Landtag Brandenburg **Drucksache 2/2601**
2. Wahlperiode

Vierter Tätigkeitsbericht

des Landesbeauftragten für den Datenschutz

Berichtszeitraum: vom 1. April 1995 bis 31. März 1996

Inhaltsverzeichnis Seite

Datum des Eingangs: 08.05.1996 / Ausgegeben: 09.05.1996

1 Rechtliche und technische Entwicklungen

1.1 Einleitung

Die Bemühungen um einheitliche europäische Mindeststandards im Datenschutzrecht sind erfolgreich zum Abschluß gebracht worden; am 24. Oktober 1995 ist die EU-Datenschutzrichtlinie in Kraft getreten. Dies dürfte unstrittig als das im Berichtszeitraum entscheidende Ereignis mit noch nicht konkret absehbaren Folgen für die Ausgestaltung des Rechts auf informationelle Selbstbestimmung anzusehen sein. Sowohl die Konferenz der Datenschutzbeauftragten des Bundes und der Länder als auch der Düsseldorfer Kreis sind seitdem intensiv damit befaßt, die Fragen ihrer Umsetzung in nationales Recht - insbesondere den Änderungsbedarf beim Bundesdatenschutzgesetz - zu klären.

Im Berichtszeitraum hat meine Dienststelle die Datenverarbeitung bei verschiedenen Behörden (z. B. Polizei, Verfassungsschutz, Gemeinsames Krebsregister der neuen Bundesländer, Erhebungsstellen der Gebäude- und Wohnungsstellen) kontrolliert. Für die Auswahl dieser Stellen entscheidend waren wiederum zum einen die Fortsetzung von Prüfungen aus dem Vorjahr, zum anderen bevorstehende landesweite Erhebungen und nicht zuletzt Hinweise durch Eingaben von Bürgern.

Was die Gestaltung des Tätigkeitsberichts anbelangt, haben mich die Reaktionen auf die vergangenen Berichte bestärkt, mit der Abfassung - abgesehen von zwei Ausnahmen - wie bisher zu verfahren, d. h., am Anfang werden zunächst ausgewählte rechtliche und technische Schwerpunktthemen dargestellt, danach wird die Zusammenarbeit mit den Ministerien nach dem Ressortprinzip abgehandelt und am Ende wird auf Personal- sowie kommunale Angelegenheiten nunmehr in eigenständigen Kapiteln eingegangen.

Die Ausführungen zu den neuen Technologien unter 1.5 sind letztendlich auch Ausdruck für mein geändertes Rollenverständnis als Datenschutzbeauftragter. Eine Dienststelle wie die meine hat keine Zukunft, wenn sie sich lediglich als Kontrollinstanz versteht. Es reicht angesichts der neuen technischen Entwicklungen nicht mehr aus, im nachhinein als "Polizist der Datenautobahnen" aufzutreten. Ich stimme mit meinen Kollegen des Bundes und der anderen Bundesländer darin überein, daß nur dann, wenn wir uns als Akteure im gesellschaftlich-politischen Raum bewegen und uns beispielsweise als Instanzen eines medienpolitischen und rechtlichen "Frühwarnsystems" betätigen, als Ansprechpartner für kompetente Technikberatung fungieren, bei der Technikfolgenabschätzung mitwirken und u. U. als Gesprächspartner für Hersteller, Netzbetreiber und Diensteanbieter zur Verfügung stehen, in der Lage sein werden, eine effiziente Sicherstellung des Rechts auf informationelle Selbstbestimmung in einer in absehbarer Zeit weltweit agierenden Informationsgesellschaft zu gewährleisten.

Meinen Kollegen vom Bund und den Kollegen in den anderen Bundesländern habe ich wiederum für die zweckdienliche Zusammenarbeit zu danken. Sowohl die Entwicklungen im technischen als auch im gesetzgeberischen Bereich erfordern eine Spezialisierung hinsichtlich der zu lösenden Probleme, die nur noch arbeitsteilig unter den Datenschutzbeauftragten bewältigt werden können. Ergebnisse dieser intensiven Zusammenarbeit im Berichtszeitraum sind insbesondere die Beschlüsse zweier Konferenzen zu grundlegenden Fragen des Datenschutzes (s. Anlagen 3 - 12). Darüber hinaus haben die schon regional bedingten, engen Kontakte zum Berliner Datenschutzbeauftragten eine Fortsetzung beispielsweise durch eine gemeinsame Prüfung des Krebsregisters der neuen Bundesländer erfahren. Hervorheben möchte ich auch die gute Zusammenarbeit mit der für den nicht-öffentlichen Bereich zuständigen Aufsichtsbehörde für den Datenschutz beim Ministerium des Innern. Schließlich ist meinerseits an dieser Stelle ausdrücklich meinen Mitarbeitern für ihr beharrliches Engagement zu danken, mit denen sie sich für die Belange des Datenschutzes und damit für die Persönlichkeitsrechte der Bürgerinnen und Bürger des Landes Brandenburg erfolgreich eingesetzt haben.

Für den Jahresbericht wurde als Stichtag der 31. März 1996 gewählt.

1.2 Schaffung einzelgesetzlicher Regelungen im Land Brandenburg

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

Die nachfolgende Auflistung von Gesetzen sowie Verordnungen und Verwaltungsvorschriften entspricht der Gliederung des Tätigkeitsberichts nach dem Ressortprinzip. Eine Gewichtung erfolgt ausschließlich jeweils in dem in der Klammer angegebenen Einzelkapitel.

Gesetze:

- Erstes Gesetz zur Änderung des Brandenburgischen Datenschutzgesetzes (Bbg DSG) vom 8. Februar 1996, GVBl. II S. 17 (s. unter 2.1)

- Gesetz zur Änderung des Brandenburgischen Kommunalwahlgesetzes zur Umsetzung der Richtlinie 94/80/EG des Rates vom 19. Dezember 1994 über die Einzelheiten der Ausübung des aktiven und passiven Wahlrechts bei Kommunalwahlen für Unionsbürger mit Wohnsitz in einem Mitgliedsstaat, dessen Staatsangehörigkeit sie nicht besitzen, und zur Änderung des Landesbeamtengesetzes vom 14. Dezember 1995, GVBl. I S. 274

- Gesetz über die Aufgaben und Befugnisse der Polizei im Land Brandenburg (Brandenburgisches Polizeigesetz - BbgPolG) vom 19. März 1996, GVBl. I S. 74 (s. unter 3.2.1.1)

- Gesetz über das Versorgungswerk der Rechtsanwälte im Land Brandenburg (Brandenburgisches Rechtsanwaltsversorgungsgesetz - BbgRAVG) vom 4. Dezember 1995, GVBl. I S. 266 (s. 3. Tätigkeitsbericht unter 4.1.1)

- Gesetz über die Schulen im Land Brandenburg (Brandenburgisches Schulgesetz - BbgSchulG) vom 12. April 1996, GVBl. I S. 102 (s. unter 5.1)

- Gesetz über Hilfe und Schutzmaßnahmen sowie über den Vollzug gerichtlich angeordneter Unterbringung für psychisch Kranke (Brandenburgisches Psychisch-Kranken-Gesetz - PsychKG) vom 25. Januar 1996 (s. unter 7.3.1.1)

- Zweites Gesetz zur Änderung des Brandenburgischen Hochschulgesetzes (s. unter 7.4.1)

Verordnungen und Verwaltungsvorschriften:

- Verordnung zur Änderung der Brandenburgischen Kommunalwahlverordnung vom 18. Dezember 1995, GVBl. II S. 738

- Verordnung über das Verfahren bei Volksentscheiden im Land Brandenburg (Volksentscheidsverfahrensverordnung - VEVVBbg) vom 29. Februar 1996, GVBl. II S. 158

- Ausbildungs- und Prüfungsordnung mittlerer Justizdienst (APOmJD) vom 4. Dezember 1995, GVBl. II S. 6

- Verwaltungsvorschriften über wissenschaftliche Untersuchungen an Schulen (VV-WissU) vom 1. August 1995, ABl. MBJS S. 408 (s. 2. Tätigkeitsbericht unter 5.1.4)

- Verordnung über Prüfungen für Nichtschüler im Land Brandenburg (Nichtschülerprüfungsordnung - PO-NSch) vom 25. September 1995, ABl. MBJS 1995 S. 483 (s. 3. Tätigkeitsbericht unter 5.1.3)

- Verwaltungsvorschriften über die Durchführung von Hausunterricht - (VV-Hausunterricht - VVHauunt) vom 28. Juni 1995, ABl. MBJS 1995 S. 338 (s. 3. Tätigkeitsbericht unter 5.1.4)

- Verwaltungsvorschriften über die Durchführung von Schülerpraktika (VV-Schülerpraktika) vom 4. September 1995, ABl. MBJS S. 502 (s. 3. Tätigkeitsbericht unter 5.1.7)

- Erste Verwaltungsvorschrift zur Änderung der Verwaltungsvorschriften über den Schutz personenbezogener Daten in Schulen und über statistische Erhebungen (VV-Datenschutz/Statistik) vom 3. Dezember 1995, ABl. S. 1285 (s. unter 5.2)

- Erste Verordnung zur Änderung der Feststellungsprüfung vom 15. November 1995, GVBl. II S. 710 (s. unter 5.3)

- Berufsordnung für Hebammen und Entbindungspfleger im Land Brandenburg (HebBOBbg) vom 8. November 1995, BVBl. II S. 702 (s. unter 7.2.2.2)

- Verordnung zum Schutz von Patientendaten im Krankenhaus (Krankenhausdatenschutzverordnung - KHDsV) vom 4. Januar 1996, GVBl. II S. 54 (s. unter 7.3.1.2)

- Verordnung über die bevorzugte Berücksichtigung von Unternehmen bei der Vergabe öffentlicher Aufträge zur Förderung von Frauen im Erwerbsleben (Frauenförderungsverordnung - FrauFöV) (s. unter 7.4.1)

- Verordnung zur Überwachung und Kontrolle des Wildhandels (Wildhandelsüberwachungsverordnung - WildÜV) vom 25. März 1996, GVBl. II S. 250 (s. unter 8.5)

- Allgemeine Verwaltungsvorschrift zur Durchführung der §§ 14, 15 und 15c Gewerbeordnung (GewAnzVwV) vom 25. Januar 1996, ABl. S. 186 (s. unter 11.1)

- Verwaltungsvorschrift zum Wohnungsbindungsgesetz (VV-WoBindG) vom 15. Mai 1995, ABl. S. 486

- Grundsätze der Landesregierung für die Überprüfung von Dienstkräften des Landes Brandenburg hinsichtlich einer Tätigkeit für das ehemalige Ministerium für Staatssicherheit/Amt für Nationale Sicherheit (MfS/AfNS) vom 10. Oktober 1995, ABl. S. 914 (s. unter 13.2.3)

Ergänzend zu dieser Auflistung ist darauf hinzuweisen, daß trotz der im Berichtszeitraum verabschiedeten, aus der Sicht des Datenschutzes wichtigen Gesetze wie Polizei-, Schul- und Psychisch-Kranken-Gesetz im Land Brandenburg nach wie vor noch gesetzliche Regelungen fehlen, denen eine grundsätzliche Bedeutung zukommt. Dies trifft beispielsweise für das noch ausstehende Brandenburgische Statistikgesetz und für das Gesetz über das den Bürgern gem. Art. 21 Abs. 4 Brandenburgische Verfassung (BbgVerf)[1] garantierte Akteneinsichtsrecht zu.

An die Landesregierung ist deshalb zu appellieren, daß sie - unabhängig von dem Ausgang der Volksabstimmung am 5. Mai 1996 - diesen unbefriedigenden Zustand abhilft, indem sie dem Parlament so schnell als möglich Entwürfe hierzu zur Verabschiedung vorlegt.

---

[1] vom 20. August 1992, GVBl. I S. 298, geänd. durch Art. 2 d. NVG v. 27. Juni 1995, GVBl. I. 150

1.3 Internationaler Datenschutz

1.3.1 EU-Richtlinie in Kraft getreten - Umsetzung in nationales Recht angesagt

Es hat gut vier Jahre gedauert, bis die "Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr"[2] endlich am 24. Oktober 1995 in Kraft getreten ist. In diesen Jahren sind die Vorgaben für das Datenschutzrecht der nahen Zukunft so ausgestaltet worden, daß nicht nur in einigen EU-Ländern ein von Anfang an modernes Datenschutzrecht entsteht, sondern auch altbewährtes Datenschutzrecht neue Impulse erhält. In bezug auf das deutsche Recht ist letzteres zu erwarten.

Den entscheidenen Durchbruch zur Veränderung des Datenschutzrechts in Deutschland hat die Beratung des Entwurfs im Februar 1995 im Europäischen Parlament gebracht. Infolge dieser parlamentarischen Behandlung ist die ursprünglich vorgedachte Zweiteilung in einen öffentlichen und einen privaten Teil entfallen.

Nachfolgend sollen nur ausgewählte Aspekte Erwähnung finden:

- keine Unterscheidung zwischen Datenverarbeitung im öffentlichen und nicht-öffentlichen Bereich

In der Richtlinie wird bei der Aufzählung derer, die für die Verarbeitung der personenbezogenen Daten "verantwortlich" sind, kein Unterschied zwischen "natürlicher und juristischer Person, Behörde, Einrichtung oder jede(r) andere(n) Stelle gemacht, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung ... entscheidet" (Art. 2 Buchst. d). Dies wird freilich nicht dazu führen, daß in Deutschland die Unterscheidung zwischen öffentlichen und nicht-öffentlichen Stellen beim Datenschutz und die Vorgabe unterschiedlicher Regelungen hierzu künftig entfallen wird. Es wird jedoch sicherlich dazu führen, daß diese Unterschiede bei jedem weiteren Gesetzgebungsschritt verkleinert oder ein geringeres Gewicht erhalten werden als bisher.

Dies entspricht aber nicht nur den Vorgaben der EU-Richtlinie, es ist eher umgekehrt. Die EU-Richtlinie spiegelt deutlicher als das geltende Datenschutzrecht in Deutschland den inzwischen erreichten Stand der Datentechnik einerseits und der Tendenz der Verwischung der Grenzen zwischen öffentlichem Recht und Privatrecht andererseits wider. So wird, wenn das Umsetzen der EU-Richtlinie in nationales Recht richtig genutzt wird, dem tatsächlichen oder angeblichen Erfordernis, den Staat "schlanker" zu machen und deshalb mehr und mehr Aufgaben auf Private zu verlagern, Bereiche auszugliedern und notwendige ursprünglich staatliche Handlungen durch Private ausführen zu lassen, in Bezug auf den Datenschutz direkt und ohne Fiktionen nachgekommen, und es wird ein Datenschutzrecht geschaffen werden können, das öffentliche und private Stellen nach der gleichen datenschutzrechtlichen Elle mißt.

Dem liegt der Gedanke zu Grunde, daß das Persönlichkeitsrecht der durch Datenverarbeitung betroffenen Person nicht deshalb ein anderes Schutzniveau erfordert, weil der Staat durch öffentliche Stellen handelt oder statt dessen dieses Handeln auf eine durch den Staat privat organisierte Stelle überträgt, oder ob er eine private Stelle eine Vorleistung erbringen läßt, die dann von Staat abgenommen wird.

Anders gesagt: wenn der Staat sich aus mehr und mehr Bereichen zurückzieht oder wenn er aus wirtschaftlichen Gründen keine andere Möglichkeit sieht als sich zurückzuziehen, dann ist es für die betroffenen Bürger nicht hinnehmbar, daß aus diesem Grund als eine Folge, die in Kauf genommen wird, das Datenschutzniveau sinkt, allein schon deshalb, weil der Anteil staatlichen

---

2 ABl. EG 1995 Nr. L 281/50, S. 31

Handelns mit direkter Wirkung auf den Bürger kontinuierlich zurückgeht, oder weil bei unterschiedlichem Schutzniveau immer eine Tendenz besteht, das jeweils einfachere und den Bürger weniger schützende Verfahren zu bevorzugen. Das Persönlichkeitsrecht muß vielleicht sogar, richtig verstanden, im privaten Bereich - durchgehend - stärker geschützt werden als im öffentlichen Bereich.

Ein künftiges gesetzgeberisches Vorgehen derart, daß zwischen privatem und öffentlichem Bereich keinen Unterschied mehr zu machen sein wird, d. h., daß durch die Richtlinie die Möglichkeit eröffnet wird, diesen Unterschied zu verringern oder sogar aufzuheben, ist für das deutsche Datenschutzrecht der eigentliche Schritt in die Zukunft.

- Schutz der Privatsphäre

Die EU-Richtlinie gibt deutliche Standpunkte und Gewichtungen vor. Ganz vornan steht der Schutz der Grundrechte und Grundfreiheiten, in diese ist der Schutz der Privatsphäre mit dem Datenschutz eingebettet (Art. 1). Dem deutschen Datenschutzrecht haftet dagegen noch die Tendenz des Ringens um Freiräume an. Dies ist sehr deutlich erkennbar, wenn immer wieder auf das "Volkszählungsurteil" vom 15. Dezember 1983[3] hingewiesen wird und hingewiesen werden muß; denn erst durch ein Urteil des Bundesverfassungsgerichts konnte das Persönlichkeitsrecht im Zusammenhang mit der Verarbeitung personenbezogener Daten aus der Nichtbeachtung herausgelöst werden.

- Umgang mit sensiblen Daten

Ein weiteres Beispiel bietet die Behandlung des Umgangs mit besonders sensiblen Daten. Dazu gehören solche, die die rassische oder ethnische Herkunft, die politische Meinung oder das Sexualverhalten betreffen. Eine derartige Kennzeichnung und herausgehobene Beachtung von sensiblen Daten ist in dem deutschen Datenschutzrecht die Ausnahme, durch die Vorgaben der Richtlinie wird dies zur Regel gemacht. In der Richtlinie steht das Verbot der Verarbeitung solcher Daten im Vordergrund (Art. 8 Abs. 1), erst an zweiter Stelle werden die Ausnahmen genannt, die von diesem Verbot zugelassen werden können.

- Rechte der Betroffenen

Auch die Rechte der betroffenen Person werden im Vergleich zum geltenden deutschen Recht deutlicher hervorgehoben. Die Informationen, die schon bei der Erhebung der Daten gegeben werden müssen, sind als Mindestvorgaben ausgestaltet. Dies wird in der Richtlinie als eine Ausprägung der Grundaussage des Gedankens gekennzeichnet, daß die Erhebung und Verarbeitung personenbezogener Daten immer unter dem Gesichtspunkt von Treu und Glauben gesehen werden muß (Art. 10 und 11). Sofern der betroffenen Person diese Informationen nicht sofort bei der Erhebung oder zumindest bei der Speicherung der Daten gegeben werden können, oder wenn z. B. die Speicherung oder Weitergabe von personenbezogenen Daten durch Gesetz ausdrücklich geregelt ist, hat der Staat "geeignete Garantien" vorzusehen (Art. 11 Abs. 2). Konsequenterweise steht der betroffenen Person ein "garantiertes" Auskunftsrecht (Art. 12) und darüber hinaus ein Widerspruchsrecht (Art. 14) gegen die Verarbeitung ihrer personenbezogenen Daten zu, das ausdrücklich auch dann greift, wenn die betreffenden Daten rechtmäßig erhoben und übermittelt worden waren.

- Kontrollbefugnisse

Der ständigen Kontrolle der Einhaltung der Schutzvorschriften wird größeres Gewicht gegeben; sie kann - dies ist gegenüber dem geltenden deutschen Recht eine geänderte Sicht - je nach Wahl der datenverarbeitenden Stelle künftig durch zwei unterschiedliche Maßnahmen vorgenommen

---

3 BVerfGE 65, 1

werden. Der Verantwortliche für die Datenverarbeitung hat der zur Überwachung des Datenschutzes zuständigen Kontrollstelle (Art. 28) zu melden, daß und welche automatisierte Datenverarbeitung vorgesehen ist. Die Kontrollstelle stellt die gemeldeten Angaben in ein Register ein (Art. 21). Die zweite Möglichkeit besteht darin, einen (internen) Datenschutzbeauftragten zu bestellen (Art. 18), der die Einhaltung der Vorschriften zum Datenschutz überwacht.

- Völlige Unabhängigkeit der Kontrollstelle

Auch die Stellung und die Befugnisse der übergeordneten Kontrollstellen nach Art. 28 werden der europäischen Sicht des Datenschutzes gerecht, die von der Person und ihren Grundfreiheiten ausgeht, denn der diesbezügliche Text der Richtlinie (Art. 28 Abs. 1 Satz 2) lautet: "Diese Stellen nehmen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahr". Hier wird ein Gedanke deutlich, der in dem geltenden deutschen Recht noch keine durchgehende Ausprägung gefunden hat. Die rechtliche Einbindung des Landesbeauftragten für den Datenschutz z. B. in eine Ministerialverwaltung, wie dies in einigen der alten Bundesländer der Fall ist, kann, nimmt man das Europarecht ernst, nicht mehr gerechtfertigt werden. Außerdem legt diese Textstelle in Verbindung mit der Gesamtintention der Datenschutzrichtlinie nahe, daß diese "völlig unabhängigen Kontrollstellen" gleichermaßen für den öffentlichen wie für den nicht-öffentlichen Bereich des Datenschutzes zuständig sein müßten.

Im Zuge der Umsetzung der Datenschutzrichtlinie werden darüber hinaus die Kompetenzen der Kontrollstellen zu erweitern sein. Die unabhängige Stelle hat "Untersuchungsbefugnisse" zu erhalten, die wohl die jetzt schon bestehenden Informationsrechte übersteigen dürften. Zusätzlich hat sie "wirksame Einwirkungsbefugnisse" und ein "Klagerecht oder eine Anzeigebefugnis" bei Verstößen gegen die Datenschutzvorschriften (Art. 28 Abs. 3). Auch hier zeigt sich die Tendenz, dem Datenschutz mehr Gewicht zu verleihen. Die Auswirkungen dieser europarechtlichen Vorgaben werden sich vor allem im nicht-öffentlichen Bereich zeigen, denn von anlaßbezogener Kontrolle, wie sie jetzt noch im Bundesdatenschutzgesetz verankert ist, ist nicht die Rede, und Verstöße gegen den Datenschutz werden jedenfalls im privaten Bereich künftig nicht mehr nur von der verletzten Person, sondern auch durch die Kontrollstellen auf den Weg der Strafverfolgung gebracht werden können.

- Technikfolgenabschätzung

Bei einem so, wie hier dargestellt, umfassender und konsequenter als bisher ausgestalteten Datenschutzrecht werden die Gesetzgeber im Bund und in den Ländern nicht daran vorbeigehen können, die neueren und auch kommenden technischen Entwicklungen im Bereich von Information, Kommunikation und Dokumentation zu bedenken und die Auswirkungen der sich ständig weiterentwickelnden Datenverarbeitungstechniken in ihren Auswirkungen auf die Freiheiten und Selbstbestimmungsrechte der Menschen, soweit diese Auswirkungen negativ sind, in Schranken zu halten. Der Datenschutz wird, das ist durch die Datenschutzrichtlinie deutlicher geworden als bisher, an Gewicht gewinnen.

1.3.2 Entschließung des Bundesrates "Forderung der Länder zur Regierungskonferenz 1996"

Die Datenschutzbeauftragten der Mitgliedsländer der Europäischen Union (EU) haben sich 1995 auf ihrer Konferenz in Kopenhagen intensiv mit der anstehenden Revision des Unionsvertrages (Maastricht II) befaßt und dazu die von der deutschen Delegation vorgelegte Erklärung verabschiedet (s. Anlage 2). Sie enthält im wesentlichen drei Forderungen an die Regierungskonferenz 1996:

- Aufnahme eines Grundrechts auf Datenschutz in den vorgesehenen Grundrechtskatalog

- Schaffung eines verbindlichen Datenschutzrechts für die EU-Organe

- Einrichtung einer unabhängigen Datenschutzkontrollinstanz für die EU-Institutionen.

Vor dem Hintergrund der anstehenden Beratung der Entschließung "Forderung der Länder zur Regierungskonferenz 1996 (BR-Drs. 608/95)" im Bundesrat habe ich sowohl den hiesigen Innen- als auch den Justizminister gebeten, diese Gedanken in die Ausschußsitzungen einzubringen, ggf. vorliegende Anträge anderer Bundesländer zu unterstützen.

Bedauerlicherweise enthält die Ende des vergangenen Jahres gefaßte Entschließung des Bundesrates (BR-Drs. 667/95) diesbezüglich keine Präzisierungen. Unter II.1 ist unverändert und unverbindlich die Rede davon, daß "langfristig" "bei der entsprechenden Weiterentwicklung der europäischen Integration ein Grundrechtskatalog im Gemeinschaftsrecht verankert werden sollte".

1.4 Technisch-organisatorische Maßnahmen bei der Einhaltung des Datenschutzes

1.4.1 Sicherheitsempfehlungen des Bundesamtes für Sicherheit in der Informationstechnik

Eine moderne Verwaltung erfordert den Einsatz automatisierter Verfahren, wodurch Verwaltungsaufgaben effektiver gestaltet werden können und die Bürgerfreundlichkeit der Verwaltung erhöht werden kann. Daraus resultiert aber auch, daß Sicherheitsaspekte des Einsatzes von IuK-Technik, wie Vertraulichkeit, Verfügbarkeit, Integrität und Verbindlichkeit der zu verarbeitenden personenbezogenen Daten, berücksichtigt werden müssen.

Vor Einführung automatisierter Verfahren, in denen personenbezogene Daten verarbeitet werden, ist es aus der Sicht des Datenschutzes unbedingt erforderlich, ein Sicherheitskonzept zu erstellen. Dagegen stellt es eine falsche Herangehensweise dar, wenn zunächst automatisierte Verfahren eingeführt werden und erst anhand eines nachträglich konzipierten Sicherheitskonzeptes festgestellt wird, daß die erforderlichen technisch-organisatorischen Maßnahmen gem. § 10 Bbg DSG aus Kosten-, Personal- oder anderen Gründen nicht realisierbar sind. Ausgangspunkt der Betrachtungen sollte die Einordnung der personenbezogenen Daten entsprechend eines Schutzstufenkonzeptes[4] sein, in dem die Daten in Abhängigkeit ihrer Sensibilität einer bestimmten Schutzstufe zugeordnet werden. In Abhängigkeit der ermittelten Schutzstufe sind dann entsprechende technisch-organisatorische Maßnahmen vorzusehen und zu realisieren. Stellt sich jedoch heraus, daß die erforderlichen Maßnahmen aus Kosten-, Personal- oder anderen Gründen nicht realisiert werden können, sollte auf die Einführung des jeweiligen Verfahrens überhaupt verzichtet werden.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt ein IT-Sicherheitshandbuch zur Verfügung, in dem die Methodik der Erstellung eines Sicherheitskonzeptes dargestellt wird (s. Anlage 13). Werden personenbezogene Daten der Schutzstufe C verarbeitet, ist der relativ hohe Aufwand der Erstellung eines Sicherheitskonzeptes nach dem IT-Sicherheitshandbuch des BSI vertretbar und erforderlich. Eine weitere Möglichkeit ist die Nutzung des IT-Grundschutzhandbuches des BSI, in dem konkrete Gefährdungen und Maßnahmen zur Realisierung eines mittleren Schutzbedarfs aufgeführt sind. Dieser mittlere Schutzbedarf entspricht in etwa den Stufen A und B des Schutzstufenkonzeptes[5] und kann sinnvollerweise zur Erstellung eines Sicherheitskonzeptes mit

---

[4] s. Broschüre: "Sicherheit am PC und in lokalen Netzen - Dateienregister", 1. Aufl. September 1993 aus der Informationsreihe "Der Landesbeauftragte für den Datenschutz Brandenburg informiert"

[5] s. Fußnote 4

herangezogen werden. Folgende Themen werden im aktuellen IT-Grundschutzhandbuch[6] behandelt:

- Organisation
- Personal
- Notfallvorsorge-Konzept
- Datensicherungskonzept
- Gebäude
- Verkabelung
- Büroraum
- Serverraum
- Datenträgerarchiv
- Raum für technische Infrastruktur
- DOS-PC
- Unix-System
- Tragbarer PC
- Servergestütztes PC-Netz
- Vernetzte Unix-Systeme
- Datenträgeraustausch
- Modem
- Telekommunikationsanlage
- FAX
- Anrufbeantworter
- Firewall
- Software-Abnahme/-Freigabe
- Windows for Workgroups

Die einmalige Erstellung eines IT-Sicherheitskonzeptes reicht bei weitem nicht aus. IT-Sicherheitskonzepte müssen in regelmäßigen Abständen dem Stand der Technik und den jeweiligen Sicherheitsbedürfnissen angepaßt werden.

Aufgrund der Komplexität heutiger IT-Systeme können nicht alle Schwachstellen des jeweiligen Systems erkannt und beseitigt werden. Das Computer Emergency Response Team (CERT) des Deutschen Forschungsnetzes beschäftigt sich mit aktuellen Problemen der Rechner- und Netzwerksicherheit (http://www.cert.dfn.de). Zur Erhöhung der Sicherheit sollten auch solche aktuellen Informationen für die Arbeit in den öffentlichen Stellen genutzt werden.

1.4.2 Datenschutzgerechter Zugang der Verwaltungen zum Internet

In der heutigen Informationsgesellschaft spielt der schnelle und zuverlässige Austausch von Informationen eine immer größere Rolle. Stand vor einigen Jahren der Aufbau von lokalen Anwendungsnetzen (LAN) in der Wirtschaft und den Verwaltungen im Vordergrund, geht heutzutage die Tendenz in Richtung einer Integration dieser lokalen Netze in Weitverkehrsnetze, ohne daß dabei die damit verbundenen Gefahren einer eingehenden Erörterung unterzogen werden. Im Zuge der Liberalisierung des Telekommunikationsmarktes werden im zunehmenden Maße auch andere private Netzanbieter und Netzbetreiber Telekommunikationsleistungen anbieten. Bewährte

[6] Das IT-Sicherheits- und IT-Grundschutzhandbuch kann vom Bundesanzeiger-Verlag, Postfach 10 05 34, 50455 Köln bezogen werden.

Hilfsmittel, wie z. B. die des Schutzstufenkonzeptes[7], sind auf solche neu entstandenen Weitverkehrsnetze nicht ohne weiteres übertragbar. Schon bei der Konzeption und Einführung neuer Projekte sollte daher darauf geachtet werden, daß personenbezogene Daten, die über Weitverkehrsnetze übertragen werden sollen, in jedem Fall mit Hilfe sicherer Verfahren (z.B. DES, IDEA, RSA) verschlüsselt werden. Sollten bereits derartige Verschlüsselungsverfahren im Einsatz sein, sind diese von Zeit zu Zeit dem Stand der Technik anzupassen.

Eines der bekanntesten und beliebtesten Weitverkehrsnetze stellt das Internet dar. Derzeit sind ca. 40 Millionen Nutzer aus 140 Ländern im Internet registriert. Über sogenannte Internet-Provider (Diensteanbieter) kann ein Anschluß an dieses Netz erfolgen. Das Internet besteht aus einer Vielzahl von Rechnern, auf denen die unterschiedlichsten Dienste angeboten werden. Der Internet-Nutzer kann auf all diese Dienste weltweit und relativ schnell zugreifen; dies stellt die erste Stufe einer künftigen globalen Informationsstruktur dar.

Einer der beliebtesten Dienste ist das World Wide Web (WWW). Mit Hilfe eines Browsers (Anzeigeprogrammms) können Bildschirmseiten weltweit von einem WWW-Server geladen und angezeigt werden. Problematisch sind hierbei aus datenschutzrechtlicher Sicht die Protokolle, die auf den WWW-Servern geführt werden, mit deren Hilfe Nutzerprofile erstellt werden können. Komfortable Auswertungsprogramme stehen hierfür im Internet kostenlos zur Verfügung. Nach deutschem Recht (vgl. hierzu § 4 Abs. 1 Bbg DSG) dürfen personenbezogene Daten aber nur erhoben werden, wenn ein Gesetz dies vorsieht oder wenn der Betroffene eingewilligt hat. Da es sich beim Internet um eine weltweite Angelegenheit handelt, kann die Bundesrepublik allein hierfür und ebenfalls für die noch anzusprechenden Probleme keine Rechtsgrundlage schaffen; dies kann nur über internationale Verträge erreicht werden.

Neuere WWW-Browser ermöglichen die Verwendung sogenannter Plug-Ins (Zusatzmodule). Mit diesen Zusatzmodulen kann die Funktionalität des jeweiligen Browsers erweitert werden. In diesem Zusammenhang ist die neue Internet-Programmiersprache „Java“ zu nennen. Beim Laden einer WWW-Seite werden sogenannte Applets (kleine Programme) zum lokalen Rechner übertragen und dort auch ausgeführt. Hierzu ist kritisch anzumerken, daß diese kleinen Programme nicht nur Grafiken und Animationen auf dem Bildschirm darstellen können, sondern auch Daten des lokalen Systems u. U. relativ unbemerkt an einen anderen Rechner im Internet übertragen werden könnten. Diese Art der Datenausspähung muß unter allen Umständen verhindert werden, indem z. B. die Funktionalitäten solcher Zusatzprogramme genauestens untersucht werden. Besteht keine Möglichkeit, sicherheitskritische Funktionen zu deaktivieren, muß auf den Einsatz solcher Zusatzmodule verzichtet werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat mit ihrer Entschließung zum Internet (s. Anlage 9) zumindest Orientierungshilfen zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltungen an das Internet erarbeitet, in der datenschutzrelevante Risiken und Forderungen beschrieben werden. Wesentliche Elemente dieser Orientierungshilfe lassen sich auch auf andere Weitverkehrsnetze übertragen.

1.4.3 Veränderte Regelungen zur Entsorgung von Datenträgern

Die Anfang letzten Jahres neugefaßte DIN 32757[8] definiert die Vernichtung von Informationsträgern als "Vorgang, bei dem Form oder Zustand von Informationsträgern in

---

7 s. Fußnote 4

8 DIN, Deutsches Institut für Normung e. V., Ref. Nr. DIN 32757-1: 1995-01

der Regel durch Verkleinern oder Stoffumwandlung verändert wird". Als Arten von Informationsträgern werden Papier, Filmmaterial aus Polyester für Normaldarstellung und für Mikrofilm, Metall (z. B. Druckformen), Kunststoff (z. B. Identifikationskarten) und Chipkarten berücksichtigt.

Nicht berücksichtigt wird hier die Vernichtung von magnetischen Datenträgern. Falls aus Sicherheitsgründen personenbezogene Daten auf flexiblen Datenträgern (Magnetbänder, Magnetbandkassetten, Disketten, Identifikationskarten mit Magnetstreifen u. ä.) vor ihrer Entsorgung sicher gelöscht werden sollen, ist die DIN 33 858 zu beachten. Sie regelt Mindestanforderungen an Löschgeräte und entsprechende Prüfverfahren. Diese Norm gilt allerdings nicht für das Löschen von Fest- und Wechselplatten. Die Daten solcher Medien sollten vor ihrer Vernichtung mittels Zerkleinerung oder Stoffumwandlung durch starke Magneten gelöscht werden; ein solches Entmagnetisierungsverfahren ist bisher allerdings noch nicht genormt.

Die Vernichtung der Daten erfolgt entsprechend ihrer Sensibilität nach 5 Sicherheitsstufen (S 1 bis S 5). Sehr sensible Daten (wie Gesundheits-, Strafverfolgungs-, Steuer-, Sozial- und psychologische Daten sowie Daten zu religiösen oder politischen Anschauungen, Arbeitsrechtsverhältnissen, Unterbringungen in Anstalten, Adoptionen, Betreuungen, Wahlausschlüssen und Paßversagungsgründen) sollten bei der Datenträgervernichtung wenigstens nach der Sicherheitsstufe S 4 für geheimzuhaltendes Schriftgut gem. DIN 32757 behandelt werden.

Dabei ist zu bedenken, daß die Entsorgung der Datenträger und die damit verbundene Löschung der Daten in der Stufe S 4 tatsächlich nur einen praktischen Kompromiß darstellt, der einer Anonymisierung gem. § 3 Abs. 3 Bbg DSG entspricht, da die Reproduktion des Vernichtungsguts unter Verwendung gewerbeunüblicher Einrichtungen bzw. Sonderkonstruktionen immerhin noch möglich ist, wenn auch nur mit hohem Aufwand. Zwar sieht die Legaldefinition für Löschen (vgl. § 3 Abs. 2 Nr. 6 Bbg DSG) das Unkenntlichmachen gespeicherter Daten als Löschen vor, jedoch kann dies mit der Schutzstufe S 4 nicht ganz erreicht werden.

Hinzu kommt, daß die Neufassung der DIN 32757 nunmehr sogar einen gewissen Toleranzbereich für das Vernichtungsgut zuläßt. Danach dürfen bei der Sicherheitsstufe S 4 10 % der Einzelstichprobe nach der Entsorgung eine Teilchenfläche bis zu 90 mm^2 haben, während für 90 % des Abfallguts nur 30 mm^2 (2 mm x 15 mm Partikelgröße) zulässig sind. Mir ist bekannt geworden, daß speziell vor diesem Hintergrund z. B. Versicherungsträger und Bankinstitute dazu übergehen, für ihre Unterlagen eine Entsorgungsstufe vorzusehen, die über der Sicherheitsstufe S 4 liegt.

Generell läßt die DIN 32757 die Möglichkeit zu, daß bei großen Durchsatzmengen und durch eine spezielle Nachbehandlung des Entsorgungsguts (z. B. Verwirbelung, Verpressung und Vermischung mit anderem Entsorgungsgut) eine höhere Sicherheitsstufe erreicht werden kann. Allerdings sollten die Ergebnisse solcher zusätzlichen Maßnahmen durch Kontrollbesuche des Auftraggebers überprüft werden. Obwohl dies in der DIN 32757 nicht ausdrücklich erwähnt wird, ist daran zu denken, daß auch Zwischenstufen - entweder durch die primäre Art der maschinellen Vernichtung oder durch die geschilderten zusätzlichen Maßnahmen - erreicht werden können.

Generell haben Entsorgungsfirmen das anzuerkennende Interesse, das Vernichtungsgut zu recyceln. Bei Papierdatenträgern (z. B. Akten, Drucklisten, Karteikarten) wäre dies nach der Entsorgung mit der Sicherheitsstufe S 4 (und höher) für die übliche Papierherstellung für Druckerzeugnisse jedoch nicht mehr möglich. Allerdings dürfte der Anfall solch sensiblen Papierguts im Verhältnis zum sonstigen Altpapieraufkommen gering sein. Wenn es sich dann auch nicht mehr lohnen sollte, dieses spezielle Vernichtungsgut für hochwertige Zwecke zu verwenden, so besteht immer noch die Möglichkeit der ökologisch sinnvollen

Endverwertung als Hygienepapier.

1.5 Neue Technologien

1.5.1 Pilotprojekte zum interaktiven Fernsehen

Bereits in meinem 3. Tätigkeitsbericht[9] berichtete ich über die neu entstehenden Mediendienste. Im Berichtszeitraum startete die Telekom Multimedia-Pilotprojekte in mehreren deutschen Großstädten. Obwohl Brandenburger Bürger davon nicht betroffen sind, erscheint es mir bedeutungsvoll, diese Versuche aus der Sicht des Datenschutzes zu beobachten, da die aus ihnen gewonnenen Erkenntnisse in die vorgesehene flächendeckende Einführung der interaktiven Videodienste einfließen sollen.

Voraussetzung für eine Teilnahme an den Pilotprojekten sind ein Kabelanschluß, ein digitaler Decoder (Set-Top-Box) und ein Fernsehgerät. Folgende Dienste stehen den Teilnehmern am Pilotprojekt u. a. zur Verfügung:

- Beim "Pay-per-Channel" erfolgt die Verteilung eines ganzen verschlüsselten Fernsehprogramms, für das auch vollständig bezahlt werden muß.

- Beim "Pay-per-View" erfolgt die Verteilung von Fernsehprogrammen mit der Möglichkeit, nur einzelne Programmteile zu nutzen und auch nur dafür zu bezahlen.

- Beim "Near Video on Demand" werden Filme verteilt, die zeitversetzt in mehreren Kopien parallel gesendet werden. Auf Wunsch kann der Kunde wählen, welche Filme er innerhalb des vorgeschriebenen Zeitrasters entgeltpflichtig abrufen möchte.

- Beim "Video on Demand" werden individuell abrufbare Filme, die mit typischen Videorecorderfunktionen wie Anhalten und Vor- oder Rücklauf gesteuert werden können, angeboten.

- Bei den "Video-Games" wird individuell abrufbare Software für Videospiele, die in einen angeschlossenen Computer eingespielt wird, kostenpflichtig angeboten. In einer späteren Phase soll ein individuelles Spielen mit anderen Teilnehmern möglich sein.

- Beim "Service on Demand" werden im Auftrag von Versandhäusern, Reiseveranstaltern, Banken, Verlagen usw. individuell abrufbare Produktinformationen in der Regel kostenfrei angeboten. So kann beispielsweise in einem elektronischen Katalog mit "Bewegt-Bildern", Texten und Audio-Unterstützung geblättert und per Fernbedienung bestellt werden.

Während das alte klassische Fernsehen einen typischen "Verteilerdienst" darstellt, d. h., die Sendungen werden zeitgleich an eine unbestimmte Anzahl von nicht bekannten Empfängern ausgestrahlt, benötigen die meisten interaktiven Video-Dienste einen Rück-Kanal vom Teilnehmer zum Programmanbieter.

Die datenschutzrechtliche Problematik besteht darin, daß für den einzelnen Anschluß dabei vielfältige Verbindungs- und Abrechnungsdaten über die Nutzung, insbesondere über den Zugriff auf bestimmte Informationen, entstehen und ausgewertet werden müssen. So läßt sich beispielsweise erkennen, wer sich welche Filme oder politischen Magazine ansieht und wer in welcher Form und mit welchem Bedarf Kontakte zu Versandhäusern, Reiseveranstaltern, Banken usw. aufgenommen hat. Diese Datenspuren können ohne Wissen

---

[9] s. unter 1.4

der Betroffenen zu aussagefähigen Benutzungsprofilen verdichtet werden. Auf diese Weise können äußerst sensible Datensammlungen entstehen, die zur Verhaltens- und Umfeldkontrolle der Fernsehteilnehmer sowie zur Ausforschung ihrer persönlichen Lebensgewohnheiten bestens geeignet sind.

Derartige Datensammlungen sind deshalb aus der Sicht des Datenschutzes nicht hinnehmbar. Sie können jedoch relativ einfach durch die Wahl geeigneter anonymer Abrechnungsverfahren weitestgehend vermieden werden. Um so erstaunlicher ist es, daß nach meiner Kenntnis bisher in den Multimedia-Pilotprojekten der Telekom keinerlei dafür in Frage kommende Abrechnungsverfahren in die Erprobung einbezogen werden. Es wäre aus meiner Sicht sehr zu begrüßen gewesen, wenn dabei von Anfang an solche Abrechnungsverfahren erprobt würden, bei denen keine oder möglichst wenige Daten über das Informations-, Fernseh- und Kommunikationsverhalten der Betroffenen entstehen. Vor allem für die Entgeltabrechnung können anonyme Bezahlungsverfahren (sog. Prepaid-Verfahren)[10] eingesetzt werden, bei denen die Gebühren für die in Anspruch genommenen Leistungen direkt von einer wiederaufladbaren Chipkarte des Benutzers abgebucht werden. Ein derartiges Verfahren würde weitgehend ohne zentrale Speicherung von personenbezogenen Verbindungs- und Abrechnungsdaten auskommen.

Lediglich wenn der Teilnehmer schriftlich einen Einzelnachweis über seine in Anspruch genommenen Dienste für Abrechnungszwecke beantragt, ist eine Speicherung der dafür erforderlichen Daten wie der Zeitpunkt, die Dauer, der Inhalt und die Art des Dienstes zu vertreten. Wie beim Einzelverbindungsnachweis der Telefonabrechnung ist dem betreffenden Antragsteller jedoch anzuraten, vorher genau abzuwägen, ob eine detaillierte Abrechnung das mit der Datenspeicherung verbundene Risiko rechtfertigt. Denn wo immer Daten entstehen, entwickeln sich wegen der darin enthaltenen Informationen Begehrlichkeiten nach ihnen. Daran könnten insbesondere Angehörige, Arbeitgeber, Polizei und Staatsanwaltschaft sowie persönliche und politische Gegner interessiert sein.

1.5.2 Starker Zuwachs bei Online-Diensten

In den letzten Jahren hat ein neues Massenmedium den Weg zu den privaten und gewerblichen Nutzern gefunden. Wurden früher primär Telefon, Radio und Fernsehen zum Austausch von Informationen und zur Informationsgewinnung genutzt, ist derzeit ein regelrechter Boom bei den sogenannten Online-Diensten festzustellen. Diese Dienste bieten eine Fülle von Einzeldiensten an, mit denen Informationen weltweit gesammelt und ausgetauscht werden können. Die Innovationszeiten in diesem Bereich werden stetig kürzer; ständig werden neue Dienste zur Verfügung gestellt.

Die Voraussetzung zur Nutzung solcher Online-Dienste ist in der Regel das Vorhandensein eines Computers, eines Modems, eines Telekommunikationsanschlusses (Analog- oder ISDN-Anschluß) und einer Zugangsberechtigung zu einem Diensteanbieter. Mit Hilfe spezieller Software können jetzt u. a. Texte, Grafiken, Musikdateien und Videos auf den heimischen Computer übertragen und weiterverarbeitet werden. Neuere Techniken gestatten auch die Dienste-Nutzung unter Verwendung von sogenannten Fernseh-Modems.

Die größten kommerziellen Anbieter von Online-Diensten sind in Deutschland derzeit Telekom-Online, America Online, Compuserve und Microsoft Network. Die Informationsangebote sind bei allen Online-Anbietern ähnlich; aber der Stand des Ausbaus der einzelnen Dienste recht unterschiedlich. Über folgende Themen kann man sich beispielsweise mit Hilfe dieser Dienste informieren: Datenbanken, Archive, Bibliotheken, Börsenkurse, Gesetzestexte, Urteile der Rechtsprechung, Reiseveranstaltungstips, Produktpräsentationen, Angebote von Versandhäusern, aktuelle Zeitschriften,

---

[10] s. 2. Tätigkeitsbericht unter 1.4.3.1

wissenschaftliche Forschungsergebnisse, Lehrangebote u. a. Weitere beliebte Dienste sind u. a. der elektronische Nachrichtenaustausch (E-Mail) und Online-Diskussionsforen.

Bei der Nutzung von Online-Diensten werden aber auch personenbezogene Daten erhoben und verarbeitet. Die daraus resultierenden Risiken des Mißbrauchs müssen auf ein Minimum reduziert werden. Schon bei der erstmaligen Anmeldung zu einigen Online-Diensten wird die Angabe der Kreditkartennummer verlangt, die dann mehr oder weniger unzureichend verschlüsselt über das Netz übertragen wird. Die mißbräuchliche Verwendung der Kartennummer kann hierbei nicht ausgeschlossen werden. Alternative Zahlungsformen sind aus Sicherheitsgründen unbedingt erforderlich.

Ein weiteres Problem bei einigen Diensteanbietern ist, daß die personenbezogenen Daten im Ausland verarbeitet werden. Hier findet zwangsläufig das deutsche Datenschutzrecht keine Anwendung, es sei denn, der Diensteanbieter macht dies beim Vertragsabschluß über die Datenverarbeitung im Auftrag zum Vertragsgegenstand, wie dies vergleichsweise bei der Nutzung der Bahn-Card erreicht werden konnte.

Auch bei den Online-Diensten können die umfänglich gespeicherten personenbezogenen Daten (z. B. wer hat wann welche Informationsangebote genutzt) zur Erstellung von Benutzerprofilen verwendet werden. Entsprechende Marktforschungsunternehmen haben schon reges Interesse an der Nutzung dieser Daten bekundet. Eine mißbräuchliche Nutzung der bei den Online-Diensten entstandenen Daten durch Dritte muß unter allen Umständen verhindert werden.

Weiterhin ist zu fordern, daß nur solche Daten gespeichert werden, die zu Abrechnungszwecken unbedingt erforderlich sind. Auch sollte die Einführung von anonymen Nutzungsverfahren forciert werden, was sich auch gut als Marketingargument für den jeweiligen Online-Anbieter verwenden lassen dürfte.

1.5.3 Geographische Informationssysteme

Geographische Informationssysteme (GIS) zeichnen sich durch die Möglichkeit aus, Sachinformationen aus Politik, Wirtschaft und Verwaltung und ihre logisch-inhaltlichen und räumlichen Zusammenhänge vor dem Hintergrund beeindruckender Computerlandkarten und Geländeanimationen räumlich darzustellen und daraus neue Informationen zu gewinnen. Während vor einigen Jahren anspruchsvolle Anwendungen Großrechnern vorbehalten blieben, geht der Trend heute mit steigender Leistungsfähigkeit der Rechentechnik zunehmend zu Systemen auf PC-Plattformen unter Windows und mit Austauschmöglichkeiten zu Datenbanksystemen, Textverarbeitung und Tabellenkalkulation. So werden beispielsweise im kommunalen Bereich GIS-Anwendungen u. a. für Straßen-, Leitungs-, Meßstellen-, kommunale Beleuchtungs-, Wohnungs-, Biotop- und Altlastenkataster genutzt.

Lag in früheren Projekten der Aufwand von Anwendungen geographischer Informationssysteme überwiegend in der Beschaffung, Pflege und Archivierung der geographischen Daten, so ist gegenwärtig ein starker Trend zur Vereinheitlichung und zentralen Bereitstellung dieser Informationen durch staatliche Dienststellen erkennbar. Die Landesregierung Brandenburg hat speziell hierfür das Vorhaben "Digitale Karte"[11] beschlossen, wonach für alle raumbezogenen Informations- und Entscheidungssysteme des Landes die Karten der folgenden drei Projekte in Form von geometrischen Basisdaten zugrunde zu legen sind:

---

[11] Grundlagenfunktion der topographischen Landeskarten und der Liegenschaftskarten für den Aufbau von raumbezogenen Informationssystemen (Vorhaben "Digitale Karte") vom 29. August 1994, ABl. S. 1365

- Amtliches topographisch-kartographisches Informationssystem (ATKIS),
- Rasterdaten topographischer Karten (RTK) und
- Automatisierte Liegenschaftskarte (ALK).

Der Grundgedanke des Vorhabens "Digitale Karte" besteht darin, daß die graphischen Karteninhalte unter Nutzung einheitlicher Datenbankschnittstellen und einheitlicher Formate in datenverarbeitungsfähiger Form erarbeitet, gespeichert und unmittelbar an Nutzer in der Landesverwaltung, den regionalen Planungsgemeinschaften sowie den Landkreisen und kreisfreien Städten zum Teil kostenlos abgegeben werden. Unter Berücksichtigung der o. a. Gründe prognostiziert eine Studie der Universität Münster, daß sich der Umfang geographischer Anwendungen bis zum Jahre 2000 mehr als verdoppeln wird.

So verfügen nach meiner Kenntnis bundesweit schon mehrere Landesvermessungsämter über automatisierte Liegenschaftskarten, für Großstädte sogar im Maßstab zwischen 1 : 500 und 1 : 2000 und geben diese an interessierte Nutzer - auch aus dem nicht-öffentlichen Bereich - weiter. In diesen großmaßstäblichen Kartendarstellungen können bereits personenbezogene Daten u. a. von Grundstückseigentümern, -nutzern, Anlagenbetreibern in zusätzlichen Dateien hinterlegt sein. Hierfür liegen in der Regel die gesetzlichen Befugnisnormen noch vor. Da es jedoch - wie oben dargestellt - technisch heute möglich ist, mehrere Informationsebenen beliebig zu überschichten, wird in Zukunft genau zu beobachten sein, mit welchen weiteren personenbezogenen Informationen dieses Kartenmaterial durch Nutzer (Dritte) ergänzt wird und inwieweit dabei Datenschutzbestimmungen eingehalten werden. Dabei können besondere Gefahren für das Recht auf informationelle Selbstbestimmung durch die Konzentration personenbezogener Daten auftreten, indem Daten von geographischen Informationssystemen mit anderen Anwendungen zusammengeführt werden.

Gegenwärtig bin ich dabei, mir einen Überblick zum aktuellen Stand des Einsatzes geographischer Informationssysteme in Brandenburg zu verschaffen.

1.5.4 Chipkarten im Zahlungsverkehr

Die Einführung von elektronischem Geld steht unmittelbar bevor. Ab nächstem Jahr werden ec-Karten ausgegeben, die mit einem multifunktionalen Chip ausgestattet sind und mit dem vor allem die bargeldlose Bezahlung im Kleingeldbereich ermöglicht werden soll. Der Kunde lädt seine Geldbörse mit einem limitierten Betrag auf und kann dann bei bestimmten Handels- und Dienstleistungsunternehmen mit diesem elektronischen Geld bezahlen. Dies unterscheidet sie ganz wesentlich von den schon seit langer Zeit im Einsatz befindlichen geschlossenen Systemen wie z. B. die vorbezahlte Telefonkarte. Im Gegensatz zu den elektronischen Geldbörsen sind diese nämlich nicht wieder aufladbar und ermöglichen eine völlig anonyme Bezahlung.

Bedenklich sind aus datenschutzrechtlicher Sicht Bestrebungen der am System beteiligten Stellen, aus Sicherheitsgründen für jede elektronische Geldbörse sogenannte Schattenkonten zu führen, in denen alle Einzeltransaktionen der Kartenbenutzer gespeichert werden sollen. Aus diesen Datensammlungen könnten ohne weiteres umfängliche Konsum- und Bewegungsprofile der Kartenbenutzer vor allem deswegen erstellt werden, weil die Anzahl der Transaktionen aufgrund der gegenüber von Kreditkarten kleineren Zahlungseinheiten wesentlich größer sind. Dies würde zwangsläufig zur weiteren Einschränkung der Persönlichkeitsrechte des einzelnen führen, nämlich sich frei und unbeobachtet in der Gesellschaft zu bewegen. Sei es beim Bezahlen am Zigarettenautomaten oder im öffentlichen Nahverkehr, im Erotikshop oder beim Schnellimbiß, der Kartenbenutzer würde überall seine Spuren hinterlassen.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher in einer Entschließung zum Datenschutz bei elektronischen Geldbörsen und anderen kartengestützten

Zahlungssystemen gefordert (s. Anlage 8), daß nur kartengestützte Systeme zum Einsatz kommen, die möglichst ohne personenbezogene Daten auskommen. Der Gesetzgeber ist hier gefordert, gesetzliche Regelungen zu schaffen, so daß auch in Zukunft - analog zum Bargeld - anonyme Zahlungsverfahren weiterhin bestehen bleiben.

