle der Landesregierung, gegenüber den Staatsanwaltschaften und den Polizeidienststellen in geeigneter Weise klarzustellen, dass bei Presseanfragen zu laufenden Verfahren die Betroffenen, die hiervon noch keine Kenntnis haben, generell vorab zu unterrichten sind. Ferner rege ich an, diesen Sachverhalt auch ausdrücklich in der Allgemeinen Verwaltungsvorschrift des Landes Mecklenburg-Vorpommern für die Zusammenarbeit der Justizbehörden mit den Medien zu regeln.

5 Internet und Online-Banking bei Gerichtsvollziehern

Gerichtsvollzieher möchten vermehrt das Internet und moderne Kommunikationsdienste nutzen. Dabei haben sie jedoch zu berücksichtigen, dass sie auf ihren IT-Systemen besonders

sensible personenbezogene Daten verarbeiten. Durch einen Internetanschluss ohne wirksame Schutzvorkehrungen werden diese Daten leicht angreifbar. Gerichtsvollzieher sind daher im Besonderen verpflichtet, geeignete Vorkehrungen zum Schutz ihrer IT-Systeme zu treffen.

Das Justizministerium hat bereits im Juli 2003 eine Verwaltungsvorschrift erlassen, die den Einsatz von EDV-Technik im Gerichtsvollzieherbüro regelt. Die Details der Vorschrift sind seinerzeit mit mir abgestimmt worden und entsprechen den datenschutzrechtlichen Anforderungen bereits sehr weitgehend.

In der Regel verfügen die Gerichtsvollzieher jedoch nicht über Personal mit Kenntnissen im Bereich der IT-Sicherheit, so dass sie zur Umsetzung der oben genannten Vorschrift auf die Hilfe von Dienstleistern angewiesen sind. Ein Mindestmaß an Grundkenntnissen und Sensibilität hinsichtlich datenschutztechnischer Fragen ist jedoch erforderlich, um externe Fachleute beauftragen und kontrollieren zu können.

Vor diesem Hintergrund hat der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ (siehe Punkt A.0.) die „Orientierungshilfe zum datenschutzgerechten Anschluss an Internet und Online-Banking bei Gerichtsvollziehern“ erarbeitet (abrufbar unter www.datenschutz-mv.de). Hier wird kurz und anschaulich beschrieben, was bei einem Internetanschluss zu beachten ist und warum auf eine Firewall nicht verzichtet werden darf. Weiterhin sind die wesentlichen Grundregeln zur datenschutzgerechten Nutzung des E-Mail-Dienstes dargestellt und Maßnahmen erläutert, mit denen Personalcomputer vor Viren geschützt werden können. Die Orientierungshilfe präzisiert und ergänzt somit die Verwaltungsvorschrift des Justizministeriums.

Mit Blick auf das zunehmende Interesse der Gerichtsvollzieher, ihren dienstlichen Zahlungsverkehr bargeldlos mit Online-Banking-Verfahren abzuwickeln, werden darüber hinaus Vorschläge für eine geeignete technische Infrastruktur unterbreitet und Empfehlungen für die erforderlichen Sicherheitsvorkehrungen gegeben. Die Forderungen der Verwaltungsvorschrift folgen den Empfehlungen der Orientierungshilfe in vollem Umfang.

35 Ich empfehle der Landesregierung, die Gerichtsvollzieher bei der Umsetzung der Verwaltungsvorschrift zum Einsatz von EDV-Technik im Gerichtsvollzieherbüro zu unterstützen. Gerichtsvollzieher, die moderne Informations- und Kommunikationstechnik im dienstlichen Umfeld nutzen möchten, sollten auch die ergänzenden Hinweise der „Orientierungshilfe zum datenschutzgerechten Anschluss an Internet und Online-Banking bei Gerichtsvollziehern“ beachten, um ein Mindestmaß an Sicherheit für die auf ihren IT-Systemen gespeicherten Daten zu gewährleisten.

6 Rahmenbeschluss zur Vorratsdatenspeicherung in der Telekommunikation

Die Europäische Kommission hat den Entwurf einer Richtlinie über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, veröffentlicht. Danach sollen alle Telekommunikations- und Internet-Anbieter verpflichtet werden, eine Vielzahl von Daten über jeden einzelnen Kommunikationsvorgang über einen längeren Zeitraum zu speichern, ohne dass diese Daten für betriebliche Zwecke, zum Beispiel für die Abrechnung, erforderlich sind. Telefondaten sollen ein Jahr,

Internetdaten sechs Monate gespeichert werden. Hierbei geht es um die Speicherung von Verbindungs- und Standortdaten, die bei der Abwicklung von Diensten wie Telefonieren, SMS, E-Mailen, Surfen oder File Sharing**.**

> Als **File Sharing** bezeichnet man die gemeinsame Nutzung bzw. den Austausch von Dateien über ein Computernetzwerk, zum Beispiel das Internet. Über Systeme zum File Sharing kann man Dateien beliebiger Art zum Kopieren anbieten und herunterladen.

anfallen. Zu diesen Daten gehören zum Beispiel Informationen über Ort, Zeitpunkt, Dauer und Gesprächspartner von Telefongesprächen, Fax, E-Mail, SMS sowie anderen über das Internetprotokoll abgewickelten Diensten.

Die Kommission will mit dieser Datenspeicherung erreichen, dass gegen schwere Straftaten wie Terrorakte oder kriminelle Handlungen im Rahmen des organisierten Verbrechens besser vorgegangen werden kann.

In einer Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. Oktober 2005 (siehe Anlage 21) haben die Datenschutzbeauftragten an die Bundesregierung, den Bundestag und das Europäische Parlament appelliert, einer Verpflichtung zur systematischen und anlasslosen Vorratsdatenspeicherung auf europäischer Ebene nicht zuzustimmen, da eine solche Vorratsdatenspeicherung auf der Grundlage des Grundgesetzes verfassungswidrig wäre.

Das Bundesverfassungsgericht hat im Volkszählungsurteil eine Speicherung von Daten zu noch unbestimmten Zwecken generell für verfassungswidrig erklärt (BVerfGE 65, 46). Insbesondere ist die Verpflichtung zur Vorratsdatenspeicherung sämtlicher Verkehrsdaten mit Artikel 10 Grundgesetz (Fernmeldegeheimnis) unvereinbar, weil sie alle Teilnehmer der elektronischen Kommunikation in Anspruch nimmt und damit unter Generalverdacht stellt. Zwar dürfen für die Speicherung und Verwendung von Verbindungsdaten für die Bekämpfung schwerer Straftaten Auskünfte nach §§ 100 a und 100 b Strafprozessordnung eingeholt werden. Das Strafverfolgungsinteresse unter Berücksichtigung der Schwere und Bedeutung der aufzuklärenden Straftat muss jedoch überwiegen, das heißt, es muss ein konkreter Tatverdacht für eine Straftat mit erheblicher Bedeutung vorliegen. Eine Datenspeicherung auf Vorrat, wie sie im Entwurf der Richtlinie vorgesehen ist, würde diesen verfassungsrechtlichen Anforderungen nicht standhalten.

Weiterhin wird durch eine solche Vorratsdatenspeicherung in das informationelle Selbstbestimmungsrecht des Bürgers und in das durch Artikel 8 der Europäischen Menschenrechtskonvention garantierte Recht auf Achtung des Privat- und Familienlebens, der Wohnung und der Korrespondenz unverhältnismäßig eingegriffen. Eingriffe in die Ausübung dieser Rechte sind nur zugelassen, soweit sie gesetzlich vorgesehen und in einer demokratischen Gesellschaft zwingend notwendig sind.

Eine über Zwecke des Betriebes hinausgehende Speicherung von Verkehrsdaten ist unverhältnismäßig, weil sie insbesondere auch gegen den Grundsatz der Erforderlichkeit verstößt. Es gibt Methoden, die weniger stark in die Privatsphäre des Bürgers eingreifen. Gemeinsam mit den Datenschutzbeauftragten von Bund und Ländern habe ich daher in der Entschließung der Konferenz (siehe Anlage 21) darauf verwiesen, dass man mit dem US-amerikanischen

Quick-Freeze-Verfahren dem Interesse einer effektiven Strafverfolgung wirksam und zielgerichtet nachkommen kann.

Bei dem in den USA praktizierten **Quick-Frezze-Verfahren** wenden sich die US-Ermittlungsbehörden in begründeten Verdachtsfällen an die Internet-Provider mit der Bitte, die Kommunikationsdaten einzelner verdächtiger Kunden „einzufrieren“, also zu speichern. Anschließend haben die Behörden neunzig Tage Zeit, um Beweise zu sammeln und damit die Herausgabe der gespeicherten Daten per Gerichtsbeschluss zu erwirken.

36 Ich empfehle der Landesregierung, die verfassungs- und datenschutzrechtlichen Aspekte bei der Vorratsdatenspeicherung in der Telekommunikation zu berücksichtigen und sich im Bundesrat gegen eine Speicherung von Daten, wie sie im Entwurf der Richtlinie der Europäischen Kommission vorgesehen ist, auszusprechen.

IV Finanzausschuss / Finanzministerium

1 Data Center Steuern

Das Finanzministerium beabsichtigt, das Rechenzentrum für die Steuerverwaltung neu zu organisieren, um Kosten zu sparen. Unter anderem wurde nach Wegen gesucht, mit anderen Dienstleistern zusammenzuarbeiten oder zu fusionieren. Bereits 1999, als das Rechenzentrum noch ein Referat der inzwischen aufgelösten Oberfinanzdirektion Rostock war, wurden mir dazu erste Konzepte vorgelegt.

Zum 1. Januar 2006 soll nun das Rechenzentrum für die Steuerverwaltung, welches jetzt Data Center Steuern heißt, dem bisherigen zentralen IT-Dienstleister der Verwaltungen Hamburgs und Schleswig-Holsteins „Dataport“ angegliedert werden. Während Dataport als Anstalt öffentlichen Rechts künftig auch für Bremen arbeiten wird, behält Mecklenburg-Vorpommern die DVZ M-V GmbH als zentralen Dienstleister. Das Data Center Steuern mit Standorten in Rostock und Schwerin wird aber die Steuerverwaltung aller vier Bundesländer mit Rechenzentrumsleistungen versorgen. Lediglich der zentrale Druck von Steuerbescheiden und anderen Unterlagen wird künftig in Kiel-Altenholz stattfinden.

Aus Sicht des Datenschutzes ist dabei zu beachten, dass das Steuergeheimnis nach § 30 Abgabenordnung (AO) gewahrt bleiben muss. Die Datenschutzbeauftragten aller beteiligten Länder haben deshalb den Entwurf des Staatsvertrages für den Beitritt Bremens und Mecklenburg-Vorpommerns zu Dataport geprüft. Meine Kollegen und ich waren mit dem Entwurf im Wesentlichen einverstanden. Der Finanzausschuss unseres Landtages hat dem Gesetzentwurf zum Staatsvertrag bereits zugestimmt.

Der Entwurf enthält unter anderem folgende Grundsätze:

Für Dataport gilt schleswig-holsteinisches Datenschutzrecht, für die Auftragsdatenverarbeitung das Recht des Auftraggebers und für die Verarbeitung personenbezogener Daten von Bediensteten oder Bewerbern das Recht der jeweiligen Niederlassung. Für Sicherheitsüberprüfungen ist hamburgisches Recht anzuwenden.

Die Datenschutzkontrolle obliegt dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein und bei Auftragsdatenverarbeitung dem für den Auftraggeber zuständigen Datenschutzbeauftragten. Die Datenschutzbeauftragten können sich jedoch gegenseitig mit Kontrollen beauftragen.

37 Ich empfehle der Landesregierung, mich auch weiterhin frühzeitig bei der Gestaltung der länderübergreifenden Steuerdatenverarbeitung zu beteiligen. Wenn der Staatsvertrag wie vorgesehen verabschiedet wird, verbleibt für Dataport und die Steuerverwaltungen die Aufgabe, die Vorschriften zum Steuergeheimnis technisch und organisatorisch umzusetzen. So muss das Data Center Steuern von den anderen Teilen von Dataport abgeschottet werden, und die Steuerverwaltungen der beteiligten Länder dürfen nicht auf Daten eines anderen Bundeslandes zugreifen können.

2 Bargeldlose Zahlverfahren

Bürger, Behörden und Unternehmen sollen künftig die Möglichkeit erhalten, kostenpflichtige Leistungen der Verwaltung bargeldlos zu bezahlen. Hierfür geeignete Waren sollen in so genannten E-Shops angeboten werden. Das Landesvermessungsamt könnte beispielsweise elektronisches Kartenmaterial zum Kauf anbieten. Auch die Entgelte für eine elektronische Melderegisterauskunft (siehe Punkt A.1.II.2.13) könnten auf elektronischem Weg entrichtet werden.

Der E-Government-Masterplan der Landesregierung sieht mit der so genannten Zahlungsverkehrsplattform (ZVP) eine Basiskomponente vor, die vom IT-Landesdienstleister DVZ M-V GmbH betrieben wird und den bargeldlosen Zahlungsverkehr in der Landesverwaltung unterstützen soll. Die ZVP ist Kopfstelle zur Integration der E-Shops an die von einem weiteren Dienstleister (Provider) betriebene E-Payment-Komponente. Der Provider führt das Clearing der Zahlungen durch, initiiert die Zahlungsströme und stellt dem Haushalts-Kassen-Rechnungs-Verfahren ProFiskal Buchungsdaten auf elektronischem Weg zur Verfügung. So wird sichergestellt, dass Einnahmen für das Land einfach und schnell realisiert werden können (zu ProFiskal siehe Fünfter Tätigkeitsbericht, Punkt 3.10.4 und Sechster Tätigkeitsbericht, Punkt 2.10.4).

Die Software für die Basiskomponente ZVP entwickelt das Finanzministerium gemeinsam mit dem Innenministerium und der DVZ M-V GmbH. Auf meine Anfrage erhielt ich vom Finanzministerium einige Planungsunterlagen zur Zahlungsverkehrsplattform. Auf die folgenden datenschutzrechtlichen Aspekte habe ich in meiner Stellungnahme hingewiesen:

Auch ein elektronisches, bargeldloses Zahlverfahren muss sich an den im Datenschutzgesetz des Landes normierten Grundsätzen der Datenvermeidung orientieren (§ 5 Abs. 1 DSG M-V). Für die datenschutzgerechte Ausgestaltung der ZVP bedeutet dies unter anderem, dass jede an einem Kaufvorgang beteiligte Stelle (Verkäufer, Provider, Landeszentralkasse, DVZ M-V GmbH) nur die personenbezogenen Daten des Kunden erheben und nutzen darf, die für den jeweiligen Teil des Kaufvorgangs erforderlich sind. Beispielsweise benötigt der Verkäufer nicht die Bankverbindung des Kunden. Der Provider braucht die Kontodaten des Kunden nur für den Fall des Lastschriftverfahrens und muss für die Abwicklung des Zahlvorganges im Übrigen auch nicht wissen, welche Ware der Kunde erworben hat. Schließlich muss die Landeszentralkasse erst nach Lieferung der Ware und nach Abschluss des Zahlvorganges zwischen Kunde und Provider vom Kauf erfahren.

Nach den Planungen des Finanzministeriums soll der Provider ein Scoring als Risikoprävention bei der Bezahlart „Überweisung nach Lieferung“ durchführen.

> **Scoring** bedeutet zunächst lediglich das Zählen von Punkten. Im hier verwendeten Zusammenhang beschreibt Scoring ein analytisch statistisches Verfahren, mit dem aus erhobenen Daten anhand von Erfahrungswerten eine Risikoabschätzung zur Bonität eines Kunden abgegeben werden kann. Diese Verfahren stehen insbesondere angesichts der mangelnden Transparenz regelmäßig in der Kritik der Datenschützer (siehe dazu auch Punkt B.11).

Im Ergebnis soll der Provider so genannte „Blacklists“ mit Daten der „auffällig gewordenen Zahlungspflichtigen“ führen. Welche Kriterien zu einer solchen Bewertung führen, ist jedoch

völlig intransparent. Da somit nicht nachvollziehbar ist, auf welche Weise die für die Bonitätseinschätzung des Kunden erforderlichen Daten gewonnen werden, und darüber hinaus den Betroffenen in der Regel keine Auskunft zum Verfahren gegeben wird, habe ich erhebliche Bedenken gegen diese Pläne geäußert.

38 Ich empfehle der Landesregierung, beim bargeldlosen Zahlungsverkehr in der Landesverwaltung auf Scoring-Verfahren beim Betrieb der Zahlungsverkehrsplattform generell zu verzichten. Darüber hinaus ist bei der weiteren Entwicklung des Verfahrens der Grundsatz der Datenvermeidung zu berücksichtigen.

3 Personalkonzepte

Die Verwaltung des Landes Mecklenburg-Vorpommern steht vor tiefgreifenden Strukturreformen, die mit einem erheblichen Stellenabbau verbunden sein werden. So soll allein die Landesverwaltung bis Ende 2007 ca. 5.100 Stellen sozialverträglich, also möglichst ohne Kündigungen, abbauen. Außerdem sollen künftig im Zuge der Kreisgebietsreform Aufgaben des Landes auf die Kommunen verlagert werden, was mit Personalumsetzungen vom Land zu den Kommunen sowie innerhalb der Kommunen verbunden ist.

In der Landesverwaltung ist ein Personalmanagement (PeM) eingerichtet worden. Im Rahmen eines Kontroll- und Informationsbesuches habe ich mich über den geplanten Umgang mit den dazu erforderlichen Mitarbeiterdaten informiert. Das PeM soll die Koordinierungsaufgaben zwischen den durch Umstrukturierung entstehenden neuen Stellen und den dadurch frei werdenden Mitarbeitern wahrnehmen. Nach dem Personalkonzept werden diese Mitarbeiter einem so genannten Personalüberhang zugeordnet. Dabei werden soziale Belange berücksichtigt. Das gesamte Verfahren ist von datenschutzrechtlicher Relevanz, weil für die Koordinierungsaufgaben Personaldaten der Mitarbeiter erforderlich sind. Dabei wird stufenweise vorgegangen: Die Mitarbeiter sollen auf freiwilliger Basis einen Bewerberbogen beim Personalmanagement einreichen. Die auf diesem Bogen erfassten Daten bilden die Grundlage, um den Betroffenen eine geeignete Stelle anbieten zu können. Die Mitarbeiter entscheiden dann selbst, ob sie sich für die Stelle bewerben oder nicht. In Abhängigkeit vom Fortschritt der Umstrukturierung übermitteln die Personalstellen zu einem späteren Zeitpunkt an das Personalmanagement Daten von Mitarbeitern, die keinen Bewerberbogen ausgefüllt haben, um auch diesen geeignete Stellen anbieten zu können. Lehnt jemand zu diesem Zeitpunkt mehrere Angebote ab, soll wegen fehlender Mitwirkung eine verhaltensbedingte Kündigung ausgesprochen oder eine Versetzung angeordnet werden können.

Gegen das vorgestellte Personalkonzept hatte ich keine grundsätzlichen datenschutzrechtlichen Bedenken, habe jedoch Verbesserungen empfohlen. Die weitere Umsetzung der Umstrukturierungsprozesse werde ich begleiten.

39 Ich empfehle der Landesregierung, die Daten der Mitarbeiterinnen und Mitarbeiter, die im Zuge der Strukturreform der Landesverwaltung dem Personalüberhang zugeordnet werden, nur in dem Rahmen zu nutzen, wie es für die Personalverwaltung notwendig ist. Ein unbeschränkter Zugriff auf diese Daten durch Personalstellen aller Ressorts wäre mit den datenschutzrechtlichen Bestimmungen nicht vereinbar.

4 Einsichtnahme des Finanzamtes in betriebliche Unterlagen des Notars

Auf Bitten des Justizministeriums hatte ich zu einem Fall Stellung genommen, in dem ein Finanzamt von einem Notar im Rahmen einer laufenden Betriebsprüfung Unterlagen anforderte, in denen sich personenbezogene Daten seiner Mandanten befanden. Ich hatte dem Justizministerium meine Auffassung mitgeteilt, dass die notarielle Verschwiegenheitspflicht auch in Steuerverfahren gilt (siehe Sechster Tätigkeitsbericht, Punkt 2.10.5).

Mittlerweile hat auch das Finanzministerium gegenüber dem Justizministerium Stellung genommen. Das Finanzministerium führt aus, dass dem Notar Möglichkeiten einzuräumen sind, seine Besteuerungsgrundlagen auch ohne Gefahr des Verstoßes gegen seine Verschwiegenheitspflicht nachweisen zu können (z. B. automatische Trennung personenbezogener Mandantendaten von den steuerlich relevanten Daten bei elektronischer Buchführung, Abdecken der auf den Belegen befindlichen Mandantennamen, Fotokopien mit entsprechenden Schwärzungen). Nur wenn tatsächliche Anhaltspunkte vorlägen, die Zweifel an der Vollständigkeit und/oder Richtigkeit derartig aufbereiteter Unterlagen begründeten, und die Zweifel auch nicht auf andere Weise ausgeräumt werden könnten, führe eine Verweigerung unter Berufung auf das Notargeheimnis dazu, dass gegebenenfalls der Betriebsausgabenabzug verweigert würde beziehungsweise Betriebseinnahmen durch die Finanzverwaltung im Schätzungswege ermittelt würden.

Diesen ersten Schritt zur Berücksichtigung der notariellen Verschwiegenheitspflicht im Steuerverfahren habe ich – wie auch die Datenschutzbeauftragten des Bundes und der Länder – begrüßt. Nach Auskunft des Finanzministeriums wurde sie allen Finanzämtern des Landes zur Kenntnis gegeben und fand auch in der Runde der für Abgabenrecht zuständigen Referatsleiter der obersten Finanzbehörden des Bundes und der Länder allgemeine Zustimmung.

Auf Nachfrage teilte mir das Finanzministerium mit, dass die oben dargestellten Ausführungen nicht nur für Notare, sondern für sämtliche Berufe gelten, denen § 102 der Abgabenordnung (AO) ein Auskunftsverweigerungsrecht einräumt. Dies sind unter anderem Geistliche, Rechtsanwälte, Steuerberater, Ärzte, Zahnärzte, Psychotherapeuten, Apotheker, Hebammen und deren Hilfspersonal.

Somit steht für die in § 102 AO genannten Träger eines Berufs- oder besonderen Amtsgeheimnisses fest, dass sie ihre Verschwiegenheitspflicht gegenüber der Finanzverwaltung wahren können, ohne steuerliche Nachteile befürchten zu müssen.

Unbefriedigend bleibt die Situation im Streitfalle. Hier dürften die Auskunftsverweigerungspflichtigen gezwungen sein, steuerliche Nachteile in Kauf zu nehmen, um nicht gegen ihre Verschwiegenheitspflichten zu verstoßen oder in ein gerichtliches Verfahren gezwungen werden. Zur Vermeidung dieser Situation könnte sich die Einbeziehung des Landesbeauftragten für den Datenschutz aufgrund seiner Kompetenzen gemäß § 31 Abs. 1 Landesdatenschutzgesetz (DSG M-V) als hilfreich erweisen, wenn dies von beiden Seiten akzeptiert werden würde.

40 Ich empfehle der Landesregierung anzuordnen, dass die Finanzämter betroffene Geheimnisträger auf die Möglichkeit hinweisen, sich an den Landesbeauftragten für den Datenschutz zu wenden, wenn ihnen nachteilige steuerliche Entscheidun-

gen drohen, sofern sie die Bekanntgabe personenbezogener Daten ihrer Mandanten verweigern.

5 Kontoabrufverfahren

Durch Artikel 2 des Gesetzes zur Förderung der Steuerehrlichkeit vom 23. Dezember 2003 ist § 93 Abgabenordnung (AO) um die Absätze 7 und 8 erweitert worden. Diese Regelungen sind am 1. April 2005 in Kraft getreten und lauten wie folgt:

(7) Die Finanzbehörde kann bei den Kreditinstituten über das Bundesamt für Finanzen einzelne Daten aus den nach § 93 b Abs. 1 zu führenden Dateien abrufen, wenn dies zur Festsetzung oder Erhebung von Steuern erforderlich ist und ein Auskunftsersuchen an den Steuerpflichtigen nicht zum Ziele geführt hat oder keinen Erfolg verspricht.

(8) Knüpft ein anderes Gesetz an Begriffe des Einkommenssteuergesetzes an, soll die Finanzbehörde auf Ersuchen der für die Anwendung des anderen Gesetzes zuständigen Behörde oder eines Gerichtes über das Bundesamt für Finanzen bei den Kreditinstituten einzelne Daten aus den nach § 93 Abs. 1 zu führenden Dateien abrufen und der ersuchenden Behörde oder dem ersuchenden Gericht mitteilen, wenn in dem Ersuchen versichert wurde, dass eigene Ermittlungen nicht zum Ziele geführt haben oder keinen Erfolg versprechen.

Zusätzlich ist durch § 93 b AO geregelt worden, dass die nach § 24 c Kreditwesengesetz (KWG) zu führende Kontendatei auch für Abrufe nach § 93 Abs. 7 und 8 AO zu führen ist.

Neben den bereits nach § 24 c KWG hauptsächlich für bankaufsichtsrechtliche und strafrechtliche Zwecke möglichen Kontenabfragen können aufgrund der neuen Regelungen auch über das Bundesamt für Finanzen Kontenabfragen durch Finanzbehörden für steuerliche Zwecke und Kontenabfragen durch Finanzbehörden für andere Behörden und Gerichte für bestimmte außersteuerliche Zecke durchgeführt werden.

Das Bundesministerium für Finanzen hat mit Erlass vom 10. März 2005 seinen Anwendungserlass zur Abgabenordnung (AEAO) vom 15. Juli 1998 zu §§ 92 und 93, zuletzt geändert am 3. Januar 2005, um Regelungen zu § 92 und § 93 AO ergänzt, in denen es die Kontenabrufverfahren nach §§ 93 Abs. 7 und 8 erläutert. Es wird klargestellt, dass ein Kontenabruf kein Verwaltungsakt ist, sondern einer elektronischen Einnahme des Augenscheins entspricht und somit einen Realakt darstellt.

Mit Beschluss vom 23. März 2005 hat das Bundesverfassungsgericht die Anträge auf Erlass einer einstweiligen Anordnung gegen Regelungen zum automatisierten Abruf von Kontostammdaten für Zwecke der Erhebung von Steuern und Sozialversicherungsbeiträgen sowie der Überprüfung der Berechtigung für Sozialleistungen unter Berücksichtigung des o. g. Anwendungserlasses abgelehnt. Das Hauptsacheverfahren läuft noch.

Den Finanzämtern in Mecklenburg-Vorpommern liegt ein Erlass des Finanzministeriums Mecklenburg-Vorpommern vom 23. März 2005 vor, mit welchem Hinweise zur Verbesserung der Ermittlungstätigkeiten für Finanzbehörden und andere Behörden und Gerichte ab dem 1. April 2005 gegeben werden. Diese betreffen neben Hinweisen zur technischen Umsetzung des Verfahrens und zu den Vordrucken vor allem Hinweise zu den Verfahrensregelungen konkret in Mecklenburg-Vorpommern. Das Finanzministerium Mecklenburg-Vorpommern

hat in einem weiteren Erlass vom 31. März 2005 an die Finanzämter in Mecklenburg-Vorpommern weitere Hinweise für die Durchführung der Kontenabrufe, vor allem im Hinblick auf den jeweiligen Vordruck zum Kontenabrufverfahren und bzgl. der Aufbewahrungsfristen, gegeben.

Aus einem Schreiben des Finanzministeriums Mecklenburg-Vorpommern an das Bundesministerium für Finanzen, in dem über die Anzahl der jeweiligen Kontenabrufe in Mecklenburg-Vorpommern berichtet wird, geht hervor, dass die Finanzämter zwischenzeitlich angehalten worden sind, vom Kontenabrufverfahren stärker Gebrauch zu machen, da das Abrufvolumen beim BfF noch nicht ausgeschöpft sei.

Ich habe einen Kontroll- und Informationsbesuch beim Finanzamt Wismar durchgeführt, da dort die meisten Kontenabrufersuchen im Land Mecklenburg-Vorpommern gestellt worden sind.

Im 2. Quartal 2005 sind in Mecklenburg-Vorpommern insgesamt 15 Kontenabrufe durchgeführt worden. Durch das Finanzamt Wismar sind 5 Kontenabrufe nach § 93 Abs. 7 AO und ein Kontenabruf nach § 93 Abs. 8 AO erfolgt (hierzu unter A.1.II.2.6). Im 3. Quartal 2005 hat das Finanzamt Wismar 7 Anfragen nach § 93 Abs. 7 AO durchgeführt.

Das Kontenabrufverfahren nach § 93 Abs. 7 AO ist im gesamten Besteuerungsverfahren nach der AO, also auch im Haftungsverfahren, Erhebungsverfahren, Rechtsbehelfsverfahren oder im Vollstreckungsverfahren möglich. Im Finanzamt Wismar hat bisher lediglich die Vollstreckungsstelle vom Kontenabruf Gebrauch gemacht. Der Kontenabruf diente somit der Ermittlung bisher unbekannter Konten, um in diese Vollstrecken zu können.

Das Bundesamt für Finanzen hat dem Finanzamt aufgrund der Kontenabrufersuchen folgende Daten übermittelt:

- die Nummer der Konten oder Depots,
- den Tag der Einrichtung und den Tag der Auflösung der Konten oder Depots,
- den Namen des Kontoinhabers,
- die Namen sämtlicher Verfügungsberechtigter in der Historie,
- die gelöschten Konten innerhalb des letzten halben Jahres und ebenfalls
- die Namen von finanzierenden Banken.

Der Umfang dieser Daten entspricht nicht den datenschutzrechtlichen Anforderungen, insbesondere nicht den Grundsätzen der Erforderlichkeit und Datensparsamkeit. Das Finanzamt erhielt wesentlich mehr Daten, als zur Aufgabenerfüllung erforderlich war. Zugleich wurde, entgegen dem Anwendungserlass, der Betroffene in der Regel nicht vorab informiert, um den Erfolg der Maßnahme nicht zu gefährden. Die Tatsache, dass bei einem Kontenabruf grundsätzlich sämtliche Verfügungsberechtigte in der Historie mit Namen und Anschrift und außerdem die gelöschten Konten des letzten halben Jahres übermittelt werden, ist jedoch dem Finanzamt Wismar nicht vorzuhalten. Diese Problematik habe ich an den Bundesbeauftragten für den Datenschutz herangetragen, um eine Überarbeitung der bundesgesetzlichen Regelungen anzumahnen.

6 Telefonische Befragungen von Sparkassenkunden

Ein Bürger machte mich auf die Homepage seiner Sparkasse aufmerksam, auf der mitgeteilt wird, dass ein Meinungsforschungsinstitut mit einer telefonischen Kundenbefragung beauftragt wurde. Er hat mich gebeten, den Sachverhalt zu prüfen.

Die Sparkasse hatte dem Meinungsforschungsinstitut die Anschriften und die Telefonnummern ihrer Kunden übermittelt. Das Institut sollte die Kunden anrufen und fragen, ob sie mit den Leistungen zufrieden sind und welche Wünsche sie haben. Die Ergebnisse sollten dann in grafischer und tabellarischer Form der Sparkasse zur Verfügung gestellt werden. Somit handelte es sich um eine Datenverarbeitung im Auftrag.

Die Sparkasse ist ein öffentlich-rechtliches Unternehmen, das am Wettbewerb teilnimmt (§ 2 Abs. 5 Landesdatenschutzgesetz – DSG M-V). Deshalb hat sie hinsichtlich der Datenverarbeitung im Auftrag die Bestimmungen des Bundesdatenschutzgesetzes anzuwenden (§ 11 BDSG). Diese Bestimmungen waren in der mir übersandten Vereinbarung zur Kundenbefragung nicht vollständig umgesetzt. Der Auftragnehmer wurde hier lediglich verpflichtet, mit den übermittelten Daten vertraulich umzugehen und sie nur zu dem vom Auftraggeber bestimmten Zweck zu verarbeiten. Insbesondere fehlte ein schriftlicher Auftrag zur Datenverarbeitung und -nutzung und zu den dabei vom Auftragnehmer zu treffenden technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes. Außerdem hätte die Sparkasse konkret vorgeben müssen, wie die Befragung durchzuführen ist. Kundenbefragungen sind nur auf freiwilliger Basis zulässig. Die Sparkasse hätte daher festlegen müssen, dass die Kunden zu Beginn des Gespräches darüber aufgeklärt werden. Der Sparkasse habe ich empfohlen, die datenschutzrechtlichen Vorgaben umzusetzen.

41 Ich empfehle der Landesregierung, gegenüber den Sparkassen und anderen öffentlichen Einrichtungen bei Kundenbefragungen auf die Einhaltung datenschutzrechtlicher Bestimmungen hinzuweisen und deren Einhaltung zu prüfen.

V Wirtschaftsausschuss und Tourismusausschuss / Wirtschaftsministerium

1 Terrorbekämpfung im Bereich der Häfen und der internationalen Schifffahrt

Ein Mitarbeiter einer Seehafen-Umschlagsgesellschaft machte mich darauf aufmerksam, dass von allen Mitarbeitern der im Hafen ansässigen Firmen Daten wie Name, Vorname, Geburtsdatum, Personalausweisnummer, Lichtbild und Arbeitgeber erhoben würden. Diese Daten würden zur Erstellung eines Betriebsausweises benötigt. Man habe sich auf sein Nachfragen hin dabei allgemein auf Maßnahmen zur Umsetzung des ISPS (International Ship Port Security)-Codes bezogen.

Ich habe daraufhin den Wirtschaftsminister unseres Landes nach der konkreten Rechtsgrundlage für die Datenerhebung und deren weiteren Verwendung befragt. Er hat mir mitgeteilt, dass diese Maßnahmen in Ausübung des Hausrechts auf der EU-Verordnung 725/2004 (Vertragsgesetz vom 22.12.2003) in Verbindung mit dem ISPS-Code, der einen Plan zur Gefahrenabwehr in der Hafenanlage vorsieht, in Verbindung mit § 28 Bundesdatenschutzgesetz (BDSG) beruhen. Dies sei im Zuge der Terrorbekämpfung für die Hafensicherheit auch erforderlich. Auf dieser Grundlage werde für die im Seehafen ansässigen Hafenanlagenbetreiber ein einheitliches Zugangskontrollsystem betrieben. Die angeforderten Daten seien zur Erstellung eines einheitlichen Betriebsausweises notwendig gewesen.

Auch aus datenschutzrechtlicher Sicht ist verständlich, dass für den Hafen ein einheitliches Zugangskontrollsystem installiert wird, um zu verhindern, dass unberechtigte Personen Zugang zum Hafengelände erhalten. Dennoch sind die schutzwürdigen Belange der betroffenen Mitarbeiter zu berücksichtigen. Das bedeutet, dass sie zumindest aufgeklärt werden müssen, zu welchem Zweck ihre Daten weitergeleitet werden. Inzwischen hat die Gesellschaft eine Datenschutzerklärung erstellt, in der genau festgelegt ist, zu welchem Zweck die Daten benötigt werden, wer Zugriff darauf hat und wie sie aufbewahrt werden.

42 Ich empfehle der Landesregierung, im Rahmen des noch immer ausstehenden Wasserverkehrs- und Hafenanlagensicherheitsgesetzes (WVHaSiG), die datenschutzrechtlich bedeutsame Zuverlässigkeitsüberprüfung, welche umfangreiche Abfragemöglichkeiten zu bestimmten Hafenmitarbeitern bei Polizei und gegebenenfalls weiteren Sicherheitsbehörden erlaubt, gesetzlich zu regeln und mich hieran frühzeitig zu beteiligen.

2 Datenübermittlung nach dem Schornsteinfegergesetz

Ein Bürger fragte mich, welche personenbezogenen Daten Schornsteinfeger verarbeiten und an andere Stellen übermitteln. Er befürchtete, dass Schornsteinfeger Daten rechtswidrig an die Zollbehörden übermitteln.

Ich habe daraufhin die Schornsteinfegerinnung um eine Stellungnahme zur Verarbeitung personenbezogener Daten gebeten. Der Innungsobermeister teilte mir mit, dass sich die Schornsteinfeger an die Bestimmungen des Schornsteinfegergesetzes (SchfG), insbesondere an dessen § 19 halten. Dort ist festgelegt, dass Schornsteinfeger zur Erfüllung ihrer eigenen Aufgaben, zur Bekämpfung von Luft-, Boden- und Gewässerverschmutzung, zur rationellen Energieverwendung, zur Bauaufsicht und zur Brandbekämpfung personenbezogene Daten verar-

beiten und gegebenenfalls an andere öffentliche Stellen übermitteln dürfen, soweit dies erforderlich ist. In einem Gespräch räumte er jedoch ein, dass Mitarbeiter des Zolls häufig bei den Bezirksschornsteinfegern nachgefragt hätten, ob bestimmte Personen Eigentümer einer Ölfeuerungsanlage seien. Die Schornsteinfeger würden darauf nur mit „ja“ oder „nein“ antworten. Dies betrachtete er noch nicht als eine Übermittlung personenbezogener Daten. Hintergrund der Frage des Zolls ist, dass er mit dieser Information besser einem möglichen Missbrauch von Heizöl als Dieselkraftstoff nachgehen kann.

Dem Innungsobermeister habe ich erklärt, dass bereits die Beantwortung dieser Frage mit „ja“ oder „nein“ eine Übermittlung personenbezogener Daten darstellt, denn es werden Daten über die sachlichen Verhältnisse einer Person weitergegeben (§ 3 Abs. 1 Landesdatenschutzgesetz). § 19 SchfG enthält keine Vorschrift, nach der eine Übermittlung von personenbezogenen Daten für Zwecke der Strafverfolgung zulässig wäre. Ich habe empfohlen, die Bezirksschornsteinfeger darüber zu informieren, dass sie personenbezogene Daten nur übermitteln dürfen, wenn die ersuchende Stelle ihnen eine Rechtsgrundlage – beispielsweise nach dem Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern – mitteilt, nach der sie zur Auskunft verpflichtet sind.

Der Innungsobermeister hat zugesagt, die Empfehlung umzusetzen.

Dem Wirtschaftsministerium als Aufsichtsbehörde für das Schornsteinfegerwesen habe ich meine Rechtsauffassung hierzu mitgeteilt. Es hat ihr nicht widersprochen.

3 Kurverwaltung als Schrankenwärter

Ein Gast eines Ostseebades berichtete mir von einer Ferienhausanlage, in der er sich nicht ausreichend diskret behandelt fühlte.

Zur Anlage gehört ein Parkplatz, der mit einer Schranke gegen unbefugtes Befahren gesichert ist. Eigentümer und Gäste erhalten von der Kurverwaltung eine kontaktlose Chipkarte, mit der sie die Schranke öffnen können. Genauere Hinweise zur Funktion des Systems erhielten aber nur die Eigentümer der Ferienhäuser. Der Petent erfuhr davon zufällig, als er sich wegen eines Defektes seiner Karte an die Kurverwaltung wandte. Dort sah er verwundert, dass alle seine Ein- und Ausfahrten der letzten Tage mit Datum und Uhrzeit personenbeziehbar protokolliert waren.

Die Kurverwaltung teilte mir mit, dass diese Daten benötigt würden, um Manipulationsversuche zu erkennen, beispielsweise die Weitergabe von Karten an Unberechtigte. Die Schrankensteuerung könnte somit unter anderem registrieren, dass mit derselben Karte zweimal auf den Parkplatz gefahren wurde, ohne dass der Benutzer zwischendurch ausgefahren ist.

Die Zulässigkeit der Datenverarbeitung war in diesem Fall nach dem Bundesdatenschutzgesetz (BDSG) zu beurteilen, weil die Kurverwaltung als öffentlich-rechtliches Unternehmen (Eigenbetrieb der Gemeinde) am Wettbewerb teilnimmt (§ 2 Abs. 5 DSG M-V). § 28 Abs. 1 Nr. 1 BDSG erlaubt die Verarbeitung personenbezogener Daten, wenn es der Zweckbestimmung eines Vertragsverhältnisses oder eines vertragsähnlichen Ver-

trauensverhältnisses dient. Letzteres besteht zwischen Gast und Kurverwaltung. Die Zeitpunkte korrekter Ein- und Ausfahrten dürfen jedoch nicht gespeichert werden, weil dies weder zur Gebührenberechnung noch zur Erkennung von Missbrauch oder Defekten erforderlich ist. Außerdem hat die Kurverwaltung die Gäste nicht über die Verarbeitung ihrer Daten informiert, wie in § 4 Abs. 3 BDSG vorgeschrieben.

Auf meine Empfehlung hin hat die Kurverwaltung das Verfahren wie folgt geändert:

Neben den Stammdaten (Kartennummer, Gültigkeitsdauer, Parkplatznummer, Autokennzeichen und Meldescheinnummer) wird im regulären Betrieb nur noch gespeichert, wann die Karte zuletzt benutzt wurde und ob es sich dabei um eine Ein- oder Ausfahrt handelt. Dieser Datensatz wird bei der nächsten zulässigen Durchfahrt überschrieben. Der Versuch einer unzulässigen Durchfahrt wird protokolliert und bleibt eine Woche gespeichert. Dieser Zeitraum reicht aus, um zu klären, ob es sich um einen Defekt oder einen Missbrauchsversuch handelt. Darüber hinaus erklärt die Kurverwaltung den Gästen nun in einem Merkblatt, was genau mit ihren Daten passiert.

43 Ich empfehle der Landesregierung, im Rahmen der Tourismusförderung insbesondere Unternehmen und Kurverwaltungen für einen datenschutzgerechten Umgang mit den Daten ihrer Gäste zu sensibilisieren. Das gilt insbesondere bei der Einführung elektronischer Systeme.

VI Landwirtschaftsausschuss / Ministerium für Ernährung, Landwirtschaft, Forsten und Fischerei

1 Auskunft an den Eigentümer einer landwirtschaftlichen Fläche

Als gerade bestätigter Eigentümer einer landwirtschaftlichen Fläche wollte ein Landwirt vom zuständigen Amt für Landwirtschaft Namen und Adresse des Nutzers seiner Flächen wissen, um mit diesem die Nutzungsbedingungen vertraglich zu vereinbaren. Das Amt hatte diese Auskunft jedoch mit dem Hinweis auf eine Datenschutzklausel in den Anträgen auf Agrarförderung verweigert. Der Landwirt hat mich gebeten, den Sachverhalt zu prüfen.

In der Regel beantragt jeder landwirtschaftliche Betrieb oder jede landwirtschaftlich tätige Person Mittel der Agrarförderung bei dem jeweiligen Amt für Landwirtschaft. Dazu müssen auch die bewirtschafteten Flächen angeben werden. Somit liegt dort ein fast vollständiges Verzeichnis der genutzten Flächen vor. Das Amt wäre also durchaus in der Lage gewesen, die Frage des Eigentümers zu beantworten. Es teilte ihm jedoch mit, dass in der Datenschutzklausel der Anträge auf Agrarförderung aufgeführt ist, an welche Stellen Daten des Antrages übermittelt werden dürfen. Eine Übermittlung an Privatpersonen war nicht darunter. Deshalb sah es sich nicht in der Lage, die erbetene Auskunft zu erteilen.

Die Frage der Auskunftserteilung habe ich mit dem zuständigen Mitarbeiter unseres Landwirtschaftsministeriums diskutiert. Datenübermittlungen sind aufgrund einer Rechtsvorschrift oder mit Einwilligung des Betroffenen zulässig. Weil die Einwilligung des betroffenen Nutzers zur Weitergabe seines Namens und seiner Anschrift nicht vorlag, war zu prüfen, ob eine Rechtsvorschrift es gestattet, diese Angaben zu übermitteln. Name und Anschrift des Nutzers der landwirtschaftlichen Fläche können nach meiner Auffassung auf der Basis des § 15 Abs. 1 Landesdatenschutzgesetz an den Eigentümer übermittelt werden, denn er hat ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft dargelegt, und es ist nicht ersichtlich, dass der betroffene Nutzer ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung dieser Daten hat. Dieses Ergebnis habe ich dem Landwirt mitgeteilt.

44 Ich empfehle der Landesregierung und allen anderen öffentlichen Stellen in Mecklenburg-Vorpommern, bei Auskunftsbegehren aufgrund eines berechtigten oder rechtlichen Interesses genau zu prüfen, ob dem Wunsch entsprochen werden kann.

2 Cross Compliance in der Landwirtschaft

Die Europäische Union hat ihre Gemeinsame Agrarpolitik (GAP) in den zurückliegenden Jahren entscheidend reformiert. Ein wesentlicher Punkt dieser Reform ist, dass Direktzahlungen an Landwirte mit anderweitigen Verpflichtungen, insbesondere des Umwelt-, Verbraucher- und Tierschutzes verbunden werden. Diese Verbindung ist die so genannte Cross Compliance, bei der es im Kern darum geht, dass Verstöße gegen den Umwelt-, Tier- oder Verbraucherschutz zu Sanktionen bei der Agrarförderung führen.

Die landwirtschaftliche Förderung wird bei Verstößen in Abhängigkeit von ihrer Schwere und Anzahl nach vorgegebenen Kriterien schrittweise gekürzt. Die Einhaltung der umwelt-, tier- und verbraucherschutzrechtlichen Bestimmungen obliegt den zuständigen Fachüberwachungsbehörden, beispielsweise den Natur- und Umweltschutz- oder den Jagdbehörden. In den Rechtsgrundlagen zur Cross Compliance ist die Datenübermittlung zwischen den für die

Förderung zuständigen landwirtschaftlichen Behörden und den Fachüberwachungsbehörden nicht geregelt. Unser Landwirtschaftsministerium hatte vorgesehen, dass die Antragsteller auf Fördermittel in die Übermittlung ihrer Daten einwilligen sollten.

Eine datenschutzrechtliche Einwilligung unterliegt jedoch der freien Entscheidung des Betroffenen, sie muss jederzeit widerrufen werden können, und es dürfen in der Regel keine Nachteile entstehen, wenn sie verweigert wird, anderenfalls ist hierauf besonders hinzuweisen. Diese Voraussetzungen lassen sich hier nicht umsetzen, denn eine landwirtschaftliche Förderung wird nur gewährt, wenn die Daten vorliegen und kontrolliert werden kann, ob die Rahmenbedingungen eingehalten werden. Eine freie Entscheidung der Antragsteller über die Datenverarbeitung ist folglich nicht möglich. Es sollte ihnen daher durch die Einwilligung auch nicht suggeriert werden, dass die Datenverarbeitung sowie die Kontrollen von ihrem Willen beeinflussbar sind.

Ich habe statt dessen dem Landwirtschaftsministerium empfohlen, die Antragsteller umfassend über die mit der Förderung zusammenhängenden Datenverarbeitungen sowie Kontrollen aufzuklären. Das Landesdatenschutzgesetz schreibt vor, dass die Betroffenen über den Zweck der Erhebung, die Art und den Umfang der Verarbeitung, über Empfänger beabsichtigter Übermittlungen der Daten sowie über ihre Auskunfts- und Berichtigungsansprüche aufzuklären sind – § 9 Abs. 3 Satz 1 Landesdatenschutzgesetz. Sofern keine speziellen Datenverarbeitungs- und Datenübermittlungsregelungen vorhanden sind, können die erforderlichen Daten dann auf der Grundlage der allgemeinen datenschutzrechtlichen Bestimmungen des Landesdatenschutzgesetzes verarbeitet werden.

45 Die Landesregierung und die anderen öffentlichen Stellen sollten auch bei anderen Projekten, bei denen Vorteile für betroffene Personen unabdingbar mit Datenverarbeitungen verbunden sind, umfassend darüber aufklären und eine Einwilligung nur dort vorsehen, wo die Betroffenen tatsächlich Alternativen haben.

VII Bildungsausschuss / Ministerium für Bildung, Wissenschaft und Kultur

1 Datenerhebungen für Forschungsprojekte

Forscher und Forschungseinrichtungen bitten mich häufig um eine datenschutzrechtliche „Genehmigung“, wenn sie für einen Forschungszweck personenbezogene Daten erheben und verarbeiten wollen. Solche Datenverarbeitungen zu genehmigen, liegt jedoch außerhalb meines Aufgabenbereiches. Dies kann in der Regel nur das zuständige Ministerium als oberste Aufsichtsbehörde, sofern eine öffentliche Stelle des Landes an dem Projekt beteiligt werden soll. Ungeachtet dessen gehört es zu meinen Aufgaben, Stellen zu beraten, die personenbezogene Daten verarbeiten wollen.

Ausgangspunkt für viele Forschungsprojekte ist eine Befragung von Personen oder bestimmten Personengruppen. Sie werden meist über das Ziel des Projektes informiert. Dabei wird jedoch häufig vergessen, ausdrücklich darauf hinzuweisen, dass die Teilnahme an Befragungen für Forschungszwecke freiwillig ist (§ 9 Abs. 3 Landesdatenschutzgesetz). Übrigens bedeutet Freiwilligkeit auch, dass es den Teilnehmern freigestellt sein muss, einzelne Fragen nicht zu beantworten. Es kann niemand gedrängt werden, für einen Forschungszweck einen vollständig ausgefüllten Fragebogen abzugeben.

Den zu Befragenden wird außerdem meist zugesichert, dass ihre Daten anonym verarbeitet werden. Dies trifft aber nur dann zu, wenn Dritte aus einem Datensatz keine Person mehr bestimmen können. Allein auf den Namen und die Adresse oder eine Versicherungsnummer etc. zu verzichten, genügt dafür nicht. In jedem Fall sind Angaben zu vermeiden, die wegen ihrer Singularität und des in der Region vorhandenen Wissens dazu führen würden, dass aus dem inhaltlichen Kontext eine Person bestimmt werden kann. Das lässt sich dadurch erreichen, dass nicht nach konkreten Daten gefragt wird, sondern die Merkmale einer Antwort so gruppiert werden, dass keine Einzelfälle auftreten können. Beispielsweise sollte nicht nach der konkreten Zahl der Kinder einer teilnehmenden Person gefragt werden, weil Dritte daraus unter Umständen eine Person bestimmen können, wenn in der Region allgemein bekannt ist, welche Familie beispielsweise zehn Kinder hat. Besser wäre es deshalb, Gruppen vorzugeben und zu fragen, ob die befragte Person keine, ein, zwei oder drei, vier oder mehr Kind(er) hat. Dies würde dazu beitragen, dass mit hoher Wahrscheinlichkeit keine Einzelfälle erfasst werden.

46 Ich empfehle der Landesregierung, Forschungsprojekte mit personenbezogenen oder aus diesen gewonnenen Daten nur zu genehmigen, wenn dazu ein datenschutzrechtliches Votum des jeweiligen behördlichen Datenschutzbeauftragten vorliegt.

2 Das Schulberichtssystem

Das Ministerium für Bildung, Wissenschaft und Kultur Mecklenburg-Vorpommern hat ein Schulberichtssystem eingeführt, um die Informationsgrundlagen für die Schulaufsicht zu verbessern und damit gleichzeitig die Unterrichtsversorgung fachgerecht planen zu können. Außerdem soll das System die Schulen bei den durchzuführenden Schulstatistiken entlasten.

Die Daten der Schüler und Lehrer werden auf einem Server im Datenverarbeitungszentrum des Landes so gespeichert, dass in der Regel nur die berechtigten Mitarbeiter in den Schulen die personenbezogenen Daten ihrer Schüler und Lehrer zur Kenntnis nehmen können. In Ausnahmefällen, wie Einschulungen, können auch berechtigte Mitarbeiter des zuständigen Schulamtes auf personenbezogene Daten der Schüler zugreifen. Die berechtigten Nutzer des Systems in den Schulämtern sowie im Ministerium können sonst nur pseudonymisierte Daten verarbeiten.

Auch das Statistische Landesamt erhält in regelmäßigen Zeitabständen die zur Durchführung der Schulstatistik erforderlichen pseudonymisierten Daten. Anonymisierte Daten können dafür nicht genutzt werden, weil Plausibilitätsprüfungen durchgeführt werden müssen.

Die Begriffe **„anonymisieren“** und **„pseudonymisieren“** sind in § 3 Abs. 4 Nr. 8 bzw. 9 Landesdatenschutzgesetz (DSG M-V) datenschutzrechtlich definiert. Danach darf nach dem Anonymisieren ein Datensatz keine identifizierenden Daten (Name oder Schülernummer) mehr enthalten und die weiteren Daten (z. B. Alter, Nationalität oder Bildungsstand) dürfen nicht mehr oder nur mit einem unverhältnismäßig hohem Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Durch Anonymisierung soll die Zuordnung der Daten zu einer Person generell ausgeschlossen sein, während nach dem Pseudonymisieren die Zuordnung in vorher bestimmten Fällen möglich sein soll. Dafür wird eine Zuordnungsfunktion verwendet. Diese Funktion kann im einfachsten Fall eine Zuordnungstabelle sein. Die Stellen und Personen, die diese Zuordnungsfunktion besitzen, können den Personenbezug ohne weiteres herstellen. Es handelt sich für sie also um personenbezogene Daten. Der datenschutzrechtliche Effekt tritt erst dann auf, wenn die pseudonymisierten Daten an Stellen oder Personen gelangen, die keinen Zugriff auf die Zuordnungsfunktion haben. Sie dürfen die pseudonymisierten Daten nicht auf Personen beziehen können.