1.5.5 Elektronische Telefonverzeichnisse "D-Info" auf CD-ROM

Seit Juni 1995 vertreibt die Firma TopWare eine Telefonbuch-CD-ROM mit dem Namen "D-Info", die auf einem einzigen Datenträger den Informationsbestand aus allen Telefonbüchern der Bundesrepublik Deutschland in elektronischer Form enthält. In kurzer Zeit wurden ca. 800.000 Exemplare verkauft und damit rangiert "D-Info" an der Spitze der bundesweiten CD-ROM-Bestsellerliste. Seinen Erfolg hatte der Datenträger neben seinem niedrigen Preis vor allem seinen vielseitigen Nutzungsmöglichkeiten, die weit über ein normales Telefonbuch in Papierform hinausgehen, zu verdanken.

Obwohl zwischenzeitlich von der zuständigen Aufsichtsbehörde für den Datenschutz die Herausgabe der Telefonbuch-CD-ROM als datenschutzrechtlich unzulässig eingestuft und ein Bußgeldverfahren gegen den Herausgeber eingeleitet wurde, konnte der Verkauf im Einzelhandel nicht mehr gestoppt werden. Die datenschutzrechtliche Unzulässigkeit ergibt sich vor allem daraus, daß einem Telefonkunden, der gem. § 10 Abs. 3 TELEKOM-Datenschutzverordnung (TDSV)[12] mit der Veröffentlichung seiner Teilnehmerdaten in einem Telefonbuch einverstanden ist, nicht unterstellt werden kann, er hätte damit auch der Veröffentlichung seiner Daten in elektronischer Form zugestimmt. Denn für das Persönlichkeitsrecht eines Betroffenen ist es ein großer Unterschied, ob seine Daten nur in einem gedruckten Telefonbuch oder auf einem elektronischen Datenträger, der am Computer in beliebiger Form ausgewertet werden kann, der Öffentlichkeit zugänglich gemacht werden. Darum muß der Telefonkunde die Möglichkeit erhalten, differenziert zu entscheiden, ob seine Teilnehmerdaten nur im gedruckten Telefonbuch oder auch im elektronischen Telefonbuch erscheinen sollen (vgl. hierzu auch unter 3.1.1.6).

Die Forderung nach einer solchermaßen differenzierten Zustimmungsregelung ergibt sich aus den vielfältigen Nutzungsmöglichkeiten des elektronischen Telefonbuches, die weit über das übliche Telefonbuch in Papierform hinausgehen und damit den Telefonteilnehmer beispielsweise in folgender Weise beeinträchtigen können:

- Die Recherche nach der Rufnummer (sog. Invertsuche) ermöglicht es, durch Eingabe der Rufnummer nach dem Namen und der Adresse von Teilnehmern zu suchen und diese zu identifizieren. Ein Telefonteilnehmer kann also nicht mehr davon ausgehen, daß er etwa bei der Aufgabe von Annoncen mit der Angabe seiner Telefonnummer anonym bleibt.

- Ein Arbeitgeber kann beispielsweise anhand der Einzelgebührenabrechnungen oder anderen Ausdrucken von Verbindungsdaten Namen und Adressen der Telefongesprächspartner seiner Angestellten ermitteln.

- Durch die in ISDN-Netzen mögliche Übermittlung der Rufnummern des Anrufers an den angerufenen Teilnehmer werden diesem unmittelbar Name und Adresse des Anrufers bekannt. Jede Person, die telefonisch Kontakt mit irgendeinem Unternehmen aufnimmt, muß damit rechnen, daß auch ihre Adresse gespeichert und für weitere Zwecke genutzt werden kann. Dies ist selbst dann bereits möglich, wenn das beabsichtigte Telefongespräch gar nicht zustande gekommen ist.

- Da der Computer mit geringem Aufwand auch Suchmöglichkeiten nach unvollständigen Angaben, z. B. Teile des Namens oder nur des Wohnortes und entsprechenden

---

[12] vom 24. Juni 1991, BGBl. I S. 1390

Kombinationen zuläßt, sind zahlreiche kriminelle Nutzungsmöglichkeiten denkbar. So kann ein zufällig wahrgenommener Name - beispielsweise am Bankschalter - schnell zur Adresse der betreffenden Person führen, sofern er über einen Telefonanschluß verfügt.

Da die Telefonbuch-CD-ROM auch als ein bundesweit multifunktionales Adreßregister genutzt und mit ihr die ursprünglich anonyme Telefonnummer zum bundeseinheitlichen "Personenkennzeichen" werden kann, sollte sich jeder Telefonteilnehmer gründlich überlegen, ob er der Aufnahme seiner Teilnehmerdaten in das Telefonbuch in Zukunft nicht doch widerspricht. Dies kann gem. § 10 Abs. 3 TDSV jederzeit geschehen, wird aber erst mit jeder Neuauflage des Telefonbuches wirksam.

2 Allgemeiner Datenschutz

2.1 Novellierung des Brandenburgischen Datenschutzgesetzes

Das Gesetz zum Schutz personenbezogener Daten im Land Brandenburg (Brandenburgisches Datenschutzgesetz - Bbg DSG)[13] ist im Berichtszeitraum zum ersten Mal geändert worden. Der Anlaß zu dieser Änderung ergab sich letztlich aus der Selbstbindung des Gesetzgebers, der in § 41 Abs. 2 der ursprünglichen Gesetzesfassung festgelegt hatte, daß mit Ablauf von 48 Monaten nach Inkrafttreten des Gesetzes personenbezogene Daten nicht mehr auf der Grundlage der §§ 12 Abs. 1, 13 bis 17 erhoben, gespeichert und übermittelt werden dürfen.

Bei Erlaß des Gesetzes Anfang 1992 hatte das Parlament gehofft, damit Druck auf die Landesregierung ausüben zu können, daß diese innerhalb von 4 Jahren die eigentlich erforderlichen genaueren und den jeweiligen Regelungsbereich entsprechenden sogenannten "bereichsspezifischen Regelungen" für den Datenschutz zur Einarbeitung in die einzelnen Spezialgesetze vorzulegen bzw. bisher fehlende Gesetzesentwürfe vorzubereiten. Diese Hoffnung hat getrogen: Die enormen gesetzgeberischen Aufgaben im Land Brandenburg waren in diesen ersten vier Jahren nach Verabschiedung des Brandenburgischen Datenschutzgesetzes offensichtlich wesentlich umfangreicher als erwartet worden war. Überlegungen, die darauf abstellten, nicht das ganze Datenschutzgesetz neueren Entwicklungen anzupassen, sondern nur die in § 41 vorgegebenen Fristen zu verlängern, gewannen immer mehr an Gewicht, je näher der im Gesetz selbst festgelegte Zeitpunkt heranrückte. Die Landesregierung hielt zeitweise sogar "situationsbedingt" eine solche "Mini-Lösung" für u. U. völlig ausreichend. Ich habe hiergegen vehement vorgetragen, daß damit eine sich nicht so schnell noch einmal bietende Chance für die Weiterentwicklung des Datenschutzes im Land Brandenburg ungenutzt bleiben würde. Außerdem bestünde an dem Gesetz bereits seit 1993 permanent Nachbesserungsbedarf. Die Landesregierung habe dies jedoch stets im Hinblick auf die zu verabschiedende EU-Datenschutzrichtlinie abgelehnt. Diese liegt nunmehr vor.

Das Erste Gesetz zur Änderung des Brandenburgischen Datenschutzgesetzes[14] hat mit insgesamt 22 Änderungspunkten tatsächlich dann jedoch einen Umfang erhalten, den man als eine "Mittel-Lösung" bezeichnen kann: weder wurde ausschließlich der Zeitraum für die Schaffung bereichsspezifischer Regelungen verlängert, noch wurde das Datenschutzgesetz wesentlich verändert. Das Gesetz ist aber insofern modernisiert worden, als einige Regelungs-Lücken geschlossen und bestimmte Ausdrücke dem heutigen Sprachgebrauch angepaßt worden sind. So ist in dem gesamten Datenschutzgesetz der Ausdruck "speichernde Stelle" durch den treffenderen Ausdruck "datenverarbeitende Stelle" ersetzt

---

13 vom 20. Januar 1992, GVBl. I S. 2

14 vom 8. Februar 1996, GVBl. I S. 17

worden. Und der Endpunkt, bis zu welchem die erforderlichen Regelungen in Spezialgesetzen geschaffen sein sollen, ist gem. § 41 Abs. 2 n. F. auf den 31. Dezember 1998 hinausgeschoben worden.

Erstmalig ist in einem Datenschutzgesetz in Deutschland mit § 11 a n. F. eine Regelung zu "Wartung und Fernwartung" aufgenommen. Wartung und Fernwartung sind damit als eine besondere Form der Datenverarbeitung gekennzeichnet und geregelt worden, beide wurden bis zur Novellierung meist mit unter dem Begriff "Datenverarbeitung im Auftrag" (§ 11 Bbg DSG) erfaßt. Diesen Formen der Datennutzung wird künftig eine immer größere und damit gewichtigere Rolle zukommen, die Regelung im Brandenburgischen Datenschutzgesetz trägt dieser Tendenz Rechnung und macht zugleich auf die Gefahren aufmerksam, die immer mit einer durch Fremde vorgenommene Maßnahmen in der Datenverarbeitung verbunden sind.

Der "Datenverarbeitung im Auftrag", § 11, hat der Gesetzgeber über das Problem der Wartung und Fernwartung hinaus seine erhöhte Aufmerksamkeit zugewandt und zwei weitere Unterpunkte neu bzw. besser geregelt. Durch einen zusätzlich angefügten 4. Absatz ist - auch dies gab es in der bisherigen Datenschutzregelung noch nicht - ausdrücklich gesetzlich festgelegt worden, daß in Unterauftragsverhältnissen ein (mindestens) gleichhoher Datenschutz-Standard eingehalten werden muß, wie er in dem ursprünglichen Vertragsverhältnis mit der öffentlichen Stelle vorgesehen war; so kann verhindert werden, daß durch das Eingehen von Untervertragsverhältnissen z. B. mit privaten Stellen, der hohe Stand des Datenschutzes der öffentlichen Stellen unterlaufen werden könnte. In Abs. 3 ist der Gesetzestext in einer Weise ergänzt worden, daß dem Rechtsanwender künftig sehr deutlich wird, daß bei Datenverarbeitung im Auftrag durch eine Stelle außerhalb des Landes Brandenburg durch Information sowohl an die im Bundesland der Auftragsdatenverarbeitung tätige Datenschutzkontrollbehörde als auch an die zuständige Aufsichtsbehörde der Datenschutzstandard des Landes Brandenburg sichergestellt wird.

Die hohe Stellung, die der Datenschutz inzwischen im Rechtsleben einnimmt, wird dadurch deutlich, daß eine Bestimmung in das Brandenburgische Datenschutzgesetz aufgenommen worden ist, daß der Landesbeauftragte für den Datenschutz künftig nicht mehr nur vor Erlaß von Verwaltungsvorschriften, sondern auch vor dem Erlaß von Rechtsvorschriften, also vor allem von Gesetzen, gehört werden muß; um eine derartige Regelung ist § 7 Abs. 2 erweitert worden.

Die Zuständigkeit des Landesbeauftragten für den Datenschutz ist außerdem insoweit ergänzt worden, als bei nicht-öffentlichen Stellen, die hoheitliche Aufgaben einer öffentlichen Stelle wahrnehmen - d. h. bei den sogenannten "Beliehenen" - infolge der Novellierung des Datenschutzgesetzes der Datenschutzbeauftragte zuständig ist; hier wurde eine Lücke im Gesetz geschlossen (§ 2 Abs. 1 Satz 3 Bbg DSG).

Mit § 33 c ist auch die Regelungsmaterie "Videoüberwachung und -aufzeichnung" neuaufgenommen worden. Die Videoüberwachung wird zur Wahrung des Hausrechts dessen, der eine solche Überwachung in seinem Haus oder auf seinem Grundstück vornimmt, eingesetzt; dies geschah bereits bisher schon, jedoch ohne rechtliche Grundlage.

Ähnliche Überlegungen wie zur Einführung einer gesetzlichen Regelung zur Videoüberwachung haben zu den beiden weiteren zusätzlichen Paragraphen (§ 33 a: "Öffentliche Auszeichnungen und Ehrungen"; § 33 b: "Begnadigungsverfahren") geführt: es wurde geregelt, unter welchen Voraussetzungen und in welchem Umfang die Datenerhebung und -übermittlung zur Vorbereitung sowohl öffentlicher Auszeichnungen und Ehrungen als auch für ein Begnadigungsverfahren in Zuständigkeit des Landes Brandenburg zulässig sind.

Mit der Landesregierung war ich darüber einig, daß künftig bei durch das Datenschutzgesetz genauer bestimmten Stellen des öffentlichen Bereichs die Einführung eines behördlichen

Datenschutzbeauftragten zwingend vorgeschrieben werden sollte. Leider ist die Mehrheit des Parlaments aus "Kostengründen" einem diesen Gedanken umsetzenden Vorschlags für das Brandenburgische Datenschutzgesetz nicht gefolgt. Es bleibt daher dabei, daß die Einrichtung eines behördlichen Datenschutzbeauftragten eine Angelegenheit ist, die z. B. von Gemeinden und Landkreisen freiwillig aufgegriffen werden kann - oder auch nicht aufgegriffen wird. Glücklicherweise haben diese nach meinen Kenntnissen größtenteils erkannt, daß behördliche Datenschutzbeauftragte eine "Institution" vor Ort darstellen, die sehr wesentlich zum guten Image gegenüber den Bürgern beitragen können. Soweit ich Einblick in die Tätigkeit der behördlichen Datenschutzbeauftragten erhalten konnte, nehmen diese ihre Aufgaben sehr engagiert wahr.

Die vorgenannten Neuerungen, die in das Brandenburgische Datenschutzgesetz eingearbeitet worden sind, habe ich bei ihrer Entstehung beratend begleitet und ausdrücklich begrüßt. Dies gilt auch für die kleineren Änderungen und sprachlichen Verbesserungen, die das Gesetz erhalten hat. Dies gilt jedoch nicht für eine bestimmte Neuregelung, die erst im letzten Moment in das Änderungsgesetz und damit in das Datenschutzgesetz eingefügt worden ist: es betrifft die Herausnahme der Geltung des Gesetzes für den Landtag, soweit der Landtag Verwaltungsaufgaben wahrnimmt. Der Landtag hat statt dessen in dem neueingefügten Abs. 1 a in § 2 Bbg DSG die Absicht vorgestellt, eine "Datenschutzordnung" erlassen zu wollen, um darin in der Zukunft die Verarbeitung personenbezogener Daten im Parlamentsbereich zu regeln. Um dieser Datenschutzordnung eine "gesetzliche Grundlage" zu geben, solle eine sogenannte "Parlamentsklausel" in das Brandenburgische Datenschutzgesetz eingefügt werden. Ich habe jedoch ernsthafte Zweifel daran, daß durch eine Datenschutzordnung für das Parlament, die ja nicht im Rang eines Gesetzes stehen würde, im Verhältnis zu Dritten (hier: der Bürger) eine den Kriterien des sogenannten "Volkszählungsurteils"[15] gemäße Regelung gefunden wird (s. hierzu unter 2.2).

Schließlich hat das Brandenburgische Datenschutzgesetz nicht nur Korrekturen und Ergänzungen erfahren, sondern es hat auch Streichungen hinnehmen müssen. Aus Vereinfachungsgründen ist § 24 (Dateienregister) weggefallen. Bisher war die "speichernde Stelle" verpflichtet gewesen, dem Landesbeauftragten für den Datenschutz eine Beschreibung aller automatisiert geführten Dateien, in denen personenbezogene Daten gespeichert sind, vorzulegen; der Landesbeauftragte hatte ein Register dieser Dateien anzulegen. Mit den Meldungen zum Dateienregister war den öffentlichen Stellen aufgegeben worden, ihre Dateien an eine Stelle außerhalb der eigenen Behörde zu melden und daher bewußt mit dem Einrichten von Dateien umzugehen. Zugleich war den Bürgern die Möglichkeit gegeben worden, sich über solche Dateien zu informieren. Künftig werden solche Aufstellungen der verwendeten Dateien einer Behörde nur noch bei der Behörde selbst geführt werden, eine Einsichtsnahme der Bürger gibt es nicht mehr. Die Sorgfalt bei dem Anlegen solcher Verzeichnisse wird nur noch hin und wieder vom Landesbeauftragten für den Datenschutz bei Kontrollen vor Ort überprüft werden. Die Abschaffung des Registers läuft darüber hinaus in die entgegengesetzte Richtung gegenüber den Tendenzen des neuen europäischen Datenschutzrechts.

Bei der Novellierung ist das Thema Privatisierung öffentlicher Stellen seitens des MI ausgeklammert worden. Nach meiner Überzeugung hätte der Trend der öffentlichen Verwaltung, Aufgaben in den Privatbereich zu verlagern oder kommunale Betriebe in privatrechtliche Organisationsformen zu überführen, unbedingt bei der Novellierung berücksichtigt werden müssen.

Durch diese inzwischen üblich gewordenen Verfahrensweisen, die zumeist die Effektivität der öffentlichen Verwaltung steigern sollen, ergeben sich unerwünschte Nebeneffekte beim Datenschutz. Zum einen werden öffentliche Stellen zu nicht-öffentlichen Stellen, mit der

---

[15] BVerfGE 65, 1

Folge, daß die Zuständigkeit für Kontrollen vom Landesbeauftragten für den Datenschutz auf das MI übergeht, zum anderen aber ist das Bbg DSG für diejenigen der so entstandenen privatrechtlich organisierten Einrichtungen, die zuvor nicht bereits als Eigenbetriebe gegolten hatten, insofern nicht mehr das maßgebliche Datenschutzgesetz, als in § 2 Abs. 2 Satz 2 Bbg DSG für nicht-öffentliche Stellen auf die Vorschriften des Bundesdatenschutzgesetzes (BDSG) und dessen - gegenüber den Vorschriften für öffentliche Stellen weniger strenge Datenschutzvorgaben - verwiesen wird.

Der Bundesgesetzgeber hat auf derartige Tendenzen, die im Prinzip seit langem zu beobachten sind, reagiert und in § 2 Abs. 3 BDSG festgelgt, daß "Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen" als öffentliche Stellen gelten, sofern die absolute Mehrheit der Anteile dem Bund oder den Länden gehört oder diesen die absolute Mehrheit der Stimmen zusteht. Vergleichbare Regelungen finden sich auch in den Datenschutzgesetzen anderer Bundesländer. Durch diese Regelung wird erreicht, daß eine privatrechtliche Rechtsform nicht automatisch eine Änderung der Zuständigkeiten im Datenschutz zur Folge hat. In vergleichbarer Weise hätte die Problematik der Privatisierung öffentlicher Aufgaben bei der Novellierung des Bbg DSG berücksichtigt werden können.

2.2 Beantwortung von Petitionen / Datenschutz im Landtag

Anläßlich der Beantwortung einer Petition im Landtag wurde das Problem deutlich, daß im Zusammenhang mit manchen Petitionen zugleich personenbezogene Daten Dritter z. B. an Ministerien weitergegeben werden, damit die Petition überhaupt behandelt werden kann. Der Petitionsausschuß wollte mit dem Ministerium des Innern (MI) eine Verfahrensweise absprechen, wie vorgegangen werden sollte, wenn z. B. eine Petition nicht durch den Betroffenen selbst eingereicht wird oder wenn Angehörige des Petenten durch die Petition betroffen sind. Hierzu bin ich vom MI um Stellungnahme gebeten worden.

Das Bbg DSG enthält für diesen Fall keine Regelung. Die Formulierung der ursprünglichen Gesetzesfassung besagte, daß das Datenschutzgesetz für den Landtag und für die Gerichte nur Geltung habe, "soweit sie Verwaltungsaufgaben wahrnehmen". Das bedeutete demnach, daß das Bbg DSG als Ganzes auf die Bereiche des Landtages, die nicht zur Verwaltung zu rechnen sind, nicht anzuwenden war, so daß weder der Landesbeauftragte für den Datenschutz noch die nach § 38 BDSG für nicht-öffentliche Stellen zuständige Behörde, das MI, für den Datenschutzes im Nicht-Verwaltungsbereich des Landtages zuständig waren.

Dem MI und den zuständigen Stellen des Landtages - dem Präsidenten und der Vorsitzenden des Petitionsausschusses - habe ich daraufhin einen Vorschlg unterbreitet, wie man das hier deutlich gewordene Problem angehen und bewältigen könnte. Es liegt auf der Hand, die Lösung des Problems durch die Schaffung einer spezialgesetzlichen Regelung im Petitionsgesetz anzustreben. Da eine parlamentarische Behandlung dieses Gesetzes in der nächsten Zeit nicht in Aussicht steht, habe ich die ebenfalls denkbare Variante angeregt, die Aufnahme einer solchen Regelung in das Datenschutzgesetz zu erwägen, zumal dessen Novellierung zu diesem Zeitpunkt unmittelbar bevorstand.

Die Regelungen, die damals noch zusätzlich in das Bbg DSG hätten eingearbeitet werden sollen, betrafen mindestens die folgenden Punkte:

- die Zuständigkeit des LfD durch Anwendung der Vorschriften des Abschnittes 2 des Bbg DSG,

- die Einhaltung der Regelungen über das Datengeheimnis, der technisch-organisatorischen Maßnahmen, der Einhaltung der Zweckbindung und der Vorschriften über die Übermittlung innerhalb des öffentlichen Bereichs durch Anwendung der §§ 6, 10, 13 und

14 Bbg DSG. Regelungen von sehr speziellen Fragen des Datenschutzes könnten in jedem Fall nur in das Petitionsgesetz eingearbeitet werden.

Meinen Vorschlägen wurde nicht gefolgt.

Statt dessen wurde ein eher gegensätzlicher Vorschlag vom Parlament aufgegriffen. Dieser Vorschlag fußt auf einer Ausarbeitung der Direktoren der Landtage (Thesen und Musterentwurf für eine Datenschutzordnung der Landtage), den die Präsidenten der Landtage im Mai 1995 bestätigt hatten. Nach meiner Ansicht, die ich auch vor Verabschiedung des Änderungsgesetzes für das Brandenburgische Datenschutzgesetz dem Innenausschuß des Landtages vorgetragen habe, bestehen rechtliche Zweifel daran, ob eine Parlamentsordnung den Anforderungen gerecht werden kann, die durch das Bundesverfassungsgericht im "Volkszählungsurteil" in bezug auf Eingriffe in das Persönlichkeitsrecht aufgestellt worden sind. Bei der Behandlung von Petitionen, die nicht von betroffenen Personen selbst beim Landtag eingereicht worden sind, oder welche Angehörige von Petenten betreffen (beides sog. "Dritte"), können derartige Eingriffe in das Recht auf informationelle Selbstbestimmung dieser Personen stattfinden. Darüber hinaus wird in dem Musterentwurf für eine Datenschutzordnung zum Petitionsausschuß und dessen spezifischen Probleme gar nichts gesagt.

Eine genauere Wertung dieser Angelegenheit wird erst möglich sein, wenn der Landtag darangeht, eine "Datenschutzordnung" - wohlgemerkt nicht als Gesetz (!) - zu erlassen, deren Inhalt und Reichweite werden zu beurteilen sein, und gegebenenfalls wird sich die Notwendigkeit zeigen, daß das Bbg DSG erneut zu ändern oder das Petitionsgesetz im Hinblick auf den Umgang mit Petitionen unter datenschutzrechtlichen Aspekten zu ergänzen sein wird.

Da es sich um eine bundesweit relevante Thematik handelt, hat sich auf meine Anregung hin inzwischen die Konferenz der Datenschutzbeauftragten des Bundes und der Länder damit befaßt und beschlossen, diese Problematik zu einem Schwerpunktthema für ihre Herbstkonferenz 1996 vorzusehen.

2.3 Gestaltung von Erhebungsvordrucken

Durch zahlreiche Nachfragen von Betroffenen bei meiner Behörde bin ich auch im Berichtszeitraum wiederholt darauf gestoßen, wie wichtig die Gestaltung von Formularen aus der Sicht des Datenschutzes für den Rechtsverkehr mit Behörden ist. Bereits das äußere Bild, aber auch die Art der Fragestellungen und die Hinweise zum Ausfüllen von Formularen sind für die Sicherstellung des Datenschutzes wegweisend.

Behörden verwenden nicht selten z. B. Erhebungsbögen, die von Seiten privater Verlage vorbereitet und den öffentlichen Stellen zum Erwerb angeboten werden. Es scheint manchmal so zu sein, daß derartige Verlage die von ihnen angebotenen Vordrucke völlig in eigener Verantwortung planen und herstellen und auf die Belange des Datenschutzes dabei wenig achten.

Ganz ähnlich gehen offenbar auch einige Ersteller von Software vor, deren Programmausdrucke Formularcharakter haben oder wie Formulare verwendet werden: Anbieter von Programmen z. B., die der Erstellung von Lohn- und Gehaltsaberechnungen dienen, und deren Ergebnisse schließlich zum Nachweis der vom Arbeitgeber abgeführten Lohnsteuer und anderer Vergütungsanteile ausgedruckt und auf der Lohnsteuerkarte angebracht werden, haben sich offenbar um den Datenschutz wenige oder garkeine Gedanken gemacht. Aus der Sicht der Programm-Anbieter ist der Datenschutz möglicherweise kaum beeinträchtigt - da aber Lohnsteuerkarten oder deren Kopie recht häufig zum Nachweis der gezahlten Vergütung oder der einbehaltenen Sozialbeiträge von

anderen Stellen als dem Finanzamt angefordert werden, muß die Forderung erhoben werden, daß auch in solchen Fällen auf den Datenschutz zu achten ist.

Die Anforderungen, die an ein datenschutzgerechtes Formular zu stellen sind, können jedoch ohne einen besonderen Aufwand eingehalten werden, sei es, daß die Anbieter solcher Formulare oder Programme sich selbst verpflichten, durch fachliche Beratung sicherzustellen, daß der Datenschutz beachtet wird, sei es, daß die Behörde, die bestimmte Formulare verwendet, auf deren datenschutzgerechte Gestaltung hinwirkt, bevor sie solche Formular-Vordrucke bestellt. In jedem Fall ist dem Datenschutz am besten gedient, wenn er, sofern das überhaupt möglich ist, immer bereits vorbeugend beachtet wird.

Selbst dann, wenn Formulare privater Anbieter in einem weiträumigen Gebiet - Ländergrenzen übergreifend - verwendet werden können, ist die Berücksichtigung des Datenschutzes immer möglich.

Die gesetzlichen Grundlagen für eine datenschutzgerechte Ausgestaltung von Erhebungsbögen (gem. §§ 12 Abs. 3 und 4 Abs. 2 Bbg DSG), finden ihre Entsprechung in den Regelungen der Datenschutzgesetze anderer Bundesländer und des Bundesdatenschutzgesetzes. In jedem Fall sind auf dem Antragsformular

- die datenverarbeitende Stelle (§ 12 Abs. 3 Bbg DSG),
- der Zweck der Erhebung (§ 12 Abs. 1 Bbg DSG),
- die Angabe, aus welchem Grund die Beantwortung aller oder bestimmter Fragen des Erhebungsbogens erforderlich ist (§ 12 Abs. 1 Bbg DSG) und was geschieht, falls Antworten fehlen oder falsch sind,
- ein Hinweis darauf, ob bzw. daß die Übermittlung der Daten an eine andere Stelle beabsichtigt ist (§ 14 Bbg DSG),
- der Dritte, an den möglicherweise oder in jedem Falle die Daten übermittelt werden (§ 14 Bbg DSG),
- die Rechtsvorschriften, auf welche bezug genommen wird (§ 14 Bbg DSG) und
- die Kennzeichnung derjenigen Fragen, deren Beantwortung dem Betroffenen freigestellt ist (§ 12 Abs. 3 Bbg DSG)

anzugeben, um der Verpflichtung zur Aufklärung nachzukommen und dem Transparenzgebot zu entsprechen.

Wenn es darum geht, die Freiwilligkeit der Beantwortung bestimmter Fragen zu verdeutlichen, bieten sich mehrere Wege an: entsprechende Hinweise können an den Anfang oder in eine - gut sichtbare - Fußnote aufgenommen werden, sie können, was möglicherweise sicherer wirkt, jeweils mit der Frage selbst verbunden werden, in einem Merkblatt kann auf die Art der Beantwortung hingewiesen, und derartige Fragen können drucktechnisch hervorgehoben werden. Schließlich ist auch denkbar, daß die Reihenfolge der zu beantwortenden Fragen so ausgestaltet wird, daß freiwillig zu beantwortende Fragen an einer Stelle des Formulars - z. B. am Ende - zusammengefaßt werden.

Sofern es der Erfahrung nach wahrscheinlich ist, daß das Formular in einem anderen Zusammenhang, d. h. zu einem anderen Zweck zusätzlich verwendet werden wird (z. B. Kopie der Lohnsteuerkarte), kann bereits bei der Gestaltung des Formulars darauf hingewirkt werden, daß zu übermittelnde Daten nur in reduziertem Umfang weitergegeben werden, d. h., daß nur diejenigen Angaben für den zusätzlichen Zweck verwendet werden, die für den betreffenden Zweck erforderlich sind.

Selbstverständlich habe ich nicht die Absicht zu verlangen, daß alle Formulare, die nicht datenschutzgerecht sind, wegzuwerfen seien. Das Aufbrauchen von Vordrucken, in denen der Datenschutz nicht oder nicht ausreichend beachtet ist, kann durchaus auch in datenschutz-gerechter Form erfolgen: durch die Beigabe eines Merkblattes kann z. B. auf die

Freiwilligkeit bestimmter Antworten hingewiesen werden. Betonen möchte ich allerdings, daß selbst eine hilfreiche Nachbesserung eine ordnungsgemäße Formulargestaltung nicht ersetzen kann.

3 Inneres

3.1 Meldewesen

3.1.1 Meldedaten - Regelmäßige Übermittlungen

Das Brandenburgische Meldegesetz (BbgMeldeG)[16] läßt regelmäßige Übermittlungen von Meldedaten durch Meldebehörden an andere Behörden und sonstige öffentliche Stellen nur in dem Umfang zu, in dem diesen Stellen auf Anfrage Auskunft zu geben wäre. In § 29 Abs. 2 BbgMeldeG hat der Gesetzgeber festgelegt, daß dies durch Rechtsverordnung zugelassen werden kann, in der Anlaß und Zweck der Übermittlung, die Datenempfänger, die zu übermittelnden Daten, ihre Form sowie das Nähere über das Verfahren festzulegen sind.

Hiervon hat der Minister des Innern Brandenburgs mit der Verordnung über regelmäßige Datenübermittlungen der Meldebehörden (MeldDÜV)[17] Gebrauch gemacht, die zuletzt 1995 geändert wurde[18]. Eine weitere vorgesehene Änderung, mit der insbesondere Datenübermittlungen an den Ostdeutschen Rundfunk Brandenburg (ORB) bzw. die Gebühreneinzugszentrale (GEZ), an amtsangehörige Gemeinden, an Wasser- und Abwasserzweckverbände und an die Ausländerbehörden erstmalig geregelt werden sollten, ist zurückgestellt worden, weil alle bisherigen und beabsichtigten Regelungsinhalte in einer neuen Rechtsverordnung zusammengefaßt werden sollen. Die komplette Neufassung dient der besseren Überschaubarkeit des Umgangs mit Meldedaten im Land Brandenburg.

Meine Ergänzungs- und Änderungsvorschläge zu dem Entwurf konnten sich aufgrund des Verhandlungsvorlaufs abschließend auf die einleitenden Grundsätze und Verfahrensregelungen beschränken, da der Entwurf eine ursprünglich vorgesehene und von mir abgelehnte regelmäßige Datenübermittlung an den ORB bzw. die GEZ nicht mehr vorsieht (s. unter 3.1.1.1) und bezüglich der neu hinzugenommenen Datenübermittlungen an Bürgermeister amtsangehöriger Gemeinden (s. unter 3.1.1.2) eine Regelung gefunden sein wird, die zumindest meine bis dahin geäußerten Bedenken hinsichtlich des ursprünglich vorgesehenen Empfängerkreises - ins- besondere auch bezüglich der Übermittlung von Jubiläumsdaten - berücksichtigt.

Unter Hinweis darauf, daß die Grundsätze und Verfahrensregelungen in ihrer bisherigen Fassung mit ihren zu allgemeinen Formulierungen nicht mehr den zwischenzeitlich deutlich verbesserten Arbeitsbedingungen vor Ort entsprechen und deshalb in Hinblick auf die veränderte Situation nachgebessert werden müssen, habe ich folgende Ergänzungsvorschläge unterbreitet:

- Datenübermittlung nach Maßgabe der Verordnung umfassen auch das Vorhalten von Daten zum Abruf (systematische Ergänzung bezüglich der Online-Verfahren).

---

16 vom 25. Juni 1992, GVBl. I S. 236

17 vom 26. Oktober 1992, GVBl. II S. 688

18 Erste Verordnung zur Änderung der Verordnung über regelmäßige Datenübermittlungen der Meldebehörden (1. MeldDÜÄV) vom 8. Dezember 1993, GVBl. II S. 776
Zweite Verordnung zur Änderung der Verordnung über regelmäßige Datenübermittlungen der Meldebehörden (2. MeldDÜÄV) vom 13. Februar 1995, GVBl. II S. 239

- In automatisierten Verfahren sind die zu übermittelnden personenbezogenen Daten als zusätzliche Sicherungsmaßnahmen grundsätzlich zu verschlüsseln (Dies entspricht den gewachsenen Anforderungen, die heute speziell an eine regelmäßige Datenübermittlung in öffentlichen Netzen zu realisieren sind. Damit würde sich der Aufwand erhöhen, der erforderlich wäre, um unbefugt auf die Daten während deren Übermittlung zugreifen zu können.).

- Zur Sicherstellung der Kenntnisnahme nur durch berechtigte Personen und der unverzüglichen Löschung der Daten, die zur Aufgabenerfüllung nicht mehr erforderlich sind, sind Maßnahmen vor der ersten Datenübermittlung zwischen der übermittelnden Stelle und dem Datenempfänger schriftlich festzulegen und ihre Einhaltung regelmäßig zu überprüfen (Diese Ergänzung würde eine Konkretisierung des Grundsatzes von § 14 Abs. 4 Bbg DSG darstellen. Danach darf der Empfänger die übermittelten Daten nur für die Zwecke verarbeiten und nutzen, zu deren Erfüllung sie ihm übermittelt worden sind.).

Im übrigen habe ich auch angeregt, die Vorgaben der Datenübermittlungsgrundsätze Brandenburg[19], die auch nach heutiger Bewertung keinesfalls überholt sind, direkt in die Verordnung aufzunehmen, um eine den inhaltlichen Regelungen angemessen bindende Konkretisierung auch der technisch-organisatorischen Maßnahmen in der Verordnung selbst zu garantieren.

Informationen über den weiteren Fortgang in dieser Angelegenheit lagen mir zum Ende des Berichtszeitraumes noch nicht vor.

3.1.1.1 Datenübermittlungen an ORB bzw. GEZ für Rundfunkgebühreneinzug

Die ursprünglich beabsichtigte 3. Ergänzung der MeldDÜV sah vor, daß die Meldebehörden dem ORB oder der GEZ zum Zwecke der Erhebung und des Einzugs der Rundfunkgebühren im Falle der Anmeldung, Abmeldung oder des Todes regelmäßig Familiennamen, Vornamen, Doktorgrad, Tag der Geburt, gegenwärtige und frühere Anschriften, Tag des Ein- und Auszugs, Familienstand und Sterbetag volljähriger Einwohner übermitteln dürfen.

Dies war insbesondere auf einen Beschluß der Konferenz der Innenminister des Bundes und der Länder[20] zurückzuführen, mit dem den Ländern empfohlen wird, in ihren Datenübermittlungsverordnungen den freien Zugang der Rundfunkanstalten zu den Meldedaten zu verankern. Obwohl danach in anderen Bundesländern entsprechende Regelungen in die jeweiligen Meldedaten-Übermittlungsverordnungen eingefügt wurden, bin ich einer solchen Umsetzung in Brandenburg insbesondere aus folgenden Gründen entgegengetreten:

- Mit der Schaffung einer solchen Rechtsgrundlage würde die Datenübermittlung in einer dem informationellen Selbstbestimmungsrecht zuwiderlaufenden Weise nicht auf die eigentliche Zielgruppe ("Schwarzhörer bzw. -seher") beschränkt oder zumindest ausgerichtet bleiben. Es sollten andere Lösungsmöglichkeiten im Rahmen der bestehenden rechtlichen Gegebenheiten genutzt werden[21].

- Im Hinblick auf die Vorgaben des Staatsvertrages der Länder Berlin und Brandenburg sollte eine solche Rechtsgrundlage im Vorfeld der angestrebten Fusion zur Vermeidung von Irritationen - wenn überhaupt - nur in Abstimmung mit Berlin (das eine solche

---

19 vgl. RdErl. des Ministerium des Innern vom 17. September 1991 - II/7-2.100, ABl. S. 728

20 Sitzung am 26. November 1993

21 s. 2. Tätigkeitsbericht, Anlage 14 (Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 in Berlin)

Übermittlungsregelung bislang ebenfalls nicht vorgesehen hat) geschaffen werden.

Mit Genugtuung kann ich feststellen, daß das Ministerium des Innern (MI) zumindest auf eine diesbezügliche Ergänzung in dem kürzlich vorgelegten Entwurf zu einer neuen MeldDÜV verzichtet hat (s. unter 3.1.1).

3.1.1.2 Datenübermittlungen an Bürgermeister amtsangehöriger Gemeinden

Mit der Neuregelung der MeldDÜV (s. unter 3.1.1) soll es auch erlaubt werden, daß ehrenamtliche Bürgermeister zum Zwecke ihrer Aufgabenerfüllung folgende Daten von Einwohnern ihres Gemeindegebietes regelmäßig übermittelt bekommen:

- Familiennamen und Vornamen, Doktorgrad, Tag der Geburt, gegenwärtige Anschrift, Tag des Ein- oder Auszugs sowie eingetragene Übermittlungssperren bei An- und Abmeldungen

- Namen, Tag der Geburt, gegenwärtige Anschrift und eingetragene Übermittlungssperren bei Geburt eines Kindes und

- die genannten Daten (ausschließlich Tag des Ein- und Auszugs) zuzüglich Sterbedatum bei Tod eines Einwohners.

Zusätzlich sollen zum Zwecke der Ehrung von Altersjubilaren, die den 60. oder einen späteren Geburtstag begehen, und von Ehejubilaren, die das 50jährige oder ein späteres Ehejubiläum begehen, der Tag und die Art des Jubiläums übermittelt werden dürfen.

In einer ursprünglichen Fassung war noch vorgesehen, daß diese Daten neben den ehrenamtlichen Bürgermeistern auch den Gemeindevertretungen übermittelt werden dürfen und daß die Übermittlungen auch durch das regelmäßige Überlassen des fortgeschriebenen Bestandes der genannten Daten aller Einwohner erfolgen können, womit rechtlich unzulässig parallele Melderegister entstanden wären.

Von diesen Regelungen ist das MI in dem Entwurf nach eingehendem Argumentationsaustausch mit mir jetzt abgegangen. Insbesondere begrüße ich den Verzicht auf eine Übermittlung auch an die Gemeindevertretungen, jedoch wollte das MI nicht auch meiner Forderung nachkommen, wegen des Regelungsmangels in § 59 Abs. 3 und 4 Gemeindeordnung (GO)[22] hinsichtlich der Aufgabenstellung ehrenamtlicher Bürgermeister die Übermittlungen auf den Zweck der Ehrung von Alters- und Ehejubiläen zu beschränken. Selbst bei allem Verständnis dafür, daß ein ehrenamtlicher Bürgermeister auch über Veränderungen der Einwohnerstruktur seiner Gemeinde - also über An- und Abmeldungen sowie über Geburten und Todesfälle - Kenntnis haben sollte, bedarf es dennoch dafür einer dem Recht auf informationelle Selbstbestimmung entsprechenden normenklaren materiell-rechtlichen Regelung. Mit dem MI gehe ich immerhin davon aus, daß auch die ehrenamtlichen Bürgermeister die allgemeinen Verfahrensgrundsätze des Verordnungsentwurfs bezüglich der Datensicherungsmaßnahmen und der unverzüglichen Löschung unmittelbar nach Erfüllung ihrer Aufgaben, die sich aus ihrem genannten Informationsbedürfnis ergeben, beachten werden.

3.1.1.3 Jubiläumsdaten an das Bundespräsidialamt

Auf Schreiben vom 24. Juli 1995 hatte das Bundespräsidialamt den Staatskanzleien der Länder mitgeteilt, daß vom 1. Oktober 1995 an geänderte "Grundsätze für Ehrung von Alters- und Ehejubilaren durch den Herrn Bundespräsidenten" (Grundsätze) gelten, die

---

[22] vom 15. Oktober 1993, GVBl. I S. 398, geänd. d. Art. 3 d. 1. BbgFRG vom 30. Juni 1994, GVBl. I S. 230

jeweils in den Ländern mit dem Ziel veröffentlicht werden sollten, u. a. die kreisfreien Städte, Landkreise und Gemeinden "entsprechend anzuweisen".

Mit der Änderung sollte ein bereits seit 1992 bekanntes Verfahren, wonach dem Bundespräsidialamt "von den zuständigen Behörden" Vornamen, Namen, Anschriften und Geburtsdaten bzw. Hochzeitsdaten von Altersjubilaren ab Vollendung des 100. Lebensjahres und von Ehejubilaren aus Anlaß des 65., 70. und 75. Hochzeitstages in Antragsform zum Zweck der Gratulation durch den Herrn Bundespräsidenten und der evtl. Gewährung eines Geldgeschenkes zuzuleiten sind, insbesondere dahingehend modifiziert werden, daß

- der Herr Bundespräsident Bürgern zur Vollendung des 100. Geburtstags - und dann erst wieder zum 105. und jeden folgenden Geburtstag - gratuliert,

- "aus Gründen der Belegprüfung durch den Bundesrechnungshof" unbedingt auch er- und übermittelt werden muß, ob die vorgesehene Einkommensgrenze für die Gewährung einer Ehrengabe unter- oder überschritten wird,

- bei Altersjubiläen - soweit bekannt - auch Informationen über den Gesundheitszustand des zu Ehrenden übermittelt werden.

Die neuen Grundsätze haben in Brandenburg Niederschlag in einer Bekanntmachung der Staatskanzlei vom 4. Juli 1995[23] gefunden. Neben der Tatsache, daß in der Bekanntmachung nicht definiert ist, wer die "zuständigen Behörden" sind, die die Anträge "zuzuleiten" haben, fehlt es an einem Hinweis sowohl auf die Erhebungsbefugnis durch bzw. für das Bundespräsidialamt als auch auf die Norm für die Übermittlungsbefugnis der "zuständigen Behörden".

Mit Kollegen in anderen Bundesländern vertrete ich die Auffassung, daß ungeachtet evtl. landesrechtlicher Erhebungs- oder Übermittlungsbefugnisse bezüglich der erforderlichen Daten - insbesondere auch unter dem Aspekt, daß mit der Ermittlung von Einkommensverhältnissen und gesundheitlichen Gegebenheiten - so deutlich in die intime Privatsphäre Betroffener eingegriffen wird, daß dies spätestens seit dem Volkszählungsurteil[24] nur noch durch eine materiell-rechtliche Erhebungsbefugnis für das Bundespräsidialamt gerechtfertigt werden kann. Eine solche Rechtsgrundlage gibt es zur Zeit aber nicht.

Auch eine landesrechtliche Befugnis zum "Sammeln" und regelmäßigen Übermitteln der geforderten Daten ist nicht erkennbar. Zwar könnte diese zunächst in dem neu hinzugekommenen § 33 a Bbg DSG[25] vermutet werden, wonach gem. Abs. 1 Satz 1 zur Vorbereitung öffentlicher Auszeichnungen und Ehrungen die zuständigen Stellen die dazu erforderlichen Daten auch ohne Kenntnis des Betroffenen erheben und weiter verarbeiten dürfen. Dies kann aber nur Dienststellen des Landes Brandenburg im Rahmen eigener Aufgabenerfüllung betreffen. Eine Verarbeitung der erhobenen Daten für eine - wenn auch vergleichbare - Verarbeitung an anderer Stelle, wäre jedenfalls eine Zweckänderung und insoweit nach Abs. 1 Satz 2 nur mit Einwilligung des Betroffenen möglich.

Jedoch kann diese allgemeine Rechtsgrundlage ohnehin nicht auch für die Verarbeitung der Daten herangezogen werden, die zugleich Meldedaten sind, weil hierfür die spezialgesetzlichen Regelungen des BbgMeldeG greifen. Danach wäre eine regelmäßige Datenübermittlung gem. § 29 Abs. 1 und 2 unmittelbar von den Meldebehörden an das

---

23 vom 20. März 1996, ABl. S. 298 f.

24 BVerfGE 65, 1

25 1. Gesetz zur Änderung des Brandenburgischen Datenschutzgesetzes vom 8. Februar 1996, GVBl. I S. 17

Bundespräsidialamt zumindest des vollständigen Namens, der Anschrift, des Geburtsdatums bzw. des Hochzeitsdatums der Jubilare auf der Grundlage einer Rechtsverordnung, etwa der MeldDÜV (s. unter 3.1.1), möglich, jedoch nur, "soweit dies durch Bundes- oder Landesrecht unter Festlegung des Anlasses und des Zwecks der Übermittlungen, der Datenempfänger und der zu übermittelnden Daten bestimmt ist".

Somit ist der in einer ersten Stellungnahme vom MI vorgeschlagene Weg ausgeschlossen, daß die Übermittlung über die Staatskanzlei, die bereits gem. § 7 MeldDÜV regelmäßig "Jubiläumsdaten" von den Meldebehörden erhält, erfolgen könnte, weil diese Datenübermittlung nur zur Erfüllung dortiger - wenn auch vergleichbarer - Aufgaben zugelassen ist.

Selbst wenn - noch über die Grundsätzeregelung wie z. B. in Niedersachsen hinaus - nicht nur die Erhebung und Übermittlung der Einkommens- und Gesundheitsverhältnisse, sondern die Übermittlung sämtlicher geforderter Daten von der Einwilligung der Jubilare abhängig gemacht würden, müßte zumindest normenklar und insoweit für Betroffene nachvollziehbar und nachprüfbar festgelegt werden, welche Stellen hierfür zuständig sind.

Ich begrüße zwar das Angebot des MI, einvernehmlich mit mir eine (geeignete) Regelung für Brandenburg vorbereiten zu wollen, jedoch halte ich es für wichtiger, daß zunächst länderübergreifend mit dem Bundespräsidialamt für die im Rahmen der Bürgernähe ohne Zweifel wichtigen und begrüßenswerten Maßnahmen des Herrn Bundespräsidenten nach Verfahrensregelungen gesucht wird, die modernen Anforderungen auch bezüglich der Rechtsgestaltung entsprechen.

3.1.1.4 Regelmäßige Übermittlung an Finanzämter

Zu Recht wandte sich der Datenschutzbeauftragte eines anderen neuen Bundeslandes gegen die Absicht, mittels einer dortigen Meldedaten-Übermittlungsverordnung zuzulassen, daß die Meldebehörden den jeweils zuständigen Finanzämtern "zur Erfassung der Einwohner für Zwecke der Besteuerung ... sowie zur Sicherung des Steueraufkommens" regelmäßig Daten derjenigen Einwohner übermitteln dürfen, die sich "an- oder abgemeldet haben".

Mit einer solchen Regelung würde nicht nur der Rahmen der Erforderlichkeit weit überschritten, da nicht jeder Bürger (z. B. Kinder, Empfänger von Sozialleistungen) abgabepflichtig ist, es würde auch ein zweites (wenngleich auf die Einwohner des Zuständigkeitsbereiches reduziertes) Melderegister entstehen. Dies zu führen und fortzuschreiben ist allerdings ausschließlich Aufgabe der Meldebehörden. Die pauschale Begründung, "die vorgesehene regelmäßige Datenübermittlung an Finanzämter ist bereits seit Jahren bewährte Praxis in alten und neuen Bundesländern", konnte ich dem Kollegen auf Brandenburg bezogen erfreulicherweise nicht bestätigen.

Nach § 4 MeldDÜV ist in Brandenburg eine solche Übermittlung ausschließlich bei Abmeldungen in das Ausland erlaubt. Zwar sah ich zunächst in der Entwurfsphase zu dieser Regelung die Gefahr der Stigmatisierung einer bestimmten Personengruppe, mußte allerdings zugestehen, daß mit der Datenübermittlung von Abmeldungen in das Ausland nicht automatisch der Verdacht der Steuerhinterziehung verbunden ist, vielmehr eventuellen Gefahren der nicht rechtzeitigen Steuereinnahme begegnet werden soll. Insoweit kommt mit der Übermittlung lediglich die Tatsache eines dem Betroffenen freigestellten Umzugs ins Ausland zum Ausdruck, ohne daß damit auch eine unmittelbare Verdachtsannahme der Steuerhinterziehung verbunden wäre. Jedenfalls ist mit der brandenburgischen Regelung nicht eine allgemeine Datenübermittlung und somit die Gefahr des Aufbaus eines unerlaubten "Zweiten Melderegisters" verbunden.

3.1.1.5 Auskünfte an Detekteien

Die Beschreibung der Arbeitsweisen einer Detektei in einem anderen Bundesland in einer bekannten Wochenzeitschrift ließ meinen dortigen Kollegen darauf schließen, daß möglicherweise datenschutzrechtliche Vorschriften durch das Unternehmen verletzt worden waren. Bei der in seiner gleichzeitigen Eigenschaft als Aufsichtsbehörde für den Datenschutz im privaten Bereich deswegen durchgeführten Prüfung stellte sich u. a. heraus, daß auch von brandenburgischen Meldebehörden Auskünfte an die Detektei erteilt worden waren, die möglicherweise auch durch hiesige meldegesetzliche Bestimmungen nicht abgedeckt waren.

So war - wie mich mein Kollege informierte - nach dortigen Aufzeichnungen u. a.

- vom Einwohnermeldeamt einer großen Gemeinde neben der Adresse zu einer Person auch deren Geburtsdatum telefonisch übermittelt worden

- von einem anderen Einwohnermeldeamt zu einer bestimmten Person mitgeteilt worden, daß keine aktuelle Anschrift bestehe, die Person sich "jedoch unangemeldet in dem Ort aufgehalten" habe.

Darüber hinaus hatte sich die Detektei offensichtlich in mehreren Fällen die Auskünfte unter falschem Namen (Kreditinstitut u. ä.) eingeholt.

Da § 32 Abs. 1 BbgMeldeG die Möglichkeit einer mündlichen bzw. schriftlichen Auskunft an Private ohne berechtigtes Interesse auf einen genau bestimmten Datenumfang - nämlich Familiennamen, Vornamen, akademische Grade, gegenwärtige Anschriften (Haupt- und Nebenwohnung) sowie die Tatsache, daß ein Einwohner verstorben ist - begrenzt, war im ersten Fall die Übermittlung auch des Geburtsdatums unzulässig. Im zweiten Fall war die Mitteilung insoweit unzulässig, als durch den Mitarbeiter des Einwohnermeldeamtes auch private Kenntnisse mitgeteilt worden waren, die nicht Bestandteil des Melderegisters sind.

Nach übereinstimmender datenschutzrechtlicher Beurteilung zumindest der genannten Fälle folgte das MI unverzüglich meiner Anregung, die Meldebehörden in geeigneter Weisung zu einer den rechtlichen Bestimmungen entsprechenden Praxis bei der Erteilung von Melderegisterauskünften anzuhalten, indem es noch einmal sein einschlägiges Schreiben vom 5. März 1993 an alle Meldebehörden des Landes Brandenburg über die Oberbürgermeister sowie die Landräte als Sonderfachaufsichtsbehörden übersandte. In diesem Schreiben ist in erfreulicher Klarheit zur einfachen Melderegisterauskunft gem. § 32 Abs. 1 BbgMeldeG u. a. unter Verweis auf Rahmen und Umfang der einfachen Melderegister folgendes ausgeführt:

- In der Regel sollte die Auskunft schriftlich erteilt werden,

- nur in Ausnahmefällen kann auch mündliche bzw. fernmündliche Auskunft gegeben werden; diese sollte dann aber aktenkundig gemacht werden,

- bei fernmündlichen Anfragen empfiehlt es sich, sich in geeigneter Weise von der Identität des Antragstellers (z. B. durch Rückruf) zu überzeugen.

3.1.1.6 Meldedaten auf CD-ROM für Adressenverzeichnisse

Ein bundesweites Problem stellt die Frage dar, ob Meldedaten auf CD-ROM übernommen und entsprechend ihrer Verwendung in Adreßbüchern oder ähnlichen Nachschlagewerken vertrieben werden dürfen (vgl. hierzu auch unter 1.4.5).

Nach § 33 Abs. 3 BbgMeldeG dürfen Meldebehörden Adreßbuchverlagen Auskunft erteilen

über Vor- und Familiennamen, akademische Grade und gegenwärtige Anschriften sämtlicher Einwohner, die das 18. Lebensjahr vollendet haben, sofern diese einer solchen Weitergabe nicht widersprochen haben.