Dabei festgestellte fehlerhafte Datensätze können nur korrigiert werden, wenn die berechtigten Mitarbeiter in der jeweiligen Schule und im Statistischen Landesamt den Bezug zu dem implausiblen Datensatz eindeutig herstellen können.

Ich habe das Bildungsministerium umfassend bei der Gestaltung des Schulberichtssystems beraten. Im Mittelpunkt stand dabei die Festlegung des Datenkatalogs für die einzelnen Nutzergruppen sowie der Zugriffsrechte. Es sind Sicherheitsmaßnahmen getroffen worden, die grundsätzlich gewährleisten, dass die berechtigten Nutzer nur die Daten verarbeiten können, die zur Erfüllung ihrer konkreten Aufgabe erforderlich sind. Nach wie vor fehlt aber ein Datenschutz- und Datensicherheitskonzept, so dass eine vollständige datenschutzrechtliche Bewertung nicht möglich ist. Zu klären ist auch noch, ob und in welcher Weise andere Stellen, zum Beispiel die Schulverwaltungsämter bei den kreisfreien Städten und Landkreisen, das Schulberichtssystem nutzen dürfen. Außerdem ist offen, ob und zu welchem Zweck das Statistische Amt die übermittelten pseudonymisierten Daten weiter speichern und nutzen darf.

47 Ich empfehle der Landesregierung, unverzüglich das Datenschutz- und Datensicherheitskonzept für das Schulberichtssystem nachzureichen und die offenen

Punkte zu klären. Künftig sollten Verfahren zur Datenverarbeitung erst in Betrieb genommen werden, wenn ein solches Konzept geprüft vorliegt.

VIII Bauausschuss /Ministerium für Arbeit, Bau und Landesentwicklung

1 Höhe des Vermögens bei Wohngeldbeantragung

Ein Petent hatte Wohngeld beantragt und dazu seinen Einkommensteuer- und seinen Arbeitslosengeld-II-Bescheid vorgelegt. Aus dem Einkommensteuerbescheid waren Kapitaleinkünfte ersichtlich. Das Arbeitslosengeld II wurde aufgrund vorhandenen Vermögens nicht gewährt, was aus dem Bescheid hervorging. Die Wohngeldstelle forderte ihn nun auf, die Höhe seines Vermögens anzugeben. Er wurde auch darauf hingewiesen, dass er hierzu gemäß §§ 60, 66 Erstes Buch Sozialgesetzbuch (SGB I, Mitwirkungspflichten) verpflichtet sei. Der Petent hat mich gebeten, den Sachverhalt zu prüfen.

Nach den Bestimmungen des Wohngeldgesetzes (WoGG) ist der Wohngeldanspruch von der Höhe des monatlichen Einkommens abhängig (§ 2 Abs. 1 WoGG). Welche Daten bei der Einkommensermittlung zu Grunde zu legen sind, regeln die §§ 9 ff. WoGG. Zum Einkommen zählen beispielsweise auch Zinsen, Kapitalerträge, Einnahmen aus Vermietungen und Verpachtungen, so dass indirekt das Vermögen berücksichtigt wird. Die Höhe des Vermögens geht aber nicht in die Berechnung des Wohngeldes ein und darf somit auch nicht erhoben werden.

Denkbar wäre allenfalls eine Fallkonstellation, dass ein Antragsteller ein beträchtliches Vermögen nicht gewinnbringend anlegt und somit kein Einkommen daraus erzielt, obwohl dies zumutbar wäre. In einem solchen Fall könnte die Mitteilung der Vermögenshöhe erforderlich sein, um festzustellen, ob das Wohngeld missbräuchlich in Anspruch genommen wird. Ich habe den Bundesbeauftragten für den Datenschutz gebeten, diese Frage auf Bundesebene zu erörtern.

Im vorliegenden Fall muss der Einkommensteuerbescheid für die Berechnung des Wohngeldes ausreichen. Daten über die Höhe des Vermögens sind nicht zu erheben, weil der Betroffene alle gesetzlich vorgeschriebenen Angaben zum Einkommen nachgewiesen hat.

48 Ich empfehle der Landesregierung gegenüber den Wohngeldstellen im Land klarzustellen, dass bei der Berechnung des Wohngeldes die Höhe des Vermögens nicht erhoben werden darf.

2 JobCard-Verfahren

Mit dem JobCard-Verfahren wird eine der umfangreichsten Sammlungen personenbezogener Daten in Deutschland entstehen, denn an zentraler Stelle werden Daten von ca. 40 Millionen abhängig Beschäftigten gespeichert. Da dieses Verfahren praktisch jeden Arbeitnehmer und jeden Arbeitgeber – unabhängig von der Zahl der Beschäftigten – betreffen wird, sollte man eine breite öffentliche Diskussion erwarten. Dies ist erstaunlicher Weise nicht der Fall.

Die Arbeitgeber und ihre Dachverbände verfolgen seit einigen Jahren das Ziel, eine zentrale Datenbank zur elektronischen Speicherung von Arbeitnehmerdaten einzurichten. Die Arbeitgeber sollen im hierfür entwickelten JobCard-Verfahren monatlich für jeden Beschäftigten die Leistungs- und Entgeltdaten in elektronischer Form melden. Aus dieser Datenbank sollen berechtigte Stellen anstelle der bisher erforderlichen papiergebundenen Bescheinigungen

künftig Verdienst-, Entgelt- und Arbeitsbescheinigungen unter Mitwirkung der Antragsteller elektronisch abrufen, um die Anspruchsvoraussetzungen für die Gewährung von Sozialleistungen wie Arbeitslosengeld, Wohngeld oder Kindergeld zu prüfen. Die Arbeitgeber erhoffen sich erhebliche Einsparungen, wenn sie künftig keine papiergebundenen Bescheinigungen mehr ausstellen müssen.

Vor diesem Hintergrund hat die Bundesregierung im Sommer 2002 beschlossen, für alle Arbeitnehmer eine so genannte JobCard einzuführen und das JobCard-Verfahren unter Federführung des Bundesministeriums für Wirtschaft und Arbeit (BMWA) zunächst in einem Modellversuch zu erproben. Als JobCard kann jede Chipkarte verwendet werden, mit der qualifizierte Signaturen nach dem Signaturgesetz erzeugt werden können.

> Die **qualifizierte elektronische Signatur** ist eine Form der elektronischen Unterschrift und kann unter bestimmten Bedingungen die handschriftliche Unterschrift ersetzen. Die Signatur wird mit kryptographischen Verfahren erzeugt. Der zur Erzeugung der Signatur erforderliche geheime Signaturschlüssel wird auf einer Chipkarte gespeichert, die in der alleinigen Verfügungsgewalt des Eigentümers ist und den Anforderungen des Signaturgesetzes genügen muss.

Mit einer solchen Signaturkarte soll sichergestellt werden, dass berechtigte Stellen nur dann Daten elektronisch abgerufen können, wenn der Antragsteller eingewilligt hat.

Die geplante zentrale Speicherung der Leistungs- und Entgeltdaten jedes abhängig Beschäftigten stellt einen erheblichen Eingriff in das verfassungsmäßige Recht auf informationelle Selbstbestimmung dar und bedarf deshalb einer gesetzlichen Regelung. Eine solche erarbeitet zurzeit das BMWA mit dem JobCard-Verfahrensgesetz.

Mit der Einführung der JobCard verfolgt die Bundesregierung ein weiteres Ziel. Das Signaturgesetz regelt die Details zur technischen Ausgestaltung der digitalen Signatur und schafft somit wichtige Voraussetzungen, um rechtsverbindliche Unterschriften auch im elektronischen Geschäftsverkehr leisten zu können (siehe Sechster Tätigkeitsbericht, Punkt 2.16.3). Bisher gibt es jedoch kaum Anwendungen hierfür, so dass Signaturgesetz konforme Chipkarten wenig Verbreitung fanden. Diese Chipkarten werden nun für das JobCard-Verfahren gesetzlich vorgeschrieben. Damit wären die besten Voraussetzungen gegeben, um weiteren Signatur basierten Verfahren beispielsweise aus den Bereichen E-Commerce oder E-Government zum Durchbruch zu verhelfen.

Zwei Aspekte sind von grundsätzlicher datenschutzrechtlicher Bedeutung. Einerseits entsteht durch dieses Verfahren ein sehr großer zentraler Bestand sensibler Daten. Die Speicherung dieser Daten ist jedoch nur für diejenigen erforderlich, die tatsächlich Leistungen beantragen. Das wird nur einen bisher nicht näher bezifferten Bruchteil der Beschäftigten betreffen. Mit Blick auf die Rechtsprechung des Bundesverfassungsgerichts stellt sich damit die Frage, ob nicht Daten in unzulässiger Weise auf Vorrat gespeichert werden und damit das gesamte Verfahren dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit widerspricht.

Andererseits müssen technische und organisatorische Vorkehrungen getroffen werden, die sicherstellen, dass Daten ausschließlich von berechtigten Mitarbeitern abgerufen werden können. Um den erforderlichen Zugriffsschutz zu gewährleisten, sollen unter anderem die Daten

in der zentralen Speicherstelle verschlüsselt gespeichert werden. Da jedoch die Verfahrensbetreiber selbst über die Schlüssel verfügen, ist prinzipiell nicht auszuschließen, dass die Daten ohne Zustimmung des Betroffenen ausgelesen werden. Somit sind weitere Sicherungsmechanismen erforderlich, deren Wirksamkeit nicht ausschließlich durch die Verfahrensbetreiber kontrollierbar sein dürfen.

Diese beiden Aspekte führen zu zwei zentralen Forderungen an die Bundesregierung, die vor der schrittweisen Inbetriebnahme des JobCard-Verfahrens ab dem 1. Januar 2007 umgesetzt sein müssen:

- Die Bundesregierung muss nachweisen, dass das geplante Verfahren verfassungsrechtlich zulässig ist. Die Datenschutzbeauftragten des Bundes und der Länder erwarten, dass die Begründung zum JobCard-Verfahrensgesetz diesen Nachweis enthält.
- Am JobCard-Verfahren muss eine unabhängige Vertrauensstelle beteiligt werden, die jederzeit kontrollieren kann, ob der Zugriff auf die Daten der zentralen Speicherstelle zulässig ist, und die bei Verstößen den Zugriff auf die zentralen Datenbestände sofort unterbinden kann.

49 Ich empfehle der Landesregierung, dem JobCard-Verfahrensgesetz im Bundesrat nur dann zuzustimmen, wenn die Verfassungsmäßigkeit des Verfahrens nachgewiesen, die Sicherheit der Daten garantiert und eine Kontrolle durch unabhängige Stellen gewährleistet ist.

3 Arbeitslosengeld II

Die Arbeitsgemeinschaften (ARGEn) zur Grundsicherung für Arbeitssuchende unterstützen nun seit einem Jahr Hilfebedürftige dabei, dass diese eine Erwerbstätigkeit aufnehmen oder behalten und ihren Lebensunterhalt sichern können. Das datenschutzrechtliche Fazit nach dieser einjährigen Tätigkeit ist allerdings sehr ernüchternd. So hat die 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. Oktober 2005 gefordert, endlich die gravierenden datenschutzrechtlichen Mängel beim Arbeitslosengeld II (ALG II) zu beseitigen (siehe Anlage 20).

Sozialgeheimnis wird verletzt

Ein wesentlicher Mangel bei der Umsetzung des ALG II besteht darin, dass die gesetzlichen Anforderungen an das Sozialgeheimnis bei der Datenverarbeitung nicht im vollen Umfang eingehalten werden. So lautet § 35 Abs. 1 Satz 2 Sozialgesetzbuch Erstes Buch (SGB I): „Die Wahrung des Sozialgeheimnisses umfasst die Verpflichtung, auch innerhalb des Leistungsträgers sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden.“ Diese Verpflichtung wird aber durch das angewandte Datenverarbeitungsverfahren A2LL nach wie vor nicht umgesetzt. Es ist gegenwärtig nicht möglich, den Zugriff auf die Daten nach dem Grundsatz der Erforderlichkeit zur Aufgabenerfüllung einzuschränken. Vielmehr ist es so, dass rund 40.000 Mitarbeiter der Bundesagentur für Arbeit und der ARGEn auf alle dort gespeicherten Daten der ALG-II-Empfänger aus ganz Deutschland voraussetzungslos und ohne jegliche Kontrolle zugreifen können. Diesen Mangel hat der Bundesbeauftragte für den Datenschutz bereits im November 2004 beanstandet; doch bisher

hat sich nichts geändert. Dadurch ist das Sozialgeheimnis nach § 35 Sozialgesetzbuch Erstes Buch (SGB I) permanent verletzt.

Weil die Bundesagentur für Arbeit den ARGEn in Mecklenburg-Vorpommern vorschreibt, diese Software zu nutzen, ist es mir allein nicht möglich, eine datenschutzgerechte Verarbeitung zu erreichen. Es gibt Hinweise aus der Bundesagentur, dass demnächst ein neues Datenverarbeitungssystem eingeführt werden soll. In diesem Zusammenhang sollte darüber nachgedacht werden, es den ARGEn freizustellen, welche Software sie einsetzen. Ohne zentrales Datenverarbeitungssystem könnte zumindest der bundesweite Zugriff auf die Daten vermieden werden. Die zur Aufgabenerfüllung der Bundesagentur für Arbeit erforderlichen und gesetzlich bestimmten Daten könnten die ARGEn dann über definierte Schnittstellen übermitteln.

Aufgrund verschiedener Petitionen kam es mir darauf an, eigene Eindrücke von der Datenverarbeitung zu gewinnen. Deshalb habe ich im April 2005 das Job-Center Uecker-Randow – eine Arbeitsgemeinschaft, die von der Bundesagentur für Arbeit und dem Landkreis gebildet wurde – sowie die Sozialagentur des Landkreises Ostvorpommern – die als einzige in Mecklenburg-Vorpommern allein vom Landkreis errichtet wurde – kontrolliert. Die Kontrolle dieser beiden Stellen war vor allem deshalb aufschlussreich, weil jede ein anderes Datenverarbeitungsprogramm nutzt.

Die ARGE muss die von der Bundesagentur vorgegebene Software A2LL nutzen. Bei der Kontrolle habe ich ebenfalls den Zustand vorgefunden, den der Bundesbeauftragte für den Datenschutz beanstandet hat (siehe oben). So konnten Mitarbeiter der Arbeitsgemeinschaft in der gesamten Bundesrepublik nach Personen suchen und deren Daten zur Kenntnis nehmen. In meinem Kontrollbericht habe ich auf diesen datenschutzrechtlichen Mangel hingewiesen. Die Bundesagentur für Arbeit hat zu diesem Punkt meines Berichtes unter anderem Folgendes geschrieben: „Vor allen anderen Fragen hatte absolute Priorität die pünktliche und nahtlose Gewährung von Geldleistungen für Arbeitssuchende ab dem 1. Januar 2005. ... Vor diesem Hintergrund konnte das zur Zahlbarmachung dieser Leistungen entwickelte Verfahren A2LL naturgemäß nicht von Anfang an so eingerichtet werden, dass allen berechtigten Belangen des Datenschutzes sofort und vollumfänglich Rechnung getragen wurde.“ Bis heute hat sich jedoch an diesem Zustand nichts Wesentliches geändert. Ein Zugriffsberechtigungskonzept ist immer noch nicht umgesetzt worden. Die Zugriffe auf den Datenbestand werden auch nicht protokolliert. Damit wird also nach wie vor das Recht der betroffenen Personen auf informationelle Selbstbestimmung gegen die für sie unbestritten dringend notwendigen Grundsicherungsleistungen ausgespielt. Somit bleibt nur die Hoffnung, dass durch den unzureichenden Zugriffsschutz für die Betroffenen kein größerer Schaden entsteht.

Die Sozialagentur der Optionskommune konnte hingegen bei der Software unter den Angeboten frei wählen. Sie hat sich für das Produkt einer Firma entschieden, die über Erfahrungen bei der Entwicklung von Sozialleistungssoftware verfügt und deren Produkt zur Berechnung von Sozialhilfe beispielsweise vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein zertifiziert worden ist und ein Datenschutz-Gütesiegel erhalten hat. Bei der Software der Sozialagentur gab es daher nicht nur keinen bundesweiten Zugriff, sondern sie erfüllt auch alle weiteren datenschutzrechtlichen Anforderungen.

Zuständigkeiten ungeklärt

Nach wie vor bestreitet die Bundesagentur für Arbeit die Eigenverantwortlichkeit der ARGEn als datenverarbeitende Stellen – ein weiterer gravierender Mangel bei der Umsetzung des ALG II. Das führt dazu, dass die Zuständigkeit für datenschutzrechtliche Fragen ungeklärt ist. Besonders deutlich zeigte sich dies bei meinen Versuchen, die kommunalen Träger und die ARGEn zu beraten. So habe ich zunächst Kontakt mit dem Städte- und Gemeindetag Mecklenburg-Vorpommern aufgenommen, um mit dessen Mitgliedern als Teil der kommunalen Träger der Arbeitsgemeinschaften in unserem Bundesland die offenen datenschutzrechtlichen Fragen zu diskutieren. Die Resonanz war gering – auch zu meinem Angebot weiterer Beratungen. Ein Teilnehmer meinte zum Beispiel, dass er keinen Computer an seinem Arbeitsplatz habe und er deswegen meine Hinweise nicht umsetzen könne. Er fühlte sich offensichtlich für die Datenverarbeitung in der ARGE nicht verantwortlich.

Im August 2005 habe ich dann alle Arbeitsgemeinschaften des Landes gebeten, mir ihre Datenschutzbeauftragten zu nennen, um mit ihnen eine Informationsveranstaltung zum Datenschutz beim ALG II durchzuführen. Auf mein Schreiben haben nur zwei ARGEn reagiert. Andere haben meine Einladung an die Bundesagentur für Arbeit weitergeleitet. Diese teilte mir mit, dass die Frage, ob Arbeitsgemeinschaften verpflichtet sind, eigene Datenschutzbeauftragte zu bestellen, nicht abschließend geklärt sei. Nach dortiger Auffassung würden die Leistungsträger, die nach dem Recht der Grundsicherung für Arbeitssuchende zuständig sind, verantwortliche Stellen sein. Daraus folgert man wohl, dass der Datenschutzbeauftragte des kommunalen Trägers und derjenige der Bundesagentur für Arbeit die entsprechenden Aufgaben wahrnehmen. Eine der ARGEn teilte mit, dass der kommunale Träger keine rechtliche Grundlage zur Bestellung eines behördlichen Datenschutzbeauftragten der Arbeitsgemeinschaft sehe. So kann man Verantwortung ab- und die Lösung datenschutzrechtlicher Fragen zu Lasten der Betroffenen auf die lange Bank schieben.

Die ungeklärte Zuständigkeit führt dazu, dass ich Fragen von betroffenen Personen nicht effektiv bearbeiten kann, weil ARGEn, die ich um Stellungnahme zu einer Angelegenheit bitte, in der Regel mein Schreiben an die Bundesagentur weiterleiten. Dadurch wird das Verfahren unnötig verzögert. Die Datenschutzbeauftragten des Bundes und der Länder hingegen betrachten die ARGEn als eigenverantwortliche datenverarbeitende Stellen, die damit uneingeschränkt der Kontrolle der Landesbeauftragten für den Datenschutz unterliegen.

Unzulässige Telefonbefragungen

In der zweiten Hälfte des Jahres 2005 führte der von der Bundesregierung nicht erwartete Anstieg der Kosten des Arbeitslosengeldes II zu einer öffentlichen Missbrauchsdiskussion mit teilweise abenteuerlichen Zahlen. So ist verbreitet worden, dass bis zu 20 % der ALG-II-Empfänger zu Unrecht Leistungen beziehen würden. Diese Quote ist aus einer datenschutzrechtlich ohnehin sehr zweifelhaften Telefonaktion der Bundesagentur für Arbeit hochgerechnet worden: Betroffene, die telefonisch nicht erreicht werden konnten oder eine Teilnahme an der Aktion ablehnten, wurden dem Generalverdacht des Leistungsmissbrauchs ausgesetzt. Mit der Wirklichkeit hatte diese Zahl jedoch nichts gemein, worauf auch Fachleute der Bundesagentur hingewiesen haben. Dennoch wurden im politischen Raum weitere datenschutzrechtliche Einschnitte gefordert, beispielsweise weitere anlassunabhängige Abgleiche über die bereits gesetzlich geregelten Datenabgleiche hinaus.

50 Ich empfehle der Landesregierung, die Stellung der ARGEn in Mecklenburg-Vorpommern als eigenverantwortliche datenverarbeitende Stellen zu stärken, eine datenschutzgerechte Verarbeitung von Sozialdaten in den ARGEn zu fördern und die Kontrollkompetenz durch den Landesbeauftragten für den Datenschutz klarzustellen.

4 Hochbau-Statistik

Wie in meinem Fünften Tätigkeitsbericht, Punkt 3.8.2, und in meinem Sechsten Tätigkeitsbericht, Punkt 3.2, dargestellt, hatten die Baubehörden seit mehreren Jahren in rechtswidriger Weise personenbezogene Daten von Bauherren für Zwecke der Hochbaustatistik erhoben. Der zugrunde liegende Erlass ist nun endlich mit der Landesverordnung zur Durchführung des Hochbaustatistikgesetzes vom 18. Oktober 2004 aufgehoben worden. Diese Verordnung legt ein Verfahren zur Datenerhebung fest, das den Vorgaben des Hochbaustatistikgesetzes entspricht und auch datenschutzgerecht ist.

IX Sozialausschuss / Sozialministerium

1 Neugeborenenscreening

Das Blut neugeborener Kinder kann kurz nach der Geburt auf mehrere schwerwiegende Stoffwechselerkrankungen untersucht werden. Diese freiwillige Reihenuntersuchung wird als Screening bezeichnet. Für Kinder in Mecklenburg-Vorpommern untersucht das Screeninglabor der Ernst-Moritz-Arndt-Universität Greifswald diese Blutproben. Ich habe das Labor besucht und die mit dem Neugeborenenscreening zusammenhängende Datenverarbeitung kontrolliert.

Das Labor erhält die Proben auf Testkarten, auf die das Blut in der Geburtseinrichtung aufgeträufelt wurde. Diese Karte hat neben einem Teil für die Blutprobe auch einen Abschnitt mit den Identitätsdaten des Kindes. Nach der Analyse der Probe werden die gewonnenen Werte zunächst personenbezogen gespeichert. Dies ist erforderlich, um die Geburtseinrichtungen über festgestellte Erkrankungen zu benachrichtigen oder auch um Nachfragen von diesen zu beantworten. Nach Ablauf von sechs Monaten werden die Testkarten und die gespeicherten Daten pseudonymisiert. Identifizierende Daten und pseudonymisierte Daten werden getrennt gespeichert und dürfen nur zusammengeführt werden, wenn Untersuchungen nachträglich im Interesse der betroffenen Kinder oder Eltern überprüft werden müssen. Nach zehn Jahren werden die Daten gelöscht und die Testkarten vernichtet. Ich habe hierzu ergänzend Folgendes empfohlen:

In dem nach § 18 Abs. 1 Nr. 2 Landesdatenschutzgesetz erstellten Verfahrensverzeichnis wurde als Rechtsgrundlage für die Datenverarbeitung die „Richtlinie zur Organisation des Neugeborenenscreenings auf angeborene Stoffwechselstörungen und Endokrinopathien in Deutschland“ genannt. Das Screening ist jedoch eine freiwillige Untersuchung. Deshalb ist Voraussetzung für die Datenerhebung und -verarbeitung die informierte Einwilligung der Eltern beziehungsweise der Mutter (§ 15 Abs. 1 Landeskrankenhausgesetz). Des Weiteren sollte in das Informationsblatt über das Screening, welches die Mutter erhält, ein Blatt mit einer datenschutzrechtlichen Einwilligungserklärung eingefügt werden. Diese Einwilligungserklärung sollte in der Patientenakte der Geburtseinrichtung aufbewahrt werden. Eine entsprechende Erklärung wurde in Abstimmung mit mir erarbeitet.

Im Ergebnis der Kontrolle kann ich feststellen, dass das Neugeborenenscreening in unserem Land den datenschutzrechtlichen Bestimmungen entspricht.

2 Krankenhausinformationssystem

Anlässlich eines Kontroll- und Informationsbesuches in einem Krankenhaus habe ich festgestellt, dass dort die datenschutzrechtlichen Bestimmungen des Landeskrankenhausgesetzes (LKHG M-V) nicht vollständig umgesetzt waren.

Das Krankenhaus nutzt zur Verarbeitung der Patientendaten ein Krankenhausinformationssystem. Dieses System ist auf einer Datenverarbeitungsanlage installiert, die das Krankenhaus geliehen hat. Mit dem Eigentümer wurde die Systembetreuung vertraglich vereinbart. Bei dieser Datenverarbeitung handelt es sich um eine Datenverarbeitung im Auftrag nach § 21 LKHG M-V. In dieser Rechtsvorschrift ist geregelt, unter welchen Bedingungen Patientenda-

ten von einem Auftragnehmer verarbeitet werden dürfen und was dabei zu beachten ist. So sind unter anderem die vom Auftragnehmer zu treffenden technischen und organisatorischen Sicherungsmaßnahmen schriftlich zu vereinbaren. Dies war nicht realisiert. Vielmehr war die Firma eigenständig für die Pflege des Betriebssystems und der systemnahen Software verantwortlich.

Bei der Datenverarbeitung im Auftrag bleibt der Auftraggeber – hier also das Krankenhaus – dafür verantwortlich, dass die gesetzlichen Bestimmungen eingehalten werden. Deshalb habe ich das Krankenhaus aufgefordert, die vorgeschriebenen Zulässigkeitsvoraussetzungen für die Datenverarbeitung im Auftrag nachzuweisen und die technischen und organisatorischen Sicherungsmaßnahmen vertraglich zu vereinbaren.

Eine Stellungnahme zu meinem Bericht liegt mir bis heute nicht vor. Das Krankenhaus bat um Terminaufschub, da alle Mitarbeiter der Verwaltung in die anstehende Privatisierung eingebunden sind.

51 Ich empfehle der Landesregierung, im Rahmen ihrer Fachaufsicht den datenschutzrechtlichen Vorgaben des § 21 LKHG M-V Beachtung zu schenken und die Krankenhäuser bei der Umsetzung der Vorgaben zu unterstützen, indem beispielsweise Maßnahmen zur Datensicherheit wie Investitionen behandelt werden.

3 Biographiebogen in Pflegeheimen

In Pflegeheimen werden häufig Biographiefragebogen genutzt, welche die Heimbewohner oder ihre Angehörigen bei der Aufnahme ausfüllen sollen. Darin wird teilweise nach sehr intimen Erlebnissen und Lebensgestaltungen gefragt, beispielsweise nach der ersten Liebe. Diese Daten seien ein wichtiges Hilfsmittel, um die Bewohner umfassend betreuen und mit ihnen über wichtige Themen ihres Lebens sprechen zu können. Der Liga-Fachausschuss Altenhilfe hatte mich eingeladen, um die damit zusammenhängenden datenschutzrechtlichen Fragen zu diskutieren.

Biographische Angaben sind für eine individuell zu gestaltende Pflege und Betreuung von Heimbewohnern sicher hilfreich. Eine gesetzliche Grundlage für die Datenerhebung existiert jedoch nicht, so dass diese Angaben nur auf der Grundlage der Freiwilligkeit, also mit dem Einverständnis der betroffenen Person, erhoben werden dürfen. Freiwilligkeit bedeutet, dass die betroffene Person darüber sowie über den Zweck der Datenerhebung, über die Art und den Umfang der Verarbeitung sowie über ihre weiteren Rechte aufzuklären ist. Außerdem ist sie darauf hinzuweisen, dass sie die Einwilligung jederzeit widerrufen kann. In diesem Fall sind bestimmte Daten oder das gesamte Biographieblatt zu löschen. Ein formalistisches Herangehen an diese Datenerhebung nach dem Motto, der Standardfragebogen muss ausführlich beantwortet werden, ist aus datenschutzrechtlicher Sicht abzulehnen.

Dies habe ich auch dem Sozialministerium unseres Landes sowie dem Medizinischen Dienst der Krankenversicherung, der bei Qualitätskontrollen die individuelle Betreuung der Heimbewohner prüft, mitgeteilt und empfohlen, die Heimbewohner und ihre Angehörigen ausführlich über die Datenerhebung und deren Freiwilligkeit aufzuklären. Ich habe auch vorgeschla-

gen, lediglich Fragenkomplexe vorzugeben, bei denen es freigestellt ist, wie umfangreich sie beantwortet werden.

Beide Stellen haben meine datenschutzrechtlichen Bedenken geteilt. Das Sozialministerium hat meine Stellungnahme auch an die Einrichtungsträger weitergeleitet und sie aufgefordert, meine Hinweise zu beachten. Der Medizinische Dienst der Krankenversicherung hat in Abstimmung mit dem Sozialministerium auch die Vereinigung kommunaler Pflegeeinrichtungen Mecklenburg-Vorpommern darüber informiert. Der Liga-Fachausschuss Altenhilfe hat ein Informationsblatt erarbeitet, das Auszüge der von den Alten- und Pflegeeinrichtungen zu beachtenden datenschutzrechtlichen Bestimmungen enthält.

4 Verarbeitung von Sozialdaten in Vietnam?

Ein Kollege aus einem anderen Bundesland unterrichtete mich darüber, dass ein Auftragnehmer, der im Rahmen einer Datenverarbeitung im Auftrag tätig ist, möglicherweise rechtswidrig Sozialdaten in Vietnam verarbeiten ließ. Es handelte sich dabei um Daten von Versicherten der gesetzlichen Krankenversicherung, die sich in ein Disease-Management-Programm (DMP) eingeschrieben haben (siehe Fünfter Tätigkeitsbericht, Punkt 3.11.7). Die Daten sollen zur Dokumentation der Behandlung und zu Qualitätssicherungszwecken verarbeitet werden.

Wesentliche Voraussetzungen für diese Datenverarbeitungen sind in §§ 137f, 137g Sozialgesetzbuch Fünftes Buch (SGB V) und der Risikostruktur-Ausgleichsverordnung geregelt. Danach werden Daten über die Behandlung von Versicherten, welche sich freiwillig in ein DMP eingeschrieben haben, an eine Datenstelle übermittelt, die auf Landesebene von den gesetzlichen Krankenkassen und der Kassenärztlichen Vereinigung betrieben wird. Die Datenstelle verarbeitet die Daten jedoch nicht selbst, sondern hat zu diesem Zweck einen Vertrag zur Datenverarbeitung im Auftrag mit einem Dienstleistungsunternehmen geschlossen. Dieser Auftragnehmer, der neben Mecklenburg-Vorpommern auch für andere Bundesländer tätig war, soll die Daten rechtswidrig an eine Firma in Vietnam übermittelt haben, um sie dort verarbeiten zu lassen. Die Medien haben darüber umfassend berichtet.

Im Ergebnis einer Prüfung des von den gesetzlichen Krankenkassen beauftragten Technischen Überwachungsvereins konnte nicht zweifelsfrei nachgewiesen werden, ob und welche DMP-Daten in Vietnam verarbeitet worden sind. Die Beteiligten sind aber davon ausgegangen, dass dort in unzulässiger Weise eine Verarbeitung von Sozialdaten stattfand.

Derartige Fehler beruhen auf menschlichem Versagen. Sie lassen sich daher nicht vollständig ausschließen. Ihre Auswirkungen könnten allerdings begrenzt werden, wenn die Vorgaben zur Datenvermeidung und Datensparsamkeit umgesetzt würden. Ich habe mich daher an die Sozialministerin unseres Landes, den Vorsitzenden der Kassenärztlichen Vereinigung, die Vorstandsvorsitzenden der landesunmittelbaren Krankenkassen und den Bundesbeauftragten für den Datenschutz gewandt und sie gebeten, sich dafür einzusetzen, dass die Vorgaben des Sozialgesetzbuches zur Datenvermeidung und Datensparsamkeit bei der Verarbeitung der DMP-Daten umgesetzt und nur die Daten gespeichert werden, die auch für die regelmäßige Evaluierung der Programme erforderlich sind.

Datenvermeidung und Datensparsamkeit

Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig Sozialdaten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§ 78b Sozialgesetzbuch Zehntes Buch (SGB X)

Ich habe mich bei dieser Bitte davon leiten lassen, dass die AOK M-V beispielsweise in der Vergangenheit bereits ein Programm zur Betreuung von Zuckerkranken durchgeführt hat, bei dem bedeutend weniger Daten verarbeitet worden sind.

Der Bundesbeauftragte für den Datenschutz hat mir hierzu mitgeteilt, dass er meine Initiative gern aufgreift und bei seinen Beteiligungen an künftigen Änderungen der Risikostruktur-Ausgleichsverordnung den Umfang der zu dokumentierenden und zu übermittelnden Daten weiter kritisch hinterfragen wird, um ihn auf das unbedingt notwendige Maß zu begrenzen.

52 Ich empfehle der Landesregierung, sich in der Gesundheitsministerkonferenz dafür einsetzen, dass der Umfang der zu verarbeitenden Daten im Rahmen von Disease-Management-Programmen kritisch auf die Erforderlichkeit hin untersucht wird.

5 Datenaustausch zwischen dem Disease-Management-Programm „Brustkrebs“ und den Krebsregistern

Bereits im Fünften Tätigkeitsbericht hatte ich über Disease-Management-Programme (DMP) (siehe Punkt Fünfter Tätigkeitsbericht 3.11.7) sowie über die Speicherung von Patientendaten in klinischen Krebsregistern (siehe Punkt Fünfter Tätigkeitsbericht 3.12.5) informiert.

Um die Versorgung von Krebskranken zu verbessern, befasste sich die 77. Konferenz der für das Gesundheitswesen zuständigen Ministerinnen und Minister, Senatorinnen und Senatoren der Länder mit dem Ausbau der Krebsregister. Sie forderte das Bundesministerium für Gesundheit und Soziale Sicherung auf, für eine sach- und fachgerechte ressourcensparende Einbindung der Krebsregister in das DMP Brustkrebs Sorge zu tragen. Außerdem sollen durch eine enge Zusammenarbeit zwischen klinischen und epidemiologischen Registern Doppelmeldungen von Krebserkrankungen vermieden und Kosten gespart werden.

In Mecklenburg-Vorpommern sind bereits seit einigen Jahren mehrere klinische Krebsregister etabliert. Vor diesem Hintergrund habe ich die Frage des Datenaustausches zwischen den Registern und den Stellen, die DMP-Daten verarbeiten, mit unserem Sozialministerium diskutiert. Aus meiner Sicht ist eine rechtliche Regelung des Datenaustausches problematisch. Dies vor allem deshalb, weil die wesentliche Grundlage für die Teilnahme an einem DMP und für die Datenspeicherung in einem klinischen Krebsregister jeweils die informierte Einwilligung der betroffenen Person ist. Der Datenaustausch zwischen diesen beiden Stellen kann daher

nach meiner Auffassung auch nur stattfinden, wenn die betroffene Person auch hierin eingewilligt hat.

53 Ich empfehle der Landesregeierung, sofern sie weiterhin die Notwendigkeit sieht, zwischen dem Disease-Management-Programm „Brustkrebs“ und der Krebsregister Daten auszutauschen, Verfahrensregelungen zu erlassen, die das Recht der Frauen auf informationelle Selbstbestimmung respektieren und dennoch dazu beitragen, dass Doppelmeldungen vermieden werden.

6 Einsicht in Krankenunterlagen

Viele Patienten haben sich an mich gewandt, wenn ihnen das Recht verwehrt wurde, ihre Krankenakte einzusehen. Zum überwiegenden Teil betrafen diese Anfragen Gesundheitseinrichtungen oder Ärzte, für die nicht das Auskunfts- und Einsichtsrecht des Landeskrankenhausgesetzes (§ 18 LKHG M-V) oder des Psychischkrankengesetzes (§ 44 Abs. 2 PsychKG M-V) anwendbar war. Neben diesen spezialgesetzlich geregelten stehen den Patienten jedoch die allgemeinen Auskunfts- und Einsichtsrechte nach dem Landesdatenschutzgesetz (§ 24 DSG M-V; bei öffentlichen Stellen des Landes) oder nach dem Bundesdatenschutzgesetz (§§ 6, 34 BDSG; bei nichtöffentlichen Stellen) zur Seite. Außerdem ist ihnen Einsicht zu gewähren nach § 10 Abs. 2 Berufsordnung für die Ärztinnen und Ärzte Mecklenburg-Vorpommern (BOÄ M-V).

§ 10 Abs. 2 BOÄ M-V

Der Arzt hat dem Patienten auf dessen Verlangen grundsätzlich in die ihn betreffenden Krankenunterlagen Einsicht zu gewähren. Auf Verlangen sind dem Patienten Kopien der Unterlagen gegen Erstattung der Kosten herauszugeben.

Auf diese Rechte der Patienten habe ich die Ärzte hingewiesen. In einigen Fällen, insbesondere auch bei psychischen Krankheiten, haben sie geltend gemacht, dass die Patienten kein Recht hätten, die vom Arzt dokumentierten subjektiven Daten, also Bewertungen, einzusehen. Das datenschutzrechtliche Einsichtsrecht unterscheidet allerdings nicht zwischen objektiven und subjektiven Daten, sondern gesteht den betroffenen Personen zu, ihre Daten einzusehen. Ein Versagungsgrund nach dem Landesdatenschutzgesetz kann aber beispielsweise dann vorliegen, wenn die Erfüllung der Aufgabe durch die Auskunftserteilung gefährdet würde. Dies wäre der Fall, wenn die ärztliche Aufgabe – Heilung von einer Krankheit – durch die Akteneinsicht gefährdet würde. Sofern einem Patienten unter diesen Umständen keine Einsicht gewährt werden kann, sollte der Arzt ihm jedoch soweit als möglich Auskunft geben. Diese allgemeine datenschutzrechtliche Regelung findet sich in entsprechender Ausformung daher auch im PsychKG.

§ 44 Abs. 2 Satz 3 PsychKG M-V

Ist bei einer vollständigen Auskunft oder Einsichtnahme mit schwerwiegenden gesundheitlichen Nachteilen bei dem Betroffenen zu rechnen, so soll der behandelnde Arzt die entsprechenden Inhalte unter Berücksichtigung des Gesundheitszustandes an den Betroffenen vermitteln.

Auf dieser Grundlage wurde den Patienten dann die begehrte Einsicht oder Auskunft gewährt.

54 Ich empfehle der Landesregierung, die Ärzte in der Wahrnehmung ihrer Auskunftspflichten und sonstigen datenschutzrechtlichen Verpflichtungen durch Schulungs- oder Informationsmaßnahmen zu unterstützen und Maßnahmen zur Stärkung der Patientenrechte zu ergreifen.

7 Einrichtung einer Datenbank über gefälschte Rezepte

Ein Datenschutzbeauftragter eines anderen Bundeslandes informierte mich, dass die Apothekerkammern mehrerer Länder planen, eine Datenbank über gefälschte Rezepte einzurichten. Nach seiner Information wollte sich daran auch die Apothekerkammer Mecklenburg-Vorpommern beteiligen. Die Kammer bestätigte dies auf meine Nachfrage und nannte als Grund, dass die Rezeptfälschungen zugenommen hätten und die Apotheker bei Unstimmigkeiten in der ärztlichen Verschreibung häufig nicht den verordnenden Arzt befragen könnten, wenn die gefälschten Rezepte außerhalb der Sprechstunden im Nacht-, Sonntags- oder Feiertagsdienst der Apotheken eingelöst würden. Die Datenbank soll daher helfen, Arzneimittelmissbrauch entgegenzuwirken. Bei einem Fälschungsverdacht sollten das Präparat und dessen Menge, die Daten des Praxisstempels des Arztes, Ort und Datum der Verdachtsfeststellung sowie der auf dem Rezept vermerkte Patientenname und das Geburtsdatum erfasst und gespeichert werden. Personen, die solche Rezepte einlösen, verwenden in der Regel nicht ihre richtigen, sondern irreale Daten. Die gespeicherten Daten sollten dann von allen anderen Apothekern der beteiligten Kammern eingesehen werden können, um die Einlösung gefälschter Rezepte zu verhindern.

Der Apothekerkammer habe ich mitgeteilt, dass nur die Daten natürlicher Personen datenschutzrechtlichen Bestimmungen unterliegen. Die Daten des Arztstempels sind in der Regel richtig und betreffen somit eine natürliche Person. Sie dürfen deshalb nur verarbeitet werden, wenn eine Rechtsvorschrift dies zulässt oder der Betroffene eingewilligt hat. Eine Rechtsvorschrift, nach der die Daten des Arztes zu diesem Zweck verarbeitet werden dürfen, existiert nicht. Folglich ist die Verarbeitung dieser Daten nur zulässig, wenn der Betroffene eingewilligt hat.

Daten irrealer Personen unterliegen keinen datenschutzrechtlichen Bestimmungen. Es sollte jedoch berücksichtigt werden, dass in der Praxis nicht immer ohne weiteres festzustellen ist, ob die Verordnung auf eine natürliche oder auf eine irreale Person ausgestellt ist. Außerdem kann der Fall eintreten, dass die Daten der irrealen Person mit denen einer natürlichen Person identisch sind. Eine natürliche Person darf dann keinen Nachteil daraus erleiden, wenn sie später ein Rezept einlösen möchte und zufällig als irreale Person gespeichert ist.

Schließlich habe ich zu bedenken gegeben, dass mit der Einführung der elektronischen Gesundheitskarte und des dann darauf gespeicherten elektronischen Rezeptes die Fälschungen zunächst eingedämmt werden können und es daher zu überlegen ist, ob sich der Aufbau der Datenbank lohnt.

Die Apothekerkammer hat bisher die Datenbank noch nicht eingerichtet. Sie hat zugesichert, mich über ihre weiteren Schritte zu informieren, und will sich datenschutzrechtlich beraten lassen, wenn sie weiter daran arbeitet.

8 Gesetzesänderung zur Gewährleistung von Vorsorgeuntersuchungen

Seit einiger Zeit wird in Deutschland über das Mammographie-Screening diskutiert. Hierbei handelt es sich um Brustkrebsvorsorgeuntersuchungen für Frauen. Das Verfahren ist im Wesentlichen in den Krebsfrüherkennungs-Richtlinien vom 15. Dezember 2003 des Bundesausschusses der Ärzte und Krankenkassen geregelt. Danach sollen Frauen ab einem Alter von 50 Jahren bis zum Ende des 70. Lebensjahres in regelmäßigen Zeitabständen zur Mammographie eingeladen werden. Sie können auf freiwilliger Basis an dieser Vorsorgeuntersuchung teilnehmen. Das Verfahren selbst muss hohe Qualitätsansprüche erfüllen. So soll beispielsweise anhand des Röntgenbildes der Befund von zwei hochqualifizierten Ärzten unabhängig voneinander erstellt werden.

Beim Mammographie-Screening müssen zwangsläufig personenbezogene und pseudonymisierte Daten der Frauen verarbeitet werden. Das Sozialministerium unseres Landes hat mich deshalb schon frühzeitig in das Projekt einbezogen, um datenschutzrechtliche Standards von Beginn an zu berücksichtigen. Ein Schwerpunkt war dabei, wie die Daten der Frauen gewonnen werden können, die in der entsprechenden Altersgruppe sind, um an dem Screening teilzunehmen. Der Datenbestand dafür ist zweifelsohne bei den Meldeämtern vorhanden. Dort ist es relativ einfach möglich, die Adressen aller Frauen im Alter von 50 bis 70 Jahren herauszufinden, um sie zur Untersuchung einladen zu können.

Das Melderecht lässt eine solche Auskunft bzw. Übermittlung zu, wenn sie im öffentlichen Interesse liegt. Es existierte jedoch keine Rechtsvorschrift, nach der Daten der Meldeämter für Vorsorgeuntersuchungen genutzt werden konnten. Mit unserem Sozialministerium habe ich deshalb eine entsprechende Änderung des Gesetzes über den Öffentlichen Gesundheitsdienst (ÖGDG M-V) diskutiert, die der Gesetzgeber nun auch in Kraft gesetzt hat (§ 15a).

> **§ 15a Maßnahmen der Prävention, Abs. 1**
>
> Öffentlich-rechtliche Stellen, die im Rahmen der Durchführung von Maßnahmen der Prävention zur Früherkennung von Erkrankungen eine Genehmigung des Sozialministeriums erhalten haben, sind befugt, Familienname, Vorname, frühere Namen, Tag und Ort der Geburt und Anschrift der von der einzelnen Maßnahme der Prävention betroffenen Personen von den Meldebehörden zu erheben und zu verarbeiten, soweit das zur Durchführung der jeweiligen Maßnahme erforderlich ist.

Damit wird es möglich sein, dass die Meldeämter die Daten aller Frauen im Alter von 50 bis 70 Jahren an eine Stelle übermitteln, die diese Vorsorgeuntersuchung organisiert. Diese einladende Stelle wird voraussichtlich der Medizinische Dienst der Krankenversicherung sein. Dabei bleibt es jeder Frau selbst überlassen, ob sie an der Untersuchung teilnimmt. Sofern eine Frau keine Einladung zur Untersuchung mehr wünscht, muss sie dies der einladenden Stelle mitteilen. Frauen, die am Mammographie-Screening teilnehmen, werden umfassend über die damit zusammenhängende Datenverarbeitung informiert.

Das Sozialministerium und alle Beteiligten sind bestrebt, mit dem Mammographie-Screening möglichst bald zu beginnen. Ich werde das Verfahren weiter datenschutzrechtlich begleiten.

9 Neue Strukturen bei Sozialleistungsträgern

Bei Sozialleistungsträgern ist ein Trend zur Konzentration zu beobachten. So hat sich bereits zum 1. Oktober 2005 die Landesversicherungsanstalt Mecklenburg-Vorpommern mit den Landesversicherungsanstalten Hamburg und Schleswig-Holstein zur Deutschen Rentenversicherung Nord zusammengeschlossen. Damit wurde auch die bisherige Trennung in Arbeiter- und Angestelltenversicherung aufgehoben. Demnächst werden die Innungskrankenkassen Mecklenburg-Vorpommern und Schleswig-Holstein fusionieren. Es ist abzusehen, dass dieser Trend weitergeht und andere Krankenkassen sich ebenfalls zusammenschließen werden.

Diese Entwicklung ist auch von datenschutzrechtlicher Bedeutung, weil mit solchen Zusammenschlüssen die Datenverarbeitung neu strukturiert wird. Ebenso ändern sich die Kontrollzuständigkeiten. Die datenschutzrechtliche Kontrolle wird bei dem Landesbeauftragten für den Datenschutz liegen, in dessen Bereich die Datenverarbeitung stattfindet. Sofern allerdings der Bund an solch einer neuen Stelle beteiligt ist, nimmt der Bundesbeauftragte für den Datenschutz die Kontrolle wahr (§ 81 Abs. 3 Sozialgesetzbuch Zehntes Buch – SGB X).

Versicherte aus Mecklenburg-Vorpommern, die von solchen Zusammenschlüssen betroffen sind, können sich bei Fragen nach wie vor gern an mich wenden. Ich werde ihre Anfragen beantworten oder sie an die zuständige Kontrollbehörde weiterleiten.

10 Beurteilung der Dienstfähigkeit

Ein Angestellter einer gesetzlichen Krankenkasse befürchtete, dass eine Begutachtung über seine Dienstfähigkeit, die der Medizinische Dienst der Krankenversicherung (MDK) im Auftrag seines Arbeitgebers durchgeführt hatte, nicht den rechtlichen Normen entsprach.

Ich habe die Krankenkasse gebeten, mir mitzuteilen, auf welcher rechtlichen Grundlage die Begutachtung durchgeführt wurde und wie der entsprechende Auftrag dazu lautete. Die Kasse hatte Zweifel an der Dienstunfähigkeit des Betroffenen. Ihre Dienstordnung sieht in diesem Fall vor, dass die entsprechenden Vorschriften des Landesbeamtengesetzes (LBG M-V) anzuwenden sind. Nach dem Landesbeamtengesetz ist ein Beamter verpflichtet, sich nach Weisung des Dienstvorgesetzten ärztlich untersuchen zu lassen, wenn Zweifel an seiner Dienstunfähigkeit bestehen (§ 45 Abs. 1 Satz 3 LBG M-V). Beamte müssen für eine solche Begutachtung in der Regel den Amtsarzt aufsuchen.

Die Krankenkasse hatte jedoch den MDK gebeten, die Dienstfähigkeit zu beurteilen. Dies war in der Dienstordnung so nicht geregelt. Deshalb habe ich empfohlen, dies dort ausdrücklich festzulegen, wenn auch künftig der MDK mit solchen Begutachtungen betraut werden soll. Aus datenschutzrechtlicher Sicht muss normenklar geregelt sein, welche Stelle die hierfür erforderlichen Daten rechtmäßig verarbeiten darf. Darüber hinaus habe ich angeregt, in der Dienstordnung zu normieren, welche Daten das Gutachten regelmäßig enthalten muss, damit die Krankenkasse eine sachgerechte und medizinisch gesicherte Entscheidung über die

Dienstfähigkeit oder die Versetzung in den Ruhestand treffen kann. Üblicherweise enthalten solche Gutachten keine Anamnesedaten und auch keine Diagnosen, sondern die Aussage, dass die betroffene Person vollständig oder eingeschränkt dienstfähig beziehungsweise zeitweise oder dauerhaft dienstunfähig ist. Bei entsprechenden Einschränkungen der Dienstfähigkeit oder bei zeitweiser Dienstunfähigkeit kann ein Gutachter dazu Näheres ausführen, damit der Dienstherr bzw. ein öffentlicher Arbeitgeber die notwendigen Maßnahmen treffen kann.

11 Erforschung einer Herzkrankheit

Das Institut für Community Medicine der Ernst-Moritz-Arndt-Universität Greifswald (siehe auch Zweiter Tätigkeitsbericht, Punkt 2.14.5 Forschungsprojekt Regionale Basisstudie) stellte mir das Projekt „Inflammatorische Kardiomyopathie – Molekulare Pathogenese und Therapie“ zur datenschutzrechtlichen Bewertung vor. Für die freiwillige Teilnahme an diesem Vorhaben sollen möglichst viele an der entzündlichen Herzmuskelerkrankung leidende und in Greifswald sowie an Kliniken in Berlin und in Baden-Württemberg behandelte Patienten gewonnen werden. Greifswald war dabei vor allem deshalb als Standort ausgewählt worden, weil auch bevölkerungsbezogene medizinische Vergleichsdaten genutzt werden sollten. Diese Daten wurden insbesondere durch die oben erwähnte Regionale Basisstudie gewonnen.

Den Forschern habe ich insbesondere empfohlen, die Information über die Datenverarbeitung für die potentiellen Teilnehmer sowie die Einwilligungserklärung klarer zu formulieren. So ist den Patienten unter anderem zu erklären, dass ihnen keine Nachteile bei der Behandlung ihrer Krankheit entstehen, wenn sie an dem Forschungsvorhaben nicht teilnehmen möchten. Darüber hinaus sind sie umfassend über die Verarbeitung ihrer Daten sowie über ihr Recht aufzuklären, die erteilte Einwilligung jederzeit ohne Begründung zu widerrufen.

Die Nutzung anonymisierter Daten war wegen der erforderlichen Langzeitbeobachtung des Therapieverlaufs nicht möglich. Deshalb hatten sich die Forscher entschlossen, pseudonymisierte Daten zu verwenden. Hier war sicherzustellen, dass Dritte aus den Daten keine Person bestimmen und nur zugriffsberechtigte Personen die Daten verarbeiten können. Schließlich muss auch gewährleistet sein, dass Behandlungs- und Forschungsdaten voneinander getrennt verarbeitet werden. Diese und weitere Verbesserungen wurden in das mir vorgelegte Datenschutz- und Datensicherheitskonzept eingearbeitet.

Den Datenschutzbeauftragten der Länder Berlin und Baden-Württemberg habe ich wegen der dort beteiligten Kliniken ebenfalls die Unterlagen zur Verfügung gestellt. Ihre Hinweise und Empfehlungen haben die Forscher ebenso berücksichtigt. Gegen die Durchführung des Projektes gab es keine weiteren datenschutzrechtlichen Einwände.

An diesem Beispiel zeigt sich aber auch die Aktualität der Forderung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder nach der Einführung eines Forschungsgeheimnisses für medizinische Daten (Anlage 6).

55 Ich empfehle der Landesregierung, mich bei der Planung von Forschungsprogrammen unter Einbeziehung von Patientenakten frühzeitig zu beteiligen bzw. darauf hinzuwirken und die Initiative der 67. Konferenz der Datenschutzbeauftragten zur Einführung eines Forschungsgeheimnisses aufzugreifen.

12 Auskunft aus Patientenakten von Verstorbenen

Ein Journalist beabsichtigte, über eine Bürgerin zu berichten, die vom Staatssicherheitsdienst der ehemaligen DDR verfolgt worden war und sich deswegen damals in psychiatrischer Behandlung befand. Sie ist vor einigen Jahren verstorben. Der Journalist hatte für seine Reportage bereits die Staatssicherheitsakte einsehen können und wollte nun auch die Patientenakte nutzen, um die psychische Beeinflussung der Bürgerin durch die Staatssicherheit darzustellen. Die Patientenakte wurde im Gesundheitsamt aufbewahrt (§ 25 Abs. 4 Gesetz über den Öffentlichen Gesundheitsdienst Mecklenburg-Vorpommern). Der Journalist bat mich um eine Stellungnahme, ob er die Akte einsehen könne.

Bei Daten aus Patientenakten verstorbener Personen handelt es sich nicht um Daten einer natürlichen Person (§ 3 Abs. 1 Landesdatenschutzgesetz), also nicht um personenbezogene Daten. Daten toter Personen werden nicht von den datenschutzrechtlichen Regelungen umfasst, wenngleich die allgemeinen Persönlichkeitsrechte auch über den Tod hinaus fortwirken. Die Einsichtnahme Dritter in Patientenunterlagen ist im Lichte der ärztlichen Schweigepflicht und der Strafvorschrift des § 203 Abs.1 Nr. 1 Strafgesetzbuch (StGB) zu sehen. Insbesondere die Pflicht zur Verschwiegenheit über die persönlichen und sachlichen Verhältnisse von Patienten besteht über deren Tod hinaus uneingeschränkt fort (§ 203 Abs. 4 StGB). Daten von Patienten dürfen nur aufgrund einer Rechtsvorschrift oder durch eine von der betroffenen Person abgegebene Erklärung zur Entbindung des behandelnden Arztes von der Schweigepflicht straffrei offenbart werden. Beides lag nicht vor.

Ein behandelnder Arzt ist nicht an seine Pflicht zur Verschwiegenheit gebunden, wenn nach seiner Einschätzung der mutmaßliche Wille des Patienten für eine Offenbarung von Daten spricht. Es liegt dann in der Verantwortung des Arztes zu entscheiden, in welchem Umfang er Auskunft gibt oder Einsicht gewährt.

In diesem Fall war es jedoch so, dass nicht der behandelnde Arzt, sondern das Gesundheitsamt eine Entscheidung über die Einsicht in die Patientenakte treffen sollte. Die Mitarbeiter des Gesundheitsamtes waren aber gar nicht in der Lage, sich dabei vom mutmaßlichen Willen der Patientin leiten zu lassen, weil sie ihn nicht kennen können, denn sie haben sie nicht behandelt. Außerdem würden bei einer Einsicht in die vollständige Patientenakte alle Behandlungsdetails offenbart, also auch höchstpersönliche, die den Hintergrund der psychischen Beeinflussung durch die Staatssicherheit nicht erhellen.

Dem Journalisten habe ich deshalb empfohlen, dass er sich wegen der Auskünfte an die behandelnden Ärzte wendet.

56 Ich empfehle der Landesregierung, gegenüber den Gesundheitsämtern klarzustellen, dass aus den bei ihnen vorhandenen Patientenakten Auskünfte an Dritte nur mit einer Schweigepflichtentbindungserklärung des jeweiligen Patienten zulässig sind, aus der Umfang und Tragweite hervorgehen müssen.

13 Vergabe neuer Krankenversichertennummern

Das im Jahr 2003 beschlossene Gesetz zur Modernisierung der gesetzlichen Krankenversicherung hat die Verarbeitung von Versichertendaten wesentlich verändert. So sollen jetzt auch

arzt- und versichertenbezogene Zufälligkeitsprüfungen und gezielte Prüfungen bei der Verordnung von Arzneimitteln ermöglicht werden. Darüber hinaus sollen Versichertendaten pseudonymisiert werden, um beim Risikostrukturausgleich, den die Krankenkassen untereinander durchführen, einen Krankheitsfaktor berücksichtigen zu können. Zu diesem Zweck ist es notwendig, eine Krankenversichertennummer zu bilden, die wie die Rentenversicherungsnummer lebenslang unveränderlich bleibt. Bisher hatte jede Krankenkasse eine eigene Nummer für jeden ihrer Versicherten. Bei einem Wechsel der Krankenkasse wurde folglich eine neue Krankenversichertennummer vergeben. Mit möglicherweise häufigen Kassenwechseln und damit ständig wechselnden Nummern wären aber die oben genannten Ziele nicht zu erreichen.

Der Gesetzgeber hat daraufhin mit dem Gesetz zur Organisationsstruktur der Telematik im Gesundheitswesen festgelegt, dass die neue Krankenversichertennummer mit Hilfe der Rentenversicherungsnummer von einer neu einzurichtenden, unabhängigen Vertrauensstelle zu bilden ist. Diese Stelle soll dabei insbesondere unabhängig von den Krankenkassen und deren Verbänden tätig sein. Es ist vorgesehen, dass die Krankenkassen die Rentenversichertennummer und ein Aktenzeichen an die Vertrauensstelle senden. Mit Hilfe einer Hash-Funktion (Verschlüsselung) wird aus der Rentenversicherungsnummer eine Krankenversichertenhilfsnummer berechnet. Aus dieser Nummer wird nach weiteren Kriterien die Krankenversichertennummer bestimmt. Dieses Verfahren darf nur innerhalb der Vertrauensstelle erfolgen. So soll verhindert werden, dass Dritte aus einer bekannten Rentenversicherungsnummer die neue Krankenversichertennummer ermitteln können.

Für krankenversicherte Personen, die noch keine Rentenversicherungsnummer haben, müsste sie beantragt werden. Dazu wären dann Daten wie Geburtsname, Geburtsort, Geburtsland sowie Staatsangehörigkeit des Versicherten erforderlich. Da die Kassen über diese Daten bisher nicht verfügen, wurde in einigen Bundesländern erwogen, sie bei den jeweiligen Einwohnermeldeämtern zu erheben.

Ich habe bei den beiden landesunmittelbaren gesetzlichen Krankenkassen in Mecklenburg-Vorpommern nachgefragt, ob sie die fehlenden Daten bei den Einwohnermeldeämtern erheben wollen. Sie teilten mir mit, dass die meisten Versicherten in Mecklenburg-Vorpommern eine Rentenversichertennummer haben. Versicherte ohne Rentenversichertennummer sind überwiegend im Rahmen der Familienversicherung mitversicherte Kinder. Es wäre daher nur für relativ wenige Versicherte notwendig, eine Rentenversichertennummer zu beantragen. Deshalb würden diese Versicherten angeschrieben und um die erforderlichen Daten gebeten. Nur, wenn die Versicherten auf dieses Anschreiben nicht reagieren sollten, ist vorgesehen, die erforderlichen Daten bei den Einwohnermeldeämtern in Mecklenburg-Vorpommern zu erheben. Die Vergabe neuer Krankenversichertennummern wird nach und nach erfolgen und sich über einen längeren Zeitraum hinziehen.

Datenschutzrechtliche Einwände bestehen gegen dieses Vorhaben der Krankenkassen in Mecklenburg-Vorpommern nicht. Es ist zu begrüßen, dass in einem ersten Schritt der Ersterhebungsgrundsatz beim Betroffenen gewahrt wird.

14 Krankentransport

Datenschutzrechtliche Unsicherheiten gab es bei der Umsetzung der Richtlinie über die Verordnung von Krankenfahrten, Krankentransportleistungen und Rettungsfahrten (Krankentransport-Richtlinie vom 22. Januar 2004) des Gemeinsamen Bundesausschusses der Spitzenverbände der Krankenkassen und der Kassenärztlichen Bundesvereinigung. Ärzte sprachen mich an und vertraten die Auffassung, dass hier ein Eingriff in das Recht der Patienten auf Schutz ihrer Daten vorliegen würde.

Mit der Umsetzung des Gesundheitsmodernisierungsgesetzes wurden auch die Voraussetzungen und das Verfahren zur Übernahme von Fahrkosten und Krankentransporten in § 60 Sozialgesetzbuch Fünftes Buch (SGB V) neu geregelt. Danach übernimmt die Krankenkasse diese Kosten nur noch, wenn der Transport aus zwingenden medizinischen Gründen notwendig ist. Die zuständige Krankenkasse muss ihn deshalb vorher genehmigen. Deswegen wurde die Krankentransportrichtlinie und damit auch das Verordnungsformular geändert. Es war vorgesehen, dass der verordnende Arzt auf dem Krankentransportschein die Diagnose der zu transportierenden Person als ICD Code (International Classification of Diseases and Related Health Problems) anzugeben hat. Damit können diese medizinischen Daten von den Leistungserbringern, die nicht der ärztlichen Schweigepflicht unterliegen und die diese Daten zur Erfüllung ihrer Aufgabe nicht benötigen, beispielsweise Taxifahrer, zur Kenntnis genommen werden. Der ICD-Code ist kein Schutz gegen die Offenbarung der Diagnose, da der Schlüssel allgemein zugänglich ist.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher bei den Spitzenverbänden der Krankenkassen und der Kassenärztlichen Bundesvereinigung eine datenschutzgerechte Lösung angemahnt. Bis zur Neugestaltung des Krankentransportscheines wurde eine Übergangslösung vereinbart. Danach sind keine Diagnosen anzugeben, wenn die Fahrt mit einem Taxi/Mietwagen erfolgen soll.

Ein neues, mit dem Bundesbeauftragten für den Datenschutz abgestimmtes Formular, das zum 1. Januar 2005 zugesagt worden war, wurde bis heute nicht herausgegeben.

X Umweltausschuss / Umweltministerium

1 Umweltinformationsgesetz

Am 14. Februar 2005 trat das Gesetz zur Neugestaltung des Umweltinformationsgesetzes und zur Änderung der Rechtsgrundlagen zum Emissionshandel in Kraft. Dieses Gesetz gilt für informationspflichtige Stellen des Bundes und für bundesunmittelbare juristische Personen des öffentlichen Rechts. Demzufolge habe ich beim Umweltministerium nachgefragt, welche Rechtsgrundlagen für die öffentlichen Stellen des Landes über den Zugang zu Umweltinformationen geschaffen werden.

Der mir zur Stellungnahme zugesandte Gesetzentwurf über den Zugang zu Umweltinformationen in Mecklenburg Vorpommern orientierte sich am neuen Umweltinformationsgesetz des Bundes. Dazu hatte bereits der Bundesbeauftragte für den Datenschutz im Rahmen seiner Beratung Stellung genommen. Seine Hinweise waren im Gesetz berücksichtigt worden. Von daher bestanden aus meiner Sicht keine Bedenken gegen den Entwurf des Landes. Das Gesetz ist vom Landtag Mecklenburg-Vorpommern noch nicht beschlossen worden.

2 Erfassung der Abwasserentsorgung in Kleingartenanlagen

Ein Kleingärtner informierte mich darüber, dass eine Forschungseinrichtung die Situation der Abwasserentsorgung in Kleingartenanlagen erfassen soll. Danach soll sie vorschlagen, in welcher Weise das Abwasser kostengünstig und umweltgerecht entsorgt werden kann. Den Auftrag dazu hat das Umweltministerium erteilt, das sich wiederum mit dem Landesverband der Gartenfreunde Mecklenburg und Vorpommern sowie dem Landwirtschaftsministerium abgestimmt hatte.

Nach Auffassung des Kleingärtners war dieses Projekt datenschutzrechtlich fragwürdig. Er kritisierte insbesondere, dass die Betroffenen nicht ausreichend über die Datenverarbeitung aufgeklärt und insbesondere nicht auf die Freiwilligkeit der Angaben hingewiesen worden sind. So war beispielsweise auch vorgesehen, dass aus ausgewählten Abwassergruben in Kleingärten Proben gezogen und analysiert werden. Wie diese für den Einzelnen möglicherweise sehr schutzwürdigen Daten weiter verarbeitet werden, war allerdings nicht erläutert worden.

Die Kritik an dem Projekt war für mich nachvollziehbar. Die Forscher legten zwar dar, dass sie keine personenbezogenen Daten verarbeiten wollen. Doch gerade in der Phase der Datenerhebung kann leicht ein Personenbezug hergestellt werden, beispielsweise über die Kleingartennummer oder auch durch Namensschilder an Lauben. Deshalb sind für dieses Projekt die datenschutzrechtlichen Vorschriften in vollem Umfang anzuwenden. Ich habe empfohlen, die Betroffenen auf die Freiwilligkeit ihrer Teilnahme an der Datenerfassung und -verarbeitung umfassend aufzuklären und sie über ihre Rechte zu informieren. Die Forschungseinrichtung hat meine Vorschläge realisiert. Es wurden Informationsblätter erarbeitet, die über den Zweck der Datenerhebung und die Verwendung der Daten informieren. Die zunächst personenbezogen erhobenen Daten werden lediglich statistisch ausgewertet, so dass nach der Zusammenstellung der Ergebnisse kein Bezug zu einer Person mehr hergestellt werden konnte. Sobald die Erhebungsbögen ausgewertet worden sind, werden sie datenschutzgerecht vernichtet.

57 Ich empfehle der Landesregierung, bei der Vergabe von Forschungsvorhaben auf die datenschutzrechtlichen Bestimmungen des § 34 Landesdatenschutzgesetz Mecklenburg Vorpommern hinzuweisen.

2 Zusammenfassung der Empfehlungen

Lfd. Nr.:	Empfehlung	Gliederungspunkt
1	Ich empfehle dem Landtag, im Rahmen einer Änderung der Geschäftsordnung des Landtages mit Beginn der nächsten Legislaturperiode das Rede- und Zutrittsrecht des Landesbeauftragten für den Datenschutz analog der Rechte der Bürgerbeauftragten zu gestalten, um so die Einbeziehung der Sachkompetenz meiner Behörde in Beratungsgegenstände der Fachausschüsse zu ermöglichen.	A.0
2	Ich empfehle daher der Landesregierung, bei einer Überarbeitung der GGO II die förmliche Beteiligung des Landesbeauftragten für den Datenschutz im Stadium des Referentenentwurfes zu Gesetzen und zu Verordnungen mit aufzunehmen.	A.0
3	Ich empfehle der Landesregierung, beim Verfahren zur Befreiung von der Rundfunkgebührenpflicht den Gesetzesvorschlag der Datenschutzbeauftragten des Bundes und der Länder zu befürworten und damit ein datenschutzgerechtes Verfahren zu unterstützen.	A.1.I
4	Ich empfehle daher dem Landtag, die Ankündigung der Landesregierung und der Koalitionsfraktionen, noch vor Ende dieser Legislaturperiode ein Informationsfreiheitsgesetz für Mecklenburg-Vorpommern zu beschließen, umgehend umzusetzen.	A.1.II.1.2
5	Ich empfehle daher der Landesregierung, auf der Grundlage der bisher geleisteten Vorarbeiten umgehend eine Verordnung nach § 5 Abs. 2 Landesdatenschutzgesetz (DSG M-V) zu erlassen.	A.1.II.1.3
6	Ich empfehle der Landesregierung, für die neuen elektronischen Verfahren im Meldewesen – insbesondere für die elektronische Melderegisterauskunft – angemessene technische und organisatorische Vorkehrungen zu treffen und bei der Novellierung des Landesmeldegesetzes zu normieren.	A.1.II.1.4
7	Ich empfehle der Landesregierung sicherzustellen, dass die erforderlichen Abschottungsmaßnahmen eingehalten werden. Neben der oben genannten technischen Abschottung sind dies vor allem • die personelle Trennung zwischen Mitarbeitern des Statistischen Amtes und denen aus anderen Abteilungen des Landesamtes für innere Verwaltung, • die bauliche Abschottung mit entsprechender Schlüsselverwaltung, • die Verpflichtung der Mitarbeiter des Statistischen Amtes auf Wahrung der statistischen Geheimhaltung auch gegenüber dem Leiter des Landesamtes für innere Verwaltung und	A.1.II.1.5

	• die Verarbeitung statistischer Einzeldaten im Auftrag nur aufgrund einer schriftlichen Verfügung des Leiters des Statistischen Amtes.	
8	Ich empfehle dem Landtag, eine Klarstellung dahingehend vorzunehmen, dass auch in diesem Bereich dem Trennungsgebot Rechnung getragen wird.	A.1.II.1.7
9	Ich empfehle der Landesregierung, Datenschutz- und IT-Sicherheitsaspekte der Landesfirewall im IT-Sicherheitsrahmenkonzept angemessen zu berücksichtigen und die hierfür erforderlichen Ressourcen zur Verfügung zu stellen, um das hohe Sicherheitsniveau auch weiterhin gewährleisten zu können.	A.1.II.1.9
10	Ich empfehle der Landesregierung, bereits bei den Planungen zur IP-Telefonie die Empfehlungen der Datenschutzbeauftragten zu berücksichtigen, um künftig auch bei der Nutzung dieser modernen Kommunikationstechnologie das Fernmeldegeheimnis wahren zu können.	A.1.II.1.10
11	Ich empfehle der Landesregierung, dem Landtag und den weiteren öffentlichen Stellen des Landes, die „Orientierungshilfe zu Datenschutzfragen bei der Präsentation öffentlicher Stellen im Internet“ zu nutzen, um bestehende oder geplante Internetportale zu prüfen (www.datenschutz-mv.de). Bei der Ausgestaltung der Internetportale sind die Prinzipien der Transparenz und der Datenvermeidung in vollem Umfang umzusetzen.	A.1.II.1.11
12	Ich empfehle der Landesregierung, bei der Planung und beim Betrieb der landeseigenen Virtuellen Poststelle die Hinweise der Broschüre „Die virtuelle Poststelle im datenschutzgerechten Einsatz“ zu berücksichtigen. Für die datenschutzgerechte Ausgestaltung dieser zentralen E-Government-Komponente sind die Handlungsempfehlungen der Kapitel 8 und 9 besonders hilfreich.	A.1.II.1.12
13	Ich empfehle der Landesregierung, gegebenenfalls zu überprüfen, ob sich an der aktuellen Sicherheitslage in Mecklenburg-Vorpommern seit dem Jahre 2000 etwas geändert hat. Ansonsten ist gegenüber den kommunalen Behörden klarzustellen, dass Videoüberwachungsanlagen auf öffentlichen Straßen und Plätzen nur bei Vorliegen der gesetzlichen Voraussetzungen zulässig sind. Bei entsprechenden Planungen sind die behördlichen Datenschutzbeauftragten frühzeitig einzubeziehen.	A.1.II.2.1
14	Ich empfehle dem Landtag, meine Vorschläge zur Sicherstellung ordnungsgemäßer Akten-/Datenübermittlung bei Aufgabenübertragungen und Verwaltungsfusionen im Gesetzgebungsverfahren zu berücksichtigen, um so bei der Verwaltungsmodernisierung die notwendige Rechtssicherheit in Datenschutzfragen zu erhalten.	A.1.II.2.2

15	Ich empfehle der Landesregierung sowie allen öffentlichen Stellen des Landes, im Rahmen der regelmäßigen Belehrungen ihre Mitarbeiter darauf hinzuweisen, dass Gesprächsteilnehmer generell vor Betätigen der Freisprechtaste beziehungsweise sonstigen Mithörens durch weitere Personen um ihr Einverständnis zu bitten sind. Diese Verfahrensweise ist verbindlich zu regeln.	A.1.II.2.3
16	Ich empfehle der Landesregierung, im Rahmen der Kommunalaufsicht verstärkt darüber zu wachen, dass verdeckte Beobachtungen von Sozialleistungsempfängern nicht durchgeführt oder angeordnet werden.	A.1.II.2.4
17	Ich empfehle der Landesregierung, im Rahmen der Kommunalaufsicht die Hinweise für die Durchführung von Hausbesuchen bei Sozialleistungsempfängern in den Landkreisen und kreisfreien Städten bekannt zu geben.	A.1.II.2.5
18	Ich empfehle der Landesregierung, die Ausführungshinweise des Finanzministeriums und die Vollzugshinweise für die Durchführung des Wohngeldgesetzes des Ministeriums für Arbeit, Bau und Landesentwicklung um eine Regelung für den Fall zu ergänzen, wie mit dem Ergebnis des Kontenabrufes verfahren werden soll, wenn sich der Anlass für einen Kontenabruf im laufenden Verwaltungsverfahren erledigt hat.	A.1.II.2.6
19	Der Landesregierung empfehle ich, bei der Novellierung der Vorschriften der Kommunalverfassung Mecklenburg-Vorpommern über die Informations- und Prüfungsrechte der Gemeinde bei Unternehmen oder Einrichtungen des privaten Rechts klarstellende Regelungen zur Zulässigkeit der Datenübermittlung an die Gemeinde- / Stadtvertreter im Rahmen ihrer Kontrollfunktion aufzunehmen.	A.1.II.2.7
20	Ich empfehle der Landesregierung, die Gemeindevertretungen darauf hinzuweisen, dass Tonbandmitschnitte zur Protokollerstellung während einer Einwohnerfragestunde nur zulässig sind, wenn die Betroffenen hierüber in geeigneter Weise aufgeklärt wurden.	A.1.II.2.8
21	Ich empfehle der Landesregierung zu prüfen, ob zum Umgang mit personenbezogenen Daten im Rahmen von Bürgerbegehren Regelungen in die Kommunalverfassung aufgenommen werden sollten, um hier mehr Rechtssicherheit zu erreichen.	A.1.II.2.9
22	Ich empfehle der Landesregierung sowie allen weiteren öffentlichen Stellen, darauf zu achten, dass bei Privatisierungen öffentlicher Unternehmen die von der Bundesbeauftragten für die Unterlagen des Staatssicherdienstes übermittelten Daten vor dem Betriebsübergang datenschutzgerecht vernichtet werden. Im Übrigen dürfen die Unterlagen nur bis Ende des Jahres 2006 für die Überprüfung von Mitarbeitern des öffentlichen Dienstes genutzt werden. Vor diesem Hintergrund ist dafür zu sorgen, dass die in den Personalakten enthaltenen Daten danach durch alle personalbearbeitenden Dienststellen gelöscht werden.	A.1.II.2.10

23	Ich empfehle der Landesregierung vor dem Hintergrund weiterer Fusionen im kommunalen Bereich, dafür Sorge zu tragen, dass die ordnungsgemäße Übergabe von Aktenbeständen sowie die Verantwortlichkeiten, die Fristen, die Archivierung beziehungsweise die Vernichtung der Unterlagen verbindlich geregelt wird.	A.1.II.2.11
24	Ich empfehle der Landesregierung, die Ausländerbehörden darauf hinzuweisen, dass das Vorliegen der Voraussetzungen für die Speicherung im Schengener Informationssystem in jedem Einzelfall genau zu prüfen und zu dokumentieren ist.	A.1.II.2.12
25	Ich empfehle der Landesregierung, die Meldebehörden auf ihre Dokumentationspflichten bei erweiterten Melderegisterauskünften hinzuweisen, deren Einhaltung im Rahmen der Fachaufsicht zu prüfen und bei einer Neugestaltung des Verfahrens die Dokumentationspflichten zu berücksichtigen.	A.1.II.2.13
26	Ich empfehle den öffentlichen Stellen des Landes, vor der Beschaffung einer Videoüberwachungsanlage den behördlichen Datenschutzbeauftragten zu beteiligen sowie die technischen Anforderungen mit Hilfe des Schutzprofils zu beschreiben. Anbieter sollten bereits im Vergabeverfahren aufgefordert werden, die Kompatibilität ihrer Anlage mit den Anforderungen des Schutzprofils möglichst durch eine Zertifizierung nachzuweisen.	A.1.II.2.17
27	Ich empfehle der Landesregierung und dem Landtag, ein Akkreditierungsverfahren bei Großveranstaltungen, die besondere Sicherheitsmaßnahmen erfordern, auf eine generelle gesetzliche Grundlage zu stellen.	A.1.II.3.1
28	Ich empfehle der Landesregierung Vorkehrungen zu treffen, damit sowohl die Staatsanwaltschaften als auch die Polizei aktuelle Ausgänge zu Ermittlungsverfahren mitteilen und die sich daran anschließende Korrektur von Eintragungen in Dateien und Verzeichnissen durchgeführt wird. Dies ist den Betroffenen auch in jedem Fall mitzuteilen.	A.1.II.3.2
29	Ich empfehle der Landesregierung, der Novellierung des Pass- und Personalausweisgesetzes im Bundesrat nur zuzustimmen, wenn gewährleistet ist, dass bei der Einführung biometrischer Ausweisdokumente • die biometrischen Merkmale ausschließlich von den für die Passkontrollen zuständigen Behörden für hoheitliche Zwecke genutzt werden können, • die in Ausweisen gespeicherten Daten mit den biometrischen Merkmalen nicht als Referenzdaten genutzt werden, um Daten aus unterschiedlichen Systemen und Kontexten zusammenzuführen, • die für die Ausstellung und das Auslesen verwendeten Geräte	A.1.II.3.3

	nach internationalen Standards von einer unabhängigen Stelle zertifiziert werden und • Verfahren festgelegt werden, die einen Datenmissbrauch beim Erfassen der Referenzdaten und im weiteren Verfahren verhindern.	
30	Ich empfehle der Landesregierung, gegenüber den Staatsanwaltschaften und den Polizeidienststellen klarzustellen, dass eine Übermittlung personenbezogener Daten an einen öffentlichen Arbeitgeber nur aufgrund einer normenklaren gesetzlichen Grundlage zulässig ist.	A.1.II.3.4
31	Ich empfehle dem Landtag und der Landesregierung, für den Übergang zu einem papierlosen Büro bei der Verfassungsschutzbehörde eine gesetzliche Grundlage zu schaffen, wie das beispielsweise beim Verfassungsschutz im Land Brandenburg praktiziert wurde.	A.1.II.3.5
32	Ich empfehle der Landesregierung, bei der Überarbeitung der Richtlinie für das DNA-Verfahren der Landespolizei Mecklenburg-Vorpommern und der Richtlinie für die Staatsanwaltschaften des Landes die datenschutzrechtlichen Aspekte zu beachten, mich hieran rechtzeitig zu beteiligen und im Übrigen eine Evaluierung der Neuregelungen vorzunehmen.	A.1.III.1
33	Ich empfehle der Landesregierung und dem Landtag, sich im Rahmen der Länderbeteiligung bei einer erneuten Bundesinitiative für eine datenschutzfreundliche Ausgestaltung der gesetzlichen Regelungen des Vollzugs der Untersuchungshaft einzusetzen, mich frühzeitig hieran zu beteiligen und im Rahmen der eigenen Zuständigkeit für eine Beachtung – auch des Rechtes auf informationelle Selbstbestimmung von Untersuchungsgefangenen – Sorge zu tragen.	A.1.III.2
34	Ich empfehle der Landesregierung, gegenüber den Staatsanwaltschaften und den Polizeidienststellen in geeigneter Weise klarzustellen, dass bei Presseanfragen zu laufenden Verfahren die Betroffenen, die hiervon noch keine Kenntnis haben, generell vorab zu unterrichten sind. Ferner rege ich an, diesen Sachverhalt auch ausdrücklich in der Allgemeinen Verwaltungsvorschrift des Landes Mecklenburg-Vorpommern für die Zusammenarbeit der Justizbehörden mit den Medien zu regeln.	A.1.III.4
35	Ich empfehle der Landesregierung, die Gerichtsvollzieher bei der Umsetzung der Verwaltungsvorschrift zum Einsatz von EDV-Technik im Gerichtsvollzieherbüro zu unterstützen. Gerichtsvollzieher, die moderne Informations- und Kommunikationstechnik im dienstlichen Umfeld nutzen möchten, sollten auch die ergänzenden Hinweise der „Orientierungshilfe zum datenschutzgerechten Anschluss an Internet und Online-Banking bei Gerichtsvollziehern“ beachten, um ein Mindestmaß an Sicherheit für die auf ihren IT-Systemen gespeicherten Daten	A.1.III.5

	zu gewährleisten.	
36	Ich empfehle der Landesregierung, die verfassungs- und datenschutzrechtlichen Aspekte bei der Vorratsdatenspeicherung in der Telekommunikation zu berücksichtigen und sich im Bundesrat gegen eine Speicherung von Daten, wie sie im Entwurf der Richtlinie der Europäischen Kommission vorgesehen ist, auszusprechen.	A.1.III.6
37	Ich empfehle der Landesregierung, mich auch weiterhin frühzeitig bei der Gestaltung der länderübergreifenden Steuerdatenverarbeitung zu beteiligen. Wenn der Staatsvertrag wie vorgesehen verabschiedet wird, verbleibt für Dataport und die Steuerverwaltungen die Aufgabe, die Vorschriften zum Steuergeheimnis technisch und organisatorisch umzusetzen. So muss das Data Center Steuern von den anderen Teilen von Dataport abgeschottet werden, und die Steuerverwaltungen der beteiligten Länder dürfen nicht auf Daten eines anderen Bundeslandes zugreifen können.	A.1.IV.1
38	Ich empfehle der Landesregierung, beim bargeldlosen Zahlungsverkehr in der Landesverwaltung auf Scoring-Verfahren beim Betrieb der Zahlungsverkehrsplattform generell zu verzichten. Darüber hinaus ist bei der weiteren Entwicklung des Verfahrens der Grundsatz der Datenvermeidung zu berücksichtigen.	A.1.IV.2
39	Ich empfehle der Landesregierung, die Daten der Mitarbeiterinnen und Mitarbeiter, die im Zuge der Strukturreform der Landesverwaltung dem Personalüberhang zugeordnet werden, nur in dem Rahmen zu nutzen, wie es für die Personalverwaltung notwendig ist. Ein unbeschränkter Zugriff auf diese Daten durch Personalstellen aller Ressorts wäre mit den datenschutzrechtlichen Bestimmungen nicht vereinbar.	A.1.IV.3
40	Ich empfehle der Landesregierung anzuordnen, dass die Finanzämter betroffene Geheimnisträger auf die Möglichkeit hinweisen, sich an den Landesbeauftragten für den Datenschutz zu wenden, wenn ihnen nachteilige steuerliche Entscheidungen drohen, sofern sie die Bekanntgabe personenbezogener Daten ihrer Mandanten/Patienten/Kunden verweigern.	A.1.IV.4
41	Ich empfehle der Landesregierung, gegenüber den Sparkassen und anderen öffentlichen Einrichtungen bei Kundenbefragungen auf die Einhaltung datenschutzrechtlicher Bestimmungen hinzuweisen und deren Einhaltung zu prüfen.	A.1.IV.6
42	Ich empfehle der Landesregierung, im Rahmen des noch immer ausstehenden Wasserverkehrs- und Hafenanlagensicherheitsgesetzes (WVHaSiG), die datenschutzrechtlich bedeutsame Zuverlässigkeitsüberprüfung, welche umfangreiche Abfragemöglichkeiten zu bestimmten Hafenmitarbeitern bei Polizei und gegebenenfalls weiteren Sicherheitsbehörden erlaubt, gesetzlich zu regeln und mich hieran frühzeitig zu beteiligen.	A.1.V.1

43	Ich empfehle der Landesregierung, im Rahmen der Tourismusförderung insbesondere Unternehmen und Kurverwaltungen für einen datenschutzgerechten Umgang mit den Daten ihrer Gäste zu sensibilisieren. Das gilt insbesondere bei der Einführung elektronischer Systeme.	A.1.V.3
44	Ich empfehle der Landesregierung und allen anderen öffentlichen Stellen in Mecklenburg-Vorpommern, bei Auskunftsbegehren aufgrund eines berechtigten oder rechtlichen Interesses genau zu prüfen, ob dem Wunsch entsprochen werden kann.	A.1.VI.1
45	Die Landesregierung und die anderen öffentlichen Stellen sollten auch bei anderen Projekten, bei denen Vorteile für betroffene Personen unabdingbar mit Datenverarbeitungen verbunden sind, umfassend darüber aufklären und eine Einwilligung nur dort vorsehen, wo die Betroffenen tatsächlich Alternativen haben.	A.1.VI.2
46	Ich empfehle der Landesregierung, Forschungsprojekte mit personenbezogenen oder aus diesen gewonnenen Daten nur zu genehmigen, wenn dazu ein datenschutzrechtliches Votum des jeweiligen behördlichen Datenschutzbeauftragten vorliegt.	A.1.VII.1
47	Ich empfehle der Landesregierung, unverzüglich das Datenschutz- und Datensicherheitskonzept für das Schulberichtssystem nachzureichen und die offenen Punkte zu klären. Künftig sollten Verfahren zur Datenverarbeitung erst in Betrieb genommen werden, wenn ein solches Konzept geprüft vorliegt.	A.1.VII.2
48	Ich empfehle der Landesregierung gegenüber den Wohngeldstellen im Land klarzustellen, dass bei der Berechnung des Wohngeldes die Höhe des Vermögens nicht erhoben werden darf.	A.1.VIII.1
49	Ich empfehle der Landesregierung, dem JobCard-Verfahrensgesetz im Bundesrat nur dann zuzustimmen, wenn die Verfassungsmäßigkeit des Verfahrens nachgewiesen, die Sicherheit der Daten garantiert und eine Kontrolle durch unabhängige Stellen gewährleistet ist.	A.1.VIII.2
50	Ich empfehle der Landesregierung, die Stellung der ARGEn in Mecklenburg-Vorpommern als eigenverantwortliche datenverarbeitende Stellen zu stärken, eine datenschutzgerechte Verarbeitung von Sozialdaten in den ARGEn zu fördern und die Kontrollkompetenz durch den Landesbeauftragten für den Datenschutz klarzustellen.	A.1.VIII.3
51	Ich empfehle der Landesregierung, im Rahmen ihrer Fachaufsicht den datenschutzrechtlichen Vorgaben des § 21 LKHG M-V Beachtung zu schenken und die Krankenhäuser bei der Umsetzung der Vorgaben zu unterstützen, indem beispielsweise Maßnahmen zur Datensicherheit, wie Investitionen, behandelt werden.	A.1.IX.2
52	Ich empfehle der Landesregierung, sich in der Gesundheitsministerkonferenz dafür einsetzen, dass der Umfang der zu verarbeitenden Daten im Rahmen von Disease-Management-Programmen kritisch auf	A.1.IX.4

	die Erforderlichkeit hin untersucht wird.	
53	Ich empfehle der Landesregeierung, sofern sie weiterhin die Notwendigkeit sieht, zwischen dem Disease-Management-Programm „Brustkrebs“ und der Krebsregister Daten auszutauschen, Verfahrensregelungen zu erlassen, die das Recht der Frauen auf informationelle Selbstbestimmung respektieren und dennoch dazu beitragen, dass Doppelmeldungen vermieden werden.	A.1.IX.5
54	Ich empfehle der Landesregierung, die Ärzte in der Wahrnehmung ihrer Auskunftspflichten und sonstigen datenschutzrechtlichen Verpflichtungen durch Schulungs- oder Informationsmaßnahmen zu unterstützen und Maßnahmen zur Stärkung der Patientenrechte zu ergreifen.	A.1.IX.6
55	Ich empfehle der Landesregierung, mich bei der Planung von Forschungsprogrammen unter Einbeziehung von Patientenakten frühzeitig zu beteiligen bzw. darauf hinzuwirken und die Initiative der 67. Konferenz der Datenschutzbeauftragten zur Einführung eines Forschungsgeheimnisses aufzugreifen.	A.1.IX.11
56	Ich empfehle der Landesregierung, gegenüber den Gesundheitsämtern klarzustellen, dass aus den bei ihnen vorhandenen Patientenakten Auskünfte an Dritte nur mit einer Schweigepflichtentbindungserklärung des jeweiligen Patienten zulässig sind, aus der Umfang und Tragweite hervorgehen müssen.	A.1.IX.12
57	Ich empfehle der Landesregierung, bei der Vergabe von Forschungsvorhaben auf die datenschutzrechtlichen Bestimmungen des § 34 Landesdatenschutzgesetz Mecklenburg Vorpommern hinzuweisen.	A.1.X.2

B Zweiter Tätigkeitsbericht gemäß § 38 Absatz 1 des Bundesdatenschutzgesetzes (BDSG)

1 Einführung

Im Rahmen meiner Zuständigkeit als Aufsichtsbehörde für den nicht-öffentlichen Bereich lege ich dem Landtag erstmalig einen Bericht über die Tätigkeit der Aufsichtsbehörde vor, der den Zeitraum vom 1. Januar 2004 bis zum 31. Dezember 2005 umfasst und damit die Tätigkeit des Innenministeriums als Aufsichtsbehörde bis zum Wechsel der Zuständigkeit am 11. November 2004 einschließt.

Die Berichterstattung der für den Datenschutz zuständigen Kontrollstellen ist in der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Europäische Datenschutzrichtlinie) vorgesehen und wurde mit der Regelung in § 38 Abs. 1 Satz 6 Bundesdatenschutzgesetz (BDSG) in nationales Recht übernommen. Der Erste Bericht wurde durch die Landesregierung für den Berichtszeitraum vom 23. Mai 2001 bis 31. Dezember 2003 dem Landtag auf Drucksache 4/1294 mit Schreiben vom 13. August 2004 zugeleitet.

Nach § 1 Abs. 2 BDSG ist das Bundesdatenschutzgesetz Grundlage für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch nicht-öffentliche Stellen (Unternehmen und Betriebe) und regelt die Zulässigkeit für die Datenverarbeitung, die Rechte der Betroffenen und die Aufsicht über den Datenschutz im nicht-öffentlichen Bereich. Der vorliegende Bericht gibt einen Überblick über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörde im Land Mecklenburg-Vorpommern für den oben genannten Berichtszeitraum von zwei Jahren.

Die Datenschutzaufsicht im nicht-öffentlichen Bereich hat sich mit der Novellierung des BDSG im Jahre 1990 zu einer auf die Datenverarbeitung zugeschnittenen Form der allgemeinen staatlichen Wirtschaftsaufsicht entwickelt. § 38 BDSG legt den rechtlichen Rahmen für die Tätigkeit der Aufsichtsbehörde fest und definiert deren Stellung gegenüber den verantwortlichen Stellen.

In Fragen der Zulässigkeit der einzelnen Datenverarbeitung oder -nutzung spricht die Aufsichtsbehörde – auch nach Prüfungen – zunächst Empfehlungen aus, die allerdings keinen Verwaltungsakt darstellen, weil nicht konkret regelnd eingegriffen wird. Wenn nach meiner Überzeugung eine unzulässige Datenverarbeitung vorliegt, habe ich ferner die Möglichkeit, ein Ordnungswidrigkeitsverfahren einzuleiten (§ 43 BDSG) oder – in besonders gravierenden Fällen – Strafantrag zu stellen (§ 44 Abs. 2 BDSG).

Die Aufsichtsbehörde klärt – ähnlich wie in einem vorgerichtlichen Verfahren – im Rahmen ihrer Möglichkeiten den Sachverhalt auf und nimmt eine rechtliche Bewertung vor. Mit dieser Bewertung liegt auch für den Petenten eine Grundlage vor, auf Grund derer die datenverarbeitende Stelle in einer Vielzahl der Fälle zu einem datenschutzrechtlich korrekten Verfahren zurückkehrt. Die Stellungnahme der Aufsichtsbehörde kann zum Beispiel auch im Gerichtsverfahren wie ein Gutachten verwendet werden.

Im Rahmen ihrer Prüfungstätigkeit kann die Aufsichtsbehörde Auskünfte verlangen (§ 38 Abs. 3 BDSG), Geschäftsräume zu Prüfungen und Besichtigungen betreten und Einsicht in Unterlagen nehmen. Stellt sie nicht ausreichende Datensicherungsmaßnahmen fest, kann sie anordnen, dass die Mängel beseitigt werden, oder – bei schwerwiegenden Mängeln – unter bestimmten Umständen Zwangsgelder festsetzen beziehungsweise den Einsatz einzelner Verfahren untersagen (§ 38 Abs. 5 BDSG) sowie die Abberufung des betrieblichen Datenschutzbeauftragten verlangen, wenn ihm Fachkunde und Zuverlässigkeit fehlen (§ 38 Abs. 5 Satz 3 BDSG). Gegen einen solchen anordnenden Bescheid gemäß § 38 Abs. 5 BDSG sind Widerspruch und Klage vor dem Verwaltungsgericht möglich.

Nach § 4 d in Verbindung mit § 3 Abs. 2 BDSG besteht vor der Inbetriebnahme von Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen grundsätzlich eine Meldepflicht gegenüber der Aufsichtsbehörde. Die Pflicht zur Meldung entfällt, wenn die verantwortliche Stelle einen betrieblichen Datenschutzbeauftragten bestellt hat. Sie entfällt ebenso, wenn bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten höchstens vier Arbeitnehmer beschäftigt sind und entweder eine Einwilligung des Betroffenen vorliegt oder die Datenverarbeitung zu Vertragszwecken beziehungsweise im Rahmen eines vorvertraglichen Vertrauensverhältnisses mit dem Betroffenen erfolgt. Die genannten Befreiungen gelten allerdings nach § 4 d Abs. 4 BDSG nicht für Verfahren automatisierter Verarbeitung personenbezogener Daten durch nichtöffentliche Stellen, die geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung (Handelsauskunfteien und andere Auskunftsdienste) oder der anonymisierten Übermittlung speichern (Markt- und Meinungsforschungsinstitute). Diese unterliegen immer der Meldepflicht. Die Aufsichtsbehörde führt ein Register, in dem die nach § 4 d BDSG meldepflichtigen automatisierten Verarbeitungen erfasst werden. Es dient der Transparenz und kann von jedermann eingesehen werden. Insgesamt waren am Ende des Berichtszeitraumes neun meldepflichtige Unternehmen registriert, darunter vier Auskunfteien, drei Markt- und Meinungsforschungsinstitute und zwei sonstige Unternehmen.

Nach § 21 Abs. 1 Satz 1 BDSG kann sich jedermann an die Aufsichtsbehörde wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch nicht-öffentliche Stellen in seinen Rechten verletzt worden zu sein. Die Eingaben im Berichtszeitraum reichten inhaltlich von einfachen Anfragen und Hinweisen bis hin zu konkreten Beschwerden über den Umgang mit personenbezogenen Daten im Einzelfall. Die Anfragen und Beschwerden betrafen oft die Bereiche Werbung, Adresshandel, Handels- und Wirtschaftsauskunfteien, aber auch die Datenverarbeitung im Handel und den Einsatz von Videokameras.

In einem Fall wurde von mir als Aufsichtsbehörde Strafantrag gestellt. Bußgeldverfahren, die ein Bußgeld von bis zu 25.000,- € bei Verstößen gegen formale Vorschriften und bis zu 250.000,- € bei Verstößen gegen materielles Datenschutzrecht nach sich ziehen können, musste die Aufsichtsbehörde während des Berichtszeitraums nicht einleiten.

Zu meinem Aufgabenbereich als Aufsichtsbehörde zählt ferner die Beratung betrieblicher Datenschutzbeauftragter. Nicht-öffentliche Stellen, die personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen, haben grundsätzlich die Pflicht, einen betrieblichen Beauftragten für den Datenschutz zu bestellen (§ 4 f Abs. 1 BDSG). Der betriebliche Datenschutzbeauftragte hat insbesondere die Aufgabe, auf die Einhaltung der Datenschutzregelungen in seinem Betrieb hinzuwirken. Er muss die zur Erfüllung seiner Aufgaben erforderliche Fach-

kunde und Zuverlässigkeit besitzen, ist der Geschäftsleitung unmittelbar unterstellt und in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei.

Zur Fortbildung der betrieblichen Datenschutzbeauftragten haben Mitarbeiter meiner Behörde unter anderem ein datenschutzrechtliches und datensicherheitstechnisches Seminar für rund 30 künftige betriebliche Datenschutzbeauftragte im Gesundheitsbereich durchgeführt. Daneben gab es viele Einzelberatungen von Betrieben, zum Teil vor Ort. Ferner organisiert die Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD) in Deutschland die Einrichtung von regionalen Erfahrungsaustauschkreisen – so genannten ERFA-Kreisen. Auch in Mecklenburg-Vorpommern treffen sich im ERFA-Kreis regelmäßig bis zu 60 betriebliche Datenschutzbeauftragte aus Betrieben des Landes unter Beteiligung von Vertretern aus Behörden und anderen öffentlichen Stellen. Seit 1992 ist die Aufsichtsbehörde jeweils zu den Sitzungen eingeladen und nimmt regelmäßig an diesen zwei- bis dreimal im Jahr stattfindenden Gesprächsrunden teil – ebenso wie an den jährlichen Datenschutz-Fachtagungen.

Die Aufsichtsbehörden aller Bundesländer für den Datenschutz im nicht-öffentlichen Bereich arbeiten ferner seit vielen Jahren im so genannten Düsseldorfer Kreis zusammen, um eine möglichst einheitliche Anwendung des Bundesdatenschutzgesetzes in den Ländern zu erreichen. Hierzu kommen die Referenten der Länder-Datenschutz-Aufsichtsbehörden jährlich zweimal zusammen, um die wichtigsten Fachfragen der Datenschutzaufsicht im nicht-öffentlichen Bereich zu diskutieren und abgestimmte Lösungen zu entwickeln. Dies ist insbesondere dann von Bedeutung, wenn sich die Beratungs- und Kontrolltätigkeit der Aufsichtsbehörden auf länderübergreifend handelnde Wirtschaftsunternehmen oder eine ganze Branche bezieht. Schwerpunkte innerhalb des Berichtszeitraums waren unter anderem die Themenbereiche Auskunfteien und Wohnungswirtschaft, Kredit-Scoring und das Akkreditierungsverfahren für die Fußball-Weltmeisterschaft 2006. Daneben war ich als Aufsichtsbehörde für Mecklenburg-Vorpommern zusätzlich beteiligt an der „Arbeitsgruppe SCHUFA / Handels- und Wirtschaftsauskunfteien“ des Düsseldorfer Kreises, die sich ebenfalls zweimal jährlich trifft. Aufgrund des finanziellen und personellen Aufwandes muss ich diese Mitarbeit jedoch voraussichtlich einschränken. Weitere Arbeitsgruppen des Düsseldorfer Kreises befassen sich mit der Versicherungswirtschaft, der Kreditwirtschaft, der Telekommunikation, den Tele- und Mediendiensten und mit Fragen des internationalen Datenschutzes.

2 Unabhängigkeit der Datenschutzaufsicht – Vertragsverletzungsverfahren der Europäischen Kommission

Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie) verlangt, dass die Einhaltung datenschutzrechtlicher Vorschriften in den Mitgliedsstaaten von Stellen überwacht wird, die ihre Aufsichtaufgaben in völliger Unabhängigkeit wahrnehmen. In der Mehrzahl der deutschen Bundesländer ist demgegenüber die Datenschutzaufsicht über die Privatwirtschaft (so genannte nicht-öffentliche Stellen) überwiegend in den jeweiligen Innenministerien angesiedelt und damit in den hierarchischen Weisungsstrang des Ministeriums eingebunden. Diese Aufsichtsstruktur bei der Datenschutzkontrolle verstößt nach Feststellung der Europäischen Kommission gegen europäisches Recht und ist Gegenstand eines Vertragsverletzungsverfahrens gegen die Bundesrepublik Deutschland.

In Mecklenburg-Vorpommern ist die Funktion der Aufsichtsbehörde gemäß § 33 a Landesdatenschutzgesetz (DSG M-V) dem Landesbeauftragten für den Datenschutz übertragen worden, der in Ausübung dieser Tätigkeit der Rechtsaufsicht der Landesregierung unterliegt. In dem von der Europäischen Kommission eingeleiteten Vertragsverletzungsverfahren vertritt die Kommission auch zu dieser Regelung die Auffassung, dass die Unterstellung unter die Rechtsaufsicht der Landesregierung ebenso wie die verschiedenen Formen von Fach-, Rechts- und Dienstaufsicht in anderen Bundesländern nicht mit Gemeinschaftsrecht vereinbar sind, da diese Organisationsformen nicht den Anforderungen der verlangten „völligen Unabhängigkeit“ im Sinne des Artikels 28 Abs. 1 Satz 2 der Europäischen Datenschutzrichtlinie entsprechen.

Ich habe daher zusammen mit meinen Kollegen anlässlich der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. Oktober 2005 unterstrichen, dass die Datenschutzbeauftragten des Bundes und der Länder eine einheitliche Datenschutzkontrolle des öffentlichen und privaten Bereichs in völliger Unabhängigkeit sicherstellen können. Sie sollte dazu beim Bund und in allen Ländern als eigenständige oberste Behörde eingerichtet werden, die keinen Weisungen anderer administrativer Organe unterliegt (siehe Anlage 16).

Auch bei völliger Aufsichtsfreiheit bestehen ausreichend Elemente, die nach meiner Auffassung eine hinreichende demokratische Legitimation gewährleisten, so die Wahl des Landesbeauftragten durch das Parlament, befristete Amtszeit, Möglichkeit der Abwahl durch das Parlament, die zweijährige Berichtspflicht und – im nicht-öffentlichen Bereich – die Möglichkeit der betroffenen Unternehmen, belastende Maßnahmen auch gerichtlich überprüfen lassen zu können.

3 Gesetzesinitiative zur Änderung des Bundesdatenschutzgesetzes

Das Bundesdatenschutzgesetz (BDSG) legt für Firmen und Betriebe (so genannte nichtöffentliche Stellen) fest, dass Verfahren zur automatisierten Verarbeitung von personenbezogenen Daten vor ihrer Inbetriebnahme grundsätzlich der zuständigen Aufsichtsbehörde zu melden sind (§ 4 d Abs. 1 BDSG). Das Gesetz sieht allerdings Ausnahmen von der Meldepflicht vor.

Zum einen entfällt eine Meldung, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat – zum anderen, wenn mit der Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten für eigene Zwecke höchstens vier Arbeitnehmer beschäftigt sind und eine Einwilligung der Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertrages bzw. vertragsähnlichen Vertrauensverhältnisses mit den Betroffenen dient (§ 4 d Abs. 3 BDSG).

Die Bestellung eines betrieblichen Datenschutzbeauftragten (gemäß § 4 f Abs. 1 BDSG) ist – als wichtige Maßnahme der Selbstkontrolle des Datenschutzes in Firmen und Betrieben – für den Fall vorgesehen, dass wenigstens fünf Arbeitnehmer in automatisierter Weise (z. B. per Computer) oder mindestens 20 Personen auf „andere“ Weise (nicht automatisiert) personenbezogene Daten erheben, verarbeiten oder nutzen.

Betrieblicher Datenschutzbeauftragter: Der betriebliche Datenschutzbeauftragte wirkt innerhalb seines Unternehmens auf die Einhaltung des Bundesdatenschutzgesetzes und anderer Datenschutzvorschriften hin (§ 4 g BDSG). Er ist Ansprechpartner sowohl der Geschäftsleitung als auch der Beschäftigten des Unternehmens für alle Fragen des Datenschutzes. Er führt eine Übersicht, in der sämtliche Computerverfahren mit Löschungsfristen, Datenempfängern etc. aufgelistet sind (Verfahrensbeschreibung). Diese Angaben sind auf Antrag für jedermann einsehbar.

Der betriebliche Datenschutzbeauftragte überwacht die ordnungsgemäße Anwendung von Datenverarbeitungsprogrammen, führt – etwa bei der Verarbeitung von sensiblen Daten – Vorabkontrollen durch und organisiert Datenschutzschulungen für das Personal.

Er ist der Geschäftsleitung unmittelbar unterstellt, auf dem Gebiet des Datenschutzes weisungsfrei und muss die zur Erfüllung seiner Aufgaben erforderliche Fachkunde (Recht, Technik, Organisationsstruktur des Unternehmens etc.) sowie Zuverlässigkeit besitzen (persönliche Integrität / keine Interessenkollisionen – insbesondere mit sonstigen übertragenen Tätigkeiten).

Die Länder Niedersachsen und Hessen haben im Bundesrat einen Gesetzentwurf zur Änderung dieser Regelungen im BDSG eingebracht, dessen Hauptgegenstand die Reduzierung des Anwendungsbereichs für die genannten Pflichten bildet. Danach soll die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten für Firmen künftig erst dann bestehen, wenn in einem Unternehmen mehr als 19 Arbeitnehmer mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt sind. Auch die Meldepflicht soll künftig erst ab einer Zahl von mindestens 20 Arbeitnehmern einsetzen.

Dieser Vorschlag zur Änderung des BDSG zielt darauf ab, kleinere Betriebe und Unternehmen von der Meldepflicht und der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten freizustellen. Dies sei zur Anpassung an geänderte Lebenssachverhalte und zur Berücksichtigung des technischen Wandels erforderlich, der zu einer weiten Verbreitung von automatisierten Datenverarbeitungsformen in fast allen Lebensbereichen geführt habe.

Der Bundesrat hat in seiner Sitzung am 23. September 2005 mit der Mehrzahl der Stimmen der Länder dem Gesetzentwurf zugestimmt und ihn an den Bundestag zur Stellungnahme weitergeleitet. Das Land Mecklenburg-Vorpommern hat sich meiner Argumentation angeschlossen und den Gesetzentwurf nicht unterstützt.