Zwar ist - anders als in anderen Bundesländern - diese Übermittlungsbefugnis in Brandenburg nicht unmittelbar an den Zweck der Verwendung zur Herausgabe von Adreßbüchern oder ähnlichen Nachschlagewerken gebunden, jedoch ist der Bezeichnung der Empfänger "Adreßbuchverlage" zu entnehmen, daß der Gesetzgeber zunächst nur an eine Verwendung der Daten in Buchform dachte. Dies ist von den Bürgern auch nur insoweit für ihre Entscheidung, eventuell vom Widerspruchsrecht Gebrauch zu machen, nachvollziehbar.

Der qualitative Unterschied der Herausgabe von Daten auf CD-ROM zu einer listenmäßigen Auskunft besteht aber darin, daß die Daten mit entsprechender Hard- und Software mit anderen Daten und Datensammlungen zusammengeführt und jederzeit nach nicht überschaubaren Kriterien umsortiert und ausgewertet werden können. Dies ist im Lichte des Rechts auf informationelle Selbstbestimmung jedoch ohne eine klare rechtliche Regelung, die auch für diesen Verwendungszweck ein spezielles Widerspruchsrecht vorsehen müßte, nicht möglich. In ersten Gesprächen hierzu hat mir das MI signalisiert, daß dies im Zusammenhang mit der vorgesehenen Novellierung des BbgMeldeG berücksichtigt werden solle.

Ungeachtet dessen kann nicht ausgeschlossen werden, daß nach derzeitiger Rechtslage zunächst ordnungsgemäß übermittelte Daten im Nachhinein aus Adreßbüchern, Telefonbüchern u. a. durch "Einscannen" digitalisiert und anschließend kommerziell genutzt werden. Hiergegen können sich die Einwohner in Brandenburg allerdings schon jetzt schützen, indem sie gem. § 33 Abs. 3 Satz 2 BbgMeldeG bei ihrer Meldestelle bereits der Weitergabe ihrer Daten an Adreßbuchverlage widersprechen.

Ein besonderes Gefahrenpotential besteht darin, daß nicht nur mittels der direkt auf CD-ROM weitergegebenen Daten, sondern auch durch eine Zusammenführung aller in der o. g. Weise digitalisierten Meldedaten unerlaubt ein bundesweites bzw. parallele regionale Melderegister aufgebaut werden können. Hier sind die Gesetzgeber der Länder aufgerufen, in den jeweiligen Meldegesetzen angemessene Nutzungsbeschränkungen zu verankern.

3.2 Polizei/Verfassungsschutz

3.2.1 Stellungnahme zu Gesetzen/Errichtungsanordnungen

3.2.1.1 Brandenburgisches Polizeigesetz

Mit der im Berichtszeitraum abgeschlossenen Novellierung des brandenburgischen Polizeirechts[26] ist das noch von der letzten Volkskammer der ehemaligen DDR im Herbst 1990 verabschiedete Polizeigesetz[27], das das Land Brandenburg (wie die anderen neuen Bundesländer) mit einem Vorschaltgesetz[28] übernommen hatte, außer Kraft getreten. Länger als in den anderen neuen Bundesländern - und mit positivem Ergebnis - bildete es die Basis für die Um- und Neugestaltung der Landespolizei, war Rechtsgrundlage für polizeiliches und ordnungsbehördliches Handeln in einer offenen, demokratisch verfaßten Gesellschaft.

---

[26] Gesetz zur Neuordnung des Polizeirechts im Land Brandenburg vom 19. März 1996, GVBl. I S. 73

[27] Gesetz über die Aufgaben und Befugnisse der Polizei vom 13. September 1990, DDR-GBl. I S. 1489

[28] Vorschaltgesetz zum Polizeigesetz des Landes Brandenburg (VGPolGBbg) vom 11. Dezember 1991, GVBl. S. 636

Ungeachtet einiger durchaus als liberal zu bezeichnender Regelungen in Einzelbereichen, wie z. B. die Festlegung einjähriger Prüffristen für Datenspeicherung oder die Kennzeichnungspflicht für Polizeibedienstete, war es jedoch ein "modernes" Gesetz mit weitreichenden Eingriffsbefugnissen nicht nur gegen Störer oder Tatverdächtige, sondern gegen jedermann.

Auch die Neufassung ist ein solches "modernes" Gesetz, indem es zur vorbeugenden Bekämpfung von Straftaten dieselben Eingriffe in die Persönlichkeitsrechte nicht nur verdächtiger, sondern auch unverdächtiger Bürger vorsieht. Die polizeilichen Befugnisse erstrecken sich nicht nur auf den Kreis der Störer (also derjenigen Personen, die für die Gefahrenlage verantwortlich sind), sondern auch auf Nicht-Störer und sogenannte "andere Personen". Der rechtsstaatliche Grundsatz, daß der gesetzestreue Bürger das Recht hat, vom Staat in Ruhe gelassen zu werden, scheint im Bereich des Polizeirechts seine Gültigkeit verloren zu haben.

Viele Befugnisse für weitreichende Eingriffe in das Recht auf informationelle Selbstbestimmung sind mit dem Begriff "Straftat von erheblicher Bedeutung" verknüpft. Seine Definition in § 10 Abs. 3 Brandenburgisches Polizeigesetz (BbgPolG)[29] ist daher der gesetzliche Dreh- und Angelpunkt der besonderen Ermittlungsinstrumente.

Die in den §§ 31 - 36 BbgPolG geregelten - besonders eingriffsintensiven - Befugnisse der verdeckten Datenerhebung sowie die Eingriffsbefugnisse gegen Nicht-Störer setzen mit Ausnahme von § 33 Abs. 3 BbgPolG (der große Lauschangriff, siehe unten) eine Straftat von erheblicher Bedeutung in der Definition des § 10 Abs. 3 BbgPolG voraus. Diese legt fest, daß alle Verbrechen sowie Vergehen gem. § 100 a StPO einer Straftat von erheblicher Bedeutung gleichkommen. Wenn die Strafwürdigkeit einer Störung der öffentlichen Sicherheit entscheidend sein soll, um die besonders eingriffsintensiven Befugnisse zu begrenzen, ist der Rückgriff auf das Strafgesetzbuch die logisch konsequente Lösung. Sie ist jedenfalls normenklarer als vom Strafgesetzbuch losgelöste Definitionsversuche anderer Polizeigesetze und insofern eine datenschutzrechtliche Verbesserung. Dies gilt jedoch nur, soweit mit dem Definitionskatalog in § 10 Abs. 3 BbgPolG überhaupt eine Eingrenzung versucht wird. Gegen die Norm als solche ergeben sich wegen ihrer Ausdehnung datenschutzrechtliche Bedenken.

Ursprünglich wurden die Instrumente zur verdeckten Datenerhebung damit begründet, daß sie als Ausnahmeregelungen für die Fälle von besonders schwerer Kriminalität bzw. für besondere Gefahrenlagen erforderlich seien. Wenn nunmehr aber alle Verbrechen sowie Vergehen (wenn auch eingeschränkt auf die in § 100 a StPO aufgeführten Straftaten) unter den Begriff "Straftat von erheblicher Bedeutung" fallen sollen, kehrt sich das ursprüngliche Regel-Ausnahme-Verhältnis um. Die Aufklärung und Verfolgung von Verbrechen, d. h. von mehr oder minder schweren Straftaten, gehört zur alltäglichen Arbeit der Polizei. Eine Begriffbestimmung, die jede rechtswidrige Tat, die im Mindestmaß mit einer Freiheitsstrafe von einem Jahr belegt ist (so die Definition eines Verbrechens in § 12 StGB), in den Rang einer Straftat von erheblicher Bedeutung erhebt, macht den Einsatz grundrechtlich gravierender Eingriffsbefugnisse rechtlich zum Regelfall. Dies verletzt das Verfassungsgebot der Verhältnismäßigkeit. Eine gesetzliche Regelung, die ihre Schranken erst in der verfassungsrechtlich gebotenen Beachtung des Verhältnismäßigkeitsgrundsatzes als der letzten Rechtsstaatsgarantie findet, wird den Vorgaben des Bundesverfassungsgerichts im Volkszählungsurteil nicht gerecht. Der Gesetzgeber sollte gesetzliche Regelungen nicht darauf abstellen, daß die Behörde die Befugnisse in der alltäglichen Aufgabenerfüllung schon sparsam und verantwortungsbewußt anwenden werde. Vielmehr sollten die gesetzlichen Regelungen so beschaffen sein, daß sich aus ihnen die zur

---

[29] Art. 1 d. Gesetzes zur Neuordnung des Polizeirechts im Land Brandenburg vom 19. März 1996, GVBl. I S. 73

Aufgabenerfüllung zulässige Anwendung der Befugnisse ergibt.

- Personalienüberprüfung als Standard - oder Ausnahmebefugnis

Beispielshaft soll das oben Gesagte an § 12 BbgPolG verdeutlicht werden, der neben der Standardregelung zur Identitätsfeststellung auch die Befugnis zu verdachts- und/oder ereignislosen Personalienüberprüfungen an kriminogenen Orten (§ 12 Abs. 1 Ziff. 2 und 3 BbgPolG) und an Kontrollstellen (§ 12 Abs. 1 Ziff. 4 BbgPolG) enthält.

Die Personalienüberprüfung als Standardmaßnahme polizeilichen Handelns wird durch eine, für alle Beteiligten erkennbare, Störung der öffentlichen Sicherheit ausgelöst und richtet sich nur gegen diesen Personenkreis. An einem Ort jedoch, von dem die Polizei vermutet, daß dort Personen "Straftaten von erheblicher Bedeutung" gem. § 10 Abs. 3 BbgPolG verabreden, vorbereiten oder verüben, muß sich im Kontrollfall jeder ausweisen. Für die Kontrollmaßnahme sind nicht mehr das Individuum und ihm vermutlich zuordenbare Handlungen entscheidend, sondern einzig der nach polizeilicher Einschätzung kriminalitätsbehaftete Ort. Die Identitätsfeststellung wird voraussetzungslos möglich. Ohne daß ihm die polizeiliche Einschätzung des Ortes bekannt sein muß und ohne eigenes Zutun sowie ohne erkennbaren Anlaß nimmt die Vorschrift auch den gesetzestreuen Bürger in die Pflicht. Damit ist der verfassungswidrige Zugriff auf jedermann eröffnet. Da der Rechtsgrundlage selbst die erforderlichen Schranken fehlen, wird ein verfassungswidriger Mißbrauch erst durch den Rückgriff des Anwenders, also der Polizei, auf das Verfassungsgebot der Verhältnismäßigkeit verhindert.

- Kontrollstellen und weitere Eingriffe in das Grundrecht auf Versammlungsfreiheit

Verfassungsrechtlich bedenklich sind auch die Eingriffe in das Grundrecht auf Versammlungsfreiheit (Art. 8 Grundgesetz), die verschiedene Vorschriften des Brandenburgischen Polizeigesetzes ermöglichen. Neben den o. g. Kontrollstellen (§ 12 Abs. 1 Ziff. 4 BbgPolG) sind dies die Regelungen zum Gewahrsam (§ 17 Abs. 1 Ziff. 2 BbgPolG) und Unterbindungsgewahrsam (§ 20 Abs. 1 Ziff. 3 BbgPolG).

In § 12 Abs. 1 Ziff. 4 BbgPolG ist im Voraussetzungskatalog für Kontrollstellen auch § 27 Versammlungsgesetz (VersammlG)[30] aufgeführt. Damit sollen Kontrollstellen im Zusammenhang mit Demonstrationen auf eine gesetzliche Grundlage gestellt werden. Durch die Befugnis zur verdachtsunabhängigen Kontrolle kann an solchen Stellen die Identität aller potentiellen Teilnehmer einer Demonstration festgestellt werden.

Grundsätzlich hat jeder das Recht, an einer Versammlung oder Demonstration ohne staatlichen Eingriff (Art. 8 Abs. 1 Grundgesetz) teilzunehmen. Einschränkungen dieses Rechts (Art. 8 Abs. 2 Grundgesetz) sind im Versammlungsgesetz geregelt. Erst wenn gegen Auflagen gem. § 15 Abs. 1 VersammlG verstoßen wird oder bei Verdacht von Störungen (§ 3 VersammlG) kann die Polizei eingreifen. Eine Befugnis zur verdachtsunabhängigen Kontrolle ist nicht vorgesehen.

Das Versammlungsrecht fällt unter Bundeskompetenz. Der Bundesgesetzgeber hat es abschließend im Versammlungsgesetz ausgefüllt. Gerade die im Brandenburgischen Polizeigesetz aufgeführten Regelungsbereiche (§§ 26 - 28 VersammlG) wurden erst 1989 durch den Bundesgesetzgeber präzisiert und geändert. Es stellt sich also die Frage, ob überhaupt eine Gesetzgebungskompetenz des Landes gegeben ist und wo angesichts der Regelungen im Versammlungsgesetz sowie einschlägiger Vorschriften des Strafgesetzbuches überhaupt noch Raum für Präventivmaßnahmen nach dem Polizeirecht gem. § 12 Abs. 1 Ziff. 4, § 17 Abs. 1 Ziff. 2 und § 20 Abs. 1 Ziff. 3 BbgPolG bleibt.

---

30 BGBl. III, 2180-4

- Großer Lauschangriff

Besonders schwere verfassungsrechtliche Bedenken richten sich gegen den großen Lauschangriff, den Brandenburg als viertes Bundesland - und damit auch abweichend von bundesgesetzlichen Regelungen - mit seinem Polizeigesetz ermöglicht.

Bei dem großen Lauschangriff handelt es sich um einen Grundrechtseingriff von hoher Intensität, der über die Telefonüberwachung noch hinausgeht, da der Bürger beim Telefonieren aufgrund allgemeiner Lebenserfahrung die Möglichkeit in Betracht ziehen muß, abgehört zu werden. Er kann sich darauf einstellen und ggf. Vorkehrungen dagegen treffen. Das mit dem großen Lauschangriff verbundene Eindringen in die Privatsphäre geht auch weiter als ein Informationseingriff durch einen verdeckten Ermittler. In Anwesenheit einer anderen Person errichtet jeder Mensch Schranken, die er fallen läßt, wenn er allein und unbeobachtet ist.

Die Persönlichkeitsrechte des Grundgesetzes garantieren jedem Menschen einen absolut geschützten Kernbereich privater Lebensgestaltung, in den der Staat selbst dann nicht eingreifen darf, wenn ein überwiegendes Allgemeininteresse vorliegt. Diese Privatsphäre, die sich in der Wohnung materialisieren dürfte, wird in Artikel 7 und 15 Verfassung des Landes Brandenburg (BbgVerf)[31] sowie in Artikel 1 und 13 Grundgesetz (GG) in Verbindung mit der Wesensgehaltsgarantie (Art. 5 Abs. 2 BbgVerf bzw. Art. 19 Abs. 2 GG) grundrechtlich geschützt.

Ein heimliches Belauschen oder Beobachten eines Menschen in seiner Privatsphäre ist nur dann hinnehmbar, wenn es (z. B. im Fall einer Geiselnahme in einer Wohnung) unerläßlich ist, um im konkreten Einzelfall Leib, Leben oder Freiheit einer Person zu schützen (§ 33 Abs. 3 Ziff. 1 BbgPolG). Die Norm geht jedoch in § 33 Abs. 3 Ziff. 2 BbgPolG weit darüber hinaus. Sie befugt die brandenburgische Polizei zu einem großen Lauschangriff immer dann, wenn Tatsachen die Annahme rechtfertigen, daß bestimmte - in einem Katalog aufgeführte - Straftaten organisiert begangen werden sollen und die vorbeugende Bekämpfung dieser Straftaten sonst aussichtslos oder wesentlich erschwert wäre. Der Katalog umfaßt neben schweren Straftaten gegen die körperliche Unversehrtheit (wie z. B. Mord, Totschlag oder Völkermord) auch Staatsschutzdelikte sowie Verstöße gegen das Waffengesetz. Hier handelt es sich jedoch um eine Präventivmaßnahme der Polizei in solchen Fällen, in denen noch nicht einmal der Anfangsverdacht einer Straftat vorliegt. Schon im Vorfeld, noch ehe Tatsachen den Verdacht auslösen, daß jemand eine im Katalog aufgeführte Straftat zusammen mit anderen Personen plant, kann die Polizei nach Genehmigung durch einen Richter (§ 33 Abs. 4 BbgPolG) die Betroffenen in ihrer Wohnung heimlich beobachten und belauschen. Dies kann auch den unverdächtigen, gesetzestreuen Bürger treffen, der sich keiner Verbindung zu solchen Straftaten bewußt ist. Für den einzelnen wird nicht absehbar, wann und ob er Ziel eines großen Lauschangriffs werden kann. Es verletzt die Würde des einzelnen, wenn er ständig, ohne daß äußere Umstände ihn darauf hinweisen, befürchten muß, in seiner Wohnung ausgeforscht zu werden.

Im Strafverfahren hat der Anfangsverdacht eine besondere rechtsstaatliche Schwellenfunktion. Zwangsmaßnahmen dürfen erst eingeleitet werden, wenn ein Anfangsverdacht festgestellt worden ist. Dies gilt auch für die in der Strafprozeßordnung vorgesehenen heimlichen Erhebungsmethoden wie Observation und Abhören (der große Lauschangriff ist nicht darunter). Im Präventivbereich ist die Schwelle für polizeiliche Informationseingriffe bei den Befugnissen für die besonderen Ermittlungsmethoden einschließlich großer Lauschangriff sehr viel niedriger.

In der Öffentlichkeit wird dies mit den Gefahren der organisierten Kriminalität begründet.

---

[31] vom 20. August 1992, GVBl. I S. 298

Die gerade für die Bekämpfung der organisierten Kriminalität vorgesehenen Instrumente wie Observation, polizeiliche Beobachtung, Rasterfahndung, verdeckter Einsatz technischer Mittel zum Abhören und Aufzeichnung des gesprochenen Wortes und zur Anfertigung von Bildaufnahmen und Bildaufzeichnungen stehen den Strafverfolgungsbehörden einschließlich der Polizei schon seit Jahren zur Verfügung. Bisher fehlt es jedoch an einem Nachweis der Effizienz der in Rede stehenden Ermittlungsmethoden und -möglichkeiten. Erörterungen über die Gefahren, die der Allgemeinheit von der organisierten Kriminalität drohen, ersetzen weder die Begründung der Erforderlichkeit noch die Effektivitätsanalyse. Von den zuständigen Stellen muß erwartet werden, daß sie detailliert darlegen, in welchen konkreten Situationen derartige Befugnisse zur Gefahrenabwehr oder vorbeugenden Straftatenbekämpfung unerläßlich sind und inwieweit sie bisher zur Aufklärung bzw. zur Verhinderung von Straftaten beigetragen haben.

Da sich im Verlauf des Gesetzgebungsverfahrens herausstellte, daß grundlegende Änderungen nicht zu erwarten seien, habe ich Verfahrensregelungen vorgeschlagen, die besondere Begleitmaßnahmen zum Schutz des Rechts auf informationelle Selbstbestimmung zum Inhalt haben wie z. B.:

- Erweiterung der Berichtspflicht: Die in § 33 Abs. 9 geregelte Berichtspflicht an den Landtag sollte auf alle Datenerhebungsmaßnahmen mit besonderen Aufklärungsinstrumenten (§§ 33 - 36 und § 46 BbgPolG) erweitert und inhaltlich aussagefähiger gestaltet werden.

- Nachermittlungsverpflichtung: Um sicherzustellen, daß personenbezogene Daten nicht länger als erforderlich aufbewahrt werden, sollte die Polizei verpflichtet werden, bei den Justizbehörden den Ausgang des Straf- bzw. Gerichtsverfahrens gegen einen Betroffenen in Erfahrung zu bringen, ehe die endgültige Speicherungsdauer seiner personenbezogenen Daten festgelegt wird (s. unter 3.3.5 und 4.3).

- Protokollierungsverpflichtung: Um sicherzustellen, daß eine angemessene datenschutzrechtliche Kontrolle der polizeilichen Informationssammlungen durchgeführt werden kann, aber auch, um unzulässige Datenzugriffe zu verhindern, sollte eine automatisierte Protokollierung der Datenzugriffe im Gesetz festgeschrieben werden.

Meine Vorschläge, die im übrigen die polizeilichen Befugnisse nicht eingeschränkt hätten, wurden jedoch nicht aufgenommen. Zusammenfassend ist festzustellen, daß der brandenburgische Gesetzgeber bei der Novellierung des Polizeigesetzes Datenschutzrechte der Bürger und polizeiliche Eingriffsbefugnisse nicht angemessen gewichtet hat.

3.2.1.2 Errichtungsanordnung zum DV-unterstützten Vorgangstagebuch der Polizeipräsidien und des Landeskriminalamts

In meinem 2. Tätigkeitsbericht[32] hatte ich die im Jahr 1993 betriebene Version des Automatisierten Vorgangstagebuchs (AVA) problematisiert. Das MI hatte damals darauf hingewiesen, daß an einer Nachfolgeanwendung für diese Datei gearbeitet werde. Planung und Realisierung der neugestalteten Datei "Anzeigentagebuch" sind nunmehr abgeschlossen. Die neue Anwendung "DV-unterstütztes Vorgangstagebuch" wird auf einem deutlich höheren technischen Niveau betrieben als ihre Vorgängerin AVA. Zur Führung des Gesamtbestandes steht in jedem Polizeipräsidium ein UNIX-Server zur Verfügung. In der letzten Ausbaustufe, die noch nicht in allen Polizeipräsidien erreicht ist, greift der zuständige Sachbearbeiter on-line auf den in seinem Polizeipräsidium geführten Datenbestand zu. Ein landesweiter Gesamtbestand aller Vorgangsdaten ist nicht vorgesehen. Das MI hat mir den Entwurf einer Errichtungsanordnung zur Stellungnahme übersandt. Ich habe mich

---

[32] s. unter 3.6.2.3

insbesondere zu den technischen und organisatorischen Maßnahmen gem. § 10 Abs. 2 Bbg DSG geäußert, die nach der Errichtungsanordnung von den jeweiligen Polizeipräsidien bzw. dem Landeskriminalamt entsprechend ihren örtlichen Gegebenheiten geregelt werden.

In § 10 Abs. 1 Bbg DSG ist festgelegt, daß die technischen und organisatorischen Maßnahmen geeignet sein müssen, um die Ausführung der gesetzlichen Vorschriften sicherzustellen. Der Verwaltungsaufwand muß in einem angemessenen Verhältnis zu der Schutzwürdigkeit der personenbezogenen Daten stehen. Bei den in der Datei "DV-unterstütztes Vorgangstagebuch" eingestellten Daten handelt es sich zweifelslos um äußerst sensible Daten aus unterschiedlichen Lebenssachverhalten der Betroffenen, die eine hohe Schutzstufe erfordern. Bei den in § 10 Abs. 2 Ziff. 1 - 10 Bbg DSG aufgeführten Kontrollmaßnahmen ist demgemäß ein hoher technischer und organisatorischer Standard vorzusehen, zu deren wesentlichen Bestandteilen die automatisierte Protokollierung und - bei Übermittlung der Daten in öffentlichen Netzen sowie per Datenfunkterminals - die Verschlüsselung gehören.

Es ist ebenfalls eine Protokollierung vorzusehen, die an den mit der Neuanwendung erreichten Stand der Technik angepaßt ist. Das bedeutet in der Regel eine automatisierte umfassende Protokollierung des Zugriffs auf die Datenbank. Eine manuelle Protokollierung der Datenzugriffe - wie bisher - ist nicht mehr hinzunehmen. Dies gilt nicht für alle Schritte der Datenverarbeitung. So ist beispielsweise die Übermittlungskontrolle (§ 10 Abs. 2 Ziff. 6 Bbg DSG) ausreichend sichergestellt, wenn der Sachbearbeiter manuell vermerkt, an wen er Daten übermittelt hat.

Ich habe das MI gebeten, mir mitzuteilen, welche Protokollierungs- und Verschlüsselungsmaßnahmen (ggf. Software-immanent) bei der Datei vorgesehen sind. Eine Antwort stand bei Redaktionsschluß noch aus.

3.2.2 Kontrollstellen und Platzverweise anläßlich der Gedenkfeiern zum 50. Jahrestag der Befreiung der Konzentrationslager in Brandenburg

Mit über 100 Veranstaltungen im April 1995 - verteilt über das ganze Land Brandenburg mit mehr als einer Million Teilnehmern - waren die Gedenkfeiern zum 50. Jahrestag der Befreiung der Konzentrationslager der größte Einsatz, den die brandenburgische Polizei bisher zu bewältigen hatte. Nicht nur die Vorbereitungen[33], die getroffen wurden, um einen ungestörten Ablauf der zentralen Veranstaltungen am 23. April 1995 auf dem Gelände der ehemaligen Konzentrationslager Sachsenhausen und Ravensbrück zu sichern, sondern auch die polizeilichen Maßnahmen vor Ort, veranlaßten mehrere Betroffene, sich mit Eingaben an meine Behörde zu wenden. Auf die Prüfung der mit den Einsätzen im Zusammenhang stehenden Datenverarbeitung im Landeskriminalamt Brandenburg (LKA) und im Polizeipräsidium Oranienburg wird unter 3.2.2.1 bis 3.2.2.4 eingegangen.

3.2.2.1 Rechtsgrundlage der Polizeieinsätze

Rechtsgrundlage der gesamten polizeilichen Maßnahmen einschließlich der Vorbereitungen war das Brandenburgische Polizeigesetz. Unmittelbar auf dem Gelände der ehemaligen Konzentrationslager hat das von der Stiftung Brandenburgische Gedenkstätten beauftragte Wachschutzunternehmen ebenfalls Personenkontrollen vorgenommen.

---

[33] s. 3.Tätigkeitsbericht unter 3.5.5.2

3.2.2.2 Nachrichtensammelstelle

Zur Vorbereitung der polizeilichen Maßnahmen richtete das LKA eine Nachrichtensammelstelle (NASISTE) ein, die die von den Polizeibehörden der anderen Bundeländer eingehenden Meldungen über geplante Störungen sammelte, auswertete und den für die örtlichen Einsätze zuständigen Polizeipräsidien zur Verfügung stellte. Rechtsgrundlage für die Datenerhebung und -übermittlung waren § 33 a Abs. 1 Ziff. 1 und 4 und § 43 Abs. 1 i. V. m. § 1 Abs. 1 VGPolGBbg[34]. Danach kann die Polizei zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung personenbezogene Daten über diejenigen Personen erheben, die eine Gefahr verursachen sowie über andere Personen, wenn sie mit den Erstgenannten in Kontakt stehen und dies zur Gefahrenabwehr oder zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. Soweit zur Erfüllung polizeilicher Aufgaben nötig, dürfen die erhobenen personenbezogenen Daten an andere Polizeidienststellen übermittelt werden.

3.2.2.3 Kontrollstellen und Platzverweise

Die Veranstaltungorte Gedenkstätte Sachsenhausen und Gedenkstätte Ravensbrück waren am 23. April 1995 für den Pkw-Verkehr weiträumig abgesperrt. Ein Kreis von Kontrollstellen gem. § 15 Abs. 1 Ziff. 4 VGPolGBbg sollte nicht nur die Absperrung sichern, sondern darüber hinaus waren die dort eingesetzten Polizeibeamten gem. § 15 VGPolGBbg befugt, die Personalien der Passanten festzustellen, mit polizeilichen Datenbeständen abzugleichen und die Betroffenen ggf. zurückzuweisen, wenn sich beim Passieren oder bei der Personalienfeststellung Hinweise ergaben, die den Verdacht nahelegten, daß sie die Veranstaltung stören wollten. Dazu stand neben dem INPOL-Personenfahndungsbestand auch der besondere Personenfahndungsbestand zur Verfügung. Letzterer wird vom Bundeskriminalamt in den INPOL-Personenfahndungsbestand eingespielt und dem jeweiligen Bundesland bei großen Veranstaltungen mit politischem Bezug zum Datenabgleich freigegeben. In ihm sind Personen registriert, die wegen des Tatbestandes Landfriedensbruch u. ä. Delikte gerichtlich belangt worden sind.

Die NASISTE hatte den Kontrollstellen u. a. die Kennzeichen von vier Fahrzeugen übermittelt. Diese waren anzuhalten, die Personalien der Insassen festzustellen - die Betroffenen ggf. gem. § 16 Abs. 2 Ziff. 1 VGPolGBbg erkennungsdienstlich zu behandeln - und ihnen Platzverweise gem. § 19 VGPolGBbg zu erteilen.

3.2.2.4 Ergebnis der Prüfung

Die Prüfung der Datenverarbeitung in LKA und im Polizeipräsidium Oranienburg ergab, daß

- die an den Kontrollstellen erhobenen Daten zum größten Teil (so z. B. alle erkennungsdienstlichen Unterlagen) bereits vernichtet waren,

- die Einsatzberichte (einschl. personenbezogener Daten, soweit dort noch registriert) zur Vorgangsverwaltung bzw. zur befristeten Dokumentation polizeilichen Handelns (gem. § 42 VGPolGBbg) bis zum vorgesehenen Löschungstermin im April 1996 aufbewahrt werden und

- weder LKA noch Polizeipräsidium Oranienburg personenbezogene Daten, die im Zusammenhang mit den polizeilichen Maßnahmen erhoben worden sind, an Polizeidienststellen oder Verfassungsschutzbehörden übermittelt haben.

Insgesamt hat die Prüfung keine datenschutzrechtlichen Mängel ergeben. Da die

---

[34] vom 11. Dezember 1991, GVBl. I S. 636

Maßnahmen und die in ihrem Zusammenhang erfolgte Erhebung und Verwendung personenbezogener Daten ausschließlich der Gefahrenabwehr dienten, waren auch die zwischenzeitlich bereits erfolgten Löschungen datenschutzrechtlich nicht zu beanstanden. Unbefriedigend blieb dieser Sachverhalt nur insoweit, als sich die Rechtmäßigkeit der Grundrechtseingriffe im Einzelfall nicht mehr überprüfen ließ.

Im übrigen stellte sich heraus, daß die von der Koordinierungsstelle[35] erhobenen und zur Sicherheitsüberprüfung an die NASISTE übermittelten personenbezogenen Daten der zur Betreuung der Gäste eingesetzten Personen ebenfalls bereits vernichtet waren.

3.2.3 Polizeiliches Informations- und Kommunikationssystem Brandenburg/Berlin

Im vergangenen Jahr informierte mich mein Berliner Kollege über die Planungen zu einem gemeinsamen polizeilichen Informations- und Kommunikationssystem (POLIKS BB/BR) und stellte mir den Entwurf einer Verordnung der Berliner Polizei über den automatisierten Datenabruf aus dem polizeilichen Informationssystem für Verbrechensbekämpfung Berlin (ISVB) durch die Brandenburger Polizei zur Verfügung. Die Verordnung entsprach nicht dem brandenburgischen Polizeirecht und enthielt darüber hinaus erstaunlich weitreichende Befugnisse für den behördeninternen Datenschutzbeauftragten der Berliner Polizei.

Eine Rückfrage beim MI ergab, daß dem Ministerium der Verordnungsentwurf nicht bekannt war. Zu dem gemeinsamen Informations- und Kommunikationssystem teilte das Ministerium mir mit, daß die Berliner und die Brandenburger Polizei ein inhaltlich und technisch kompatibles Informations- und Kommunikationssystem zur Aufgabenerfüllung entwickelten. Die Planungen sehen zunächst ein Verbundsystem zweier eigenständiger Landessysteme vor. Nach der evtl. erfolgenden Fusion muß POLIKS BB/BR aber auch als gemeinsames Landessystem einsetzbar sein. Auf der Grundlage einer Verwaltungsvereinbarung zwischen den beiden Ländern ist ein gemeinsames Soll-Konzept erarbeitet und eine Voruntersuchung in Auftrag gegeben worden, die im September 1994 abgeschlossen wurde. Das Ministerium hat zugesagt, mich über die Entwicklung von POLIKS BB/BR unaufgefordert in regelmäßigen Abständen zu unterrichten.

3.2.4 Auskunftsbegehren

Das Datenscheckheft[36] hat die Wißbegierde der Brandenburger, ob und was Polizei und Verfassungsschutz über sie gesammelt haben, spürbar und nachhaltig angeregt. So ist im Verlauf des Berichtszeitraumes die Anzahl der Auskunftsbegehren und damit zusammenhängender Eingaben auch in meiner Behörde deutlich angestiegen. Nach dem ersten Schrecken über die auf sie einstürzenden Bürgeransinnen haben die Behörden sich darauf eingestellt und arbeiten die verwaltungs- und zeitaufwendigen Auskunftserteilungen routiniert ab.

Aufgrund mehrerer Eingaben habe ich den Verwaltungsablauf der Auskunftserteilung in zwei Polizeipräsidien und im Landeskriminalamt geprüft.

3.2.4.1 Rechtsgrundlage

Rechtsgrundlage der Auskunftserteilung ist § 49 VGPolGBbg[37]. Die Vorschrift legt fest, daß dem Betroffenen Auskunft über die zu seiner Person gespeicherten Daten zu erteilen ist.

---

35 s. 3. Tätigkeitsbericht unter 3.5.5.2

36 aus der Informationsreihe "Der Landesbeauftragte für den Datenschutz Brandenburg informiert", 1. Aufl. Dez. 1994

37 vom 11. Dezember 1991, GVBl. S. 636

Dabei ist die Art oder der Ort der Datenspeicherung unerheblich. Das Auskunftsrecht bezieht sich auf alle bei der Polizei geführten Unterlagen. In Ermittlungsfällen, die bereits an die Staatsanwaltschaft abgegeben worden sind, muß gem. § 49 Abs. 5 VGPolGBbg die Einwilligung der Staatsanwaltschaft bzw. die Einwilligung des Gerichts, falls das Verfahren bereits bei Gericht anhängig ist, eingeholt werden. Die Auskunft wird jedoch auch in diesen Fällen von der Polizei erteilt. Sie ist verantwortlich für Umfang und Richtigkeit des Bescheids. Gem. § 49 Abs. 3 VGPolGBbg kann die Auskunft verweigert werden, wenn die Rechte Dritter oder das öffentliche Interesse an der Geheimhaltung das Auskunftsrecht des Antragstellers überwiegen. Die Entscheidung darüber treffen die behördlichen Datenschutzbeauftragten.

3.2.4.2 Verfahren

Der Eingang des Auskunftsbegehrens ist entscheidend für den Zeitraum, über den Auskunft erteilt wird. Speicherungen, die erst während der Antragsbearbeitung anfallen, werden nicht mehr berücksichtigt.

Bei den geprüften Behörden ist die gesamte Auskunftserteilung den behördeninternen Datenschutzbeauftragten übertragen. Damit ist sichergestellt, daß Anträge und weitere Verwaltungsvorgänge nur dort veraktet werden. Es wäre datenschutzrechtlich nicht hinnehmbar, wenn solche Daten zur Kriminalakte bzw. zu den Ermittlungsakten genommen würden.

Die Datenschutzbeauftragten fragen bei allen Abteilungen und Kommissariaten ihres Zuständigkeitsbereichs ab, ob dort personenbezogene Daten zum Antragsteller registriert sind. Die jeweiligen Organisationseinheiten sind verpflichtet, alle in ihrem Bereich geführten Dateien, Akten und sonstigen Unterlagen dahingehend zu prüfen und dem Datenschutzbeauftragten das Ergebnis mitzuteilen.

In bereits an die Staatsanwaltschaft abgegebenen Ermittlungsfällen holt der Datenschutzbeauftragte deren Einwilligung ein. Des weiteren prüft er, ob Geheimhaltungsgründe vorliegen und entscheidet über die Auskunftserteilung.

3.2.4.3 Ergebnis der Prüfungen

Als datenschutzrechtlich erfreulicher Sachverhalt hat sich herausgestellt, daß die Polizeibehörden dem Auskunftsrecht der Bürger insgesamt eine höhere Priorität einräumen als den (in manchen Einzelfällen ebenfalls vertretbaren) Geheimhaltungsinteressen der Ermittlungsbehörden. Dies gilt auch für die Staatsanwaltschaften, soweit sie im Einzelfall an der Auskunftserteilung beteiligt waren. Im Ergebnis wird damit einer deutlichen Mehrheit der anfragenden Bürger ein dem tatsächlichen Sachstand entsprechender Bescheid gegeben. Ich bin überzeugt, daß der gesamtgesellschaftliche Nutzen den Schaden, der durch eine eventuell zu Recht befürchtete "Ausforschung" entstehen könnte, bei weitem überwiegt.

Die durch die Auskunftsanträge bzw. Eingaben veranlaßte Erforderlichkeitsprüfung führte in mehreren Einzelfällen zur Löschung der personenbezogenen Daten in Landes- oder Bundesdateien sowie zur Vernichtung der Aktenvorgänge.

In zwei Fällen wurde der Tatvorwurf der Bildung einer terroristischen Vereinigung (§ 129 a StGB) nicht mehr aufrechterhalten. Die Überprüfung hatte ergeben, daß die den Petenten zur Last gelegte Tatbeteiligung für den hier in Frage kommenden Tatbestand der Werbung für eine terroristische Vereinigung nicht ausreichte. Bei dem nunmehr erhobenen Tatvorwurf der Billigung von Straftaten (§ 140 StGB) sind so gravierende Eingriffe in die Persönlichkeitsrechte der Betroffenen ausgeschlossen, wie sie bei Ermittlungen wegen § 129 a StGB möglich gewesen wären.

Insgesamt ist festzustellen, daß die Auskunftsbegehren der Bürger ein wichtiger Beitrag zur Durchsetzung des Rechts auf informationelle Selbstbestimmung sind. Sie verursachen zwar einerseits einen beträchtlichen Verwaltungsaufwand, zwingen jedoch andererseits die Verwaltungen immer wieder, die Datenbestände auf ihre Erforderlichkeit hin zu überprüfen und nicht mehr erforderliche Daten zu löschen.

Bei den Prüfungen stellte sich neben einigen geringfügigen Mängeln, deren Behebung die Polizeipräsidien bereits eingeleitet oder zugesagt haben, die Informationsbeziehung zwischen Polizei und Staatsanwaltschaft als Hauptproblem heraus (s. unter 3.2.1.1).

Für die Bürger war anhand des Auskunftsbescheids nicht nachvollziehbar, warum die Polizei sie weiterhin im Zusammenhang mit Tatvorwürfen speichert, wenn die zuständige Staatsanwaltschaft ihnen bereits mitgeteilt hatte, daß das Ermittlungsverfahren eingestellt worden sei. In der Mehrzahl der Eingaben hatten die Staatsanwaltschaften eine entsprechende Meldung an die Polizei unterlassen. In diesen Fällen habe ich mich an die zuständigen Staatswaltschaften gewandt und sie gebeten, die Polizei über die Verfahrenseinstellung sowie die Rechtsgrundlage zu informieren. Darüber hinaus habe ich dem hiesigen Justizministerium die datenschutzrechtliche Problematik des nicht durchgeführten Rückmeldeverfahrens dargelegt und es um Stellungnahme gebeten (s. unter 4.3). Eine Antwort lag bei Redaktionsschluß noch nicht vor.

3.2.5 Wie gelangen Informationen aus einem kriminalpolizeilichen Ermittlungsverfahren an einen Arbeitgeber ?

Ein Petent beschwerte sich, weil das Ordnungsamt des Landkreises seinem Arbeitgeber in einem Schreiben Sachverhalte aus einer kriminalpolizeilichen Ermittlungsakte mitgeteilt hatte. Die Prüfung bei den beteiligten Behörden ergab folgenden Sachverhalt:

In einem Ermittlungsverfahren benötigte eine Dienststelle der Kriminalpolizei Auskünfte eines kommunalen Ordnungsamtes. Unter dem weiten Mantel der Amtshilfe entwickelte sich die erforderliche und rechtlich zulässige Anfrage bei dem Ordnungsamt zu einer rechtlich nicht mehr zulässigen Übersendung von Kopien aus der Ermittlungsakte an das Ordnungsamt, das sie zur Akte nahm. Das kommunale Ordnungsamt seinerseits leitete die Akte samt Kopien im Zuge eines Bußgeldverfahrens wegen Gewerbeausübung ohne Genehmigung an den zuständigen Landkreis weiter. Letzterer teilte dem Arbeitgeber Sachverhalte aus den Kopien der kriminalpolizeilichen Ermittlungsakte mit. Das um Stellungnahme gebetene zuständige Polizeipräsidium hielt die Datenübermittlung für unzulässig. In seiner Stellungnahme führte es aus, daß Rechtsgrundlage für die Datenübermittlung der Kriminalpolizei an das Ordnungsamt das Gesetz über Ordnungwidrigkeiten (OWiG)[38] ist.

In § 53 OWiG sind die Aufgaben der Polizei geregelt. Sie hat nach pflichtgemäßem Ermessen Ordnungswidrigkeiten zu erforschen. Wenn, wie im vorliegenden Fall, zwischen einer Straftat und einer Ordnungswidrigkeit ein Zusammenhang besteht, kann nach § 52 Abs. 1 OWiG die Staatsanwaltschaft die Verfolgung der Ordnungswidrigkeit übernehmen. In diesem Fall können Datenübermittlungen nur mit Zustimmung der Staatsanwaltschaft erfolgen. Sie hat die Möglichkeit, das Verfahren im Zuge der Ermittlungen wieder an das zuständige Ordnungsamt abzugeben (§ 43 OWiG). Dies war hier geschehen. Auf Antrag an die Staatsanwaltschaft kann die zuständige Verwaltungsbehörde Einsicht in die staatsanwaltschaftliche Ermittlungsakte erhalten (§ 49 OWiG).

Das Ordnungsamt erhält also Informationen, die es gem. § 49 OWiG zur Aufgabenerfüllung benötigt, von der zuständigen Staatsanwaltschaft. Der direkte Übermittlungsweg von der

---

[38] i. d. Fass. vom 19. Februar 1987, BGBl. I S. 602

Kriminalpolizei an das Ordnungsamt ist jedoch unzulässig.

Für die Übermittlung der in Rede stehenden Informationen an den Arbeitgeber des Petenten gibt es keine bereichsspezifische Rechtsgrundlage, so daß das Brandenburgische Datenschutzgesetz heranzuziehen ist. Gem. § 16 Abs. 1 Buchst. a Bbg DSG dürfen personenbezogene Daten an Personen außerhalb des öffentlichen Bereichs übermittelt werden, wenn es zur rechtmäßigen Erfüllung der Aufgaben der übermittelnden Stelle erforderlich ist und die Zweckbindung gewahrt bleibt. Zur Zweckbindung legt § 13 Abs. 1 Bbg DSG fest, daß die Stelle, die die Daten ohne eigene Ermittlung erhalten hat, diese auch nur zu dem Zweck nutzen darf, für den sie erstmals gespeichert wurden. Erstspeicherungsstelle der in Rede stehenden Informationen war die Kriminalpolizei, die sie in einem kriminalpolizeilichem Ermittlungsverfahren - nicht jedoch zur Betreibung des ordnungsbehördlichen Verfahrens - gespeichert hatte, so daß die Voraussetzungen gem. § 16 Abs. 1 Buchst. a i. V. m. § 13 Abs. 1 Bbg DSG nicht erfüllt waren. Das ordnungsbehördliche Verfahren hätte auch ohne die Übermittlung dieser Informationen an den Arbeitgeber des Petenten betrieben werden können.

Die beteiligten Behörden haben sich der vom Polizeipräsidium und mir geteilten Rechtsauffassung angeschlossen und wollen diese beachten.

3.2.6 Verfassungsschutz

Im Berichtszeitraum stand die Bearbeitung problematischer Einzelfälle sowie grundsätzlicher Fragen, die sich durch die Prüfungen bei der Verfassungsschutzbehörde[39] ergeben hatten, im Mittelpunkt meiner Tätigkeit.

Zur Speicherung der Daten von Teilnehmern, die der Verfassungsschutzbehörde durch die von der Polizei übermittelten Festnahmelisten bekannt werden, hat die Verfassungsschutzbehörde zugesichert, solche Daten nur mit einer kurzen Speicherungsfrist zu erfassen. Es hatte sich allerdings schon bei den Prüfungen herausgestellt, daß die Festlegung von kurzen Speicherungsfristen ins Leere läuft, wenn keine regelmäßige Bestandspflege praktiziert wird. Die meisten der anläßlich der Prüfungen bemängelten Karteikarten sind unterdessen vernichtet worden.

Ungeachtet der datenschutzrechtlich befriedigenden Lösung der Einzelfälle bleibt die Übermittlung von Daten, die die Polizei im Rahmen der Gefahrenabwehr oder Strafverfolgung erhebt, an die Verfassungsschutzbehörde problematisch. § 14 Brandenburgisches Verfassungsschutzgesetz (BbgVerfSchG)[40] legt allen Landesbehörden eine sehr weitreichende Unterrichtungsverpflichtung an die Verfassungsschutzbehörde auf. Sie ist über alle Tatsachen einschließlich personenbezogener Daten zu unterrichten, die sicherheitsgefährdende oder Spionagetätigkeiten erkennen lassen oder die durch Gewalt (bzw. durch Vorbereitungshandlungen zu Gewalttätigkeiten) gegen Verfassungsgrundsätze gerichtet sind. Polizei und Staatsanwaltschaften müssen den Verfassungsschutz zusätzlich immer dann informieren, wenn ihnen Erkenntnisse über Bestrebungen vorliegen,

- die gegen die freiheitlich-demokratische Grundordnung,

- den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder

- eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziel haben, und wenn tatsächliche Anhaltspunkte bestehen, daß diese Information für die Erfüllung der Aufgaben der

---

39 s. 3. Tätigkeitsbericht unter 3.3.6.2

40 vom 5. April 1993, GVBl. I S. 7

Verfassungsschutzbehörde erforderlich sind (§ 14 Abs. 2 BbgVerfSchG).

Weiterhin ist die Verfassungsschutzbehörde selbst befugt, bei allen Behörden des Landes um Übermittlung von Informationen, die zur Erfüllung ihrer Aufgaben erforderlich sind, nachzusuchen. Seine Schranken findet der gesetzlich vorgeschriebene Informationsfluß an die Verfassungsschutzbehörde im Verfassungsgrundsatz der Verhältnismäßigkeit.

Die Prüfungen beim Verfassungsschutz haben ergeben, daß in der überwiegenden Mehrzahl der Fälle Betroffene aufgrund von Übermittlungen brandenburgischer Polizeidienststellen erstmalig erfaßt und über einen längeren Zeitraum gespeichert werden, ohne daß weitere (verfassungsschutzeigene) Erkenntnisse hinzukommen. Es trägt dem Verhältnismäßigkeitsgrundsatz nicht mehr Rechnung, wenn personenbezogene Daten immer dann an die Verfassungsschutzbehörde übermittelt werden, sobald das auslösende Ereignis einen politischen Hintergrund hat oder haben könnte. Anders als bei Übermittlungen auf Ersuchen der Verfassungsschutzbehörde gem. § 14 Abs. 2 BbgVerfSchG muß hier in jedem Einzelfall der Übermittlung geprüft werden, ob er einer Bestrebung der oben aufgeführten Art entspricht und ob bei der übermittelnden Behörde tatsächliche Anhaltspunkte dafür vorliegen, daß die zu übermittelnden Daten für die Aufgabenerfüllung der Verfassungsschutzbehörde erforderlich sind. Die Kriterien für die Verhältnismäßigkeitsprüfung sowie Einzelheiten des Übermittlungsverfahrens sollten in einem Erlaß für die brandenburgischen Polizeibehörden näher bestimmt werden.

Ich habe daher beim MI nachgefragt, ob es dazu bereits Überlegungen gibt. Gestützt auf die Ergebnisse der Prüfungen habe ich einige Eckpunkte aufgelistet, die in dem Erlaß festgelegt werden sollten. Dazu gehört u. a., daß

- die Erhebung personenbezogener Daten ausschließlich zur polizeilichen Aufgabenerfüllung erfolgt,

- vor der Übermittlung von Daten geprüft wird, ob tatsächliche Anhaltspunkte für die Verfassungsschutzrelevanz des Ereignisses vorliegen,

- nur die Daten derjenigen Personen an den Verfassungsschutz übermittelt werden, bei denen zumindest der Anfangsverdacht einer Straftat besteht, die auch verfassungsschutzrelevant ist.

Erste Entwürfe der "Richtlinien über die Zusammenarbeit der Polizei des Landes Brandenburg mit den Nachrichtendiensten" sind noch im innerministeriellen Abstimmungsverfahren.

3.2.6.1 Speicherung nicht verfassungsschutzrelevanter Personen in Sachakten

Bei der Prüfung von Sachakten habe ich festgestellt, daß dort Personen registriert sind, die - obwohl selbst nicht verfassungsschutzrelevant - zum engeren Umfeld einer solchen Person gehören. So fanden sich beispielsweise in einer Sachakte die personenbezogenen Daten eines Fahrzeughalters, der - im Gegensatz zum Fahrer - selbst keiner Bestrebung im Sinne des Verfassungsschutzgesetzes zuzurechnen ist. Da in diesen Fällen die Daten der Betroffenen für die Aufgabenerfüllung des Verfassungsschutzes nicht erforderlich sind, müssen sie gem. § 10 Abs. 2 BbgVerfSchG gelöscht werden. Ich habe angeregt, daß die Verfassungsschutzbehörde, um unnötigen Verwaltungsaufwand bei erneuter Befassung mit dem Vorgang zu vermeiden, in solchen Fällen die bereits erfolgte Personenfeststellung mit einem Kurzzeichen dokumentiert. Dadurch würde deutlich, daß eine Prüfung stattgefunden hat, ohne daß die Daten der Betroffenen registriert werden müssen.

Die Verfassungsschutzbehörde hat vorgeschlagen, den Sachakten ein Vorblatt einzufügen, das eine Verarbeitung personenbezogener Daten aus den Sachakten nur in einem genau

bestimmten Umfang zuläßt und sämtliche anderen personenbezogenen Informationen sperrt. Dieser Vorschlag kann jedoch die Verpflichtung zur Löschung nicht zur Aufgabenerfüllung erforderlicher Daten nicht aufheben und ist daher auf das oben angeführte Beispiel nicht anwendbar. Inwieweit er eine sachgerechte Lösung für andere Datenkategorien darstellt, bedarf noch der Erörterung. Für Verdachts- oder Prüffälle könnten solche Vorblätter zusammen mit der Vergabe von kurzen Prüffristen eine datenschutzrechtliche Verbesserung darstellen.

3.2.6.2 Auskunftsbegehren

Meine Broschüre "Datenscheckheft" (s. hierzu auch unter 3.2.4), von dem im übrigen die Verfassungsschutzbehörde dankenswerterweise einen größeren Posten zur Verteilung an die Bürger angefordert hatte, hat auch dort einen deutlichen Anstieg von Auskunftsersuchen ausgelöst.

Die Prüfung der Eingaben von Bürgern, die sich aufgrund des Auskunftsbescheids an mich gewandt hatten, ergab, daß die Verfassungsschutzbehörde von der in § 12 Abs. 2 BbgVerfSchG geregelten Befugnis, die Auskunft zu verweigern, bislang keinen Gebrauch gemacht hat. Bei den überprüften Fällen waren tatsächlich keine personenbezogenen Daten zu den Antragstellern beim Verfassungsschutz erfaßt. Im Ergebnis ist festzustellen, daß in der Mehrzahl der Fälle eine umfassende Auskunft erteilt wird.

3.3 Rückführung vietnamesischer Staatsbürger

Im Juli 1995 haben die Bundesrepublik Deutschland und die sozialistische Republik Vietnam ein Abkommen zur Rückübernahme von vietnamesischen Staatsangehörigen unterzeichnet. Die vietnamesische Regierung verpflichtet sich in diesem Abkommen, alle Staatsangehörigen zurückzunehmen, die sich ohne gültigen Aufenthaltstitel in Deutschland aufhalten.

Im Abkommen sowie im Protokoll zu dessen Durchführung ist das Verfahren der Rücknahme festgelegt. Von besonderer datenschutzrechtlicher Problematik ist ein umfänglicher Fragebogen, mit dem die Ausländerbehörden bei den betroffenen Vietnamesen Daten für die Maßnahme erheben und an die vietnamesischen Behörden übermitteln.

Nachdem das Abkommen im September 1995 in Kraft getreten ist, haben auch die brandenburgischen Behörden mit den Vorbereitungen zur Durchsetzung des Abkommens begonnen. Der Fragebogen veranlaßte die Brandenburgische Ausländerbeauftragte, mich um Stellungnahme zu den datenschutzrelevanten Fragen und Problemen zu bitten.

Die Ausländerbehörden erheben personenbezogene Daten beim Betroffenen und bei öffentlichen Stellen im Rahmen ihrer Aufgabe nach Maßgabe der ausländerrechtlichen Vorschriften. Dabei ist der Grundsatz der Verhältnismäßigkeit zu beachten. Zu den Aufgaben der Ausländerbehörden zählen gem. §§ 5 ff. Ausländergesetz[41] u. a. die Erteilung von Aufenthaltserlaubnissen. Ausländer ohne gültige Aufenthaltserlaubnis, wie diese vietnamesischen Staatsbürger, sind verpflichtet, die Bundesrepublik Deutschland zu verlassen.

Der Umfang der zu verarbeitenden Daten muß erforderlich sein, um die Rückführung der vietnamesischen Staatsbürger durchführen zu können. Die vietnamesischen Behörden prüfen anhand der ihnen von den deutschen Behörden übermittelten Daten, ob die Betroffenen vietnamesische Staatsbürger sind. Dazu benötigen sie Daten, aus denen sich unzweifelhaft

---

41 vom 9. Juli 1990, BGBl. III 26-6

die Identität der betroffenen Personen ergibt. Diese Daten werden durch das Selbstangabeformular erhoben. Fragen nach

- Religion,
- Ausreisetransportmittel, Reiseweg sowie ausgeübte Tätigkeiten während der Reise,
- Gründe und Zweck der Einreise in die Bundesrepublik,
- Angabe der Zeiten, Wohnorte in der Bundesrepublik,
- Aufenthaltszeiten und -orte, Antragstellung eines deutschen Aufenthaltstitels und
- Familienangehörige im Ausland

stoßen auf datenschutzrechtliche Bedenken, da sie für die Prüfung der vietnamesischen Staatsbürgerschaft durch die vietnamesischen Behörden nicht benötigt werden und somit zur Aufgabenerfüllung nicht erforderlich sind. Dies gilt insbesondere für die Frage nach dem Grund und dem Zweck der Einreise, da hier der Betroffene mitteilen muß, wenn er hier um Asyl nachgesucht hat.