Ich habe mich bereits im Vorfeld des Bundesratsbeschlusses gegen diese Gesetzesinitiative ausgesprochen. Die vorgeschlagenen Änderungen sind nicht geeignet, das Ziel des Gesetzentwurfs – Entbürokratisierung und Kostensenkung in kleineren Betrieben – umfassend zu erreichen. Bei Entfallen der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten bleibt die datenschutzrechtliche Verantwortung und Haftung der Firmengeschäftsführung voll bestehen, so dass der angestrebte Entlastungszweck insofern nicht erreicht wird. Auch bei Inkrafttreten des Gesetzentwurfs bleibt die Pflicht zur Bestellung des betrieblichen Datenschutzbeauftragten für Betriebe bestehen, die einer Vorabkontrolle unterliegen (etwa solche, die besonders sensible Arten von personenbezogenen Daten verarbeiten), wodurch sich der Anwendungsbereich des Gesetzentwurfs entsprechend relativieren würde.

Der Gesetzentwurf ist insbesondere nicht vereinbar mit Artikel 18 der Europäischen Datenschutzrichtlinie vom 24. Oktober 1995, der die angestrebte Ausnahmeregelung bei der Meldepflicht nicht vorsieht.

> **EU-Datenschutzrichtlinie:** Die Richtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr – EU-Datenschutzrichtlinie – konkretisiert und ergänzt die Grundsätze der Datenschutzkonvention des Europarates von 1981 und schafft ein einheitliches Datenschutzniveau für die Ausführung und Anwendung des Gemeinschaftsrechts in allen Mitgliedsstaaten. Das BDSG wurde im Jahre 2001 – das DSG M-V im Jahre 2002 – entsprechend den Regelungen der EU-Datenschutzrichtlinie novelliert.

Nach Artikel 18 der Europäischen Datenschutzrichtlinie kann von der Meldepflicht nur abgegangen werden, wenn für Verarbeitungskategorien, bei denen eine Beeinträchtigung der Rechte der betroffenen Personen unwahrscheinlich ist, die Zweckbestimmung der Verarbeitung, die Daten oder Datenkategorien sowie die Kategorien der betroffenen Personen, die Empfänger oder Empfängerkategorien, an die Daten weitergegeben werden, und die Dauer der Aufbewahrung festgelegt sind oder die Bestellung eines betrieblichen Datenschutzbeauftragten vorgeschrieben wird. Dabei erscheint es bereits zweifelhaft, ob der bisherige § 4 d Abs. 3 BDSG diesen Anforderungen genügt. Eine Ausweitung dieser Ausnahmeregelung auf eine sehr große Zahl von verantwortlichen Stellen und faktisch auf weite Bereiche in Handwerk, Handel und den freien Berufen wäre aber in keinem Fall mehr richtlinienkonform.

Durch den Bedeutungswandel der automatisierten Datenverarbeitung seit der erstmaligen Regelung im Bundesdatenschutzgesetz im Jahre 1978 ist nicht nur – wie die Befürworter der Gesetzesänderung vorbringen – die Anzahl der eingesetzten Datenverarbeitungssysteme gestiegen. Gesteigert hat sich insbesondere auch die Komplexität der IT-Systeme und ihre Vernetzung untereinander.

Dies führt zu einem wachsenden Bedarf an Organisation und Kontrolle dieser immer komplexeren Datenverarbeitungssysteme durch spezialisierte Mitarbeiter in Datenschutz- und Datensicherheitsfragen – sowohl im Interesse des Betriebes selbst, seiner Kunden und Geschäftspartner als auch der Aufsichtsbehörden.

Vor diesem Hintergrund würde sich die durch den Gesetzentwurf angestrebte Befreiung von der Meldepflicht und der Pflicht zur Bestellung eines spezialisierten betrieblichen Datenschutzbeauftragten in Mecklenburg-Vorpommern – auch im Hinblick auf die hier vorherrschenden Betriebsgrößen – eher kontraproduktiv auswirken.

4 Handels- und Wirtschaftsauskunfteien

Oft erreichten mich Anfragen, ob und inwieweit die Tätigkeit von Handels- und Wirtschaftsauskunfteien mit dem Datenschutzrecht vereinbar sei. Anlass der Fragen war in allen Fällen die Mitteilung einer Auskunftei an einen Bürger, dass sie Informationen über ihn gespeichert hätte.

Handels- und Wirtschaftsauskunfteien sammeln Informationen über die Kreditwürdigkeit, wirtschaftliche Betätigung und Bonität von Unternehmen und Privatpersonen. Ihre Tätigkeit ist zulässig, sofern sie sich im Rahmen des Bundesdatenschutzgesetzes (BDSG) bewegt.

Die Benachrichtigung war Anlass für die Irritation und Sorge, in Datenbanken von Auskunfteiunternehmen gespeichert zu sein, ohne bisher davon gewusst zu haben, und für die Frage nach der rechtlichen Zulässigkeit und eigenen („Abwehr“)-Rechten. Inhalt und Form der Benachrichtigungen selbst waren in den genannten Fällen nicht zu beanstanden. Mit der Benachrichtigung kamen die Auskunfteien ihrer Verpflichtung aus § 33 Abs. 1 BDSG nach. Das Wissen um das Vorhandensein von Daten ist Voraussetzung für die Wahrnehmung der weiteren Rechte durch den Betroffenen. Dieser hat nach § 34 BDSG das Recht auf Auskunft über die zu seiner Person gespeicherten Daten, den Speicherungszweck und die Kategorien von Empfängern, an die die Daten im Allgemeinen weitergegeben werden. Falls die Daten unrichtig sind, besteht gemäß § 35 BDSG das Recht auf Berichtigung, Sperrung oder – bei Unzulässigkeit der Speicherung – auch auf Löschung der Daten.

Daneben wurde regelmäßig die Frage nach der Zulässigkeit der Weiterübermittlung der Daten an Dritte gestellt. Nach § 29 Abs. 2 BDSG ist die Übermittlung von personenbezogenen Daten durch Auskunfteien an Dritte nur zulässig, wenn der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und insbesondere kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat.

Das berechtigte Interesse des Anfragenden ist bei jeder Anfrage zu begründen. Anfragen erfolgen zum überwiegenden Teil durch Geschäftsleute. Ein großer Teil des Auskunftsverkehrs betrifft Firmen, die sich über andere Unternehmen oder Freiberufler erkundigen. Für Privatpersonen werden Anfragen vor allem vom Versandhandel gestellt. Daneben fragen aber auch Hypothekenbanken, Handels- und Kaufhäuser, Heizöl-Lieferanten oder andere Firmen an, die Kontakte mit Privatkunden haben. Sie können eine Auskunft erhalten, wenn ein konkretes berechtigtes Interesse vorliegt. In der Regel ist dies ein Kauf, für den die Rechnung erst später erstellt wird. Für diese Auskunftsempfänger ist es in erster Linie wichtig zu wissen, dass diese Person tatsächlich existiert und ihre Anschrift aktuell ist – ihnen liegt oft daran, bereits bekannte Angaben bestätigt zu sehen. Außerdem interessieren sie sich dafür, ob Eintragungen im öffentlichen Schuldnerregister vorhanden sind.

Schutzwürdige Interessen der Betroffenen stehen der Verwendung der gespeicherten Daten dann entgegen, wenn die Angaben nicht der Beurteilung der Kreditwürdigkeit und Zahlungsfähigkeit der Betroffenen dienen. Dies ist etwa der Fall bei unrichtigen Daten oder bei Vermögensangaben über Ehepartner und Verwandte. Das schutzwürdige Interesse des Betroffenen wäre insbesondere verletzt bei Angaben wie „schlechter Gesundheitszustand“ (sensible personenbezogene Information gemäß § 3 Abs. 9 BDSG). Zugleich läge eine Verletzung seines allgemeinen Persönlichkeitsrechts vor.

5 Kein Profiling ohne Aufklärung

Ein Petent hat sich an mich gewandt, weil er vom Arbeitsamt eine Aufforderung zur Teilnahme an einem so genannten Profiling erhalten hatte. Dazu wurde ihm die Kurzbeschreibung eines vom Arbeitsamt beauftragten Bildungsträgers und ein Fragebogen zugesandt, in dem

nach Familienverhältnissen, Telefon- und Faxverbindung, gesundheitlichen Einschränkungen, Sprachkenntnissen, Schulbildung, Berufsausbildung, beruflichem Werdegang und der Art der Beendigung des letzten Arbeitsverhältnisses gefragt wurde.

Da sich der Petent hinsichtlich der Verwendung dieser Daten unsicher war, erkundigte er sich beim Bildungsträger, ob dieser Fragebogen für das Arbeitsamt oder für den Bildungsträger vorgesehen sei. Man erklärte ihm, diese Angaben sollten zum Abgleich mit den Daten beim Arbeitsamt verwendet werden – beim Bildungsträger verblieben keine Daten. In der Annahme, die Angaben im Fragebogen seien für das Arbeitsamt bestimmt, verwies er auf die dort bereits vorhandenen Informationen und füllte den Fragebogen nicht aus.

Als der Petent sich beim Bildungsträger vorstellte, forderte dieser den Fragebogen ab und verlangte das vollständige Ausfüllen. Nach kurzer Auseinandersetzung stellte sich heraus, dass die Daten vom Bildungsträger genutzt und ausgewertet werden sollten. Der Bildungsträger war wegen seiner besonderen Fachkenntnisse vom Arbeitsamt mit dieser Aufgabe zur selbständigen Erledigung beauftragt worden.

Auch die Tatsache, dass im Rahmen des Profiling psychologische Tests vorgenommen werden sollten, war zuvor nicht angekündigt worden. Eine spezialgesetzliche Grundlage für die Erhebung und Speicherung seiner Daten konnte dem Petenten nicht genannt werden, obwohl sie nach dem Sozialgesetzbuch in Verbindung mit dem Job-Aktiv-Gesetz vorhanden war. Vielmehr drohte der Bildungsträger in rechtswidriger Weise mit Konsequenzen bis hin zu Leistungskürzungen. Nach aufklärender Rücksprache des Petenten mit dem Arbeitsamt füllte der Petent den Fragebogen aus und nahm an dem Profiling teil.

Aus datenschutzrechtlicher Sicht war gegenüber dem Bildungsträger zu beanstanden, dass über die beabsichtigte Datenverarbeitung in der Aufforderung zum Profiling nur andeutungsweise aufgeklärt wurde. Es fehlten detaillierte Informationen über Inhalte sowie Sinn und Zweck des Profiling-Verfahrens. Auch fehlte der Hinweis auf die Verschwiegenheitspflichten der Psychologen nach § 203 Strafgesetzbuch.

Die Geschäftsführung wurde darauf hingewiesen, dass diese Informationen zur Unterrichtung des Betroffenen nach § 4 Abs. 3 Bundesdatenschutzgesetz unabdingbar sind. Darüber hinaus tragen sie zur Förderung der Akzeptanz und der Motivation der Betroffenen im Rahmen des Gesamtverfahrens bei.

Die Geschäftsführung sicherte zu, die Mitarbeiter so zu schulen, dass sie den genannten datenschutzrechtlichen Aufklärungspflichten künftig nachkommen werden.

6 Anfangsverdacht der rechtswidrigen Verarbeitung von Mandantendaten

Ein Petent schilderte mir seinen Verdacht, dass sich ein ehemaliger Administrator einer Steuerberaterkanzlei in sehr großem Umfang personenbezogene Daten von Mandanten beschafft und für die Tätigkeit in einem anderen Steuerberatungsbüro verwendet habe.

Aus einer Vielzahl von detaillierten Anhaltspunkten ergab sich nach seiner Auffassung, dass sich der ehemalige Mitarbeiter unberechtigt personenbezogene Daten von möglicherweise eintausend Personen verschafft und weitergegeben habe.

Der Petent hatte unter Verweis auf diesen Sachverhalt bereits Strafanzeige bei der zuständigen Staatsanwaltschaft gestellt. Er wandte sich an mich mit der Bitte, ihn im Rahmen meiner Befugnisse in dem laufenden Strafverfahren und insbesondere hinsichtlich der Veranlassung einer Beweissicherung zu unterstützen.

Übliche Verwahrensweise meiner Behörde in Fällen dieser Art ist es, die Gegenseite – in diesem Fall den ausgeschiedenen Mitarbeiter – um Stellungnahme zu bitten. Im vorliegenden Fall habe ich, wegen der möglichen Gefahr einer Beweismittelbeseitigung und im Hinblick auf die laufenden Ermittlungen der Staatsanwaltschaft, hiervon zunächst Abstand genommen.

Vor dem Hintergrund des erheblichen Umfangs eines möglichen Datenschutzverstoßes habe ich mich an den Generalstaatsanwalt gewandt und in dieser Sache als Aufsichtsbehörde Strafantrag gemäß § 44 Abs. 2 in Verbindung mit § 43 Abs. 2 Bundesdatenschutzgesetz (BDSG) gestellt.

Strafantrag des Landesbeauftragten für den Datenschutz: Bei vorsätzlich begangenen Verstößen gegen das Bundesdatenschutzgesetz, die nach § 43 Abs. 2 BDSG mit Bußgeld geahndet werden können, handelt es sich nach § 44 Abs. 1 BDSG dann um Straftatbestände, wenn die Tat gegen Entgelt beziehungsweise in Bereicherungs- oder Schädigungsabsicht begangen wird. Solche Straftaten sind Antragsdelikte. Die Tat wird daher nach § 44 Abs. 2 BDSG nur verfolgt, wenn ein Strafantrag gestellt wird. Antragsberechtigt sind der von der Straftat Betroffene und – nach § 44 Abs. 2 BDSG – auch die Aufsichtsbehörde, hier der Landesbeauftragte für den Datenschutz.

Da die Gefahr bestand, dass es sich hier um einen Datenschutzverstoß von gravierendem Umfang handeln könnte, habe ich – auch im Hinblick auf die Eilbedürftigkeit und die große Zahl möglicher Drittbetroffener – von meinem Strafantragsrecht Gebrauch gemacht, um so dazu beizutragen, dass mögliche Beeinträchtigungen von Datenschutzrechten aller Betroffenen so gering wie möglich gehalten werden.

Zu meinen Aufgaben zählt es auch zu prüfen, ob der Betrieb oder das Unternehmen als verantwortliche Stelle die erforderlichen technischen und organisatorischen Maßnahmen trifft, um Datenschutz und Datensicherheit zu gewährleisten. Ich habe deshalb die von dem Vorfall betroffene Steuerberatungskanzlei gebeten, mir die Schutzmaßnahmen gemäß § 9 BDSG mitzuteilen, die sie als für die Datenverarbeitung nach § 3 Abs. 7 BDSG verantwortliche Stelle getroffen hat. Diese waren nicht zu beanstanden.

§ 9 BDSG: Nach § 9 BDSG sind nicht-öffentliche Stellen, die personenbezogene Daten verarbeiten, verpflichtet, alle technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die gesetzlichen Datenschutz- und Datensicherheitsanforderungen zu gewährleisten. Dazu zählt insbesondere die Kontrolle darüber, dass die zur Benutzung des Systems berechtigten Personen nur auf die Daten Zugriff haben, zu denen sie eine Zugriffsberechtigung besitzen.

Der Generalstaatsanwalt hat mir mitgeteilt, dass bei der zuständigen Staatsanwaltschaft Ermittlungen gegen den ehemaligen Mitarbeiter unter anderem wegen Unterschlagung geführt werden und Beweissicherungsmaßnahmen angeordnet worden sind. Nach Mitteilung der zu-

ständigen Staatsanwaltschaft haben diese Maßnahmen zur Sicherstellung diverser Datenträger geführt, die derzeit ausgewertet werden.

Unabhängig von den noch laufenden Ermittlungen bleibt festzustellen, dass es faktisch kaum zu verhindern ist, dass ein in Datenverarbeitungssystemen „hochprivilegierter“ Nutzer wie ein Systemadministrator seine Rechte missbräuchlich anwenden kann. In technischer Hinsicht ist deshalb eine möglichst manipulationssichere Protokollierung unabdinglich, mit der unabhängige Revisoren zumindest nachträglich feststellen können, welche Aktivitäten im Einzelnen zu welchem Zeitpunkt stattgefunden haben und welche Personen Zugriff hatten.

Bei Unternehmen und Betrieben, die mit personenbezogenen Daten in sensiblen Bereichen arbeiten (insbesondere Rechtsanwälte, Steuerberater, Ärzte oder Angehörige anderer Heilberufe, Versicherungen), ist es deshalb von besonderer Bedeutung, dass die personelle Auswahl der Administratorposition sich nicht nur nach Fachkompetenz bemisst, sondern persönliche Integrität und ein besonderes Vertrauensverhältnis als unbedingte Voraussetzung bei der Auswahl eine herausgehobene Rolle spielt.

7 Unzureichend geschützte Lagerung von Personalunterlagen

Von einem Petenten erhielt ich den Hinweis, dass im Gebäude eines ehemaligen Volkseigenen Betriebes Personaldokumente nur unzureichend geschützt gelagert seien. Für den ehemaligen Betrieb war ein Konkursverwalter eingesetzt worden, der seinen Sitz in einem anderen Bundesland hatte. Dieser hatte nach Mitteilung des Petenten den von ihm vorgeschlagenen Abtransport der Unterlagen zur Gewährleistung einer sicheren Aufbewahrung aus Kostengründen abgelehnt.

Ich habe den Konkursverwalter um Stellungnahme zum Sachverhalt gebeten und auf die Pflichten nach § 9 Bundesdatenschutzgesetz beziehungsweise § 21 Landesdatenschutzgesetz Mecklenburg-Vorpommern hingewiesen. Danach sind die technischen und organisatorischen Maßnahmen zu treffen, die nach dem Stand der Technik und nach der Schutzbedürftigkeit der Daten erforderlich sind, um den Schutz der Personalunterlagen insbesondere gegen die Kenntnisnahme durch Unbefugte sowie gegen Abhandenkommen oder Beschädigungen sicherzustellen.

Der Konkursverwalter hat mir inzwischen bestätigt, dass die Personalunterlagen durch eine Speditionsfirma abgeholt und danach archiviert worden sind. Beim Abtransport sei der ehemalige Geschäftsführer des Betriebes anwesend gewesen, um für eine entsprechende Kennzeichnung der einzelnen Dokumente zu sorgen. Da sich der Aufbewahrungsort der archivierten Unterlagen nunmehr in einem anderen Bundesland befindet, habe ich die dort zuständige Datenschutzaufsichtsbehörde informiert.

8 Wonach darf der Arbeitgeber fragen?

Mir wurde ein Personalfragebogen eines überregionalen Ausbildungszentrums zur datenschutzrechtlichen Prüfung übersandt. Die Mitarbeiter des Ausbildungszentrums sollten darin

Daten angeben, die für das Arbeitsrechtsverhältnis nicht erforderlich sind. Folgende Angaben waren beispielsweise gefordert:

- Religionszugehörigkeit des Mitarbeiters und seines Ehepartners: Diese Daten dürfen nicht erhoben werden, es sei denn, es handelt sich um einen religionsgebundenen Arbeitgeber – siehe § 28 Abs. 6 bis 9 Bundesdatenschutzgesetz bzw. § 7 Abs. 2 Landesdatenschutzgesetz.
- Wehrdienstzeiten, der letzte Dienstgrad sowie Erwartung der Einberufung zur Bundeswehr: Die Frage nach Wehrdienstzeiten oder einer bevorstehenden Einberufung zur Bundeswehr ist zulässig, weil der Arbeitgeber Anspruch auf einen lückenlosen beruflichen Werdegang hat beziehungsweise die Angabe für seine Planung benötigt. Jedoch darf nicht verpflichtend nach dem letzten Dienstgrad gefragt werden. Dies kann allenfalls eine freiwillige Angabe sein, wenn es darum geht, Führungserfahrungen eines Mitarbeiters festzustellen, der im Betrieb mit Führungsaufgaben betraut werden soll.
- Externe ehrenamtliche oder sonstige Funktionen: Solche Daten sind für einen Arbeitgeber nur erforderlich, wenn sich die Aktivitäten auf die berufliche Tätigkeit auswirken, zum Beispiel wenn ein Mitarbeiter bei der Freiwilligen Feuerwehr oder beim Technischen Hilfswerk tätig ist und während der Arbeitszeit entsprechende Einsätze zu erwarten sind.
- Im Haushalt lebende Kinder, unterschieden nach leiblichen oder Adoptivkindern: Die Frage nach Adoptivkindern ist nicht zulässig, weil diese leiblichen Kindern gleichgestellt sind. Außerdem steht dieser Angabe das Offenbarungs- und Ausforschungsverbot des Bürgerlichen Gesetzbuches (§ 1758 BGB) entgegen.

Ich habe den Arbeitgeber aufgefordert, den Fragebogen entsprechend zu korrigieren. Er hat meine Hinweise umgesetzt.

9 Datenschutz bei der Planung von Gästeanfragen im Hotelleriebereich

Ein Hotelberatungsunternehmen informierte mich über ein geplantes Verfahren für Gästebefragungen im Hotelleriebereich, um so durch frühzeitige Beratung bereits im Planungsstadium Aspekte des Datenschutzes berücksichtigen zu können. Die Ergebnisse von Umfragen sollten den Hotels zur Verbesserung von Angebot und Leistung dienen. Ziel war es, die Erwartungen des Gastes an das einzelne Hotel zu ermitteln und dessen Zufriedenheit nach dem Aufenthalt abzufragen.

Hierzu war ein umfangreicher Befragungsbogen entwickelt worden, der nahezu alle Aspekte des Aufenthalts erfassen sollte (Anreise, Reservierungsbearbeitung, Lagebeschilderung, Servicedetails, Hilfe durch das Personal, Eindruck der Lokalität, Raumklima, Funktionalität der Zimmerausstattung, Gastronomiedetails etc.). Nach der Planung des Hotelberatungsunternehmens sollte der Hotelgast bei Anreise über die Umfrage schriftlich informiert und gebeten werden, seine Anschrift und Telefonnummer zum Zwecke der Befragung zur Verfügung zu stellen. Teilnahmebereite Gäste sollten nach schriftlicher Zustimmung den Fragebogen postalisch zugesandt erhalten, auf dessen Grundlage dann ein Telefoninterview geplant war. Danach war vorgesehen, die zusammengefassten Ergebnisse der Auswertung an das Hotel zu übergeben. Hierbei sollten personenbezogene Angaben der an der Umfrage teilnehmenden

Gäste grundsätzlich nicht an das Hotel übermittelt werden (anonymisierte Einzelangaben). In Ausnahmefällen besonderer Unzufriedenheit des Gastes mit dem Aufenthalt sollte – sofern der Gast sein Einverständnis hierzu erteilt – auch dessen Name an das Hotel übermittelt werden können, um diesem die Möglichkeit zu geben, den negativen Eindruck in geeigneter Form ausgleichen zu können.

Soweit personenbezogene Angaben der Gäste erhoben werden, um sie in anonymisierter Auswertungsform an das Hotel zu übermitteln, ist ein solches Gästebefragungsverfahren datenschutzrechtlich als geschäftsmäßige Datenerhebung und Speicherung nach § 30 Bundesdatenschutzgesetz (BDSG) zu bewerten. Nach § 30 BDSG sind personenbezogene Merkmale der Gäste gesondert zu speichern und dürfen intern – hier für Zwecke der Auswertung – zusammengeführt werden. Voraussetzung für die Zulässigkeit ist – soweit wie hier die Erhebung der Daten beim Betroffenen selbst erfolgt – dessen vorherige Einwilligung. Da die Einwilligung nach § 4 a BDSG nur wirksam ist, wenn sie auf der freien Entscheidung des Gastes beruht, muss dieser zuvor auf den vorgesehenen Zweck der Erhebung, Verarbeitung und Nutzung seiner Daten ebenso detailliert hingewiesen worden sein wie über den genauen Ablauf des Verfahrens und der beabsichtigten Daten(weiter)übermittlung.

Soweit in Ausnahmefällen geplant war, auch den Namen des Gastes an das Hotel übermitteln zu können, setzt dies nach § 29 BDSG insbesondere voraus, dass kein Grund zur Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. Auch muss das Hotel, dem die Daten übermittelt werden sollen, ein berechtigtes Interesse an der Kenntnis dieser Daten glaubhaft dargelegt haben.

Kein Grund zur Annahme eines schutzwürdigen Interesses des Gastes am Ausschluss der Datenübermittlung besteht insbesondere dann, wenn dessen eindeutiges Einverständnis in die Übermittlung an das Hotel vorliegt. Gerade in diesem Fall ist das dokumentierte ausdrückliche Einverständnis des Gastes in die Rückübermittlung seines Namens in Verbindung mit den Angaben des Fragebogens von besonderer Bedeutung. In der Regel kann nicht zwangsläufig davon ausgegangen werden, dass ein Gast, der sich im Rahmen einer anonymen Fragebogenaktion mit einem Hotelaufenthalt unzufrieden zeigt, auch möchte, dass sein Name im Zusammenhang mit seiner „Beschwerde“ an das Hotel übermittelt wird.

Umgekehrt unterliegt das Hotel, dem die Daten übermittelt worden sind, einer strengen Zweckbindung – es darf diese Daten also nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt worden sind.

Aus datenschutzrechtlicher Sicht vorzugswürdig ist eine anonyme Rückübermittlung von Fragebögen an Hotelleriebetriebe. Bei der Entscheidung für ein Verfahren, nach dem auch der Name des Gastes zurückübermittelt werden soll, müssen – wie oben dargestellt – insbesondere Zweck und genauer Anlass der Datenübermittlung sowie eine detaillierte Beschreibung des Gesamtverfahrens als Information für den Gast vorliegen, die er zusammen mit seiner Einwilligung unterschreibt. Nach Abschluss der Befragungsaktion sind Dateien und Unterlagen – soweit personenbezogene Daten enthalten sind – zu löschen beziehungsweise zu vernichten, da mit der Beendigung der Zweck der Speicherung entfällt.

Das Hotelberatungsunternehmen wird die beschriebenen und sonstigen datenschutzrechtlichen Anforderungen bei der Gestaltung des Verfahrens beachten.

Aus Datenschutzsicht positiv zu bewerten war insbesondere die Gestaltung des sehr detaillierten Fragebogens, da – bei anonymisierter Rückübermittlung an das Hotel – trotz der Detailliertheit der Fragen eine Identifikation des einzelnen Gastes auch durch Kombination einzelner Antworten nicht möglich war. Datenschutzfreundlich war auch die detaillierte Untersetzung mit formatierten Wahlmöglichkeiten („Kästchen“), die die Anonymisierung zusätzlich erhöht, weil auf diese Weise individuelle (und damit individualisierbare) Anmerkungen des Gastes reduziert werden können.

Insgesamt war zu begrüßen, dass das Hotelberatungsunternehmen – im Sinne eines präventiven Datenschutzes – Datenschutzaspekte bereits im Planungsstadium der beabsichtigten Hotelbefragungen berücksichtigt hat.

10 Einkauf per EC-Lastschriftverfahren

Ein Petent, der Kunde einer Filiale einer bundesweiten Einzelhandelskette ist, informierte mich darüber, dass in dieser Filiale bei Einkäufen mit EC-Karte ab einem Kaufpreis von 100 Euro zusätzlich zur Vorlage des Personalausweises Name und Anschrift des Kunden auf dem Kassenbon notiert werden, welcher bei der Filiale verbleibt. Einen vorherigen Hinweis auf diese Verfahrensweise gibt die Filiale nicht.

Ich habe mich daraufhin an die Geschäftsleitung der Filiale und parallel an den Datenschutzbeauftragten der Einzelhandelskette mit der Bitte um Stellungnahme gewandt und darauf hingewiesen, dass gemäß § 4 Abs. 3 Bundesdatenschutzgesetz (BDSG) der Betroffene über

- die Identität der verantwortlichen Stelle,
- die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und
- die Kategorie von möglichen Datenempfängern

zu unterrichten ist. Ich habe ferner darauf hingewiesen, dass diese Unterrichtung nicht erst während des Zahlvorgangs, sondern bereits vor Erreichen des Kassenbereichs – beispielsweise durch einen gut sichtbaren Aushang – erfolgen sollte.

Bei der Bezahlung per EC-Lastschriftverfahren (also mit EC-Karte ohne Angabe der PIN-Nummer) ist eine Kontrolle des Ausweises zur Betrugsbekämpfung grundsätzlich nicht zu beanstanden, sofern es sich nicht nur um einen geringfügigen Betrag handelt. Dabei werden die Daten der EC-Karte mit dem Ausweis und das Lichtbild im Ausweis mit der zahlenden Person verglichen.

Zusätzlich werden jedoch die Ausweisdaten teilweise oder vollständig auf der Rückseite der Kassenbelege notiert beziehungsweise mit dem EC-Karten-Beleg verbunden. Die Unternehmen, die sich des EC-Lastschriftverfahrens bedienen, begründen diese Praxis damit, dass Banken häufig die Einlösung von EC-Zahlungsbelegen verweigern, etwa wegen unleserlichen Namens. Da die Banken in diesen Fällen auch keine Auskunft über Namen und Anschrift des Kunden geben, kann das Unternehmen die Kaufpreisforderung weder einlösen noch weiter verfolgen. Ein weiterer Grund für das beschriebene Verfahren liegt nach Angabe der Unternehmen in der zunehmenden Benutzung gestohlener EC-Karten.

Aus diesen Gründen kann beim EC-Lastschriftverfahren eine kurzzeitige Speicherung von Namen und Anschrift des Kunden im berechtigten Interesse des Unternehmens liegen. Allerdings ist durch gut erkennbare Schilder, beispielsweise an der Kasse, auf dieses Verfahren und die Gründe seiner Anwendung hinzuweisen. Auch dürfen diese Daten nur bis zu dem Zeitpunkt gespeichert werden, an dem die Zahlung vom Kreditinstitut erfolgt ist. Danach sind die Daten zu löschen.

Der Konzerndatenschutzbeauftragte der Einzelhandelskette hat mir mitgeteilt, dass Kunden durch einen Aushang (Aufkleber) auf das beschriebene Verfahren aufmerksam gemacht werden, die Lastschriftbelege mit den erhobenen Daten verschlossen gelagert sind und nur bei Nichteinlösung der Zahlungsverpflichtung Verwendung finden. Nach Ablauf der Einlösefristen würden die Originalbelege – von denen keine weiteren Kopien existieren – vernichtet werden.

Die betreffende Filiale habe die festgelegte und für den Kunden durch Hinweis angekündigte Grenze von 200 Euro, ab der eine Kontrolle und Datenaufnahme erfolgt, entgegen der gültigen Anweisung auf 100 Euro gesenkt, ohne die Kundeninformation anzupassen. Es habe sich um eine Sicherungsmaßnahme gehandelt, nachdem eine Zunahme der Verwendung gestohlener EC-Karten registriert worden sei.

Der Konzerndatenschutzbeauftragte hat mir ferner mitgeteilt, dass die Geschäftsführung der Filiale aufgefordert worden ist, sich an die organisatorischen Vorgaben zu halten. Außerdem werde auch die Beschilderung in der Filiale überprüft und gegebenenfalls erneuert.

Da in der letzten Zeit nicht nur mich, sondern auch meinen Kollegen in Schleswig-Holstein zunehmend Anfragen von Petenten zu dieser Thematik erreichen, haben wir die datenschutzrechtlichen Vorgaben bei der Erhebung personenbezogener Daten im EC-Lastschriftverfahren in einem Gespräch mit dem Einzelhandelsverband Nord-Ost e. V. erörtert. Der Einzelhandelsverband Nord-Ost vertritt rund 2.000 Mitgliedsunternehmen aus beiden Bundesländern.

Die Vertreter des Einzelhandelsverbandes haben bestätigt, dass Banken bei Problemfällen der Zahlung mit EC-Karte oft keine Auskunft über die Kundendaten erteilen (teilweise mit dem Argument „Datenschutz“). Solche Fälle seien in der Regel sowohl bei mangelnder Kontodeckung des Kunden als auch dann zu registrieren, wenn ein Kunde zunächst per EC-Karte zahlt, die Transaktion in den folgenden Tagen jedoch über seine Hausbank „zurückruft“, etwa weil er mit der Ware nicht zufrieden ist. In der Vergangenheit habe es hierzu bereits Gespräche mit dem zentralen Kreditausschuss der Banken gegeben, die allerdings bisher ohne Ergebnis verlaufen seien.

Die Erörterung der Datenschutzaufsichtsbehörden Schleswig-Holstein und Mecklenburg-Vorpommern mit dem Einzelhandelsverband wird fortgesetzt werden, um im Ergebnis nach Klärung der genauen Zahlungsabläufe mit den Verbandsmitgliedern zu einem Verfahren zu gelangen, das im Einklang mit den Bestimmungen des Bundesdatenschutzes steht und in möglichst großem Maße die beschriebenen praktischen Probleme des Einzelhandels beim EC-Lastschriftverfahren berücksichtigt.

11 Risiken beim Einsatz von Scoring – Verfahren

In den letzten Jahren kommen zunehmend so genannte Score- (oder Rating-)Verfahren zum Einsatz und werden als Grundlage für wirtschaftliche Entscheidungen gegenüber Dritten (insbesondere gegenüber Kunden) genutzt. Dabei handelt es sich um Verfahren, die auf mathematisch-statistischer Grundlage beruhen, nach denen Risikoklassen gebildet werden. Diesen Risikoklassen wird der individuelle Kaufinteressent, Kreditsuchende etc. zugeordnet und erhält auf dieser Basis einen bestimmten Score-Wert. Die Verfahren werden unter anderem von Versicherungen, Telekommunikationsunternehmen, vom Versandhandel und von Banken eingesetzt.

Während die Bewertung der Schuldnerbonität bei der Vergabe von Krediten bisher anhand einer Einschätzung des zuständigen Sachbearbeiters erfolgte, soll diese „subjektive“ Bewertung durch „objektive“ Bewertungsmaßstäbe ersetzt werden. Ziel ist eine Reduzierung von Kreditausfallrisiken, welche auch Einfluss auf die Ausfallrisikoversicherung hat.

Die Risiken des Kredit-Scoring für den Bankkunden liegen darin, dass er einer bestimmten statistischen Kategorie zugeordnet werden kann, die seinen individuellen Lebensumständen nicht gerecht wird. Ein weiteres Risiko bestünde dann, wenn der betroffene Kunde keinen Einblick darin erhält, welche seiner Daten verarbeitet werden und nach welchen Maßstäben aus diesen Daten innerhalb der im Verfahren eingesetzten Kategorien sein persönlicher Bewertungswert ermittelt worden ist.

Die zu der Ermittlung des Score-Wertes eingesetzten Daten müssen zu dem Kreditgeschäft in einem unmittelbaren Zusammenhang stehen. Grundsätzlich dürfen deshalb in diesem Zusammenhang keine Daten aus anderen Vertragsverhältnissen des Betroffenen zum Einsatz kommen. In unmittelbarem Zusammenhang zu dem Kreditgeschäft stehen beispielsweise Vermögen, Einkommen, Beruf, Sicherheiten, Schulden, bereits bestehende Kredite, Insolvenzverfahren etc. In diesem Zusammenhang sind demgegenüber Wohnumfeld, Religionszugehörigkeit, politische Überzeugung etc. nicht relevant und somit unzulässig.

Problematisch wäre beispielsweise auch eine negative Bewertung eines Bankkunden deshalb, weil sich der Kunde – etwa im Vorfeld eines Hausbaus – zum Kreditvergleich bei mehreren Bankinstituten über die Konditionen für einen Kredit informiert, jedoch keinen Vertrag abschließt, weil er zunächst Vergleichsangebote einholt. Soweit eine Bank aufgrund dieser Informationen auf mangelnde Kreditwürdigkeit des Kunden schließt, weil bei mehreren Kreditinstituten trotz Nachfrage kein Kredit zustande kam, handelt es sich um eine unzulässige Bewertung im Rahmen des Scoring-Verfahrens.

Die wachsende Verbreitung der Scoring-Verfahren ist insgesamt auch gesellschaftspolitisch problematisch, weil ein solches Verfahren der Einzelperson die Möglichkeit nehmen kann, über seinen äußeren Eindruck gegenüber Dritten frei zu entscheiden. Deshalb wird im Rahmen meiner Kontrollzuständigkeit die datenschutzrechtliche Bewertung dieser Verfahren von besonderer Bedeutung sein.

12 Einzugsermächtigung per Postkarte

Ein Petent sandte mir das Muster einer vorgefertigten Einzugsermächtigung eines Unternehmens. Es handelte sich um eine voradressierte Postkarte, die mit dem Hinweis versehen war, dass das Rückporto bereits bezahlt sei. Der Aufdruck auf der Rückseite der Karte enthielt die Rubriken: Kundennummer, Geldinstitut, Name und Anschrift des Kontoinhabers, Bankleitzahl, Kontonummer und die Unterschriftszeile des Kunden als Kontoinhaber.

Diese Art der Einzugsermächtigung legt dem Kunden nahe, sensible personenbezogene Daten ohne geschlossenen und somit schützenden Briefumschlag in den Postweg zu geben. Das Angebot, diesen ungeschützten Verfahrensweg zu wählen, wird zusätzlich verstärkt durch den Hinweis, dass das Unternehmen das Rückporto bereits bezahlt habe.

Es handelt sich hier aus meiner Sicht um eine Verfahrensweise, die datenschutzrechtlich bedenklich ist. Dies gilt ungeachtet der Tatsache, dass keine direkte Verletzung des Datenschutzrechts vorliegt, weil die Wahlfreiheit des Kunden unter mehreren Rücksendungsmöglichkeiten weiterhin besteht und er sich mit seiner Unterschrift und der Rücksendung in Form einer ungeschützten Postkarte für eben diese Übersendungsform entscheidet.

Dennoch ist das Verfahren problematisch, weil die Kunden in dem Postkartenvordruck nicht über die möglichen Risiken der offenen Versendung ihrer sensiblen Bankverbindungsdaten informiert werden. Vielmehr wird ihnen – gerade durch den Hinweis auf das bereits bezahlte Rückporto – nahe gelegt, mit ihrer Unterschrift unter die Einzugsermächtigung zugleich für ihre personenbezogenen Bankverbindungsdaten eine Versendungsform zu akzeptieren, die beispielsweise im Bankverkehr unter Gefährdungsgesichtspunkten nicht in Erwägung gezogen werden würde.

Ich habe deshalb das Unternehmen gebeten, auf eine Änderung der Verfahrensweise hinzuwirken, die sicherstellt, dass die Kundendaten in hinreichend geschützter Form übermittelt werden.

Das Unternehmen hat das kritisierte Verfahren inzwischen ausgesetzt und strebt für die Zukunft eine datenschutzfreundliche Verfahrensweise an, wobei der Kunde insbesondere Hinweise auf datenschutzgerechte, sichere Übersendungsalternativen erhalten soll.

13 Adresshandel und unerwünschte Werbepostsendungen

Viele Anfragen erhielt ich zu unerwünschter Werbepost. Insbesondere wollten die Betroffenen wissen, wie die werbenden Unternehmen an die Zustelladressen kommen, was sie selbst zum Schutz gegen die Weitergabe ihrer Adressen und die Zusendung von unerwünschter Post unternehmen können und inwieweit Adressen von Firmen weitergegeben werden dürfen.

Adressquelle für die Werbung von Unternehmen sind häufig Kundenbindungsprogramme und Rabattsysteme („ ... sammeln Sie Treuepunkte?“). Viele Betriebe bedienen sich auch der Adressbestände anderer Unternehmen und Organisationen oder führen Verlosungen und Preisausschreiben mit dem Ziel durch, an Anschriften und Informationen zu kommen, die für die Werbung genutzt werden können.

Vorsicht ist vor allem bei so genannten Gewinnmitteilungen angeraten. Häufig wird der Gewinn nicht ausgeschüttet, weil an verborgener Stelle auf die Unverbindlichkeit der Gewinnmitteilung hingewiesen wird. Oft ist der „Gewinn“ auch an bestimmte Bedingungen geknüpft, die den Vorteil des Gewinns aufheben.

Häufig beauftragen Betriebe andere Firmen, für sie zu werben, so dass bei dem werbenden Unternehmen selbst weder die Adresse des Betroffenen noch sonstige Informationen über ihn gespeichert sind. Adresshandelsunternehmen erhalten diese Daten aus allgemein zugänglichen Quellen (Adress- und Telefonbüchern, E-Mail-Verzeichnissen, Handels- und Vereinsregistern, Internetseiten etc.). Nicht selten werden diese Informationen zur Weitergabe an die werbeinteressierten Unternehmen auf spezielle Zielgruppen zugeschnitten (z. B. nach Altersgruppen – Senioren etc.).

Die Weitergabe und Nutzung der Adressen ist nach dem Bundesdatenschutzgesetz (BDSG) grundsätzlich auch ohne die Einwilligung des Betroffenen zulässig. Bestimmte personenbezogene Daten, wie etwa Berufs- oder Branchenbezeichnung, Name, Anschrift und auch Geburtsjahr, dürfen nach § 28 Abs. 3 BDSG für Werbezwecke genutzt und weitergegeben werden, solange nicht Grund zur Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung oder Nutzung hat.

Der wichtigste Anhaltspunkt zur Annahme, dass der Betroffene ein solches Interesse hat, ist dessen Widerspruch. Dieser kann oft schon beim Abschluss von Verträgen eingelegt werden, indem beispielsweise auf Vertragsformularen handschriftlich der Hinweis ergänzt wird, dass keine Übermittlung oder Nutzung zu Werbezwecken erwünscht ist. Der Vertragspartner ist dann verpflichtet, dies als Widerspruch zu akzeptieren.

Beabsichtigt ein Unternehmen, die von Betroffenen erhaltenen Daten auch für Werbezwecke zu nutzen, muss es bereits bei der Erhebung der Daten über diese Zwecke und über die möglichen Arten von Empfängern der Daten unterrichten (§ 4 Abs. 3 BDSG). Dies gilt auch bei Verlosungen und Preisausschreiben mit denen Daten gewonnen werden, die später zu Werbezwecken genutzt werden sollen.

Der Betroffene muss ferner mit dem Werbeschreiben über die so genannte verantwortliche Stelle (etwa das werbende Unternehmen) und über sein Widerspruchsrecht informiert werden. Beauftragt ein Betrieb ein anderes Unternehmen mit der Werbung (und sind die Adress- und Namensdaten nur bei dem beauftragten Unternehmen gespeichert), so muss der Betrieb auch sicherstellen, dass der Betroffene über die Herkunft der Daten Kenntnis erhalten kann (§ 28 Abs. 4 BDSG).

Nach § 34 Abs. 1 BDSG besteht gegenüber dem werbenden Unternehmen grundsätzlich ein Auskunftsrecht über die zu der Person des Betroffenen gespeicherten Daten, ihre Herkunft, den Zweck der Speicherung und die Empfänger bzw. Empfängerkategorien, an die die Daten gegebenenfalls weitergegeben werden. Nur wenn ein Adresshändler ein überwiegendes Interesse an der Wahrung eines Geschäftsgeheimnisses darlegt, kann er die Auskunft zu Herkunft und Empfänger der Daten verweigern. Zweckmäßig ist es, ein Auskunftsbegehren gleichzeitig an die betrieblichen Datenschutzbeauftragten der jeweiligen Unternehmen zu senden, die – oft besser als die Marketingabteilungen – über datenschutzrechtliche Bestimmungen informiert sind.

Schutz vor unadressierter Werbung bieten entsprechende Briefkastenaufkleber („Bitte keine Werbung“). Wird der Wunsch ignoriert, liegt ein Verstoß gegen das Gesetz gegen den unlauteren Wettbewerb vor. Gegen persönlich adressierte Werbung hilft ein Eintrag in die „Robinson-Liste“. Der Deutsche Direkt-Marketing-Verband (DDV) ermöglicht es Verbrauchern, sich hinsichtlich persönlich adressierter Werbepost in diese Liste aufnehmen zu lassen. Diejenigen Unternehmen, die dem DDV angeschlossen sind, werden dann benachrichtigt, dass die Person auf der Liste keine Werbung wünscht. Auf diese Weise können postalische Werbesendungen zumindest reduziert werden. Der Eintrag in die Liste gilt für fünf Jahre. Das Formular für die Aufnahme in die Robinson-Liste ist erhältlich bei:

DDV, Robinson-Liste, Postfach 14 01, 71243 Ditzingen, Telefonnummer 07156/951010 oder unter www.direktmarketing-info.de.

Schutz gegen Werbung per SMS bietet ein Online-Eintrag der Telefonnummer in die vom Interessenverband Deutsches Internet e. V. (I. D. I.) geführte SMS-Schutzliste (www.sms-robinson.de). Vom Eintrag in eine E-Mail-Robinsonliste ist eher abzuraten, da nicht auszuschließen ist, dass diese Listen selbst wieder für Werbemaßnahmen missbraucht werden.

Werbetreibende Betriebe und Unternehmen im Land sollten darauf achten, dass bei Werbeaktionen die Betroffenen über ihr Widerspruchsrecht informiert und ihre Auskunftsersuchen schnell und kooperativ bearbeitet werden. Insbesondere ist zu empfehlen, Aufträge für Werbeaktionen nur an „seriöse“ Adresshandelsfirmen zu vergeben und beispielsweise auf fragwürdige „Gewinnmitteilungsaktionen“ zu verzichten.

14 Austausch-MDA nicht gelöscht

Ein Petent hat sich an mich gewandt, weil die Daten aus seinem Mobile Digital Assistant (MDA, Handcomputer mit integriertem Mobiltelefon) in falsche Hände geraten waren. Der Petent hatte unter anderem Termine, Adressen und Telefonnummern von Geschäftspartnern auf dem Gerät gespeichert. Nach einem Defekt übergab er den MDA seinem Händler und erhielt ein Austauschgerät. Aufgrund des Fehlers konnte der Petent die auf dem Gerät gespeicherten Daten nicht mehr selbst löschen, deshalb beauftragte er seinen Händler schriftlich damit. Nach einiger Zeit erhielt der Petent einen Hinweis von einem Dritten, der den nunmehr reparierten MDA erhalten hatte und die immer noch darauf gespeicherten Daten fand. Der neue Besitzer hat die Daten auf Bitten des Petenten letztlich gelöscht und den Schaden so in Grenzen gehalten.

Meine Nachfragen haben ergeben, dass auch der Händler die Daten nicht löschen konnte. MDA lässt er nicht in der eigenen Werkstatt reparieren, sondern übergibt sie bestimmten Servicebetrieben. Der Händler ging davon aus, dass diese Betriebe eventuell vorhandene Daten löschen.

Damit hatte der Händler die Vorschriften zur Datenverarbeitung im Auftrag in § 11 Abs. 2 Bundesdatenschutzgesetz (BDSG) missachtet. Er wäre verpflichtet gewesen, den Auftrag schriftlich zu erteilen und sich davon zu überzeugen, ob der Servicebetrieb die Daten tatsächlich löscht (Auftragskontrolle nach der Anlage zu § 9 BDSG).

Ich habe den Händler auf diese Pflichten hingewiesen. Darüber hinaus habe ich den Händler daran erinnert, dass er auch dafür zu sorgen hat, dass die Daten beim Transport der Geräte nicht unbefugt gelesen oder verändert werden können (Weitergabekontrolle nach der Anlage zu § 9 BDSG).

Allen nicht-öffentlichen Stellen, die Daten im Auftrag verarbeiten lassen, empfehle ich, sich von der korrekten Abwicklung des Auftrages zu überzeugen (Auftragskontrolle nach der Anlage zu § 9 BDSG).

C Anhang

0 Anlagen

1 Übermittlung von Flugpassagierdaten an die US-Behörden

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 13. Februar 2004

Die Datenschutzbeauftragten des Bundes und der Länder bestärken die Bundesregierung darin, sich für Verbesserungen des Datenschutzes bei der Übermittlung von Flugpassagierdaten an die Zoll- und Sicherheitsbehörden der USA einzusetzen.

Durch einseitigen Rechtsakt haben die USA die Fluggesellschaften, die ihr Land anfliegen, unter Androhung teilweise empfindlicher Strafen verpflichtet, den US-Zoll- und Sicherheitsbehörden den Zugang zu ihren Reservierungsdatenbanken zu eröffnen, um anhand der darin enthaltenen Informationen über die Fluggäste mögliche terroristische oder kriminelle Aktivitäten frühzeitig zu erkennen. In den Reservierungsdatenbanken halten die an der Reisedurchführung beteiligten Stellen alle Informationen fest, die sie benötigen, um die Flugreise abzuwickeln. Es werden z.B. Name, Reiseverlauf, Buchungsstelle, Art der Bezahlung, bei Zahlung mit Kreditkarte deren Nummer, Sitzplatz, Essenswünsche, notwendige Reisevorkehrung wegen einer Erkrankung eines Fluggastes, Hotel- und Mietwagenreservierungen im Buchungssystem gespeichert. Teilweise sind die gespeicherten Daten sensitiv, weil sie Rückschlüsse auf die Gesundheit einzelner Fluggäste oder religiöse oder politische Anschauungen ermöglichen. Die US-Zollbehörden wollen alle Reservierungsdaten mindestens 3,5 Jahre speichern ungeachtet der Tatsache, ob gegen eine Person ein Verdachtsmoment vorlag oder nicht. Passagierdaten, die im Einzelfall überprüft wurden, sollen zudem weitere 8 Jahre gespeichert werden.

Die Datenschutzbeauftragten verkennen nicht, dass nach den Ereignissen des 11. Septembers 2001 ein erhöhtes Bedürfnis nach Sicherheit im Flugverkehr offensichtlich ist. Sie verschließen sich deshalb keineswegs Forderungen, die auf eine sichere Identifikation der Fluggäste zielen. Dennoch muss festgestellt werden, dass die Forderungen der USA weit über das hinausgehen, was erforderlich ist. Da die Reservierungsdatenbanken nicht für Sicherheitszwecke sondern zur Durchführung der Flugreisen angelegt werden, enthalten sie auch eine Vielzahl von Daten der Reisenden, die für eine Sicherheitsüberprüfung der Passagiere irrelevant sind.

Mit dem Zugriff ist wegen der teilweise hohen Sensibilität der Daten ein tiefer Eingriff in die Persönlichkeitsrechte der Betroffenen verbunden. Besonders hervorzuheben ist in diesem Zusammenhang, dass die US-Behörden hier aufgrund US-amerkanischen Rechts auf Datenbanken außerhalb ihres Hoheitsbereichs zugreifen. Die betroffenen Personen werden gegenüber dem Zugriff auf ihre Daten durch eine ausländische Stelle in ihren Datenschutzrechten weitgehend schutzlos gelassen. Ein vergleichbares Ansinnen deutscher Sicherheitsbehörden wäre schwerlich mit unserer Verfassung vereinbar.

Die Problematik kann sich weiter verschärfen, wenn die USA die Passagierdaten zukünftig auch im sog. CAPPS II - System einsetzen wollen. Dieses System ermöglicht sowohl einen automatisierten Abgleich mit Fahndungslisten als auch mit Informationen aus dem privaten

Sektor. Insbesondere sollen Kreditkarten- und Adressdaten mit Informationen aus der Kreditwirtschaft abgeglichen werden.

Die Europäische Kommission bemüht sich seit über einem Jahr in Verhandlungen darum, den Datenzugang der US-Behörden auf ein angemessenes Maß zu beschränken. Leider führten die Verhandlungen nur in Teilbereichen zum Erfolg. Die erzielten Ergebnisse in ihrer Gesamtheit gewähren den Reisenden keinen angemessenen Schutz ihrer Persönlichkeitsrechte. Dies hat die Gruppe nach Art. 29 der europäischen Datenschutzrichtlinie (EG-DSRL) in ihrer Stellungnahme vom 29.01.2004 deutlich herausgearbeitet. Die darin vertretenen Positionen werden von den Datenschutzbeauftragten ausdrücklich unterstützt. Dennoch beabsichtigt die Europäische Kommission das Ergebnis ihrer Verhandlungen als einen angemessenen Datenschutzstandard förmlich anzuerkennen. Die Datenschutzbeauftragten appellieren an die Bundesregierung, sich gegen diese Entscheidung der Kommission zu wenden. Wenn die Kommission diesen unbefriedigenden Verhandlungsergebnissen ein angemessenes Datenschutzniveau attestiert, setzt sie damit Maßstäbe sowohl für die Auslegung der EU-Datenschutzrichtlinie als auch für Verhandlungen mit anderen Staaten über die Anerkennung des dortigen Datenschutzniveaus. Die Bundesregierung sollte sich demgegenüber für eine Lösung einsetzen, die Sicherheitsaspekte und den Schutz der Persönlichkeitsrechte in ein angemessenes Verhältnis setzt. Insbesondere sind die Informationen ausdrücklich zu benennen, die für die Passagieridentifikation benötigt werden. Diese Daten können zu einem angemessenen Zeitpunkt vor dem Abflug bereitgestellt werden. Ein unmittelbarer pauschaler Zugriff auf europäische Datenbanken, wie er zur Zeit praktiziert wird, muss ausgeschlossen werden.

http://www.europa.eu.int/comm/internal_market/privacy/workingroup/wp2004/wpdocs04_de.htm

2 Entschließung zu Radio-Frequency Identification vom 20. November 2003

Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken

Entschließung der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre

(Übersetzung)

Radio-Frequency Identification (RFID) Technologie wird zunehmend für eine Reihe unterschiedlicher Zwecke eingesetzt. Während es Situationen gibt, in denen diese Technologie positive und günstige Auswirkungen hat, sind auch negative Folgen für Privatsphäre möglich. RFID-Etiketten werden bisher vorwiegend zur Identifikation und Organisation von Gegenständen (Produkten), zur Kontrolle der Logistik oder zum Schutz der Authentizität einer Produktmarke (Warenzeichen) verwendet; sie können aber auch mit personenbezogenen Informationen wie Kreditkarten-Daten verknüpft werden und auch zur Erhebung solcher Informationen oder zur Lokalisierung oder Profilbildung über Personen benutzt werden, die Gegenstände mit RFID-Etiketten besitzen. Diese Technologie würde die unbemerkte Verfolgung und das Aufspüren von Individuen ebenso wie die Verknüpfung erhobener Daten mit bestehenden Datenbanken ermöglichen.