Da es sich bei dem Rückübernahmeabkommen um ein Verwaltungsabkommen handelt, kann es nicht als Rechtsgrundlage für die zur Durchführung erforderliche Informationsverarbeitung herangezogen werden. Daraus ergibt sich, daß die Datenerhebung mittels des Selbstangabeformulars nur mit der Zustimmung der Betroffenen erfolgen kann. Diese unterdessen allgemein vertretene Auffassung hat das Bundesministerium des Innern im August 1995 dem Bundesbeauftragten für den Datenschutz bestätigt. Folgerichtig enthält das Selbstangabeformular auch keinen Hinweis auf eine Rechtsgrundlage gem. § 75 Abs. 3 AuslG, die die Betroffenen zum (vollständigen) Ausfüllen des Formulars verpflichtet.

Gem. § 4 Abs. 1 Buchst. b Bbg DSG ist eine Verarbeitung personenbezogener Daten zulässig, wenn der Betroffene eingewilligt hat. Für die Fälle, in denen mangels spezialgesetzlicher Regelung mit Einwilligung der Betroffenen Daten verarbeitet werden, ist eine umfassende Aufklärung vorgesehen. Das vorliegende Selbstauskunftsformular wird den Voraussetzungen für eine rechtswirksame Einwilligungserklärung der Betroffenen nicht gerecht. Es erweckt vielmehr den Eindruck, daß es sich nicht um eine freiwillige Datenerhebung handelt. Dies wird insbesondere durch die Gestaltung der Unterschrift verstärkt, mit der der Betroffene bestätigt, die Fragen wahrheitsgemäß beantwortet zu haben.

Da das Formular fester Bestandteil des Durchführungsabkommens ist und von der Bundesrepublik Deutschland nicht einseitig verändert werden kann, muß ein anderer Weg gefunden werden, die Vorschriften des Brandenburgischen Datenschutzgesetzes in die Praxis umzusetzen. Dies könnte (ebenso wie in Mecklenburg-Vorpommern) durch ein zweisprachiges Merkblatt geschehen, das den Betroffenen zusammen mit dem Selbstangabeformular übergeben wird.

Ich habe mich deshalb an das MI gewandt. Ungeachtet seiner anderen Auffassung über die Freiwilligkeit der Datenerhebung mittels des Selbstangabeformulars hat das MI mitgeteilt, daß es zur Zeit ein Merkblatt erstellt, dessen Entwurf mir rechtzeitig zugesandt werden soll. Im übrigen habe eine ausdrückliche Nachfrage ergeben, daß die zuständigen Ausländerbehörden die Betroffenen in verbaler Form auf die Freiwilligkeit der Angaben hinweisen und ihr Einverständnis einholen.

Im Protokoll zur Durchführung des Abkommens vom 21. Juli 1995 ist in Art. 3 Nr. 4 vermerkt, daß ärztliche Unterlagen über den Gesundheitszustand von Rückkehrern im Rahmen der geltenden deutschen Datenschutzbestimmungen an die vietnamesischen Stellen übermittelt werden. Erfreulicherweise hat mir dazu das MI mitgeteilt, daß die brandenburgischen Ausländerbehörden keine ärztlichen Unterlagen weiterleiten.

3.4 Statistik

3.4.1 Brandenburgisches Statistikgesetz

Leider ist die Verabschiedung eines Brandenburgischen Statistikgesetzes erneut nicht gelungen[42], obwohl es zwischen dem MI und mir auch in diesem Berichtszeitraum zu einer Reihe konstruktiver Gespräche gekommen war. Im Ergebnis dieser Gespräche liegt seit Oktober 1995 der Entwurf eines Gesetzes vor, gegen den aus datenschutzrechtlicher Sicht keine Bedenken bestehen. Der meiste Widerstand gegen die Verabschiedung dieses Gesetzes kam bisher von den Kommunalverbänden.

Die Gemeinden sind verfassungsrechtlich Bestandteile des Staates, deren Aufgabenumfang als Selbstverwaltungsträger durch Gesetze festgelegt werden kann. So ist denn auch jedes Gemeindeamt, jedes Kreisamt, jede Landes- oder Bundesbehörde verfassungsrechtlich für den Bürger "gleichermaßen der Staat", der die personenbezogenen Daten der Bürger nur im Rahmen der Gesetze verarbeiten darf, da die vollziehende Gewalt gem. Art. 20 Abs. 3 Grundgesetz an Gesetz und Recht gebunden ist und der Gesetzgeber von Verfassungs wegen eine Allzuständigkeit besitzt. Jedoch schließt die eigene Verantwortung der Kommunen und ihrer Verbände eine Staatsaufsicht nicht aus.

Dies wurde allerdings in der Vergangenheit von Vertretern der brandenburgischen Kommunen nicht gesehen. Sie hielten daher Regelungen, wie sie im Entwurf zum Landesstatistikgesetz vorgesehen sind, für Eingriffe in ihre Organisations- und Personalhoheit und sahen dazu überhaupt keinen Bedarf. Die Vorteile, die objektive statistische Daten bei der Planung für die Politik bieten können, wurden ebenfalls nicht berücksichtigt. Andererseits wurde auch nicht erkannt, daß der Schutz des Rechts auf informationelle Selbstbestimmung des Bürgers durch kommunale öffentliche Stellen ebenso zu garantieren ist wie durch Landes- oder Bundeseinrichtungen.

Einige Aspekte des Entwurfs sollen nachfolgend hervorgehoben werden:

- Erstellung von Geschäftsstatistiken

Zur Zeit können öffentliche Stellen gem. § 31 Bbg DSG aus den bei ihnen rechtmäßig angefallenen personenbezogenen Datenbestände für ihre eigenen Zwecke Statistiken (sog. Geschäftsstatistiken) erstellen. Nunmehr soll auch die jeweils übergeordnete Stelle dazu ermächtigt werden, die Anfertigung von solchen Statistiken aus personenbezogenen Verwaltungsdaten von der untergeordneten Stelle einfordern zu dürfen. Da Geschäftsstatistiken von der Verwaltung selbst erstellt werden können, bedarf es keines zusätzlichen Personals. Damit könnten insbesondere in kleineren Gemeinden und Ämtern alle statistischen Bedürfnisse abgedeckt werden.

- Kommunalstatistik

Darüber hinaus sollen künftig Gemeinden und Gemeindeverbände ermächtigt werden, eigene Kommunalstatistiken erstellen zu können, und zwar durch eigene primäre Erhebungen oder auf Basis von bereits vorhandenen personenbezogenen Datenbeständen anderer Verwaltungsstellen. Hierzu werden allerdings Satzungen und abgeschottete kommunale Statistikstellen erforderlich, damit das Statistikgeheimnis gewahrt werden kann. Auch ist die Möglichkeit vorgesehen, daß sich Gemeinden und Gemeindeverbände zusammenschließen, um gemeinsam eine Statistikstelle zu betreiben, weil dies unter Kostengesichtspunkten günstiger sein könnte. Allerdings ist keine Kommune und kein Kommunalverband verpflichtet, Kommunalstatistiken zu erstellen.

---

[42] s. 2. Tätigkeitsbericht unter 3.9.3 und 3. Tätigkeitsbericht unter 3.9.2

- Kommunale Statistikstellen

Erfahrungsgemäß bestehen die besonderen kommunalstatistischen Bedürfnisse eher für größere Verwaltungseinheiten wie Landkreise, kreisfreie Städte oder größere Städte. Hier wären dann kommunale Statistikstellen einzurichten, die räumlich, organisatorisch und personell von anderen Stellen des Verwaltungsvollzugs getrennt sind. Solchen Stellen können auch Einzelangaben aus Bundesstatistiken zur weiteren ausschließlich statistischen Verarbeitung übermittelt werden, sofern ein Einzelstatistikgesetz dies vorsieht. "Gerade wenn sich die Angaben - wie im gemeindlichen Bereich - auf kleinere Personengruppen beziehen, muß der Gesetzgeber für organisatorische Vorkehrungen sorgen, welche die vorgesehene Zweckbindung garantieren. Dazu ist die Trennung der Kommunalstatistik von anderen Aufgabenbereichen der Gemeinden und ihrer Verbände ("informationelle Gewaltenteilung") unerläßlich."[43] Dabei sei die statistische Zweckbindung personenbezogener Einzelangaben wie in den Statistischen Ämtern des Bundes und der Länder zu sichern.

Solche speziellen kommunalen Statistikstellen werden auch die Aufgaben der örtlichen Erhebungsstellen übernehmen können, wie sie für Erhebungen von Statistiken der EU, des Bundes oder des Landes benötigt werden. Ich erinnere daran, daß nach wie vor Erhebungen zur umfänglichen amtlichen Agrarstatistik[44] in den Kreisämtern für Landwirtschaft und nicht in eigenen Statistikstellen durchgeführt werden. Dies hatte ich bereits in meinem 3. Tätigkeitsbericht[45] moniert. Hier böte sich eine Kombination der kommunal- und der bundesstatistischen Aufgabenerfüllung auch unter dem Blickwinkel knapper Kassen geradezu an.

Da der Landesgesetzgeber nur die grundsätzlichen Anforderungen an die kommunalen Statistikstellen formuliert, ist es für die praktische Umsetzung erforderlich, vor Ort in einer speziellen Dienstanweisung die konkreten Maßnahmen zum Schutz des Statistikgeheimnisses darzustellen. Dies hatte ich bereits in meinem 3. Tätigkeitsbericht[46] empfohlen. Dazu kann auch eine Musterdienstanweisung, die das MI vorlegen will, hilfreich sein.

3.4.2 Wohnungsstatistik

3.4.2.1 Durchführung und Probleme

Mit Stichtag 30. September 1995 wurde auch im Land Brandenburg eine vollständige Gebäude- und Wohnungszählung gemäß Wohnungsstatistikgesetz[47] und Verordnung zur Durchführung der Gebäude- und Wohnungszählung 1995[48] durchgeführt. Dazu hatte das Landesamt für Datenverarbeitung und Statistik (LDS) eine Erhebungsstellenanleitung mit Anlagen[49] entwickelt, die der technisch-organisatorischen, räumlichen und personellen Abschottung der Erhebungsstellen von der übrigen Verwaltung zum Zweck der Sicherung des Statistikgeheimnisses und der Aufgabenbeschreibung dieser statistischen Stellen dient. Meine Hinweise zur datenschutzgemäßen Ausgestaltung waren dabei berücksichtigt

---

43 BVerfGE 65, 1 (69)

44 Agrarstatistikgesetz vom 23. September 1992, BGBl. I S. 1632

45 s. unter 3.9.5

46 s. unter 3.9.8

47 vom 18. März 1993, BGBl. I S. 337

48 vom 29. Dezember 1994, GVBl. II S. 97

49 Entwurf einer Musterdienstanweisung, Verpflichtungserklärung zur Geheimhaltung und zur Sicherung des Datenschutzes für Erhebungsstellenmitarbeiter und Erhebungsbeauftragte und entsprechende Entwürfe für förmliche Verpflichtungsakte und Bestellungen

worden[50].

Insgesamt wurden im Land Brandenburg 32 Erhebungsstellen installiert, je Landkreis zwei und je kreisfreier Stadt eine. Im Zeitraum von August 1995 bis März 1996 haben Mitarbeiter meiner Behörde davon 17 Erhebungsstellen kontrolliert, und zwar je Landkreis mindestens eine und eine in einer kreisfreien Stadt.

Die Prüfung der Erhebungsstellen erfolgte unter Berücksichtigung des Gleichbehandlungsgrundsatzes bei Kontrollen nach einem einheitlichen Fragenkatalog, der sich an der Erhebungsstellenanleitung des LDS ausrichtete. Schwerpunkt der Prüfung waren die erforderlichen Abschottungsmaßnahmen gegenüber der sonstigen Verwaltung. In keinem Fall waren datenschutzrechtliche Beanstandungen auszusprechen. Vielmehr stellte sich bei den ausgewählten Stellen erfreulicherweise ein hohes Maß an Sensibilität und Verantwortungsbewußtsein in datenschutzrechtlichen Belangen heraus.

- Personelle, organisatorische, räumliche und technische Abschottung

In allen Fällen war feststellbar, daß die Erhebungsstellenmitarbeiter für die gesamte Zeit ihrer Tätigkeit ausschließlich in Erhebungsstellen beschäftigt wurden, insoweit war die gebotene Abschottung zur übrigen Verwaltung konsequent beibehalten.

Die personell-organisatorische Abschottung war so geregelt worden, daß für jede Erhebungsstelle ein Leiter und ein Stellvertreter und ein oder mehrere Mitarbeiter eingesetzt wurden. Diese sind dienstaufsichtlich häufig dem Hauptamtsleiter, aber auch dem Landrat oder dem Oberbürgermeister unterstellt worden. Die Dienstaufsicht beinhaltet die Kontrolle des ordnungsgemäßen Dienstablaufs, nicht jedoch die Einsicht in personenbezogene Daten der Auskunftspflichtigen. In keinem Fall sind meinen Mitarbeitern in dieser Hinsicht Klagen zu Gehör gekommen, so daß ich davon ausgehen kann, daß auch die Leitungen der kommunalen Verwaltung die Abschottung der statistischen Erhebungsstellen zur Wahrung des Statistikgeheimnisses zu ihrer eigenen Sache gemacht haben.

Auch die räumliche Abschottung war durch die Einrichtung separater Räumlichkeiten, deren Türen stets mit Sicherheitsschlössern und meistens mit Türknauf von außen versehen waren, und durch entsprechende zusätzliche Sicherungen, wie festgelegte Arbeitszeit- und Schlüsselregime, gewährleistet.

Das LDS hatte die Rechentechnik (PC und Drucker) leihweise geliefert und auch das Programm zur Registrierung der eingegangenen Erhebungsbögen zur Verfügung gestellt. Da diese PC Einzelplätze waren und ausdrücklich nicht in das Behördennetz, sofern überhaupt vorhanden, einbezogen wurden, war auch die Abschottung in dieser Hinsicht stets gesichert.

- Mängel

Als großes Problem stellte sich für die Erhebungsstellen das teilweise schlechte Adressenmaterial heraus. Das LDS baute auf der Basis von § 8 Wohnungsstatistikgesetz[51] vor Beginn der eigentlichen Zählung eine Adreßleitdatei über alle Gebäude mit Wohnraum und bewohnte Unterkünfte und deren Eigentümer für das Land Brandenburg auf, die aus den Unterlagen der für die Grundsteuer und für die Führung des Grundbuchs zuständigen Stellen zur Verfügung zu stellen war.

Trotz Vorbegehungen durch Erhebungsbeauftragte und Aktualisierungen der Adressendatei kam es immer wieder zu erheblichen Belastungen für die Erhebungsstellenmitarbeiter wegen

---

50 s. 3. Tätigkeitsbericht unter 3.9.3

51 vom 18. März 1993, BGBl. I S. 337

nicht zustellbarer Erhebungsunterlagen. Die von den zuständigen Ämtern der Kommunen gelieferten Adressen- und Eigentümerdaten waren bis zu 25 % nicht brauchbar, so daß ein erheblicher Zeitaufwand in Nacherhebungen investiert werden mußte. Es wurde wiederholt berichtet, daß es in ein und demselben Einzugsbereich einer Erhebungsstelle Ämter gebe, deren Daten "fast ganz aktuell", und andere, deren Daten "fast nicht" zu gebrauchen seien.

Die objektiven Ursachen für die häufig falschen Adressen- und Eigentümerdaten in den zuständigen kommunalen Ämtern waren für die Mitarbeiter meiner Behörde nicht eindeutig feststellbar. Als Gründe wurden in den Erhebungsstellen die längst abgeschlossene Bildung der Großkreise und Ämterneubildungen vermutet.

Diese Feststellungen führen noch zu einem anderen Gesichtspunkt. Vor dem Hintergrund der allgemein beklagten Finanznot der Kommunen ist es kaum verständlich, daß beispielsweise die für die Grundsteuer zuständigen kommunalen Stellen häufig unrichtige Gebäude- und Eigentümerdaten speichern, obwohl ihnen dadurch erhebliche Steuereinnahmen verlorengehen. Wohl aus diesem Grund sind gelegentlich Begehrlichkeiten dieser Ämter bekannt geworden, das von den statistischen Erhebungsstellen mit viel Aufwand aktualisierte Datenmaterial über Gebäudeadressen und Besitzverhältnisse übermittelt zu erhalten. Diese Ansinnen sind allerdings schon von den Erhebungsstellen stets zu Recht zurückgewiesen worden, weil dadurch gerade die verfassungsrechtlich und gesetzlich geforderte Trennung der Statistik vom Verwaltungsvollzug aufgehoben und das Statistikgeheimnis massiv verletzt worden wäre.

3.4.2.2 Bereitstellung statistischer Einzelangaben für die Kommunen

Etwa ab Juli 1996 können kommunale Statistikstellen für ihren Zuständigkeitsbereich gem. § 11 Wohnungsstatistikgesetz statistische Einzelangaben nach Straße und Hausnummer der Gebäude vom LDS zur Erstellung eigener Kommunalstatistiken erhalten, sofern diese Stellen den erforderlichen Abschottungskriterien entsprechen[52]. Wegen des derzeit noch nicht verabschiedeten Landesstatistikgesetzes würden die allgemeinen Regelungen in § 32 Bbg DSG zur Anwendung kommen. Hierzu könnte die vorgenannte Muster-Dienstanweisung dienlich sein (s. unter 3.4.1).

Auch an eine hiernach installierte kommunale Statistikstelle - die übrigens auch von mehreren Kommunen unterhalten oder als datenverarbeitende Stelle für Datenverarbeitung im Auftrag auch durch weitere Kommunen genutzt werden kann - sind hierfür Anforderungen zu stellen, die im wesentlichen vergleichbar mit den Regelungen für die derzeit noch bestehenden Erhebungsstellen zur Gebäude- und Wohnungszählung sind.

3.4.2.3 Bürgereingaben zur Wohnungsstatistik

Zur Gebäude- und Wohnungszählung 1995 gab es zahlreiche Eingaben. Petenten bezweifelten die Rechtmäßigkeit von statistischen Erhebungen überhaupt, und ich mußte sie auf die entsprechenden verfassungsrechtlichen und gesetzlichen Grundlagen der amtlichen Statistik hinweisen.

Die nicht aktualisierten Eigentümereintragungen (s. unter 3.4.2.1), die teilweise durchaus auch einen datenschutzrechtlich bedenklichen Hintergrund haben, führten zu Verärgerungen in der Bevölkerung. So monierte beispielsweise ein Petent aus einem anderen Bundesland, daß er zur Gebäude- und Wohnungszählung herangezogen worden sei, obwohl er sein Haus bereits vor über 10 Jahren verkauft hatte. Durch die Offenbarung seiner ehemaligen Besitzverhältnisse, für die im datenschutzrechtlichen Sinne kein Erfordernis bestand, war gegenüber seiner jetzigen Lebenspartnerin auch herausgekommen, daß er bereits einmal

---

[52] s. 3. Tätigkeitsbericht unter 3.9.3

verheiratet war. Dies führte nun in der jetzigen Beziehung zu Belastungen und zeigt, wie eine unrichtige Datenspeicherung - und erscheint sie für sich genommen noch so belanglos - die Privatsphäre beeinträchtigen kann.

Ein anderer Petent beschwerte sich über die Eintragung seiner Telefon-Nr. auf dem Deckblatt seines Erhebungsbogens, die die Erhebungsstelle handschriftlich dort vermerkt hatte. Hierin sah er einen Verstoß gegen § 9 Abs. 4 Wohnungsstatistikgesetz (WoStatG)[53], wonach die Angabe dieses Hilfsmerkmals als freiwillig deklariert ist. Die zuständige Erhebungsstelle wies ihrerseits darauf hin, daß ihr Erhebungsbeauftragter Schwierigkeiten bei der Ermittlung der Anschrift des Gebäudebesitzers gehabt habe und deshalb über das öffentliche Telefonbuch zu dieser Angabe gekommen sei. Außerdem seien Erhebungsbeauftragte nach § 7 Abs. 1 WoStatG dazu direkt ermächtigt. Obwohl einerseits die Angabe der Telefon-Nr. gem. § 9 Abs. 4 WoStatG freiwillig ist, wird andererseits durch § 7 Abs. 1 WoStatG der Erhebungsbeauftragte - nicht jedoch die Erhebungsstelle - befugt, in Fällen, in denen es bei der Feststellung der Adreßdaten des Auskunftspflichtigen die geschilderten Schwierigkeiten gibt, hilfsweise eigene Ermittlungen anzustellen und deren Ergebnisse im Rahmen des § 7 Abs. 1 WoStatG auch in den Erhebungsbogen einzutragen. Will nun aber der Auskunftspflichtige, nachdem ihm endlich sein Erhebungsbogen ordnungsgemäß zugestellt werden konnte, seine Telefon-Nr. als freiwillige Angabe weiterhin nicht mitteilen, könnte er dies etwa durch Schwärzen im Bogen erreichen.

In einem anderen Fall führte ein Petent darüber Beschwerde, daß in einem ihm zugeschickten Mahnbrief der Mahnbescheid an einen anderen Bürger beigefügt worden sei. Daraus schloß er allgemein auf einen recht leichtfertigen Umgang mit den personenbezogenen Daten der Bürger durch das zuständige Amt und überhaupt durch alle öffentlichen Stellen. Tatsächlich waren völlig unbeabsichtigt in einigen wenigen Fällen durch eine nicht fein genug eingestellte Briefkuvertiermaschine zwei Schreiben in einen Umschlag gelangt. Dieses technische Problem führte zu einem eindeutigen Verstoß gegen technisch-organisatorische Regelungen gem. § 10 Bbg DSG. Wegen sofortiger Beseitigung dieses technischen Mißstandes und weiterer vorbeugender Maßnahmen habe ich auf eine förmliche Beanstandung verzichtet.

3.4.3 Mikrozensus 1996 und Novellierung des Bundesstatistikgesetzes

Für 1996 gilt ein neues Mikrozensusgesetz[54], das das Erhebungsprogramm der jährlich laufenden Haushalts- und Familienstatistik (nach Personen, Haushalten und Wohnungen) bis zum Jahr 2004 regelt und zugleich die Anforderungen der EU-Arbeitskräftestichprobe berücksichtigt.

In die Erhebung werden wie bisher 1 % der Bevölkerung jeweils über 4 Jahre einbezogen, wobei ein jährlicher Austausch von 0,25 % der alten durch neue Auswahlbezirke vorgenommen wird. Die Auswahl erfolgt ebenfalls wie bisher aufgrund von mathematischen Zufallsverfahren auf der Basis von Flächen oder vergleichbarer Bezugsgrößen (Auswahlbezirke). Dabei wird für jedes Erhebungsjahr dasselbe feste Grundprogramm im 4-Jahresrhythmus mit einem wechselnden Zusatzprogramm kombiniert.

Neben Pflichtauskünften gibt es wieder solche, die freiwillig gegeben werden können. Insgesamt hat der Fragenkatalog in seinem Umfang deutlich zugenommen; auch die Anzahl der Pflichtauskünfte ist gestiegen. Eine gewisse Entlastung ergibt sich durch die jährlich wechselnden Zusatzprogramme, die z. T. für weniger als 1 % der Bevölkerung erhoben werden.

---

53 vom 18. März 1993, BGBl I S. 337

54 BT-Drs. 13/3107

Die Datenschutzbeauftragten des Bundes und der Länder hatten an den Erhebungsbögen zum Mikrozensus 1995 moniert, daß hier im Gegensatz zu früheren Jahren Pflicht- und freiwillige Auskünfte vermischt worden waren. Zudem war diese Unterscheidung für den Ausfüllenden, sei es nun der Bürger selbst oder der Interviewer, optisch kaum auszumachen. Es war also nicht mehr eindeutig und klar zu erkennen, welche Fragen zwingend zu beantworten waren und welche nicht.

Die zuständigen Stellen des Bundes und der Länder haben sich dieser Problematik angenommen. Herausgekommen ist ein vertretbarer Kompromiß. Zwar wurde die Vermischung von auskunftspflichtigen und freiwilligen Fragen zur Betonung der sachlichen Zusammengehörigkeit beibehalten. Jedoch werden die freiwilligen Angaben nun durch den senkrechten Ausdruck "freiwillig", eine andere Farbgestaltung der Zeile und durch die zusätzliche Zeile "Keine Angabe" für den Bürger eindeutig unterscheidbar. Auch der Erhebungsbogen des Interviewers ist durch die zwei letztgenannten Angaben ergänzt worden. Daraus folgt auch, daß, wenn bei der Erhebung tragbare Computer (Laptops, Notebooks) oder stationäre Arbeitsplatzcomputer direkt zur Datenerfassung eingesetzt werden, deren Bildschirmmasken durch eine entsprechend programmierte optische Gestaltung für den Interviewer leicht und rechtlich korrekt bedienbar sein müssen.

Im Zusammenhang mit den neuen Bestimmungen des Mikrozensusgesetzes hat der Bundesgesetzgeber auch das Bundesstatistikgesetz (BStatG) geändert. Geregelt wird nunmehr in § 11 a der Einsatz von computergestützten statistischen Erhebungsverfahren. Dies betrifft einmal den Einsatz von Computern, in die die Erhebungsbeauftragten die Daten der Auskunftspflichtigen direkt einspeichern können. Andererseits schließt dies laut Begründungstext auch telefonische Erhebungen ein.

Zur Problematik telefonischer Erhebungen hat die Bundesregierung[55] darauf hingewiesen, daß für jede Art von Erhebung, so auch für die telefonische, § 17 BStatG gilt, wonach die Betroffenen zuvor schriftlich über Zweck, Art und Umfang der Erhebung u. a. zu unterrichten sind.

Problematisch bleiben telefonische Erhebungen aber trotzdem; von Gesetzes wegen deshalb, weil nicht eindeutig gesichert ist, daß der Auskunftspflichtige stets auch die schriftliche Auskunftserteilung wählen kann, wie § 15 Abs. 4 BStatG beim Einsatz von Erhebungsbeauftragten bestimmt. Denn in dem neuen § 11 a Abs. 2 BStatG wird diese ausdrückliche Möglichkeit dadurch eingeschränkt, daß eine Rechtsvorschrift für eine Einzelstatistik diese freie Wahl der Auskunftserteilung ausschließen kann. Zudem ist bekannt, daß öffentliche Übertragungsleitungen ziemlich leicht abgehört werden können. So sensible personenbezogene Daten, wie sie durch den Mikrozensus abgefragt werden, beschreiben einen erheblichen Bereich der sozialen und gesundheitlichen Befindlichkeit aller Haushaltsangehörigen. Nur wenige Bürger dürften sich deshalb zu telefonischen Befragungen bereitfinden, zumal das vom LDS gewählte Verfahren trotz schriftlicher und mündlicher Vorstellung und mit Rückrufmöglichkeit grundsätzlich datenschutzrechtlich problematisch bleibt.

3.4.4 Amtliche Statistiken als Grundlage für Sekundärstatistiken von Verwaltungsdaten - datenschutzrechtlich nicht unbedenklich

Aus Gründen der Kosteneinsparung und zur geringeren Belastung der Auskunftspflichtigen läßt die Bundesregierung zur Zeit prüfen, inwieweit amtliche Statistiken eingeschränkt und rationalisiert werden können. Beispielsweise wird in einigen Bundesländern untersucht, ob etwa aus den Antragsdaten auf die EU-Agrarförderung mittels Sekundärstatistik die Erhebung für die amtliche Agrarstatistik abgeleitet werden kann.

---

55 BT-Drs. 13/3131

Solche Vorhaben sind stets problematisch, weil es bei ihrer praktischen Umsetzung sehr schwer ist, die verfassungsrechtlich und gesetzlich geforderte Trennung von Statistik und Verwaltungsvollzug tatsächlich durchzuhalten. Es wäre auch gegenüber den Auskunftspflichtigen unfair und verletzte ihre freie Entscheidungsmöglichkeit, rechtliche Unzulässigkeiten, die in der Praxis der Verwaltung nicht behoben werden können, durch Abforderung von persönlichen Zustimmungserklärungen zu umgehen, auch wenn diese als "freiwillige Erklärung", die widerrufen werden kann, deklariert sind.

Auch muß man sich darüber im klaren sein, daß die sekundärstatistische Verarbeitung von solchen personenbezogenen Verwaltungsdaten, die zum Zweck der Leistungsgewährung erhoben wurden, in bezug auf ihre statistische Aussagekraft grundsätzlich fragwürdig sind, weil sie im allgemeinen die für eine Statistik vorausgesetzte Neutralität und Objektivität der Daten vermissen lassen.

Diese grundsätzlichen Bedenken habe ich in bezug auf vergleichbare Vorhaben gegenüber den zuständigen Stellen im Lande geäußert und werde darüber zu gegebener Zeit erneut berichten.

4 Justiz

4.1 Führung Schuldnerverzeichnis - eine Verwaltungsaufgabe

Bereits während der Entwurfs-Phase für die Neugestaltung der Regelungen für das Schuldnerverzeichnis in der ZPO[56], §§ 915 ff., hatte das Ministerium der Justiz und für Bundes- und Europaangelegenheiten (MdJBE) den Standpunkt vertreten, die Führung des Schuldnerverzeichnisses sei eine gerichtliche und keine Verwaltungs-Angelegenheit, so daß der Landesbeauftragte für den Datenschutz für diesen Bereich nicht zuständig sei. Diesen Standpunkt vertrat die Landesregierung auch noch in ihrer Stellungnahme zu meinem 3. Tätigkeitsbericht[57]. Das MdJBE hatte zuvor dennoch meine Beteiligung an dem Gesetzgebungsverfahren akzeptiert, so daß ich hier meine Überlegungen wiedergeben möchte, auf die ich meine Auffassung stütze, daß die Führung des Schuldnerverzeichnisses eine Verwaltungstätigkeit ist. Wenn es sich dabei aber um eine Verwaltungstätigkeit handelt, ist meine Zuständigkeit gem. § 2 Abs. 1 Satz 2 Bbg DSG gegeben.

Die Regelungen über das Schuldnerverzeichnis in der neuen Fassung enthalten zwar keine ausdrückliche Aussagen zu dieser Frage, man findet jedoch mehrere Textstellen, die jeweils für sich genommen den Schluß zulassen, daß die Führung dieses Verzeichnisses eine Verwaltungstätigkeit ist, und die in der Zusammenschau diese Aussage "Verwaltungstätigkeit" absichern.

Es handelt sich bei der Führung des Schuldnerverzeichnisses insbesondere deshalb nicht um eine gerichtliche Tätigkeit, da

- keine Entscheidungen getroffen werden (die Eintragungen betreffen bereits vorliegende Entscheidungen),

- von Gesetzes wegen die Führung des Verzeichnisses nicht an ein bestimmtes Amtsgericht gebunden ist, weil ein anderes als das zuständige Amtsgericht das Register führen oder ein Amtsgericht das Register für die Bezirke mehrerer Amtsgerichte führen kann und

---

56 vom 12. September 1950, BGBl. III 310-4, geänd. d. Ges. vom 15. Juli 1994, BGBl. I S. 1566

57 s. unter 4.1.2

- die Zulässigkeit des automatisierten Abrufs aus dem Register mit gerichtlicher Tätigkeit nicht vereinbar ist.

Im übrigen werden in der Kommentierung des Gesetzes[58] zur Novellierung der §§ 915 ff. in der Übersicht vor diesen Paragraphen unter dem Stichwort "Systematik" als eine "Verknüpfung von Justizverwaltungs- und Verfahrensrecht" und die zugehörigen Tätigkeiten als "Akte der gerichtlichen Verwaltung" bezeichnet. Diese systematische Zuordnung war zum bisherigen Recht (§ 915 a. F.) nicht so offensichtlich und daher streitig; auch der hier erwähnte Kommentar sah die systematische Einordnung bezüglich des alten Rechts offenbar anders, wenn er z. B. dazu ausführt, daß das Schuldnerverzeichnis von dem Vollstreckungsgericht, und "nicht etwa" von der Justizverwaltung geführt werde. In jedem Fall wird künftig im Zusammenhang mit der Führung des Schuldnerverzeichnisses von Verwaltungshandeln und nicht von gerichtlicher Tätigkeit auszugehen sein, daher erwarte ich, daß meine Zuständigkeit nicht (mehr) bestritten werden wird.

4.2 Staatsanwaltliches Verfahrensregister (Bundes-SISY) und Mehrländer-Staatsanwaltschaft-Automation (MESTA)

Mit der Verabschiedung des Verbrechensbekämpfungsgesetzes[59] ist die Rechtsvorschrift (§§ 476 - 477 StPO) für die Errichtung eines länderübergreifenden staatsanwaltlichen Verfahrensregisters in Kraft getreten. Im August 1995 hat das Bundesministerium der Justiz eine Allgemeine Verwaltungsvorschrift über eine Errichtungsanordnung für das länderübergreifende staatsanwaltschaftliche Verfahrensregister (Bundes-SISY)[60] erlassen.

Die verschiedenen Entwürfe der Errichtungsanordnung habe ich ebenso wie meine Kollegen in Bund und Ländern kritisiert[61]. Im Mittelpunkt meiner Kritik stand, daß sie keine grundsätzlichen Festlegungen über die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherung enthalten, obwohl § 476 Abs. 5 StPO eine solche Festlegung ausdrücklich vorschreibt. Nähere Einzelheiten zu den technischen und organisatorischen Maßnahmen fehlen in der nunmehr in Kraft gesetzten Errichtungsanordnung immer noch. Sie führt lediglich aus, daß die in Rede stehenden Daten besonders sensibel seien und daher besonderer technischer und organisatorischer Schutzmaßnahmen bedürften. Die Errichtungsanordnung bleibt damit datenschutzrechtlich unbefriedigend.

Die Justizverwaltungen der Länder müssen nun die Anbindung der Staatsanwaltschaften an die beim Generalbundesanwalt als Registerbehörde im Bundeszentralregister geführte Datei realisieren. Brandenburg betreibt den Anschluß zusammen mit Hamburg und Schleswig-Holstein in einem gemeinsamen Entwicklungsprojekt. In dem Verwaltungsabkommen über die Zusammenarbeit im Rahmen des Vorhabens Mehrländer-Staatsanwaltschaft-Automation (MESTA) ist festgelegt, daß die Abstimmung in einer Lenkungsgruppe erfolgen soll, der neben Vertretern der beteiligten Justizverwaltungen auch der Hamburgische Datenschutzbeauftragte als Vertreter der zuständigen Landesbeauftragten für den Datenschutz angehören soll. Der Hamburgische Datenschutzbeauftragte hat sich dazu bereit erklärt, diese Vertretung unter der Voraussetzung wahrzunehmen, daß sie auf informatorische und beratende Funktionen begrenzt ist und dadurch die Informationszugänge, Beratungen und Prüfungen der jeweiligen Landesbeauftragten für den Datenschutz nicht berührt werden. Ich habe dem Hamburgischen Datenschutzbeauftragten

---

58 Hartmann in: Baumbach/Lauberbach/Albers/Hartmann, ZPO, 53. Auflg.

59 vom 28. Oktober 1994, BGBl. I S. 3186

60 vom 7. August 1995, BAnz. Nr. 163 S. 9761

61 s. 3. Tätigkeitsbericht unter 4.1.4

mitgeteilt, daß ich seine Bereitschaft, mich in der Lenkungsgruppe zu vertreten, dankbar aufgreife. Die Beachtung der - sich aus der gesetzlichen Aufgabenzuweisung des Brandenburgischen Datenschutzgesetzes ergebenden - Voraussetzungen halte ich für selbstverständlich. Das Ministerium der Justiz teilt meine Auffassung. Es hat meine fortlaufende Beteiligung an dem Automatisierungsvorhaben zugesichert.

4.3 Rückmeldeverfahren

Es erwies sich erneut als besonders problematisch[62], daß die Staatsanwaltschaften den Polizeibehörden keine Rückmeldung über den Ausgang der staatsanwaltschaftlichen Ermittlungen machen (s. unter 3.2.4.3), ganz zu schweigen von der Tatsache, daß die Polizeibehörden keine Mitteilung über den Ausgang des Gerichtsverfahrens erhalten.

Gem. Nr. 11 Abs. 1 b der Anordnung über Mitteilungen in Strafsachen der Justizminister und Justizsenatoren des Bundes und der Länder (MiStra)[63] teilt die Staatsanwaltschaft der Polizei die Verfahrenseinstellung mit, wenn diese bei der Übersendung der Ermittlungsakten darum bittet. Rein formal betrachtet sind die brandenburgischen Staatsanwaltschaften jedoch nicht verpflichtet, das Rückmeldeverfahren zu praktizieren, da das Land die MiStra nicht in Kraft gesetzt hat.

In der überwiegenden Zahl der Fälle werden Verfahren gem. § 170 Abs. 2 StPO eingestellt, weil die Ermittlungen nicht genügend Anhaltspunkte für eine Anklageerhebung vor Gericht ergeben haben. Nicht jede Einstellung hiernach führt aber zur Löschung der Daten, die bei der Polizei im Zusammenhang mit der Ermittlung erhoben und gespeichert worden sind. Sie veranlaßt jedoch in jedem Fall eine Prüfung, ob die Daten für die Aufgabenerfüllung der Polizei weiterhin erforderlich sind. Die Betroffenen müssen die mit der weiteren Aufbewahrung verbundenen Eingriffe in ihr Recht auf informationelle Selbstbestimmung nur hinnehmen, wenn die Speicherung gem. § 41 Abs. 3 VGPolGBbg zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. Ungeachtet der nicht in Kraft gesetzten MiStra benachrichtigen die brandenburgischen Staatsanwaltschaften im allgemeinen den Betroffenen über die Einstellung des Ermittlungsverfahrens (Nr. 10 MiStra). Dies hat zusammen mit der fehlenden Rückmeldung bei der Auskunftserteilung zur Folge, daß die Polizei den Betroffenen auch (in Einzelfällen sogar ausschließlich) Ermittlungsverfahren mitteilt, die die Staatsanwaltschaft bereits eingestellt hat.

Eine Stellungnahme des Ministeriums der Justiz zu der Problematik steht noch aus. Daher ist bislang auch noch ungeklärt, warum die Staatsanwaltschaft die Anfragen der polizeilichen Datenschutzbeauftragten (s. unter 3.3.5), über ggf. bestehende Einwände gegen die Auskunftserteilung nicht zum Anlaß nehmen nicht nur ihre Einwilligung sondern auch die Verfahrenseinstellung mitzuteilen.

4.4 Forschungsprojekt "Strafjustiz und DDR-Vergangenheit"

Im Berichtszeitraum ist das MdJBE mit der Bitte an mich herangetreten, zur justizseitigen Unterstützung des Forschungsprojektes "Strafjustiz und DDR-Vergangenheit" an der Humboldt Universität zu Berlin aus datenschutzrechtlicher Sicht eine Stellungnahme abzugeben. Ziel dieses Projektes ist eine Edition strafrechtlicher Entscheide nach dem Vorbild der sog. "Amsterdamer Sammlung". In dieser unterdessen 23-bändigen Sammlung sind sämtliche (west-)deutschen Urteile wegen nationalsozialistischer Tötungsverbrechen im

---

62 s. 2. Tätigkeitsbericht unter 3.6.2.2

63 vom 15. März 1985, BAnz. Nr. 60

Wortlaut enthalten. Sie hat entscheidend zu der heute vorwiegenden Auffassung beigetragen, daß ohne den Einsatz der deutschen Justiz das ganze Ausmaß der NS-Gewaltkriminalität weder aufgeklärt noch ins öffentliche Bewußtsein gerückt worden wäre.

Angesichts der hierzu vorliegenden Materialfülle sind einerseits die Justizverwaltungen nicht in der Lage, die Unterlagen (Einstellungsverfügungen, Anklageschriften und Urteile) in hinreichend anonymisierter Form bereitzustellen. Da andererseits nicht davon auszugehen war, daß die Veröffentlichung mit Einwilligung der Betroffenen hätte durchgeführt werden können, galt es, auf der Grundlage des Forschungsprivilegs gem. § 28 Abs. 2 Bbg DSG eine Lösung zu finden, die den geringst möglichen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt.

Hierzu gab es bereits Vorschläge des Berliner Datenschutzbeauftragten, der zuständigkeitshalber bereits zuvor mit dem Problem befaßt worden war. Er hatte für die Anonymisierung angeregt, entweder ein Kopieren von geschwärzten Kopien zu ziehen oder gescannte Unterlagen unter Zuhilfenahme von Rechtschreibhilfen im wesentlichen zur Suche von Namen zu fertigen. Dies sollte jeweils durch eine am Projekt nicht unmittelbar beteiligte Person erfolgen. Ich habe dies in meiner Stellungnahme aufgegriffen und darüber hinaus weitere organisatorisch-technische Maßnahmen in den Justizverwaltungen selbst ergänzend vorgeschlagen.

Außerdem habe ich dem Ministerium erklärt, daß ich es begrüßen würde, wenn es auch künftig bei der Feststellung des überwiegenden öffentlichen Interesses gem. § 28 Abs. 2 Buchst. b Bbg DSG als selbstverständlich betrachten würde, die Zumutbarkeit des vorgesehenen Eingriffs gegenüber dem Betroffenen durch eine Stellungnahme aus meiner Behörde abwägen zu lassen.

5 Bildung, Jugend und Sport

5.1 Brandenburgisches Schulgesetz

Dem 1991 in nur fünf Monaten entworfenen und vom Landtag verabschiedeten Ersten Schulreformgesetz (1. SRG)[64] war die Funktion eines "Vorschaltgesetzes" zugedacht worden, auf dessen Grundlage zunächst einmal die entscheidenden Voraussetzungen für den Aufbau eines neuen Bildungswesens im Land Brandenburg geschaffen werden sollten. Situationsbedingt wurde daher auch die oberste Schulaufsichtsbehörde zum Erlaß sowohl von Rechtsverordnungen als auch zu Verwaltungsvorschriften für insgesamt 15 Paragraphen - u. a. Vorschriften zum Datenschutz gem. § 75 Abs. 4 - ermächtigt, wobei Inhalt, Zweck und Ausmaß der erteilten Ermächtigung entgegen Art. 80 Abs. 1 Satz 2 Grundgesetz (GG) unbestimmt blieben. Darüber hinaus wurden Rechtsverordnungen und Verwaltungsvorschriften der ehemaligen DDR als fortgeltendes Landesrecht bestimmt, soweit sie nicht dem 1. SRG widersprachen. Daraus hat sich zwangsläufig eine Entwicklung ergeben, zu der ich aus datenschutzrechtlicher Sicht schon mehrfach meine Bedenken[65] geäußert habe; mit der Verabschiedung des Brandenburgischen Schulgesetzes (BbgSchulG) ist in dieser Hinsicht nunmehr glücklicherweise ein Schlußstrich gezogen worden.

Im Vorfeld hat es dazu zahlreiche Entwürfe gegeben. Die im Gesetz zunächst verstreut enthaltenen Einzelregelungen sind meinen Anregungen entsprechend in einen eigenständigen Abschnitt 5 Datenschutz, der aus zwei Paragraphen besteht, zusammengefaßt worden, wobei § 66 die Erhebung und Verarbeitung personenbezogener Daten von

---

64 vom 26. April 1991, GVBl. S. 258

65 s. 2. Tätigkeitsbericht unter 1.3 und 3. Tätigkeitsbericht unter 5.1.1

Schülerinnen, Schülern, Eltern, Lehrkräften und sonstigen Schulpersonal für die Aufgabenwahrnehmung der Schule und der Schulbehörden und - davon abgetrennt - § 67 die wissenschaftlichen Untersuchungen an Schulen zum Gegenstand hat.

Lediglich in bezug auf die Aufnahme des Ausnahmetatbestandes "Nutzung privater PC" in das Gesetz selbst konnte vor dem Mitzeichnungsverfahren nicht mehr ein Einvernehmen erzielt werden. Hierauf hatte ich deshalb großen Wert gelegt, weil bereits verschiedene öffentliche Verwaltungen bei mir angefragt haben, ob diesbezüglich den Wünschen engagierter Mitarbeiter nicht entgegenzukommen wäre, was zu verneinen ist. Im Gegensatz zu Mitarbeitern anderer öffentlicher Verwaltungen geht es bei Lehrern und sonstigem pädagogisch tätigen Schulpersonal um eine Konkretisierung einer bestehenden Befugnis bei der Wahrnehmung von beruflichen Aufgaben. Die Abgeordneten haben sich erfreulicherweise meine Argumentation zu eigen gemacht und § 65 um einen Absatz 5 für diesen Ausnahmetatbestand ergänzt.

Entsprechend den vom BVerfG im Volkszählungsurteil aufgestellten Grundsätzen für eine Verarbeitung personenbezogener Daten wird die zuständige oberste Landesbehörde in § 65 Abs. 10 und § 66 Abs. 3 ermächtigt, Rechtsverordnungen zu erlassen. Das Ministerium für Bildung, Jugend und Sport (MBJS) hat mir mitgeteilt, daß auf dieser Grundlage nunmehr meinem ständigen Drängen zufolge die bestehenden Verwaltungsvorschriften VV-Schulakten[66], VV-Datenschutz/Statistik[67] und VV wissenschaftliche Untersuchungen an Schulen[68] in Rechtsverordnungen geändert werden sollen. Entsprechende Entwürfe seien bereits erarbeitet worden und würden demnächst mit mir abgestimmt werden.

Darüber hinaus sind aber auch die Bestimmungen der Allgemeinen Vorschriften datenschutzrechtlich von Bedeutung. Hinweisen möchte ich hier lediglich auf § 44 Abs. 1 (Einschulung als Begründung eines öffentlich-rechtlichen Schulverhältnisses), § 45 (Schulgesundheitspflege, Pflichtuntersuchungen mit entsprechenden Einsichtsrechten in Absatz 2) sowie § 47 Abs. 1 (Meinungsfreiheit) und § 48 (Schülerzeitungen).

5.2 Einsatz privater PC durch Lehrer

In meinem 3. Tätigkeitsbericht[69] war ich auf Überlegungen seitens des MBJS eingegangen, Lehrern für die Wahrnehmung ihrer schulischen Aufgaben auch die Verwendung ihres privaten PC zu Hause zu gestatten. Mit Inkrafttreten der Ersten Verwaltungsvorschrift zur Änderung der Verwaltungsvorschriften über den Schutz personenbezogener Daten in Schulen und über statistische Erhebungen[70] haben zwischenzeitlich diese Regelungen als § 3 a Eingang in die VV-Datenschutz/Statistik gefunden.

Damit ist aus meiner Sicht ein akzeptables Verfahren gefunden worden, unter welchen Voraussetzungen welche Daten wie lange so verarbeitet werden dürfen. Die Schule bleibt dabei im Sinne von § 3 Abs. 4 Nr. 1 Bbg DSG datenverarbeitende Stelle. Lehrer haben hierfür einen Antrag bei der Schulleitung zu stellen, in dem ausdrücklich das Einverständnis mit der Kontrolle durch den Landesbeauftragten für den Datenschutz erklärt wird. Diese Genehmigung kann unverzüglich widerrufen werden, wenn der Zugriff Unbefugter auf diese Dateien oder sonstige Verstöße gegen Datenschutzbestimmungen festgestellt wurden.

---

66 vom 17. November 1994, ABl. MBJS S. 884

67 vom 3. Dezember 1995, ABl. MBJS 1995 S. 560

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

69 s. unter 5.2.1

70 vom 3. Dezember 1995, ABl. MBJS 1995 S. 560

Ich bedaure lediglich, daß das MBJS meine Idee, hierfür Standardprogramme zu verwenden, weder aufgegriffen noch dazu Stellung genommen hat.

5.3 Unterrichtung über Nichtbestehen der Feststellungsprüfung

Ausländische und staatenlose Studienbewerber, die nur über eine außerhalb des Geltungsbereiches des Grundgesetzes erworbene Studienbefähigung verfügen, müssen zur Aufnahme eines Studiums an einer deutschen Universität oder gleichgestellten Hochschule als Nachweis für die angestrebte Studienrichtung eine Feststellungsprüfung ablegen. Voraussetzung für die Zulassung ist, daß Prüflinge gem. § 3 Abs. 3 Feststellungsprüfungordnung (FestPO)[71] nicht bereits zweimal erfolglos an einem Studienkolleg teilgenommen haben.

Seit Anfang der 90iger Jahre wird in der Bundesrepublik Deutschland wiederholt ein Verfahren dafür erörtert, wie eine mißbräuchliche Inanspruchnahme dieser nur limitiert zur Verfügung stehenden Angebote (sog. Studienkollegs) verhindert werden kann, ohne daß die Betroffenen eine unverhältnismäßige Einschränkung ihres Rechts auf informationelle Selbstbestimmung hinnehmen müssen. Die Kultusministerkonferenz (KMK)[72] hat sich über die verschiedentlich geäußerten Bedenken der Landesbeauftragten für den Datenschutz hinweggesetzt und in einer Rahmenordnung für die Feststellungsprüfung unter Ziff. 4.10 beschlossen, daß sich Studienkollegs "über die Prüflinge, die die Feststellungsprüfung nicht bestanden haben, und über gefälschte Zeugnisse" gegenseitig informieren.

Vor diesem Hintergrund wurde in Brandenburg § 13 FestPO durch einen Abs. 3 ergänzt, der es dem Studienkolleg erlaubt, mit Einverständnis des Prüflings anderen Studienkollegs seinen Namen, Vornamen, Geburtsdatum und Herkunftsland zu übermitteln. Die Freiwilligkeit besteht allerdings darin - und deshalb halte ich die Verfahrensweise für problematisch -, daß der Prüfling auf dem Aufnahmebogen unterschreiben muß, daß seine personenbezogenen Daten bei Erforderlichkeit an andere Studienkollegs oder an Einrichtungen, deren Dienste er im Zusammenhang mit der Studienvorbereitung in Anspruch genommen hat, übermittelt werden dürfen. "Erforderlichkeit der Datenübermittlung besteht bei Nichtbestehen von Ausbildungsabschnitten und der Feststellungsprüfung bzw. bei Ausschluß aus dem Studienkolleg." Die Freiwilligkeit dieser Erklärung ist insofern zu verneinen, da diese zusammen mit dem Antrag auf Aufnahme in die entsprechende Bildungsinstitution eingeholt wird, der Prüfling aber nicht zugelassen werden würde, falls er seine "Einwilligung" verweigern sollte.

5.4 Sorgen von Lehrern, Schülern und Eltern

5.4.1 Unterrichtsstoff nach zentralen Vorgaben im Geschichtsunterricht

Zu Recht haben sich aus meiner Sicht Eltern wegen im Geschichtsunterricht der 5. Klasse eingesetzter Arbeitsblätter ("Die Reise in die Vergangenheit") empört und an mich gewandt, nachdem sie damit auf kein Verständnis bei der Schulleitung gestoßen waren. Die Schüler sollten hierbei Namen, ggf. Geburtsnamen, Geburts- und auch Todesdatum der näheren Verwandten (bis zu den Urgroßeltern) auflisten. Weder in der Petition noch von mir wird in Abrede gestellt, daß es didaktisch sehr dem Verständnis dieser Altersstufe entgegenkommt, wenn Kinder, die sich offensichtlich mit der geschichtlichen Zeitrechnung auseinandersetzen sollen, sich selbst in Verbindung mit Familiendaten als Bestandteil der Entwicklung der

---

71 vom 27. Juli 1993, GVBl. II S. 608

72 am 14./15. April 1994

menschlichen Geschichte verstehen lernen. Die Frage ist lediglich, ob hierzu das genaue Geburts- und Sterbedatum vonnöten bzw. überhaupt geeignet ist, diese pädagogische Absicht zu vermitteln oder ob nicht gerade die zu große Detailgenauigkeit eher davon ablenkt. Hinzu kommt, daß die Schüler dieser Altersstufe noch überhaupt keine Vorstellungen davon haben, daß personenbezogene Daten für Dritte unter Umständen begehrte Informationen darstellen können und insoweit grundsätzlich schutzwürdig sind.

Zu Recht stellte im übrigen die Eingabe darauf ab, daß die Verarbeitung personenbezogener Daten gem. § 4 Abs. 1 Bbg DSG nur zulässig ist, wenn dieses Gesetz oder ein anderes Gesetz bzw. eine Rechtsvorschrift dies erlauben oder der Betroffene zugestimmt hat. Keine der Voraussetzungen an eine Datenverarbeitung traf hier zu.

Insoweit habe ich es für sinnvoll erachtet, mich an das MBJS zu wenden und um Stellungnahme gebeten, ob es sich bei den in Rede stehenden Arbeitsblättern um von der Landesregierung erstelltes Lehrmaterial handelt, und ob sie meine datenschutzrechtlichen Bedenken hierzu teilt und insofern die weitere Verwendung dieser Arbeitsblätter reglementieren wird. Die Antwort des Ministeriums war unbefriedigend. Es hat zwar einerseits klargestellt, daß es sich in diesem Fall um pauschalgenehmigte Lernmittel gem. Nr. 4 a der VV Lernmittelzulassung[73] handelt, über deren Verwendung gem. § 15 Abs. 2 Nr. 1 Mitwirkungs-VO[74] die Fachkonferenz an der jeweiligen Schule entscheidet. Andererseits hat es als zuständiges Ministerium bisher - selbst auf erneutes Nachfragen - nicht für nötig befunden, die erbetene Stellungnahme zur Sache abzugeben.