Die Konferenz hebt die Notwendigkeit hervor, Datenschutzprinzipien zu berücksichtigen, wenn RFID-Etiketten verknüpft mit personenbezogenen Daten eingeführt werden sollen. Alle Grundsätze des Datenschutzrechts müssen beim Design, der Einführung und der Verwendung von RFID-Technologie berücksichtigt werden. Insbesondere

a. sollte jeder Datenverarbeiter vor der Einführung von RFID-Etiketten, die mit personenbezogenen Daten verknüpfbar sind oder die zur Bildung von Konsumprofilen führen zunächst Alternativen in Betracht ziehen, die das gleiche Ziel ohne die Erhebung von personenbezogenen Informationen oder die Bildung von Kundenprofilen erreichen;

b. wenn der Datenverarbeiter darlegen kann, dass personenbezogene Daten unverzichtbar sind, müssen diese offen und transparent erhoben werden;

c. dürfen personenbezogene Daten nur für den speziellen Zweck verwendet werden, für den sie ursprünglich erhoben wurden und sie dürfen nur solange aufbewahrt werden, wie es zu Erreichung dieses Zwecks erforderlich ist und

d. soweit RFID-Etiketten im Besitz von Personen sind, sollten diese die Möglichkeit zur Löschung der gespeicherten Daten oder zur Deaktivierung oder Zerstörung der Etiketten haben. Diese Grundsätze sollten bei der Gestaltung und bei der Verwendung von Produkten mit RFID berücksichtigt werden.

Das Auslesen und die Aktivierung von RFID-Etiketten aus der Ferne ohne vernünftige Gelegenheit für den Besitzer des etikettierten Gegenstandes, diesen Vorgang zu beeinflussen, würde zusätzliche Datenschutzrisiken auslösen.

Die Konferenz und die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation wird die technischen Entwicklungen in diesem Bereich genau und detaillierter verfolgen, um die Achtung des Datenschutzes und der Privatsphäre in einer Umgebung allgegenwärtiger Datenverarbeitung sicherzustellen.

3 Entscheidungen des Bundesverfassungsgerichts vom 3. März 2004 zum Großen Lauschangriff und zur präventiven Telekommunikationsüberwachung

Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken

Das Urteil des Bundesverfassungsgerichts vom 3. März 2004 zum Großen Lauschangriff ist ein wichtiger Orientierungspunkt in der rechts- und sicherheitspolitischen Diskussion um den sachgerechten Ausgleich zwischen dem staatlichen Auftrag zur Verfolgung und Verhütung von Straftaten einerseits und dem Schutz der grundgesetzlich garantierten Bürgerrechte andererseits. Das Urteil bekräftigt den hohen Rang des Grundrechts auf Unverletzlichkeit der Wohnung und des Rechts auf informationelle Selbstbestimmung. Das Gericht betont, dass der absolut geschützte Kernbereich privater Lebensgestaltung nicht zugunsten der Strafverfolgung eingeschränkt werden darf. Damit darf es keine Strafverfolgung um jeden grundrechtlichen Preis geben.

Die Ausführungen des Bundesverfassungsgerichts sind nicht nur für die Vorschriften über die akustische Wohnraumüberwachung in der Strafprozessordnung von Bedeutung. Auf den Prüfstand müssen jetzt auch andere Eingriffsbefugnisse, wie etwa die Telekommunikationsüberwachung und andere Formen der verdeckten Datenerhebung mit zwangsläufigen Berührungen zum Bereich privater Lebensgestaltung gestellt werden, wie etwa die längerfristige Observation, der verdeckte Einsatz technischer Mittel, der Einsatz von Vertrauenspersonen oder von verdeckten Ermittlern. Hiervon betroffen sind nicht nur Bundesgesetze, sondern beispielsweise auch die Polizei- und Verfassungsschutzgesetze der Länder.

Insbesondere angesichts zunehmender Bestrebungen, auch die Telefonüberwachung für präventive Zwecke in Polizeigesetzen zuzulassen, ist darauf hinzuweisen, dass das Bundesverfassungsgericht in einem Beschluss zum Außenwirtschaftsgesetz ebenfalls am 3. März 2004 der präventiven Überwachung des Postverkehrs und der Telekommunikation klare Grenzen gesetzt hat.

Die Datenschutzbeauftragten fordern die Gesetzgeber des Bundes und der Länder deshalb auf, zügig die einschlägigen Vorschriften nach den Maßstäben der verfassungsgerichtlichen Entscheidungen vom 3. März 2004 zu korrigieren. Die mit der praktischen Durchführung der gesetzlichen Eingriffsbefugnisse befassten Gerichte, Staatsanwaltschaften und die Polizeien sind aufgerufen, die Vorgaben des Gerichts schon jetzt zu beachten.

4 Automatische Kfz-Kennzeichenerfassung durch die Polizei

Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken

Die Datenschutzbeauftragten des Bundes und der Länder betrachten einen anlassfreien und lageunabhängigen Einsatz von automatischen Kfz-Kennzeichen-Lesesystemen im Straßenverkehr mit Sorge, weil sich diese Maßnahmen zu einem weiteren Schritt zur Überwachung aller Bürgerinnen und Bürger entwickeln können. Es ist zu befürchten, dass mit dem Einsatz der automatischen Kfz-Kennzeichenerfassung eine neue Infrastruktur geschaffen wird, die künftig noch weit tiefer gehende Eingriffe in das Persönlichkeitsrecht ermöglicht.

Die Nutzung dieser neuen Technik hätte zur Folge, dass die Kfz-Kennzeichen aller an den Erfassungsgeräten vorbeifahrenden Verkehrsteilnehmerinnen und -teilnehmer erfasst und mit polizeilichen Fahndungsdateien abgeglichen würden. Schon der mit der Feststellung gesuchter Fahrzeuge verbundene Abgleich würde zu einem neuen Eingriff in das Recht auf informationelle Selbstbestimmung von Personen führen, die weit überwiegend keinen Anlass für eine polizeiliche Verarbeitung ihrer personenbezogenen Daten gegeben haben.

Auf jeden Fall muss ausgeschlossen werden, dass Daten über unverdächtige Personen gespeichert werden und dass ein allgemeiner Datenabgleich mit polizeilichen Informationssystemen durchgeführt wird.

Die Datenschutzbeauftragten weisen darauf hin, dass schon mehrere Länder eine Kfz-Kennzeichen-Erfassung ablehnen.

5 Personennummern

Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken

Das Bundesverfassungsgericht hat schon in seinem „Volkszählungsurteil“ aus dem Jahre 1983 besonders betont, dass ein Personenkennzeichen nicht verfassungsgemäß ist. Deshalb gibt die Einführung von einheitlichen Personennummern z.B. im Steuerbereich oder auch im Arbeits-, Gesundheits- und Sozialbereich Anlass zu grundsätzlicher Kritik. Der Staat darf seine Bürgerinnen und Bürger nicht zur Nummer abstempeln. Durch die technische Entwicklung sind vorhandene Dateien leicht miteinander zu verknüpfen und könnten zu einer vom Bundesverfassungsgericht strikt abgelehnten allgemeinen Personennummer führen.

Die Konferenz appelliert an die Gesetzgeber, solche Personennummern zu vermeiden. Soweit jedoch im Einzelfall derartige Nummern unerlässlich sind, muss der Gesetzgeber strenge Zweckbindungen und Verwendungsverbote vorsehen.

6 Einführung eines Forschungsgeheimnisses für medizinische Daten

Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. März 2004 in Saarbrücken

In vielen Bereichen der Forschung werden sensible medizinische Daten der Bürgerinnern und Bürger verarbeitet. Dabei ist häufig eine Verarbeitung auch personenbezogener Daten erforderlich. Diese Daten können mit Einwilligung der Betroffenen insbesondere von Ärztinnen und Ärzten, aber auch von Angehörigen anderer Heilberufe an Forscher und Forscherinnen übermittelt werden. Dies ist im Interesse der Forschung zwar grundsätzlich zu begrüßen. Mit der Übermittlung verlieren die Daten aber regelmäßig den strafrechtlichen Schutz vor Offenbarung und den Beschlagnahmeschutz im Strafverfahren. Auch ein Zeugnisverweigerungsrecht bezüglich dieser Daten steht den Forschenden - anders als insbesondere den behandelnden Ärztinnen und Ärzten - nicht zu. Zum Schutze der Forschung, vor allem aber zum Schutz der durch die Datenübermittlung und -verarbeitung Betroffenen, sollte vom Gesetzgeber deshalb sichergestellt werden, dass die bei den übermittelnden Stellen geschützten personenbezogenen medizinischen Daten auch nach ihrer Übermittlung zu Forschungszwecken den gleichen Schutz genießen.

Die Datenschutzbeauftragten fordern daher den Bundesgesetzgeber auf,

in § 203 StGB die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe zu stellen,

in §§ 53, 53 a StPO für personenbezogene medizinische Daten ein Zeugnisverweigerungsrecht für Forscher und ihre Berufshelfer zu schaffen,

in § 97 StPO ein Verbot der Beschlagnahme personenbezogener medizinischer Forschungsdaten zu schaffen.

Die Datenschutzbeauftragten sehen in diesen Vorschlägen einen ersten Schritt zu einer generellen Regelung des besonderen Schutzes personenbezogener Daten in der Forschung.

7 Beteiligung der GEZ am Adresshandel (8. Rundfunkänderungsstaatsvertrag)

Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. Oktober 2004 in Saarbrücken

Die für die Rundfunkanstalten zuständigen Datenschutzbeauftragten haben im Rahmen der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu dem 8. Rundfunkänderungsstaatsvertrag nachstehende Feststellung getroffen.

Die Datenschutzbeauftragten des Bundes und der Länder haben sich wiederholt dafür eingesetzt, bei der Finanzierung des öffentlich-rechtlichen Rundfunks in Deutschland das Prinzip von Datenvermeidung und Datensparsamkeit in stärkerem Maße zu berücksichtigen. In der Kritik steht dabei im Besonderen die Beschaffung von jährlich mehreren Millionen Adressen hinter dem Rücken der Betroffenen beim kommerziellen Adresshandel durch die von den Rundfunkanstalten beauftragte Gebühreneinzugszentrale (GEZ), die diese Adressen für flächendeckende Mailing-Aktionen nutzt. Zahlreiche Beschwerden und Anfragen von Bürgerinnen und Bürgern beziehen sich auf diese Praxis der GEZ, die die zuständigen Landesdatenschutzbeauftragten als rechtswidrig bezeichnet haben.

Anstatt gemeinsam mit den Datenschutzbeauftragten datenschutzfreundliche Varianten einer gerechten Finanzierung des öffentlich-rechtlichen Rundfunks ernsthaft zu prüfen, haben die Ministerpräsidenten der Länder mit dem Entwurf eines 8. Rundfunkänderungsstaatsvertrages neben der Erhöhung der Rundfunkgebühren und deren Erstreckung auf Computer weitgehend ohne die gebotene Beteiligung der zuständigen Landesdatenschutzbeauftragten eine weitere Verschlechterung des Datenschutzes beschlossen:

Um die Beschaffung von Daten beim kommerziellen Adresshandel gesetzlich zu legitimieren, soll der Rundfunkgebührenstaatsvertrag um eine Befugnis erweitert werden, nach der die Rundfunkanstalten und die GEZ personenbezogene Daten unter den gleichen Bedingungen verarbeiten dürfen wie privatwirtschaftliche Unternehmen.

Die vorgesehene Befugnis ist mit datenschutzrechtlichen Grundsätzen nicht zu vereinbaren. Während öffentlich-rechtliche Institutionen personenbezogene Daten nur verarbeiten dürfen, wenn dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist, ist die Datenverarbeitung der im Wettbewerb stehenden Privatwirtschaft vom Prinzip der Vertragsfreiheit geprägt. Die öffentlich-rechtlichen Rundfunkanstalten stehen hinsichtlich des Gebühreneinzugs in keinem Wettbewerb zu anderen Rundfunkveranstaltern. Schließlich haben die Länder gegen das Votum der Datenschutzbeauftragten bereits vor Jahren regelmäßige Übermittlungen von Meldedaten an die Rundfunkanstalten zugelassen, weil dies für erforderlich gehalten wurde. Eine parallele Nutzung von Daten aus den Melderegistern bei gleichzeitiger Beschaffung von Adressen im privaten Adresshandel ist jedoch unverhältnismäßig.

Zudem wird durch die ohnehin fragwürdige Befugnis das Ziel der Rundfunkanstalten nicht erreicht. Auch bei einem Inkrafttreten der vorgesehenen Regelung bliebe die Beschaffung von Adressen beim kommerziellen Adresshandel durch die GEZ rechtswidrig, da sich die Erhebung von personenbezogenen Daten bei Dritten ohne Kenntnis der Betroffenen weiterhin nach dem maßgeblichen Landesrecht richtet.

Die Konferenz hat davon Kenntnis genommen.

8 Gravierende Datenschutzmängel bei Hartz IV

Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. Oktober 2004 in Saarbrücken

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass es bei der praktischen Umsetzung der Zusammenlegung von Arbeitslosen- und Sozialhilfe zu erheblichen datenschutzrechtlichen Mängeln gekommen ist. Diese bestehen sowohl bei den Verfahren der Datenerhebung durch die verwendeten Antragsformulare als auch bei der Leistungsberechnungs-Software (A2LL). Die Datenschutzdefizite wären vermeidbar gewesen, wenn datenschutzrechtliche Belange von Anfang an angemessen berücksichtigt und umgesetzt worden wären.

Zwar stellt die Bundesagentur für Arbeit (BA) seit dem 20.09.2004 sog. „Ausfüllhinweise zum Antragsvordruck Arbeitslosengeld II“ zur Verfügung, in denen viele Bedenken der Datenschutzbeauftragten aufgegriffen werden. Allerdings ist hierbei zu berücksichtigen, dass durch die Ausfüllhinweise nicht mehr alle antragstellenden Personen erreicht werden können. Umso wichtiger ist es, dass die örtlich zuständigen Leistungsträger die verbindlichen Ausfüllhinweise beachten und die antragstellenden Personen, die ihren Antrag noch nicht eingereicht haben, vor der Abgabe auf diese hingewiesen werden. Personen, die ihren Antrag früher gestellt haben, dürfen nicht benachteiligt werden. Überschussinformationen, die vorhanden sind und weiterhin erhoben werden, sind zu löschen.

Darüber hinaus will die BA die in den Antragsformularen nachgewiesenen Datenschutzmängel in vielen Bereichen in der nächsten Druckauflage korrigieren und für das laufende Erhebungsverfahren zur Verfügung stellen. Gleichwohl ist zu befürchten, dass die Formulare nicht das erforderliche Datenschutzniveau erreichen.

Hinsichtlich der Software A2LL bestehen immer noch wesentliche Datenschutzmängel, die zu erheblichen Sicherheitsrisiken führen. Insbesondere besteht für die Sachbearbeitung ein uneingeschränkter bundesweiter Zugriff auf alle Daten, die im Rahmen von A2LL erfasst wurden, auch soweit diese Daten für die Sachbearbeitung nicht erforderlich sind. Dieser Mangel wird dadurch verschärft, dass noch nicht einmal eine Protokollierung der lesenden Zugriffe erfolgt und damit missbräuchliche Zugriffe nicht verfolgt werden können. Das Verfahren muss über ein klar definiertes Zugriffsberechtigungskonzept verfügen. Die Beschäftigten der zuständigen Leistungsträger dürfen nur den zur Aufgabenerfüllung erforderlichen Zugriff auf die Sozialdaten haben.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die BA auf, die notwendigen Schritte unverzüglich einzuleiten und nähere Auskunft über den Stand des Verfahrens zu erteilen.

9 Datensparsamkeit bei der Verwaltungsmodernisierung

Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. Oktober 2004 in Saarbrücken

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Bemühungen, Dienstleistungen der öffentlichen Verwaltung bürgernäher und effizienter zu erbringen. Sie fordern, dass im Zug von Maßnahmen der Verwaltungsreform die sich dadurch bietenden Möglichkeiten genutzt werden, um das Datenschutzniveau zu verbessern. Verwaltungsvereinfachung muss auch dazu genutzt werden, weniger personenbezogene Daten zu verarbeiten. Künftig müssen Verfahren und Datenflüsse wesentlich besser überschaubar und nachvollziehbar sein. Besonders sollen die Möglichkeiten der Technik genutzt werden, Risiken zu minimieren, die mit der Zentralisierung von Datenbeständen verbunden sind.

Werden Rechtsvorschriften, etwa im Steuerrecht oder im Arbeits- und Sozialrecht und hier insbesondere bei Änderungen in den Systemen der sozialen Sicherung, mit dem Ziel der Verwaltungsvereinfachung erlassen, sind die Auswirkungen auf den Datenschutz frühzeitig zu prüfen. Im Ergebnis müssen die Normen den gesetzlich verankerten Grundsatz der Datenvermeidung umsetzen und somit das Recht auf informationelle Selbstbestimmung gewährleisten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deswegen, bei Vorschlägen zur Verwaltungsvereinfachung und darüber hinaus bei allen Regelungsvorhaben darauf zu achten, dass das damit verbundene Potential an Datensparsamkeit und Transparenz ausgeschöpft wird.

Hierzu ist eine Folgenabschätzung auf mögliche Beeinträchtigungen der informationellen Selbstbestimmung vorzunehmen. Die Ergebnisse sind in geeigneter Form zu dokumentieren.

10 Gesetzentwurf der Bundesregierung zur Neuregelung der akustischen Wohnraumüberwachung

Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. Oktober 2004 in Saarbrücken

Die Bundesregierung hat einen Gesetzentwurf zur Neuregelung der akustischen Wohnraumüberwachung vorgelegt. Sie setzt damit in großen Teilen das Urteil des Bundesverfassungsgerichts vom 3. März 2004 um, wonach die Vorschriften der Strafprozessordnung zum „großen Lauschangriff“ in wesentlichen Teilen verfassungswidrig sind. Allerdings sind zentrale Punkte, wie die Begriffsbestimmung des „unantastbaren Kernbereichs der privaten Lebensgestaltung“ und die Bestimmung des Kreises der Menschen „des persönlichen Vertrauens“ offen geblieben.

Ungeachtet dessen drohen im weiteren Verlauf des Gesetzgebungsverfahrens schwerwiegende Verschlechterungen: So wird diskutiert, die Vorgaben des Bundesverfassungsgerichts dadurch zu unterlaufen, dass auch bei erkannten Eingriffen in den absolut geschützten Kernbereich die technische Aufzeichnung fortgesetzt wird. Dies steht in eklatantem Widerspruch zur eindeutigen Vorgabe des Bundesverfassungsgerichts, die Aufzeichnung in derartigen Fällen sofort zu beenden. Darüber hinaus wird versucht, den Anwendungsbereich der akustischen Wohnraumüberwachung dadurch auszuweiten, dass auch nicht strafbare Vorbereitungshandlungen einbezogen werden. Auch dies widerspricht den verfassungsgerichtlichen Vorgaben und verwischt die Grenzen zwischen Strafverfolgung und Gefahrenabwehr.

Die Datenschutzbeauftragten bekräftigen im Übrigen ihre Forderung, dass es im Hinblick auf die Heimlichkeit der Überwachung und ihrer zwangsläufigen Berührung mit dem Kernbereich privater Lebensgestaltung erforderlich ist, alle Formen der verdeckten Datenerhebung an den Maßstäben der verfassungsgerichtlichen Entscheidung vom 3. März 2004 zu messen und auszurichten sowie die einschlägigen gesetzlichen Befugnisregelungen des Bundes und der Länder auf den Prüfstand zu stellen und gegebenenfalls neu zu fassen. Dies gilt etwa für die präventive Telekommunikationsüberwachung, die längerfristige Observation, den verdeckten Einsatz technischer Mittel, den Einsatz nachrichtendienstlicher Mittel und von verdeckten Ermittlern. Dabei sind insbesondere Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung und zum Schutz vertraulicher Kommunikation mit engsten Familienangehörigen und andern engsten Vertrauten sowie mit Personen, die einem Berufsgeheimnis unterliegen, zur Einhaltung der Zweckbindung bei Weiterverwendung der durch die Eingriffsmaßnahmen erlangten Daten, zu der dazu erforderlichen Kennzeichnungspflicht und zur Benachrichtigung aller von der Eingriffsmaßnahme Betroffenen sowie zur detaillierten Ausgestaltung von Berichtspflichten gegenüber den Parlamenten vorzusehen.

11 Staatliche Kontrolle muss auf den Prüfstand!

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 26. November 2004

Das „Gesetz zur Förderung der Steuerehrlichkeit“ vom 23.12.2003 (BGBl. I 2003, S. 2928) enthält mit den §§ 93 Abs. 7, 8 und 93 b der Abgabenordnung Regelungen, die das Grundrecht auf informationelle Selbstbestimmung aller Bürgerinnen und Bürger im Bereich ihrer finanziellen und wirtschaftlichen Betätigung in erheblichem Maße beschränken. Die neuen Regelungen treten am 1. April 2005 in Kraft. Sie sehen vor, dass nicht nur Finanzbehörden, sondern auch eine unbestimmte Vielzahl weiterer Behörden Zugriff auf Bankdaten erhalten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, diese Regelungen mit dem Ziel zu überarbeiten, das Recht auf informationelle Selbstbestimmung zu gewährleisten. Insbesondere das verfassungsrechtliche Gebot der Normenklarheit und die Transparenz des Verfahrens müssen beachtet werden.

Die Neuregelung erlaubt einen Zugriff auf Bankdaten, die von den Kreditinstituten bereits seit April 2003 zur Aufdeckung illegaler Finanztransaktionen vor allem zur Terrorismusbekämpfung nach § 24 c des Kreditwesengesetzes vorgehalten werden müssen. Dabei handelt es sich um die Kontenstammdaten der Bankkundinnen und Bankkunden und sonstigen Verfügungsberechtigten, wie z.B. Name, Geburtsdatum, Kontonummern. Mit der neuen Regelung einher geht bereits eine von den Datenschutzbeauftragten des Bundes und der Länder im Gesetzgebungsverfahren Ende 2003 kritisierte Zweckänderung der Verwendung der von den Kreditinstituten vorzuhaltenden Daten.

Nunmehr sollen neben Finanzbehörden auch andere Behörden, z.B. die zahlreichen Stellen der Sozialleistungsträger, Auskunft erhalten, wenn die anfragende Behörde ein Gesetz anwendet, das „an Begriffe des Einkommensteuergesetzes“ anknüpft und eigene Ermittlungen dieser Behörde ihrer Versicherung nach nicht zum Ziel geführt haben oder keinen Erfolg versprechen. Welche Behörden dies sein sollen, geht aus dem Gesetz nicht eindeutig hervor. Da das Einkommensteuerrecht eine Vielzahl von „Begriffen“ verwendet (neben den Begriffen „Einkommen“ und „Einkünfte“ etwa auch „Wohnung“, „Kindergeld“, „Arbeitnehmer“), ist wegen fehlender Begriffsbestimmungen nicht abschließend bestimmbar, welche Behörden die Auskunftsersuchen stellen dürfen. Dies jedoch ist nach dem verfassungsrechtlichen Bestimmtheitsgebot unverzichtbar. Zudem wird nicht deutlich, welche Zwecke ein Auskunftsersuchen rechtfertigen und nach welchen Regeln sie erfolgen sollen.

Von der Tatsache des Datenabrufs erfahren Kreditinstitute und Betroffene zunächst nichts. Die Betroffenen erhalten hiervon allenfalls bei einer Diskrepanz zwischen ihren Angaben (z.B. anlässlich Steuererklärung, BafögG-Antrag) und den Ergebnissen der Kontenabfragen Kenntnis, nicht jedoch bei einer Bestätigung ihrer Angaben durch die Kontenabfragen. Die Auskunft erstreckt sich zwar nicht auf die Kontostände; auf Grund der durch den Abruf erlangten Erkenntnisse können jedoch in einem zweiten Schritt weitere Überprüfungen, dann auch im Hinblick auf die Guthaben direkt beim Kreditinstitut erfolgen.

Dass Betroffene von Abfragen, die zu keiner weiteren Überprüfung führen, nichts erfahren, widerspricht dem verfassungsrechtlichen Transparenzgebot. Danach sind sie von der Speicherung und über die Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen

der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Geschieht dies nicht, hat das zur Konsequenz, dass die Rechtsschutzgarantie des Art. 19 Abs. 4 Grundgesetz verletzt wird. Die Bürgerinnen und Bürger haben einen substantiellen Anspruch auf eine tatsächlich wirksame gerichtliche Kontrolle (s. Volkszählungsurteil, BVerfGE 65, 1, 70).

12 Keine Gleichsetzung der DNA-Analyse mit dem Fingerabdruck

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 17. Februar 2005

Die strafprozessuale DNA-Analyse ist – insbesondere in Fällen der Schwerstkriminalität wie bei Tötungsdelikten – ein effektives Fahndungsmittel. Dies hat zu Forderungen nach der Ausweitung ihres Anwendungsbereichs zur Identitätsfeststellung in künftigen Strafverfahren geführt. So sieht ein Gesetzesantrag mehrerer Bundesländer zum Bundesratsplenum vom 18. Februar 2005 die Streichung des Richtervorbehalts und der materiellen Erfordernisse einer Anlasstat von erheblicher Bedeutung sowie der Prognose weiterer schwerer Straftaten vor.

Das zur Begründung derartiger Vorschläge herangezogene Argument, die DNA-Analyse könne mit dem herkömmlichen Fingerabdruck gleichgesetzt werden, trifft jedoch nicht zu:

Zum einen hinterlässt jeder Mensch permanent Spurenmaterial z. B. in Form von Hautschuppen oder Haaren. Dies ist ein Grund für den Erfolg des Fahndungsinstruments „DNA-Analyse“, weil sich Täter vor dem Hinterlassen von Spuren nicht so einfach schützen können, wie dies bei Fingerabdrücken möglich ist. Es birgt aber – auch unter Berücksichtigung der gebotenen vorsichtigen Beweiswürdigung – in erhöhtem Maße die Gefahr, dass Unbeteiligte aufgrund zufällig hinterlassener Spuren am Tatort unberechtigten Verdächtigungen ausgesetzt werden oder dass sogar bewusst DNA-Material Dritter am Tatort ausgestreut wird.

Zum anderen lassen sich bereits nach dem derzeitigen Stand der Technik aus den sog. nicht-codierenden Abschnitten der DNA über die Identitätsfeststellung hinaus Zusatzinformationen entnehmen (Verwandtschaftsbeziehungen, wahrscheinliche Zugehörigkeit zu ethnischen Gruppen, aufgrund der räumlichen Nähe einzelner nicht-codierender Abschnitte zu codierenden Abschnitten möglicherweise Hinweise auf bestimmte Krankheiten). Die Feststellung des Geschlechts ist bereits nach geltendem Recht zugelassen. Nicht absehbar ist schließlich, welche zusätzlichen Erkenntnisse aufgrund des zu erwartenden Fortschritts der Analysetechniken zukünftig möglich sein werden.

Mit gutem Grund hat daher das Bundesverfassungsgericht in zwei Entscheidungen aus den Jahren 2000 und 2001 die Verfassungsmäßigkeit der DNA-Analyse zu Zwecken der Strafverfolgung nur im Hinblick auf die derzeitigen Voraussetzungen einer vorangegangenen Straftat von erheblicher Bedeutung, einer Prognose weiterer schwerer Straftaten und einer richterlichen Anordnung bejaht. Es hat besonders gefordert, dass diese Voraussetzungen auch nach den Umständen des Einzelfalls gegeben sein müssen und von der Richterin oder dem Richter genau zu prüfen sind.

Eine Prognose schwerer Straftaten und eine richterliche Anordnung müssen im Hinblick auf diese Rechtsprechung und den schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung, den die DNA-Analyse darstellt, auch zukünftig Voraussetzung einer derartigen Maßnahme bleiben.

Die besondere Qualität dieses Grundrechtseingriffs muss auch im Übrigen bei allen Überlegungen, die derzeit zu einer möglichen Erweiterung des Anwendungsbereichs der DNA-Analyse angestellt werden, den Maßstab bilden; dies schließt eine Gleichsetzung in der Anwendung dieses besonderen Ermittlungswerkzeugs mit dem klassischen Fingerabdruckverfahren aus.

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

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

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

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

14 Entschließung zur Einführung der elektronischen Gesundheitskarte

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

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

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

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

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

15 Einführung biometrischer Ausweisdokumente

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 1. Juni 2005

Obwohl die Verordnung Nr. 2252/2004 des Europäischen Rates vom 13. Dezember 2004 die Mitgliedstaaten verpflichtet, bis Mitte 2006 mit der Ausgabe biometriegestützer Pässe für die Bürgerinnen und Bürger der Europäischen Union zu beginnen, sollen in Deutschland noch im laufenden Jahr die ersten Pässe ausgegeben werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist der Auffassung, dass mit der Ausgabe von elektronisch lesbaren biometrischen Ausweisdokumenten erst begonnen werden kann, wenn die technische Reife, der Datenschutz und die technische und organisatorische Sicherheit der vorgesehenen Verfahren gewährleistet sind. Diese Voraussetzungen sind bisher jedoch noch nicht in ausreichendem Maße gegeben.

Daher sind in einem umfassenden Datenschutz- und IT-Sicherheitskonzept zunächst technische und organisatorische Maßnahmen zur Wahrung des Rechts auf informationelle Selbstbestimmung festzulegen. Darüber hinaus sind im Passgesetz Regelungen zur strikten Zweckbindung der Daten erforderlich.

Die Konferenz begrüßt das Eintreten des Europäischen Parlaments für verbindliche Mindestanforderungen biometriegestützter Pässe zur Verhinderung des Missbrauchs, insbesondere des heimlichen Auslesens und der Manipulation der Daten. Die Konferenz bedauert es jedoch, dass die Einführung dieser Pässe beschlossen wurde, ohne dass die Chancen und Risiken der Technik ausreichend diskutiert wurden. Besonders problematisch ist es, dass die Entscheidung durch den Europäischen Rat der Regierungsvertreter entgegen der entsprechenden Stellungnahme des Europäischen Parlaments und der nationalen Gesetzgeber der EU-Mitgliedstaaten getroffen wurde.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass die Einführung biometrischer Merkmale nicht automatisch zur Verbesserung der Sicherheit führt. Noch immer weisen manche biometrische Identifikationsverfahren hohe Falscherkennungsraten auf und sind oft mit einfachsten Mitteln zu überwinden. Scheinbar besonders sichere Ausweisdokumente werden durch den Einsatz unsicherer biometrischer Verfahren somit plötzlich zu einem Risikofaktor. Fehler bei der Erkennung von Personen haben zudem erhebliche Konsequenzen für die Betroffenen, weil sie einem besonderen Rechtfertigungsdruck und zusätzlichen Kontrollmaßnahmen ausgesetzt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine objektive Bewertung von biometrischen Verfahren und tritt dafür ein, die Ergebnisse entsprechender Untersuchungen und Pilotprojekte zu veröffentlichen und die Erkenntnisse mit der Wissenschaft und der breiten Öffentlichkeit zu diskutieren. Mit der Ausgabe von elektronisch lesbaren, biometrischen Ausweisdokumenten darf erst begonnen werden, wenn durch rechtliche, organisatorische und technische Maßnahmen gewährleistet wird,

- dass die biometrischen Merkmale ausschließlich von den für die Passkontrollen zuständigen Behörden für hoheitliche Zwecke genutzt werden,

- dass die in Ausweisen gespeicherten Daten mit den biometrischen Merkmalen nicht als Referenzdaten genutzt werden, um Daten aus unterschiedlichen Systemen und Kontexten zusammenzuführen,
- dass die für die Ausstellung und das Auslesen verwendeten Geräte nach internationalen Standards von einer unabhängigen Stelle zertifiziert werden,
- dass die verwendeten Lesegeräte in regelmäßigen zeitlichen Intervallen durch eine zentrale Einrichtung authentisiert werden,
- dass eine verbindliche Festlegung der zur Ausgabe oder Verifikation von Dokumenten zugriffsberechtigten Stellen erfolgt,
- dass vor der Einführung biometrischer Ausweise Verfahren festgelegt werden, die einen Datenmissbrauch beim Erfassen der Referenzdaten (sicheres Enrollment), beim weiteren Verfahren und bei der Kartennutzung verhindern,
- dass diese Verfahrensfestlegungen durch eine unabhängige Stelle evaluiert werden.

Darüber hinaus muss sichergestellt sein, dass keine zentralen oder vernetzten Biometriedatenbanken geschaffen werden. Die biometrischen Identifizierungsdaten dürfen ausschließlich auf dem jeweiligen Ausweisdokument gespeichert werden. Durch international festzulegende Standards sowie Vorschriften und Vereinbarungen ist anzustreben, dass die bei Grenzkontrollen erhobenen Ausweisdaten weltweit nur gemäß eines noch festzulegenden einheitlichen hohen Datenschutz- und IT-Sicherheitsstandards verarbeitet werden.

16 Unabhängige Datenschutzkontrolle in Deutschland gewährleisten

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

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

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

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

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

17 Schutz des Kernbereichs privater Lebensgestaltung bei verdeckten Datenerhebungen der Sicherheitsbehörden

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

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

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

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

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

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

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

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

18 Telefonieren mit Internettechnologie (Voice over IP - VoIP)

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

Die Internet-Telefonie verbreitet sich rasant. Mittlerweile bieten alle großen Provider in Deutschland das Telefonieren über das Internet an. Dabei ist den Kunden und Kundinnen oft nicht bekannt, dass diese Verbindungen in den meisten Fällen noch wesentlich unsicherer sind als ein Telefongespräch über das herkömmliche Festnetz.

Bei Telefongesprächen über das Internet kommt die Internet-Technologie Voice over IP (VoIP) zum Einsatz. In zunehmendem Maße wird angeboten, Telefongespräche mit Hilfe der Internet-Technologie VoIP zu führen. Das Fernmeldegeheimnis ist auch für die Internettelefonie zu gewährleisten. Während jedoch bei separaten, leitungsvermittelten Telekommunikationsnetzen Sicherheitskonzepte vorzulegen sind, ist dies bei VoIP bisher nicht die Praxis. Vielmehr werden diese Daten mit Hilfe des aus der Internetkommunikation bekannten Internet-Protokolls (IP) in Datenpakete unterteilt und paketweise über bestehende lokale Computernetze und/oder das offene Internet übermittelt.

Eine derartige Integration von Sprache und Daten in ein gemeinsames Netzwerk stellt den Datenschutz vor neue Herausforderungen. Die aus der Internetnutzung und dem Mail-Verkehr bekannten Unzulänglichkeiten und Sicherheitsprobleme können sich bei der Integration der Telefonie in die Datennetze auch auf die Inhalte und näheren Umstände der VoIP-Kommunikation auswirken und den Schutz des Fernmeldegeheimnisses beeinträchtigen. Beispielsweise können VoIP-Netzwerke durch automatisierte Versendung von Klingelrundrufen oder Überflutung mit Sprachpaketen blockiert, Inhalte und nähere Umstände der VoIP-Kommunikation mangels Verschlüsselung ausgespäht, kostenlose Anrufe durch Erschleichen von Authentifizierungsdaten geführt oder Schadsoftware wie Viren oder Trojaner aktiv werden. Darüber hinaus ist nicht auszuschließen, dass das Sicherheitsniveau der vorhandenen Datennetze negativ beeinflusst wird, wenn sie auch für den VoIP-Sprachdaten-Verkehr genutzt werden. Personenbezogene Daten der VoIP-Nutzenden können außerdem dadurch gefährdet sein, dass Anbieter von VoIP-Diensten ihren Sitz mitunter im außereuropäischen Ausland haben und dort möglicherweise weniger strengen Datenschutzanforderungen unterliegen als Anbieter mit Sitz in der Europäischen Union (EU).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deshalb Hersteller und Herstellerinnen, Anbieter und Anbieterinnen sowie Anwender und Anwenderinnen von VoIP-Lösungen auf, das grundgesetzlich geschützte Fernmeldegeheimnis auch bei VoIP zu wahren und hierfür

- angemessene technische und organisatorische Maßnahmen zu treffen, um eine sichere und datenschutzgerechte Nutzung von VoIP in einem Netzwerk zu ermöglichen,
- Verschlüsselungsverfahren für VoIP anzubieten bzw. angebotene Verschlüsselungsmöglichkeiten zu nutzen,
- Sicherheits- und Datenschutzmängel, die die verwendeten Protokolle oder die genutzte Software bisher mit sich bringen, durch Mitarbeit an der Entwicklung möglichst schnell zu beseitigen,

- auf die Verwendung von offenen, standardisierten Lösungen zu achten beziehungsweise die verwendeten Protokolle und Algorithmen offen zulegen,
- VoIP-Kunden über die Gefahren und Einschränkungen gegenüber dem klassischen, leitungsvermittelten Telefondienst zu informieren und
- bei VoIP alle datenschutzrechtlichen Vorschriften genauso wie bei der klassischen Telefonie zu beachten.

In den benutzten Netzen, auf den beteiligten Servern und an den eingesetzten Endgeräten müssen angemessene Sicherheitsmaßnahmen umgesetzt werden, um die Verfügbarkeit, die Vertraulichkeit, die Integrität und die Authentizität der übertragenen Daten zu gewährleisten.

19 Telefonbefragungen von Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II datenschutzgerecht gestalten

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

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist anlässlich von durch die Bundesanstalt mit Hilfe privaten Callcentern durchgeführten Telefonbefragungen bei Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II darauf hin, dass es den Betroffenen unbenommen ist, sich auf ihr Grundrecht auf informationelle Selbstbestimmung zu berufen. Da die Befragung freiwillig war, hatten sie das Recht, die Beantwortung von Fragen am Telefon zu verweigern.

Die Ablehnung der Teilnahme an einer solchen Befragung rechtfertigt nicht den Verdacht auf Leistungsmissbrauch. Wer seine Datenschutzrechte in Anspruch nimmt, darf nicht deshalb des Leistungsmissbrauchs bezichtigt werden.

Die Konferenz fordert daher das Bundesministerium für Wirtschaft und Arbeit und die Bundesanstalt für Arbeit dazu auf, die Sach- und Rechtslage klarzustellen und bei der bereits angekündigten neuen Telefonaktion eine rechtzeitige Beteiligung der Datenschutzbeauftragten sicherzustellen.

20 Die gravierenden Datenschutzmängel beim Arbeitslosengeld II müssen endlich beseitigt werden

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

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass bei der Umsetzung der Zusammenlegung von Arbeitslosenhilfe und Sozialhilfe weiterhin erhebliche datenschutzrechtliche Mängel bestehen. Die Rechte der Betroffenen werden dadurch stark beeinträchtigt. Zwar ist das Verfahren der Datenerhebung durch die unter Beteiligung der Datenschutzbeauftragten des Bundes und der Länder überarbeiteten Antragsvordrucke auf dem Weg, datenschutzkonform ausgestaltet zu werden. Bei der Leistungs- und Berechnungssoftware A 2 LL gibt es jedoch entgegen den Zusagen des Bundesministeriums für Wirtschaft und Arbeit (BMWA) und der Bundesagentur für Arbeit (BA) immer noch keine erkennbaren Fortschritte.

Weder ist ein klar definiertes Zugriffsberechtigungskonzept umgesetzt, noch erfolgt eine Protokollierung der lesenden Zugriffe. Damit ist es über 40.000 Mitarbeiterinnen und Mitarbeitern in der BA und den Arbeitsgemeinschaften nach SGB II (ARGEn) nach wie vor möglich, voraussetzungslos auf die Daten aller Leistungsempfänger und -empfängerinnen zuzugreifen, ohne dass eine Kontrolle möglich wäre.

Dies gilt auch für das elektronische Vermittlungsverfahren coArb, das ebenfalls einen bundesweiten lesenden Zugriff erlaubt. Äußerst sensible Daten, wie z.B. Vermerke über Schulden-, Ehe- oder Suchtprobleme, können so eingesehen werden. Den Datenschutzbeauftragten sind bereits Missbrauchsfälle bekannt geworden. Einzelne ARGEn reagieren auf die Probleme und speichern ihre Unterlagen wieder in Papierform. Es muss sichergestellt sein, dass das Nachfolgesystem VerBIS, das Mitte 2006 einsatzbereit sein soll, grundsätzlich nur noch einen engen, regionalen Zugriff zulässt und ein detailliertes Berechtigungs- und Löschungskonzept beinhaltet. Der Datenschutz muss auch bei der Migration der Daten aus co Arb in VerBIS beachtet werden.

Mit Unterstützung der Datenschutzbeauftragten des Bundes und der Länder hat die BA den Antragsvordruck und die Zusatzblätter überarbeitet. Soweit die Betroffenen auch die ergänzenden neuen Ausfüllhinweise erhalten, wird ihnen ein datenschutzgerechtes Ausfüllen der Unterlagen ermöglicht und damit eine Erhebung von nicht erforderlichen Daten vermieden. Doch ist immer noch festzustellen, dass die bisherigen Ausfüllhinweise nicht überall verfügbar sind. Es ist daher zu gewährleisten, dass allen Betroffenen nicht nur baldmöglichst die neuen Antragsvordrucke sondern diese gemeinsam mit den Ausfüllhinweisen ausgehändigt werden („Paketlösung“).

Es handelt sich bei den ARGEn um eigenverantwortlich Daten verarbeitende Stellen, die uneingeschränkt der Kontrolle der Landesbeauftragten unterliegen. Dies haben die Bundesanstalt und die ARGEn zu akzeptieren. Es ist nicht hinnehmbar, dass über die Verweigerung einer Datenschutzkontrolle rechtsfreie Räume entstehen und damit in unzumutbarer Weise in die Rechte der Betroffenen eingegriffen wird.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die BA und die sonstigen verantwortlichen Stellen auf Bundes- und Länderebene auf, im Rahmen ihrer Rechtsaufsicht

die Datenschutzmissstände beim Arbeitslosengeld II zu beseitigen. Für den Fall einer völligen Neugestaltung des Systems A 2 LL wegen der offenbar nicht zu beseitigenden Defizite erwarten die Datenschutzbeauftragten ihre zeitnahe Beteiligung. Es ist sicherzustellen, dass die datenschutzrechtlichen Vorgaben, wie die Protokollierung der lesenden Zugriffe und ein klar definiertes Zugriffsberechtigungs- und Löschungskonzept ausreichend berücksichtigt werden, um den Schutz des informationellen Selbstbestimmungsrechts zu gewährleisten.

21 Keine Vorratsdatenspeicherung in der Telekommunikation

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

Die Europäische Kommission hat den Entwurf einer Richtlinie über die Vorratsspeicherung von Daten über die elektronische Kommunikation vorgelegt. Danach sollen alle Telekommunikationsanbieter und Internet-Provider verpflichtet werden, systematisch eine Vielzahl von Daten über jeden einzelnen Kommunikationsvorgang über einen längeren Zeitraum (ein Jahr bei Telefonaten, sechs Monate bei Internet-Nutzung) für mögliche Abrufe von Sicherheitsbehörden selbst dann zu speichern, wenn sie diese Daten für betriebliche Zwecke (z. B. zur Abrechnung) gar nicht benötigen. Die Annahme dieses Vorschlags oder des gleichzeitig im Ministerrat beratenen, weiter gehenden Entwurfs eines Rahmenbeschlusses und ihre Umsetzung in nationales Recht würde einen Dammbruch zulasten des Datenschutzes unverdächtiger Bürgerinnen und Bürger bedeuten. Sowohl das grundgesetzlich geschützte Fernmeldegeheimnis als auch der durch die Europäische Menschenrechtskonvention garantierte Schutz der Privatsphäre drohen unverhältnismäßig eingeschränkt und in ihrem Wesensgehalt verletzt zu werden.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen ihre bereits seit 2002 geäußerte grundsätzliche Kritik an jeder Pflicht zur anlassunabhängigen Vorratsdatenspeicherung. Die damit verbundenen Eingriffe in das Fernmeldegeheimnis und das informationelle Selbstbestimmungsrecht lassen sich auch nicht durch die Bekämpfung des Terrorismus rechtfertigen, weil sie unverhältnismäßig sind. Insbesondere gibt es keine überzeugende Begründung dafür, dass eine solche Maßnahme in einer demokratischen Gesellschaft zwingend notwendig wäre.

Die anlassunabhängige Vorratsdatenspeicherung aller Telefon- und Internetdaten ist von großer praktischer Tragweite und widerspricht den Grundregeln unserer demokratischen Gesellschaft. Erfasst würden nicht nur die Daten über die an sämtlichen Telefongesprächen und Telefax-Sendungen beteiligten Kommunikationspartner und -partnerinnen, sondern auch der jeweilige Zeitpunkt und die Dauer der Einwahl ins Internet, die dabei zugeteilte IP-Adresse, ferner die Verbindungsdaten jeder einzelnen E-Mail und jeder einzelnen SMS sowie die Standorte jeder Mobilkommunikation. Damit ließen sich europaweite Bewegungsprofile für einen Großteil der Bevölkerung für einen längeren Zeitraum erstellen.

Die von einigen Regierungen (z.B. der britischen Regierung nach den Terroranschlägen in London) gemachten Rechtfertigungsversuche lassen keinen eindeutigen Zweck einer solchen Maßnahme erkennen, sondern reichen von den Zwecken der Terrorismusbekämpfung und der Bekämpfung des organisierten Verbrechens bis hin zur allgemeinen Straftatenverfolgung. Alternative Regelungsansätze wie das in den USA praktizierte anlassbezogene Vorhalten („Einfrieren“ auf Anordnung der Strafverfolgungsbehörden und „Auftauen“ auf richterlichen Beschluss) sind bisher nicht ernsthaft erwogen worden.

Mit einem Quick-freeze Verfahren könnte man dem Interesse einer effektiven Strafverfolgung wirksam und zielgerichtet nachkommen.

Der Kommissionsvorschlag würde zu einer personenbezogenen Datensammlung von beispiellosem Ausmaß und zweifelhafter Eignung führen. Eine freie und unbefangene Telekommuni-

kation wäre nicht mehr möglich. Jede Person, die in Zukunft solche Netze nutzt, würde unter Generalverdacht gestellt. Jeder Versuch, die zweckgebundene oder befristete Verwendung dieser Datensammlung auf Dauer sichern zu wollen, wäre zum Scheitern verurteilt. Derartige Datenbestände würden Begehrlichkeiten wecken, aufgrund derer die Hürde für einen Zugriff auf diese Daten immer weiter abgesenkt werden könnten. Auch aus diesem Grund muss bereits den ersten Versuchen, eine solche Vorratsdatenspeicherung einzuführen, entschieden entgegengetreten werden. Zudem ist eine Ausweitung der Vorratsdatenspeicherung auch auf Inhaltsdaten zu befürchten. Schon jetzt ist die Trennlinie zwischen Verkehrs- und Inhaltsdaten gerade bei der Internetnutzung nicht mehr zuverlässig zu ziehen. Dieselben – unzutreffenden – Argumente, die jetzt für eine flächendeckende Speicherung von Verkehrsdaten angeführt werden, würden bei einer Annahme des Kommissionsvorschlags alsbald auch für die anlassfreie Speicherung von Kommunikationsinhalten auf Vorrat ins Feld geführt werden.

Die Konferenz appelliert an die Bundesregierung, den Bundestag und das Europäische Parlament, einer Verpflichtung zur systematischen und anlasslosen Vorratsdatenspeicherung auf europäischer Ebene nicht zuzustimmen. Auf der Grundlage des Grundgesetzes wäre eine anlasslose Vorratsdatenspeicherung verfassungswidrig.

22 Appell der Datenschutzbeauftragten des Bundes und der Länder: Eine moderne Informationsgesellschaft braucht mehr Datenschutz

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

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

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

Die Bürgerinnen und Bürger müssen auch in Zukunft frei von Überwachung sich informieren und miteinander kommunizieren können. Nur so können sie in der Informationsgesellschaft ihre Grundrechte selbst bestimmt in Anspruch nehmen. Dem laufen Bestrebungen zuwider, mit dem Argument einer vermeintlich höheren Sicherheit immer mehr alltägliche Aktivitäten der Menschen elektronisch zu registrieren und für Sicherheitszwecke auszuwerten. Die längerfristige Speicherung auf Vorrat von Verkehrsdaten bei der Telekommunikation, die zunehmende Videoüberwachung im öffentlichen Raum, die anlasslose elektronische Erfassung des Straßenverkehrs durch Kfz-Kennzeichenabgleich, die Erfassung biometrischer Merkmale der Bevölkerung oder Bestrebungen zur Ausdehnung der Rasterfahndung betreffen ganz überwiegend völlig unverdächtige Bürgerinnen und Bürger und setzen diese der Gefahr der **Ausforschung ihrer Lebensgewohnheiten** und einem ständig wachsenden Anpassungsdruck aus, ohne dass dem immer ein adäquater Sicherheitsgewinn gegenübersteht. Freiheit und Sicherheit bedingen sich wechselseitig Angesichts zunehmender Überwachungsmöglichkeiten kommt der Freiheit vor staatlicher Beobachtung und Ausforschung sowie dem Grundsatz der Datensparsamkeit und Datenvermeidung eine zentrale Bedeutung zu.

Den Sicherheitsbehörden steht bereits ein breites Arsenal an gesetzlichen Eingriffsbefugnissen zur Verfügung, das teilweise überstürzt nach spektakulären Verbrechen geschaffen worden ist. Diese Eingriffsbefugnisse der Sicherheitsbehörden müssen einer umfassenden systematischen **Evaluierung durch unabhängige Stellen** unterworfen und öffentlich zur Diskussion gestellt werden. Unangemessene Eingriffsbefugnisse, also solche, die mehr schaden als nützen, sind wieder zurückzunehmen.

Die Kontrolle der Bürgerinnen und Bürger wird auch mit den Argumenten der Verhinderung des Missbrauchs staatlicher Leistungen und der Erhöhung der Steuerehrlichkeit vorangetrie-

ben. So richtig es ist, in jedem Einzelfall die Voraussetzungen für staatliche Hilfen zu prüfen und bei hinreichenden Anhaltspunkten Steuerhinterziehungen nachzugehen, so überflüssig und rechtsstaatlich problematisch ist es, alle Menschen mit einem Pauschalverdacht zu überziehen und Sozial- und Steuerverwaltung mit dem Recht auszustatten, verdachtsunabhängig Datenabgleiche mit privaten und öffentlichen Datenbeständen vorzunehmen. Es muss verhindert werden, dass mit dem Argument der **Leistungs- und Finanzkontrolle** die Datenschutzgrundsätze der Zweckbindung und der informationellen Gewaltenteilung auf der Strecke bleiben.

Die Entwicklung in Medizin und Biotechnik macht eine Verbesserung des Schutzes des Patientengeheimnisses notwendig. Telemedizin, der Einsatz von High-Tech im **Gesundheitswesen**, gentechnische Verfahren und eine intensivierte Vernetzung der im Gesundheitsbereich Tätigen kann zu einer Verbesserung der Qualität der Gesundheitsversorgung und zugleich zur Kosteneinsparung beitragen. Zugleich drohen die Vertraulichkeit der Gesundheitsdaten und die Wahlfreiheit der Patientinnen und Patienten verloren zu gehen. Diese bedürfen dringend des gesetzlichen Schutzes, u. a. durch ein modernes Gendiagnostikgesetz und durch datenschutz- und patientenfreundliche Regulierung der Computermedizin.

Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, insbesondere durch neue Möglichkeiten der Kontrolle bei der Nutzung elektronischer Kommunikationsdienste, Videotechnik, Funksysteme und neue biotechnische Verfahren. Schranken werden bisher nur im Einzelfall durch Arbeitsgerichte gesetzt. Das seit vielen Jahren vom Deutschen Bundestag geforderte **Arbeitnehmerdatenschutzgesetz** muss endlich für beide Seiten im Arbeitsleben Rechtsklarheit und Sicherheit schaffen.

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

Die Europäische Union soll ein „Raum der Freiheit, der Sicherheit und des Rechts“ werden. Die Datenschutzbeauftragten des Bundes und der Länder sind sich bewusst, dass dies zu einer verstärkten Zusammenarbeit der Strafverfolgungsbehörden bei der Verbrechensbekämpfung in der Europäischen Union führen wird.

Die grenzüberschreitende Zusammenarbeit von Polizei- und Justizbehörden darf jedoch nicht zur Schwächung von Grundrechtspositionen der Betroffenen führen. Der vermehrte Austausch personenbezogener Daten setzt deshalb ein hohes und gleichwertiges Datenschutzniveau in allen EU-Mitgliedstaaten voraus. Dabei ist von besonderer Bedeutung, dass die Regelungen in enger Anlehnung an die Datenschutzrichtlinie 95/46/EG erfolgen, damit ein möglichst einheitlicher **Datenschutz in der Europäischen Union** gilt, der nicht zuletzt dem Ausgleich zwischen Freiheitsrechten und Sicherheitsbelangen dienen soll.

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

23 Sicherheit bei eGovernment durch Nutzung des Standards OSCI

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 15. Dezember 2005

In modernen eGovernment-Verfahren werden personenbezogene Daten zahlreicher Fachverfahren zwischen unterschiedlichen Verwaltungsträgern in Bund, Ländern und Kommunen übertragen. Die Vertraulichkeit, Integrität und Zurechenbarkeit der übertragenen Daten kann nur gewährleistet werden, wenn dem Stand der Technik entsprechende Verschlüsselungs- und Signaturverfahren genutzt werden.

Mit dem Online Services Computer Interface (OSCI) steht bereits ein bewährter Sicherheits-Standard für eGovernment-Anwendungen zur Verfügung. Verfahren, die diese Standards berücksichtigen, bieten die Gewähr für eine durchgehende Sicherheit bei der Datenübermittlung vom Versand bis zum Empfang (Ende-zu-Ende-Sicherheit) und erlauben somit auch rechtsverbindliche Transaktionen zwischen den beteiligten Kommunikationspartnerinnen und -partnern.

Die durchgehende Sicherheit darf nicht dauerhaft durch Vermittlungs- und Übersetzungsdienste, die nicht der OSCI-Spezifikation entsprechen, beeinträchtigt werden. Werden solche Dienste zusätzlich in die behördlichen Kommunikationsströme eingeschaltet, wird das mit OSCI-Transport erreichbare Sicherheitsniveau abgesenkt. Der Einsatz von so genannten Clearingstellen, wie sie zunächst für das automatisierte Meldeverfahren vorgesehen sind, kann daher nur eine Übergangslösung sein.

Werden Programme und Schnittstellen auf der Basis derartiger Standards entwickelt, ist sichergestellt, dass die Produkte verschiedener Anbieterinnen und Anbieter im Wettbewerb grundlegende Anforderungen des Datenschutzes und der Datensicherheit in vergleichbar hoher Qualität erfüllen. Gleichzeitig erleichtern definierte Standards den öffentlichen Verwaltungen die Auswahl datenschutzkonformer, interoperabler Produkte.

Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die vom Koordinierungsausschuss Automatisierte Datenverarbeitung (KoopA ADV), dem gemeinsamen Gremium von Bund, Ländern und Kommunalen Spitzenverbänden, getroffene Festlegung, in eGovernment-Projekten den Standard OSCI-Transport für die Übermittlung von personenbezogenen Daten einzusetzen. Um die angestrebte Ende-zu-Ende-Sicherheit überall zu erreichen, empfiehlt sie einen flächendeckenden Aufbau einer OSCI-basierten Infrastruktur.

24 Erklärung von Montreux

„Ein universelles Recht auf den Schutz personenbezogener Daten und der Privatsphäre unter Beachtung der Vielfalt in einer globalisierten Welt“

Die Beauftragten für Datenschutz und den Schutz der Privatsphäre sind auf ihrer 27. Internationalen Konferenz in Montreux (14. bis 16. September 2005) übereingekommen, die Anerkennung des universellen Charakters der Datenschutzgrundsätze zu fördern, und haben folgende Schlusserklärung angenommen:

Die Datenschutzbeauftragten

1. Entsprechen der bei der 22. Internationalen Konferenz der Beauftragten für Datenschutz und den Schutz der Privatsphäre in Venedig verabschiedeten Erklärung,
2. Erinnern an die auf der 25. Internationalen Konferenz der Beauftragten für Datenschutz und den Schutz der Privatsphäre in Sydney angenommene Entschließung über den Datenschutz und die internationalen Organisationen,
3. Stellen fest, dass die Entwicklung der Informationsgesellschaft durch die Globalisierung des Informationsaustausches, den Einsatz zunehmend invasiver Datenverarbeitungstechnologien und verstärkte Sicherheitsmassnahmen beherrscht wird,
4. Sind besorgt angesichts der wachsenden Risiken einer allgegenwärtigen Personenüberwachung auf der ganzen Welt,
5. Verweisen auf die Vorteile und potentiellen Risiken der neuen Informationstechnologien,
6. Sind besorgt über die weiterhin bestehenden Abweichungen zwischen den Rechtssystemen in verschiedenen Teilen der Welt und insbesondere über den mancherorts herrschenden Mangel an Datenschutzgarantien, der einen effektiven und globalen Datenschutz untergräbt,
7. Sind sich bewusst, dass aufgrund des rasch wachsenden Kenntnisstandes im Bereich der Genetik Daten über die menschliche DNA zu den sensibelsten überhaupt werden können, und dass die Gewährleistung eines angemessenen rechtlichen Schutzes dieser Daten angesichts der beschleunigten Wissensentwicklung wachsende Bedeutung erlangt,
8. Erinnern daran, dass die Erhebung personenbezogener Daten und ihre spätere Verarbeitung im Einklang mit den Erfordernissen des Datenschutzes und des Schutzes der Privatsphäre erfolgen müssen,
9. Anerkennen die in einer demokratischen Gesellschaft bestehende Notwendigkeit einer wirksamen Bekämpfung des Terrorismus und des organisierten Verbrechens, wobei jedoch daran zu erinnern ist, dass dieses Ziel unter Achtung der Menschenrechte und insbesondere der menschlichen Würde besser erreicht werden kann,
10. Sind der Überzeugung, dass das Recht auf Datenschutz und den Schutz der Privatsphäre in einer demokratischen Gesellschaft unabdingbare Voraussetzung für die Gewährleistung der Rechte der Personen, des freien Informationsverkehrs und einer offenen Marktwirtschaft ist,

11. Sind überzeugt, dass das Recht auf Datenschutz und den Schutz der Privatsphäre ein grundlegendes Menschenrecht ist,
12. Sind überzeugt, dass die universelle Geltung dieses Rechts verstärkt werden muss, um eine weltweite Anerkennung der Grundsatzregeln für die Verarbeitung personenbezogener Daten unter gleichzeitiger Beachtung der rechtlichen, politischen, wirtschaftlichen und kulturellen Vielfalt durchzusetzen,
13. Sind überzeugt, dass allen Bürgern und Bürgerinnen der Welt bei der Verarbeitung sie betreffender personenbezogener Daten ohne jegliche Diskriminierung individuelle Rechte zugesichert werden müssen,
14. Erinnern daran, dass der Weltgipfel zur Informationsgesellschaft (Genf 2003) in seiner Grundsatzerklärung und seinem Aktionsplan die Bedeutung des Datenschutzes und des Schutzes der Privatsphäre für die Entwicklung der Informationsgesellschaft hervorgehoben hat,
15. Erinnern daran, dass die internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation empfiehlt, im Rahmen multilateraler Abkommen den von ihr im Jahre 2000 erarbeiteten Zehn Geboten zum Schutz der Privatheit Rechnung zu tragen',
16. Anerkennen, dass die Datenschutzprinzipien auf verbindlichen und nicht verbindlichen internationalen Rechtsurkunden beruhen, namentlich den Leitlinien der OECD für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten, dem Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, den Richtlinien der Vereinten Nationen betreffend personenbezogene Daten in automatisierten Dateien, der europäischen Richtlinie 95/46 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und den Datenschutz-Leitsätzen der Asian Pacific Economic Cooperation (APEC),
17. Erinnern daran, dass es sich dabei insbesondere um folgende Prinzipien handelt:
    - Prinzip der Zulässigkeit und Rechtmäßigkeit der Erhebung und Verarbeitung der Daten,
    - Prinzip der Richtigkeit,
    - Prinzip der Zweckgebundenheit, -Prinzip der Verhältnismäßigkeit, -Prinzip der Transparenz,
    - Prinzip der individuellen Mitsprache und namentlich der Garantie des Zugriffsrechts für die betroffenen Personen,
    - Prinzip der Nicht-Diskriminierung,
    - Prinzip der Sicherheit,
    - Prinzip der Haftung,
    - Prinzip einer unabhängigen Überwachung und gesetzlicher Sanktionen,
    - Prinzip des angemessenen Schutzniveaus bei grenzüberschreitendem Datenverkehr.

In Anbetracht dieser Erwägungen

bekunden die Datenschutzbeauftragten ihren Willen, den universellen Charakter dieser Grundsätze zu stärken. Sie vereinbaren eine Zusammenarbeit insbesondere mit den Regierun-

gen und den internationalen und supranationalen Organisationen bei der Ausarbeitung eines universellen Übereinkommens zum Schutz des Menschen bei der Verarbeitung personenbezogener Daten.

Zu diesem Zweck ersuchen die Datenschutzbeauftragen

a. die Organisation der Vereinten Nationen um Vorbereitung einer verbindlichen Rechtsurkunde, in der das Recht auf Datenschutz und Schutz der Privatsphäre als vollstreckbare Menschenrechte im Einzelnen aufgeführt werden;
b. sämtliche Regierungen der Welt, sich für die Annahme von Rechtsurkunden zum Datenschutz und zur Wahrung der Privatsphäre gemäß den Grundprinzipien des Datenschutzes einzusetzen, auch in ihren gegenseitigen Beziehungen;
c. den Europarat, gemäß Artikel 23 des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten die Nichtmitgliedstaaten des Europarates, die über eine Datenschutzgesetzgebung verfügen, zum Beitritt zu dem Übereinkommen und seinem Zusatzprotokoll aufzufordern;

Zudem ermutigen die Datenschutzbeauftragten

die Staats- und Regierungschefs, die sich im Rahmen des Weltgipfels zur Informationsgesellschaft in Tunis (16.-18. November 2005) versammeln, in ihre Schlusserklärung die Verpflichtung aufzunehmen, einen Rechtsrahmen zu entwickeln oder zu verstärken, der das Recht auf Privatsphäre und den Schutz der Personendaten aller Bürgerinnen und Bürger der Informationsgesellschaft gewährleistet, im Einklang mit der Verpflichtung, die die iberoamerikanischen Staats- und Regierungschefs im November 2003 in Santa Cruz (Bolivien) sowie die Staats- und Regierungschefs der frankophonen Länder am Gipfel in Ouagadougou (November 2004) eingegangen sind.

Die Datenschutzbeauftragten richten im Weiteren eine Aufforderung an

a. die internationalen und supranationalen Organisationen, damit diese sich verpflichten, mit den wichtigsten internationalen Urkunden betreffend den Datenschutz und den Schutz der Privatsphäre vereinbare Grundsätze einzuhalten und insbesondere unabhängige und mit Kontrollbefugnissen ausgestattete Aufsichtsbehörden einzurichten;
b. die internationalen nichtstaatlichen Organisationen wie Wirtschafts- und Handelsverbände oder Verbraucherorganisationen zur Ausarbeitung von Normen, die auf den Grundprinzipien des Datenschutzes beruhen oder mit diesen Prinzipien im Einklang sind;
c. die Hersteller von Informatikmaterial und Software zur Entwicklung von Produkten und Systemen, deren integrierte Technologien den Schutz der Privatsphäre gewährleisten.

Die Datenschutzbeauftragten kommen außerdem überein

a. namentlich den Informationsaustausch, die Koordinierung ihrer Überwachungstätigkeiten, die Entwicklung gemeinsamer Standards, die Förderung der Information über die Aktivitäten und die Entschließungen der Konferenz zu verstärken;
b. die Zusammenarbeit mit den Staaten zu fördern, die noch nicht über unabhängige Datenschutz-Aufsichtsbehörden verfügen;
c. den Informationsaustausch mit den im Bereich des Datenschutzes und des Schutzes der Privatsphäre tätigen nichtstaatlichen internationalen Organisationen zu fördern;
d. mit den Datenschutzberatern von Organisationen zusammenzuarbeiten;
e. eine ständige Website einzurichten, die insbesondere als gemeinsame Informations- und Ressourcenverwaltungsdatenbank dienen soll.

Die Beauftragten für den Datenschutz und den Schutz der Privatsphäre vereinbaren, die Zielvorgaben der vorliegenden Erklärung regelmäßig auf ihre Verwirklichung zu überprüfen. Eine erste Beurteilung wird anlässlich der 28. Internationalen Konferenz im Jahre 2006 erfolgen.

25 Resolution zur Verwendung der Biometrie in Pässen, Identitätskarten und Reisedokumenten

27. Internationale Konferenz der Datenschutzbeauftragten, Montreux, 14.-16. September 2005

Die 27. Internationale Konferenz der Datenschutzbeauftragten beschließt:

In Anbetracht der Tatsache, dass Regierungen und internationale Organisationen, namentlich die Internationale Zivilluftfahrtorganisation (ICAO), sich zur Zeit anschicken, Vorschriften und technische Normen zur Integration biometrischer Daten (Fingerabdrücke, Gesichtserkennung) in Pässe und Reisedokumente zu beschließen, um zum einen den Terrorismus bekämpfen und zum andern Grenzkontrollen und Check-in-Verfahren beschleunigen zu können;

Wissend, dass auch im Privatsektor zunehmend biometrische Daten verarbeitet werden, meistens auf freiwilliger Basis;

Unter Berücksichtigung des Umstandes, dass biometrische Daten gesammelt werden können, ohne dass die betroffene Person Kenntnis davon erhält, da sie biometrische Spuren unbewusst hinterlassen kann;

Im Hinblick darauf, dass die Biometrie den menschlichen Körper „maschinenlesbar“ machen wird und dass biometrische Daten als weltweit einheitlicher Identifikator benutzt werden könnten;

Unter Hinweis darauf, dass die verbreitete Verwendung der Biometrie weitreichende Folgen für die Weltgesellschaft haben wird und deshalb Gegenstand einer offen geführten weltweiten Diskussion bilden sollte;

fordert die Konferenz

1. wirksame Schutzmassnahmen, die zu einem möglichst frühen Zeitpunkt Anwendung finden sollen, damit die der Biometrie inhärenten Risiken vermindert werden können,

2. die strikte Trennung zwischen biometrischen Daten, die auf der Grundlage gesetzlicher Verpflichtungen zu öffentlichen Zwecken (z. B. Grenzkontrollen) gesammelt und gespeichert werden, und solchen, die mit Einwilligung zu Vertragszwecken gesammelt und gespeichert werden,

3. die technische Beschränkungen der Verwendung biometrischer Daten in Pässen und Identitätskarten auf den Zweck der Identifizierung durch Vergleich der Daten des Dokuments mit Daten des Dokumentinhabers im Moment der Dokumentvorlage.

26 Resolution zur Verwendung von Personendaten für die politische Kommunikation

27. Internationale Konferenz der Datenschutzbeauftragten, Montreux, 14.-16. September 2005

Die Konferenz

In Erwägung, dass politische Kommunikation ein grundlegendes Instrument für die Beteiligung der Bürgerinnen und Bürger, der politischen Kräfte und der Kandidatinnen und Kandidaten am Leben einer Demokratie ist, und in Anerkennung der Wichtigkeit der Freiheit der politischen Meinungsäußerung als ein Grundrecht;

In Erwägung, dass gelebte Staatsbürgerschaft das Recht der Bürgerinnen und Bürger voraussetzt, im Rahmen von Wahlkampagnen von Politik und Verwaltung Informationen zu erhalten und angemessen informiert zu werden; in Erwägung, dass diese Rechte auch geeignet sind um bei weiteren Themen, Ereignissen und politischen Positionen in Kenntnis der Sachlage seine Wahl zu anderen Themen des politischen Lebens treffen zu können, sei es bei Referenden, bei der Wahl von Kandidatinnen und Kandidaten oder beim Zugang zu Informationen innerhalb politischer Organisationen oder von gewählten Amtsträgern;

In Erwägung, dass die politischen Kräfte und politische Organisationen im Allgemeinen sowie gewählte Abgeordnete sich verschiedener Formen der Kommunikation und der Geldmittelbeschaffung bedienen und Informationsquellen und neue Technologien nutzen, um direkte und persönliche Kontakte mit verschiedensten Kategorien von betroffenen Personen zu knüpfen;

In Erwägung, dass in einer wachsenden Zahl von Ländern ein Trend hin zu immer stärkerer institutioneller Kommunikation gewählter Kandidatinnen und Kandidaten und Körperschaften zu beobachten ist, ebenfalls auf lokaler Ebene und mittels E-Government; in der Erwägung, dass diese Aktivitäten, die die Verarbeitung von Personendaten voraussetzen können, in Einklang stehen mit dem Recht der Staatsbürgerinnen und -bürger, über die Tätigkeiten der gewählten Kandidatinnen und Kandidaten und Körperschaften informiert zu werden;

In Erwägung, dass in diesem Rahmen von politischen Organisationen fortlaufend eine große Menge von Personendaten gesammelt und manchmal in aggressiver Art und Weise verwendet werden, unter Anwendung verschiedener Techniken wie Umfragen, Sammlung von E-Mail-Adressen mittels geeigneter Software oder Suchmaschinen, flächendeckender Stimmenwerbung in Städten oder Formen politischer Entscheidbildung durch interaktives Fernsehen oder Computerdateien, die die Herausfilterung einzelner Stimmenden erlauben; in Erwägung, dass in diesen Daten – zusätzlich zu elektronischen Adressen, Telefonnummern, E-Mail-Konten, Informationen über berufliche Tätigkeiten und familiäre Verhältnisse – zuweilen unrechtmäßig auch sensible Daten enthalten sein können wie Informationen über – tatsächliche oder bloß vermutete – ethische oder politische Überzeugungen oder Aktivitäten oder über das Wahlverhalten;

In Erwägung, dass von verschiedenen Personen invasive Profile erstellt und sie klassifiziert werden – manchmal unzutreffenderweise oder auf der Grundlage eines flüchtigen Kontakts – als solche, die mit einer bestimmten politischen Strömung sympathisieren, sie unterstützen,

ihr angehören oder gar Parteimitglieder sind, um so mit bestimmten Gruppen von Bürgerinnen und Bürgern vermehrt persönlich kommunizieren zu können;

In Erwägung, dass diese Aktivitäten gesetzeskonform und ordnungsgemäß ausgeübt werden müssen;

In Erwägung, dass es nötig ist, die Grundrechte und Grundfreiheiten der betroffenen Personen zu schützen und mit geeigneten Maßnahmen zu verhindern, dass diese Personen ungerechtfertigtes Eindringen in ihre Privatsphäre erfahren, Schaden erleiden oder ihnen Kosten entstehen, dass sie namentlich negative Auswirkungen und mögliche Diskriminierungen erleiden oder auf die Ausübung bestimmter Formen der politischen Beteiligung verzichten müssen;

In Erwägung, dass es möglich sein sollte, das Schutzziel zu erreichen, indem sowohl die Interessen der Öffentlichkeit an bestimmten Formen politischer Kommunikation als auch angemessene Modalitäten und Garantien in Bezug auf die Kommunikation mit Parteimitgliedern und mit andern Bürgerinnen und Bürgern in Betracht gezogen werden;

In Erwägung, dass in diesem Sinne ein verantwortungsbewusstes Marketing gefördert werden kann, ohne dass der Austausch politischer Ideen und Vorschläge behindert zu werden braucht, und dass die politische Kommunikation, auch wenn sie gelegentlich Elemente typischer Werbetätigkeiten aufweist, doch Eigenheiten hat, die sie vom kommerziellem Marketing unterscheiden;

In Erwägung, dass Datenschutzgesetze bereits in vielen Gerichtsbarkeiten auf politische Kommunikation anwendbar sind;

In Erwägung, dass es nötig ist, die Einhaltung der Datenschutzesgrundsätze zu garantieren und dazu einen weltweiten Minimalstandard zu schaffen, der dazu beitragen könnte, dass das Schutzniveau für Personen, von denen Daten gesammelt werden können, zu harmonisieren, indem zum einen nationale und internationale Verhaltensregeln zur Grundlage genommen und zum andern spezifische Lösungen und Regelungen einzelner Länder berücksichtigt werden;

In Erwägung, dass die Datenschutzbeauftragten künftig eine stärkere Rolle in der Planung koordinierter Aktionen spielen könnten, auch in Zusammenarbeit mit anderen Aufsichtsbehörden in den Bereichen des Telekommunikation, Information, Meinungsumfragen oder Wahlverfahren;

verabschiedet folgende Resolution

Jede Aktivität politischer Kommunikation, die die Verarbeitung von Personendaten voraussetzt – auch diejenige, die nicht im Zusammenhang mit Wahlkampagnen steht – muss die Grundrechte und Grundfreiheiten der von der Datenverarbeitung betroffenen Personen respektieren, einschließlich des Rechts auf Schutz der persönlichen Daten, und muss im Einklang stehen mit den anerkannten Grundsätzen des Datenschutzes, namentlich:

Datenminimierung

Personendaten sollen nur so weit verarbeitet werden, als es zur Erreichung des spezifischen Zwecks,

zu welchem sie gesammelt werden, erforderlich ist.

Erhebung auf rechtmäßige Weise und nach Treu und Glauben

Personendaten sollen aus erkennbaren Quellen rechtmäßig erhoben werden und sie sollen nach Treu und Glauben verarbeitet werden. Es soll sichergestellt werden, dass die Quellen, im Einklang mit dem Gesetz, entweder öffentlich zugänglich sind, oder dass andernfalls respektiert wird, dass sie nur zu bestimmten Zwecken, unter bestimmten Modalitäten, für einen begrenzten Anlass oder Zeitraum genutzt werden dürfen.

Besondere Aufmerksamkeit soll jenen Fällen geschenkt werden, in denen aggressive Methoden für die Kontaktaufnahme mit den betroffenen Personen gewählt werden.

Datenqualität

Bei der Verarbeitung sollen die anderen Grundsätze zur Sicherung der Datenqualität beachtet werden. Die Daten müssen insbesondere richtig, relevant und auf das notwendige Minimum beschränkt sein und à jour gehalten werden im Hinblick auf den bestimmten Zweck, zu dem sie erhoben wurden, besonders wenn sich die Informationen auf gesellschaftliche oder politische Anschauungen oder ethische Überzeugungen der betroffenen Person beziehen.

Zweckmäßigkeit

Personendaten aus privaten oder öffentlichen Informationsquellen, Institutionen oder Organisationen dürfen für die politische Kommunikation verwendet werden, wenn ihre Weiterverarbeitung im Einklang steht mit dem Zweck, zu dem sie ursprünglich erhoben wurden, und den betroffenen Personen zur Kenntnis gebracht wird; dies gilt insbesondere für sensible Daten. Gewählte Abgeordnete müssen diese Grundsätze beachten, wenn sie Daten, die zur Ausübung der amtlichen Funktionen gesammelt wurden, für die politische Kommunikation benützen wollen.

Personendaten, die ursprünglich mit aufgeklärter Einwilligung der betroffenen Person zu Marketingzwecken erhoben wurden, dürfen für die politische Kommunikation verwendet werden, wenn der Zweck der politischen Kommunikation in der Zustimmungserklärung ausdrücklich genannt wird.

Verhältnismäßigkeit

Personendaten dürfen nur auf die Art und Weise verarbeitet werden, die dem Zweck der Datensammlung entspricht, insbesondere wenn es um Daten zu potenziellen Wählerinnen und Wählern oder um den Vergleich von Daten geht, die aus verschiedenen Archiven oder Datenbanken stammen.

Personendaten, insbesondere solche, die über den Anlass hinaus, zu dem sie erhoben wurden, aufbewahrt werden, dürfen weiter verwendet werden, bis die Ziele der politischen Kommunikation erreicht sind.

Information der betroffenen Person

Den betroffenen Personen muss eine dem gewählten Kommunikationsmittel entsprechende Informationsnotiz zugestellt werden, bevor von ihnen Daten gesammelt werden; die Notiz hat den für die Datensammlung Verantwortlichen zu bezeichnen (die einzelne kandidierende Person; den externen Kampagnenleiter; die lokale Unterstützungsgruppe; lokale oder assoziierte Vereinigungen; die Partei insgesamt) sowie den zu erwartenden Datenaustausch zwischen diesen Instanzen.

Die Person, von der Daten gesammelt werden, muss informiert werden, wenn diese Daten ohne ihr Zutun gesammelt werden, zumindest wenn die Daten nicht nur vorübergehend aufbewahrt werden.

Einwilligung

Es muss sichergestellt sein, dass die Verarbeitung von Personendaten auf der Eiwilligung der betroffenen Person oder auf einen anderen gesetzlich vorgesehen Grund beruht. Die Verarbeitung muss die im jeweiligen Staat geltenden, den spezifischen Informationsquellen und -mitteln entsprechenden Regelungen beachten, namentlich im Falle von E-Mail-Adressen, Faxnummern, SMS oder andern Text/Bild/Video-Mitteilungen oder von aufgezeichneten Telefonkontakten.

Datenaufbewahrung und Datensicherheitsmassnahmen

Jede für eine Datensammlung verantwortliche Person, sei es eine politische Gruppierung oder eine einzelne kandidierende Person, muss alle technischen und organisatorischen Maßnahmen treffen, die nötig sind, um die Integrität der Daten zu schützen und um zu verhindern, dass die Daten verloren gehen oder von unbefugten Personen oder Stellen benutzt werden.

Rechte der betroffenen Person

Die betroffene Person hat das Recht auf Zugang, Berichtigung, Sperrung und Löschung ihrer Daten; sie hat das Recht, sich gegen unerwünschte Kommunikation zu wehren und – kostenlos sowie auf einfache Weise – zu verlangen, keine neuen Mitteilungen mehr zu erhalten. Diese Rechte müssen in der an sie gerichteten Informationsnotiz ausdrücklich genannt werden.

Für den Fall, dass diese Rechte verletzt werden, sind angemessene Maßnahmen und Sanktionen vorzusehen.

27 Fachtagung: Moderne Verwaltung zwischen Informationsfreiheit und Datenschutz

Vorwort

Karsten Neumann

Landesbeauftragter für den Datenschutz

Mecklenburg-Vorpommern

Meiner Einladung in das Schweriner Schloss folgten rund 80 Vertreter aus Politik, Verwaltung, Verbänden und Organisationen des Landes Mecklenburg-Vorpommern. Der bewusst provokante Titel der Veranstaltung, die hochkarätigen Akteure und die plötzliche Aktualität des Themas durch den unmittelbar bevorstehenden Beschluss des Bundestages zu einem Informationsfreiheitsgesetz auf Bundesebene belebten die Diskussion und steigerten auch das öffentliche Interesse an dieser zweiten Fachtagung des Datenschutzbeauftragten Mecklenburg-Vorpommern. Für mich war es die erste "Feuerprobe``, nachdem ich im Dezember 2004 das Amt von Herrn Dr. Kessel übernommen habe.

Der nunmehr vorliegende Tagungsband dokumentiert nicht nur die Beiträge der Akteure, sondern bietet damit zugleich eine Übersicht der wichtigsten Pro- und Contra-Argumente zur Einführung eines generellen Rechtes aller Bürgerinnen und Bürger auf Einsichtnahme in die Akten der öffentlichen Verwaltung. Somit dient er einerseits der Erläuterung des voraussichtlich am 1. Januar 2006 in Kraft tretenden Informationsfreiheitsgesetzes des Bundes und andererseits versteht es sich als Anregung und Materialsammlung für die Diskussion eines Informationsfreiheitsgesetzes für Mecklenburg-Vorpommern.

Die Fachtagung hat die Potentiale, Chancen und Risiken für Bürgerinnen und Bürger, Politik, Verbände und Vereine, aber auch für die Landes- und Kommunalverwaltungen aufgezeigt und deutlich gemacht, dass die Chancen durch eine transparente Verwaltung die Risiken für personenbezogene Daten und Betriebs- und Geschäftsgeheimnisse bei Weitem überwiegen.

Die öffentlichen Reaktionen nach der Konferenz und das bevorstehende In-Kraft-Treten des Bundesgesetzes stimmen mich überwiegend optimistisch, dass der Landesgesetzgeber bald dem Beispiel von über 50 Staaten weltweit, vier deutschen Bundesländern und nun auch der Bundesbehörden folgen wird und die Chance erkennt, durch die Einführung dieses Rechtes die öffentliche Verwaltung in Land und Gemeinden durch Transparenz auch inhaltlich zu modernisieren.

Moderne Verwaltung wird regelmäßig mit der Vorstellung verknüpft, die Behörden zum Dienstleister zu entwickeln und somit bürgernah und effizient die öffentlichen Belange zu verwalten. Bürgernähe beschreibt dabei nicht die Entfernung zwischen Verwaltungssitz und Wohnort, sondern vor allem eine direkte und unmittelbare Kommunikation. Diese wird durch moderne Kommunikationsmittel ergänzt und eröffnet als eGovernment neue Möglichkeiten. Zugleich wird mit einem Informationsfreiheitsgesetz das Prinzip der Amtsverschwiegenheit zugunsteneines Selbstverständnisses der Verwaltung als Dienstleister weiterentwickelt. Transparenz der Verwaltungsentscheidungen wird somit ebenso ermöglicht, wie die unmittelbare Einbeziehung der Öffentlichkeit in demokratische Entscheidungen. Die Mitbestimmung

durch informierte Bürgerinnen und Bürger ist als Grundlage eines demokratischen Gemeinwesens Ausdruck einer bürgernahen Verwaltung.

Zwischen Informationsfreiheit und Datenschutz entspannt sich dabei nur ein scheinbarer Widerspruch. Selbstverständlich darf der Schutz personenbezogener Daten gerade bei der Modernisierung der öffentlichen Verwaltung nicht hinten anstehen, sondern muss bereits bei der Entwicklung aller eGovernment-Projekte berücksichtigt werden. Zugleich bietet die neue Technologie aber auch die Chance, das Verwaltungshandeln transparent zu machen und so dem Bürger die Möglichkeit einer umfassenden Information zu eröffnen.

Diesen Prozess hoffe ich mit der Fachtagung auch in Mecklenburg-Vorpommern angestoßen zu haben. Ich freue mich über jede weitergehende Initiative und hoffe mit diesem Tagungsband einen wirksamen Beitrag leisten zu können.

Schwerin, September 2005

Grußwort

Andreas Bluhm, MdL

2. Vizepräsident des Landtages

Mecklenburg-Vorpommern

Die Formulierung des Themas der heutigen Fachtagung „Zwischen Informationsfreiheit und Datenschutz“ stimmt nachdenklich. Sind Informationsfreiheit und der Schutz der personenbezogenen Daten nicht Forderungen, die einander widersprechen? So scheint es zumindest auf den ersten Blick. Sicherlich ist diese Formulierung mit Bedacht gewählt worden, um das Thema der heutigen Veranstaltung pointiert zuzuspitzen, vielleicht auch etwas zu provozieren und Sie, die Teilnehmer der Fachtagung, zum Nachdenken anzuregen.

Das schon in der Überschrift anklingende Spannungsfeld zwischen Informationsfreiheit und den Fragen des Datenschutzes oder anders: Den Fragen des Zugangs zu und des Umgangs mit Informationen und Wissen macht auch den besonderen Reiz der heutigen Veranstaltung aus.

Seit längerem schon befinden wir uns in einem gesellschaftlichen Wandel - von der Industriegesellschaft hin zu einer Wissens- und Informationsgesellschaft. Immer mehr Menschen nutzen etwa die Möglichkeiten des Internets, um schnell viele, neue Informationen zu bekommen, um zu lernen und sich zu bilden. Digitale Techniken und Neuerungen der Informations- und Kommunikationsmöglichkeiten dringen in immer weitere Bereiche unseres Lebens vor, prägen diese und sind heute nicht mehr wegzudenken, sei es am Arbeitsplatz, in der Schule, der Ausbildung oder im privaten Bereich. Und bei allem ist damit eng verbunden die Frage des Informationsrechtes - also die Frage des Zugangs zu Informationen in der Wissens- und Informationsgesellschaft. So sind Information und Kommunikation die Voraussetzung für eine erfolgreiche Kommunikation, sowohl im privaten als auch im öffentlichen Bereich und der Verwaltung.

Doch nicht nur die Verwaltung, damals wie heute, ist auf den Zugang zu Informationen zur Erfüllung ihrer Aufgaben angewiesen. Auch für die Bürgerinnen und Bürger ist der Zugang zu Informationen von immenser Bedeutung, wollen sie am demokratischen Willensbildungsprozess teilhaben. Grundvoraussetzung der Demokratie ist jedoch Öffentlichkeit, die wiederum ohne Information und Kommunikation undenkbar ist.

Die noch zu verabschiedenden Informationsgesetze des Bundes und der meisten Länder - Schleswig-Holstein, Nordrhein-Westfalen, Brandenburg und Berlin sind die ersten, die bereits Informationsfreiheitsgesetze geschaffen haben - sollen künftig den Zugang der Bürgerinnen und Bürger zu relevanten, amtlichen Dokumenten und Informationen regeln. Ziel ist es dabei, die öffentliche Verwaltung durch erleichterten Informationszugang transparenter zu gestalten, um die Menschen in die Lage zu versetzen, das Verwaltungshandeln nachzuvollziehen und konstruktiv an ihm mitwirken zu können. Information und Transparenz sind für die effektive Wahrnehmung von demokratischen Beteiligungsrechten zentrale Voraussetzung. Nur die informierte Gesellschaft vermag ihre Aufsichts- und Kontrollpflichten sachgerecht und effektiv zu erfüllen und gesellschaftliche Fehlentwicklungen frühzeitig zu erkennen.

Doch dem öffentlichen Informationszugang auf der einen Seite steht auf der anderen Seite das Recht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung gegenüber. Aus

dem Volkszählungsurteil des Bundesverfassungsgerichtes wurde abgeleitet, dass es kein von vornherein belangloses personenbezogenes Datum gibt. Insoweit wird von den Datenschützern zu Recht darauf verwiesen, dass es für die Datenverarbeitung entscheidend auf den Verwendungszusammenhang ankommt. Aber wie vertragen sich dann damit Informationsansprüche, die unter Umständen auch personenbezogene Daten Dritter einschließen können und deren Spezifikum gerade ihre voraussetzungslose Inanspruchnahme ist? Ein Grund, ein Zweck oder eine Verwendungsabsicht muss - anders als im Datenschutzrecht - nicht genannt werden, weil gerade die Information voraussetzungslos verlangt werden kann. Wie kann aber dann der Verwendungszusammenhang und damit ein mögliches Risiko für die Betroffenen geprüft werden? Fragen über Fragen.

Und Sie sehen, sehr geehrte Damen und Herren, hier zeigt sich das Spannungsverhältnis, das schon vom Titel der Tagung angedeutet worden ist.

Bei der Diskussion um Informationsfreiheit und Informationszugang muss dafür gesorgt werden, dass bei aller Leidenschaft für den gesetzlich geregelten Informationszugang nicht die datenschutzrechtlichen Standards abgesenkt werden und das Recht auf informationelle Selbstbestimmung eines jeden Einzelnen verletzt wird. Dem gegenüber darf der Datenschutz auch nicht als Blockadeinstrument gegen Informationswünsche missbraucht werden.

Ich bin der Auffassung, dass das ausgewählte Thema brisant und vielschichtig ist und einen spannenden Verlauf Ihrer Fachtagung verspricht. Sie kann dazu beitragen, das Problembewusstsein für das Spannungsfeld von Informationsfreiheit und Datenschutz in der Politik und Verwaltung zu schärfen. Vielleicht stehen am Ende auch Anregungen für ein Informationsfreiheits- oder -zugangsgesetz in Mecklenburg-Vorpommern.

Ich wünsche Ihnen viele interessante Beiträge und Diskussionen sowie einen ertragreichen und konstruktiven, fachlichen Austausch. Ihnen allen danke ich für Ihr Interesse und die Bereitschaft der Mitarbeit!

Begrüßung

Karsten Neumann

Landesbeauftragter für den Datenschutz

Mecklenburg-Vorpommern

„Moderne Verwaltung: Zwischen Informationsfreiheit und Datenschutz“.

Im Jahr 1766 wurde der Zugang zu Verwaltungsunterlagen erstmals als allgemeines Bürgerrecht in Schweden rechtlich anerkannt. Es galt somit auch in meiner Heimatstadt Stralsund, die bis zum Wiener Kongress im Jahre 1815 zum Territorium des Königreiches Schweden gehörte.

1946 stellte die UN-Generalversammlung fest, dass das Recht auf Information ein fundamentales Menschenrecht sei und 1966 brach der „Freedom of Information Act“ in den USA die Bahn für ein Prinzip, dass mittlerweile in den meisten Demokratien Anerkennung gefunden hat.

Heute sind es über 50 Staaten weltweit und 4 deutsche Bundesländer, in denen das Recht auf einen grundsätzlich freien Zugang zu allen bei den öffentlichen Stellen existierenden Informationen verankert ist.

Ich würde es sehr begrüßen, wenn das Jahr 2006 für Mecklenburg-Vorpommern mit einem Informationsfreiheitsgesetz einen neuen Standard des Verhältnisses zwischen Verwaltung und Bürger setzen würde.

Die Zeit dafür ist reif und die Gelegenheit aus vielerlei Gründen günstig.

„Verwaltungsreform Mecklenburg-Vorpommern – in Zukunft einfach besser“ so lautet der selbstbewusste Slogan, unter dem in Mecklenburg-Vorpommern bis zur Kommunalwahl 2009 stufenweise eine umfassende Verwaltungsmodernisierung umgesetzt werden soll.

Einem der Teilziele auf dem Weg zur Modernisierung der Verwaltung will sich diese Fachkonferenz widmen. Wenn auch noch vieles bei dieser Verwaltungsreform umstritten ist, so scheinen sich alle Beteiligten in einem Ziel zumindest einig zu sein: der Herstellung von mehr Bürgernähe und Transparenz.

Aber was verstehen wir eigentlich konkret unter Bürgernähe?

Die einen verstehen darunter die Fahrzeiten vom Wohnort zum Sitz der Verwaltung, andere vertreten eher eine Verlagerung von möglichst allen Zuständigkeiten auf die kommunale Ebene, manche wollen sogar Bürgernähe als Verhältnis aus der Anzahl der Wahlberechtigten pro kommunalem Abgeordneten berechnen.

Wenn wir Bürgernähe jedoch nicht in ihrer räumlichen Dimension, sondern eher als die emotionale Nähe zwischen Bürgerinnen und Bürgern zu den Verwaltungen in Umfragen beleuchten würden, müssten wir sehr schnell feststellen, dass die Kluft zwischen Bürgern und Beamten unüberbrückbar tief zu sein scheint.

Der hoheitliche Staat rechtfertigt sich heute noch durch Uniformen, Wappen, Siegel, Amtsstuben, Öffnungszeiten oder auch Sprechzeiten, Bekanntmachungen, amtliche Mitteilungen und mit Gebühren- und Widerspruchsbescheiden. So wird dem Bürger förmlich mitgeteilt, wie an den Amtstischen über seine Belange entschieden wurde. Sind diese Entscheidung oft schon unverständlich, so sind es die Begründungen umso mehr.

Der demokratische Rechtsstaat ist inzwischen in einer Art und Weise verrechtlicht, dass demokratische Teilhabe oft durch informierte Fachleute normiert wird.

Die Verwaltungsfachleute bestimmen Art und Umfang der demokratischen Teilhabe durch ihre eigene Informationspolitik gegenüber dem einzelnen Bürger, der Öffentlichkeit, der Presse und den Parlamenten – und das sowohl auf kommunaler, Landes-, Bundes- oder Europaebene.

Im Informationszeitalter bestimmt der Zugang zu Informationen auch Art und Ausmaß von Macht.

Es scheint paradox: In der Informationsgesellschaft nimmt die Flut der Informationen solch bedrohliche Ausmaße an, dass es unmöglich scheint, alle relevanten Informationen tatsächlich zu erhalten.

Der freie – selbst bestimmte und anlassunabhängige – Zugang zu Informationen wird somit zu einer Bedingung für die Demokratisierung der Informationsgesellschaft.

Sicher wird Verteilungsgerechtigkeit nicht herstellbar sein, aber wenigstens gleiche Zugangschancen auch zu Informationen sollte ein Grundprinzip für die gesellschaftliche Organisation eines demokratischen Rechtsstaates bleiben.

Der Rechtsstaat versuchte bisher auf diese Herausforderungen mit der Einräumung individueller Abwehrrechte zu reagieren und schuf hierfür die elementaren Voraussetzungen in den Auskunftsansprüchen des unmittelbar Betroffenen, den Beteiligungsrechten von potentiell Betroffenen, der gerichtlichen Überprüfungsmöglichkeit von Verwaltungsentscheidungen durch den Belasteten und die unabhängige Überwachung durch privilegierte Kontrollorgane.

Diese Auskunfts-, Informations- und Beteiligungsrechte füllen momentan bereits ganze Bände. Das Grundproblem bleibt allerdings: der Bürger muss um seine Rechte wissen, diese einfordern und durchsetzen können.

Dieses Prinzip gilt es durch einen freien Zugang zu Informationen jedenfalls in einem Teilbereich umzukehren:

nicht der Bürger soll wissen und begründen können, gegenüber wem er welche Auskunftsrechte hat, sondern sein Recht soll generell sein,

die Auskunftsverweigerungsrechte müssen speziell sein und

der Verwaltung den Begründungszwang für den Ausnahmefall auferlegen.

Hierfür bietet der Modernisierungsprozess in der öffentlichen Verwaltung in Mecklenburg-Vorpommern eine bedeutende Chance. eGovernment verlangt einerseits die Umorientierung

von Verwaltungsabläufen hin zu einer Dienstleistungsorientierung und eröffnet so andererseits die Chance zu einer unbürokratischen Zugangsgewährleistung.

„Gläserne Rathäuser“ sind im Gegensatz zum „Gläsernen Bürger“ kein Schreckensbild für Datenschutzbeauftragte: Auf der einen Seite steht eine Organisation öffentlicher Angelegenheiten – auf der anderen Seite das Recht des Individuums auf freie – und staatlich unbeeinflusste und unbeobachtete – Entfaltung seiner Persönlichkeit.

Die Informationsfreiheit ist somit eng verbunden mit dem Recht auf informationelle Selbstbestimmung. Wurde dieses Konstrukt des Bundesverfassungsgerichtes noch ausschließlich als Abwehranspruch gegen staatliche Fremdbestimmung zur Sicherung der persönlichen Freiheit als Garant staatlicher demokratischer Entwicklung begriffen, erfährt es in der Informationsfreiheit seinen Wandel zu einem aktiven Teilhaberecht. Und hier treffen sich die Intentionen von Datenschutz, Bürgerrechtsbewegungen und Verwaltungsmodernisierern, als unser gemeinsames Bild vom demokratischen Rechtsstaat auf der Grundlage der Mitbestimmung und Kontrolle durch mündige Bürgerinnen und Bürger.

Datenschutz und Informationsfreiheit sind die zwei Säulen der Informationsgesellschaft, beide gehören zur rechtsstaatlichen Grundausstattung, die nun auch in Mecklenburg-Vorpommern komplettiert werden sollte.

Der Gesetzentwurf für ein Informationsfreiheitsgesetz auf Bundesebene wurde umfangreich diskutiert und steht hoffentlich trotz des vorgezogenen Endes dieser Legislaturperiode vor seiner Vollendung. Damit wird es auch für Mecklenburg-Vorpommern Zeit, dass sich das Parlament diesem Thema stellt.

Informationsfreiheit für die Bürgerinnen und Bürger -

Stand der bundespolitischen Diskussion

Dr. Cornelie Sonntag-Wolgast, MdB

Vorsitzende des Innenausschusses des

Deutschen Bundestages

Der hürdenreiche Weg zum Informationsfreiheitsgesetz

„Der Staat ist für die Menschen und nicht die Menschen für den Staat“. Dieser Satz Albert Einsteins macht im Jubiläumsjahr 2005 die Runde; er steht an der Seitenfassade des Bundeskanzleramtes in Berlin und er könnte auch als Motto unser Informationsfreiheitsgesetz kennzeichnen.

Ich freue mich, heute hier in Schwerin als Vorsitzende des Bundestags-Innenausschusses und – das darf ich gleich hinzufügen – engagierte Befürworterin dieses Reformwerkes – zu Ihnen sprechen zu dürfen. Noch vor ein paar Wochen dachte ich: die Tagung zum Thema kommt eigentlich ein bisschen zu spät – denn laut ursprünglicher Planung wollten wir im Ausschuss schon im Mai unsere Beratungen abschließen; vielleicht wäre es dann auch schon zur 2. und 3. Lesung im Plenum gekommen. Dem ist aber nicht so. Es ist typisch für den langen, mühsamen und hürdenreichen Weg dieses Gesetzes, dass - nachdem die vermeintlich letzten Konfliktpunkte bereinigt schienen – sozusagen um 3 Minuten vor 12 noch einmal ein Bedenkenträger so nachdrücklich in die parlamentarische Entscheidungsfindung eingriff, dass wir vor etwa 2 Wochen sowohl die Behandlung im Innenausschuss als auch die für den übernächsten Tag im Plenum vorgesehene Debatte von der Tagesordnung streichen mussten.

Den Krankenkassen und der kassenärztlichen Bundesvereinigung war es gelungen, das Gesundheitsministerium in Stellung zu bringen. Man befürchtete die Freigabe von Sozialdaten nach dem SGB. Nach meiner Einschätzung eine unbegründete Sorge, denn solche Angaben unterliegen dem Geheimnisschutz. Nach dem Motto „nun haben wir schon so viele Hürden genommen - dann werden wir auch diese bewältigen“ – stoppten wir die endgültige Verabschiedung, um den Einwand zu überprüfen. Nun sind der heutige Tag für die Ausschussberatungen, der 16. Juni fürs Plenum und die Beratung im Bundesrat für den 17. Juni oder den 8. Juli ins Auge gefasst. Die Entstehungsgeschichte des Informationsfreiheitsgesetzes (IFG abgekürzt) beträgt rund 7 Jahre. Das Vorhaben war schon im Koalitionsvertrag von 1998 vermerkt, geriet dann in die Mühlsteine ministerieller Einwände verschiedener Art. Die Front der Zweifler umfasste die Ministerien für Verteidigung, Wirtschaft und Inneres sowie Kreise der Unternehmer. Eine Kabinettsvorlage scheiterte an der Kritik aus den Ressorts. So brachten denn die Koalitionsfraktionen von SPD und Bündnis 90/Die Grünen einen eigenen Gesetzentwurf am 14. Dezember 2004 ein. Eine Initiative also aus dem Parlament, zustande gekommen nach hartnäckigem Drängen. Vielleicht ist das auch ganz folgerichtig so. Das Parlament versteht sich als Sachwalter von Bürgerrechten.

Das Gesetz schafft den voraussetzungslosen Zugang zu amtlichen Informationen der Behörden des Bundes und lässt normal werden, was in über 50 Staaten der Erde längst selbstverständlich ist. Der Staat schuldet seinen Bürgern Auskunft zu allen Belangen, soweit der Ge-

heimnis- oder Datenschutz nicht entgegensteht. Das allerdings wird durchaus ernst genommen und anhand von Fallkonstellationen aufgeführt.

Wir stehen, meine Damen und Herren, kurz vor dem Ende einer überraschend verkürzten Legislaturperiode. Falls es zu einem Regierungswechsel kommt – ganz hypothetisch formuliert - , wird man fragen, welche Gesetze und Neuerungen die rotgrüne Ära unter Führung Gerhard Schröders geprägt haben. Und da werden neben dem Stichwort Agenda 2010, den mit ihr verbundenen sozial- und arbeitsmarktpolitischen Neuerungen, vielleicht am ehesten Gesetze genannt werden, die unsere Gesellschaft, das Zusammenleben der Menschen, ihr Verhältnis zum Staat und das Reagieren auf veränderte Einstellungen im privaten bzw. familiären Bereich nachzeichnen. Dazu zähle ich die Staatsangehörigkeitsreform, das Gesetz über die eingetragenen Lebensgemeinschaften, das Zuwanderungsgesetz, das Antidiskriminierungsgesetz und eben auch das Informationsfreiheitsgesetz. Es war öffentlich weniger umstritten als die zuvor genannten Initiativen – möglicherweise weil es den Bürgern weniger stark ins Bewusstsein gedrungen ist. Aber es gehört zweifellos in die sensible Reihe der Vorhaben, die den Kernbereich der Gesellschaft, ihrer Motivation und Befindlichkeit berühren. Es ist dazu angetan, einen kulturellen Wandel einzuleiten, es soll die Wissbegierde der Menschen wecken, ihrem Recht auf Auskunft über Belange staatlichen Handelns eine Bresche schlagen – und es soll der Verwaltung verdeutlichen, dass der Begriff „Amtsgeheimnis“ seine Grenze am Interesse der Öffentlichkeit findet.

Zu den Kernpunkten des IFG:

Das Gesetz soll das Verwaltungshandeln des Bundes durch erleichterten Informationszugang transparenter machen und die demokratischen Beteiligungsrechte der Bürgerinnen und Bürger stärken. Deshalb wird der allgemeine und voraussetzungslose Zugang zu amtlicher Information des Bundes unter Berücksichtigung des Daten- und Geheimnisschutzes eröffnet. Ein rechtliches Interesse muss man nicht darlegen. Das Gesetz gilt außer für die Behörden des Bundes auch für sonstige Bundesorgane und -einrichtungen, soweit sie öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen. Die Behörde kann Auskunft erteilen, Akteneinsicht gewähren oder auf andere Weise Informationen zur Verfügung stellen. Als Information gilt jede Aufzeichnung, die amtlichen Zwecken dient – unabhängig von der Art ihrer Speicherung. Entwürfe und Notizen, die in den Vorgang nicht einfließen, gehören nicht dazu. Ausführlich ist dann aber der Katalog, der Ausnahmen von dieser Möglichkeit unter dem Kapitel „Schutz von besonderen Belangen“ nennt.

Ein Anspruch auf Informationszugang besteht z.B. dann nicht, wenn das Bekannt werden der Information nachteilige Auswirkungen auf

Internationale Bemühungen,

militärische und sonstige sicherheitsempfindliche Belange der Bundeswehr, der inneren oder äußeren Sicherheit, Angelegenheiten der externen Finanzkontrolle oder Maßnahmen zum Schutz vor unerlaubtem Außenwirtschaftsverkehr haben könnte.

Weitere Punkte im Ausnahmekatalog sind die mögliche Benachteiligung gesetzlicher Interessen des Bundes oder auch Fälle, in denen die allgemeine Verwaltungsvorschrift Geheimhaltungs- oder Vertraulichkeitspflicht zum materiellen und organisatorischen Schutz von Verschluss-Sachen vorsieht.

Wichtig – auch im politischen oder journalistischen Umgang mit den Informationen – ist außerdem der Schutz des Entscheidungsprozesses in den Behörden. Damit gemeint sind Fälle, in denen Entwürfe und Beschlüsse, die vorzeitig bekannt werden, dem gesamten Projekt schaden oder es zum Misserfolg verdammen. Bei personenbezogenen Daten muss das Interesse des Antragstellers dasjenige des Dritten überwiegen, oder der Betroffene muss in die Herausgabe der Daten eingewilligt haben.

Die Informationen sollen unverzüglich, spätestens aber nach einem Monat und – falls besonders umfangreich und komplex – nach zwei Monaten herausgegeben werden.

Das IFG benennt außerdem die Modalitäten der Aushändigung von Informationen und legt fest, dass der Bundesbeauftragte für die Informationsfreiheit mit dem Bundesdatenschutzbeauftragten identisch ist.

Schließlich möchte ich noch die Befristung des Gesetzes erwähnen: es gilt zunächst einmal für 5 Jahre.

Soweit die Kernpunkte des Gesetzes. Und nun zur Kernfrage: Brauchen wir das Gesetz? Ist es sinnvoll und wirkungsvoll? Besteht ein starkes öffentliches Bedürfnis danach? Meine Antwort: Ganz klar, wir brauchen es, es ist sinnvoll. Es kann wirkungsvoll sein, wenn das bislang nicht sehr stark ausgeprägte öffentliche Interesse wächst, wenn die Bürger das neue Recht abfordern und wenn die Verwaltung selbst ihr Scherflein zur Akzeptanz des Gesetzes beisteuert. Auch der Verfassungsvertrag für die EU, den wir im deutschen Bundestag gerade eben mit großer Mehrheit beschlossen haben, enthält ein Grundrecht auf Informationszugang ebenso wie ein Grundrecht auf eine gute Verwaltung!

Am 14. März 2005 haben wir Fachleute im Rahmen einer öffentlichen Sachverständigenanhörung vor dem Innenausschuss zu unserem Gesetzentwurf befragt. Von 9 Experten haben nur 3 sich gegen das Gesetz ausgesprochen bzw. deutliche Bedenken dagegen artikuliert. Die übrigen begrüßten die Initiative, fanden sie jedoch in einigen Punkten zu zaghaft und zu stark mit Möglichkeiten ausgestattet, den Informationsanspruch auszubremsen.

Setzen wir uns erst mal mit Kritik und Bedenken auseinander.