5.4.2 Interne Schulbefragungen

Auf die Fragebogenaktion "Wie sehe ich meine Schule und meine Lehrer?" an einem Gymnasium in Brandenburg bin ich sowohl von der Schulkonferenz, der Schulleitung als auch der Lehrerschaft angesprochen und aus datenschutzrechtlicher Sicht um Stellungnahme gebeten worden. Die Schulkonferenz hatte die Fragebogenaktion initiiert und mit der Zielvorstellung vorbereitet, nach Lösungswegen zu suchen, wie an dieser Schule die Atmosphäre, die Kommunikation und die Arbeit der Mitwirkungsgremien zu verbessern wäre.

Es sei dahingestellt, ob für das beabsichtigte und durchaus unterstützenswerte Ziel nicht auch andere und möglicherweise sogar geeignetere Wege zur Umsetzung dieser Zielvorstellung in Frage kämen. Aus datenschutzrechtlicher Sicht ergaben sich zumindest aus dreierlei Gründen Bedenken gegen die beabsichtigte Verfahrensweise. Die Beteiligung von Schülern an einer solchen Befragung kann, soweit es sich nicht um Volljährige handelt, gem. Art 6 Abs. 2 Satz 1 Grundgesetz nur mit Einverständnis ihrer Eltern erfolgen, denn diesen steht nicht nur das Erziehungsrecht gegenüber den Kindern zu, sondern sie tragen auch die an diese Pflichten gebundene Verantwortung. Diese Zustimmung muß gem. § 4 Abs. 2 Bbg DSG schriftlich vorliegen und ist im vorab einzuholen. Soweit es Fragen insbesondere zum Unterricht betrifft, ist entscheidend, welche Bezugsbasis gewählt wird; beabsichtigt war hierfür, die einzelne Klasse bzw. den einzelnen Kurs zu wählen. Damit wären gem. § 3 Abs. 1 Bbg DSG personenbezogene Daten jeweils des unterrichtenden Lehrers erfaßt worden. Die Zulässigkeit dafür bestimmt sich aus § 4 Abs. 1 Bbg DSG, wonach nur personenbezogene Daten auf der Basis einer gesetzlichen Grundlage oder der Freiwilligkeit der Betroffenen (hier: Lehrer) erhoben und verarbeitet werden dürfen. Beides sah ich als nicht gegeben an. Schließlich bin ich der Ansicht, daß eine solche interne Fragebogenaktion an einer Schule nicht ohne Kenntnis der Aufsichtsbehörde (staatliches Schulamt) stattfinden kann. Sie ist zumindest darüber zu informieren.

---

73 vom 21. September 1992, ABl. MBJS S. 475, geänd. d. VV vom 7. Juli 1994, ABl. MBJS S. 768

74 vom 26. Juni 1991, GVBl. S. 293, geänd. d. VO v. 17. Juni 1993, GVBl. II S. 276

Der Schulleiterin habe ich deshalb vorgeschlagen, ausgehend von der Schulstundentafel Überlegungen anzustellen, welche Möglichkeiten es gäbe, speziell die Fragen zum Unterricht durch Zusammenfassung von Parallelzügen, Klassenstufen oder Fachgruppen auf eine abstraktere Ebene zu bringen, so daß nach den Grundsätzen der Statistik in der Regel mindestens drei Lehrer als Betroffene bei der Auswertung zugrunde liegen, und damit das mit der Fragebogenaktion beabsichtigte Ziel trotzdem noch zu erreichen ist. In dieser Form wäre es dann dem zuständigen staatlichen Schulamt zur Genehmigung vorzulegen. Die Schulleiterin hat diesen Vorschlag dankbar aufgenommen.

6 Wissenschaft, Forschung und Kultur

6.1 Forschung

6.1.1 Medizinisches Forschungsgeheimnis

Die Arbeitsgemeinschaft der Wissenschaftlichen Medizinischen Fachgesellschaften (AWMF) hat am 6. Mai 1995 in Frankfurt/Main eine Resolution zum medizinischen Forschungsgeheimnis verabschiedet. In dieser wird unterstellt, daß im Datenschutzrecht "unverantwortlich Blockaden medizinischer Forschung" bestünden, die unbedingt beseitigt werden müssen, um den Forschungsstandort Deutschland zu sichern und um "derzeitige datenschutzbedingte Blockaden, Hemmungen und Entmutigungen deutscher medizinischer Forschungen abzubauen, die vor allem zur Bekämpfung bedeutender Volkskrankheiten erforderlich" seien. Diese Blockaden seitens des Datenschutzes beträfen die Zusammenführung personenbezogener Daten aus verschiedenen Quellen, insbesondere "bei der in Deutschland unterentwickelten Epidemiologie". Diesen "deutschen Forschungsmängeln" stünde eine "blühende internationale Forschung" gegenüber. Als "Beispiele für einschlägige Datenschutzschäden" werden das Mannheimer Schizophrenieregister[75], das ehem. Nationale Krebsregister der DDR (s. unter 7.3.2.1) und ein nicht näher definiertes Diabetes-Register aufgeführt.

Nachdem ich Kenntnis von der Resolution des AWMF erhalten hatte, habe ich hierzu unmittelbar gegenüber dem Ministerium für Wissenschaft, Forschung und Kultur (MWFK) und dem Ministerium für Arbeit, Soziales, Gesundheit und Frauen eine gleichlautende Stellungnahme abgegeben und um deren Auffassung hierzu gebeten. Zu meinem Bedauern hat darauf noch keines der beiden Ministerien reagiert.

Wie bei allen datenschutzrechtlichen Problemen geht es auch hier um einen Interessenausgleich zwischen zwei Grundrechten: Freiheit der Forschung gem. Art. 5 Abs. 3 Grundgesetz (GG) und Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG. In solchen Fällen fordert das Grundgesetz, daß zwischen diesen eine Abwägung vorgenommen wird, daß nach dem "Prinzip der praktischen Konkordanz" die geschützten Güter einander so zugeordnet werden, daß jedes von ihnen Wirklichkeit gewinnt. Beiden Gütern müssen Grenzen gezogen werden, damit beide zu optimaler Wirksamkeit gelangen können[76]. Die Beteiligung des Betroffenen an einem medizinischen Forschungsprojekt auf der Basis - wie sie in § 28 Abs. 1 i. V. m. § 4 Abs. 1 Bbg DSG vorgesehen ist - stellt hierfür ein geeignetes Instrument dar.

Aus der Resolution geht nicht eindeutig hervor, ob den Verfassern die in allen Landesdatenschutzgesetzen enthaltenen Forschungsklauseln bekannt sind, die die Nutzung personenbezogener Daten auch ohne die Einwilligung des Betroffenen - allerdings nach

---

75 2. Tätigkeitsbericht LfD Baden-Württemberg, S. 10 - 30

76 BVerfGE 30, S. 195; 67, S. 228

einer Güterabwägung - erlauben (§ 28 Abs. 2 Bbg DSG). Daneben gibt es auch in den brandenburgischen Landesgesetzen (§ 28 Abs. 3 Nr. 11 Krankenhausgesetz[77] i. V. m. § 10 Krankenhausdatenschutzverordnung[78], § 10 Abs. 4 Brandenburgisches Archivgesetz[79]) sowie in einigen Bundesgesetzen (§ 8 Krebsregistergesetz[80], § 75 Sozialgesetzbuch X[81], Entwurf eines Unfallversicherungs-Einordnungsgesetzes[82]) spezialgesetzliche Forschungsklauseln, auf deren Grundlage nach dem gleichen Prinzip der Güterabwägung Eingriffe in das Recht auf informationelle Selbstbestimmung und Offenbarung des Arztgeheimnisses zulässig ist.

Offensichtlich geht die Resolution der AWMF davon aus, daß eine Kontrolle medizinischer Forscher nicht nur lästig, sondern sogar überflüssig ist. Und weiter: Die Abwägung der Geheimhaltungsinteressen der Patienten mit den Forschungsinteressen wäre besser in die Hände der Forschenden selbst gelegt und sollte notfalls den Ethik-Kommissionen der Medizinischen Fakultäten oder den Ärztekammern übertragen werden. Damit wird einer rechtlich und parlamentarisch-demokratisch nicht legitimierten und nicht transparenten Selbstkontrolle das Wort geredet, über deren Unwirksamkeit im Vergleich zu der Anzeigepflicht gegenüber dem Datenschutzbeauftragten gem. § 28 Abs. 2 Satz 4 Bbg DSG kein Zweifel besteht.

Die Resolution unterstellt zu Unrecht, daß der Datenschutz die "anonyme Forschungsnutzung" vormals personenbezogener Daten verhindere. Dies ist schon allein deshalb falsch, weil nach einer Anonymisierung die Wissenschaftler keinen datenschutzrechtlichen Restriktionen unterliegen; insoweit können auch anonymisierte Daten veröffentlicht und ggf. mit anderen Datenbeständen abgeglichen werden, was für personenbeziehbare Datensätze nicht zutrifft.

Der Vorschlag des AWMF, ein "medizinisches Forschungsgeheimnis" auf gesetzlicher Grundlage einzuführen, erübrigt sich, weil ein solches bereits existiert. Auch im Brandenburgischen Datenschutzgesetz gibt es in § 28 Abs. 2 Satz 2 eine entsprechende Zweckbindungsregelung: "Der Empfänger darf die übermittelten Daten nicht für andere Zwecke verwenden." Ansonsten ist die Verletzung des Forschungsgeheimnisses strafbewehrt und, soweit es medizinische Forschung durch Ärzte, Hilfspersonal und Auszubildende betrifft, gem. § 97 Abs. 2 StPO durch ein Beschlagnahmeverbot und gem. § 53 Abs. 1 Nr. 3 bzw. § 53a Abs. 1 StPO durch ein Zeugnisverweigerungsrecht abgesichert.

Darüber hinaus ist es als ein großes Mißverständnis anzusehen, wenn Mediziner meinen, die ärztliche Schweigepflicht ziele nur darauf ab, persönliche und gar intime Geheimnisse "Partnern, Verwandten, Bekannten, Freunden und Feinden, Kollegen, Arbeitgebern oder Behörden" vorzuenthalten, nicht aber dem "sehr kleinen Kreis Forschungsbeteiligter", der "in aller Regel desinteressiert" sei. Dieses Berufsgeheimnis gilt vielmehr auch gegenüber allen an der Behandlung unbeteiligten Ärzten. Wie anders soll sonst das personale Vertrauensverhältnis zwischen der hilfsbedürftigen und der helfenden Person zustandekommen und aufrechterhalten bleiben; Forschende haben darin nichts zu suchen.

Soweit es im übrigen die praktische Tätigkeit meiner Behörde bezüglich der Umsetzung des medizinischen Forschungsgeheimnisses anbelangt, so bin ich im Berichtszeitraum gebeten worden, zu drei Forschungsprojekten aus datenschutzrechtlicher Sicht Stellung zu nehmen. Die in diesem Zusammenhang gegebenen Hinweise beschränken sich auf nach meinen

---

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

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

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

80 vom 4 November 1994, BGBl. I S. 3351

81 vom 30. Juni 1995, BGBl. I S. 890

82 BT-Drs. 13/2204

Erfahrungen für Laien nicht nachzuvollziehende Formulierungen im vorbereiteten Informationsblatt zum Zweck der Untersuchung und den dafür vorgesehenen Untersuchungsparametern, die Rechtswirksamkeit der Einwilligungserklärung und einzuhaltende technisch-organisatorische Maßnahmen. Diese Verfahrensweise ist mir vor kurzem von einem der davon betroffenen Forscher ausdrücklich als eine "konstruktive Hilfestellung" bescheinigt worden.

6.1.2 Historische Forschung

Ein Petent wandte sich an mich, weil er als beauftragter Mitarbeiter für die Aufarbeitung der Vergangenheit eines Berliner Krankenhauses Einsicht in das Sterberegister einer brandenburgischen Gemeinde für den Zeitraum 1942 - 1945 wünschte, dies ihm - für ihn unverständlich - aber nicht gewährt wurde. Hieran bestehe nach seiner Aussage ein spezielles Interesse, weil während dieser Zeit in diesem Ort ein "Russenlager" existiert habe, in dem Pflegekräfte des Krankenhauses tätig gewesen seien. Die zuständige Kreisverwaltung habe ihm mit nachfolgender Begründung sein Anliegen verweigert: Gem. § 61 Personenstandsgesetz (PStG)[83] steht das Recht zur Benutzung der Personenstandseinträge bei Anwendung der Grundprinzipien des Datenschutzes nur Personen zu, auf die sich der Eintrag bezieht sowie deren Ehegatten, Vorfahren und Abkömmlingen. Andere Personen haben nur dann ein Recht dazu, wenn sie ein rechtliches Interesse glaubhaft machen oder die schriftliche Vollmacht eines Berechtigten vorlegen. § 61 PStG i. V. m. § 70 PStG gelte auch für Auskünfte aus Sammelakten. Damit war die augenblickliche Situation korrekt wiedergegeben, und auch ich konnte ihm aufgrund der Rechtslage bedauerlicherweise leider keine andere Auskunft erteilen.

Da es für mich nicht akzeptabel ist, dem Datenschutz auch hier ohne weiteres die Rolle des Verhinderers unterzuschieben, habe ich mich näher mit der Problematik beschäftigt. Interessanterweise gibt es dazu seit 1984 verschiedene Gerichtsurteile. Beispielhaft sei hier lediglich auf ein Urteil des AG Frankenthal[84] hingewiesen, worin dieses selbst einem Universitätsprofessor - obwohl seine Einrichtung als Körperschaft des öffentlichen Rechts zwar unter den Behördenbegriff gem. § 61 PStG falle - nicht zugestanden hat, zum Zwecke statistischer Erhebungen im Rahmen eines Forschungsprojektes "Soziale Mobilität und Heiratsverhalten - Deutschland im 19. und 20. Jahrhundert" in Personenstandsbücher einzusehen. Es hat aber unter Berücksichtigung der vom Bundesverfassungsgericht im "Volkszählungsurteil"[85] aufgestellten Grundsätze empfohlen, die Vorschriften des § 61 PStG entsprechend zu ändern oder zu ergänzen.

Auch anderweitig ist das unbefriedigend gelöste Problem sehr wohl bekannt. So habe ich herausgefunden, daß selbst über die Notwendigkeit einer Überarbeitung des § 61 PStG zwischen dem Bundesministerium des Innern und dem Bundesbeauftragten für den Datenschutz seit Jahren Konsens besteht. In den hierzu vorliegenden Vorschlägen orientiert man sich an archivrechtlichen Verfahrensweisen (Schutzfristen), womit das in Art. 2 Abs. 1 GG gewährleistete Grundrecht auf freie Entfaltung des Persönlichkeit vollständig Beachtung findet. Es wirkt nach dem Tod der Person nicht mehr fort, weil Träger dieses Grundrechts nur eine lebende Person ist[86] und somit mit dessen Tod der Schutz aus diesem Grundrecht erlischt. Das Grundrecht aus Art. 2 Abs. 1 GG setzt die Existenz einer wenigstens potentiell oder zukünftig handlungsfähigen Person unabdingbar voraus. Die Versagung eines Persönlichkeitsschutzes nach dem Tode stellt dagegen keinen Eingriff dar, der die in Art. 2 Abs. 1 GG gewährleistete Handlungs- und Entscheidungsfreiheit voraussetzt.

---

83 vom 3. November 1937, RGBl. I S. 1146 i. d. Fass. vom 8. August 1957, BGBl. I S. 1125

84 vom 30. Januar 1985, III 41/84

85 BVerfGE 65, S. 1

86 BVerfGE 30, S. 194

Vor diesem Hintergrund habe ich sowohl das Ministerium des Innern als auch das MWFK gebeten, sich im Rahmen ihrer Möglichkeiten für eine derartig erweiterte Nutzungsmöglichkeit von Personenstandsbüchern für wissenschaftliche Zwecke einzusetzen.

6.1.3 Verwaltungsvorschriften zum Brandenburgischen Archivgesetz lassen warten

In ihrer Stellungnahme zu meinem 3. Tätigkeitsbericht bestätigte mir die Landesregierung[87], daß hinsichtlich der Schaffung einer Regelung auf der Grundlage von § 17 Abs. 2 Brandenburgisches Archivgesetz (BbgArchivG)[88] Bedarf "angesichts eines Zielkonflikts zwischen den Benutzerinteressen und der Wahrung schutzwürdiger Belange Dritter" besteht. Entsprechende Vorschriften "werden gegenwärtig vorbereitet".

Die übereinstimmende Beurteilung des Problems sowie dessen in Aussicht gestellte Lösung habe ich zum Anlaß genommen, beim MWFK nach dem Stand der diesbezüglichen Entwürfe nachzufragen. Zu meinem großen Erstaunen erhielt ich drei Monate später die Auskunft, daß hierzu noch nichts vorliege; im übrigen sei mit konkreten Entwürfen nicht vor Mitte Mai 1996 zu rechnen. Der darauf angesprochene Minister hat mir nunmehr versichert, sich darum persönlich kümmern zu wollen. Über den Fortgang der Dinge werde ich zu gegebener Zeit berichten.

Unabhängig davon bin ich im vergangenen Jahr gebeten worden, auf dem 4. Brandenburgischen Archivtag einen Beitrag über "Archivwesen und Datenschutz" zu halten, der zwischenzeitlich veröffentlicht worden ist[89]. Da hier die Thematik ausführlich behandelt ist, könnten Teile davon in die zukünftigen Regelungen einfließen.

6.2 Hochschulangelegenheiten

6.2.1 Vorlage eines ärztlichen Attestes für die Immatrikulation

Ein Petent teilte mir mit, daß die Technische Fachhochschule Wildau (TFH) von Bewerbern verlangt, als eine der Zulassungsvoraussetzungen ein ärztliches Gesundheitsattest vorzulegen, und bat mich um Prüfung der Rechtslage hierfür.

Die Fachhochschule wurde daraufhin meinerseits um Stellungnahme gebeten und führte die diesbezügliche Regelung in § 2 Abs. 3 Nr. 4 ihrer Immatrikulationsordnung (Stand: September 1992) auf die Übernahme einer Muster-Ordnung von Niedersachsen aus dem Jahre 1990 zurück. Darin ist in § 4 Abs. 2 Nr. 2 die Versagung der Immatrikulation möglich, wenn "der Bewerber an einer Krankheit i. S. d. § 45 Abs. 1 Bundesseuchengesetz (BSeuchenG)[90] leidet oder trotz des Verdachtes einer solchen Krankheit ein gefordertes amtsärztliches Zeugnis nicht beibringt". Da sich § 45 Abs. 1 BSeuchenG jedoch abschließend nur auf "Lehrer, zur Vorbereitung auf den Beruf des Lehrers in Schulen tätige Personen, Schüler, Schulbedienstete und in Schulgebäuden wohnende Personen" bezieht, kann somit dieser Paragraph nicht als eine gesetzliche Grundlage zur Datenverarbeitung für einen anderen Personenkreis herangezogen werden. Ich kann darüber hinaus auch keine Erforderlichkeit der Vorlage eines ärztlichen Attests selbst in allgemeinster Form für Zwecke der Immatrikulation erkennen, soweit es sich nicht um Studiengänge bzw. künftige Berufe handelt, deren Ausübung (auch Ableistung von Praktika) in der Regel

---

87 LT-Drs. 2/1834, S. 20

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

89 Brandenburgische Archive, Heft 6/95, S. 12 f.

90 i. d. Fass. vom 18. Dezember 1979, BGBl. I S. 2262, ber. BGBl. 1980 I S. 151

Mindestanforderungen an die körperliche Konstitution der Betroffenen voraussetzt.

Dies habe ich dem MWFK, das für die Genehmigung von Immatrikulationsordnungen gem. § 39 Abs. 6 BbgHG zuständig ist, mitgeteilt und um Abhilfe in bezug auf künftige Beschwerden über die TFH Wildau gebeten. Darüber hinaus habe ich es im Sinne des Gleichheitsgrundsatzes aufgefordert, mir sämtliche Immatrikulationsordnungen der Fachhochschulen und Universitäten für Prüfungszwecke zur Verfügung zu stellen. Dabei fanden sich vergleichbare Regelungen in den Immatrikulationsordnungen der Universität Potsdam (Sportwissenschaft) und der FH Eberswalde.

Erfreulicherweise hat sich das Ministerium meiner Meinung angeschlossen und mir mitgeteilt, daß es seinerseits die TFH Wildau und die Fachhochschule Eberswalde aufgefordert habe, in ihren Immatrikulationsordnungen die Passagen gänzlich zu streichen bzw. - als nur zutreffend für den Studiengang Forstwirtschaft - zu präzisieren. Über die Umsetzung dieser Auflagen werde ich ggf. zu einem späteren Zeitpunkt berichten.

6.2.2 Datenerhebung im Rahmen der Promotion

Bereits 1994 war ich mit diesem Problem an das MWFK herangetreten. Dieses teilte mir daraufhin mit, daß es ebenfalls den Standpunkt vertrete, Lebensläufe seien lediglich bei der Beantragung der Zulassung zum Promotionsverfahren mit Angaben, die sich auf den Ausbildungs-, beruflichen und wissenschaftlichen Werdegang beziehen, abzufordern. Darüber hinausgehende personenbezogene Daten seien für die Durchführung des Promotionsverfahrens nicht erforderlich. Promovenden solle es im übrigen freigestellt bleiben, mit ihrer Dissertation zugleich auch ihren akademischen Lebenslauf zu veröffentlichen.

Um zu prüfen, ob und inwieweit diese Verfahrensweise im Land Brandenburg umgesetzt ist, bat ich im Berichtszeitraum das MWFK, das nach § 22 Abs. 2 BbgHG die Promotionsordnungen zu genehmigen hat, mir die Promotionsordnungen der hiesigen Universitäten bzw. deren Fakultäten zur Verfügung zu stellen. Zu meinem Erstaunen stellten sich bei deren Durchsicht mehrheitlich Anhaltspunkte auf datenschutzrechtliche Mängel heraus.

Soweit überhaupt Promotionsordnungen vorliegen, entsprechen diese in mehreren Punkten nicht dem Erforderlichkeitsgrundsatz nach § 12 Abs. 1 Bbg DSG. Dieser besagt, daß personenbezogene Daten nur verarbeitet werden dürfen, wenn diese zur Aufgabenerfüllung und für einen damit verbundenen Zweck erforderlich sind. Wenn also - fast wörtlich übereinstimmend - in den mir vorgelegten Promotionsordnungen der Zweck einer Dissertation "als Nachweis einer wissenschaftlichen Leistung und der Fähigkeit des Bewerbers zur selbständigen sowie vertieften wissenschaftlichen Arbeit" definiert wird, dann verstoßen verschiedene, vom MWFK genehmigte Promotionsordnungen in Teilen gegen den Erforderlichkeitsgrundsatz.

Dies trifft zunächst einmal für die Promotionsordnungen zu, die vorschreiben, daß den Pflichtexemplaren der Dissertation ein Lebenslauf des Promovenden als Anlage beizufügen ist; denn einerseits können sich Prüfer anhand des in der Prüfungsakte beigefügten Lebenslaufes über den beruflichen Werdegang des Doktoranden informieren, andererseits wären dabei auch die Voraussetzungen des § 16 Abs. 1 Bbg DSG nicht erfüllt. Danach dürfen öffentliche Stellen zwar unabhängig von ihrer Aufgabenerfüllung privaten Dritten personenbezogene Daten übermitteln, wenn die Voraussetzungen einer der dort aufgeführten Alternativen erfüllt sind. Zumindest muß gem. § 16 Abs. 1 Alternative d Bbg DSG der Empfänger eine berechtigtes Interesse an der Kenntnis der Daten geltend machen. Jedoch dürfen keine Anhaltspunkte dafür bestehen, daß schutzwürdige Belange der Betroffenen durch die Veröffentlichung beeinträchtigt werden können. Selbst wenn man von einem berechtigten Interesse der Leser einer Dissertation ausgeht, den Lebenslauf des

Promovenden zu erfahren, kann von der zweiten Alternative nicht ohne weiteres ausgegangen werden.

In der Mehrzahl der Promotionsordnungen wird als Voraussetzung für eine Zulassung zum Promotionsverfahren ein ordnungsgemäßes Studium (entsprechender Fachrichtung) an einer Universität oder gleichgestellten Hochschule im Geltungsbereich des Hochschulrahmengesetzes genannt. Dies setzt in der Regel voraus, daß eine Hochschulzugangsberechtigung vorgelegen hat. Deshalb dürfte es regelmäßig auch nicht nötig sein, ein Reifezeugnis für ein Promotionsverfahren vorzulegen.

Während ich inzwischen in bezug auf die Veröffentlichung der Lebensläufe mit dem MWFK ein Einvernehmen erzielen konnte und dies mir zugesagt hat, die entsprechenden Universitäten aufzufordern, ihre Promotionsordnungen entsprechend abzuändern, begründet das Ministerium die Nachweise schulischer und beruflicher Abschlüsse mit "gängiger Verwaltungspraxis". Dies ist aus meiner Sicht auf keinen Fall zu akzeptieren; denn Tradition kann kein Argument sein, ein rechtswidriges Verwaltungsverfahren zu legalisieren. Eine abschließende Äußerung hierzu seitens des Ministeriums liegt mir bisher trotz mehrfacher Bitten nicht vor. Zu gegebener Zeit werde ich darüber erneut berichten.

6.2.3 Verwendung der Matrikelnummer als Ordnungsmerkmal

Aufgrund der Eingabe eines Petenten aus dem Hochschulbereich wurde ich auf folgende Datenverarbeitungspraxis aufmerksam gemacht:

In allgemein zugängigen Gebäudeteilen der Hochschule werden Listen mit Prüfungsergebnissen und anderen Noten ausgehängt. Auf den Listen wird zur Anonymisierung die jeweilige Matrikelnummer anstatt des Namens des Betroffenen angegeben. Das Verfahren ist dabei nur akzeptabel, wenn Dritte keine Möglichkeit erhalten, von der Matrikelnummer auf die jeweilige Person schließen zu können. Der Bezug zwischen Matrikelnummer und Namen des Betroffenen war jedoch durch die im Netzwerk der Hochschule angemeldeten Studenten relativ leicht herstellbar. Ich habe die Hochschule daher aufgefordert, für die im Hochschulnetz benötigten Ordnungsmerkmale andere wahlfreie Nummern anstatt der Matrikelnummern zu verwenden.

7 Arbeit, Soziales, Gesundheit und Frauen

7.1 Soziales

7.1.1 Neue Gesetze und Verordnungen

7.1.1.1 Gesetz zur Änderung des Sechsten Buches Sozialgesetzbuch (SGB VI) und anderer Gesetze

Die Novellierung der Bestimmungen zur Rentenversicherung im Sozialgesetzbuch und damit in Zusammenhang stehender Gesetze ist Ende vergangenen Jahres mit Zustimmung des Bundesrates mit dem Gesetz zur Änderung des Sechsten Buches Sozialgesetzbuch (SGB VI) und anderer Gesetze[91] abgeschlossen worden.

---

[91] vom 15. Dezember 1995, BGBl. I S. 1824

- Änderung des Sozialgesetzbuches VI (Rentenversicherung)

Zur Neufassung des SGB VI hatten die Datenschutzbeauftragten im wesentlichen Änderungen zu zwei Punkten angeregt.

Zum einen erschien in § 148 Abs. 1 Satz 1 SGB VI eine Anpassung an das neuere Datenschutzrecht notwendig. Die Vorschrift stammte aus der Zeit des alten Bundesdatenschutzgesetzes, das zum einen das Erheben von Daten nicht regelte und die Datenverarbeitung und -nutzung nur, soweit sie dateimäßig erfolgte. Diesem Vorschlag hat der Gesetzgeber entsprochen.

Zum anderen war bereits seit längerem diskutiert worden, ob eine Verpflichtung der Geldinstitute geschaffen werden sollte, gegenüber dem Rentenversicherungsträger oder der die Rente auszahlenden Stelle die Person namhaft zu machen, die über Geldleistungen, die noch nach dem Tode des Rentenempfängers erbracht wurden, verfügt und damit eine Rücküberweisung der überzahlten Rente verhindert hat. Eine solche Regelung ist nunmehr in § 118 Abs. 4 SGB VI enthalten. Bisher hatten die Sozialversicherungsträger einen erheblichen Verwaltungsaufwand zu betreiben, um über Anfragen bei Krankenkassen, Nachlaßgerichten und sonstigen Stellen zu ermitteln, wer sich zu Unrecht bereichert hatte. Die Datenschutzbeauftragten haben deshalb grundsätzlich eine Lösung begrüßt, durch die die Versicherungsträger in die Lage versetzt werden, mit vertretbarem Aufwand die überzahlten Beträge zugunsten der Solidargemeinschaft zurückzufordern, indem die Auskunftspflicht der Geldinstitute in § 118 Abs. 4 SGB VI aufgenommen wurde. Ihren Wunsch nach einer konkreteren und alle denkbaren Fälle umfassenden Formulierung dieser Auskunftspflicht konnten die Datenschutzbeauftragten jedoch nicht durchsetzen.

- Änderung des § 620 Reichsversicherungsordnung (Unfallversicherung)

Für den Fall, daß über Geldleistungen des Trägers der Unfallversicherung, die für die Zeit nach dem Tode des Berechtigten zu Unrecht auf ein Konto im Inland überwiesen worden waren, anderweitig verfügt wurde, ist nunmehr in § 620 Abs. 4 Reichsversicherungsordnung (RVO)[92] eine dem § 118 Abs. 4 SGB VI entsprechende Regelung getroffen worden.

- Änderung des Bundesversorgungsgesetzes

Für Leistungen aufgrund einer gesundheitlichen Schädigung im Sinne des Bundesversorgungsgesetzes (BVG)[93] gilt gem. § 66 Abs. 2 Satz 4 BVG, § 118 Abs. 4 SGB VI entsprechend.

7.1.1.2 Unfallversicherungseinordnungsgesetz (SGB VII)

Durch das Unfallversicherungseinordnungsgesetz sollen die bisher in der Reichsversicherungsordnung enthaltenen Regelungen über die gesetzliche Unfallversicherung in das Sozialgesetzbuch überführt und aktualisiert werden. Der Entwurf des Unfallversicherungseinordnungsgesetzes war Gegenstand eines Beschlusses der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder[94]. Seitens der Datenschutzbeauftragten wurden zum einen Grundsatzanforderungen deutlich gemacht, zum anderen weitreichende Formulierungsvorschläge in das Gesetzgebungsverfahren eingebracht. Außerdem habe ich mich mit einer Stellungnahme an das hiesige Ministerium für Arbeit, Soziales, Gesundheit und Frauen (MASGF) gewandt und um Unterstützung

---

92 i. d. Fass. vom 15. Dezember 1924, RGBl. I S. 779

93 vom 22. Januar 1982, BGBl. I S. 21

94 s. 3. Tätigkeitsbericht, Anlage 14

wegen wesentlicher Bedenken gebeten, die vielfach in einer Nichtbeachtung der datenschutzrechtlichen Grundsätze der Erforderlichkeit und der Transparenz für den Betroffenen begründet waren.

7.1.1.3 Pflegeversicherung: Pflegebedürftigkeitsrichtlinien

Zur Abgrenzung der Merkmale der Pflegebedürftigkeit und der Pflegestufen sowie zum Verfahren der Feststellung der Pflegebedürftigkeit haben die Spitzenverbände der Pflegekassen aufgrund von § 17 SGB XI[95] i. V. m. § 213 SGB V[96] sogenannte Pflegebedürftigkeitsrichtlinien (PflRi) beschlossen. Diese liegen nunmehr in der geänderten Fassung vom 21. Dezember 1995 vor, der das Bundesministerium für Arbeit und Sozialordnung mit Schreiben vom 29. Dezember 1995 seine Genehmigung erteilt hat.

In den bereits im 3. Tätigkeitsbericht[97] kritisierten Punkten blieben die Regelungen im wesentlichen unverändert.

7.1.2 Aktuelle Fälle

7.1.2.1 Offenbarung von Sozialdaten auf Überweisungsträgern

Mit Urteil vom 23. Juni 1994 hat das Bundesverwaltungsgericht[98] entschieden, daß es unzulässig sei, bei der Auszahlung von Sozialhilfe die Überweisungsträger generell ohne Zustimmung des Sozialhilfeempfängers mit dem Vermerk "Sozialleistung" zu kennzeichnen. Auf dieses Urteil habe ich die Ministerien für Arbeit, Soziales, Gesundheit und Frauen (MASGF), für Bildung, Jugend und Sport (MBJS) sowie für Wissenschaft, Forschung und Kultur (MWFK) hingewiesen und darum gebeten, zu veranlassen, daß innerhalb ihres Zuständigkeitsbereiches dieses Urteil beachtet wird.

Von den Sozialämtern, die über das MASGF informiert worden waren, kamen nur vereinzelte Rückmeldungen. Dabei konnte festgestellt werden, daß sie teilweise die Vorgaben des Bundesverwaltungsgerichts bereits einhielten; in anderen Fällen erfolgte eine Anpassung an diese Rechtsprechung. Ich habe das MASGF gebeten zu klären, ob und wie die von ihm darüber hinaus angeschriebenen Sozialämter das Urteil umsetzen.

Das MBJS hat sich ausführlich mit der Problematik befaßt und sich bereit erklärt, Empfehlungen an die Jugendämter abzugeben, zu denen ich lediglich geringfügige Änderungen vorzuschlagen hatte, die aber bedauerlicherweise noch nicht aufgegriffen wurden. Das MBJS hat vielmehr mitgeteilt, daß bereits die von ihm vorgeschlagenen Formulierungen bzw. Abkürzungen eine Arbeitserschwerung für die Jugendämter beinhalteten, weshalb zunächst eine Erprobungsphase stattfinden solle.

Die AOK Brandenburg vertrat zunächst die Ansicht, daß das Urteil des Bundesverwaltungsgerichts im Bereich der gesetzlichen Krankenversicherung nicht einschlägig sei. Das MASGF teilte jedoch meine Auffassung und forderte die AOK auf, die dem Bundesverwaltungsgerichtsurteil entsprechende Verfahrensweise künftig sicherzustellen. Die AOK hat sich inzwischen bereit erklärt - außer für die Fälle, in denen Empfänger der Leistungen Dritte sind -, eine datenschutzgerechte Formulierung zu wählen. In der Mehrzahl der Fälle findet dementsprechend die Entscheidung des Bundesverwaltungsgerichts weiterhin keine Beachtung. Nähere Erläuterungen hat die AOK

---

95 vom 1. Januar 1995, BGBl. 1994 I S. 1014

96 vom 20. Dezember 1988, BGBl. I S. 2477

97 s. unter 7.1.2.6

98 Az.: 5 C 16.92, RdV 1995 S. 28 f.

hierzu nicht abgegeben. Das MASGF hat seine Bereitschaft signalisiert, sich bezüglich des weiteren Vorgehens in dieser Angelegenheit mit mir zu verständigen.

Seitens des MWFK wurde mitgeteilt, dem Begehren, die Kennzeichnung der Überweisungsträger mit dem Namen des Sozialleistungsgesetzes "BAföG" zu unterlassen, stehe eine zum Bundesausbildungsförderungsgesetz (BAföG)[99] ergangene Verwaltungsvorschrift entgegen, die die Bundesregierung mit Zustimmung des Bundesrates erlassen habe. Der Bundesbeauftragte für den Datenschutz wurde daher gebeten, sich für eine Änderung der Verwaltungsvorschrift einzusetzen.

7.1.2.2 Offenbarung der Diagnose an den Arbeitgeber bei Arbeitsbefreiung wegen Betreuung eines erkrankten Kindes

Krankenversicherte haben nach § 45 Abs. 1 SGB V "Anspruch auf Krankengeld, wenn es nach ärztlichem Zeugnis erforderlich ist, daß sie zur Beaufsichtigung, Betreuung oder Pflege ihres erkrankten und versicherten Kindes der Arbeit fernbleiben, eine andere in ihrem Haushalt lebende Person das Kind nicht beaufsichtigen, betreuen oder pflegen kann und das Kind das zwölfte Lebensjahr noch nicht vollendet hat". Für die Dauer dieses Anspruchs haben diese Versicherten gem. § 45 Abs. 3 SGB V ebenfalls "gegen ihren Arbeitgeber Anspruch auf unbezahlte Freistellung von der Arbeitsleistung, soweit nicht aus dem gleichen Grund Anspruch auf bezahlte Freistellung besteht".

Für die Gewährung des o. g. Krankengeldes benötigen die Krankenkassen ein ärztliches Zeugnis. Dieses enthielt früher die Diagnose des erkrankten Kindes, wogegen datenschutzrechtliche Bedenken bestanden. Seit dem 1. Januar 1995 steht ein neuer Vordruck ohne diese Angabe zur Verfügung, der im Bereich der Kassenärztlichen Vereinigung Brandenburg von den Ärzten verwendet wird.

Die für die Krankenkasse gedachte Bescheinigung wird in der Praxis häufig zugleich als Nachweis gegenüber dem Arbeitgeber genutzt. Auch wenn sich die Diagnose inzwischen nicht mehr aus der Bescheinigung ergibt, enthält diese immer noch Daten, deren Kenntnis für den Arbeitgeber nicht notwendig ist, z. B. die Angabe, ob ein Unfall für die Erkrankung ursächlich war. Ich habe deshalb einen Vorschlag des Sächsischen Datenschutzbeauftragten zur Einführung eines durchschreibfähigen Vordrucks - wie er auch bei Krankschreibungen von Arbeitnehmern verwendet wird - unterstützt, der auch ein für den Arbeitgeber bestimmtes Exemplar vorsieht, das aber nur die für diesen erforderlichen Daten enthält.

7.1.2.3 Forschungsvorhaben einer Krankenkasse

Das MASGF teilte mir mit, daß eine der Landesaufsicht unterstehende Betriebskrankenkasse die aufsichtsbehördliche Zustimmung zu einem Forschungsvorhaben nach § 287 SGB V begehre. Im Rahmen dieses Forschungsvorhabens sollte ein betrieblicher Gesundheitsbericht erarbeitet werden, aus dem sich die Krankenkasse Erkenntnisse über Zusammenhänge zwischen Erkrankungen und Arbeitsbedingungen erhoffte. Für die Auswertung sollten die Daten durch den Datenschutzbeauftragten des Arbeitgeberbetriebes verschlüsselt und an eine externe Firma übergeben werden.

Das Ministerium teilte mir mit, der Genehmigung des Vorhabens aus mehreren Gründen zurückhaltend gegenüberzustehen. Das Vorhaben sei nicht wie in § 287 SGB V gefordert, zeitlich und hinsichtlich des Umfangs begrenzt. Mit den geplanten Auswertungen werde nach seinem Eindruck die in § 287 SGB V gebotene Beschränkung auf leistungserbringer- oder fallbeziehbare Daten überschritten. Auch hielt das MASGF eine Fremdauswertung der Daten für unzulässig. Es bat mich deshalb zu den Vorhaben um eine gutachterliche

---

[99] vom 6. Juni 1983, BGBl. I S. 64

Stellungnahme.

Die vom Ministerium gegen das Forschungsvorhaben vorgetragenen Kritikpunkte teilte ich. Darüber hinaus hatte ich jedoch noch weitere Bedenken. Es sollte zwar eine Verschlüsselung der Daten bei der Krankenkasse erfolgen, dies aber durch den Datenschutzbeauftragten des Arbeitgebers, wodurch der Sinn der Verschlüsselung teilweise wieder zunichte gemacht worden wäre. Außerdem war wegen der Erfassung paralleler Daten in verschiedenen Datensätzen eine relativ einfache Herstellung der Personenbeziehbarkeit nicht auszuschließen. Insgesamt habe auch ich mich deshalb gegen eine Genehmigung des Forschungsvorhabens ausgesprochen.

7.1.2.4 Keine Befugnis des Vertragsarztes zur Übermittlung des Krankenhausentlassungsberichtes an das Versorgungsamt?

Ein mit dieser Überschrift lautendes Rundschreiben des Bundesverbandes der Internisten führte zu entsprechenden Reaktionen von Ärzten gegenüber dem Landesamt für Soziales und Versorgung, das mich daher um Stellungnahme bat.

Die Versorgungsverwaltung benötigte im Rahmen von Feststellungsverfahren nach dem Schwerbehindertengesetz (SchwbG)[100] Krankenunterlagen der Antragsteller. Als einschlägige Rechtsgrundlage kommt § 4 Abs. 1 SchwbG i. V. m. § 12 Abs. 2 Satz 1 und 3 des Gesetzes über das Verwaltungsverfahren der Kriegsopferversorgung (KOVVfG)[101] in Betracht. Danach kann die Verwaltungsbehörde mit Einverständnis oder auf Wunsch des Antragstellers oder Versorgungsberechtigten von privaten Ärzten, die den Antragsteller oder Versorgungsberechtigten behandeln oder behandelt haben, Auskünfte einholen und Untersuchungsunterlagen zur Einsicht beiziehen. Da die Einverständniserklärung alle bei einem Arzt befindlichen ärztlichen Unterlagen des Betroffenen umfaßt, nämlich sowohl die von ihm selbst als auch die von anderen Ärzten erstellten und ihm im Rahmen der Behandlung überlassenen Behandlungsunterlagen, bestehen keine Bedenken dagegen, Unterlagen anderer behandelnder Ärzte, die sich bei dem angeschriebenen Arzt befinden, wie z. B. Facharzt- und Krankenhausentlassungsberichte, zu übersenden. Somit ist das Ersuchen des Versorgungsamtes um das Beifügen der Unterlagen anderer Ärzte durch die Einwilligung in genau dem gleichen Umfang gedeckt wie das Ersuchen um die Offenbarung der Unterlagen des ersuchten Arztes selbst. Die Einwilligungserklärungen sollten daher auf jeden Fall den Hinweis enthalten, daß diese auch Auskünfte und Unterlagen umfassen, die von anderen Ärzten oder Stellen erstellt sind.

Angefordert werden können jedoch nur die Unterlagen, die für die in dem Fragebogen genannte Fragestellung erforderlich sind. Die ärztliche Schweigepflicht zwingt den Arzt vor der Übermittlung aller bei ihm vorhandenen Unterlagen, diese auf ihre Erforderlichkeit für die genannte Fragestellung zu prüfen.

Dabei ist zu berücksichtigen, daß die Krankenhausentlassungsberichte, die insbesondere dem nachbehandelnden Arzt als Grundlage für die weitere Behandlung dienen, Informationen enthalten, die zum Teil nur für den nachbehandelnden Arzt relevant und für die Aufgabenerfüllung der Versorgungsämter nicht erforderlich sind. Deshalb muß im Einzelfall geprüft werden, ob lediglich Auskünfte an die Versorgungsämter auf deren gezielte Fragen gegeben werden können.

---

100 i. d. Fass. vom 26. August 1986, BGBl. I S. 1421

101 i. d. Fass. vom 6. Mai 1976, BGBl. I S. 1169

7.1.2.5 Datenübermittlungsbefugnisse im Rahmen von Verfahren nach dem Opferentschädigungsgesetz

Im Rahmen einer gerichtlichen Klärung eines Opferentschädigungsverfahrens hatte die AOK Brandenburg mich um Stellungnahme gebeten, ob die Versorgungsverwaltung im Wege der Amtsermittlung gem. § 20 SGB X[102] eine Sachverhaltsaufklärung auch ohne Schweigepflichtentbindungserklärung des Betroffenen durchführen könne.

Das von der AOK in dem Verfahren verwandte Formular enthielt zwei Seiten mit 12 Fragen, an die sich in Kleindruck am untersten Rand des Textes, jedoch noch über dem Feld für die Unterschrift und unmittelbar nach der Erklärung, die Fragen wahrheitsgemäß beantwortet zu haben, eine Erklärung über die Entbindung von der ärztlichen Schweigepflicht anschloß. Hierzu hatte ich gegenüber der AOK ausgeführt, daß gegen diese "Schweigepflichtentbindungserklärung" schon wegen der äußeren Form - insbesondere wegen des speziellen Kleindrucks - Bedenken bestehen. Im Gegenteil verlangt nämlich § 67 b Abs. 2 Satz 3 SGB X, daß eine Einwilligungserklärung, die im Zusammenhang mit anderen schriftlichen Erklärungen steht, im äußeren Erscheinungsbild besonders hervorzuheben ist.

Eine Anwendung von Vorschriften des SGB X, die eine Übermittlung auch ohne ausdrückliche Schweigepflichtentbindungserklärung zugelassen hätten, mußte meines Erachtens wegen des über § 6 Abs. 3 Opferentschädigungsgesetz (OEG)[103] primär einschlägigen § 12 Abs. 2 des Gesetzes über das Verwaltungsverfahren der Kriegsopferversorgung (KOVVfG)[104], der eine Einbeziehung von Krankenunterlagen und ähnlichem durch die Versorgungsverwaltung vom Einholen einer Einwilligungserklärung des Betroffenen abhängig macht, unterbleiben.

7.1.2.6 Anforderung von Krankenunterlagen durch eine Krankenkasse

Ein Krankenhaus hatte sich wegen einer Auseinandersetzung mit einer Krankenkasse an mich gewandt. Dem Fall lag folgender Sachverhalt zugrunde:

Bei stationären Behandlungen werden Kosten regelmäßig zunächst für eine bestimmte Verweildauer zugesagt. Eine Verlängerung der Kostenzusage setzt, sofern die Krankenkasse dies verlangt, eine medizinische Begründung durch die Ärzte für die Notwendigkeit einer Verlängerung der stationären Behandlung des Patienten voraus. Diese kann die Krankenkasse durch den Medizinischen Dienst gutachterlich prüfen lassen, dem gem. § 276 Abs. 2 SGB V auf seine Aufforderung hin die entsprechenden Sozialdaten von den Leistungserbringern unmittelbar zu übermitteln sind.

Die Krankenkasse forderte nun selbst bei den Krankenhäusern Krankenunterlagen an. Sie erklärte hierzu, der Medizinische Dienst der Krankenkassen (MDK) beauftrage in der Regel die Geschäftsstelle der Krankenkasse, so zu verfahren; ggf. könnten der Krankenkasse die Unterlagen auch in einem verschlossenen Umschlag zugesandt werden. Bei allem sei zu berücksichtigen, daß die Einschaltung des MDK im Ermessen des Bearbeiters bei der Krankenkasse liege und dieser auch der gutachterlichen Empfehlung nicht folgen müsse.

Ich habe die Krankenkasse darauf hingewiesen, daß die Daten, die die Krankenhäuser den Krankenkassen zulässigerweise übermitteln dürfen, in § 301 Abs. 1 SGB V abschließend aufgezählt sind. Krankenunterlagen gehören nicht zu den dort genannten Daten. Außerdem

---

102 vom 13. Juni 1994, BGBl. I S. 1229

103 vom 7. Januar 1985, BGBl. I S. 1

104 i. d. Fass. vom 6. Mai 1976, BGBl. I S. 1169

sieht § 276 Abs. 2 SGB V eine Datenübermittlung nur unmittelbar zwischen Leistungserbringer und MDK vor. Dies schließt die Zulässigkeit der Zusendung von Unterlagen selbst in einem verschlossenen Umschlag über die Krankenkasse aus, zumal dabei die Gefahr eines versehentlichen unbefugten Öffnens bei der Krankenkasse besteht. Insgesamt dürfen auch dem MDK nur die zu seiner Aufgabenerfüllung erforderlichen Unterlagen zugänglich gemacht werden.

7.2 Gesundheitswesen

7.2.1 Chipkarten im Gesundheitswesen

Im Zusammenhang mit der Darstellung der seit Anfang 1995 gem. § 291 Abs. 1 SGB V eingeführten Krankenversichertenkarte für Versicherte der gesetzlichen Krankenversicherungen hatte ich bereits darauf hingewiesen, daß weitere Anwendungen von Chipkarten im Gesundheitswesen zu erwarten sind. Ich hatte bereits damals laufende Projekte mit Patientenkarten erwähnt, bei denen es sich zum einen lediglich um Verweiskarten handelte, auf denen die Arztbesuche des Patienten und damit auch die Aufbewahrungsorte seiner jeweiligen Krankheitsdaten gespeichert sind, zum anderen um Dokumentationskarten, auf denen die medizinischen Daten unmittelbar gespeichert werden. Inzwischen zeichnet sich ein Trend zu Dokumentationskarten ab, wobei allgemeine Patientenkarten und krankheitsspezifische Karten unterschieden werden können.

In Übereinstimmung mit den anderen Datenschutzbeauftragten des Bundes und der Länder setze ich mich dafür ein, daß die Daten der Krankenversichertenkarte nicht in den medizinischen Chipkarten enthalten sind, weil dadurch die Krankenversichertenkarte verdrängt und deren Nutzungsbeschränkungen umgangen würden.

Ende Februar 1996 nahm ich an einer Vorstellung der "Medizinischen Patientenkarte" der Kassenärztlichen Vereinigung Hessens teil. Diese Karte wird in der Stadt Neuwied am Rhein seit Anfang des Jahres in einem bundesweit einzigartigen Modellversuch auf freiwilliger Basis erprobt. Diese Chipkarte enthält neben Adreßangaben zum einen medizinisch relevante Daten, zum anderen Daten zur Medikation, wobei auf den ersten Informationskomplex sowohl von Ärzten als auch von Apothekern, denen der Patient die Karte überläßt, zugegriffen werden kann. Die medizinischen Daten können dagegen nur durch Ärzte in deren Praxen gelesen werden, während der die Medikation betreffende Teil der Daten nur in Apotheken gelesen und ergänzt werden kann. Im übrigen erfolgt die Eintragung von Daten auf der Grundlage eines beim Arzt oder Apotheker ausgefüllten Formulars bei der Kassenärztlichen Vereinigung. Ich habe angeregt, das Recht des Karteninhabers, die auf seiner Chipkarte gespeicherten Daten vollständig lesen zu können, auch an einer "neutralen Stelle" zu ermöglichen.

Bereits in meinem 2. Tätigkeitsbericht[105] hatte ich ausgeführt, daß in jedem Fall die Freiwilligkeit einer Nutzung solcher Chipkarten im Gesundheitswesen gewährleistet bleiben muß. Dies betrifft die Frage, ob eine Chipkarte überhaupt benutzt wird, welche Daten darauf gespeichert werden bzw. bleiben und wem welche dieser Daten zugänglich gemacht werden. Dieser Punkt war auch das zentrale Thema der Entschließung der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994[106]. Diese Entschließung fand ihre Untersetzung in einem weiteren Beschluß der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. November 1995 (s. Anlage 5).

---

105 s. unter 1.4.2.3

106 s. 2. Tätigkeitsbericht, Anlage 16

Ausgehend von der besonderen Schutzwürdigkeit medizinischer Daten halte ich die Verantwortlichkeit des Patienten für die Sicherheit seiner Daten für nicht unbedenklich. Abgesehen vom Risiko des Verlustes der Karte und des fehlenden Schutzes vor Beschlagnahmen (vgl. hierzu § 97 StPO) besteht die Gefahr einer pauschalen Offenbarung der darauf befindlichen medizinischen Daten. Vor allem erzeugt jedoch die massenhafte Einführung der Karte einen sozialen Druck auf die Betroffenen, diese mitzuführen und vorzuzeigen. Eine solche Situation wäre theoretisch nicht nur im Arzt-Patienten-Verhältnis, sondern z. B. auch gegenüber Arbeitgebern oder Versicherungen denkbar. Gemeinsam mit den anderen Datenschutzbeauftragten des Bundes und der Länder habe ich deshalb den Gesetzgeber aufgefordert sicherzustellen, daß die auf der beim Patienten befindlichen Chipkarte gespeicherten medizinischen Daten gegen unbefugte Kenntnisnahme und gegen Beschlagnahme ebenso geschützt sind wie die beim Arzt gespeicherten Daten. Außerhalb des Arzt-Patienten-Verhältnisses haben wir uns für ein Vorlageverbot ausgesprochen.

Bei der Kassenärztlichen Vereinigung Hessen hat im Vorfeld des oben dargestellten Modellversuchs ein Arbeitskreis "Datenstrukturen" zehn Thesen zur Dokumentation medizinisch relevanter Daten auf Karten im Gesundheitswesen erarbeitet. Diese entsprechen zwar nicht völlig den Forderungen der Datenschutzbeauftragten, haben jedoch in ihren mehrfachen Überarbeitungen eine Annäherung an diese erfahren. Besonderes Gewicht wird in den Thesen auf die Speicherung von Notfalldaten gelegt, wobei der Begriff der Notfalldaten allerdings extrem weit ausgelegt wird. Neben erwartungsgemäß erfaßten Angaben, z. B. zur Blutgruppe und Allergien gegen die bei der Ersthilfe eingesetzten Medikamente, sind nach Ansicht des Arbeitskreises fast alle Anamnesedaten als Notfalldaten zu bewerten.

Ich bin der Ansicht, daß angesichts der aufgezeigten Gefährdungen der informationellen Selbstbestimmung von Patienten, aber auch weiterer Betroffener - z. B. der Ärzte - die Suche nach datenschutzgerechten Alternativen zur Chipkarte fortgesetzt werden muß.

7.2.2 Neue Gesetze und Verordnungen

7.2.2.1 Verordnung über die Erweiterung der Meldepflicht für übertragbare Krankheiten nach § 7 Abs. 3 Bundesseuchengesetz

§ 7 Abs. 3 Satz 1 Bundesseuchengesetz (BSeuchenG)[107] ermächtigt die Landesregierungen, solange der Bundesminister für Gesundheit von seiner Ermächtigung hierzu keinen Gebrauch macht, eine Rechtsverordnung zu erlassen, durch die die Meldepflicht für die in § 3 BSeuchenG genannten Krankheiten erweitert oder die Meldepflicht auf andere übertragbare Krankheiten ausgedehnt wird, soweit die epidemische Lage dies zuläßt oder erfordert. Hiervon möchte die brandenburgische Landesregierung Gebrauch machen und hat mir den Entwurf der Verordnung über die Erweiterung der Meldepflicht für übertragbare Krankheiten nach § 7 Abs. 3 BSeuchenG (SeuchMVO) mit der Bitte um Stellungnahme vorgelegt.