Ein Einwand lautet: das, was unter „Geschäftsgeheimnissen“ aufgeführt werde, sei nicht gesetzlich definiert. Letztendlich müsse man doch, so argumentiert z.B. Klaus Bräuning vom Bundesverband der Deutschen Industrie, darunter die „Summe aller Erfahrungen und Fabrikationsleistungen, Produktionsverfahren, Lizenzen, Vertriebswege bei Unternehmen, die im Wettbewerb stehen“, zusammenfassen. Er hat auch ein Beispiel parat: Bei der Entwicklung von Arzneien entstünden nicht selten Kosten von 700 bis 800 Millionen Dollar. Wenn dazu Daten in 600 Aktenordnern angelegt würden und daraus auch nur ein Teil – während der Entwicklungsphase, wie gesagt – bekannt würde, könne dies das Unternehmen ernsthaft treffen. Dem lässt sich entgegenhalten, dass in vielen anderen Ländern Informationsfreiheitsgesetze längst existieren, ohne dass die Wirtschaftswelt aus den Angeln geraten wäre. Dem halten die Bedenkenträger der Industrie nun wiederum entgegen: ein Rechtsvergleich mit anderen Ländern hinke insofern, als man über die reine Kenntnis der Gesetze hinaus die unterschiedlichen Rechtskulturen in einzelnen Staaten beachten müsse. In Deutschland gebe es für einen umfassenden Auskunftsanspruch des Einzelnen, ohne ein rechtliches Interesse darlegen zu müssen, keinen Bedarf.

Was mit der Rücksicht auf unterschiedliche Rechtskulturen gemeint sein könnte, präzisierte im Verlauf des Hearings ein weiterer Kritiker, nämlich Prof. Martin Ibler von der Universität Konstanz (Fachbereich Rechtswissenschaft). Mit dem voraussetzungsfreien Informationsanspruch, so seine These, werden die Rechte Dritter zurückgedrängt. Das führt zwar, so sagt er, zu einer Kontrolle der staatlichen Verwaltung, aber zu einer willkürlichen, weil jeder Bürger beliebig Fragen stellen und punktuell sich nur nach dem erkundigen könnte, was ihn persönlich interessiert – nach anderem nicht. Prof. Ibler spricht von einem „Informationszugang, der von links und rechts dazwischen schießt."

Dieser Vorwurf ist nicht ganz von der Hand zu weisen. Natürlich kann es geschehen, dass Vorgänge zu bestimmten Themen und Vorhaben heiß begehrt sind, andere ebenso wichtige aber nicht. Das spricht aber nicht gegen die Intention des Gesetzes. Man kann ja den Bürger nicht zur Neugier auf alles und jedes zwangsverpflichten! In eine ähnliche Richtung wie diejenige von Prof. Ibler zielt die Argumentation von Dr. Utz Schliesky, Universität Kiel und zugleich Vertreter des Deutschen Landkreistages. Er gewichtet besonders den rechtsstaatlichen Aspekt. Er bezweifelt, dass die demokratischen Mitwirkungsrechte durch das IFG tatsächlich gestärkt werden. Für ihn erweist sich demokratische Beteiligung dann, wenn man nicht nur einen Vorgang, eine Akte kennt – sondern wenn man aus dieser Kenntnis heraus befähigt wird, etwas zu tun. Über solche Beteiligungsrechte sage das Gesetz eigentlich gar nichts. Ein deutscher Staatsangehöriger habe wenigstens die Möglichkeit, etwa bei der nächsten Wahl zu reagieren, ein Ausländer schon mal nicht. Dem möchte ich nun entgegnen: auch das spricht nicht gegen das Informationsfreiheitsgesetz, sondern eher für eine vorsichtige und wohl durchdachte Ergänzung unserer repräsentativen Demokratie durch Elemente direkter Teilhabe, wie wir sie in der rotgrünen Koalition mit der geplanten Einführung von Plebisziten in einem dreistufigen Verfahren (Volksinitiative/Volksbegehren/Volksentscheid) anstreben – leider bislang ohne eine Chance auf die Zweidrittel-Mehrheit. Gerade wenn man sieht, wie die Bürger in den vergangenen Jahren Kommunal- und Landtagswahlen als Ventil für Frust und Unzufriedenheit über die Bundespolitik bzw. einzelne ihrer Vorhaben genutzt haben, spricht viel für einen neuen Vorstoß in Richtung „direkter Demokratie".

Zurück zu weiteren Argumenten gegen das Gesetz. Unionspolitiker vermissen in dem Vorhaben die Erfordernis zum subjektiven Rechtsschutz als einer Säule des öffentlichen Rechts. Es gibt außerdem Befürchtungen, dass das ganze Unterfangen mehr Bürokratie erzeuge und deshalb kein Beitrag zur Entbürokratisierung sei. Dagegen sprechen nun die Erfahrungen in anderen Staaten oder auch in Bundesländern, die ein Informationsfreiheitsgesetz haben. Kaum irgendwo sind in der Praxis ausufernde Bürokratie oder übermäßige Belastung der Verwaltung beklagt worden. Immer wieder wird auch gerade das Recht auf informationelle Selbstbestimmung in Deutschland genannt, dem ein Grundrecht auf Anonymität zugesellt sei, von Datenschützern konzipiert. So etwas gebe es in anderen Staaten nicht; deshalb sei unser IFG-Entwurf kritikwürdig, zumindest müsse der Ausnahmekatalog so umfangreich sein wie nun bereits formuliert.

Hochinteressant fand ich – und finden sicherlich auch die hier versammelten Datenschützer – die Auseinandersetzung um die Doppelrolle des Beauftragten für den Informationszugang und den Datenschutz. Prof. Ibler hebt hervor, dass der Staat nur Daten zu ganz bestimmten Zwecken erheben dürfe. Dem laufe die Identität zwischen Datenschutz – und Informationsbeauftragtem zuwider. Dieser werde sozusagen zum „Datenpreisgeber" gemacht. Ganz anders Dr. Falk Peters von der „European Society für eGovernment". Der findet nämlich gerade die Verquickung der beiden Funktionen deshalb positiv, weil der Datenschutz- und Informationszu-

gangs-Beauftragter ja schlichten und für das zuständig sein soll, was nach Ablehnung des Auskunftsbegehrens passiert. Die Vermittler-Rolle sollte er auch bei der Definition dessen wahrnehmen, was als Betriebs- oder Geschäftsgeheimnis geschützt werden muss. Der Datenschutz selbst ist nach Ansicht von Falk Peters durchreguliert und von einer soliden Rechtsprechung untermauert. Man müsste eigentlich nur im IFG regeln, dass der Datenschutz dem Auskunftsbegehren Schranken setzt. Gute Erfahrungen mit der Doppelrolle führt auch Dr. Alexander Dix, Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg ins Treffen.

Damit sind wir nun im Lager der Befürworter. Durch ihre Bewertung zieht sich wie ein roter Faden, dass sie das IFG für notwendig, ja überfällig halten. Sie halten allerdings den Ausnahmekatalog für zu weit gefasst. „Schaut ihn noch mal kritisch durch“, sagt z.B. Alexander Dix; „strafft ihn. Es muss auch einmal dabei herauskommen, dass Geheimhaltungsgründe hinter einem überwiegenden Offenlegungsinteresse zurücktreten sollten“. Verständnis für die Nöte des Gesetzgebers in komplizierten und langwierigen Abstimmungsprozess zeigte Prof. Michael Klöpfer von der Berliner Humboldt-Universität: die Ausnahmen nehmen für ihn einen viel zu breiten Raum ein; man müsse sich bei der Lektüre fragen, wo die „Hauptmusik“ spiele – bei der Informationsfreiheit oder beim Geheimnisschutz. Es gefällt ihm auch nicht, dass nicht nur einzelne Belange, sondern ganze Bereiche geschützt werden sollen. Er erkennt aber an, dass der Gesetzgeber „auf der sicheren Seite“ sein sollte. Man könne jedoch zur Beruhigung für die Zweifler darauf verweisen, dass im Ausland Befürchtungen über die möglichen negativen Auswirkungen der Informationszugangsgesetze nicht eingetreten seien; auch die vier Bundesländer, die über ein IFG verfügen, seien in den Verwaltungsabläufen nicht gelähmt worden; und schließlich gebe es auf Bundesebene gute Erfahrungen mit dem seit 10 Jahren existierenden Umweltinformationsgesetz.

Im Schlussteil meiner Anmerkungen zum IFG noch ein paar Überlegungen, die über den reinen Nutzwert und die Praxis des neuen Gesetzes hinausgehen.

Kann es beispielsweise das Verhalten der Verwaltung, sprich: der Mitarbeiter in den Behörden, beeinflussen? Zwar hat die Verwaltung es wahrscheinlich immer noch leicht, Gründe für die Ablehnung eines Informationsbegehrens zu finden. Aber allein die Existenz des Gesetzes kann löbliches bewirken, so versichern uns auch einige Experten. Es schütze im Übrigen vor Anwandlungen der Korruption, so meint Dr. Manfred Redelfs vom Netzwerk Recherche e.V., wenn Beamte wissen, dass es Bürgeranfragen und journalistische Recherche geben kann. Diese These vertritt, wie man unschwer vermuten kann, auch Peter Eigen von Transparency international. Transparenz und Teilhabe sind im übrigen Schlüsselwerte einer lebendigen Demokratie. Wer sie missachtet oder aber nur die Begriffe im Munde führt, ohne solcher Einsicht auch konkretes Handeln folgen zu lassen – der muss sich über Bürger-Missmut und Bürokratieschelte – so unberechtigt sie oft auch sein mag – nicht wundern.

Mir scheint’s, dass der Drang nach Einblick, nach Transparenz stark ist. Das macht den Anspruch der Bürger aus. Auf der anderen Seite bewirken demokratische Beteiligungsrechte bei den Bürgern auch einen Kulturwandel bei den Behörden. Wer weiß, dass er unter den Augen einer neugieriger werdenden Öffentlichkeit arbeitet, bemüht sich um Effizienz, Logik und Verständlichkeit, und dies tut dem Selbstverständnis des Verwaltungsapparates hoffentlich sogar gut. Mit anderen Worten: Dadurch, dass der Bürger Informationsansprüche hat und auch geltend macht, kann er die Verwaltung zugleich steuern.

Neuerdings wird häufig der Satz bemüht: „Wenn man ein Gesetz nicht unbedingt braucht, sollte man sich gut überlegen, ob man es beschließt“.

Ich sage mit Nachdruck: Wir brauchen das Gesetz, und deshalb wollen wir´s auch beschließen.

Zunächst einmal holen wir einen rechtspolitischen Rückstand gegenüber mehr als 50 Ländern dieser Erde und auch gegenüber der Rechtsentwicklung der EU auf. Wir müssen uns nicht unbedingt an Schweden messen, wo es das Prinzip, Informationen von staatlichen und kommunalen Behörden abzufordern, mit einigen kürzeren Unterbrechungen schon seit 1766 gibt. Aber festzustellen ist, dass zum gegenwärtigen Zeitpunkt in 50 Staaten ein Informationsfreiheitsgesetz existiert und die Bundesrepublik zusammen mit Luxemburg, Malta und Zypern zu den letzten gehört, die noch am Prinzip des Amtsgeheimnisses festhalten. Insofern nötigt es manchem schon ein ironisches Lächeln ab, dass einzelne Abgeordnete aus dem Unionslager mahnten, ein solcher Systemwandel gehe nicht im Hauruck-Verfahren.

Wir sind also endlich auf der Zielgerade; wir brauchen das Gesetz, weil es nicht nur Bürgerrechte, sondern auch die Verwaltung stärken kann. Das setzt freilich auch voraus, dass Menschen sich des Gesetzes bedienen und entsprechend aus den neuen Möglichkeiten lernen: die Informations-Suchenden ebenso wie diejenigen, die die Informationen herausgeben.

Vor genau 30 Jahren formulierte das Bundesverfassungsgericht die Sätze: „Die parlamentarische Demokratie basiert auf dem Vertrauen des Volkes. Vertrauen ohne Transparenz, die erlaubt zu verfolgen, was praktisch geschieht, ist nicht möglich.“ Mit diesem Gesetz, so hoffen wir, nehmen wir Abschied vom überkommenen Misstrauen des Staates und seiner Behörden gegenüber. Wenn die Bürger ihrerseits durch ihre neuen Möglichkeiten des Informationszuganges Misstrauen gegenüber dem Staat abbauen, ist ein doppelter Nutzen erreicht.

Informationsfreiheit und Verwaltungsmodernisierung

Verwaltungsmodernisierung und Funktionalreform

Dr. Gottfried Timm, MdL

Innenminister des Landes

Mecklenburg-Vorpommern

Verwaltungsmodernisierung und Funktionalreform

Das Konzept der umfassenden Verwaltungsmodernisierung und Funktionalreform strebt im Wesentlichen folgende Ziele an:

Stärkung der kommunalen Selbstverwaltung, insbesondere der kommunalen Mandatsträger in Kreistagen, Stadt- und Gemeindevertretungen, sowie Förderung der Chancen bürgerlicher Mitwirkung und des bürgerschaftlichen Engagements.

Steigerung der Leistungsfähigkeit der Verwaltung einschließlich der Organisation, der Verfahrens- und Entscheidungsabläufe und des Personals auf allen Ebenen der öffentlichen Verwaltung; effiziente Behördenstruktur; Verminderung der Kosten öffentlicher Dienstleistungen durch Aufgabenkritik; Nutzung von Synergieeffekten.

Schaffung möglichst transparenter, einfacher Verwaltungsstrukturen mit klarer Zuordnung von Kompetenz und administrativer sowie politischer Verantwortung.

Abbau von bürokratischen Hemmnissen durch Deregulierung und Aufgabenkritik.

Verbesserung der Bürgernähe möglichst aller Dienstleitungen des öffentlichen Sektors durch Vereinfachung und Verkürzung der Entscheidungsstrukturen (ortsnaher Verwaltungsvollzug); verstärkte Ergebnis- und Kundenorientierung des Verwaltungspersonals; Angebot einer einzigen Anlaufstelle für Bürger und Unternehmen.

Die Modernisierung der öffentlichen Verwaltung in Mecklenburg-Vorpommern ist ein Gesamtvorhaben, das alle Ebenen umfasst. Ihre Bestandteile sind:

- Deregulierung,
- Reform der Struktur der Gemeindeverwaltung durch Ämter- und Gemeindefusionen,
- Straffung der Landesorganisation,
- Personalkonzept für die Landesverwaltung,
- Weiterentwicklung von eGovernment,
- Funktionalreform I und II sowie
- Kreisstrukturreform.

Weite Teile wie die Ämterstrukturreform sind bereits umgesetzt, andere befinden sich in einem fortgeschrittenen Stadium.

Alle sind miteinander verbunden. Das Gesamtvorhaben der Reform ist die Antwort auf die mit Gewissheit absehbaren demografischen und finanziellen Entwicklungen im Land, die zum Handeln zwingen, um das öffentliche Wohl nicht zu gefährden.

EGovernment prägt zunehmend die Verwaltung und erschließt neue Möglichkeiten. Es verbessert die Möglichkeiten der Zusammenarbeit der Behörden und überwindet Entfernungen. Übergeordnetes Ziel des eGovernment muss es sein, Verwaltungsverfahren zwischen den Behörden des Landes und den kommunalen Körperschaften durchgehend und umfassend elektronisch abwickeln zu können.

Dem Bürger müssen Verwaltungsdienstleistungen zunehmend online angeboten werden. Ihm ist über seine örtliche Verwaltung Zugang zu den Kreisverwaltungen und Landesbehörden zu eröffnen.

Die Landesregierung hat mit den kommunalen Landesverbänden eine einvernehmliche Regelung getroffen, um die Entwicklung des eGovernment im Land und in den Kommunen aufeinander abzustimmen.

Das Land hat seine Verfahren zu Planung und Durchführung von IT-Vorhaben gestrafft. Über die Einführung neuer IT-Vorhaben wird in einem zentralen Verfahren entschieden. Alle neuen IT-Vorhaben werden einem zentralen Projektcontrolling unterzogen, das auf operablen Zielen aufbaut.

Informationsfreiheit als Grundlage der Demokratie

Zitat: „Der erfolgreichste im Leben ist der, der am besten informiert ist.“ (Benjamin Disraeli, Britischer Premierminister (1804-1881)

Der freie Zugang des Bürgers zu Informationen ist eine der Grundlagen der Funktionsfähigkeit der repräsentativen Demokratie. Voraussetzung der Ausübung der demokratischen Teilhabe des Einzelnen ist zum einen die Kenntnis dieser Rechte. Um Entscheidungen treffen zu können, benötigt er zum anderen auch das Wissen über Vorgänge, die im unmittelbarem Zusammenhang mit diesen Entscheidungen stehen. Er muss nicht nur wissen, dass er wählen kann, sondern auch welche Parteien sich zur Wahl stellen und Zugang zu deren Programmen erlangen.

In der Erkenntnis dieser Zusammenhänge haben die Väter des Grundgesetzes das Recht des Einzelnen in § 5 Grundgesetz aufgenommen, sich aus den allgemein zugänglichen Quellen ungehindert zu unterrichten.

Neben dem Recht auf Informationsfreiheit aus Art. 5 Grundgesetz hat das Recht des Bürgers auf freien Zugang zu Informationen der Verwaltungsbehörden in der öffentlichen Diskussion seit einigen Jahren eine zunehmend bedeutendere Rolle eingenommen. Hintergrund ist eine Weiterentwicklung der demokratischen Gesellschaft hin zu einem bürgerschaftlichen Engagement, dass über die Teilnahme an Wahlen hinausgeht. Die Bürger haben das legitime und wichtige Bedürfnis, sich aktiver und verantwortlicher an der Gestaltung des Gemeinwesens zu

beteiligen. Voraussetzung für ein solches Engagement ist die Möglichkeit, sich Meinungen und Haltungen auf der Grundlage gesicherter und umfassender Information bilden zu können.

Übertragen auf die politischen Entscheidungsprozesse in unserer Demokratie bedeutet dies, dass der Bürger schon in einem frühem Stadium Zugangsmöglichkeiten zu Informationen aus der staatlichen Verwaltung erhalten sollte, um an der Willensbildung teilhaben zu können. Nur der informierte Bürger hat die Möglichkeit, über das Herantreten an die Öffentlichkeit, Parteien und Volksvertreter Einfluss zu nehmen. Dergestalt aktive Bürger identifizieren sich mit der bewährten Staatsform und bilden so das Rückrat einer gesunden demokratischen Gesellschaft.

Informationsfreiheitsgesetz: kein aktueller Gesetzgebungsbedarf in Mecklenburg-Vorpommern

Die Landesregierung Mecklenburg-Vorpommern verfolgt mit Interesse das Gesetzgebungsverfahren zum Informationsfreiheitsgesetz im Bund und die Diskussion in den Ländern. Die praktischen Erfahrungen der Länder Brandenburg, Berlin, Nordrhein-Westfalen und Schleswig-Holstein, die in der jüngeren Vergangenheit einen verfahrensunabhängigen Informationsanspruch der Bürger gegenüber der Verwaltung normiert haben, wird bei weiteren Überlegungen im Land hilfreich sein.

Angesichts dieses Befundes mag es Sie überraschen, dass die Landesregierung Mecklenburg-Vorpommern derzeit jedoch keinen aktuellen Gesetzgebungsbedarf hinsichtlich eines Informationsfreiheitsgesetzes sieht. Lassen Sie mich die Bedenken kurz darstellen:

Einerseits bestehen bereits rechtliche Instrumentarien zum freien Zugang von Informationen in einer Anzahl von Gesetzen. Andererseits sehe ich für das Land Mecklenburg-Vorpommern die Möglichkeit, den freien Informationszugang für die Bürger in das Gesamtkonzept der Verwaltungsreform einzubetten. Ich bin der Überzeugung, dass wir so den Bedürfnissen der Menschen in der Informationsgesellschaft entsprechen und unser Ziel der Modernisierung der öffentlichen Verwaltung gleichermaßen erfüllen können.

Ich will auch darauf hinweisen, dass bisher in unserem Land in der Öffentlichkeit keine Forderungen nach einem gesetzlichen Anspruch in größerem Umfang wahrgenommen werden konnten. So sind in den vergangenen Jahren sind nur einige wenige Anfragen und Petitionen zu dieser Frage im zuständigen Ministerium bearbeitet worden, wobei die Mehrzahl der Petenten aus anderen Bundesländern stammte.

Nach meinem Kenntnisstand belaufen sich die Fallzahlen in den Ländern mit einem Informationsfreiheitsgesetz auf erheblich weniger Anfragen als im Vorfeld erwartet. (Aber auf diese Frage wird Herr Professor Garstka in seinem Praxisbericht sicher eingehen). Übertragen auf das Land Mecklenburg-Vorpommern, unter Berücksichtigung der ländlichen Struktur, wären möglicherweise nur wenige hundert Anfragen im Jahr zu erwarten.
Vor diesem Hintergrund erscheinen andere Wege, die ich im Anschluss vorstellen werde, zur möglichst umfassenderen Information des Bürgers für unser Land sinnvoll.

Bestehende Rechtliche Instrumente zum freien Zugang zu Informationen

Die Landesverfassung regelt in Art. 6 Abs. 3 bereits einen Anspruch des Bürgers auf Zugang zu Informationen über die Umwelt. Gem. § 4 des Umweltinformationsgesetzes hat jeder Anspruch auf freien Zugang zu Informationen über die Umwelt, die bei einer Behörde oder einer Person des Privatrechts vorhanden sind. Weitere allgemeine Aufklärungspflichten sieht unter anderem das Sozialgesetzbuch vor.

Einen umfassenden Auskunftsanspruch gegenüber den Informationen des Bundes soll das im Gesetzgebungsverfahren befindliche Informationsfreiheitsgesetz des Bundes gewähren. Daneben gibt das Bauplanungsrecht dem interessierten Bürger die Möglichkeit, Entwürfe der zuständigen Behörden einzusehen.

Das Akteneinsichtsrecht nach § 29 Landesverwaltungsverfahrensgesetz steht zwar nur den Beteiligten eines Verwaltungsverfahrens zu, also im wesentlichen Antragstellern und Antragsgegnern, darüber hinaus verpflichtet § 25 jedoch die Behörden nach pflichtgemäßen Ermessen zu einer Auskunfts- und Beratungspflicht sowohl in Bezug auf Tatsachen also auch auf Rechtsfragen. Der Wortlaut der Regelung bezieht sich unmittelbar nur auf Hinweise und Auskünfte hinsichtlich des Verfahrens. Aufgrund allgemeiner Rechtssätze wird jedoch darüber hinaus von Rechtssprechung und Lehre eine allgemeine Verpflichtung der Behörden zu Hinweisen und Belehrungen angenommen. Die Grenzen derartiger Auskünfte sind dabei immer die berechtigten Belange Dritter, insbesondere das Recht auf informationelle Selbstbestimmung und das Geheimschutzinteresse des Staates.

In der tatsächlichen Praxis der Verwaltung, insbesondere in den Kommunen erhält der interessierte Bürger bereits vielfältige Mitteilungen über rechtliche Grundlagen und tatsächliche Vorgänge. Aus der täglichen Erfahrung anhand der eingehenden Petitionen, meine ich feststellen zu können, dass Bürgerfragen im Rahmen der Möglichkeiten umfassend beantwortet werden.

Zwar ist eine Modernisierung der Verwaltung hin zu mehr Bürgernähe erforderlich, das Selbstverständnis der Verwaltung hat jedoch bereits in den letzten Jahrzehnten eine Wandlung hin zum Dienstleitungsbewusstsein erfahren. Dies hat auch die Bereitschaft zu einer offenen Haltung gegenüber dem interessierten Bürger erhöht. Der Bürger muss heute nicht mehr die Erfahrungen des Hauptmanns von Köpenick erleiden: „Bleiben Sie draußen, zu fragen haben Sie hier gar nichts“.

Neue Wege des Informationszuganges in der Informationsgesellschaft:

Das Internet und der damit verbundene Stellenwert der Information hat unsere Gesellschaft verändert.

Zitat: „Information wird zum strategischen Rohstoff, ohne den Staaten und Volkswirtschaften nicht mehr steuern, letztlich nicht mehr existieren können“. (Edzard Reuter, ehem. Vorstandsvorsitzender Daimler-Benz AG).

Milliarden von Internetseiten mit kommerziellen und nichtkommerziellen Informationen stehen den Menschen in aller Welt im Bruchteil einer Minute zur Verfügung. Inzwischen sind ein Großteil der weltweit agierenden Unternehmen, supranationalen und nationalen, staatlichen und nichtstaatlichen Organisationen über das Internet erreichbar. Es werden sowohl direkt Erkenntnisse über Tatsachen oder Rechtsgrundlagen zur Verfügung gestellt als auch der

weitergehende Kontakt angeboten. Die Fülle der derart verfügbaren Informationen schafft einen erweiterten Kenntnisstand beim in der Demokratie aktiven Bürger und auch einen erhöhten Bedarf nach Wissen. Darüber hinaus bietet das Internet über Foren, Chatrooms, virtuelle Demokratie-Projekte (eDemocracy) dem im Netz Reisenden die Möglichkeit, sich mit anderen Nutzern auszutauschen und neue Formen der Demokratie zu üben.

Das Internet bereichert die Demokratie, schafft neue Beteiligungsformen und den Wunsch nach mehr und leichter zugänglichen Informationen aus der Verwaltung. Die Anforderungen an die Verwaltung sind daher gestiegen und haben sich gleichzeitig auch verändert. Der Bürger gibt sich nicht mehr mit übersandten Broschüren zufrieden. Die gesuchten Informationen sollen möglichst im Internet eingestellt sein und auch leicht aufzufinden. Es reicht auch nicht aus, Texte der Verwaltung lediglich zu scannen und bereit zu stellen. Der Anwender erwartet Formate, die gedruckt, bearbeitet und an Dritte übermittelt werden. Auch der Stil der Texte ist entscheidend. Der Empfängerhorizont der „User“ im Netz ist schwerer einzuschätzen als der eines Adressaten im förmlichen Verwaltungsverfahren. Daher ist es erforderlich, eingestellte Informationen so verständlich zu gestalten, dass jeder sie versteht. Das Internet schafft auch eine neuen Stil des Kommunizierens, informaler und direkter. Dem entsprechend wächst eine Generation von Bürgern mit Teilhaberechten heran, die es für selbstverständlich hält, Informationen als Angebot zu erhalten, die innerhalb von Minuten im Download verfügbar sind. Ob eine Antragstellung im Sinne eines Informationsfreiheitsgesetz mit anschließender Bescheidung durch eine Behörde diesen Bedürfnissen entspricht, wird sich erst zeigen müssen.

Gesamtkonzept des Zugangs zu Informationen im Rahmen der Verwaltungsmodernisierung

Um den vorgenannten besonderen Anforderungen der Informationsgesellschaft gerecht zu werden und gleichzeitig die Ziele der Verwaltungsreform zu erreichen, strebt die Landesregierung ein Gesamtkonzept zur Verbesserung des Zuganges der Bürger zu Informationen der Verwaltung an. Der Schwerpunkt liegt hierbei beim verstärkten Einsatz von Internetportalen im Rahmen von eGovernment.

Bestehendes Angebot

Bereits jetzt ist die Mehrzahl der Behörden des Landes mit einem Informationsangebot und Angeboten zur elektronischen Kontaktaufnahme im Internet vertreten. Es werden Termine bekannt gegeben, Pressemitteilungen als elektronisches Archiv zur Verfügung gestellt und rechtliche Hinweise erteilt. Darüber hinaus stehen auch Dokumente zu einzelnen Themenbereichen zum Download bereit. Die fachlichen Ansprechpartner in der Verwaltung zu den einzelnen Aufgabengebiete sind mit Kontaktadressen aufgeführt.

Das Landesrechtsinformationssystem des Landes ermöglicht den Abruf aller geltenden Gesetze und Verordnungen des Landes Mecklenburg-Vorpommern und bietet daneben auch ein Archiv der außer Kraft gesetzten Vorschriften.

Masterplan eGovernment

Der Masterplan eGovernment, der die Strategie der Landesregierung auf dem Gebiet der elektronischen Verwaltung darstellt, zielt auf die Erweiterung und Weiterentwicklung des bestehenden Angebotes sowohl auf verwaltungsinterner Ebene als auch zur Verbesserung der Informationsbasis der Bürger ab.

Bestandteile sind unter anderem eine Erweiterung der Präsentation der Polizei nach außen, das Auskunftsverfahren elektronisches Grundbuch, das Auskunftsverfahren elektronisches Handelsregister, sowie der Aufbau eines Geodatenportals. Dies ist aus meiner Sicht jedoch nur der Anfang einer Entwicklung, deren Ende nicht abzusehen ist.

Verwirklichung der Ziele der Verwaltungsreform durch die Bereitstellung von Informationen in Internetportalen

Durch die Bereitstellung von Informationen in Internetportalen werden im Gegensatz zur Regelung eines Informationsanspruches im Gesetz die Ziele der Verwaltungsreform erreicht. So wird die Leistungsfähigkeit der Verwaltung gestärkt, da umständliche Verfahren mit Antrag und Bescheid vermieden werden. Beim Vorgang des Abrufens von Inhalten agiert der Bürger eigenständig, Personal wird für diese Vorgänge nicht gebunden. Die Bürgernähe wird verbessert. Die Informationen sind einfach und kurzfristig zugänglich, zudem besteht eine zusätzliche Kontaktmöglichkeit über eMail. Ferner stellt sich der Verzicht auf die Normierung eines Informationsanspruches im Gesetz als Maßnahme der Deregulierung dar, aus Sicht der Landesregierung eines der wichtigsten Instrumente der Verwaltungsmodernisierung.

Zusätzliche bürokratische Hemmnisse werden nicht aufgebaut, der direkte Zugriff auf die Information ist zweifellos bürgerfreundlicher als ein zusätzliches Verfahren.

Instrument eines Gesamtkonzepts zum Informationszugang: Selbstbindung der Verwaltung

Ein mögliches weiteres Instrument im Rahmen eines Gesamtkonzepts zur Verbreiterung der Informationsbasis der Bürger könnte meines Erachtens die Zielvereinbarung sein. Diese ist flexibel zu handhaben und beinhaltet gleichzeitig die Messung der Arbeitsergebnisse nach Ablauf eines bestimmten Zeitraumes. Hierbei könnte im Rahmen einer Vereinbarung zwischen der jeweiligen Behördenleitung und den Mitarbeitern das konkrete Ziel der Verbesserung des Informationszuganges der Bürger als Handlungsdirektive unter Einbeziehung der Maßnahmen zur Erreichung und Festlegung von Evaluierungszeiträumen- und Methoden vereinbart werden. Als mögliche Maßnahmen sehe ich in diesem Zusammenhang unter anderem Schulungen zur stärkeren Verankerung der Auskunft als Dienstleistung im Bewusstsein der Mitarbeiter.

Verwaltung in der Informationsgesellschaft

Professor Dr. Alexander Roßnagel
Universität Kassel
Institut für Wirtschaftsrecht und Forschungszentrum für Informationstechnik-Gestaltung,
Fachbereich Wirtschaftswissenschaften Verwaltung in der Informationsgesellschaft

Verwaltung in der Informationsgesellschaft

Übersicht

E-Government heute
Aufgaben der Verwaltung künftig
Transparenz als Handlungsmodus künftiger Verwaltung

- Information
- Kommunikation
- Transaktion

Wandel durch E-Government

- Strukturen
- Verfahren

Wandel durch M-Government
Ausblick: Wandel von Verwaltungskulturen

E-Government heute

Aufgaben und Probleme
Internetportale
Öffentliche Register und Informationsabruf
Virtuelle Poststelle
Medienbruchfreier Workflow
Sichere elektronische Identifizierung und Authentisierung
Förderung qualifizierter elektronischer Signaturen

Informationsgesellschaft und Verwaltung

Informationsgesellschaft

Erzeugung, Verteilung und Nutzung von Informationen werden zum entscheidenden Wirtschaftsfaktor

Gesellschaft verändert ihr Informations- und Kommunikationsverhalten den Möglichkeiten entsprechend

Sie stützt sich auf Informations- und Kommunikationstechniken

Verwaltung

Geordnete Sammlung von Informationen und rationale kommunikative Erzeugung von Entscheidungen zur kooperativen Gemeinwohlkonkretisierung

Verwaltung muss auf Änderungen im Informations- und Kommunikationsverhalten der Gesellschaft reagieren und die technischen Möglichkeiten für ihre Zwecke nutzen

Aufgabenentwicklung und Aufgabenwandel

Gewährleistungs- und Strukturverantwortung

Reduktion der Erfüllungsverantwortung zur Ermöglichung von Grundrechtswahrnehmung

Förderungen und Rahmensetzung für Eigenverantwortung

Ermöglichung von Selbstregulierung und Selbstbestimmung

Kooperative Handlungskoordination

Gegenseitiger Ausgleich von Informationsdefiziten

Abstimmung von Handlungsmöglichkeiten

Organisation von Informationsprozessen

Angebot von Orientierungshilfen und Handlungsentwürfen

Organisation von Ausgleichsmechanismen für Informationsasymmetrien

Informationsvorsorge

Aktives Angebot von Informationen zur Sicherung von Kompetenz und Akzeptanz

Transparenz als Handlungsmodus

Grundrechte

Garantie von Informations- und Kommunikationschancen als Grundlage persönlicher Lebensgestaltung und wirtschaftli**chen Handelns**

Informationsfreiheit

Grundlage der Grundrechtswahrnehmung – Ausweitung des Öffentlichen

Demokratie

Anregung und Kontrolle der Verwaltung – Voraussetzung demokratischer Willensbildung

Sozialstaat

Zugang und Teilhabe an Informationen – aktives Informationshandeln

Rechtsstaat

Ausgleich von Informationsmacht, Schutz des Einzelnen und Kontrolle der Verwaltung

Informierende Verwaltung

Neue Handlungsformen: Online

Ausweitung bestehender Möglichkeiten:

z.B. Bekanntmachung, Auslegung und Einsichtnahme

Neue Darstellungsformen: Hypermedia

Erweiterung von Text- und Bilddarstellungen:

z.B. Simulationen, Virtual Reality, Interaktivität

Neue Informationsinhalte: Datenbanken

Eröffnung neuer Informationsressourcen:

z.B. Öffentlicher Zugriff auf Verwaltungsdatenbanken

Neue Informationskombinationen: Verknüpfungen

Anreicherung von Verwaltungsinformationen:

z.B. Verknüpfung mit Informationsangeboten gesellschaftlicher Organisationen

Kommunizierende Verwaltung

Transparenz für Betroffene

Akteneinsicht – Kontrolle des Verfahrensstandes – Datenschutzauskunft

Transparenz für Interessierte

Einsicht in Akten und allgemeine Verwaltungsinformationen – „Elektronische Nebenakten“ wie E-Mails, Bookmarks, Histories

Transparenz für Engagierte

Organisation von Kommunikationsprozessen zwischen Verwaltung und engagierten Bürgern in Verwaltungs- und Planungsprozessen oder Bürgerprojekten

Transparenz für Informationsbedürftige

Dialogisches Verwaltungsverfahren durch Beratung und Unterstützung (Mobile Agenten oder One-Stop-Government)

Agierende Verwaltung

Elektronische Akte

Medienbruchfreie Kooperation von Antrag bis Entscheidung

Hybridakte

Umgang mit körperliche Bestandteilen – Transformation P2E

Kompatibilität

Unterstützung nur weniger Formate – Transformation E2E

Archivierung

Langfristige Aufbewahrung elektronischer Dokumente – Sicherung von Integrität, Authentizität und Lesbarkeit

Wandel der Strukturen

Virtuelle Präsenz

Unabhängigkeit von Ort und Zeit

Kooperation und Kontrolle auf Distanz

Ubiquitäres Verwaltungswissen

Keine lokale Verfügbarkeit des Verwaltungswissens notwendig

Reduzierte spezifische Ortsbindung der Verwaltung

Funktionale Verwaltungsorganisation möglich – Zentralisierung von Fachwissen – Dezentralisierung von Entscheidungskompetenz

Automatisierte Kooperation

Erfüllung von Informationspflichten

Agenten für Bürger und Verwaltung

Wandel der Verfahren

Beispiel: Technikrechtliche Genehmigungsverfahren auf der Basis von multimedialen Simulationsmodellen

Vorverlegung des Genehmigungsverfahrens

Konstruktion begleitende Prüfung

Verwendung genehmigter Komponenten

Abschichtung von Prüfthemen

Verbesserung der Öffentlichkeitsbeteiligung

Frühzeitige Beteiligung Verständliche und prüfbare Unterlagen Rationalisierung und Erhöhung von Konsenschancen

Mögliches Ergebnis

Schnellere Zulassung von Techniksystemen ohne Reduktion der Prüfungstiefe und bei verbesserten Beteiligungschancen

Mobilisierte Verwaltung

Technische Mobilität

Nicht nur neuer Zugangskanal zur Verwaltung, sondern auch neue Handlungsmöglichkeit für bürgernahe Verwaltung

E-Government

Zeit- und ortsunabhängig, aber Kommunikation mit Computer Ausrüstung und Medienkompetenz erforderlich

M-Government

E-Government mit menschlichem Gesicht

Verbindet persönlichen Kontakt mit allen Möglichkeiten des E-Government

Kooperative Verwaltung

Ergänzt bisherige Verwaltungstätigkeit, wo Informationssammlung, Augenschein, Beratung oder mangelnde Medienkompetenz dies erfordert

Ausblick: Wandel von Verwaltungskulturen

Technikunterstützte Modernisierung der Verwaltung

Nur eine Möglichkeit:

Kultur der Transparenz

Stärkt Vertrauen, Legitimation, Akzeptanz und Integration

Stärkt aktive Kräfte in der Verwaltung

Freiheit des Zugangs zu Verwaltungsinformationen

Zu informationeller Selbstbestimmung komplementäres Ordnungsprinzip kommunikativer Freiheitsorganisation

Wandel von Verwaltungskulturen erfordert lange Anpassungszeiten

Praxisbericht eines Informationsfreiheitsbeauftragten

Professor Dr. Hansjürgen Garstka

Berliner Beauftragter für Datenschutz und Informationsfreiheit,

Vorstandsvorsitzender der Europäischen Akademie für Informationsfreiheit und Datenschutz

Praktische Erfahrungen mit den Informationsfreiheitsgesetzen in den Bundesländern

Berlin war nach dem Land Brandenburg das zweite Bundesland, das am 30. Oktober 1999 ein Landesinformationsfreiheitsgesetz bekommen hatte. Die Geschichte der Berliner Gesetzgebung reicht relativ weit zurück, denn schon im Herbst 1990 hat es eine erste Gesetzesvorlage gegeben, die allerdings bald in den Koalitionswirren der ersten rot-grünen Regierung scheiterte. Die Vorlage stammt schon aus den 80er Jahren. Sie war im Auftrag der Fraktion der Grünen im nordrhein-westfälischen Landtag von einem Anwalt erarbeitet worden. Dass die Quelle für die Gesetzgebung im Jahre 1999 da zu suchen ist, ist der Grund dafür, dass das Berliner Gesetz sowohl von der Anlage als auch vom Text deutlich abweicht von den anderen Gesetzen in Brandenburg, Nordrhein-Westfalen und Schleswig-Holstein.

Welches nun sind die Besonderheiten des Berliner Gesetzes? Am deutlichsten kann man das Berliner Gesetz dadurch charakterisieren, dass es im Gegensatz zur vorherigen Rechtslage, aber auch im Vergleich zu den Gesetzen in den anderen Bundesländern eine Verschiebung zwischen der Gewichtung des Datenschutzes und der Informationsfreiheit enthält. In Berlin gab es seit der Novellierung 1990 ein besonders strenges Landesdatenschutzgesetz, weil es keine Generalklausel für die Verarbeitung personenbezogener Daten mehr kannte. Vielmehr war seither für jede einzelne Verarbeitung eine ausdrückliche Rechtsgrundlage erforderlich.

Das Informationsfreiheitsgesetz änderte das in nahezu systemwidriger Weise, indem es nunmehr bei einem Einsichts- oder Auskunftsersuchen eine Abwägung erlaubt, ob schutzwürdige Belange von Betroffenen an der Geheimhaltung ihrer Daten das Informationsinteresse des Antragstellers überwiegen. Das bedeutet, dass Behörden bei einem Ersuchen trotz des Vorhandenseins personenbezogener Daten in den Unterlagen dem Antrag stattgeben können, wenn sie das Schutzinteresse der Betroffenen gegenüber dem Informationsinteresse z.B. einer Bürgerinitiative gering erachten. Die Betroffenen müssen dann in einem nächsten Schritt beteiligt werden, aber die Behörden können sich über Einwände der Betroffenen hinwegsetzen. Dann ist die vierwöchige Widerspruchsfrist abzuwarten.

Ein anderer Aspekt ist, dass für gewisse Grunddaten von Amtsträgern, Personen, bei denen Überwachungsmaßnahmen erfolgt sind, Eigentümern, Pächtern, Gutachtern und ähnlichen Personengruppen vermutet wird, dass schutzwürdige Belange dem Informationsanspruch nicht entgegenstehen. In diesem Fall können die Behörden ohne Beteiligung der Betroffenen Unterlagen herausgeben, wenn deren Daten in den Unterlagen vorhanden sind und diese sich auf gewisse Grunddaten wie Name und Adresse beschränken.

Nun zu meinem eigentlichen Auftrag, aus der Praxis in Berlin zu berichten.

Lassen Sie mich beginnen mit Fallzahlen. Es ist schon gesagt worden, dass die ursprünglichen Befürchtungen, dass die Verwaltungen lahm gelegt würden durch Informationsanträge, sich in allen vier Ländern nicht bewahrheitet hat. Bettina Sokol hat für Nordrhein-Westfalen 1000

Anfragen pro Jahr genannt, bei einer Umfrage ein Jahr nach Inkrafttreten des Berliner Gesetzes kamen 160 Anträge heraus. Wenn man die Bevölkerungszahlen in Betracht zieht, eine durchaus vergleichbare Größenordnung. Die Flut von Anträgen bleibt aus, bis auf den heutigen Tag ist die Zahl auf eine sehr überschaubare Dimension beschränkt.

Dies sagt allerdings nichts über die Bedeutung der Anfragen aus. Die Argumentation, es gebe ja nur so wenig Fälle, ist kein legitimer Anlass für Kritik, sondern umgekehrt: Man muss sagen, dass die Bürgerinnen und Bürger verantwortungsvoll mit der Inanspruchnahme des Informationsfreiheitsgesetzes um.

Was die Situation des Beauftragten für Datenschutz und Informationsfreiheit betrifft, muss man sich vor Augen halten, dass nicht alle Anträge bei uns auf den Tisch gelangen. Wir sind nur eine Schlichtungsinstanz, wir haben die Aufgabe, das Recht auf Informationsfreiheit zu wahren. Wir beschäftigen uns auf der einen Seite mit Anfragen aus den Behörden selbst, z.B. ob bestimmte Verweigerungsgründe in Anspruch genommen werden können. Auf der anderen Seite stehen die Eingaben von Bürgerinnen und Bürgern, die sich darüber beschweren, dass einem Antrag nicht nachgekommen wurde.

Der Umfang dieser Beschwerden bei uns beträgt ungefähr 50 im Jahr, das bedeutet zusammengenommen, dass sich etwa ein Drittel aller Antragsteller bei uns darüber beschwert, dass ihre Anträge abgelehnt wurden. Das ist bemerkenswert, weil daraus zu schließen ist, dass diejenigen, die vom Informationsfreiheitsgesetz Gebrauch machen, offensichtlich weitgehend wissen, dass es die Informationsfreiheitsbeauftragten als Beschwerdeinstanz gibt. Die Antragstellenden sind offensichtlich alle informierte Personen, die um ihre Rechte wissen. Es kann aber auch bedeuten, dass bereits die ablehnenden Behörden auf die Möglichkeit der Beschwerde hinweisen. Ursachenforschung ist hierzu bisher nicht betrieben worden.

Wie verhält sich die Anzahl der Anträge, denen stattgegeben wurde, zu den abgelehnten? In der erwähnten Umfrage hat man in Berlin festgestellt, dass in 50 Prozent der Fälle den Anträgen uneingeschränkt stattgegeben wurde. Das bedeutet, dass doch in einer sehr beachtlichen Zahl der Fälle die Verwaltung selbst der Auffassung ist, dass ein entsprechender Anspruch vorliegt. In 20 Prozent der weiteren Fälle gab es eine eingeschränkte Einsicht entweder durch partielle Einsicht in die Akte oder durch Schwärzungen. In 30 Prozent der Fälle wurde die Einsicht in Berlin abgelehnt.

In anderen Ländern ist das anders. In Schleswig-Holstein ergab eine entsprechende Statistik, dass in 88 Prozent der Fälle dem Antrag stattgegeben wurde. Auch das kann man schwer interpretieren ohne die Fälle selbst zu kennen. Das könnte bedeuten, dass in Schleswig-Holstein als einem Flächenland die Antragsteller und Antragstellerinnen mehr Anliegen vorbringen, bei denen die Verwaltungen kein Problem mit dem Informationszugang haben, dass dagegen in einer eher konfliktbeladenen Stadt wie Berlin mehr Anträge gestellt werden, bei denen es der Verwaltung nicht so einsichtig ist, dass die Unterlagen offen zu legen sind.

Interessant ist es, die abgelehnten Anträge näher zu betrachten. Bei diesen gehen 30 Prozent der Antragsteller in Widerspruch. Auch daran zeigt sich, dass es sich bei diesen in der Regel um Personen handelt, die ihre Rechte kennen. Bei den Gründen für die Ablehnung steht mit 37 Prozent an erster Stelle der Datenschutz. Ich sage später noch etwas dazu, da das Verhältnis zwischen Datenschutz und Informationsfreiheit ja das Thema dieser Tagung ist. Dann kommt ein sehr problematischer Grund, nämlich „der Schutz des behördlichen Entschei-

dungsermessens“, dann gleichauf der Schutz von Betriebs- und Geschäftsgeheimnissen. Was von den Sicherheitsbehörden in der Debatte um das Bundesinformationsfreiheitsgesetz immer vorgebracht wird, hat jedenfalls im Berlin nicht die geringste Rolle gespielt. Uns liegt seit Beginn nicht ein einziger einschlägiger Fall als Beschwerde vor.

Auch bereits hier angesprochen worden ist die Frage, wie lange es dauere, bis die Anträge bearbeitet werden. In Berlin liegt die Bearbeitungszeit nach der angesprochenen Umfrage zwischen 30 Minuten und 3 Monaten – letzteres war die höchste angegebene Bearbeitungsdauer. Die weitaus größere Zahl lag im unteren Bereich, was in einem Stadtstaat wie Berlin natürlich daran liegen kann, dass die Antragsteller selbst die Behörden aufsuchen, dort umgehend Einsicht in die Unterlagen erhalten und wieder gehen. Bei den langen Bearbeitungszeiten handelt es sich um Fälle, wo hin- und hergeschrieben wird oder wo Betroffene zu beteiligen sind. Im Streitfall kann es natürlich erhebliche Zeit dauern, bis die Erstbearbeitung nach Widerspruch, Beschwerde oder gar Klagverfahren zu einem Abschluss kommt.

Interessant ist auch der Umfang der Unterlagen, in die Einsicht begeht wird. Er schwankt nach der Umfrage zwischen 6 Seiten und 40 000 Seiten. Letzteres war ein Einsichtersuchen in eine Liegenschaftsangelegenheit bei der Finanzverwaltung, die in Berlin für die Grundstücksgeschäfte zuständig ist. Gerade hieran sieht man, wie unterschiedlich die Fälle sein können.

Was wollen die Bürgerinnen und Bürger wissen?

Zahlen liegen in Berlin nur für die Senatsverwaltungen und deren nachgeordnete Behörden vor, da die Bezirksämter ihre Angaben nicht nach Sachgebieten aufgeschlüsselt haben. Danach liegt die Innenverwaltung vorne, zu der etwa die Personalverwaltung gehört. Relativ viele Anfragen kommen – wie übrigens auch bei der Einführung der Datenschutzgesetzgebung zu beobachten war – von Beamten. Diese Berufsgruppe nimmt in eigenem Interesse oft Chancen wahr, gegen die sie zuvor Widerstand geleistet haben. Als nächstes folgen Finanz- und Stadtentwicklungsverwaltung, die in Berlin für das Grundstücks- und Bauwesen zuständig sind. Dann folgen Arbeits- und Sozialverwaltung, Justiz und in ganz geringem Umfang andere Behörden. Eine entsprechende Aufschlüsselung in Schleswig-Holstein zeigt übrigens, dass auch hier 50 Prozent der Anfragen in weitestem Sinne auf das Bauwesen beziehen – offensichtlich ein besonderes Interessenfeld für Informationsfreiheit. Die Innenverwaltung kommt hier kaum vor – wohl auch ein typischer Unterschied zwischen Stadt- und Flächenland.

Einige Einzelfälle sollen die ganze inhaltliche Palette erschließen, auf die sich Informationsfreiheit beziehen kann:

In unseren letzten drei Jahresberichten haben wir zum Beispiel über folgende Fälle berichtet – Sie könnten den Verlauf im Internet nachvollziehen:

Bewohner eines Kneipenkiezes, die sich in ihrer Nachtruhe gestört fühlten, wollten Einsicht in die Gewerbeakten bei der Gaststättenaufsicht, um zu überprüfen, welche Auflagen die einzelnen Gaststätten hatten. Dies ist übrigens ein Fall, bei dem die „Listenfreigabe“ des Berliner Informationsfreiheitsgesetzes eine Rolle spielte.

Einsicht wurde begehrt in die Niederschrift der Delegiertenversammlung der Zahnärztekammer, da ein Zahnarzt nachprüfen wollte, ob eine Entscheidung korrekt getroffen wurde – eine

Anfrage, die auf die Frage führt, ob Gremien einer öffentlichen Körperschaft wie einer Kammer überhaupt nichtöffentlich tagen sollten.

Ein Student einer Universität in Berlin wollte Einsicht in die Unterlagen zur Videoüberwachung in einem Hörsaal, von der zuvor niemand etwas wusste. Die Einsicht führte in der Tat dazu, dass bekannt wurde, dass noch aus DDR-Zeiten in einigen Hörsälen Videokameras installiert waren – angeblich um den Tontechnikern zu ermöglichen, die Mikrofone für die Hochschullehrer richtig einzustellen. Der Informationsantrag hat dazu geführt, dass alle Videokameras – bis auf die Überwachungskameras auf den Parkplätzen – abgebaut wurden.

Einsicht wurde beantragt in die Investitionsunterlagen von Pflegeheimen, die zur Genehmigung des (in der Regel hohen und von der Pflegeversicherung nicht erstatteten) Investitionsanteils bei den Heimgebühren vorgelegt wurden – oft werden jedenfalls für die Betroffenen nicht erforderlich erscheinende Umbauten durchgeführt, um offenbar diesen Anteil in die Höhe zu treiben.

Interesse fanden die Aufstellungen zum Krankenstand von Ärzten in einem Krankenhaus, um Informationen darüber zu erhalten, wieso die medizinische Betreuung zu wünschen übrig ließ.

Ein unbeteiligter Gast einer Gaststätte wollte bei der Berliner Polizei Einsicht in das Protokoll einer nächtlichen Razzia, bei der eine Mutter mit einem Kleinkind mit offenbar rüden Methoden abgeführt wurde. Er wollte sich darüber informieren, wieso die Polizei in dieser Situation so vorgegangen ist. Nach einer Beschwerde bei uns wurde Einsicht gewährt – es hat sich herausgestellt, dass der Einsatz auch aus der Sicht des Antragstellers gerechtfertigt war.

Eine Frau stellte in einer öffentlichen Bildergalerie fest, dass ein ausgestelltes Kunstwerk ihre Großmutter darstellt. Sie verlangte Einsicht in die Erwerbsunterlagen, um festzustellen, ob die Galerie rechtmäßig an das Bild gelangt war. Nach Zögern wurde Einsicht gewährt, die Sache ging mit rechten Dingen zu, am Ende stritt man sich über die Gebühren.

Der neueste bemerkenswerte Fall betrifft den Terminkalender des Berliner Regierenden Bürgermeisters. Ein Journalist wollte in einem bestimmten zurückliegenden Zeitraum Einsicht in oder zumindest Auskunft über dessen Termine und zwar ausdrücklich ohne die privaten Termine. Wir sind der Auffassung, dieser Anspruch bestehe natürlich, denn die amtlichen Termine haben selbstverständlich einen „amtlichen Bezug“. Wenn Ausnahmetatbestände vorliegen (z.B. Vorbereitung von Senatssitzungen) könnten diese Termine geschwärzt werden. Der Regierende Bürgermeister hat diese Einsichtnahme abgelehnt. Der Journalist klagte. Leider hat das Verwaltungsgericht Berlin vorläufig die Entscheidung getroffen, der Terminkalender des Regierenden Bürgermeisters sei keine amtliche Unterlage und falle damit nicht unter das Informationsfreiheitsgesetz. Beide Parteien waren sich allerdings einig, dass diese Frage besser das Oberverwaltungsgericht entscheiden solle. In anderen Ländern, z.B. in Mexiko (!), stellt der Präsident seinen Terminkalender in das Internet!

Welche Schwierigkeiten gibt es?