Bedenken habe ich im wesentlichen gegenüber zwei Punkten geäußert. Zum einen enthält der Entwurf eine Auffangklausel, nach der bei einem "örtlich und zeitlich gehäuften Auftreten gleichartiger Erkrankungen, wenn Krankheitserreger als Ursache möglich sind", eine Meldepflicht bestehen soll. Aufgrund meiner Kritik, daß diese Formulierung zu weit und zugleich zu unscharf gefaßt sei, so daß danach auch Erkrankungen zu melden wären, die als ungefährlich gelten, hat sich das MASGF bemüht, eine etwas konkretere Fassung zu finden. Selbst eine solche erscheint mir jedoch nicht zulässig. § 3 BSeuchenG bezeichnet im einzelnen die meldepflichtigen Erkrankungen, weshalb davon auszugehen ist, daß bei der Ausdehnung der Meldepflicht auf andere übertragbare Krankheiten ebenfalls die konkrete

---

[107] vom 18. Dezember 1979, BGBl. I S. 2262

Krankheit zu bezeichnen ist. Auch das Bundesseuchengesetz enthält gerade keine Klausel, unter der nachträglich automatisch weitere Erkrankungen erfaßt werden könnten, sondern lediglich die Möglichkeit, die Liste des § 3 BSeuchenG durch Rechtsverordnung zu erweitern, wodurch sich eine Auffangklausel in dieser Rechtsverordnung von selbst verbietet.

Zum anderen war Gegenstand meiner Kritik die Einführung von Meldewegen, für die das Bundesseuchengesetz keine Rechtsgrundlage bietet. Allenfalls könnte aus datenschutzrechtlicher Sicht - im Vorgriff auf eine künftige gesetzliche Regelung der Meldewege im Bundesseuchengesetz - eine solche Bestimmung toleriert werden, wenn sichergestellt ist, daß die Daten von den Gesundheitsämtern nur anonymisiert weitergegeben werden.

Mit dem MASGF bin ich übereingekommen, daß wir zu beiden Punkten weitere Informationen einholen und auf dieser Grundlage versuchen werden, eine für beide Seiten akzeptable Fassung der Verordnung zu erreichen.

7.2.2.2 Berufsordnung für Hebammen und Entbindungspfleger im Land Brandenburg

Die Berufsordnung für Hebammen und Entbindungspfleger (HebBOBbg)[108], auf die ich bereits im 2.[109] und im 3. Tätigkeitsbericht[110] eingegangen bin, ist inzwischen in Kraft getreten. Wie in den früheren Tätigkeitsberichten dargestellt, wurden erfreulich viele meiner Anregungen im verordnungsgebenden Verfahren aufgegriffen. Leider wurde trotz entsprechender Hinweise von mir nicht erreicht, daß die Dokumentationen durch amtliche Formulare festgelegt werden. Auch wurde für den Fall des Todes der freiberuflich tätigen Hebammen und Entbindungspfleger bedauerlicherweise keine normenklare Regelung getroffen, daß und wie deren Dokumentationen den örtlich zuständigen Gesundheitsämtern übergeben werden.

7.2.2.3 Umsetzung der Verschlüsselung gem. § 295 SGB V vertagt

Gem. § 295 Abs. 1 Satz 1 SGB V sind die an der vertragsärztlichen Versorgung teilnehmenden Ärzte verpflichtet, in den Abrechnungsunterlagen über die von ihnen erbrachten vertragsärztlichen Leistungen sowie in den Arbeitsunfähigkeitsbescheinigungen u. a. die Diagnosen anzugeben. Diese sind gem. § 295 Abs. 1 Satz 2 SGB V zu verschlüsseln. Die codierte Diagnoseübermittlung soll den Schutz der Daten bei der Übermittlung, aber auch die datenmäßige Erfassung und die statistische Auswertung für Plausibilitätskontrollen sowie Auffälligkeits- und Zufälligkeitsprüfungen im Rahmen der Wirtschaftlichkeitsprüfung ermöglichen.

Die "Internationale statistische Klassifikation der Krankheiten und verwandter Gesundheitsprobleme", 10. Revision (ICD-10-Code), die zum 1. Januar 1996 für die Verschlüsselung eingeführt werden sollte, ist eine mit über 14.000 Ziffern (z. B. Aligatorenbisse, W 58; Opfer von Vulkanausbrüchen, X 34) ins Deutsche übersetzte Klassifikation der Weltgesundheitsorganisation für Todesstatistiken, die vom Deutschen Institut für Medizinische Dokumentation und Information im Auftrag des Bundesministeriums für Gesundheit unter Beteiligung wissenschaftlicher medizinischer Fachgesellschaften, der Kassenärztlichen Bundesvereinigung und ärztlicher Berufsverbände herausgegeben wird. Sie enthält - nach medizinischen Fachbereichen gegliedert - Listen von

---

108 vom 8. November 1995, GVBl. II S. 702

109 s. unter 7.2.6

110 s. unter 7.2.1.1

Diagnosen mit dazugehöriger Codierung, die innerhalb dieser Grobgliederung in themenbezogene Kapitel zusammengefaßt sind; etliche häufige Diagnosen wie Grippe als Einzelcode fehlen.

Besondere Kritikpunkte waren das Fehlen von Zusätzen, die Diagnosen und Verdachtsdiagnosen unterscheiden ließen, was zwangsläufig zur Verfälschung der Informationen führen mußte, und der Umstand, daß vielfach sozio-psychologische Krankheitsursachen aufgeführt waren, die gar keine Diagnose darstellen und insoweit keine medizinische Relevanz haben. Die Anwendung einzelner Kapitel, die nicht Diagnosen enthalten, sondern auch "äußere Ursachen von Morbidität und Mortalität" sowie "Faktoren, die den Gesundheitszustand beeinflussen und zur Inanspruchnahme von Einrichtungen des Gesundheitswesens führen", war schon sehr frühzeitig aufgrund der ersten Proteste durch das Bundesministerium für Gesundheit untersagt worden[111].

Die Anwendung des ICD-10-Codes wurde aufgrund des massiven Protestes von Ärzten und Datenschützern aufgeschoben und soll - nach Überarbeitung und Erprobung - erst Anfang 1998 eingeführt werden[112].

7.2.3 Aktuelle Fälle

7.2.3.1 Umgang mit personenbezogenen Daten aus Leichenschauscheinen

Die Dokumentation der Leichenschau und die Einführung eines einheitlichen Leichenschauscheines wurde inzwischen durch Runderlaß der Ministerin für Arbeit, Soziales, Gesundheit und Frauen (LeichRErl)[113] aufgrund von § 3 Abs. 2 Satz 3 der Anordnung über die ärztliche Leichenschau[114] geregelt.

Offengeblieben sind jedoch weiterhin die Fragen danach, wem unter welchen Voraussetzungen Auskünfte aus den Leichenschauscheinen erteilt oder Einsicht in diese gewährt werden darf. Des weiteren besteht bei den Gesundheitsämtern ein Bedarf nach elektronischer Datenverarbeitung der Grunddaten aus der Todesbescheinigung, da derzeit als vorgeschriebenes Ordnungskriterium die Sterbebuchnummer dient, die den Anfragenden in der Regel nicht bekannt und nur über andere Daten wie Name, Vorname, Geburtsdatum und Sterbedatum herauszufinden ist.

Der Leichenschauschein kann sich bei den verschiedensten Stellen befinden, z. B. beim Leichenschauarzt, Krematoriumsarzt, Gesundheitsamt und Landesamt für Datenverarbeitung und Statistik (LDS). Für die Gesundheitsämter ist eine zwanzigjährige Aufbewahrungsfrist festgelegt. Zumindest für die Duplikate beim Krematoriumsarzt und dem LDS kämen aber sicherlich wesentlich kürzere Aufbewahrungsfristen in Betracht. Auch ist angesichts der vielen verschiedenen Aufbewahrungsstellen zu klären, ob bei allen die Möglichkeit eines Akteneinsichtsrechts bzw. einer Auskunftserteilung bestehen soll, was die Gefahr unterschiedlicher Entscheidungen dieser Stellen mit sich bringen würde. Spezielle Regelungen sollten für Ermittlungsbehörden und Forschungseinrichtungen getroffen werden, da insbesondere diese ein Auskunftsinteresse haben können.

Nachdem ich über den Fortgang des gesetz- oder verordnungsgebenden Verfahrens nichts mehr gehört hatte, obwohl mir Mitte 1994 mitgeteilt worden war, daß ein Entwurf in

---

111 Bundesanzeiger 1995 Nr. 242, S. 12853

112 Rahmenvereinbarung der Spitzenverbände der Krankenkassen, der Kassenärztlichen Bundesvereinigung und der Deutschen Krankenhausgesellschaft vom 2. Februar 1996

113 vom 9. Januar 1995, ABl. S. 29

114 vom 4. Dezember 1978, DDR-GBl. I 1979 S. 4

Vorbereitung sei, habe ich im November 1995 aufgrund einer aktuellen Anfrage eines Gesundheitsamtes die gesamte oben dargelegte Problematik sowohl dem Ministerium für Arbeit, Soziales, Gesundheit und Frauen als auch dem Ministerium des Innern zur Kenntnis gegeben und deutlich gemacht, daß eine rasche Verständigung insbesondere über Auskunfts- und Akteneinssichtsrechte im Vorgriff auf eine gesetzliche Regelung als Verhaltensrichtlinie für die Gesundheitsämter äußerst wichtig sei. Trotzdem blieb auch eine schriftliche Nachfrage meinerseits Anfang des Jahres an das MASGF von diesem bisher unbeantwortet.

7.2.3.2 Umgang mit Impfdateien

Im 3. Tätigkeitsbericht[115] hatte ich darüber berichtet, daß der Umgang mit Impfdateien derzeit noch nicht geregelt ist, obwohl auch von seiten der Ärzte wiederholt deutlich gemacht worden war, welche Bedeutung die Pflege von Impfdateien habe. Außerdem sind unter Ziff. 3 Nr. 4 in dem "Runderlaß zur Meldung, Aufbewahrung und Nutzung von Patientenunterlagen usw. mit patientenbezogenem (medizinischem) Inhalt aus ehemaligen Gesundheitseinrichtungen der DDR"[116] hierzu gesonderte Bestimmungen angekündigt worden.

Das MASGF hatte zunächst signalisiert, eine landesweite Konzeption zur Führung von Impfdateien zu entwickeln. Nach dem Erlaß des Brandenburgischen Gesundheitsdienstgesetzes (BbgGDG)[117] ging das MASGF jedoch davon aus, daß der Impfstatus für Kinder und Jugendliche auf der Grundlage von § 8 Abs. 2 BbgGDG überprüft und vorhandene Impfkarteien dieser Altersgruppe ergänzt würden. Eine gesonderte Regelung zur Behandlung von Impfdateien wurde vom Ministerium im übrigen nicht mehr als erforderlich angesehen, da in den §§ 28 und 29 BbgGDG nunmehr bereichsspezifische gesetzliche Regelungen für den Datenschutz im öffentlichen Gesundheitsdienst getroffen worden seien und die Grundsätze des o. g. Runderlasses entsprechend auch auf Impfdaten angewandt werden könnten.

Ich habe dieser Auffassung widersprochen und darauf hingewiesen, daß nicht alle Empfehlungen der "Hinweise zur Meldung, Aufbewahrung und Nutzung von Patientenunterlagen ..." auf Impfdateien übertragbar seien, weshalb dieser Erlaß auch eine gesonderte Regelung vorsehe. Aus dem Vergleich mit den speziellen Bestimmungen zu Kindern und Jugendlichen im Gesundheitsdienstgesetz ergab sich für mich der Rückschluß, daß Impfkarteien für Erwachsene nur im Rahmen einer Behandlung durch das Gesundheitsamt oder aufgrund einer Einverständniserklärung der Betroffenen (weiter-)geführt werden dürfen. Demgegenüber erachten die Amtsärzte das Weiterführen aller Impfdateien für notwendig, z. B. weil eine hohe Nachfrage der Bürger auch nach Altdaten besteht. Aufgrund meiner Darlegungen hat das MASGF seine Entscheidung revidiert und mit der Erarbeitung eines entsprechenden Entwurfs von Regelungen zum Umgang mit Impfdaten nun doch begonnen.

7.2.3.3 Elternfragebogen zur Schulreihenuntersuchung

Bereits im 2. Tätigkeitsbericht[118] hatte ich zu Elternfragebögen, die anläßlich der Einschulungsuntersuchung Verwendung finden sollten, Stellung genommen. Ende 1995 wurde mir vom MASGF ein überarbeiteter Elternfragebogen zur Schulreihenuntersuchung vorgelegt, der etliche meiner bisherigen Bedenken berücksichtigte. So unterblieben insbesondere viele der Fragen, die sich auf das häusliche Umfeld bezogen hatten. Soweit die

---

115 s. unter 7.2.3.1

116 vom 22. November 1993, ABl. S. 1725

117 vom 3. Juni 1994, GVBl. I S. 178

118 s. unter 7.2.2.4

Fragen über Angaben, die zur Feststellung der Schulfähigkeit erforderlich waren, hinausgingen, habe ich dieses lediglich im Hinblick auf § 8 Abs. 2 und 3 BbgGDG akzeptiert, wonach der öffentliche Gesundheitsdienst regelmäßige ärztliche Untersuchungen zur Früherkennung von Krankheiten, Behinderungen und Entwicklungsstörungen durchführt und die Schuleingangsuntersuchung als eine dieser ärztlichen Untersuchungen definiert wird. Ich habe gefordert, die genannten Untersuchungszwecke als weitere Maßstäbe für die Erforderlichkeit der Datenerhebung zu berücksichtigen. Insbesondere habe ich darauf hingewiesen, daß die Gesundheitsberichterstattung nicht Zweck der Einschulungsuntersuchung ist, sondern lediglich die bei dieser Untersuchung rechtmäßig erhobenen Daten anschließend in anonymisierter Form für die Gesundheitsberichterstattung verwandt werden dürfen.

Im einzelnen schienen mir folgende Fragen problematisch:

- Zum Thema "Hatte Ihr Kind Unfälle?"

Die Erhebung des Unfallortes hat Bedeutung für die Frage der Betreuung der Kinder, der Verantwortlichkeit der Eltern u. ä.; für die o. g. zulässigen Zwecke ist er jedoch nicht erforderlich.

Bei den einzelnen Unfallarten bzw. -folgen sollte ergänzt werden, daß nur erhebliche Fälle, die z. B. Funktionsbeeinträchtigungen oder Entstellungen zur Folge haben, erfaßt werden.

Nachdem die Frage nach den Unfällen auch gestellt wird, um Teilleistungsstörungen der Motorik aufzudecken, ist ebenfalls fraglich, ob nicht erst bei einer gewissen Häufung von Unfällen eine Datenerhebung im einzelnen erforderlich erscheint.

Diesen Bedenken meinerseits wurde bedauerlicherweise nicht Rechnung getragen.

- Zum Thema "Fluortabletten, fluoridiertes Speisesalz, jodiertes Speisesalz"

Aufgrund meiner Intervention wurden jedoch Fragen zur Verwendung von jodiertem Speisesalz und zur Einnahme von Fluortabletten bzw. fluoridiertem Speisesalz gestrichen, mit denen lediglich überprüft werden sollte, ob allgemeine Prophylaxe-Empfehlungen angenommen würden.

- Zum Thema "Umweltmedizinische Angaben"

Zu den umweltmedizinischen Angaben, die Schimmelbildungen, Geruchs- und Lärmbelästigungen betrafen, hatte ich darauf hingewiesen, daß diese allgemeinen Hintergrundfragen erst dann gestellt werden dürften, wenn Anhaltspunkte für entsprechende Beschwerden bestehen (z. B. Allergien, Schlaf- oder Hörstörungen). Eine solche gestufte Fragestellung wurde jedoch nur hinsichtlich der Allergien eingeführt. Auch mein Hinweis, daß die Frage nach den Geruchsbelästigungen so nicht sinnvoll erscheint, weil Gerüche sehr subjektiv wahrgenommen werden und nicht deutlich wird, von welchem Familienmitglied konkret die Frage beantwortet werden soll, wurde nicht aufgegriffen.

Ich werde mich dafür einsetzen, daß bei einer weiteren geplanten Überarbeitung der Fragebögen auch die bisher nicht aufgegriffenen Kritikpunkte Berücksichtigung finden.

7.2.3.4 Organspendeausweis

Durch einen Zeitungsartikel wurde ich auf eine Aktion der AOK Brandenburg aufmerksam, die sich zum Ziel gesetzt hatte, die Brandenburger Bevölkerung dazu zu bewegen, einen Organspendeausweis bei sich zu tragen. Der neue Spenderausweis wurde ausdrücklich gelobt. Diese Bewertung konnte ich, nachdem mir die AOK auf meine Bitte hin ein Exem-

plar übersandt hatte, jedoch nicht teilen.

Meiner Ansicht nach ist dieser Ausweis nicht neutral genug gefaßt. So enthält er beispielsweise die Aussage: "Ich bin Organspender: Ich möchte kranken Menschen dadurch helfen, daß mir nach meinem Tod Organe/Gewebe zur Transplantation entnommen werden." Nichtspender würden damit im Umkehrschluß als Menschen stigmatisiert, die nicht bereit sind, anderen zu helfen.

Problematisch erscheint mir ebenfalls die Rückseite des Ausweises mit der Erklärung zur Organspende, wo infolge Platzmangels die Zeilen: "Ich übertrage die Entscheidung über eine Organspende nach meinem Tod auf:" und "Falls mir etwas zustößt, sollen folgende Personen benachrichtigt werden:" direkt untereinander stehen, so daß nur ein einziges Feld für die Angabe einer Person vorhanden ist. Ein Ausweisbesitzer hat daher bereits Schwierigkeiten, verschiedene Personen für beide Fragestellungen anzuführen. Sofern er nur an einer Benachrichtigung an seine Angehörigen interessiert ist, könnte es ein leichtes sein, nach seinem Tode auch das Feld für die Übertragung der Entscheidung über eine Organspende anzukreuzen. Diesen Mißbrauchsmöglichkeiten sollte durch eine andere Gestaltung dieses Teils vorgebeugt werden, worauf ich sowohl die AOK als auch die Aufsichtsbehörde des Arbeitskreises Organspende, der den Ausweis entwickelt hatte, aufmerksam gemacht habe.

Diese Erfahrung war für mich zugleich Anlaß dafür, im Gesetzgebungsverfahren zum Transplantationsgesetz (s. unter 7.3.1.4) einen amtlich vorgeschriebenen Organspendeausweis zu fordern.

7.3 Krankenhauswesen

7.3.1 Neue Gesetze und Verordnungen

7.3.1.1 Brandenburgisches Psychisch-Kranken-Gesetz

Das Brandenburgische Psychisch-Kranken-Gesetz (BbgPsychKG) wurde vom Landtag Anfang des Jahres verabschiedet. Ein Gesetzesentwurf war mir erstmals Ende 1993 vorgelegt worden. Im 2. Tätigkeitsbericht[119] hatte ich diesbezüglich auf das Fehlen bereichsspezifischer Regelungen zum Datenschutz hingewiesen; im 3. Tätigkeitsbericht[120] hatte ich u. a. im Hinblick auf die Normenklarheit verschiedene ergänzende Forderungen dargestellt, die das MASGF weitestgehend berücksichtigte.

Zwischenzeitlich haben meine wiederholten Hinweise dazu geführt, daß in das BbgPsychKG detailliertere Regelungen zur Datenspeicherung, -übermittlung und -lösch ung aufgenommen wurden. Mit den Argumenten des Verhältnismäßigkeitsgrundsatzes und der Normenklarheit konnte ich erreichen, daß Einschränkungen des grundsätzlich gewährleisteten Rechts auf ungestörten Schriftwechsel nur dann zulässig sein sollen, "wenn Tatsachen die Annahme rechtfertigen," daß bestimmte Gefahren bestehen.

Hingegen wurde leider nicht weiter konkretisiert, welche Rechte und Pflichten der Patientenfürsprecher gem. § 31 BbgPsychKG haben soll. Auf meine Intervention hin unterblieb zumindest eine zusätzliche Regelung, wonach der Patientenfürsprecher ein Einsichtsrecht in Patientenakten nach den geltenden Rechtsvorschriften haben sollte. Ein solches Akteneinsichtsrecht ist nun lediglich für die Besuchskommission vorgesehen und dort auch nur mit Einwilligung des Patienten oder dessen gesetzlichem Vertreter.

---

119 s. unter 7.2.3.2

120 s. unter 7.3.1

Mit dem BbgPsychKG selbst werden gem. § 1 Abs. 1 drei verschiedene Zwecke verfolgt:

- Hilfeleistungen für psychisch Kranke oder seelisch Behinderte,

- Schutzmaßnahmen vor psychisch Kranken oder seelisch Behinderten sowie

- Vollzugsmaßnahmen im Rahmen der Unterbringung.

Insbesondere im Vollzug, der ja Grundrechtseinschränkungen erforderlich macht, sind auch datenschutzrechtlich relevante Regelungen getroffen worden, so z. B. zum Recht auf Schriftwechsel (§ 24 BbgPsychKG), bei dem unter engen Voraussetzungen eine Überwachung - und damit Einsichtnahme - vorgesehen ist. Absender und Empfänger der Sendungen sind über eine solche Maßnahme unverzüglich zu informieren. Vergleichbares gilt gem. § 25 BbgPsychKG für fernmündliche und elektronische Nachrichtenübermittlungen, bei deren Überwachung die Beteiligten bereits vor Beginn über diese Maßnahme zu unterrichten sind.

Abschnitt 7 enthält schließlich bereichsspezifische Datenschutzbestimmungen und verweist ergänzend auf die Vorschriften des Brandenburgischen Datenschutzgesetzes (§ 49 Abs. 1 BbgPsychKG) sowie auf § 28 des Krankenhausgesetzes des Landes Brandenburg nebst der dazu ergangenen Krankenhausdatenschutzverordnung (§ 49 Abs. 2 BbgPsychKG). § 50 BbgPsychKG regelt die Verarbeitung personenbezogener Daten, wobei insbesondere § 203 Abs. 1 bzw. Abs. 3 StGB (Verletzung von Privatgeheimnissen) Berücksichtigung findet (§ 50 Abs. 3 BbgPsychKG). Aufzeichnungen von Stellen, die an der Erfüllung der Aufgaben nach dem BbgPsychKG beteiligt sind, sind grundsätzlich zehn Jahre aufzubewahren und danach zu löschen bzw. zu vernichten, wenn nicht ihre Archivierung nach besonderen Rechtsvorschriften vorzunehmen ist (§ 50 Abs. 6 BbgPsychKG).

§ 51 BbgPsychKG regelt das Zusammenwirken mit anderen Behörden und Einrichtungen, § 52 BbgPsychKG die Datenübermittlung durch die Unterbringungseinrichtung an Personen und Stellen außerhalb der Einrichtung über die Fälle hinaus, in denen die betroffene Person in die Übermittlung eingewilligt hat oder ein Fall des § 51 BbgPsychKG vorliegt. Dabei besteht eine strenge Zweckbindung dergestalt, daß der Empfänger die ihm übermittelten personenbezogenen Daten nur für die Zwecke verwenden darf, zu deren Erfüllung sie ihm übermittelt worden sind.

Gem. § 53 Abs. 2 BbgPsychKG ist die betroffene Person von der Übermittlung ihrer personenbezogenen Daten nach den §§ 51 und 52 BbgPsychKG zu unterrichten, wenn dem keine schwerwiegenden Gründe einer dadurch entstehenden gegenwärtigen erheblichen Gefahr für ihre Gesundheit oder für die öffentliche Sicherheit entgegenstehen.

7.3.1.2 Krankenhausdatenschutzverordnung

Die Verordnung zum Schutz von Patientendaten im Krankenhaus (Krankenhausdatenschutzverordnung - KHDsV)[121] wurde Anfang des Jahres endlich in Kraft gesetzt. Nach wie vor bedauere ich, wie schon im 2.[122] und 3.[123] Tätigkeitsbericht dargestellt, daß die nunmehr in der KHDsV enthaltenen Regelungen nicht ins Landeskrankenhausgesetz selbst aufgenommen wurden. Im einzelnen enthält die KHDsV u. a. folgende Regelungen:

§ 3 Abs. 1 KHDsV definiert den Begriff der Patientendaten und stellt klar, daß dieser auch

---

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

122 s. unter 7.2.3.1

123 s. unter 7.3.2

personenbezogene Daten Dritter, insbesondere Angehöriger, die im Zusammenhang mit der Behandlung bekannt werden, umfaßt. Absatz 2 der Vorschrift bestimmt, daß eine Speicherung nur in einer Weise erfolgen darf, die eine Löschung und Sperrung zuläßt; mit § 3 Abs. 2 KHDsV wurde einer meiner Formulierungsvorschläge unverändert in die Rechtsverordnung übernommen.

Die Verarbeitung von Patientendaten ist gem. § 4 Abs. 1 und 2 KHDsV nur unter engen Voraussetzungen zulässig. In der ursprünglichen Fassung der Krankenhausdatenschutzverordnung war eine Datenverarbeitung zur Aus-, Weiter- oder Fortbildung in Berufen des Gesundheitswesens als zusätzlicher Zweck vorgesehen gewesen. Aufgrund meines Vorhaltes, daß die Verarbeitung von Patientendaten zu diesem Zweck nicht erforderlich, sondern in jedem Fall mit anonymisierten Daten erreichbar ist, wurde dieser Unterpunkt gestrichen.

§ 4 Abs. 4 KHDsV enthält ausführliche Regelungen zur Einwilligung. § 4 Abs. 5 KHDsV verpflichtet den Krankenhausträger, alle erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der Patientendaten zu treffen.

In § 5 KHDsV ist die Übermittlung von Patientendaten geregelt. Grundsätzlich ist diese nur mit Einwilligung des Patienten zulässig. Übermittlungen, die mit der Behandlung und daraus resultierenden Maßnahmen zusammenhängen, sind zulässig, soweit der Betroffene nach Hinweis auf die beabsichtigte Übermittlung nicht etwas anderes bestimmt. In weiteren eng begrenzten Fällen ist eine Datenübermittlung auch ohne Einwilligung des Patienten zulässig. Hierzu zählt z. B. gem. § 5 Abs. 1 Nr. 3 KHDsV die Abwehr von gegenwärtigen Gefahren für das Leben oder die Gesundheit eines Dritten, sofern diese Rechtsgüter das Geheimhaltungsinteresse des Patienten deutlich überwiegen. In der Praxis wird man eine Mitteilungsbefugnis aufgrund dieser Vorschrift annehmen können, wenn ein sicher HIV-positiver Patient trotz eindringlicher Ermahnungen der Ärzte nicht bereit ist, Maßnahmen zu ergreifen, um seinen Sexualpartner vor einer Ansteckung zu schützen. Zulässig ist die Übermittlung von Patientendaten nach § 5 Abs. 1 Nr. 5 KHDsV auch zur Durchführung eines mit der Behandlung zusammenhängenden gerichtlichen Verfahrens. Diese Vorschrift ist eng auszulegen in dem Sinne, daß insbesondere Strafverfahren oder Zivilprozesse aufgrund behaupteter Behandlungsfehler von ihr erfaßt werden, nicht jedoch Fälle, in denen beispielsweise in einem Strafverfahren über eine Schlägerei zu entscheiden ist, deren Opfer anschließend in dem Krankenhaus behandelt wurde.

In § 7 KHDsV ist das Recht auf kostenfreie Auskunft und Akteneinsicht niedergeschrieben. Ursprünglich war eine Begrenzung der Auskunfts- und Einsichtsrechte nicht nur im Interesse der Gesundheit des Patienten vorgesehen, sondern auch in Fällen, in denen berechtigte Geheimhaltungsinteressen eines Dritten überwiegen. Letzterer Punkt wurde fallengelassen, weil davon ausgegangen wurde, daß solche gewichtigen Fälle nicht denkbar seien. Durch das Deutsche Rote Kreuz wurde ich jedoch kurz vor Abschluß des verordnungsgebenden Verfahrens darüber informiert, daß zu DDR-Zeiten üblicherweise der Name des Blutspenders auch auf den Konservenbegleitscheinen dokumentiert worden sei und Kliniken diese Unterlagen in der Krankenakte des Empfänger abgeheftet hätten. Aufgrund seines Einsichtnahmerechts könnte der Patient somit personenbezogene Daten seines Blutspenders erfahren, was verhindert werden muß. Bedauerlicherweise war das verordnungsgebende Verfahren bereits so weit fortgeschritten, daß dieser Punkt keine Berücksichtigung mehr finden konnte. Mit dem MASGF wurde jedoch vereinbart, die Verordnung bis zu einer Novellierung verfassungskonform so auszulegen, daß die Akteneinsicht sich immer nur auf Daten des Betroffenen selbst bezieht und beschränkt. Auch hat sich das Ministerium inzwischen an alle Krankenhäuser gewandt, um auf die Problematik der Konservenbegleitscheine der ehemaligen Bezirksinstitute für Blutspende- und Transfusionswesen aufmerksam zu machen, und die Kliniken aufgefordert, dem Recht auf informationelle Selbstbestimmung der Blutspender in geeigneter Weise Rechnung zu tragen.

Die KHDsV enthält außerdem bereichsspezifische Regelungen zur Datenverarbeitung im Auftrag (§ 6), zur Sperrung und Löschung von Patientendaten (§ 8), zur Wartung und Fernwartung (§ 9) und für Forschungsvorhaben (§ 10). Solange schutzwürdige Belange der Betroffenen nicht gefährdet werden, dürfen Ärzte und sonstiges wissenschaftliches Personal Patientendaten, die innerhalb ihrer Fachabteilung gespeichert sind, für eigene wissenschaftliche Forschungsvorhaben verarbeiten. Abteilungsfremden Personen dürfen Patientendaten nur mit Einwilligung des Patienten übermittelt werden. Nur in eng begrenzten Ausnahmefällen kann von einer Einwilligung der Betroffenen abgesehen werden.

7.3.1.3 Krebsregisterausführungsgesetz

Im 3. Tätigkeitsbericht[124] hatte ich darauf hingewiesen, daß die neuen Bundesländer und Berlin zur Fortführung des Nationalen Krebsregisters der DDR, das bis zum 31. Dezember 1994 auf das Krebsregistersicherungsgesetz[125] gestützt werden konnte, ein Verwaltungsabkommen abgeschlossen haben, bei dem die Bedenken der Datenschutzbeauftragten infolge Zeitdrucks nur in geringem Umfang berücksichtigt wurden, und das auch dem Gesetzesvorbehalt nicht genügte. Nach dem "Verwaltungsabkommen über ein Gemeinsames Krebsregister" wird dieses als eine nicht rechtsfähige Anstalt des öffentliches Rechts des Landes Berlin geführt.

Inzwischen haben die neuen Bundesländer und Berlin zusätzlich zu dem Verwaltungsabkommen größtenteils gleichlautende Ausführungsgesetze zum Krebsregistergesetz erarbeitet. Die Datenschutzbeauftragten dieser Länder haben hierzu eine gemeinsame Stellungnahme abgegeben, in der vor allem eine staatsvertragliche und damit gesetzliche Regelung anstelle des Verwaltungsabkommens gefordert wird.

Primär gründen sich diese Bedenken darauf, daß das Gemeinsame Krebsregister als datenverarbeitende Stelle durch ein bloßes Abkommen auf Verwaltungsebene errichtet und betrieben wird. Insbesondere die Fragen, welche Stelle wie und zu welchem Zweck Daten verarbeitet, berührt ganz wesentlich das Recht auf informationelle Selbstbestimmung, weshalb gerade auch der grundlegende organisatorische Punkt, daß das Gemeinsame Krebsregister für die Krebskranken-Daten der neuen Bundesländer und Berlins zuständig sein soll, im Hinblick auf den Gesetzesvorbehalt bei Grundrechtseinschränkungen einer gesetzlichen Regelung bedarf. Diese Voraussetzung erfüllt das Verwaltungsabkommen nicht, wohl aber ein Staatsvertrag.

Das Verwaltungsabkommen sieht die Errichtung einer Behörde vor und steht damit nach Art. 96 Abs. 1 Satz 1 Brandenburgische Verfassung (BbgVerf)[126] auch unter dem organisationsrechtlichen Gesetzesvorbehalt. Das "Verwaltungsabkommen" stellt damit eigentlich einen Staatsvertrag dar, der der Zustimmung des Landtages in Form eines Gesetzes bedurft hätte und wegen des Zustimmungsmangels im Innenverhältnis rechtswidrig ist.

Für die von meinen Kollegen und mir vertretene Auffassung spricht weiter, daß allein durch einen Staatsvertrag die Einheitlichkeit der Landesbestimmungen zum Gemeinsamen Krebsregister sichergestellt wird, indem insbesondere selbständige Änderungen oder Ergänzungen wesentlicher Grundentscheidungen ausgeschlossen werden.

Die einzelnen Länderausführungsgesetze könnten sich darüber hinaus wie ein "Vertrag zu Lasten Dritter", nämlich des Landes Berlin, darstellen, ohne die Gewähr dafür zu bieten, daß

---

124 s. unter 7.2.1.2

125 vom 21. Dezember 1992, BGBl. I S. 2335

126 vom 20. August 1992, GVBl. I S. 198

dieses Sitzland die ihm zugewiesenen Aufgaben auch tatsächlich erfüllen müßte. Eine solche Bindung Berlins an die gemeinsamen Regelungen kann aber über einen Staatsvertrag erreicht werden, was Rechtsklarheit und Rechtssicherheit zur Folge hätte.

Problematisch erscheint auch, daß in dem Verwaltungsabkommen auf Berliner Landesrecht verwiesen wird. Der Gesetzgeber ist zwar nicht gehindert, auf fremdes, nicht von ihm vorformuliertes und in Kraft gesetztes Recht eines anderen Kompetenzbereiches zu verweisen; um der Rechtsstaatlichkeit und der Rechtssicherheit zu genügen, muß ein solches Gesetz allerdings für den Rechtsunterworfenen klar erkennen lassen, welche Vorschriften im einzelnen gelten sollen. Dabei muß dem Erfordernis der Verkündung (Art. 81 Abs. 1 BbgVerf) Genüge getan werden, woran es im Hinblick auf das Verwaltungsabkommen fehlen dürfte. Zustimmungsgesetze der beteiligten Länder zum Staatsvertrag würden diese Bedingungen hingegen erfüllen.

Das MASGF hat bei den mehrfach darüber geführten Besprechungen immerhin eingeräumt, daß ein Verwaltungsabkommen aus datenschutzrechtlicher Sicht nicht unproblematisch sei. Insofern wurde eine Prüfung der erforderlichen Rechtsform zwischen den Landesbeauftragten für den Datenschutz und den Ministerien auf Länderebene vereinbart, aufgrund derer sich zwischenzeitlich das Thüringer Ministerium für Soziales und Gesundheit, das Justizministerium des Landes Mecklenburg-Vorpommern sowie die Staatskanzlei Sachsen-Anhalts der Meinung der Datenschutzbeauftragten angeschlossen haben. Dennoch wurde mir vom MASGF mitgeteilt, daß es zunächst weiter an der Entscheidung für das Verwaltungsabkommen festhalten werde. Da ich dies nicht für akzeptabel halte und nicht nachvollziehen kann, weshalb in Brandenburg trotz der vom MASGF selbst geäußerten Bedenken nicht ebenfalls absprachegemäß überprüft wird, ob ein Verwaltungsabkommen rechtlich überhaupt als ausreichende Grundlage für das Gemeinsame Krebsregister angesehen werden kann, habe ich das Ministerium aufgefordert, sich dieser Frage zu stellen.

Ein weiteres wesentliches Problem, das in den Ausführungsgesetzen geregelt werden soll, betrifft den Umgang mit den Altdaten aus dem ehemaligen Nationalen Krebsregister der DDR. Diese waren ursprünglich nach anderen Ordnungskriterien abgelegt worden (s. unter 7.3.2.1), weshalb die vom Krebsregistergesetz (KRG)[127] eigentlich vorgesehenen Schutzmechanismen nach Darstellung des Gemeinsamen Krebsregisters bei deren Anwendung einen unverhältnismäßig großen Verwaltungsaufwand zur Folge hätten. Für einen Übergangszeitraum soll deshalb die Übernahme der Altdaten auf elektronische Datenträger und die Vervollständigung des auf elektronischen Datenträgern vorhandenen Datenbestandes unter reduzierten datenschutzrechtlichen Anforderungen stattfinden. Nach Abschluß dieser Maßnahmen sollen die Papieraltdatenbestände letztlich dem Berliner Staatsarchiv zur Aufbewahrung angeboten werden. Akzeptiert haben die angesprochenen Landesministerien den Hinweis der Datenschutzbeauftragten, daß gemeldete Daten, die nicht unter das KRG oder das entsprechende Ausführungsgesetz fallen, vorbehaltlich archivrechtlicher Anbietungsfristen zu löschen sind.

Ein weiteres noch zu lösendes Problem betrifft die Kontrollbefugnisse der Landesbeauftragten für den Datenschutz der neuen Bundesländer hinsichtlich der aus ihren Ländern gelieferten personenbezogenen Daten beim Gemeinsamen Krebsregister. Ich vertrete hierzu die Meinung, daß beim Gemeinsamen Krebsregister gespeicherte Daten und die auf sie bezogene Kontrollbefugnis dem Datenschutzgesetz des jeweiligen Herkunftslandes unterliegen, soweit nicht das Krebsregistergesetz etwas anderes bestimmt.

Die Prüfung des Gemeinsamen Krebsregisters, die ich gemeinsam mit dem Berliner Datenschutzbeauftragten vorgenommen habe, ist unter 7.3.2.1 dargestellt.

---

[127] vom 4. November 1994, BGBl. I S. 3351

7.3.1.4 Transplantationsgesetz

Zu einzelnen datenschutzrechtlichen Problemen, die durch den immer wieder überarbeiteten Entwurf eines Transplantationsgesetzes aufgeworfen wurden, habe ich bereits im 2. Tätigkeitsbericht[128] Stellung genommen. Die Gründe, die mich dazu bewogen haben, statt der von den verschiedensten Stellen entworfenen unterschiedlichen Organspendeausweise ein amtlich vorgeschriebenes Exemplar zu fordern, habe ich unter 7.2.3.4 dargestellt.

Bei der Anhörung zum Transplantationsgesetz im Deutschen Bundestag ist die bisher dem Gesetzentwurf zugrunde gelegte sogenannte erweiterte Zustimmungslösung auf massiven Widerstand gestoßen. Diese ermöglicht für den Fall, daß eine Erklärung des Betroffenen nicht vorliegt, eine Entscheidung letztlich unter Einbeziehung der Angehörigen zu treffen. Die Frage des zugrunde liegenden Modells wird in der derzeitigen Fassung des interfraktionellen Entwurfs (Stand: 8. November 1995) offengelassen. In dieser Situation habe ich mich mit den einzelnen Lösungsmodellen auseinandergesetzt und beim MASGF um Unterstützung für die enge Zustimmungslösung nachgesucht, bei der dem Willen des Betroffenen dadurch am besten Rechnung getragen wird, daß dieser nicht genötigt wird, seine ablehnende Entscheidung zu dokumentieren. Darüber hinaus wird dabei nicht zwingend ein Register für die Dokumentation der Erklärungen zur Organspende vorausgesetzt. Diese Auffassung hat ihren Niederschlag in einer Entschließung der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 14./15. März 1996 in Hamburg gefunden (s. Anlage 11).

7.3.2 Krankheitsregister

7.3.2.1 Prüfung im Gemeinsamen Krebsregister

Das Gemeinsame Krebsregister der Länder Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen, Sachsen-Anhalt und Thüringen, hervorgegangen aus dem ehem. Nationalen Krebsregister der DDR, wird seit dem 1. Januar 1995 auf der Grundlage des Krebsregistergesetzes (KRG)[129] und des Verwaltungsabkommens der beteiligten Länder[130] in Berlin geführt. Vom Arbeitskreis Neue Länder der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erhielten der Berliner Datenschutzbeauftragte und ich den Auftrag, eine Prüfung dieser Einrichtung durchzuführen. Die Prüfung war mehrfach bis nach dem Umzug des Krebsregisters im Oktober letzten Jahres nach Berlin-Kaulsdorf verschoben worden und hatte zum Ziel, die technisch-organisatorischen Maßnahmen am neuen Standort und die Umsetzung der Bestimmungen der §§ 7 und 8 KRG bei der Führung des Registers zu prüfen. Die Prüfung erbrachte folgende Ergebnisse:

- Datenbestände

Das Register verfügt über Meldungen von Krebserkrankungen (jeweils bestehend aus Meldung über Ersterkrankung sowie weiteren Nachmeldungen und ggf. Leichenschauschein) seit 1955, deren Papierform nach den Kriterien Jahrgang der Erstmeldung, Geburtsjahr und Familienname geordnet sind. Eine zusätzliche regionale Zuordnung nach den ehemaligen DDR-Bezirken erfolgte 1989 nachträglich. Von diesem Gesamtbestand sind die Krebserkrankungsjahrgänge (Ersterkrankungen) ab 1961 sukzessive bereits zu DDR-Zeiten in eine EDV-Form übernommen worden. Die seitdem insgesamt registrierten Fälle machen einen Meldebestand von knapp zwei Millionen

---

128 s. unter 7.2.10

129 vom 4. November 1994, BGBl. I S. 3351

130 s. 3. Tätigkeitsbericht unter 7.2.1.2

Krebserkrankungen auf dem jetzigen Territorium der am Register beteiligten Länder aus. Näheres hierzu ist dem "Atlas der Krebsinzidenz in der DDR 1961 bis 1989"[131] zu entnehmen.

Ab 1990 liegen alle Erstmeldungen (nicht Nachmeldungen) dv-mäßig gespeichert vor, die zugehörigen Papierunterlagen wurden hingegen vernichtet. Die Nachmeldungen werden jahrgangsweise eingearbeitet; zum Zeitpunkt der Prüfung erfolgte dies für die Meldungen aus dem Jahre 1993.

Von Betroffenen ist der Wunsch nach Löschung der nach heutigen datenschutzrechtlichen Maßstäben bis 1990 rechtswidrig erhobenen "Altdaten" gegenüber dem Gemeinsamen Krebsregister bisher nicht geäußert worden.

- Datenstruktur und Kompatibilität der Meldebögen

Die Datenstruktur der Einzelmeldungen unterschied sich über die Jahrgänge hinweg zwar nur geringfügig; trotzdem ist eine Vereinheitlichung erforderlich und geschieht laufend. So sind beispielsweise bereits sog. "überschüssige Daten", die gem. § 2 KRG und § 2 Entwurf eines Krebsregisterausführungsgesetzes nicht vorgesehen sind (z. B. über Raucher- und Alkoholanamnese), bereits aus dem EDV-Datenbestand des Krebsregisters entfernt worden. Außerdem werden durch Änderung der Programmversionen inzwischen z. B. die Angaben "Krebs bei Verwandten" und "Anlaß der Erfassung" vom DV-System nicht mehr erfaßt.

Die Verschlüsselung der Identitätsdaten soll gem. § 7 Abs. 1 i. V. m. § 4 Abs. 1 Ziff. 4 KRG durch die Vertrauensstelle erfolgen, wobei der angewandte Schlüssel gem. § 8 Abs. 5 KRG bei einer anderen - durch die Landesregierung zu bestimmenden - Stelle aufzubewahren ist. Genaueres ist hierüber für das Gemeinsame Krebsregister noch nicht entschieden worden, zumal hier bundesweit einheitliche, zumindest aber bundesweit kompatible Lösungen gefunden werden müssen, für die bislang aber nur "Empfehlungen an die Bundesländer zur technischen Umsetzung der Verfahrensweisen gemäß Gesetz über Krebsregister (KRG)" vorliegen.

- Eingabe von Meldungen in das Gemeinsame Krebsregister

Das Eingeben von Meldungen in das Gemeinsame Krebsregister wird durch Dokumentationsassistenten an speziell dafür ausgerüsteten Arbeitsplätzen und menügesteuert durchgeführt. Dabei findet zunächst mittels Eingabe von Name/Vorname/Geburtsdatum und Vorerkrankungen eine Überprüfung statt, ob die Person im System bereits gespeichert ist. Dies ist insofern problematisch, als vor 1990 aus Gründen der Speicherkapazität diese Identitätsdaten in unterschiedlicher Form und Vollständigkeit abgespeichert worden sind und damit bis zum Totalabgleich mit den noch vorhandenen Papierunterlagen permanent die Gefahr von Doppelspeicherungen besteht. Aus diesem Grunde erscheint es unumgänglich, daß in einem künftigen Staatsvertrag bzw. gleichlautenden Krebsregisterausführungsgesetzen der beteiligten Länder (s. unter 7.3.1.3) eine Übergangslösung für das Gemeinsame Krebsregister in bezug auf die in § 1 Abs. 3 KRG vorgeschriebene Schaffung der selbständigen - räumlich, organisatorisch und personell voneinander getrennten - Vertrauens- und Registerstelle gefunden wird. Die weitere Eingabe der Daten läuft bei Erst- und Nachmeldungen praktisch identisch ab: Sitz bzw. genaue Region der Erkrankung, Histologie sowie weitere Spezialdiagnostik, TNM-Klassifikation (internationale Klassifikation der Tumoren), Nachbefund/Nachsorge, Befund aus dem Leichenschauschein. Zur Unterstützung einer validierten Eingabe stehen den Dokumentationsassistenten praktisch für jeden Schritt Hilfsmenüs zur Verfügung. Nach der Abspeicherung erfolgt durch das Programm automatisch eine Trennung der Identitäts- von

---

[131] von M. Möhner, R. Stabenow und B. Eisinger, Ullstein-Mosby-Verlag 1994

den epidemiologischen Daten.

Der Abgleich zwischen dem Krebsregister und den Leichenschauscheinen gem. § 4 Abs. 2 KRG erfolgt erst mit Abschluß der Erfassung des Krebskrankenjahrganges. Davon unabhängig findet zunächst ihre Prüfung auf Vollständigkeit, Lesbarkeit und Plausibilität statt.

- Ausstattung mit Hard- und Software

Im Aufbau befindlich sind getrennte Computernetze mit Serverrechner für die Vertrauens- und die Registerstelle. Das Betriebssystem wird NOVELL 4 sein. Die Software basiert nach wie vor auf Eigenentwicklungen vor 1990, die lediglich ständig erweitert und angepaßt werden. Damit erfolgt zum Zeitpunkt der Prüfung bislang keine Verschlüsselung von Identitätsdaten gem. § 7 Abs. 1 KRG und Bildung von Kontrollnummern gem. § 7 Abs. 2 KRG. Die Identitätsdaten werden jedoch in einer getrennten Datei gespeichert. Zwischenzeitlich ist mir seitens des Krebsregisters mitgeteilt worden, daß mit der Installierung des 2. Fileservers ab Anfang d. J. zunächst in einer Pilotphase die Einführung des Kontrollnummern- und Chiffriersystems beginnen kann. Die Datensicherung läuft nachts oder an Wochenenden (Komplettsicherung) auf ein direkt am Server angeschlossenes Streamer-Laufwerk.

- Sicherheitskonzept

Zum Zeitpunkt der Prüfung war weder ein Sicherheitskonzept erarbeitet noch eine Firma mit deren Erstellung betraut worden. Hierzu sind im Prüfbericht eine Reihe von Maßnahmen aufgeführt worden, die entsprechend den speziellen örtlichen Gegebenheiten unbedingt zu berücksichtigen sind.

Darüber hinaus sind gem. § 1 Abs. 3 KRG Festlegungen zur Schaffung der Vertrauens- und der Registerstelle zu treffen. Sie betreffen vor allem die organisatorische Abschottung der Computernetze (Systembetreuung, Wartung), Verfahrensfestlegungen zum Datenaustausch zwischen beiden und Zugriffsberechtigungen auf die Archivbestände.

7.3.2.2 Andere Krankheitsregister

Der Trend, für spezielle Erkrankungen überregionale, zentrale oder bundesweite Krankheitsregister zu errichten, hält offensichtlich unverändert an[132], so habe ich allein im Berichtszeitraum von Plänen zu fünf weiteren Registern Kenntnis erhalten und hierzu aus datenschutzrechtlicher Sicht Stellung genommen. Im einzelnen handelt es sich dabei um das "Nierenbehandlungsregister QuaSi-Niere", das "Zentralregister für Mukoviszidose in Deutschland", das "überregionale Kopf-Hals-Tumor-Register", das "Deutsche Zentralregister für kindliche Hörstörungen" und das "bundesweite Endoprothesen-Register". Um ansonsten unvermeidliche Wiederholungen zu umgehen, sollen diese nachfolgend zusammengefaßt dargestellt werden:

- Speicherung von anonymen oder personenbezogenen Daten

In jedem Fall sollte vor der Errichtung eines speziellen Krankheitsregisters zunächst überlegt werden, ob die Übermittlung von anonymisierten Datensätzen nicht auch für die Zwecke des jeweiligen Krankheitsregisters ausreicht. Damit wären nämlich alle nachstehenden Aspekte gegenstandslos.

---

[132] s. 2. Tätigkeitsbericht unter 6.3

- Trägerschaft

Bei den in Rede stehenden Krankheitsregistern ist häufig zu klären, ob es sich um "Eigeninitiativen" von engagierten Einzelpersonen oder Personengruppen handelt und insofern nicht um eine öffentliche Stelle. Deshalb ist auf zwei besondere Probleme hinzuweisen:

Aufgrund der Erfahrungen, die mit solchen privaten Rechtskonstruktionen im Freistaat Bayern gemacht wurden, ist hiervon unbedingt abzusehen, da einerseits bei einer nicht gesicherten Weiterführung eines solchen Registers die Übernahme durch einen anderen Träger und damit der zugesicherte Schutz der Daten vor dem Zugriff Unbefugter ungewiß ist. Dies trifft gleichermaßen bei der Einschaltung eines Datentreuhänders, z. B. für Zwecke der Anonymisierung gemeldeter Daten, zu.

Andererseits besteht hierbei die Gefahr, daß die Daten vor einer Inanspruchnahme auch gegen den Willen der datenverarbeitenden Stelle, etwa als Beweismittel in Straf- oder Zivilprozessen aufgrund von Bundesrecht, im Ernstfall nicht gesichert werden könnten. Im Gegensatz dazu bestehen diese Bedenken grundsätzlich nicht, wenn ein solches Register bei einem Krankenhaus oder einem damit betrauten Arzt organisatorisch angebunden wird; damit unterliegt das jeweilige Krankheitsregister dem Beschlagnahmeverbot gem. § 97 Abs. 2 Satz 2 StPO.

Insgesamt erscheint die Anbindung an ein Krankenhaus mit öffentlich-rechtlichem Träger die datenschutzgerechteste Lösung zu sein.

- Zusammenführung vorhandener Register

Im Falle des Zentralregisters für Mukoviszidose sollen auf diesem Gebiet vorhandene Register - nämlich das der ehemaligen Medizinischen Akademie Dresden (MAD) und des Zentrums der Kinderheilkunde an der Goethe-Universität Frankfurt am Main - zusammengeführt werden. Insofern mußte ich darauf hinweisen, daß es sich bei den Daten der MAD um solche handelt, die nach heutigen rechtsstaatlichen Maßstäben unrechtmäßig erfaßt worden sind. Eine vergleichbare Situation bestand in bezug auf die Weiterführung des ehemaligen Nationalen Krebsregister der DDR, weshalb sowohl der Datenschutzbeauftragte des Bundes als auch die der neuen Länder vehement eine gesetzliche Grundlage hierfür gefordert haben, die zunächst übergangsweise mit dem Krebsregistersicherungsgesetz[133] und ab 1. Januar 1995 mit dem Krebsregistergesetz[134] geschaffen wurde, die im Falle der Mukoviszidose-Patienten allerdings fehlt.

- Übermittlung der Daten auf der Grundlage der Einwilligungs-Lösung

Aus datenschutzrechtlicher Sicht sind Bedenken zu erheben, ob bei fehlender gesetzlicher Grundlage in jeder Hinsicht alternativ die Einwilligungs-Lösung gleichwertig in Betracht kommt. Auf die Problematik der möglichen Inanspruchnahme dieser Daten als Beweismittel im Straf- oder Zivilprozeß habe ich bereits hingewiesen.

In den Fällen, wo aufgrund der Altersstruktur der Patienten die Erziehungsberechtigten diese Einwilligungserklärung als gesetzlicher Vertreter gem. §§ 1626, 1929 Abs. 1 BGB anstelle ihres Kindes erteilen, sind darüber hinaus Überlegungen zu Verfahrensweisen anzustellen, wie mit Eintreten der Volljährigkeit der Patienten im Sinne von § 2 BGB diese Erklärung durch eine eigene zu ersetzen wäre. Dies gilt im übrigen auch für alle Daten von Geschwistern, die im Zusammenhang mit Familienanamnesen erhoben werden.

---

133 vom 21. Dezember 1992, BGBl. I S. 2335

134 vom 4. November 1994, BGBl. I S. 3351

Beim Deutschen Zentralregister für kindliche Hörstörungen war diesbezüglich wenigstens an eine Löschungsregelung der Adressen bei Erreichen der Volljährigkeit gedacht worden. Auch eine solche Regelung würde allerdings in bezug auf die bis dahin gespeicherten personenbezogenen Daten ins Leere laufen, wenn der Betroffene nicht auf sein mit Erreichen der Volljährigkeit von den Erziehungsberechtigten auf ihn übergegangenes Widerspruchsrecht in geeigneter Weise hingewiesen würde. Dazu reicht es allerdings nicht, hierauf lediglich im Informationsblatt an die Eltern einzugehen. Vielmehr ist erforderlich, daß bei diesen Krankheitsregistern die Einzelmeldungen in regelmäßigen Abständen unter diesem Aspekt einer Revision unterzogen werden und jeder Volljährige durch Anschreiben auf sein Widerspruchsrecht hingewiesen wird. Eine vergleichbare Regelung müßte für die Widerspruchsrechte von Geschwistern bei familienanamnestischen Erhebungen erwogen werden.

- Einwilligungserklärung

In allen Fällen waren die vorgesehenen Einwilligungserklärungen gem. § 4 Abs. 2 Bbg DSG zu monieren. So war die registerführende Stelle nicht immer eindeutig bezeichnet; außerdem fehlte in der Regel der Hinweis, daß die Einwilligung verweigert und mit Wirkung für die Zukunft widerrufen werden kann, sowie die Darlegung der entsprechenden Rechtsfolgen.

Die Einwilligungserklärung oder Durchschläge hiervon sollten nicht unbedingt in Patientenakten abgelegt werden. Wenn dies aber erfolgt, dann muß für den Fall, daß der Betroffene von seinem Widerrufsrecht Gebrauch macht, die Vernichtung der Einwilligungserklärung sichergestellt werden. Da primär die Einwilligungserklärung der registerführenden Stelle als Nachweis darüber dient, daß sie befugt und berechtigt ist, personenbezogene Daten des Betroffenen zu verarbeiten, sollte demzufolge die Einwilligungserklärung auch dort vorliegen.

- Zweck der Errichtung

Während bisher Krankheitsregister ausschließlich für medizinisch-wissenschaftliche Zwecke errichtet wurden, geschieht dies nunmehr auch teilweise im Zusammenhang mit § 137 SGB V. Danach sind zugelassene Krankenhäuser verpflichtet, sich an Maßnahmen zur Qualitätssicherung zu beteiligen. Für diesen Zweck wäre in der Regel nur die Angabe der Einrichtung erforderlich, womit die Daten lediglich personenbeziehbar sind. Bei gleichzeitiger Nutzung dieser Datenbestände sowohl für diese als auch für wissenschaftliche Zwecke bietet das Treuhändermodell - wie beispielsweise beim Nierenbehandlungsregister QuaSi-Niere angedacht - einen geeigneten Ausweg, beiden gerecht zu werden.

7.4 Frauen

7.4.1 Regelungen zur Gleichstellungsbeauftragten im Hochschulbereich

Die auf Autonomie bedachten Hochschulen hatten seinerzeit vor Verabschiedung des Landesgleichstellungsgesetzes (LGG)[135] erreicht, daß dessen Geltungsbereich sich gem. § 2 Abs. 3 LGG nicht auch auf sie erstreckt. Dagegen wäre nichts einzuwenden gewesen, hätte die Landesregierung möglichst gleichzeitig für vergleichbare Regelungen auch im Hochschulbereich gesorgt. Dies ist jedoch erst Ende vergangenen Jahres mit dem Entwurf eines Zweiten Gesetzes zur Änderung des Brandenburgischen Hochschulgesetzes und - "da sich hierbei datenschutzrechtliche Bedenken nicht ergeben haben" - ausdrücklich ohne die Beteiligung meiner Behörde geschehen.

---

[135] vom 4. Juli 1994, GVBl. I S. 254

Erst im Zusammenhang mit den abschließenden Beratungen im federführenden Ausschuß für Wissenschaft, Forschung und Kultur konnte ich noch rechtzeitig auf diesbezügliche elementare Regelungsdefizite bzw. -mängel hinweisen. So waren einerseits lediglich einzelne Gesichtspunkte des § 22 LGG unsystematisch übernommen worden. Anderseits bestand bei der vorgesehenen Neufassung des § 87 Brandenburgisches Hochschulgesetz (BbgHG) faktisch die Gefahr, daß die dort vorgesehenen datenschutzrechtlichen Regelungen, durch die auch unverzichtbare Rechte Dritter garantiert werden müssen, in Abhängigkeit von hochschulinternen Kompetenzzuweisungen für die Gleichstellungsbeauftragte gebracht würden. Dies konnte auch mit dem Hinweis auf die Hochschulautonomie nicht gerechtfertigt werden. Insbesondere war vermieden worden, die Gleichstellungsbeauftragte als datenverarbeitende Stelle gem. § 3 Abs. 4 Nr. 1 Bbg DSG zu definieren, was vor allem die Eigenverantwortlichkeit für die von ihr zu verarbeitenden Daten nach außen, aber auch die Abschottung gegenüber der Hochschulleitung in Frage gestellt hätte.

Für mich war es erfreulich, daß sich die Abgeordneten die von mir gegebenen Hinweise zu eigen gemacht haben und es dadurch bei der parlamentarischen Behandlung des Entwurfes gelungen ist, in § 87 Abs. 2 BbgHG sowohl die Frage der Beteiligung der Gleichstellungsbeauftragten bereits an Bewerbungsverfahren, als auch die Frage der datenverarbeitenden Stelle normenklar einzuarbeiten.

7.4.2 Frauenförderverordnung

Am Verfahren zum Erlaß der Verordnung über die bevorzugte Berücksichtigung von Unternehmen bei der Vergabe öffentlicher Aufträge zur Förderung von Frauen im Erwerbsleben (Frauenförderverordnung - FrauFöV) auf der Grundlage des § 14 LGG hat mich das MASGF frühzeitig beteiligt.

Ziel der Verordnung ist es, zur Verbesserung der Berufschancen von Frauen im Erwerbsleben einen Anreiz für Unternehmen zu schaffen, in gleicher Weise Frauen wie Männer zu beschäftigen. Infolgedessen soll bei einem gleichwertigen Angebot derjenige der Bieter bevorzugt werden, der sich der Gleichstellung von Frauen im Erwerbsleben angenommen hat. Dieser Einsatz für die Frauenförderung muß sich in einem höheren Frauenanteil an Beschäftigten überhaupt und/oder in qualifizierten Positionen niedergeschlagen haben. Um dies nachzuweisen, wird den Firmen anheimgestellt, Listen auszufüllen, in denen z. B. die Anzahl der Frauen im Verhältnis zur Anzahl der Beschäftigten und die Bruttolohnausgaben der Gruppe der Frauen sowie der Gruppe der Männer im Vergleich zu den Bruttolohnausgaben der Beschäftigten insgesamt ausgewiesen sind.

Ich habe darauf hingewiesen, daß bei Bietern mit wenigen weiblichen und/oder wenigen männlichen Beschäftigten nicht ausgeschlossen werden könne, daß einer bestimmten Person ein bestimmtes Bruttogehalt zugeordnet werden könne. Besonders evident stellt sich dieses Problem bei einem Bieter, der sich zur Vertragsausfüllung eines Unterauftragnehmers bedient, der die entsprechenden Angaben wiederum über den Bieter vorlegen muß, der in der Regel aufgrund seiner Kenntnisse konkret wissen dürfte, um welchen Mitarbeiter seines Unterauftragnehmers es sich dabei handelt.

Das Ministerium hat meinen Hinweis insoweit berücksichtigt, als Unternehmen, in denen entweder nur eine Frau oder nur ein Mann tätig ist, nur die Anzahl der im Unternehmen sozialversicherungspflichtig beschäftigten Männer und Frauen angeben müssen und die Kennziffer, die sich über die Angaben zu den Bruttolohnausgaben ergibt, selbst errechnen.

Entsprechend den für die Statistiken geltenden Grundsätzen[136] hatte ich zunächst eine solche Selbstberechnung dann gefordert, wenn es in der jeweiligen Vergleichsgruppe weniger als drei Beschäftigte gibt. Nachdem das Ministerium jedoch auch den Fall mit einbezogen hatte, daß der Anteil eines Betroffenen am durchschnittlichen Bruttostundenlohn eine Dominanz aufweisen könnte, wie dies beispielsweise bei einem außertariflich bezahlten Mitarbeiter der Fall sein könnte und weil eine Veröffentlichung der Daten wie im Falle der Statistiken nicht erfolgen soll, habe ich unter gewissen Bedenken die geplante Regelung akzeptiert.

Als ich zur Vorbereitung meines Tätigkeitsberichtes die neueste Fassung des Entwurfs der FrauFöV erbat, berücksichtigte diese für mich überraschend den zuletzt genannten Fall jedoch nicht mehr, was ich beim MASGF monierte.

7.4.3 Runderlaß zur Kindertagesstätten-Betriebskostenverordnung

Vor dem Hintergrund eines Berichts des Landesrechnungshofes hat das MASGF am 28. August 1995 einen Runderlaß an die örtlichen Träger der öffentlichen Jugendhilfe im Land Brandenburg gerichtet, wonach für die Gewährung und Verwendung von Landeshaushaltsmitteln für die Kindertagesbetreuung nicht mehr wie bisher die schriftliche Mitteilung der Zahl der gemeldeten Kinder gegenüber dem Landesjugendamt genügt, sondern aufgelistet die betreuten Kinder nachzuweisen sind.

Auf diese geänderte Praxis wurde ich durch eine Anfrage eines örtlichen Trägers der öffentlichen Jugendhilfe aufmerksam gemacht, dem von verschiedenen Jugendämtern unterschiedliche Erfassungsbögen übersandt worden waren, die im Laufe des Februars 1996 ausgefüllt bei den Jugendämtern vorgelegt werden sollten.

Ich habe das MASGF umgehend darauf hingewiesen, daß der Wortlaut des einschlägigen § 7 Abs. 2 Nr. 1 Kindertagesstätten-Betriebskosten VO (KitaBKVO)[137], der ausdrücklich von der Zahl der belegten Plätze spricht, die geänderte Verfahrensweise nicht deckt. Insbesondere trifft die Vorschrift keine Regelung dazu, daß und welche personenbezogenen Daten in diesem Zusammenhang zu übermitteln sind. Auch ein Vergleich mit § 4 KitaBKVO, wonach das für die Finanzierung zuständige Ministerium in regelmäßigen Abständen die tatsächlichen Betriebskosten der Kindertagesstätten anhand einer Stichprobe ermittelt und die Jugendämter und Träger von Kindereinrichtungen ausdrücklich verpflichtet sind, die hierfür erforderlichen Angaben zu machen und auf Aufforderung zu belegen, spricht dagegen, daß § 7 Abs. 2 KitaBKVO, der vergleichbare Formulierungen gerade nicht enthält, entsprechende Datenverarbeitungsbefugnisse eröffnet.

Darüber hinaus habe ich darauf hingewiesen, daß die mir vorgelegten Erhebungsbögen erkennen lassen, daß schon innerhalb der Jugendämter keine Einigkeit darüber besteht, welche Daten tatsächlich erforderlich sind. So wird es z. B. in einem Bogen für notwendig angesehen, die Adresse des Kindes anzugeben, in einem anderen Formular wird statt dessen die Klassenstufe und das Abschlußdatum des Vertrages abgefragt.

Angesichts der von den Jugendämtern den Trägern der Einrichtungen gesetzten Termine habe ich das MASGF umgehend um Stellungnahme bzw. Abänderung des o. g. Rundschreibens gebeten. Ich habe weiter darauf hingewiesen, daß aufgrund des in § 7 Abs. 2 KitaBKVO genannten Stichtages 1. Februar 1996 bereits Listen der zu betreuenden Kinder an das Landesjugendamt übermittelt worden sein müßten. Diese sind entsprechend der oben dargestellten Rechtsauffassung unverzüglich gem. § 19 Abs. 2 Bbg DSG zu löschen, d. h. in diesem Fall zu vernichten. Das MASGF hat bisher mir gegenüber nicht auf mein Schreiben reagiert.

---

136 s. 3. Tätigkeitsbericht unter 3.9.1

137 vom 8. Dezember 1992, GVBl. II S. 57

8 Ernährung, Landwirtschaft und Forsten

8.1 Private Kontrollstellen des ökologischen Landbaus

Wie mir im Rahmen der Zusammenarbeit mit meinen Kollegen bekannt wurde, gibt es bei der Umsetzung der Verordnung (EWG) Nr. 2092/91 des Rates vom 24. Juni 1991[138] über den ökologischen Landbau und die entsprechenden landwirtschaftlichen Erzeugnisse und Lebensmittel verschiedene datenschutzrechtliche Probleme. Das habe ich zum Anlaß genommen, die Rechtsstellung der privaten Kontrollstellen, die staatlicherseits mit der Kontrolle der Betriebe des ökologischen Landbaus beauftragt werden, im Land Brandenburg im Hinblick auf die Kontrollmöglichkeit durch meine Behörde zu überprüfen.

In meiner Stellungnahme gegenüber dem Ministerium für Ernährung, Landwirtschaft und Forsten (MELF) habe ich ausgeführt, daß die privaten Kontrollstellen als beliehene Unternehmen tätig werden. Sie sind als juristische Personen des Privatrechts mit der hoheitlichen Wahrnehmung einer Verwaltungsaufgabe im eigenen Namen, auf eigene Rechnung sowie in eigener Verantwortung betraut. Das öffentlich-rechtliche Auftragsverhältnis wird einerseits durch o. g. Verordnung und andererseits durch den konkreten Beleihungsakt, den Zulassungs- bzw. Duldungsbescheid des MELF, näher bestimmt.

Der Beliehene ist, als selbständiger Hoheitsträger nach außen auftretend, Behörde i. S. von § 1 Abs. 4 Verwaltungsverfahrensgesetz (VwVfG)[139] und unterliegt aufgrund seiner Rechtsnatur bereits der Kontrolle des Landesbeauftragten für den Datenschutz. Dieser Gedanke wurde im Zuge der Novellierung des Brandenburgischen Datenschutzgesetzs mit der Ergänzung in § 2 Abs. 1 Satz 3 klargestellt. Da es sich bei den privaten Kontrollstellen um öffentliche Stellen i. S. v. § 2 Abs. 1 Satz 3 Bbg DSG handelt, ist eine vertragliche oder durch Verwaltungsakt festzulegende Begründung von Kontrollrechten meiner Behörde nicht erforderlich.

Obwohl die privaten Kontrollstellen der Aufsicht des LfD unterliegen, sind die Mitarbeiter der Kontrollstelle nach dem Verpflichtungsgesetz[140] zu verpflichten. Ich habe deshalb das MELF gebeten, die Leitlinien des Ministeriums zum "Kontrollverfahren nach der Verordnung (EWG) Nr. 2092/91 des Rates vom 24. Juni 1991 über den ökologischen Landbau und die entsprechende Kennzeichnung der landwirtschaftlichen Erzeugnisse und Lebensmittel" (Stand: 16. März 1994) in Punkt 1.1.1 zu ändern bzw. zu ergänzen. Hierzu habe ich einen Text vorgeschlagen, der die zugelassenen Kontrollstellen als beliehene Unternehmen i. S. v. § 2 Abs. 1 Satz 3 Bbg DSG ausweist und die Verpflichtung der Mitarbeiter nach dem Verpflichtungsgesetz als zwingendes Erfordernis regelt. Das MELF hat insoweit Handlungsbedarf erkannt und sich mit meinem Regelungsvorschlag einverstanden erklärt.

8.2 Zentrale Erfassung von Zirkusbetrieben

Wie mir das MELF mitteilte, ist eine zentrale Erfassung von Zirkusbetrieben in der Bundesrepublik Deutschland im Landesamt für Ernährung, Landwirtschaft und Flurneuordnung (LELF) in Frankfurt (Oder) beabsichtigt. Dagegen habe ich grundsätzlich nichts einzuwenden. Das Führen des Registers wird vor allem von Fachleuten deswegen für

---

138 ABl. EG Nr. L 198 S. 1

139 vom 25. Mai 1976, BGBl. I S. 1253

140 vom 2. März 1974, BGBl. I. S. 469

erforderlich gehalten, weil dadurch die Kontrolle und Überwachung der Zirkus-Unternehmen mit ihren ständig wechselnden Standorten (kreis- oder länderübergreifend) erleichtert wird. Dies soll insbesondere für eine tierschutzrechtlich gebotene Beseitigung und Ahndung festgestellter Mißstände und für die unterschiedlichen Genehmigungsvoraussetzungen zutreffen.

Da es für eine diesbezügliche Datenverarbeitung derzeit im Tierschutzgesetz (TierSchG)[141] keine Rechtsgrundlage gibt, habe ich im Hinblick auf das "Volkszählungsurteil"[142] erklärt, daß der Bundesgesetzgeber die erforderliche gesetzliche Grundlage für die beabsichtigte Datenverarbeitung schaffen muß. In diesem Zusammenhang habe ich dem MELF einen entsprechenden Regelungsvorschlag unterbreitet. Mittels einer Öffnungsklausel, die die Zuständigkeit der Länder für die Einrichtung einer Zentralregistratur regelt, bliebe die Ausführung des TierSchG Ländersache und geriete nicht durch eine Verordnungsermächtigung in die Regelungskompetenz des Bundesministers. Die Öffnungsklausel sollte so normenklar formuliert sein, daß die für die Aufgabenerfüllung erforderlichen Daten ausdrücklich im Gesetz benannt werden. Ohne dem MELF in seiner fachlichen Kompetenz vorgreifen zu wollen, habe ich vorgeschlagen, folgende Daten in dem Register zu erfassen:

- der Name des Zirkus und der verantwortlichen Person,
- die erlaubniserteilende Behörde nach § 22 TierSchG,
- die Behörden, die Verwaltungsakte gegen einen Zirkus erlassen haben sowie
- Anordnungen nach § 16 a TierSchG und Verurteilungen nach § 17 TierSchG.

Wie mir das MELF mitteilte, wurde mein Vorschlag inzwischen in einen derzeit noch nicht veröffentlichten Referentenentwurf des Bundeslandwirtschaftsministeriums aufgenommen.

8.3 Fragebögen der Brandenburgischen Landestierärztekammer

Für das gesetzlich vorgeschriebene Anmeldeverfahren von Tierärzten nach § 5 Heilberufsgesetz (HeilBerG)[143] i. V. m. der Meldeordnung der Tierärztekammer Brandenburg[144] verwendet die Landestierärztekammer Brandenburg (LTK Brandenburg) zwei verschiedene Erhebungsformulare:

- den "Tierärztekammermeldebogen" und
- den Bogen "Art der Tätigkeit".

Bei der Überprüfung des "Tierärztekammermeldebogens" mußte ich feststellen, daß nicht alle vom Betroffenen geforderten Angaben auf einer gesetzlichen Grundlage beruhen und die Freiwilligkeit der Angabe nicht als solche gekennzeichnet ist. Ich habe deshalb die LTK Brandenburg darauf hingewiesen, daß für den Tierarzt durch einen entsprechenden Hinweis erkennbar sein muß, daß ihm z. B. das Ausfüllen des Feldes "Versandanschrift für Deutsches Tierärzteblatt" freigestellt ist. Die LTK Brandenburg hat mir zugesichert, auf die Freiwilligkeit der Angabe hinzuweisen.

Des weiteren habe ich den Erhebungsbogen "Art der Tätigkeit" bemängelt. Denn in diesem Bogen werden den Betroffenen neben Grunddaten auch die Privat- und Dienstanschrift, die bereits mit dem "Tierärztekammermeldebogen" erhoben wurden, abverlangt. Ich halte diese

---

141 i. d. Fass. vom 17. Februar 1993, BGBl. I S. 254

142 BVerfGE 65, 1

143 vom 28. Januar 1992, GVBl. I S. 30

144 vom 27. Oktober 1990

doppelte Datenerhebung im Rahmen der Aufgabenerfüllung der LTK Brandenburg für nicht erforderlich und habe deshalb vorgeschlagen, diese Felder zu streichen oder auf die Freiwilligkeit der Angaben im Hinblick auf das Aufklärungsgebot hinzuweisen. Für den Fall, daß die LTK Brandenburg beide Erhebungsbögen an einen Tierarzt versendet, wird sie den Betroffenen die doppelte Grunddatenerhebung freistellen. Sollte jedoch der Erhebungsbogen für Veränderungsmeldungen bereits registrierter Kammerangehöriger versandt werden, ist die neue Anschrift - und insoweit schließe ich mich der Meinung der LTK Brandenburg an - für deren Aufgabenerfüllung erforderlich.

Die Überprüfung der Erhebungsbögen habe ich erneut zum Anlaß genommen, auch die LTK Brandenburg auf eine datenschutzgerechte Formulargestaltung im Hinblick auf das Aufklärungsgebot hinzuweisen (s. unter 2.3). Die LTK Brandenburg wird künftig ein Merkblatt mit den entsprechenden Hinweisen erstellen und den Betroffenen zusammen mit den Erhebungsbögen aushändigen.

8.4 Abrechnung von Telefongebühren bei Förstern

Anfang des Jahres teilte mir das MELF mit, daß es beabsichtige, neue Regelungen für die Nachweisführung von Telefongesprächen für Förster unter Einbeziehung des Einzelverbindungsnachweises der Telekom zu erlassen und bat mich um entsprechende Beratung. Dies ist u. a. in einem gemeinsamen Gespräch mit Mitarbeitern des Ministeriums und Vertretern einer Revierförsterei geschehen.

Die Besonderheit bei den Förstern bestehe darin, daß in den meisten Fällen Arbeitsplatz und Wohnung identisch sind. Eine generelle Trennung der privaten und dienstlichen Telefongespräche durch die Bereitstellung zweier getrennter Anschlüsse in der Wohnung des Försters sei gegenwärtig aus technischen und finanziellen Gründen nicht realisierbar. Bei der Aufzeichnung der Gesprächsverbindungen gehe es nicht nur um eine Trennung dienstlicher und privater Telefongebühren, sondern auch um die Anforderung der Finanzämter zu erfüllen. Unter den Förstern bestehe ein großes Interesse an der Nutzung von Einzelverbindungsnachweisen, da das gegenwärtige Verfahren der Gesprächsaufzeichnung eine erhebliche Belastung darstelle.

Für die Abrechnung der Telefongebühren sind - sofern nur ein einzelner Anschluß zur Verfügung steht - die beiden folgenden Fälle zu unterscheiden:

1. Der Förster verfügt über einen Privatanschluß und bekommt die Kosten der geführten Dienstgespräche vom Arbeitgeber erstattet.

2. Der Förster verfügt über einen Dienstanschluß und hat die Kosten für die geführten Privatgespräche an den Arbeitgeber zu erstatten.

Aus der Sicht des Datenschutzes halte ich unter folgenden Bedingungen die Einbeziehung des Einzelverbindungsnachweises der Telekom für möglich, ohne bereits eine abschließende Beurteilung vorgenommen zu haben:

- Die Nutzung des Einzelverbindungsnachweises darf nur auf freiwilliger Basis mit Zustimmung aller im Haushalt des Försters lebenden Personen erfolgen und darf für Abrechnungszwecke nicht gefordert werden und ist unzulässig, wenn der betreffende Telefonanschluß von mehreren Förstern gemeinsam dienstlich genutzt wird.

- Bei Privatanschlüssen kennzeichnet der Förster im Einzelverbindungsnachweis, den er gemeinsam mit seiner monatlichen Telefonrechnung erhält, seine Dienstgespräche und ermittelt selbst die vom Arbeitgeber zu erstattenden Gesamtkosten. Diese Summe überträgt er auf ein Antragsformular, das dem Forstamt für die Erstattung der Kosten

zugesandt wird, und verpflichtet sich gleichzeitig, den Einzelverbindungsnachweis für eine bestimmte noch festzulegende Zeit (denkbar sind 4 - 8 Wochen) zu Kontrollzwecken durch das zuständige Forstamt bei sich aufzubewahren.

- Bei Dienstanschlüssen ist zu sichern, daß der Einzelverbindungsnachweis dem Förster direkt ohne vorherige Einsichtnahme durch das Forstamt zugesandt wird. Der Förster kennzeichnet darin seine Privatgespräche und ermittelt selbst den dem Arbeitgeber dafür zu erstattenden Gesamtbetrag. Der Einzelverbindungsnachweis wird für eine bestimmte Zeit beim Förster für Kontrollzwecke aufbewahrt.

Inwieweit mit den genannten Bedingungen die Forderungen der Finanzämter befriedigt werden können, ist noch zu klären. Ich meine, daß hierfür die monatlichen Gesamtsummen für dienstliche bzw. private Gespräche ausreichen müßten. Es wäre jedenfalls unzulässig, daß Arbeitgeber aufgrund von Anforderungen der Finanzämter Einblick in Aufzeichnungen von Telefongesprächen erhalten, die zur Leistungs- oder Verhaltenskontrolle geeignet sind oder Einblick in die Telefongewohnheiten der Betroffenen - besonders bei Privatgesprächen - gewähren.

8.5 Wildhandelsüberwachungsverordnung

Im Berichtszeitraum hatte ich Gelegenheit, zu dem Entwurf der Verordnung zur Überwachung und Kontrolle des Wildhandels (Wildhandelsüberwachungsverordnung - WildÜV)[145] gegenüber dem MELF Stellung zu nehmen.

Ziel dieser Verordnung ist neben dem Schutz der Verbraucher eine Verschärfung der Überwachung und Kontrolle des Wildhandels im Land Brandenburg gerade im Hinblick auf den beträchtlichen Anstieg der Jagdwilderei. Jedes erlegte, zum menschlichen Verzehr vorgesehene Stück Wild wird künftig mit einer Wildmarke in der Brust- bzw. Bauchwand gekennzeichnet. Anschließend erfolgt neben der Eintragung der Wildmarkennummer auch der Eintrag des Namens des Erlegers in den Wildursprungschein. Die Händler sind verpflichtet, ein Wildhandelsbuch zu führen, aus welchem die Herkunft der Tiere vom Verbraucher bis zum Erleger zurückverfolgt werden kann.

In meiner Stellungnahme habe ich erklärt, daß die Erhebung der personenbezogenen Daten auf dem Wildursprungschein einer gesetzlichen Grundlage bedarf und angeregt, das Formular eines solches Scheines zur Anlage der Verordnung zu machen. Damit wird die Datenerhebung Regelungsgegenstand der Verordnung. Des weiteren habe ich das MELF darauf hingewiesen, daß in dem Entwurf zur WildÜV eine Regelung zur beabsichtigten automatisierten Datenverarbeitung fehlt. Meine Hinweise sind sämtlich in die WildÜV übernommen worden. Für die konstruktive Zusammenarbeit mit dem MELF möchte ich mich an dieser Stelle bedanken.

9 Umwelt, Naturschutz und Raumordnung

9.1 Datenaustausch im Umweltbereich - Bund/Länder-Vereinbarung

Aufgrund einer Verwaltungsvorschrift, die seit dem 30. August 1995 in Kraft ist, sind Bund und Länder übereingekommen, einen gemeinsamen zentralen Stoffdatenpool Bund/Länder zu schaffen. Von diesem Vorhaben habe ich erst durch andere Datenschutzbeauftragte erfahren und mußte deshalb das Ministerium für Umwelt, Naturschutz und Raumordnung

---

145 vom 25. März 1996, GVBl. II S. 250

(MUNR) wegen einer Beteiligung anmahnen, bevor ich schließlich die Gelegenheit zur Stellungnahme bekam.

Es stellte sich heraus, daß der Entwurf als Datenschutzklausel lediglich die allgemeine Feststellung enthielt: "die Bestimmungen des Datenschutzes von Bund und Ländern und die sonstigen Vorschriften zur Geheimhaltung werden beachtet". Dabei war ernsthaft beabsichtigt, in den Datenaustausch - obwohl für den beabsichtigten Zweck nicht erforderlich - auch personenbezogene Daten, z. B. über Dioxinbelastung von Muttermilch, mit einzubeziehen.

Deshalb habe ich das MUNR vorsorglich darauf hingewiesen, daß auch im Umweltbereich die Übermittlung personenbezogener Daten nur zulässig ist, soweit gem. § 4 Abs. 1 Bbg DSG dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt. Die Zulässigkeit der Weitergabe personenbezogener Einzeldaten kann auf keinen Fall allein auf die Verwaltungsvereinbarung gestützt werden. Mit dem MUNR konnte letztendlich Konsens darüber erzielt werden, daß der vorgesehene § 5 dieser Verordnung nur deklaratorischen Charakter besitzt und nicht als konstitutive Regelung zu verstehen ist.

9.2 Erlaß zum Umweltinformationsgesetz

In meinem 2. Tätigkeitsbericht[146] hatte ich über die Aufgaben des Gesetzgebers bei der Umsetzung der Richtlinie 90/313/EWG des Rates vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt in nationales Recht berichtet. Der Gesetzgeber hat inzwischen die erforderliche bundeseinheitliche gesetzliche Grundlage in Form des Umweltinformationsgesetzes (UIG)[147] geschaffen.

Um den nachgeordneten Behörden eine Interpretationshilfe zu geben und eine einheitliche Anwendung des UIG zu gewährleisten, hat das MUNR einen Erlaß zum UIG erarbeitet, zu dessen 1. Entwurf es mir bereits im hausinternen Beteiligungsverfahren Gelegenheit zur Stellungnahme gab. Zum vorgenannten Entwurf konnte ich grundsätzlich meine Zustimmung erteilen, habe jedoch das MUNR gebeten, u. a. folgende Hinweise vor Verabschiedung des Erlasses zu beachten:

- In § 7 Abs. 1 Nr. 2 regelt das UIG, daß ein Anspruch auf Informationen wegen der Dauer verwaltungsbehördlicher Verfahren hinsichtlich der Daten ausscheidet, die aufgrund dieses Verfahrens bekannt werden (mit oder nach Beginn dieses Verfahrens). Aus Gründen einer fehlenden Richtlinienkonformität sowie anhängiger Beschwerdeverfahren vor der Europäischen Kommission empfahl das MUNR den Behörden in der Einzelfallprüfung, daß die Informationen ungeachtet des gesetzlichen Ausschlußgrundes auf freiwilliger Basis auch während der Dauer verwaltungsbehördlicher Verfahren herausgegeben werden können. Den Tenor dieser Aussage konnte ich sehr wohl nachvollziehen; die Argumentation des MUNR, daß der gesetzliche Ausschlußgrund zur Vermeidung weiterer Beschwerdeverfahren vor der Europäischen Kommission nicht zu beachten sei, konnte so jedoch nicht meine Zustimmung finden. Damit könnte das geltende Recht, soweit es nicht verfassungswidrig ist, vielfach ausgehebelt und für individuelle Zwecke mißbraucht werden. Deshalb habe ich das MUNR um eine Überarbeitung in diesem Punkt gebeten und gleichzeitig angeregt, diesen stärker auf das grundrechtlich geschützte Informationszugangsrecht sowie auf Art. 21 Abs. 4 der Verfassung des Landes Brandenburg[148] abzustellen. In seinem 3. Entwurf zum UIG-Erlaß

---

146 s. unter 8.1

147 vom 8. Juli 1994, BGBl. I S. 1490

148 vom 20. August 1992, GVBl. I S. 298

hat das MUNR ungeachtet meines Hinweises diesen nur sprachlich überarbeitet.

- Zu den Ausführungen zu § 8 UIG habe ich aufmerksam gemacht, daß diese widersprüchlich sind. Einerseits soll eine Abwägung schutzwürdiger Interessen erst dann zum Tragen kommen, wenn personenbezogene Daten nicht unkenntlich gemacht werden können; andererseits müssen personenbezogene Daten jedoch im Falle der Akteneinsicht unkenntlich gemacht werden, wenn sie nicht offenbart werden dürfen. Erfreulicherweise ist dieser Widerspruch beseitigt worden.

10 Stadtentwicklung, Wohnen und Verkehr

10.1 Änderung des Straßenverkehrsgesetzes - Europaweites Zentralregister in Vorbereitung

10.1.1 Beteiligungsrechte des Landesbeauftragten für den Datenschutz vereitelt

Seit 1991 sind die Verkehrsverwaltungen des Bundes und der Länder damit befaßt, die Umsetzung der sog. 2. EG-Führerscheinrichtlinie[149] in nationales Recht zu realisieren. Das Ministerium für Stadtentwicklung, Wohnen und Verkehr (MSWV) übersandte mir den 250 Seiten umfassenden Gesetzentwurf mit der Bitte um Stellungnahme binnen dreier Arbeitstage. Dies mußte ich ablehnen, zumal ich es auch für wenig sinnvoll hielt, zu Gesetzentwürfen des Bundes Stellung zu nehmen, wenn bereits abzusehen sein, daß das Ministerium in dem vom Bund vorgegebenen Verfahren offenbar gar keine Möglichkeit mehr habe, meine Stellungnahme bei der Abgabe des eigenen Votums zu berücksichtigen.

Soweit ich deshalb durch das administrative Gesetzgebungsverfahren meine Beteiligungsrechte verletzt sah, antwortete mir das Ministerium, daß mein Standpunkt von ihm geteilt werde; die diesbezügliche Vorgehensweise des Bundesministeriums für Verkehr (BMV) sei seit geraumer Zeit bekannt und schon häufig Gegenstand allgemeiner und insbesondere auch vom MSWV geübter Kritik gewesen. Das MSWV werde auch in Zukunft darauf hinwirken, daß das BMV nicht von vornherein verhindere, daß mir vom MSWV eine datenschutzrechtliche Überprüfung von Gesetzentwürfen ermöglicht werden könne.

10.1.2 Das Zentrale Fahrerlaubnisregister zum europaweiten Datenabruf - Ein Zentrales Einwohnerregister durch die Hintertür

Dieses Register, in dem zunächst rund 50 Mio. Fahrerlaubnisinhaber gespeichert werden sollen, soll europaweit ermöglichen, im automatisierten Abrufverfahren festzustellen, ob ein Fahrzeugführer über die entsprechende Fahrerlaubnis verfügt. Dazu ist eine zentrale Speicherung der Daten aller Fahrerlaubnisinhaber jedoch nicht erforderlich, denn anhand der nach wie vor mitzuführenden Fahrerlaubnis ist die ausstellende Behörde leicht festzustellen und können etwaige Fragen ohne weiteres auch bei der zuständigen örtlichen Fahrerlaubnisbehörde geklärt werden.

Das Register ist auch nicht erforderlich, um den Erwerb mehrerer Führerscheine in verschiedenen Ländern zu verhindern. Ob einem deutschen Bewerber für einen ausländischen Führerschein die Fahrerlaubnis bereits entzogen wurde oder diese durch Punkte belastet ist, kann durch eine Anfrage beim Verkehrszentralregister festgestellt werden. Im übrigen ist der Entzug der Fahrerlaubnis unabhängig davon wirksam, ob und welchen Führerschein der Betroffene noch "als Papier" besitzt. Auch läßt der geringe Anreiz, bereits vorsorglich für den Fall eines Fahrerlaubnisentzugs den Aufwand für den Erwerb eines Ersatzführerscheins zu treiben, diesen Fall eher als eine seltene Ausnahme erscheinen.

---

149 Richtlinie des Rates 91/439/EWG vom 29. Juli 1991, ABl. EG Nr. L 237 S. 1

Eine solche Ausnahme rechtfertigt nicht den Aufbau großer Dateien zum Online-Zugriff auf personenbezogene Daten, der als erhebliche Einschränkung des Rechts auf informationelle Selbstbestimmung stets im überwiegenden Allgemeininteresse erforderlich sein muß. Ein zentrales Fahrerlaubnisregister, das gleichsam per Knopfdruck ohne nennenswerten Mehraufwand jederzeit in ein zentrales Einwohnerregister umgewandelt werden kann, birgt unkalkulierbare Risiken für das Grundrecht auf informationelle Selbstbestimmung in sich, die völlig außer Verhältnis zu dem mit dieser Zentraldatei angestrebten Nutzen steht. Es läßt bereits "den gläsernen Autofahrer" als künftige Realität erahnen.

Angeblich soll den Ländern mit dem neuen "Bundeszentralregister" nunmehr die Möglichkeit eröffnet werden, die Kosten für die eigenen örtlichen Fahrerlaubnisregister durch deren sukzessiven Abbau einzusparen. Dies ist jedoch illusorisch. Denn zum einen ist die Automatisierung der örtlichen Register bereits in vollem Gange und wird bei der Arbeitsaufnahme des Zentralregisters längst abgeschlossen sein. Zum anderen können die örtlichen Verkehrsbehörden zur Wahrnehmung ihrer Aufgaben auch gar nicht auf die eigenen Datenbestände verzichten. Es ist deshalb nicht damit zu rechnen, daß von der vorgesehenen Verzichtsmöglichkeit überhaupt Gebrauch gemacht werden wird; statt dessen würde in der Regel die Errichtung des Zentralen Fahrerlaubnisregisters eine Doppelspeicherung zur Folge haben, die datenschutzrechtlich abzulehnen ist.

Die zunächst bundesweite, später dann sicherlich europaweite Zentralisierung personenbezogener Datenbanken zur Straffung des Verwaltungsvollzugs stellt sich im übrigen als schleichende Aushöhlung des Föderalismus, insbesondere der verfassungsrechtlichen Ordnung nach Art. 84 und 85 des Grundgesetzes dar, und entzieht die im Verwaltungsvollzug der Länder anfallenden personenbezogenen Daten der verfassungsrechtlich vorgegebenen Kontrolle durch die Landesbeauftragen für den Datenschutz, die in der entstehenden Bundesdatenverwaltung ihre Prüfkompetenz praktisch nicht durchsetzen können. Die Landesverwaltungen begeben sich damit außerdem in eine bedenkliche Abhängigkeit von den Datenzuweisungen des Bundes, die ihnen eine eigenständige und selbstbestimmte Aufgabenerfüllung letztlich unmöglich machen wird.

10.1.3 Das Kraftfahrsachverständigenregister - Gütesiegel "KBA-registriert"

Das Kraftfahrsachverständigenregister soll die beim Kraftfahrt-Bundesamt (KBA) registrierten Verstöße von Kraftfahrsachverständigen gegen die straßenverkehrsrechtlichen Bestimmungen dokumentieren und stellt insoweit einen berufsgruppenbezogenen Ausschnitt aus dem Verkehrszentralregister zuzüglich weiterer berufsbezogener Eintragungen dar.

Das MSWV hat mir mitgeteilt, daß es auch dieses Register für notwendig halte. Aufgrund der teilweisen Öffnung des Kfz-Prüfwesens und der damit steigenden Anzahl von Kfz-Sachverständigen habe sich ein sog. Prüftourismus etabliert, bei dem die Aufsichtsbehörden nicht mehr in der Lage seien, Sachverständige, die andernorts gegen Prüfbestimmungen der straßenverkehrsrechtlichen Vorschriften verstoßen haben, vom Prüfgeschäft auszuschließen. Dieses Anliegen erscheint zwar grundsätzlich berechtigt; das Ministerium übersieht jedoch, daß das Register keinesfalls nur berufsbezogene Verstöße speichert, sondern ohne sachliche Rechtfertigung voraussetzt, daß gerade nur bei den Kfz-Sachverständigen auch das private Verkehrsverhalten als Maßstab ihrer Zuverlässigkeit bei der Ausübung ihres Berufes zu gelten hat. Zur Begründung dieser diskriminierenden Ungleichbehandlung gegenüber anderen Berufsgruppen findet sich im Gesetzentwurf des BMV lediglich der Hinweis auf die bisherige Verwaltungspraxis.

10.1.4 Kein Durchblick im Paragraphendschungel - Verwirrung statt Normenklarheit

Nicht nachvollziehbar ist die Komplexität des Gesetzentwurfs. Wesentliche Regelungen zur Datenverarbeitung werden geradezu versteckt; außerdem erfolgen Kettenverweisungen über

mehrere Stationen. Diese Unübersichtlichkeit und Undurchsichtigkeit verstößt gegen das verfassungsrechtliche Gebot der Normenklarheit und der Transparenz der Datenverarbeitung für die Betroffenen.

10.2 Kopien von Personalausweisen in den Akten der Kfz-Zulassungsstellen

Anläßlich einer Eingabe wurde ich auf die Praxis der Kfz-Zulassungsstellen aufmerksam, eine Kopie des vorgelegten Personalausweises zu den Akten zu nehmen. Diese - im übrigen auch sonst weitverbreitete - Praxis schien mir bereits im Hinblick auf die Bestimmungen des Bundespersonalausweisgesetzes[150] bedenklich zu sein und war jedenfalls nicht erforderlich zur Erfüllung der den Kfz-Zulassungsstellen durch Gesetz zugewiesenen Aufgaben und zu dem damit verbundenen Zweck. Das MSWV stimmte mit mir darin überein, daß die Praxis deshalb als nicht datenschutzgerecht zu beurteilen war, jedoch keine Bedenken dagegen bestehen, daß ggf. durch formularmäßiges Ankreuzen die Vorlage eines Identitätspapiers dokumentiert wird; diese Auffassung wird auch vom Bundesministerium für Verkehr vertreten. Das MSWV hat die Kfz-Zulassungsstellen darüber informiert und sie gebeten, so zu verfahren.

10.3 Geblitzt - was geschieht mit den Fotos?

10.3.1 Zugriff auf Paß- bzw. Personalregister zur Überwachung von Verkehrsverstößen durch Polizei und Ordnungsämter

Im Berichtszeitraum haben Bürger, aber auch Behörden angefragt, ob es zulässig sei, daß Polizei und Ordnungsbehörden zur Verfolgung von Verkehrsordnungswidrigkeiten in die Personalausweis- bzw. Paßregister einsehen und die aus Verkehrsüberwachungsanlagen erstellten Fotos mit den dort vorhandenen Ausweisbildern abgleichen können.

Zur Erforschung des Sachverhalts ist die Einsichtnahme grundsätzlich zu bejahen. Diese Datenübermittlung an die Verfolgungsbehörden ist im

- Brandenburgischen Personalausweisgesetz (BbgPAuswG)[151],
- Personalausweisgesetz (PAuswG)[152],
- Paßgesetz (PaßG)[153] sowie im
- Vorschaltgesetz zum Polizeigesetz des Landes Brandenburg (VGPolGBbg)[154]

geregelt. Die Verfolgungsbehörden in Ordnungswidrigkeitenverfahren haben, soweit das Ordnungswidrigkeitengesetz (OWiG)[155] nichts anderes bestimmt, dieselben Rechte und Pflichten wie die Staatsanwaltschaft bei der Verfolgung von Straftaten. Sie können daher von allen Behörden Auskünfte verlangen. Der Verfassungsgrundsatz der Verhältnismäßigkeit ist jedoch zu beachten. Um den Sachverhalt aufzuklären, darf von mehreren geeigneten Mitteln nur das gewählt werden, das den Betroffenen am geringsten belastet.

---

150 i. d. Fass. vom 21. April 1986, BGBl. I S. 548

151 vom 7. April 1994, GVBl. I S. 100

152 vom 21. April 1986, BGBl. III S. 210-1

153 vom 14. April 1996, BGBl. III 210-5

154 vom 11. Dezember 1991, GVBl. S. 636

155 i. d. Fass. vom 19. Februar 1987, BGBl. I S. 602

Nach § 9 BbgPAuswG i. V. m. § 2 b Abs. 2 Nr. 3 PAuswG dürfen die Personalausweisbehörden bzw. nach § 22 PaßG die Paßbehörde anderen Behörden Daten aus dem Personalausweis- bzw. Paßregister übermitteln. Voraussetzung für die Übermittlung ist u. a., daß die Daten beim Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden können. Hierbei ist der Grundsatz der Erforderlichkeit zu beachten.

Für das OWiG-Verfahren ergibt sich daraus, daß die Verfolgungsbehörden die Daten im ersten Schritt stets beim Betroffenen selbst erheben müssen. Erst wenn dies nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist, kann abweichend davon ausnahmsweise eine Erhebung ohne Kenntnis des Betroffenen bei anderen Stellen durchgeführt werden. Die Verfolgungsbehörde hat der Personalausweis- bzw. Paßbehörde in diesem Fall darzulegen, daß die Voraussetzungen für das Ausnahmeverfahren vorgelegen haben.

Ich habe die Auffassung vertreten, daß

- der Grundsatz der Verhältnismäßigkeit verletzt wäre, wenn die Verfolgungsbehörden bei Ordnungswidrigkeiten im Bagatellbereich auf das Personal- bzw. Paßregister zugreifen würden,
- zunächst der Betroffene die Gelegenheit zur Anhörung haben muß und
- das Ergebnis dieser Anhörung abzuwarten ist, ehe die Verfolgungsbehörde sich an die o. g. Behörden wendet.

Hiergegen haben die beteiligten Behörden keine Einwände erhoben.

10.3.2 Regelungen zum Versandt der Beweisfotos

Das Ministerium des Innern hat in einem Erlaß für die Polizeipräsidien geregelt, wie mit Fotos zu verfahren ist, die bei Verkehrsüberwachungsmaßnahmen von Verkehrssündern gemacht wurden.

Danach ist dem Betroffenen in einem Bußgeldverfahren, der Anhörungsbogen mit einem Abzug des Beweisfotos zuzusenden, wenn der Halter eine natürliche Person ist. Vor der Übersendung muß die Polizeibehörde jedoch die bei der Halterfeststellung erhobenen Angaben mit dem Foto des Fahrers vergleichen, um durch eine einfache Plausibilitätskontrolle festzustellen, ob der Betroffene überhaupt der wahrscheinliche Fahrer sein kann. Bei einem negativen Ergebnis - Fahrzeughalter ist laut Halterabfrage eine Frau, das Beweisfoto bildet einen Mann ab - wird kein Abzug beigelegt.

Soweit auf dem Foto Mitfahrer zu erkennen sind, sind diese unkenntlich zu machen. Wenn die Halterabfrage eine juristische Person als Fahrzeughalter ergibt, wird ebenfalls kein Abzug des Beweisfotos beigelegt.

Gegen diese Verfahrensweise habe ich keine Einwände erhoben.

10.4 Autobahnmaut für PKW entfällt

Bereits in meinem 2.[156] und 3.[157] Tätigkeitsbericht bin ich auf den Feldversuch zur Erhebung elektronischer Autobahngebühren auf der A 555 zwischen Köln und Bonn eingegangen. Im November vergangenen Jahres legte der damit vom Bundesministerium für Verkehr beauftragte TÜV Rheinland den Ergebnisbericht vor.

---

156 s. unter 1.4.3

157 s. unter 1.4.4

Darin wird empfohlen, in den kommenden Jahren die elektronische Gebührenerhebung auf Autobahnen zunächst schrittweise in vier definierten Phasen für schwere Lkw einzuführen und stellt gleichzeitig fest, daß vor der Einführung noch zahlreiche weitere Aspekte zu untersuchen sind. Dazu gehören u. a.:

- die Erforschung von Möglichkeiten zur Nutzung elektronischer Kfz-Kennzeichen und elektronischer Kfz-Scheine,
- die Verbesserung des Zusammenwirkens der eingesetzten Techniken zur Gebührenerhebung und zur Durchführung von Kontrollen,
- die Erstellung eines Datenschutz-/Datensicherheitskonzeptes für das gesamte Autobahngebührenerfassungssystem (AGE),
- die Ausgestaltung internationaler Rechtshilfeabkommen im Zusammenhang mit Kontroll- und Ahndungsverfahren bei Verstößen gegen die Gebührenbestimmungen.

Die vorläufige Orientierung der Gebührenerhebung auf schwere Lkw stellt keinesfalls eine endgültige Absage an eine Einführung auch für andere Fahrzeugtypen dar, vielmehr ist davon auszugehen, daß die mit Lkw gesammelten Erfahrungen helfen sollen, künftige weitere politische Entscheidungen vorzubereiten. So stellt der Ergebnisbericht u. a. folgendes fest:

> "Aus ... den Ergebnissen der theoretischen Analyse der AGE-Systeme kann abgeleitet werden, daß prinzipiell geeignete Erhebungstechnologien für eine automatische Gebührenerhebung zur Verfügung stehen. Im Hinblick auf die Weiterentwicklung der Erhebungssysteme kann davon ausgegangen werden, daß die erforderliche Einsatzreife kurzfristig erreichbar ist, wenn die Qualität der Systeme auf den üblichen Industriestandard gebracht wird und das vorhandene Verbesserungs- und Entwicklungspotential auf der Grundlage der Erfahrungen des Feldversuches genutzt wird. Damit ist eine flächendeckende Einführung von AGE-Systemen auf Autobahnen mit einsatzreifen Erhebungseinrichtungen aus technischer Sicht in wenigen Jahren möglich."

Nicht zuletzt ist es ein Verdienst der Konferenz der Datenschutzbeauftragten des Bundes und der Ländern[158], daß im Ergebnisbericht die Fragen des Datenschutzes ausreichende Berücksichtigung finden. So heißt es u. a.:

> "Zur Diskussion und Bewertung der Datenschutzproblematik wurden enge Beziehungen zum Bundesbeauftragten und den Landesbeauftragten für den Datenschutz und zu anderen Datenschutzexperten unterhalten. Dabei wurden konkrete Anforderungen an den Datenschutz für AGE-Systeme formuliert. Anläßlich eines Workshops 'Datenschutz und Autobahntechnologie' am 10. Januar 1995 in der Bundesanstalt für Straßenwesen hat der BfD die wesentlichen Aspekte des Datenschutzes im Hinblick auf die Anwendung der automatischen Gebührenerhebung auf Autobahnen in Deutschland in einem knappen Satz zusammengefaßt, daß das Fahren ohne Datenspuren im System für Fahrer, Fahrzeuge und Installationen, die bestimmte Voraussetzungen erfüllen, ohne Diskriminierung möglich und gewährleistet sein müsse.
>
> Aus der Forderung des BfD läßt sich für die Erhebung ableiten, daß es ein anonymes Zahlungsverfahren geben muß, bei dem die Abrechnungsdaten als Quittung dezentral beim Nutzer gespeichert werden und ein möglicher Rechnungsbeleg an den Dienstanbieter für den Zahlungsausgleich ausschließlich anonymisierte Zahlungsdaten enthält. Der Vorgang soll für den Nutzer transparent sein. Zahlungs- und Nutzungsdaten sind eindeutig zu trennen. Daten, die dem Diensteanbieter zur

[158] s. 3. Tätigkeitsbericht, Anlage 13

Verfügung stehen, dürfen nur anonymisierte Angaben zur Nutzung enthalten."

Abschließend wird im Ergebnisbericht zum Datenschutz gesagt:

> "Zusammenfassend kann festgestellt werden, daß die Anforderungen des Datenschutzes erfüllt werden können, wenn für die Gebührenerhebung ein anonymes Zahlungsverfahren eingesetzt wird, die Vorgänge der Erhebung und der Kontrolle über den Nutzer transparent gemacht werden und durch die Kontrolle sichergestellt werden kann, daß kein Zahlungswilliger und kein Nutzer, der nicht gebührenpflichtig ist, als Falsch- oder Nichtzahler registriert wird. Systeme, die keine Speicherung von Abbuchungsdaten für den Zahlungsnachweis im Fahrzeuggerät gestatten, erfüllen nicht die Anforderungen des Datenschutzes. Die fehlerfreie Feststellung von Falsch- oder Nichtzahlern kann durch Einführung geeigneter Verfahren mit manueller Unterstützung erreicht werden."

11 Finanzen und Wirtschaft

11.1 Allgemeine Verwaltungsvorschrift zur Durchführung der §§ 14, 15 und 55c der Gewerbeordnung

Der Runderlaß des Ministeriums für Wirtschaft, Mittelstand und Technologie (MWMT)[159] zur Ausführung der mit Wirkung vom 1. Dezember 1995 umfassend geänderten Vorschriften der Gewerbeordnung (GewO)[160] über die Behandlung von Gewerbeanzeigen und die Verarbeitung personenbezogener Daten in gewerberechtlichen Verfahren geht auf einen gemeinsamen Musterentwurf des Bundes und der Länder zurück, der auch in den übrigen Ländern zwischenzeitlich zu entsprechenden Regelungen geführt hat. In meiner Stellungnahme faßte ich die von den Datenschutzbeauftragten der Länder im wesentlichen übereinstimmend als nachbesserungsbedürftig kritisierten Punkte auf die Rechtslage im Land Brandenburg bezogenen zusammen. Das Ministerium hat in der Endfassung der Verwaltungsvorschrift meine Vorstellungen weitgehend berücksichtigt.

Insbesondere ist das Ministerium meiner Empfehlung gefolgt und hat im Zusammenhang mit seinen Vorgaben für die Behandlung der Gewerbeanzeigen bei den Gewerbeämtern fallbezogen auf die allgemeine Verpflichtung der datenverarbeitenden Stellen hingewiesen, gem. § 12 Abs. 3 Bbg DSG die Betroffenen bei der Datenerhebung über Rechtsgrundlage, Zweck sowie ggf. weitere Verarbeitung seiner Angaben aufzuklären. Es hat dazu eine Musterformulierung in die Allgemeine Verwaltungsvorschrift mit aufgenommen, die den Betroffenen auch darauf hinweist, daß gem. § 14 Abs. 8 GewO sein Name, betriebliche Anschrift und angezeigte Tätigkeit auch an nicht-öffentliche Stellen (insbesondere Adressen- und Telefonbuchverlage) übermittelt werden, wenn nicht der Gewerbetreibende ein entgegenstehendes, schutzwürdiges Interesse ausdrücklich glaubhaft macht. Dies hatte ich auch im Hinblick darauf empfohlen, daß die Datenübermittlungen von den Gewerbeämtern an Adreßbuchverlage in der Vergangenheit zu zahlreichen - teils recht empörten - Anfragen und Eingaben betroffener Gewerbetreibender bei mir geführt hatten.

Ferner führte meine datenschutzrechtliche Kritik vor allem zu einer Überarbeitung der Regelungen zur Überprüfung der Zuverlässigkeit des Gewerbeanzeigenden. Diese tragen nun entsprechend den Bestimmungen des Bundeszentralregistergesetzes (BZRG)[161] dem

---

159 vom 25. Januar 1996, ABl. S. 186

160 Gesetz zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften vom 23. November 1994, BGBl. I S. 3475

161 i. d. Fass. vom 21. September 1984, BGBl. I S. 1229, ber. 1985 I S. 195

Grundsatz der unmittelbaren Datenerhebung beim Betroffenen (vgl. § 12 Abs. 2 Bbg DSG) Rechnung, indem sie vorsehen, daß, soweit erforderlich, zunächst der Betroffene selbst zur Beantragung eines Führungszeugnisses gem. § 30 Abs. 1 und 2 BZRG aufgefordert wird und nur in den Fällen, in denen der Betroffene dazu nicht bereit oder dies aus anderen Gründen nicht sachgerecht ist, statt dessen die Behörde gem. § 31 BZRG die Erteilung eines Führungszeugnisses beim Bundeszentralregister beantragt. Die dargestellte Ausgestaltung der Verfahrensweise bei der gewerberechtlichen Zuverlässigkeitsprüfung in der Allgemeinen Verwaltungsvorschrift ändert allerdings nichts daran, daß es für die entsprechende Datenverarbeitung durch Einholung einer Bundeszentralregisterauskunft bislang an einer hinreichenden bereichsspezifischen Rechtsgrundlage in der Gewerbeordnung fehlt. Nach seinen diesbezüglichen Mitteilungen gehe ich jedoch davon aus, daß sich das Ministerium im Rahmen seiner Möglichkeiten für die dazu erforderliche Änderung des § 38 GewO einsetzen wird. Dies soll auch vom Bundeswirtschaftsministerium bereits beabsichtigt sein.