Bereits der Geltungsbereich des Gesetzes macht Probleme: Was sind Akten im Sinne des Gesetzes und was nicht? Das Terminkalenderbeispiel gehört dazu. Es gibt Streit mit einigen Stellen darüber, welche materiellen Verwaltungsbereiche unter das Gesetz fallen, obwohl das Berliner Gesetz – außer der Rechtsprechung – keine Ausnahmen kennt. Das ist z.B. der Streit

über Informationsfreiheit bei fiskalischer Tätigkeit, die im Gegensatz zu Berlin im künftigen Bundesgesetz privilegiert wird. Der Rechnungshof meint, er falle nicht unter das Gesetz, ebenso der Justizvollzug – jeweils ohne ausdrückliche Rechtfertigung im Gesetz.

Ein Problem, auf das man erst bei konkreten Prüfungen stößt, ist die unterschiedliche Entscheidungspraxis von Behörden. Es taucht vor allem auf, wenn sich mehrere Behörden parallel unter ihrem jeweiligen Blickwinkel mit den gleichen Vorgängen befassen, und die eine Akteneinsicht gewährt, die andere aber nicht, obwohl sich weitgehend die gleichen Dokumente im Vorgang befinden. Hier steht eine Entscheidung darüber aus, ob nicht eine verantwortliche aktenführende Stelle zu benennen ist, die die Entscheidung über den Informationszugang zu treffen hat.

Probleme mit der Gebührenberechnung sind hier schon angesprochen worden. Auf ein Problem kommt man auch erst in der Praxis: Es hat Fälle gegeben, in denen eine besonders hohe Gebühr erhoben wurde, weil die Unterlagen in einem Zustand waren, der einen korrekten Aktenzugang gar nicht zuließ. In einem neueren Fall musste die Verwaltung über 6 000 € für ein Bauingenieurbüro ausgeben, damit dieses die Akten, in die Einsicht begeht wurde, überhaupt so sortiert, dass dem Antrag stattgegeben werden konnte. Das ist natürlich weit mehr als der Gebührenrahmen in Berlin von gut 500 € zulässt. Wir sind der Auffassung, diese Kosten dürfen dem Antragstellenden nicht überantwortet werden. Weltweit hat sich im Übrigen gezeigt, dass Informationsfreiheitsgesetze zu einer Verbesserung der Aktenführung bei der Verwaltung geführt haben!

Problematisch ist der Verweigerungsgrund, dass Urheberrechte an (Teilen) der Akte bestehen. Rechtsdogmatisch ist dies die Frage, ob die Gewährung von Akteneinsicht gleichzusetzen ist mit der – urheberrechtlich kritischen – Veröffentlichung der Akte, denn in letzterem Fall hat der Urheber ein Einspruchsrecht. Richtig wäre hier, dass – entsprechend der Regelung des Berliner Gesetzes – erst die Fertigung von Kopien, nicht schon die Einsichtgewährung Urheberrechtsfragen aufwirft. Ein Fall, der zu lösen war, war das Anliegen eines Architekten, in Bauunterlagen einzusehen, in denen sich Baupläne eines anderen Architekten befanden, die nach seiner Auffassung von ihm kopiert waren.

Ein großes Problem stellt schließlich die Frage dar, unter welchen Voraussetzungen Betriebs und Geschäftsgeheimnisse der Akteneinsicht entgegenstehen. Entscheidend ist, ob derjenige, der das Geheimnis für sich Anspruch nimmt, alleine darüber befinden können soll, ob es sich um ein Betriebs oder Geschäftsgeheimnis handelt, oder ob die Behörde, die entsprechende Unterlagen hat, jedenfalls in einem ersten Schritt nicht selbst darüber entscheiden sollte. In Berlin gibt es eine derartige Regelung, das künftige Bundesgesetz überlässt die Entscheidung alleine dem angeblichen Geheimnisträger.

Zum Abschluss eine Antwort auf die Frage nach dem Verhältnis zwischen Datenschutz und Informationsfreiheit, die ja das Motto dieser Veranstaltung ist.

In unserer Berliner Praxis hatten wir in den vergangenen fünf Jahren bei nicht einer einzigen Beschwerde eine Situation, bei der ein unlösbarer Konflikt zwischen Datenschutz und Informationsfreiheit bestanden hätte. Das liegt wohl daran, dass die Antragsteller es akzeptieren, wenn ein Antrag aus Datenschutzgründen von der Behörde abgelehnt – und dieses gegebenenfalls dann von uns bestätigt wird.

Die Antwort auf die Frage lautet aus unserer Praxis heraus jedenfalls: Den Konflikt zwischen Datenschutz und Informationsfreiheit gibt es nicht. Wenn er auftauchte, konnte er immer gelöst werden.

Informationsfreiheit - Auch ein Gewinn für die Medien?

Dr. Manfred Redelfs

Netzwerk Recherche e. V.

Mit der Titelformulierung „Informationsfreiheit – auch ein Gewinn für die Medien?“ haben es mir die Veranstalter eigentlich leicht gemacht. Die Frage lässt sich, soviel vorweg, mit einem klaren und nachdrücklichen „Ja“ beantworten. Mit dieser knappen Antwort werden Sie sich aber sicherlich nicht zufrieden geben – Anhänger der Informationsfreiheit wollen es schließlich genauer wissen. Deshalb will ich Ihnen die Gründe nicht vorenthalten, warum sich mein Verband, die Journalistenorganisation „Netzwerk Recherche“, seit Jahren für Informationsfreiheitsgesetze stark macht, auf Bundes- wie auf Landesebene.

Dass Journalisten für eine solche Transparenzregelung streiten, mag zunächst überraschen, weil diese Berufsgruppe bereits Sonderrechte genießt: Sie können, im Gegensatz zu den Bürgern, schon seit Jahrzehnten auf einen Auskunftsanspruch gegenüber Behörden zurückgreifen. Er ist in den Landespressegesetzen geregelt und beruht auf der besonderen Funktion, die die Presse als Faktor der Meinungsbildung und auch der öffentlichen Kontrolle wahrnimmt. Ohne diesen Anspruch wären die Medien gar nicht in der Lage, ihren Informationsauftrag zu erfüllen, der für das Funktionieren eines demokratischen Rechtsstaats nötig ist. Artikel 5 des Grundgesetzes, wonach jeder das Recht hat, sich aus allgemein zugänglichen Quellen zu unterrichten, gewinnt erst dadurch an Substanz, dass die Presse die Möglichkeit hat, sich Einblick in Sachverhalte zu verschaffen, die auch das Innere der Verwaltung betreffen. So entsteht mit den Zeitungen, Zeitschriften und den elektronischen Medien überhaupt erst ein großer Teil der so genannten „allgemein zugänglichen Quellen“, von denen das Grundgesetz spricht.

Trotz dieser Sonderrechte ist das Informationsfreiheitsgesetz für Journalisten interessant, weil der Auskunftsanspruch nach den Landespressegesetzen es der Behörde überlässt, wie sie die Verpflichtung erfüllt. Als Journalist muss man sich deshalb im Regelfall mit der Auskunft der Pressestelle zufrieden geben – und die kann bestimmen, wie detailliert und in welcher Form sie auf eine Journalistenanfrage reagiert.

Die Rechtslage nach dem IFG geht an dieser Stelle weiter: Dort bleibt es grundsätzlich dem Antragsteller überlassen, die Form des Informationszugangs zu definieren, also festzulegen, ob eine schnelle mündliche Auskunft am Telefon gewünscht wird, eine schriftliche Antwort, die Zusendung von Unterlagen in kopierter oder in elektronischer Form oder etwa eine Akteneinsicht im Amt. Für recherchierende Journalisten macht gerade dieser letzte Punkt einen erheblichen qualitativen Unterschied: Es kann schließlich sehr gut sein, dass man bei der Akteneinsicht Dinge erfährt, die die Pressestelle nicht mitgeteilt hätte. Außerdem ermöglicht die Akteneinsicht eine Detailtiefe und Detailgenauigkeit, die durch mündliche Auskünfte nicht zu erreichen ist.

Ein Beispiel aus der Anwendung des Umweltinformationsgesetzes mag diesen Punkt verdeutlichen: Das UIG haben wir in Deutschland seit zehn Jahren aufgrund einer EU-Richtlinie. Es folgt im Wesentlichen dem gleichen Rechtsprinzip wie das IFG, nur eben beschränkt auf Umweltinformationen. Eine Bürgerinitiative in Seelze bei Hannover wehrte sich gegen den Bau einer Giftmüllverbrennungsanlage. Bei einer Akteneinsicht fanden die Bürger heraus, dass der Anlagebetreiber zwei Millionen Euro Förderung aus dem Landesökofonds erhalten

hatte und noch mal die gleich Summe von der Bundesstiftung Umwelt. Diese Zuschüsse waren geflossen, obwohl das angewandte Verbrennungsverfahren absolut konventionell war. Mit diesen Informationen erhoben die Kritiker Beschwerde bei der EU-Wettbewerbskommission in Brüssel. Tatsächlich wurde entschieden, dass die Gelder zurückgezahlt werden müssen, da die betreffende Müllverbrennungsanlage keine ökologische Förderungswürdigkeit besitze und die Gelder aus dem Ökofonds eigentlich für ganz andere Projekte bestimmt seien, also zweckentfremdet worden waren. Eine solche Recherche, die hier von einer Bürgerinitiative gemacht wurde, wäre natürlich auch für Journalisten interessant gewesen – und möglicherweise ein schönes Projekt, um sich für den Wächterpreis der deutschen Tagespresse zu bewerben. Ohne Akteneinsicht wäre die entscheidende Information aber niemals herausgekommen.

Ein anderes Beispiel für völlig neue Recherche-Möglichkeiten war vor drei Wochen Gegenstand eines Gerichtsverfahrens in Berlin: Dort hatte ein Journalist unter Berufung auf das Informationsfreiheitsgesetz des Landes Einsicht in den Terminkalender von Bürgermeister Wowereit begehrt – und zwar nur, soweit es sich um rein dienstliche Angelegenheiten handelte. Warum kann das wichtig sein, mögen Sie fragen? Wowereit sah sich im vorigen Jahr der Kritik ausgesetzt, zu viel Zeit auf bloße Repräsentation und aufwändige Reisen zu verwenden und zu wenig für die Sacharbeit. Im Übrigen ging es auch um einen Testfall, wie weit das Berliner IFG reicht. Der Berliner Informationsfreiheitsbeauftragte, Herr Prof. Dr. Garstka, den Sie gerade schon als engagierten Verfechter der Informationsfreiheit erlebt haben, kam zu dem Ergebnis, das dieser Rechtsanspruch auf Einsicht in die dienstlichen Termine besteht. Das Verwaltungsgericht entschied in erster Instanz dagegen, weil der Richter der Meinung war, der Terminkalender des Bürgermeisters falle nicht unter den Aktenbegriff. Diese Frage geht nun in die nächste Instanz.

In anderen Ländern ist sie nach den dortigen Informationsfreiheitsgesetzen übrigens schon entschieden. Der Berliner Antragsteller hatte sich nämlich an einer Recherche der New York Times orientiert. Die führende amerikanische Zeitung wollte herausfinden, was denn dran sei an der Kritik, der Präsidentschaftskandidat Bush pflege einen eher lockeren Arbeitsstil. Zu diesem Zweck beantragte die Zeitung unter Berufung auf den Freedom of Information Act, den es in den USA bereits seit vierzig Jahren gibt, Einsicht in den Tischkalender, der für Bush in seiner Zeit als Gouverneur in Texas geführt wurde. Das Blatt kam zu dem Schluss, dass Bush seine Arbeit im Regelfall gegen 9 Uhr morgens aufnahm, mittags zwei Stunden Pause machte, um genügend Zeit zum Joggen zu haben, und letzte Besprechungen gegen 17 Uhr ansetzte. Wie man das bewertet, ist natürlich eine zweite Sache: Es mag durchaus Wähler geben, die es gut finden, wenn ein führender Politiker sich gerade nicht als Aktenfresser betätigt, sondern sich auf die großen Leitlinien konzentriert. Entscheidend ist vielmehr, dass solche Informationen in den USA wirklich zugänglich sind und damit der journalistischen Recherche eine völlig neue Qualität verleihen.

Ich will dabei die hier anwesenden Politiker keineswegs mit Beispielen erschrecken, die wie der Terminkalender von Wowereit einen gewissen exotischen Reiz haben. Bei der Mehrzahl der Recherchen geht es – wie übrigens auch bei den Bürgeranfragen in den Ländern mit IFG – um völlig naheliegende und öffentlich höchst relevante Dinge: So wurde vor eineinhalb Jahren erregt diskutiert, wie wohl die Schadensersatzleistungen wegen der Verschiebung der LKW-Maut geregelt seien. Zunächst sollten nicht einmal die Abgeordneten des Deutschen Bundestages Einsicht in das Vertragswerk bekommen. Hier wäre ein Informationsfreiheitsgesetz sehr hilfreich gewesen, damit jeder Bürger, aber natürlich auch jeder Journalist, nachprü-

fen kann, wie gut denn die öffentliche Hand, an die er seine Steuern zahlt, in dieser Angelegenheit mit einem privaten Firmenkonsortium verhandelt hat. Schützenswerte Teile, in diesem Fall die technischen Details des Toll Collect-Systems, könnten selbstverständlich abgetrennt werden und der Öffentlichkeit entzogen bleiben – aber bei diesem konkreten Beispiel interessierte sich auch niemand von der Presse für das technische System, sondern für die Einnahmeausfälle der öffentlichen Hand in Milliardenhöhe.

Ein zweiter Punkt, warum das Informationsfreiheitsgesetz dem Journalismus nützt, hat zu tun mit dem Datenschutz. Immer wieder machen Journalisten im Umgang mit Behörden die Erfahrung, dass der Datenschutz als Begründung für eine Informationsverweigerung genannt wird. Das mag in vielen Fällen berechtigt sein. In manchen ist es aber ein vorgeschobenes Argument einer Behörde, die froh ist, einen guten und jedermann einsichtigen Grund gefunden zu haben, auf eine lästige Presseanfrage nicht antworten zu müssen. Nach dem Presserecht ist die Recherche im Regelfall zuende, wenn das Argument des Datenschutzes ins Spiel kommt. Anders beim IFG: Dort ist verpflichtend geregelt, dass die Betroffenen gefragt werden müssen, ob sie mit der Weitergabe ihrer Daten einverstanden sind oder nicht. Es sind aber ja viele Fälle denkbar, in denen die Betroffenen sehr wohl ein Interesse daran haben, dass ihrem Fall von Journalisten nachgegangen wird. Denken Sie z.B. daran, dass es vielleicht Gerüchte gibt über sich häufende Behandlungsfehler in einem städtischen Krankenhaus. Die Patientendaten genießen selbstverständlich einen hohen Schutz. Aber es ist sehr gut vorstellbar, dass die Patienten oder deren Familien, wenn man sie denn fragt, sehr gerne mit einem Journalisten zusammenarbeiten, der einem Problem nachgeht, das sie auch persönlich betrifft. Der Vorteil des IFG ist hier also die Konsultationspflicht, die die Behörden gegenüber den Betroffenen haben.

Ein dritter Grund, warum das IFG für Journalisten von Vorteil ist, liegt in den besonderen Schwierigkeiten, wenn einem Korruptionsverdacht nachgegangen werden soll. Hier kann unter Umständen eine verdeckte Recherche notwendig werden, sofern sie denn ethisch gerechtfertigt ist. Der deutsche Presserat nennt für diesen Ausnahmefall zwei Voraussetzungen: Die gesuchte Information muss von erheblicher öffentlicher Bedeutung sein und sie darf nicht auf anderem, ethisch weniger problematischem Weg genauso erfolgversprechend zu beschaffen sein. Im Umgang mit Behörden gibt es dabei allerdings das Problem, dass der Auskunftsanspruch ja nur besteht, wenn sich der Fragende als Journalist legitimiert. Fragt der „Spiegel“ an, weil er einem Anfangsverdacht nachgeht, schrillen bei der Behörde naturgemäß alle Alarmglocken. Das IFG ermöglicht es dem recherchierenden Journalisten nun, seine Anfrage als Privatperson zu stellen und damit weniger Aufsehen zu erregen. Denken Sie in diesem Zusammenhang etwa an den Korruptionsskandal um die Müllverbrennungsanlage in Köln: Schon in der Planungsphase lagen Gutachten vor, diese Anlage sei viel zu groß dimensioniert und im Endeffekt für die Kommune viel zu teuer. Doch diese Gutachten sind damals nicht öffentlich geworden, sondern erst, als der Skandal aufflog. Wären die kritischen Stimmen der Sachverständigen früher publik geworden, hätte die Stadt Köln einige Millionen Euro sparen können. Der vierte Vorteil des IFG, den ich hier hervorheben möchte, ist die Möglichkeit, Informationen auch in Form von elektronischen Daten zu erhalten. Welches Erkenntnispotenzial darin liegt, sei durch einen Blick ins Ausland illustriert: In Dänemark ist es einer Journalistenvereinigung gelungen, über eine Anfrage nach dem dortigen Informationsfreiheitsgesetz alle Daten zur Agrarförderung aus den Jahren 2002 und 2003 zu bekommen. Über eine Suchmaschine, die das Dänische Radio auf seiner Homepage eingerichtet hat, kann nun jeder online in einer Datenbank recherchieren, wie die EU-Agrarsubventionen für Dänemark in Höhe von 1,3 Milliarden Euro im Jahr verteilt werden, runtergebrochen bis auf die Namen der

Empfänger. Solche Datenaufbereitungen sind natürlich besonders interessant, wenn es um mögliche Interessenverquickungen geht, wenn also überprüft werden soll, ob politische Befürworter einer bestimmten Förderpolitik davon als Privatpersonen einen wirtschaftlichen Vorteil hätten. In Deutschland ist die Freigabe personenbezogener Daten nicht denkbar, so dass die Recherche sich also nicht eins zu eins übertragen lässt. Aber es ist zu prüfen, ob nicht große Agrargesellschaften, die als GmbH organisiert sind, sehr wohl unter den Auskunftsanspruch fallen. Eine Brüsseler Journalistin hat mit dieser Einschränkung soeben Auskunftsanträge auch in Deutschland gestellt, und ich bin gespannt, wie hier entschieden wird. Die Verknüpfung und Analyse großer Datenmengen der Verwaltung durch Journalisten ist in den USA bereits seit vielen Jahren Gegenstand des sogenannten Computer-Assisted Reporting. Damit lassen sich hochinteressante Erkenntnisse gewinnen. Die Redaktion einer Lokalzeitung in St. Louis fand beim Abgleich des Wählerverzeichnisses mit dem städtischen Sterberegister z.B. heraus, dass es massiven Wahlbetrug in der Kommune gab, denn ausgerechnet die Verstorbenen erwiesen sich dort als besonders eifrige Wähler.

Mein fünfter Punkt bezieht sich auf den großen Vorteil, den Journalisten daraus ziehen können, dass engagierte Bürger oder Verbände mit Hilfe des IFG gleichsam als Trüffelschweine der Journalisten tätig werden können – mit anderen Worten, sie graben so manches aus, was auch eine breitere Öffentlichkeit interessiert und was von Journalisten aufgegriffen werden kann. In Eckernförde in Schleswig-Holstein hat sich ein Bürger unter Berufung auf das dortige IFG nach der Privatisierung der Stadtwerke erkundigt und möchte Einsicht nehmen in das Wertgutachten, das vor dem Verkauf der Stadtwerke erstellt worden ist. Das Erkenntnisinteresse ist klar: Hat die Kommune vielleicht unter Wert verkauft – mit der Folge, dass ein Loch in den öffentlichen Kassen durch neue Abgaben ausgeglichen werden muss? Ein solches Thema ist für die gesamte Stadt interessant. Journalisten sollten sich deshalb mit den Informationen auseinandersetzen, die die Bürger mit Hilfe des IFG gewinnen.

Abschließend möchte ich als sechstes und grundsätzlichstes Argument für das Informationsfreiheitsgesetz noch auf einen übergreifenden Aspekt verweisen, der den Journalisten nutzt: Bisher ist es so, dass der Grundsatz des „Amtsgeheimnisses“ zwangsläufig die Denkweise der Verwaltung prägt. Wenn dieses Prinzip durch den Grundsatz der Öffentlichkeit abgelöst wird, dann kann man die begründete Hoffnung haben, dass es mittelfristig zu einer entsprechenden Klimaveränderung in den Behörden kommt. Die Erfahrung in anderen Ländern mit Informationsfreiheit zeigt nämlich, dass die selbstverständliche Transparenz auch dann gepflegt wird, wenn sie nicht formalrechtlich bis ins Kleinste zwingend vorgeschrieben wurde - einfach weil die Verwaltung ein Selbstbild entwickelt, bei dem sie sich verstärkt als Dialogpartner und Dienstleister der Bürger begreift. Dieses Klima der Transparenz nutzt nicht nur den Journalisten bei der Recherche und den Bürgern bei der Wahrnehumg ihrer Rechte, es kommt auch den Behörden selbst zugute, denn es erhöht letztlich die Akzeptanz von Verwaltungsentscheidungen.

Ein Informationsfreiheitsgesetz ist deshalb aus vielerlei Gründen überfällig:

Es stärkt einen aufklärerischen, informationsbetonten Journalismus.

Es fördert die demokratische Teilhabe der Bürger in einer modernen Demokratie.

Es ist ein wirksames Mittel der Korruptionsprävention

und es kann von einer cleveren Verwaltung zu einem Modernisierungsschub genutzt werden.

Schlusswort

Heike Lorenz

Bürgerbeauftragte des Landes

Mecklenburg-Vorpommern

Was hat uns zusammengeführt? Wohl die Alltagserfahrung: „Wissen ist Macht“. Und die Alltagserfahrung, die in dem Begriff „Herrschaftswissen“ „geronnen“ ist. Ein Gefühl – zum Teil diffus – sich dagegen wehren zu müssen, dass Wissen, also Macht, allein in wenigen Händen konzentriert wird – etwa in den Händen der Verwaltung. Die allermeisten im Raum stimmen sicherlich mit mir überein „Wissen teilen heißt auch Macht teilen oder zumindest kontrollierbar zu machen“.

Hier ist die Charta der Grundrechte der Europäischen Union aus dem Jahr 2000. Ich will nur zwei grundsätzliche Normen daraus nennen: Im Artikel 11 sind die Freiheit der Meinungsäußerung und die Informationsfreiheit normiert, im Artikel 20 die Gleichheit vor dem Gesetz – zwei enorm wichtige Grundwerte für Demokratie. Man fragt sich doch, warum eigentlich der eine Wert – Gleichheit vor dem Gesetz – hoch akzeptiert ist (ersichtlich an der Aufnahme in das Grundgesetz), während wir um den anderen Wert immer noch so heftig ringen, wie heute zum Beispiel auf dieser Veranstaltung. Informationsfreiheit ist eine ganz notwendige Ergänzung der Gleichheit vor dem Gesetz. Wie soll man gleich werden, wenn man nicht in gleicher Augenhöhe mit der Verwaltung agieren kann? Nur ein informierter Bürger kann wirklich seinen Staat mitgestalten, seine Rechte wahrnehmen.

Die Tatsache der geringen Inanspruchnahme der Informationsfreiheitsgesetze da, wo sie existieren, zeigt, dass die Menschen ermutigt werden müssen. Ein individueller Rechtsanspruch auf eine Auskunft wäre eine solche Ermutigung. Ich möchte eine Bemerkung zur Aussage des Innenministers machen, denn ich konnte nicht ganz nachvollziehen, dass es bei allen Fällen, die ihm vorliegen, überhaupt keine Probleme mit dem Auskunftsgebaren der Verwaltung gab. Ich bestätige, dass es in der Regel ordentlich läuft und sage dazu ganz schlicht: Das möchte wohl auch sein. Aber es gibt eben auch Fälle, wo es nicht oder schlecht funktioniert oder wo wir erst auf Grund des Nachhakens bemerken, dass die Selbstauskunft, die die Verwaltung zu ihrem Vorgang gegeben hat, nicht so ganz den Kern trifft. Gar nicht aus bösem Willen, sondern weil eben die Blickwinkel verschieden sind und die Augen verschiedene sind, mit denen ein Verwaltungsmitarbeiter oder aber der betroffene Bürger darauf schaut. Das habe ich in mehreren Fällen erlebt. Wir streiten gerade wieder um einen solchen Fall. Ich denke, dass man eben nicht aus der Erfahrung, dass in der Regel die Informationen ordentlich laufen, den Schluss ziehen kann, dass es keinen Informationsanspruch geben braucht. Eine solche Argumentation ist nicht logisch.

Im Allgemeinen gilt das Bürgerinteresse nicht allein und nicht vordergründig einer umfassenden, gesicherten Information, sondern vor allen Dingen natürlich einer Verlässlichkeit des Verwaltungshandelns als solches. Das ist die eigentliche Basis für Vertrauen, das hier schon angemahnt wurde. Auch gehe ich davon aus, dass die Belastung durch Anfragen auch in unserem Land wirklich nicht enorm sein wird. Das ist hier von allen Rednern so prognostiziert worden. Es könnte einen anderen möglicherweise zunächst als Belastung empfundenen Effekt auf die Verwaltung geben, der hoffentlich recht groß ist. Die Verwaltung wird durch so ein Gesetz gezwungen, die Sachverhalte und die Entscheidungsgründe sehr sauber zu dokumen-

tieren. Das verlangt, schon am Anfang des Prozesses genau zu überlegen, welches eigentlich die entscheidungserheblichen Fragestellungen sind, die dem Bürger oder einer anderen Institution gegenüber aufzugreifen sind. Das wird letztlich dem Bürger nützen, das wird aber auch der Verwaltung selber nützen, weil sie noch professioneller wird. Professionalität wiederum wird dazu führen, dass Verwaltung auch souveräner wird. Das sage ich, weil wir mehrfach, wenn wir Ermessen hinterfragen, erfahren: Das Nichtausüben von Ermessen scheitert eigentlich nicht so sehr am Nichtwollen, es scheitert eher daran, dass mancher nicht souverän genug ist, das zu wagen.

Souveränität wird auch eine bessere Kommunikation erzeugen. Deswegen meine ich, dass ein Informationsfreiheitsgesetz der Entwicklung einer Verwaltung, wie sie von Professor Roßnagel als Idealtyp in einer Informationsgesellschaft vorgestellt wurde, nutzen kann.

Ich sage auch ganz klar: Das Herz des Bürgers hängt nicht an der Perfektionierung von Verwaltung. Wenn die Entscheidung nachvollziehbar sachgerecht getroffen wurde, kommt es nicht auf das Komma an. Wenn klar ist, dass fair mit dem Bürger umgegangen wurde, mit ihm und mit seinen Konkurrenten, zum Beispiel im Ausschreibungsverfahren, dann kommt es ihm selten darauf an, ob da vielleicht ein formaler Fehler passiert ist. Es sind eher Anwälte, die um das Komma streiten. Dem Bürger ist es in der Regel wichtig, dass er Fairness spürt und Fairness auch nachvollziehen kann in den Dokumenten in der Verwaltung.

Es wurde hier diskutiert, dass es auch originäre Aufgabe der Verwaltung ist, die Grundrechtswahrnehmung zu fördern, und zwar mit ihren ganzen Möglichkeiten, ihrer ganzen Kraft. Das möchte ich betonen und hinzufügen, dass das für jedermann gilt – auch für benachteiligte Gruppen.

Hier wurde dargestellt, so habe ich es mir jedenfalls übersetzt, dass die informierende Verwaltung ein gutes Leitbild für die künftige Verwaltung sein könnte. Mir hat die Ergänzung des E-Governments durch das M-Government sehr gut gefallen. Sie können verstehen, dass mir das nahe liegt, weil in vielen meiner Beratungsgespräche immer wieder sehr deutlich wird: Manchmal ist gar nicht die Entscheidung selber das Problem, es ist auch nicht das Problem, dass die Unterlagen nicht ordentlich dokumentiert wären. Das Problem ist, dass die Entscheidung zum Zeitpunkt des Gespräches kein Gesicht hatte und man nicht weiß: Worauf kann man sich verlassen? Wer ist das, der dir da (vielleicht virtuell) gegenübersteht? Deswegen meine ich, eine Technik-Hörigkeit wäre falsch. Es ist angeregt worden, den Prozess der Verwaltungsreform in Mecklenburg-Vorpommern zugleich zu nutzen, um die Idee des Informationsfreiheitsgesetzes zu verbreiten, wenn auch zu befürchten ist, dass ein Gesetzgebungsverfahren in dieser Legislaturperiode nicht mehr zustande kommt. Der Entwurf der CDU-Fraktion zum Parlamentsinformationsgesetz ist möglicherweise als Vehikel nutzbar.

Ich möchte an die in der Diskussion geäußerte deutliche Warnung erinnern, bei der Fassung eines Informationsfreiheitsgesetzes keine Kompromisse im fiskalischen Bereich zuzulassen, insbesondere im Bereich Vergabewesen.

Das Informationsfreiheitsgesetz ist sicherlich eine Möglichkeit, die Verwaltung in ihrer Art und Weise, wie sie dem Bürger gegenübertritt, zu beeinflussen. Einige der Mechanismen, die ich sehe, habe ich genannt. Ich will aber auch noch einmal darauf hinweisen, dass es Dokumente der EU gibt, die lange Zeit schon vorliegen. Zu nennen ist der Kodex der Europäischen Union für gutes Verwaltungshandeln, den ich in der Broschüre meines Jahresberichtes seit

drei Jahren mit veröffentliche. Der Kodex ist im Europäischen Parlament 1999 angenommen worden. Er bindet nur die Organe der Europäischen Union, aber keiner ist daran gehindert, zu prüfen, ob das nicht als Modell für seine Verwaltung gelten kann. Es gibt Leitbilder in einer Reihe der jetzt bestehenden Verwaltungen. Mit der Strukturreform sollte man Obacht geben, die Mittel, die man bereits zur Hand hat, nicht einfach zu vergeben. Ein Mittel wäre eben, diesen Europäischen Kodex zum Vorbild zu nehmen. Ich möchte einfach vorlesen, wie im Kodex das Thema Informationsbegehren behandelt wird:

„Der Beamte stellt, sofern er für die betreffende Angelegenheit verantwortlich ist, Einzelpersonen die von ihnen angeforderten Informationen zur Verfügung. Geeignetenfalls gibt der Beamte Empfehlungen für die Einleitung eines Verwaltungsverfahrens in seinem Zuständigkeitsbereich ab. Der Beamte stellt sicher, dass die übermittelte Information klar und verständlich ist.

Ist ein mündlich vorgetragenes Informationsbegehren zu kompliziert oder zu umfassend, legt der Beamte der betreffenden Person nahe, ihren Antrag schriftlich zu stellen.

Kann ein Beamter die angeforderten Informationen wegen ihres vertraulichen Charakters nicht offen legen, teilt er der betreffenden Person gemäß § 18 dieses Kodex´ die Gründe mit, warum er die Information nicht liefern kann. Informationsbegehren zu Fragen, für die er nicht verantwortlich ist, leitet der Beamte an die zuständige Person weiter und gibt deren Namen und Telefonnummer an. Der Beamte leitet ein Informationsbegehren, das eine andere Institution oder ein anderes Organ der Gemeinschaft betrifft, an dieses Organ bzw. diese Institution weiter. Gegebenenfalls weist der Beamte, je nach Gegenstand des Begehrens, die Person, die um Information bittet, an die Stelle des Organs, die für die Information der Öffentlichkeit zuständig ist“.

Schön klar und einfach. Ich weiß, dass Gesetze nicht ganz schlicht geschrieben werden können, aber ich finde es ermutigend: Klare Worte, die deutlich eine Grundhaltung ausdrücken.

Dem Veranstalter ist sehr herzlich dafür zu danken, dass er das Thema aufgegriffen hat, ebenso dem Moderator, der sehr kundig durch die Veranstaltung geführt hat. Lassen sie uns zusammen weitermachen, damit Transparenzgesetze nicht geheime Verschlusssachen bleiben.

28 Organigramm

Stand: 01.01.2006

Landesbeauftragter für den Datenschutz
Karsten Neumann
5 94 94-36

Europäischer und internationaler Datenschutz

Vorzimmer
Ute Bache
5 94 94-35

LD 1 Verwaltung, Recht

Ina Schäfer **5 94 94-31**

Birka Paul 5 94 94-53

Stefan Lang 5 94 94-32

- Grundsatzangelegenheiten des Datenschutzes
- Justiz
- Polizei
- Verfassungsschutz
- Verkehr
- Ausländerrecht
- Informationsfreiheit
- Finanzen
- Steuern
- Telekommunikations- und Medienrecht
- Kommunal- und Einwohnerwesen
- Bau-, Wohnungs- und Liegenschaftswesen
- Statistik
- Religionsgesellschaften

LD 2 Wirtschaft und Soziales

Dr. Manfred Oberbeck **5 94 94-34**

Rolf Hellwig 5 94 94-42

Hiltraud Bockholt 5 94 94-43

- Sozialversicherungen
- Gesundheitswesen
- Personalwesen
- Schulen, Hochschulen
- Land-, Forstwirtschaft
- Eigenbetriebe
- Wasserwirtschaft
- Umweltschutz
- Aufsicht nach BDSG
- gewerbliche Dienstleistungen, freie Berufe
- Kredit- und Versicherungswirtschaft
- Handel und Versandhandel
- Auskunfteien
- SCHUFA
- Werbewirtschaft

LD 3 Technik, allg. Verwaltung

Gabriel Schulz
Stellvertreter des LfD
5 94 94-37

Technik

Andreas Waldenspuhl 5 94 94-33

René Weichelt 5 94 94-41

Gisbert Pagel 5 94 94-51

- Informations- und Kommunikationstechnik
- E-Government
- Internet
- Betriebssysteme
- Netzwerke
- Standardsoftware
- Verschlüsselung, Signatur
- Biometrie
- baulicher Datenschutz
- Sicherheitskonzepte
- Verfahrensverzeichnis
- IT der Dienststelle
- Auditverfahren

Verwaltung

Iris Dahlmann 5 94 94-45

Diana Lokatis 5 94 94-55

Birgit Serfass 5 94 94-57

Auszubildende/r zur/m Kauffrau/mann für Bürokommunikation 5 94 94-56

- Öffentlichkeitsarbeit
- Haushalt
- Personal
- Betreuung der Auszubildenden
- Schreibdienst
- Registratur
- Bibliothek
- Informationsmaterial

Besuchsanschrift
Johannes-Stelling-Straße 21
19053 Schwerin

Postanschrift
Schloss Schwerin
19053 Schwerin

Telefon: 03 85/5 94 94-0
Telefax: 03 85/5 94 94-58
E-Mail: datenschutz@mvnet.de
Internet: www.datenschutz-mv.de

1 Abkürzungen

1. BMeldDÜV	1. Bundesmeldedatenübermittlungsverordnung
A2LL	Leistungsberechnungs-Software
AK Technik	Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
ALG II	Arbeitslosengeld II
AO	Abgabenordnung
ARGEn	Arbeitsgemeinschaften
BA	Bundesagentur für Arbeit
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerlichen Gesetzbuches
BMWA	Bundesministeriums für Wirtschaft und Arbeit
BOÄ M-V	Berufsordnung für die Ärztinnen und Ärzte Mecklenburg-Vorpommern
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestags-Drucksache
BVerfGE	Entscheidung des Bundesverfassungsgerichts (Band ..., Seite ...)
CN	Corporate Network
DMP	Disease-Management-Programm
DSG M-V	Landesdatenschutzgesetz
DVZ	Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH
EG-DSRL	europäische Datenschutzrichtlinie
EU	Europäische Union
GEZ	Gebühreneinzugszentrale
GKI	Gemeinsame Kontrollinstanz
HERO	Hafen-Entwicklungsgesellschaft Rostock mbH
ICD Code	International Classification of Diseases and Related Health Problems

IFG	Informationsfreiheitsgesetz
IrDA	Infrared Data Association – Spezifikationen und Protokollstandards für den Austausch von Daten mittels infrarotem Licht
ISPS	International Ship Port Security
KoopA ADV	Koordinierungsausschuss Automatisierte Datenverarbeitung
KV M-V	Kommunalverfassung Mecklenburg-Vorpommern
LArchivG M-V	Landesarchivgesetzes Mecklenburg-Vorpommern
LBG M-V	Landesbeamtengesetz Mecklenburg-Vorpommern
LDG M-V	Landesdisziplinargesetz
LDO M-V	Landesdisziplinarordnung
LKA M-V	Landeskriminalamt Mecklenburg-Vorpommern
LKHG M-V	Landeskrankenhausgesetz Mecklenburg-Vorpommern
LMG	Landesmeldegesetz
LT-Drs.	Landtagsdrucksache
MDK	Medizinischer Dienst der Krankenversicherung
ÖGDG M-V	Gesetz über den Öffentlichen Gesundheitsdienst im Land Mecklenburg-Vorpommern
OSCI-XMeld	Online Services Computer Interface
PeM	Personalmanagement
PsychKG M-V	Psychischkrankengesetz
RFID	Radio-Frequency Identification
RGebStV	Rundfunkgebührenstaatsvertrag
SchfG	Schornsteinfegergesetzes
SDÜ	Schengener Durchführungsübereinkommen
SGB I	Sozialgesetzbuch Erstes Buch
SGB II	Sozialgesetzbuch Zweites Buch

SGB V	Sozialgesetzbuch Fünftes Buch
SGB X	Sozialgesetzbuch Zehntes Buch
SHR-U	Seehafen Rostock Umschlagsgesellschaft mbH
SIS	Schengener Informationssystem
SOG M-V	Gesetz über die öffentliche Sicherheit und Ordnung Mecklenburg-Vorpommern
StGB	Strafgesetzbuch
StUG	Stasi-Unterlagen-Gesetz
TAB	Büro für Technikfolgenabschätzung beim Deutschen Bundestag
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
UMS	Unified Messaging System
VoIP	Voice over IP
VPN	virtuelles privates Netz
VPS	Virtuellen Poststelle
WLAN	Wireless-Local Area Network
WoGG	Wohngeldgesetzes
WVHaSiG	Wasserverkehrs- und Hafenanlagensicherheitsgesetz
ZVP	Zahlungsverkehrsplattform

2 Stichwortverzeichnis

Abgabenordnung 61, 135
Abschottungsgebotes 23
Abwasser 94
Administrator 111
Adressen 119
Adresshandelsfirma 121
AK Technik 12
Akkreditierungsverfahren 48, 106
Akteneinsicht 40
Akteneinsichtsrecht 56
Amtsgeheimnis 64
anonyme Nutzung 30
Arbeitskreis 58
Arbeitskreis 12
Arbeitskreis “Technische und organisatorische Datenschutzfragen“ 10, 48
Arbeitslosengeld II 76, 78
Arbeitssuchende 78
Arzneimittelmissbrauch 87
Auditierung 19
Aufenthaltstitel 51
Aufgabenübertragung 17
Aufsichtsbehörde 7, 104
Auftragsdatenverarbeitung 61
Auskunft 71, 110
Auskunfts- und Einsichtsrecht 86
Auskunftsdienste 105
Auskunftsrecht 57
Auskunftsverweigerungsrecht 64
Ausschreibung 43
Ausweisdokument 50
bargeldloser Zahlungsverkehr 62
Beanstandung 42
behördlicher Datenschutzbeauftragter 9
berechtigtes Interesse 44, 71, 110
berichtigen 46
betrieblicher Datenschutzbeauftragter 7
Beweismittelbeseitigung 112
Biographiebogen 83
biometrisches Erkennungssystem 50
biometrisches Merkmal 50
BioP II 50
Bluetooth 12
Bonität 110
BSI 31, 50
Bundesamt für Sicherheit in der Informationstechnik 31, 50
Bundesbeauftragten für die Stasi-Unterlagen 40

Bundesdatenschutzgesetz 7, 69
Bundesmeldedatenübermittlungsverordnung 22
Bundesrat 51, 108
Bundesverfassungsgericht 77
Bürgerbegehren 39
Büro für Technikfolgenabschätzung beim Deutschen Bundestag 50
Bußgeld 112
Chipkarte 69, 77
CN 27
Common Criteria 47
Corporate Network 23, 26, 27
Data Center Steuern 61
Datenaustausch 85
Datenschutzaudit 7
Datenschutzaufsicht 106
Datenschutz-Aufsichtsbehörde 17
Datenschutzerklärung 30
Datenschutzkontrolle 61
Datenschutzkonzept 51
Datenverarbeitung im Auftrag 26, 67, 84
Datenverarbeitungsanlagen 105
Datenvermeidung 29, 62
Deutschen Fußballbund 49
Deutschland sicher im Netz 13
Dienstfähigkeit 89
Disease-Management-Programm 84
DNA-Analyse 54
Dokumentation 43
drahtloser Kommunikation 12
Dritter 118
Düsseldorfer Kreis 106
DVZ 26
EG-Datenschutzrichtlinie 106
E-Government 29, 77
E-Government-Masterplan 30, 62
Einkommensermittlung 76
Einwilligungserklärung 48
Einzelhandelsverband 117
Einzugsermächtigung 119
elektronische Melderegisterauskunft 62
E-Mail 58
Entgeltbescheinigungen 76
Entschließung 51
E-Payment 62
ERFA-Kreis 7, 106
Erhebungsbeauftragte 24
Ermittlungsverfahrens 57
Ersterhebungsgrundsatz 35

E-Shop ... 62
EU-Datenschutzrichtlinie ... 17
Europäische Datenschutzkonferenz ... 10
Europäischen Kommission ... 106
Falscherkennung ... 50
Fehlerprotokoll ... 46
Fernmeldegeheimnis ... 28
Finanzamt ... 64
Finanzministerium ... 61, 64
Fingerabdruck ... 51
Firewall ... 26, 58
Flugpassagierdaten ... 10
Forschung ... 73, 90
Fortbildung ... 106
Fragebogen ... 24
Freigabe ... 33
Gästebefragung ... 114
Gebühreneinzugszentrale ... 15
Geheimschutzbeauftragter ... 25
Gemeindevertretung ... 39
Gemeinsame Geschäftsordnung II ... 8
Gerichtsvollzieher ... 57
Geschäftsgeheimnis ... 120
Gesellschaft für Datenschutz und Datensicherheit e. V. ... 7, 106
Gesichtserkennungssystem ... 50
Gesundheitsmodernisierungsgesetzes ... 93
Gewinnmitteilungen ... 120
Grundgesetz ... 136
Handelsauskunftei ... 105
Hausbesuche ... 36
Haushalts-Kassen-Rechnungs-Verfahren ... 62
Hochbaustatistik ... 81
ICD Code ... 93
Identifikationsverfahren ... 50
Impressum ... 29
Informationsfreiheit ... 11
Informationsfreiheitsbeauftragter ... 11
Informationspflicht ... 29
Informationsregister ... 22
Informationszugang ... 18
Innenministerium ... 17, 26
Interessenkonflikt ... 24
Internet ... 17, 58
Internetanschluss ... 58
Internetportal ... 29
Internet-Telefonie ... 27
IrDA ... 12
IT-Initiative ... 20

IT-Sicherheit ... 48
IT-Sicherheitsrahmenkonzept ... 27
JobCard-Verfahren ... 12, 76
Justizministeriums ... 64
Koalitionsvertrag ... 51
kommunaler Träger ... 80
Kommunalverfassung ... 39
Kommunalverwaltung ... 19
Konferenz der Datenschutzbeauftragten des Bundes und der Länder ... 28, 51
Konkursverwalter ... 113
Kontenabfragen ... 37
Kontrollzuständigkeit ... 89
Krankenakte ... 86
Krankenhauses ... 82
Krankenhausinformationssystem ... 82
Krankentransport ... 93
Krankenversichertennummer ... 92
Krebsregister ... 85
Kredit-Scoring ... 118
Kreditwesengesetzes ... 135
Kundenbefragung ... 67
Kundenbindungsprogramme ... 119
Kurverwaltung ... 69
Landesamt für innere Verwaltung ... 23
Landesbeauftragte für den Datenschutz ... 17
Landesdatenschutzgesetzes ... 17
Landeskriminalamt ... 49
löschen ... 121
Löschung ... 43, 110
Luftsicherheitsgesetz ... 49
Mammographie-Screening ... 88
Medizinischen Dienst der Krankenversicherung ... 89
Meldebehörde ... 44
Melderegister ... 40
Melderegisterauskunft ... 21, 44
Mikrozensus ... 24
mithören ... 34
Modellprojekt ... 29
Nahverkehr ... 46
Neugeborenenscreening ... 82
nicht-öffentliche Stellen ... 104, 122
nicht-öffentlicher Bereich ... 17, 104
Notar ... 64
Oberfinanzdirektion ... 61
Online-Banking ... 58
Orientierungshilfe ... 58
Pass- und Personalausweisgesetz ... 51
Passkontrolle ... 51

Personalabteilung 51
Personalausweis 51
Personaldaten 25, 63
Personaldokument 113
Personalmanagement 63
Personalunterlagen 41
Persönlichkeitsrechte 91
Pflegeheim 83
Preisausschreiben 119
Presse 57
Privatwirtschaft 7, 19
Produktaudit 20
Profiling 110
ProFiskal 62
Protection Profile 47
Protokollierung 26, 30, 34, 69
pseudonymisierte Daten 90
qualifizierte Signatur 77
Rating 118
Rechenzentrum für die Steuerverwaltung 61
Rechtsverordnung 20
Reihengentests 54
Reisepass 50
Revisionsarbeitsgruppe 26
RFID 12
Richtervorbehalts 54
Richtlinie 93
Rückweisungsrate 50
Rundfunkgebührenpflicht 15
Rundfunkgebührenstaatsvertrag 15
Schengener Informationssystem 42
Schornsteinfegergesetz 68
Schrankensteuerung 69
SCHUFA 106
Schulaufsicht 73
Schutzprofil 13, 47
schutzwürdiges Interesse 71, 110
Schweigepflicht 91
Score 118
Scoring 62, 106
Sicherheitskonzept 27
Sicherheitsüberprüfung 61
Signatur 22
Signaturgesetz 77
Signaturgesetzes 22
Signaturkarte 77
Sozialgeheimnis 78
Sozialleistungen 77

Sozialleistungsmissbrauch 35, 36
Sozialleistungsträger 35, 36
Speicherchip 50
Sperrung 110
Staatsanwaltschaft 57
Stasi-Unterlagen-Gesetz (StUG) 40
Statistikgeheimnisses 23
Statistische Landesamt 74
Statistisches Amt 23
Stellenplan 38
Steuergeheimnis 61
Steuerverwaltung 61
Stoffwechselerkrankungen 82
Strafantrag 105
Strafanzeige 112
Strafprozessordnung 56
TAB 50
TDDSG 29
TDG 29
Technikfolgenabschätzung 50
technischen und organisatorischen Maßnahmen 112
Teledienstedatenschutzgesetz 29
Teledienstegesetz 29
Telefongespräch 34
Terrorismusbekämpfung 10
Tonaufzeichnung 39
Transparenz 30, 135
Überwachung 55
Überwindungssicherheit 51
Umweltinformationsgesetz 94
Unabhängigkeit 17
Unified Messaging System 28
Unschuldsvermutung 55
Unternehmen 19
Untersuchungshaft 55
Verdunkelungsgefahr 56
Verfahrensverzeichnis 82
Verfassungsschutzbehörde 25, 52
Vermögen 76
Verordnung 19
Versandhandel 110
Verschlüsselung 28
Verschluss-Sachenanweisung 25
Verschwiegenheit 40
Verschwiegenheitspflicht 64
Vertragsverhältnis 69
Vertragsverletzungsverfahren 106
Vertrauensstelle 78

Vertrauenswürdigkeit 47
Verwaltungsreform 33
Verzeichnisdienst 28
Videoanlage 13
Videokamera 105
Videoüberwachung 32
Viren 58
Virtuelle Poststelle 30
Virtuelles Datenschutzbüro 11
virtuelles privates Netz 28
Visa 51
Voice over IP 27
Volkseigener Betrieb 113
Vorabkontrolle 108
Vorgangsbearbeitung 52
Vorratsspeicherung 58
VPN 28
VPS 30
Wählerverzeichnis 46
Weiterübermittlung 110
Werbepost 119
Werbung 119
Widerspruch 120
Wirtschaft 20
WLAN 12
Wohngeld 76
Workshop 20
Zahlungsverkehrsplattform 62
Zertifikat 48
Zertifizierung 48, 51
Zusammenarbeit 17
Zuverlässigkeit 49, 105
Zwangsgeld 105
Zweckbindung 33

3 Publikationen

Beim Landesbeauftragten für den Datenschutz sind derzeit folgende Publikationen kostenlos erhältlich bzw. stehen im Internetangebot unter [www.lfd.m-v.de] zum Abruf bereit:

Broschüren

- ☐ 1. Tätigkeitsbericht für den Zeitraum 1992/93
- ☐ 2. Tätigkeitsbericht für den Zeitraum 1994/95
- ☐ 3. Tätigkeitsbericht für den Zeitraum 1996/97
- ☐ 4. Tätigkeitsbericht für den Zeitraum 1998/99
- ☐ 5. Tätigkeitsbericht für den Zeitraum 2000/01
- ☐ 6. Tätigkeitsbericht für den Zeitraum 2002/03

- ☐ Landesdatenschutzgesetz 2002 mit Erläuterungen
- ☐ Gesetze und Verordnungen zum Datenschutz (Loseblattsammlung)

- ☐ Datenschutzgerechtes E-Government (Handlungsempfehlungen und datenschutzfreundliche Lösungen für die Verwaltung)
- ☐ Vom Bürgerbüro zum Internet – Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung
- ☐ Datenschutz im Krankenhaus
- ☐ Datenschutzfreundliche Technologien
- ☐ Technik und Datenschutz (Arbeitsergebnisse und Tagungsunterlagen des Arbeitskreises Technik)

- ☐ BfD - INFO 1 - Bundesdatenschutzgesetz (Text und Erläuterungen)
- ☐ BfD - INFO 2 - Der Bürger und seine Daten
- ☐ BfD - INFO 3 - Schutz der Sozialdaten
- ☐ BfD - INFO 4 - Die Datenschutzbeauftragten in Behörde und Betrieb
- ☐ BfD - INFO 5 - Datenschutz in der Telekommunikation

Infoblätter

- ☐ Meine Daten - Mein Recht
- ☐ Meine Daten - Mein Recht ... auch in der Schule
- ☐ Meine Daten - Mein Recht ... als Kunde und Verbraucher
- ☐ Meine Daten - Mein Recht .. auch bei Arbeitslosengeld II
- ☐ Datenschutz und Telefax
- ☐ Datenschutz und Statistik
- ☐ Ihre Datenschutzrechte im Meldewesen

Orientierungshilfen

- ☐ Empfehlungen zur Passwortgestaltung und zum Sicherheitsmanagement
- ☐ Transparente Software – eine Voraussetzung für datenschutzfreundliche Technologien
- ☐ Forderung an Wartung und Fernwartung von DV-Anlagen
- ☐ Data Warehouse und Data Mining im öffentlichen Bereich (Datenschutzrechtliche und -technische Aspekte)

- ☐ Datenschutz bei Windows XP Professional
- ☐ TCPA, Palladium und DRM

- ☐ Datensicherheit bei USB-Geräten
- ☐ Datenschutzfragen zum Anschluss von Netzen der öffentlichen Verwaltung an das Internet
- ☐ Datenschutzrechtliche Aspekte beim Einsatz von Verzeichnisdiensten
- ☐ Datenschutzgerechte Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz
- ☐ Datenschutzfragen zur Präsentation von öffentlichen Stellen im Internet
- ☐ Datenschutz und Internet in der Schule

- ☐ Datenschutzgerechte Vernichtung von Schriftgut mit personenbezogenen Daten
- ☐ Anforderungen zur informationstechnischen Sicherheit bei Chipkarten
- ☐ Datenschutzrechtliche Aspekte beim Einsatz optischer Datenspeicherung
- ☐ Datenschutz und Telefax
- ☐ Datenschutz in kommunalen Vertretungsorganen
- ☐ Datenschutz und Telemedizin - Anforderungen an Medizinnetze -
- ☐ Datenschutz bei Telearbeit
- ☐ Datenschutz in drahtlosen Netzen

Muster

- ☐ Mustervertrag zur Verarbeitung personenbezogener Daten im Auftrag
- ☐ Mustervertrag zur datenschutzgerechten Vernichtung von Schriftgut mit personenbezogenen Daten
- ☐ Musterdienstvereinbarung über die Nutzung der Telekommunikationsanlage
- ☐ Musterdienstvereinbarung zur Nutzung von Internetdiensten
- ☐ Muster einer Verpflichtungserklärung zum Datengeheimnis gemäß § 6 DSG M-V
- ☐ Muster einer Bestellung zur oder zum behördlichen Datenschutzbeauftragten

Formulare

- ☐ Verfahrensbeschreibung nach § 18 DSG M-V; Hinweise zur Führung der Verfahrensbeschreibung
- ☐ Widerspruch gegen die Weitergabe der Meldedaten gemäß §§ 32, 35 Landesmeldegesetz

Weitere Informationen unter:

www.bfd.bund.de
www.lfd.m-v.de
www.datenschutz.de (Virtuelles Datenschutzbüro)