Der Runderlaß enthält leider keine Regelungen zu Fristen, nach deren Ablauf die Gewerbeämter Auskünfte aus dem Bundeszentralregister sowie dem Gewerbezentralregister regelmäßig vernichten müssen (vgl. § 23 Nr. 2 Buchst. f Ordnungsbehördengesetz (OBG) n. F.[162] i. V. m. § 47 Abs. 2 Satz 1 Nr. 3 und Satz 3 Brandenburgisches Polizeigesetz (BbgPolG)[163]). Eine derartige Festlegung von Prüf- und Löschungsfristen ist jedoch erforderlich, damit die Gewerbeämter nicht ohne hinreichenden Grund auf Dauer Daten speichern, die in der Zwischenzeit in den Zentralregistern selbst ggf. längst gelöscht worden sind.

Das Ministerium hat mir dazu zwar mitgeteilt, daß zur Aufgabenerfüllung der Gewerbeämter in der Regel nur aktuelle Registerauskünfte erforderlich seien und Registerauszüge bzw. Führungszeugnisse nach Ablauf von sechs Monaten nicht mehr als aktuell anzusehen sein dürften. Eine Fristenregelung in der Allgemeinen Verwaltungsvorschrift hat es jedoch als verfrüht abgelehnt, da es sich um eine generelle Problematik handele, die zunächst sowohl innerhalb der Landesregierung als auch mit dem Bund und den übrigen Ländern näher erörtert werden müsse. Daran ist richtig, daß auch aus datenschutzrechtlicher Sicht eine ressortübergreifende Lösung des in der Tat auch in anderen Verwaltungsbereichen bestehenden Problems zu wünschen wäre.

Die Landesregierung ist jedoch aufgefordert, eine solche Lösung zügig zu konkretisieren, denn mit dem Aktenbestand steigt auch ständig der Verwaltungsaufwand, der mit einer Bereinigung auch nach Maßgabe der o. g. Bestimmungen des Ordnungsbehördengesetzes n. F. verbunden bleiben wird.

11.2 Erhebung der Steuernummer durch Industrie- und Handelskammer zur Festsetzung der Beiträge

Im 3. Tätigkeitsbericht[164] berichtete ich über die Praxis der Industrie- und Handelskammern (IHK), zur Festsetzung der Kammerbeiträge von ihren Mitgliedern deren Steuernummer zu erfragen, ohne auf die Freiwilligkeit einer solchen - durchaus sinnvollen - Angabe hinzuweisen. Das MWMT nahm dies zum Anlaß, sogleich von sich aus an die Kammern heranzutreten und sie zu einer entsprechenden Anpassung der Erhebungsbögen an die von mir dargestellte Rechtslage aufzufordern. Noch im vergangenen Jahr teilte mir das Ministerium mit, daß nunmehr in den von den Kammern verwendeten Schreiben und

---

[162] vom 13. Dezember 1991, GVBl. I S. 636, zul. geänd. d. Art. 2 d. Gesetz zur Neuordnung des Polizeirechts im Land Brandenburg vom 29. Februar 1996, GVBl. I S. 274

[163] vom 29. Februar 1996, GVBl. I S. 274

[164] s. unter 10.1

Erhebungsbögen auf die Freiwilligkeit der erbetenen Angabe zur Steuernummer hingewiesen werde.

11.3 Überprüfung von Bewachungsunternehmen

Bei der Überprüfung von Bewachungsunternehmen[165] nach § 34 a Gewerbeordnung kommt es zu der Schwierigkeit, daß dem Bewachungsunternehmer u. U. die Ausübung des Gewerbes mangels Zuverlässigkeit des von ihm beschäftigten Personals untersagt werden muß oder ihm diesbezügliche Auflagen zu erteilen sind. Zur Begründung seiner entsprechenden Ordnungsverfügungen muß das Gewerbeamt dem Unternehmer dann ggf. auch die beurteilungsrelevanten Angaben über die von ihm beschäftigten Wachpersonen mitteilen. Dazu zählen insbesondere auch die Informationen, die das Gewerbeamt aus den Auskünften erhält, die es über die Betroffenen beim Bundeszentralregister einholt.

Bei einer datenschutzrechtlichen Überprüfung dieser Verfahrensweise war festzustellen, daß es an einer bereichspezifischen normenklaren Rechtsgrundlage für die damit verbundene Datenverarbeitung fehlt. Eine solche ist jedoch gem. § 4 Abs. 1 Buchst. b i. V. m. § 41 Abs. 2 Bbg DSG grundsätzlich erforderlich. Ich habe deshalb das MWMT darum gebeten, sich für eine solche, dem Grundrechtsschutz besser entsprechende, klare gesetzliche Regelung der Datenverarbeitung in den Überprüfungsverfahren nach § 34 a Gewerbeordnung einzusetzen. Das Ministerium hat mir mitgeteilt, daß sich die Problematik im Bund-Länder-Ausschuß "Gewerberecht" zur Zeit noch in der Diskussion befinde.

Das Ministerium hat jedoch meiner Empfehlung entsprochen und die Gewerbeämter in einem Rundschreiben darum gebeten, zu beachten, daß die betroffenen Wachpersonen vorab über die beschriebene verfahrensbedingte Datenverarbeitung unterrichtet werden müssen, daß sie gem. § 28 Verwaltungsverfahrensgesetz (VwVfG)[166] vor Bekanntgabe der sie betreffenden Informationen an den Bewachungsunternehmer anzuhören sind und daß die Weitergabe der Informationen unterbleiben muß, wenn der Betroffene daraufhin sein Arbeitsverhältnis zu dem Bewachungsunternehmen selbst beendet.

11.4 Datenübermittlung der Industrie- und Handelskammer an die Wettbewerbszentrale (e. V.) in Frankfurt am Main zur Verfolgung unlauteren Wettbewerbs

Bei bestimmten Verstößen gegen das Gesetz gegen den unlauteren Wettbewerb (UWG)[167] können die wettbewerbsrechtlichen Unterlassungsansprüche gem. § 13 Abs. 2 Nr. 4 UWG auch von den Industrie- und Handelskammern (IHK) geltend gemacht werden. Das gleiche gilt gem. § 13 Abs. 2 Nr. 3 UWG für rechtsfähige Verbände, zu deren satzungsgemäßen Aufgaben es gehört, die Interessen der Verbraucher durch Aufklärung und Beratung wahrzunehmen.

In einem anderen Bundesland hatte eine dortige IHK der Wettbewerbszentrale zur Geltendmachung eines wettbewerbsrechtlichen Unterlassungsanspruchs im eigenen Namen personenbezogene Informationen übermittelt. Die zuständige Datenschutzbeauftragte kam bei ihrer datenschutzrechtlichen Überprüfung dieser Datenübermittlung zu der Auffassung, daß dies wohl als unzulässig zu bewerten sei, da es in dem betreffenden Bundesland an einer

---

165 vgl. auch die Antwort der Landesregierung auf die Kleine Anfrage 388, LT-Drs. 2/1490

166 vom 25. Mai 1976, BGBl. I S. 1253, zul. geänd. d. Art. 12 Abs. 5 PostneuordnungsG v. 14. September 1994, BGBl. I S. 2325

167 vom 7. Juni 1909, RGBl. S. 499, zul. geänd. d. Ges. vom 25. Oktober 1994, BGBl. I. S. 3082

dazu hinreichenden Rechtsgrundlage fehle, wandte sich jedoch wegen der bundesweiten Bedeutung der Angelegenheit zunächst an die übrigen Datenschutzbeauftragten mit der Bitte um Stellungnahme.

In Übereinstimmung mit dem MWMT habe ich die Auffassung vertreten, daß es sich um eine Datenübermittlung an eine nicht-öffentliche Stelle handelt, die im Geltungsbereich des Brandenburgischen Datenschutzgesetzes gem. § 16 Abs. 1 i. V. m. § 13 Abs. 1 Bbg DSG als unzulässig zu beurteilen ist, da es bereits an der dort vorausgesetzten Erforderlichkeit der Datenübermittlung zur Erfüllung der Aufgaben der IHK. Denn die IHK hat diese Aufgaben gem. § 13 Abs. 2 Nr. 4 UWG ggf. selbst wahrzunehmen und kann sie nicht auf Dritte übertragen. Das Ministerium hat mir mitgeteilt, daß vergleichbare Vorgehensweisen der hiesigen IHK bisher nicht bekannt geworden seien, es seine Auffassung jenen jedoch mit der Bitte um Stellungnahme zugeleitet habe.

12 Kommunale Probleme

12.1 Gesundheitsämter

12.1.1 Anfragen von Gesundheitsämtern

Im Berichtszeitraum hatte ich mich mit zahlreichen Anfragen von Gesundheitsämtern zu befassen. Sie betrafen im wesentlichen den Umgang mit Leichenschauscheinen (s. unter 7.2.3.1) und Impfdateien (s. unter 7.2.3.2). Sie boten die Grundlage, dem MASGF gegenüber klarzustellen, daß diese genannten Probleme einer datenschutzmäßig tragbaren Lösung bedürfen.

Des weiteren wurde ich vom Ministerium für Arbeit, Soziales, Gesundheit und Frauen bzw. vom Landesgesundheitsamt in die Erarbeitung eines Elternfragebogens zur Schulreihenuntersuchung (s. unter 7.2.3.3) einbezogen, der künftig von den Gesundheitsämtern verwendet werden soll.

12.1.2 Kontrollbesuch im Gesundheitsamt

Bei einem Kontrollbesuch im März 1995 in einem Gesundheitsamt mußte ich feststellen, daß die in den Archivräumen gelagerten Patientendaten sicherheits- und brandschutztechnisch unzureichend untergebracht waren. Auch der Umstand, daß der Heizungskeller nur durch einen der Archivräume betreten werden konnte und so bei den regelmäßig unbeaufsichtigten Wartungsarbeiten also ein ungehinderter Zugriff Unbefugter auf die höchst sensiblen Patientendaten nicht ausgeschlossen war, stellte einen datenschutzrechtlichen Verstoß dar, den ich beanstandet habe.

Seitens des Landkreises wurde mitgeteilt, daß die beanstandeten Punkte beseitigt würden. Bau- und Rekonstruktionspläne dazu lägen vor und könnten unmittelbar nach der Bestätigung des Haushalts 1996 in die Tat umgesetzt werden.

12.2 Meldewesen

12.2.1 Veröffentlichungen von Jubiläen in Amts- und Gemeindeblättern

Eine Regionalzeitung hat mich kürzlich darüber informiert, daß im Gemeindeblatt einer amtsangehörigen Gemeinde die Ehe- bzw. Altersjubiläen mit dem Zusatz veröffentlicht würden, daß diejenigen Personen, die dies nicht wünschten, bei der Meldebehörde Widerspruch einlegen könnten.

In einer fast gleichartigen Angelegenheit beschwerte sich ein Bürger darüber, daß im Amtsblatt einer kreisfreien Stadt unter der Rubrik "Der Oberbürgermeister gratuliert zum:" Name und Geburtstag von Personen, die ihren 90. und jeden weiteren Geburtstag begehen, veröffentlicht würden, ohne daß die Betroffenen dazu vorher befragt worden wären.

Ein solches Verfahren steht in beiden Fällen nicht mit datenschutzrechtlichen Bestimmungen im Einklang, da es für die Veröffentlichungen keine Rechtsgrundlage gibt. Gem. § 33 Abs. 2 Brandenburgisches Meldegesetz (BbgMeldeG)[168] erteilt die Meldestelle Auskunft über Alters- oder Ehejubiläen von Einwohnern, die der Auskunftserteilung nicht widersprochen haben. Die Vorschrift regelt weiterhin, daß der Betroffene bei der Anmeldung auf sein Widerspruchsrecht hinzuweisen ist. Damit das Verfahren für die in Rede stehenden Personen, die in der Regel ihrer Anmeldepflicht bereits genügt haben, nicht ins Leere läuft, muß die Meldebehörde durch eine Veröffentlichung in allgemeiner Form (z. B. durch ortsüblichen Aushang) das Widerspruchsrecht gem. § 33 Abs. 2 BbgMeldeG bekanntgeben.

Die Veröffentlichung von Alters- bzw. Ehejubiläen in Zeitungen, Amtsblättern, Rundfunksendungen oder durch öffentliche Bekanntgabe per Aushang wird von § 33 Abs. 2 BbgMeldeG nicht gedeckt. Dafür gibt es auch keine anderweitige Rechtsgrundlage. § 16 Bbg DSG, mit dem unter bestimmten Voraussetzungen die Datenübermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs zugelassen wird, kommt hier nicht in Betracht, weil die Voraussetzungen nicht erfüllt sind. Die Veröffentlichung der in Rede stehenden Daten im Amtsblatt dient weder der rechtmäßigen Erfüllung der Aufgaben der Meldebehörde, noch liegt ein rechtliches Interesse des Amtsblattes an den in Rede stehenden Daten vor. Soweit Bürgermeister bzw. Oberbürgermeister ein berechtigtes Interesse an Alters- bzw. Ehejubiläen haben, wird diesem Interesse bereits durch die Übermittlung der Meldebehörde an sie Rechnung getragen. Eine Veröffentlichung im Amtsblatt ist deswegen nicht erforderlich.

Soweit ohne Rechtsgrundlage mit personenbezogenen Daten umgegangen werden soll, bedarf dies gem. § 4 Abs. 1 Buchst. c Bbg DSG der Einwilligung der Betroffenen, die gem. § 4 Abs. 2 Bbg DSG schriftlich erfolgen muß. Daraus ergibt sich, daß für die Übermittlung der zuvor von der Meldestelle rechtmäßig übermittelten Daten an die Redaktion des Amts- bzw. Gemeindeblattes die schriftliche Einwilligung der Betroffenen eingeholt werden muß.

Eine allen Interessen entgegenkommende, unnötigen Verwaltungsaufwand vermeidende, datenschutzrechtlich einwandfreie Lösung könnte darin bestehen, das bei den Meldestellen vorliegende Widerspruchs- bzw. Einwilligungsformular um den Passus der Einwilligung in die Veröffentlichung im Amts- bzw. Gemeindeblatt zu erweitern. Vielleicht ergeben sich auch weitere Problemlösungen aus den Rückäußerungen der zuständigen Stellen.

12.2.2 Hotel-Meldeschein vertreibt Touristen

Empört abgereist ist ein Gast aus einem bekannten Ausflugsort in der Märkischen Schweiz, nachdem er an der Rezeption einen Meldeschein ausfüllen sollte, der zugleich auch der Berechnung der Kurabgabe und deren Registrierung durch die Kurverwaltung des zuständigen Amtes dienen sollte. Dabei verwies der Gast darauf, daß die Kurverwaltung nicht das Recht habe, seine personenbezogenen Angaben aus dem Meldeschein zu erhalten. Die Hotelrezeption lehnte es ab, auf das Ausfüllen des Meldescheines gänzlich zu verzichten.

Nach § 24 BbgMeldeG haben Personen, die in Beherbergungsstätten für nicht länger als zwei Monate aufgenommen werden, einen besonderen Meldeschein handschriftlich auszufüllen und zu unterschreiben, wobei Ehegatten auf einem gemeinsamen Meldeschein

---

168 vom 25. Juni 1992, GVBl. I S. 236

und Kinder in ihrer Begleitung nur der Zahl nach gemeldet werden können. Dieser Meldeschein muß gem. § 25 Abs. 2 BbgMeldeG außer dem Namen und der Anschrift der Beherbergungsstätte noch den Familiennamen, Vornamen, Tag der Geburt, Staatsangehörigkeit, Anschrift sowie den Tag der Ankunft und der voraussichtlichen Abreise der insoweit meldepflichtigen Personen enthalten. Darauf mußte die Hotelrezeption zunächst bestehen, da der Leiter der Beherbergungsstätte oder dessen Beauftragter gem. § 25 Abs. 1 BbgMeldeG die besonderen Meldescheine bereitzuhalten und darauf hinzuwirken hat, daß die aufgenommenen Personen ihre diesbezüglichen Verpflichtungen erfüllen.

Dagegen verlangte der Gast zu Recht, daß im Zusammenhang mit dieser Datenerhebung keine personenbezogenen Meldedaten zur Kurverwaltung gelangen, weil nach § 25 Abs. 3 BbgMeldeG bei einer Aufbewahrungszeit von einem Jahr die ausgefüllten Meldescheine ausschließlich der zuständigen Meldebehörde und Dienststellen der Polizei auf Verlangen zur Einsichtnahme vorzulegen oder zu übermitteln sind, wenn dies nach Feststellung dieser Stellen erforderlich ist. Diese spezialgesetzliche Bestimmung schließt jede anderweitige Nutzung der Meldedaten aus.

In vorliegendem Fall sah der Meldeschein in einer zusätzlichen, nicht abtrennbaren rechten Spalte unter einer Registriernummer weitere Angaben wie Aufenthaltstage, Anzahl Erwachsene/Kinder, Tatsache evtl. Schwerbehinderung/Begleitperson, Kurabgabe insgesamt in DM incl. MWSt. und Unterschrift des Beauftragten der Beherbergungsstätte vor, zu denen ausschließlich der Leiter der Beherbergungsstätte gegenüber der Kurverwaltung im Zusammenhang mit einer korrekten Abführung der Kurabgaben verpflichtet ist.

Für die Berechnung der Kurabgabe reichen aber die Angaben ohne Personenbezug aus; auf jeden Fall darf sich die Kurverwaltung nicht "im gleichen Zuge" der Meldedaten bedienen, da diese nach § 25 Abs. 4 BbgMeldeG nur für Zwecke der Gefahrenabwehr, der Strafverfolgung oder der Aufklärung des Schicksals von Vermißten und Unfallopfern ausgewertet und verarbeitet werden dürfen.

Daher ist die Verwendung von Meldescheinen für Beherbergungsstätten in der Kombination mit Angaben zur Kurabgabe-Berechnung datenschutzrechtlich nur dann nicht zu beanstanden, wenn der die Angaben für die Kurverwaltung betreffende Teil ohne Personenbezug überhaupt abtrennbar ist oder - entgegen dem geschilderten Fall - garantiert ist, daß auf dem als "Beleg für die Kurverwaltung" vorgesehenen Durchschlag des Meldescheins nicht auch die personenbezogenen Angaben des Gastes mit durchgeschrieben werden.

Im übrigen verweise ich auf Anlage 4 zu § 2 Abs. 1 Nr. 4 der Verordnung zur Durchführung des Gesetzes über das Meldewesen im Land Brandenburg (DVOBbgMeldeG)[169], mit der das Ministerium des Innern ein ordnungsgemäßes Vordruckmuster für die Anmeldungen nach § 24 Abs. 2 BbgMeldeG vorgibt.

12.3 Bauen

12.3.1 Umfragen privater Planungsbüros zur Beurteilung der Sanierungsbedürftigkeit

Zur Vorbereitung städtebaulicher Sanierungsmaßnahmen beauftragen die Gemeinden vielfach private Planungsbüros mit der Erstellung von Sanierungskonzepten. Dazu müssen bei den Verfügungs- und Nutzungsberechtigten, insbesondere den Eigentümern und Mietern von Wohnraum, in nicht unerheblichem Umfang personenbezogene Daten erhoben werden.

---

[169] vom 5. August 1992, GVBl. II S. 482

Das Baugesetzbuch (BauGB)[170] sieht dabei eine Auskunftspflicht der Betroffenen zu den Tatsachen vor, deren Kenntnis zur Beurteilung der Sanierungsbedürftigkeit eines Gebiets oder zur Vorbereitung oder Durchführung der Sanierung erforderlich ist. Insbesondere können gem. § 138 BauGB Angaben der Betroffenen über ihre persönlichen Lebensumstände im wirtschaftlichen und sozialen Bereich, namentlich über die Berufs-, Erwerbs- und Familienverhältnisse, das Lebensalter, die Wohnbedürfnisse, die sozialen Verflechtungen sowie über die örtlichen Bindungen erhoben werden.

Die Phase der Datenerhebung unterliegt bei den entsprechenden Umfragen stets und insbesondere auch dann der Kontrolle durch den Landesbeauftragten für den Datenschutz, wenn die Gemeinde ein privates Planungsbüro mit der Umfrage beauftragt hat. Dazu stellt § 2 Absatz 1 Satz 3 Bbg DSG (s. unter 2.1) inzwischen klar, daß nicht-öffentliche Stellen, die hoheitliche Aufgaben wahrnehmen, insoweit öffentliche Stellen sind. Bei der Durchführung von Datenerhebungen mit öffentlich-rechtlicher Auskunftspflicht handelt es sich um eine hoheitliche Aufgabe.

Ob dem Landesbeauftragten für den Datenschutz gegenüber den privaten Planungsbüros auch im übrigen eigene Kontrollbefugnisse zustehen, kann dagegen im Einzelfall zweifelhaft sein. Im Anwendungsbereich des Brandenburgischen Datenschutzgesetzes wird eine nicht-öffentliche Stelle nicht in jedem Fall bereits dadurch zu einer öffentlichen Stelle im Sinne des Gesetzes, daß sie Aufgaben der öffentlichen Verwaltung wahrnimmt[171], sondern gem. § 2 Abs. 1 Satz 3 Bbg DSG nur dann, wenn es sich dabei zugleich um eine hoheitliche Aufgabe handelt (s. unter 2.1). Bei einer bloßen Auswertung einer von der Gemeinde selbst durchgeführten Sanierungsumfrage kann es fraglich sein, ob eine solche Tätigkeit hoheitlich ist. Die auftraggebenden Gemeinden sind jedoch in jedem Fall verpflichtet, nur Unternehmen zu beauftragen, die die Gewähr für eine dem Standard des Brandenburgischen Datenschutzgesetzes entsprechende Datensicherheit bei der Verarbeitung personenbezogener Daten bieten, und müssen dies in geeigneter Weise auch vertraglich absichern.

Um die Wahrnehmung hoheitlicher Aufgaben handelt es sich jedoch, wenn das Planungsbüro nicht nur mit lediglich vorbereitenden Tätigkeiten betraut wird, sondern von der Gemeinde als eigenständiger Sanierungsträger gem. §§ 157 ff BauGB beauftragt ist. In diesen Fällen sehe ich die Planungsbüros deshalb als öffentliche Stellen im Sinne von § 2 Abs. 1 Satz 3 Bbg DSG an, deren Datenverarbeitung gem. § 23 Abs. 1 Bbg DSG unmittelbar meiner Kontrolle unterliegt. Dies sollte von den Gemeinden bei der Auftragserteilung in dem Vertrag klargestellt werden. Es wäre zu begrüßen, wenn dabei im Interesse der Rechtssicherheit für alle Beteiligten auch die oben dargestellten Zweifel zugunsten einer in allen Fällen einheitlichen Kontrollbefugnis des Landesbeauftragen für den Datenschutz ausgeräumt würden.

Soweit ich im Berichtszeitraum an der Vorbereitung von Umfragen zur Erstellung von Sanierungskonzepten beteiligt wurde, sind mir grundsätzliche datenschutzrechtliche Mängel nicht bekannt geworden. Ich konnte mich im wesentlichen auf Hinweise zur datenschutzgerechten Gestaltung der Erhebungsbögen beschränken (s. unter 2.3).

12.3.2 Datenverarbeitung in Verfahren nach § 3 Abs. 2 Baugesetzbuch

Ausgerechnet auf einer Müllkippe hatte ein Bürger Anlagen zum Bebauungsplan einer Gemeinde gefunden, die die Abwägungsempfehlungen zu den dort eingegangenen Bedenken und Anregungen der Betroffenen im Rahmen der öffentlichen Auslegung des Planentwurfs

---

170 i. d. Fass. vom 8. Dezember 1986, BGBl. I S. 2253, zul. geänd. d. Ges. vom 23. November 1994, BGBl. I S. 3486

171 Insoweit anders die Rechtslage im Land Berlin gem. § 2 Abs. 1 Satz 2 BlnDSG; vgl. Jahresbericht des Berliner Datenschutzbeauftragten 1995, S. 95

gem. § 3 Abs. 2 BauGB enthielten. Er brachte seinen Aktenfund umgehend zu meiner Dienststelle.

Die eigentlichen Abwägungsempfehlungen waren von der Gemeinde bereits sachgerecht so abgefaßt worden, daß sie keine personenbezogenen Daten enthielten. Die einzelnen Einwendungen waren den Einwendern vielmehr mit fortlaufenden Ziffern zugeordnet und ausschließlich unter diesen Ziffern abgehandelt worden. Leider hatte es die Gemeinde versäumt, die Liste, in der die Zuordnung der Schlüsselziffern zu den namentlich und unter Angabe des Datums ihres jeweiligen Einwendungsschreibens aufgeführten Einwendern erfolgte, von der Anlage zu trennen.

Dies war jedoch geboten, da nicht ersichtlich ist, daß es außerhalb des Bauamtes oder außerhalb eines konkreten Widerspruchs- oder Verwaltungsgerichtsverfahrens erforderlich sein könnte, daß sich die nach den Bestimmungen des Baurechts und der Gemeindeordnung zu beteiligenden Stellen und Personen (z. B. der Gemeinderat, der Landkreis sowie "die Bürger" oder "die Öffentlichkeit") mit den Einwendungen der Bürger im Verfahren nach § 3 Abs. 2 BauGB personenbezogen auseinandersetzen. Deshalb war es gem. § 14 Abs. 1 Bbg DSG auch nicht zulässig, diesen Stellen und Personen die Abwägungsempfehlungen personenbeziehbar weiterzugeben bzw. zu übermitteln.

Die betreffende Gemeinde hat mir auf meine Darlegungen zur Rechtslage mitgeteilt, daß es in Zukunft dementsprechend verfahren werde und die erforderlichen Vorkehrungen getroffen habe, um eine personenbeziehbare Weiterleitung von Abwägungsempfehlungen in Verfahren nach § 3 Abs. 2 BauGB künftig auszuschließen.

Das Ministerium für Stadtentwicklung, Wohnen und Verkehr (MSWV) hat mir auf Anfrage mitgeteilt, daß es meine Auffassung dazu teile und mir aufgrund meiner Bitte zugesagt, die Bauverwaltungen in einem Rundschreiben über die Rechtslage zu informieren.

Als eine parallele Problematik sehe ich die Frage an, ob es zulässig ist, in Planfeststellungsverfahren die Grunderwerbsverzeichnisse, die u. a. neben der Lage, der Größe und der Nutzungsart der planbetroffenen Grundstücke auch die Eigentümer mit Namen, Vornamen sowie Anschrift aufführen, als Bestandteil der Planungsunterlagen zur Einsichtnahme durch jedermann auszulegen. Ich gehe davon aus, daß diese Frage im Ergebnis zu verneinen sein wird; die dazu im vergangenen Jahr vom MSWV erbetene Stellungnahme steht jedoch noch aus.

12.3.3 Veröffentlichung der Abgabenpflichtigen bei der Festsetzung von Erschließungsbeiträgen - Falsch verstandene Bürgernähe

Mit einem Rundschreiben hatte eine Gemeinde den Grundstückseigentümern mitgeteilt, daß sie bei jenen gem. §§ 8 - 10 Kommunalabgabengesetz (KAG)[172] anteilig Beiträge zu den Erschließungs- und Ausbaukosten erheben werde. In dem Bemühen um "Bürgernähe" und größtmögliche Transparenz des Verwaltungsverfahrens für die Betroffenen hatte die Gemeinde in dem Schreiben zugleich auch jeweils alle anderen Abgabepflichtigen mit Namen und Anschrift aufgelistet. Dadurch sah sich einer der Betroffenen in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt und wandte sich an mich.

Der Gemeinde, die mit ihrer Vorgehensweise gem. § 12 KAG i. V. m. § 30 Abs. 4 Abgabenordnung (AO)[173] in der Tat das Steuergeheimnis verletzte, teilte ich mit, daß es für die Übermittlung der Angaben zu anderen Beitragspflichtigen an der dazu erforderlichen Rechtsgrundlage fehlt, die Datenübermittlung insbesondere auch nicht (subsidiär) auf § 16

---

172 vom 27. Juni 1991, GVBl. S. 200

173 vom 16. März 1976, BGBl. I S. 613, zul. geänd. d. Ges. vom 18. Dezember 1995, BGBl. I S. 1959

Abs. 1 Bbg DSG gestützt werden kann und mir schon grundsätzlich nicht nachvollziehbar ist, in welcher Weise eine Information der Betroffenen über ebenfalls abgabepflichtige andere Grundstückseigentümer für die Erfüllung der gesetzlichen Aufgabe der Beitragserhebung erforderlich sein kann.

In ihrer Antwort bedauerte die Gemeinde zwar, daß "die bestehende Gesetzeslage eine umfassende Information" nicht zulasse, akzeptierte jedoch meine Empfehlung, von einer derartigen Offenbarung personenbezogener Daten künftig Abstand zu nehmen, und teilte mir mit, daß sie bei weiteren Beitragserhebungen, "die etwas großzügig gehandhabte Benachrichtigung streichen" werde.

12.4 Sonstiges

12.4.1 Stundungsantrag für Abwasseranschlußgebühren

Immer wieder erreichen mich Anfragen von Bürgern, die dem Ausfüllen von Stundungsanträgen, welche ein großes Maß an Offenlegung der persönlichen und wirtschaftlichen Verhältnisse erfordern, sehr verhalten gegenüberstehen. Es erscheint den Betroffenen meist unverständlich, weshalb sie in einem Antrag auf Stundung von Abwasseranschlußgebühren gegenüber der Gemeinde die Einkommensverhältnisse ihrer Familie, ihre Vermögensverhältnisse, Schulden und sonstige Verpflichtungen offenlegen sollen.

Ich habe den Betroffenen auf ihre Anfragen mitgeteilt, daß der massive Eingriff in ihr Recht auf informationelle Selbstbestimmung erlaubt ist, weil aufgrund einer rechtmäßigen Satzung die Gemeinden den Anspruch haben, Abwasseranschlußgebühren zu erheben. Dies entspricht § 2 KAG, wonach Gemeinden ermächtigt sind, aufgrund einer Satzung kommunale Abgaben zu erheben. Kann ein betroffener Bürger seiner Abgabenpflicht nicht oder nicht rechtzeitig in voller Höhe nachkommen, so haben die Kommunen gem. § 222 AO die Möglichkeit, ihre Forderungen zu stunden oder zu erlassen. Der Gesetzgeber macht dies jedoch von ganz strengen Voraussetzungen abhängig. Einerseits muß die Einziehung der Forderung bei Fälligkeit für den Betroffenen eine erhebliche Härte bedeuten und andererseits darf der Anspruch der Kommune durch die Stundung nicht gefährdet erscheinen. Infolge dieser strengen Regelung ist es erforderlich, den Antrag auf Stundung oder Erlaß hinreichend zu begründen. Die Kommunen sind verpflichtet, zu prüfen, ob aufgrund persönlicher und wirtschaftlicher Verhältnisse ein Härtefall vorliegt, aufgrund dessen es möglich ist, dem Betroffenen entsprechende Ratenzahlung zu gewähren. Der Nachweis der Stundungsgründe ist aus Sicht des möglichen Mißbrauchs der Vorschrift des § 222 AO meines Erachtens unerläßlich, so daß der Betroffene den Eingriff in sein informationelles Selbstbestimmungsrecht hinnehmen muß.

An dieser Stelle weise ich die Kommunen nochmals ausdrücklich auf die Vordruckgestaltung, die datenschutzrechtlichen Erfordernissen zu entsprechen hat, hin (s. unter 2.3).

12.4.2 "Intelligente Mülltonnen" - Spiegelbild von Verbrauchergewohnheiten?

Wegen des Verdachts, daß mittels eines im Oktober 1995 in der Presse groß angekündigten neuen Müllidentifikationssystems durch einen Abfallzweckverband (AZV) Verhaltensprofile der Bürger erstellt werden könnten, habe ich mich über den Einsatz von sog. "intelligenten Mülltonnen" vor Ort informiert.

Mit dem neu eingeführten Müllidentifikationssystem wurde jeder Müllbehälter mit einem Chip ausgerüstet. Um den Müllbehälter bei jeder Entleerung zu identifizieren, enthält der

Chip eine Identifikations- sowie eine Behälternummer. Diese Codenummer wird einmalig vergeben und ermöglicht eine direkte Zuordnung zum Grundstück. Auf dem Chip werden weder der Name noch die Adresse des Grundstückseigentümers oder sonstigen Nutzungsberechtigten gespeichert. Die Bürger erhalten für die mit dem Chip ausgestattete Tonne einen Aufkleber mit dem Aufdruck "Chipsy an Bord". Sie können selbst entscheiden, ob sie auf diesem Aufkleber ihre Adresse bzw. den Standort der Tonne vermerken.

Beim Entleerungsvorgang nimmt das Müllfahrzeug die Tonne auf, eine Antenne am Greifarm des Fahrzeuges liest den Code vom Chip ein und speichert ihn in einem Computer an Bord. Neben der Registrierung der Codenummer werden des weiteren der Tag sowie die Uhrzeit der Entleerung sowohl auf dem Chip (sog. Schreib- und Lesechip) als auch im Bordcomputer gespeichert. Speichermedium des Bordcomputers ist eine sog. RAM-Card. Einmal wöchentlich werden die beschriebenen RAM-Cards dem AZV zum originalen Auslesen übergeben, d. h., die auf der RAM-Card vorgehaltenen Daten werden in unveränderter Form auf einer einmal beschreibbaren Worm-Platte gespeichert und können damit nicht mehr verändert werden. Es ist vorgesehen, daß die Daten für etwa zwei Jahre beim AZV verbleiben. Eine genaue Regelung zum Sperren oder Löschen dieser Daten gibt es derzeit nicht. Auf die Notwendigkeit einer solchen Festlegung habe ich nachdrücklich hingewiesen.

Anhand der auf der Worm-Platte gespeicherten Daten wird verursacherbezogen der Gebührenbescheid erstellt (ein- bis zweimal jährlich), d. h., neben einem durch die Gebührensatzung festgelegten Grundbetrag wird je nach Häufigkeit der Leerung ein Entleerungsbetrag erhoben. Obwohl der Chip die Möglichkeit der Speicherung des Abfallgewichts bietet, wird von dieser Registrierungsmöglichkeit in absehbarer Zeit jedoch kein Gebrauch gemacht.

Bei der Anwendung des neuen Müllidentifikationssystems habe ich keine datenschutzrechtlichen Mängel feststellen können. Mittels der "intelligenten Tonnen" kann jedenfalls nicht nachvollzogen werden, welcher Bürger welchen und wieviel Müll produziert; es ist sichergestellt, daß keine Verhaltensprofile der Bürger bezüglich ihrer Abfallgewohnheiten erstellt werden.

Bei der Kontrolle des ADV-Systems habe ich jedoch verschiedene Unzulänglichkeiten feststellen müssen und daher den AZV aufgefordert, diese anhand eines Forderungskataloges abzustellen. Der AZV hat mir versichert, daß er bereits begonnen habe, die von mir geforderten technisch-organisatorischen Maßnahmen gem. § 10 Bbg DSG zu treffen.

12.4.3 Gebühreneinstufung einer Kreismusikschule

Ein Bürger war über die Änderung des Verfahrens der Gebühreneinstufung bei einer Kreismusikschule befremdet und wandte sich daher an mich. Hierzu war eine antragsweise Selbsteinstufung in Gehaltsgruppen mit vorgegebenen Von-bis-Spannen vorgesehen. Auf dem Formular war zusätzlich vermerkt, daß die Musikschule sich das Recht vorbehielte, diese Angaben auch zu überprüfen. Nach seiner Ansicht greife man damit "sehr stark in Persönlichkeitsrechte ein und fordere Informationen ein, die eigentlich nur von hoheitsrechtlich befugten Personen eingeholt werden dürfen". Das hielt der Bürger zu Recht für problematisch.

Grundlage des Verfahrens und für das Formular war ein Kreistagsbeschluß, der bei der Gebührentarifeinstufung grundsätzlich von einem Nettofamilienjahreseinkommen von über 80.000,- DM ausging und nur durch den Nachweis eines Einkommenssteuerbescheides eine davon abweichende Einstufung zuließ. Faktisch hatte dies eine generelle Nachweispflicht zur Folge; denn das durchschnittliche Nettojahreseinkommen bei Privathaushalten liegt nach der Mikrozensus-Erhebung 1993 im Land Brandenburg bei ca. 30.000,- DM, die zugrunde gelegten 80.000,- DM stellen im Land nach wie vor einen absoluten Ausnahmefall dar.

Ich habe mich daher an den zuständigen Landrat gewandt und gebeten mir mitzuteilen, aus welchen Gründen in seinem Zuständigkeitsbereich von der Praxis anderer Gemeinden im Land abgewichen wird, die nur bei Erfüllung besonderer Ermäßigungsvoraussetzungen (z. B. im Fall der Unterrichtung von Geschwistern oder in außergewöhnlichen Härtefällen) eine Glaubhaftmachung der Einkommensangaben verlangen, es im übrigen aber bei einer Selbsteinstufung der Teilnehmer belassen. Erfreulicherweise hat der Landrat mir hierauf mitgeteilt, daß der Kreistag eine erneute Änderung der Gebührenordnung beschlossen habe, wonach nun die Festsetzung der Gebühren "grundsätzlich in Form einer Selbsteinstufung der Gebührenpflichtigen erfolgt. In Ausnahmefällen kann die Beibringung eines Nachweises über die Einkommensverhältnisse gefordert werden (soziale Härtefälle oder erkennbar falsche Angaben)".

Im übrigen waren auf dem mir vom Petenten übersandten Vordrucksformular nicht die Anforderungen an eine datenschutzgerechte Vordrucksgestaltung in bezug auf das Aufklärungsgebot (s. unter 2.3) zu entnehmen. Auch dies wurde geändert, und der Antrag enthält nunmehr als Grundlage für die Gebührenerhebung den Hinweis auf § 13 Landkreisordnung (LKrO)[174] und § 6 Kommunalabgabengesetz (KAG)[175].

12.4.4 Veröffentlichung der Namen der ABC-Schützen

Die Gesellschaft für Datenschutz (Erfa-Kreis Brandenburg) teilte mir mit, daß manche Schulen eines Landkreises der örtlichen Presse die Namen ihrer ABC-Schützen übermittelt hätten, ohne daß die Erziehungsberechtigten hierfür ihre Einwilligung gegeben hätten. Weiterhin habe man sich über Schulen beklagt, die nicht bereit gewesen seien, der Presse die Namen der ABC-Schützen mitzuteilen. Da dies nicht zu den gesetzlich zugewiesenen Aufgaben gehört, sind die Schulen dazu auch nicht befugt.

Nach § 16 Abs. 1 Bbg DSG ist eine solche Übermittlung außerhalb des öffentlichen Bereiches nur unter bestimmten Voraussetzungen zulässig, die aber hier nicht vorlagen. Ein öffentliches Interesse oder ein berechtigtes Interesse kann der Zeitungsleser nicht geltend machen. Vielmehr ist gerade im ländlichen Bereich mit 10 und weniger Schulanfängern pro Gemeinde davon auszugehen, daß die Namen mit einem Telefonbuch ganz einfach und fast verwechslungsfrei den dort vorliegenden Anschriften zugeordnet und gezielt ausgewertet werden können; allein diese Tatsache wäre Grund genug, diese Namen als schützenswert anzusehen, es sei denn, die Eltern als Erziehungsberechtigte hätten hierzu schriftlich gem. § 4 Abs. 2 Bbg DSG eingewilligt. Insofern stellt auch Nr. 8 Abs. 1 Buchst. c VV-Datenschutz/Statistik[176] Schülerdaten gegenüber Einzelpersonen oder privaten Einrichtungen ohne Einwilligung der betroffenen Erziehungsberechtigten unter ein Verwertungsverbot.

12.4.5 Geplanter Zweckverband löste nicht Datenverarbeitung im Auftrag

Eine kreisfreie Stadt läßt seit Jahren ein Großteil ihrer personenbezogenen Daten bei einer nicht-öffentlichen Stelle in einem der alten Bundesländer verarbeiten. Vor diesem Hintergrund hatte ich mich seit dem Herbst 1992 mit diesem Thema zu befassen[177].

Die gesamte Situation änderte sich, als die Stadt im Herbst 1994 daranging, einen Zweckverband zu gründen, dem auch die datenverarbeitende Privatfirma angehören sollte, um so die Probleme ihrer Datenverarbeitung zu lösen. Auf diese Weise wäre die Datenverarbeitung im Auftrag zu einer eigenen Angelegenheit des Zweckverbandes

---

174 vom 15. Oktober 1993, GVBl. I S. 433, geänd. d. Ges. vom 14. Februar 1994, GVBl. I S. 34

175 vom 27. Juni 1991, GVBl. S. 200

176 vom 26. November 1993, ABl. S. 1730

177 s. 2. Tätigkeitsbericht unter 1.2.1.4 und 3. Tätigkeitsbericht unter 3.3

geworden, die Datenverarbeitung würde in einem solchen Fall im Sinne des Datenschutzrechts nicht mehr als "Datenverarbeitung im Auftrag" zu qualifizieren sein. Das Gesetz über kommunale Gemeinschaftsarbeit im Land Brandenburg (GKG)[178] läßt die Einbeziehung Privater in einen Zweckverband zu.

Die Stadt übersandte mir Ende 1994 den Satzungsentwurf für den Zweckverband zur Prüfung und bat darum, ihr meinen Standpunkt mitzuteilen. Parallel wurde der Entwurf der Kommunalaufsicht beim Ministeriums des Innern (MI) zur Genehmigung vorgelegt.

Es zeigte sich, daß der Datenschutz unter anderem auch dadurch beeinträchtigt werden kann, daß die Satzung zu viele Freiräume eröffnet, vor allem dadurch, daß private Mitglieder, die ja in einem derartigen Fall mit wirtschaftlichen Interessen innerhalb des Zweckverbandes tätig werden, zwar in ihrer Eigenschaft als Zweckverbandsmitglied dem Datenschutz der öffentlichen Stellen, aber für ihr eigenes Gebaren dem weniger strengen Datenschutzrecht für die nicht-öffentlichen Stellen unterliegen. Weiterhin sah meine Behörde Probleme darin, daß sich der Zweckverband zur Erledigung seiner Aufgaben ohne weitere Auflagen Dritter bedienen können sollte.

In dem gesamten Verfahren trat danach ein Stillstand ein. Trotz mehrfacher Anmahnungen kam es zu keinen weiteren Gesprächen. Nach Ablauf von mehr als einem Jahr, im Dezember 1995, teilte das MI der Stadt schriftlich mit, daß die Satzung für den geplanten Zweckverband in der vorliegenden Form nicht genehmigungsfähig sei, da zahlreiche Regelungen in dem Entwurf nicht mit den Vorschriften des GKG vereinbar seien.

Als Konsequenz beschloß die Stadt, den Zweckverband garnicht erst zu gründen.

Ein Teil der Probleme des Datenschutzes hat damit in einer überraschenden Weise eine Erledigung gefunden. Die weiterhin bestehenden Probleme der Datenverarbeitung im Auftrag bedürfen allerdings einer Lösung. Es wird bei der Aufarbeitung der Problemsituation aus meiner Sicht darauf hinzuwirken sein, daß nicht nur die damals bereits erkannten Schwächen in dem Vertragsverhältnis zwischen Stadt und Datenverarbeiterin im Auftrag beseitigt, sondern daß zusätzlich die Weiterentwicklungen im Datenschutzrecht beachtet werden.

12.4.6 Rufnummernanzeige bei Notrufen

Mit zunehmender Modernisierung des Telefonnetzes im Land Brandenburg kann auch die in ISDN-Netzen mögliche Anzeige der Rufnummern des Teilnehmers (Anrufers) beim Angerufenen sinnvoll genutzt werden. Das aus der Sicht des Datenschutzes in bestimmten Fällen kritisch zu betrachtende Leistungsmerkmal Rufnummernanzeige[179] besitzt in Verbindung mit Notrufen, die sich an Polizei, Feuerwehr oder Stationen der Ersten Hilfe richten, einen anderen Charakter und besonderen Stellenwert. Dadurch kann selbst bei unvollständigen Angaben des Anrufers aus seiner angezeigten Rufnummer festgestellt werden, von wo der Anruf getätigt wurde. Auch in diesen Fällen kann u. U. entsprechende Hilfe ohne Zeitverlust aktiviert werden.

Ein Landkreis, der seine Notrufzentrale modernisiert hatte, und bei dem sich die zuständige Telekom-Geschäftsstelle aus Datenschutzgründen weigerte, die Anzeige der Rufnummer des Teilnehmers zu schalten, wandte sich mit der Bitte um Unterstützung an mich. Ich mußte feststellen, daß die Entscheidung der Telekom-AG rein formal richtig war, denn die zu

---

178 vom 19. Dezember 1991, GVBl. S. 685

179 s. 2. Tätigkeitsbericht unter 1.4.1.2

diesem Zeitpunkt noch gültige Telekom-Datenschutzverordnung (TDSV)[180] enthält tatsächlich keine Rechtsgrundlage für eine zwangsweise Übermittlung der Rufnummer des Teilnehmers an die angerufene Notrufzentrale.

Trotzdem erschien mir das Anliegen des Landkreises in bezug auf Notrufe unter der Nummer 110 und 112 aus zweierlei Gründen sinnvoll und insoweit unterstützenswert. Die angestrebte Rufnummernanzeige dürfte dem Zweck eines Notrufs - Hilfe möglichst schnell und sicher zu erhalten - entsprechen und so u. U. im wörtlichen Sinne lebensrettend sein. Erfreulicherweise sieht auch der noch in Beratung befindliche Entwurf der neuen TDSV aus den vorgenannten Gründen eine Rechtsgrundlage für die nicht unterdrückbare Anzeige der Rufnummern bei Notrufen unter den Nummern 110 und 112 vor. Inzwischen teilte ich dem betreffenden Landkreis mit, daß ich keine Bedenken gegen die entsprechende Schaltung durch die Telekom-AG habe.

13 Personaldatenverarbeitung

13.1 Einführung eines Personalinformationssystems für die Landesverwaltung

Im Berichtszeitraum ist die Auswahl eines Personalinformationssystems[181] für die Landesverwaltung abgeschlossen worden. An der interministeriellen Arbeitsgruppe sind sowohl Personalräte als auch meine Behörde beteiligt. Derzeit werden erste Pilotanwendungen durchgeführt. Bei der Auswahl der Software spielten neben Kostenüberlegungen auch datenschutzrechtliche Gesichtspunkte eine erhebliche Rolle.

Bei der Planung solcher Systeme ist bedeutsam, daß Personalaktendaten gem. § 64 Abs. 1 Landesbeamtengesetz (LBG)[182] und § 29 Abs. 1 Bbg DSG grundsätzlich nur von der einstellenden und beschäftigenden Behörde verarbeitet werden dürfen. Ein Verarbeitungsverbund über Behördengrenzen hinaus ist nicht zulässig. Ein solches Personalinformationssystem kann nur eine Hilfsfunktion bei der Personal- und Stellenwirtschaft und bei Bewerber- und Fortbildungsverfahren sein. Es dient also im wesentlichen der Rationalisierung von Verwaltungsabläufen und ist in diesem Sinne ausbaufähig, etwa für Zeiterfassungs- und Bezügeverfahren.

Da der Zugriff auf Personalakten und Personalaktendaten nur bestimmten Mitarbeitern einer Behörde gestattet ist, muß auch eine strikte Abschottung der automatisierten Datenverarbeitung gesichert werden. Dazu gibt es verschiedene Möglichkeiten; z. B. könnte die Personalstelle einer kleineren Behörde abteilungseigene Rechner (PC) betreiben, die wohl untereinander, nicht aber mit dem Behördennetz verbunden sind.

Größere Behörden werden es bevorzugen, ihr Personalinformationssystem im Hausnetz mit Hilfe eines speziellen Personaldaten-Servers oder eines gemeinsamen Hausservers zu betreiben. In diesen Fällen sind strengere Sicherheitsmaßnahmen erforderlich, damit nicht Unbefugte in die sehr sensiblen Personalaktendaten einsehen können. Neben einer differenzierten Rechteverwaltung bis auf Dateifeld-Ebene sind wegen der kaum geschützten Übertragungsleitungen und der software-technischen Möglichkeiten der Systemadministratoren zusätzlich Verschlüsselungsverfahren einzusetzen, die auf anerkannten kryptographischen Verfahren basieren.

---

180 vom 24. Juni 1991, BGBl. I S. 1390

181 PERS-INF der Fa. BFD

182 vom 24. Dezember 1992, GVBl. I S. 506, geänd. d. Ges. vom 15. März 1995, GVBl. I S. 38

Eine nicht-manipulierbare Protokollierung aller Dateizugriffe ist unbedingt erforderlich.

Das Softwaresystem muß die Möglichkeit bieten, Abfragen (Recherchen) zu reglementieren, damit die Personalvertretung ihrer Mitbestimmungspflicht nachkommen kann und eine willkürliche Auswertung ausschließbar ist.

Das ausgewählte Personalinformationssystem kann die genannten datenschutzrechtlichen Kriterien im wesentlichen akzeptabel erfüllen und ist auch in verschiedenen Bundesbehörden im Einsatz. Zusätzlich wird unter Federführung des Ministerium des Innern (MI) ein Sicherheitskonzept erarbeitet, das spezielle technisch-organisatorische Maßnahmen zum Datenschutz für verschiedene Szenarien modifizierbar machen soll. Allerdings muß z. B. die Fernwartung eines Personalinformationssystems ganz ausgeschlossen sein, da unbefugte Zugriffe auf diese Weise nicht gänzlich ausgeschlossen werden könnten.

Dem Datenschutzbedürfnis und -recht der Beschäftigten dient auch der Entwurf einer Muster-Dienstvereinbarung "über den Einsatz, die Anwendung und den Ausbau der Informationstechnik für die Verarbeitung von Personendaten", die von der Arbeitsgruppe entwickelt wurde und in der die Behördenleitung u. a. ausdrücklich verpflichtet ist, alle notwendigen organisatorischen und technischen Maßnahmen zu treffen, um den Mißbrauch personenbezogener Daten zu verhindern.

13.2 Personalakten

13.2.1 Personalaktenführung

In ihrer Stellungnahme[183] zu meinem 3. Tätigkeitsbericht bestätigt die Landesregierung meine Auffassung, daß es über die grundsätzlichen, insbesondere beamtenrechtlichen Regelungen in den §§ 57 - 64 LBG hinaus einer weiterführenden Verwaltungsvorschrift bedarf, die sich auf den Beamtenbereich wie auf den Bereich der Angestellten und Arbeiter erstreckt.

Ein entsprechender Entwurf, der neben der Behandlung vorhandener Altpersonalakten (Kaderakten)[184] u. a. auch landeseinheitliche Vorgaben für das Anlegen, das Führen und die Aufbewahrung von Personalakten sowie die Auskunftserteilung, das Zugangs- bzw. Vorlage- und Einsichtsrecht berücksichtigen soll, konnte mir allerdings nicht - wie zunächst vorgesehen - noch vor Ablauf des Berichtsjahres vorgelegt werden.

Jedoch hat das MI nach Gesprächen mit mir für den Übergangszeitraum den Personalreferaten der Landesregierung sog. "Allgemeine Hinweise zu datenschutzrechtlichen Vorgaben bei der Führung von Personalakten" an die Hand gegeben, die inhaltlich als Rundschreiben[185] auch den Landkreisen und kreisfreien Städten Brandenburgs zur Beachtung zugeleitet wurden. Dabei wird in kurzen Ausführungen insbesondere auf folgende Grundsätze und datenschutzrechtliche Erfordernisse bei der Personalaktenführung hingewiesen:

- Grundsatz der Vertraulichkeit und Zweckbestimmung (Schutz vor unbefugter Einsichtnahme, Zweckbindung an Personalverwaltung und Personalwirtschaft)

- Erforderlichkeitsprinzip (ausschließliche Beschränkung auf Unterlagen, die mit dem

183 LT-Drs. 2/1834: Ziff. 3.1.1

184 s. 1. Tätigkeitsbericht unter 5.3.4

185 Rundschreiben II/1-65-80 des MI vom 26. September 1995

Dienst- bzw. Arbeitsverhältnis in unmittelbarem inneren Zusammenhang stehen)

- Vollständigkeit der Dokumentationen (Aufteilung in Personalgrundakte, Teilakten; Paginierungspflicht)

- Abschottungsgebot (Pflicht der strikten Trennung zwischen Beihilfenvorgängen und Grundakte bzw. anderen Teilakten)

- Gewährleistung des Datenschutzes nach Abschluß der Personalakte (Archivierung, Vernichtung).

Diese zusammenfassende, etwas plakative Darstellung könnte immerhin geeignet sein, die Sensibilität für Fragen des Personaldatenschutzes in den Verwaltungen des Landes weiter zu erhöhen. Ich erwarte allerdings, daß die beabsichtigten Verwaltungsvorschriften tatsächlich in der Sache "weiterführend" sein werden, und werde darauf drängen, um im nächsten Tätigkeitsbericht hierüber weitere Fortschritte berichten zu können.

13.2.2 Bereinigungsanspruch nicht immer sofort durchsetzbar

In einer interessanten Eingabe beklagte der Petent, daß in seine Personalakte bei einer Landesbehörde, bei der er mehrere Jahre als Beamter beschäftigt gewesen sei, unzulässigerweise Vorgänge aufgenommen worden seien, die nicht unmittelbar sein Dienstverhältnis beträfen, nicht der Personalverwaltung dienten und die trotz seiner Bitten, diese zu entfernen, weiterhin Bestandteil seiner Personalakte seien. Darüber hinaus wandte sich der Petent auch dagegen, daß diese Personalakte im Zusammenhang mit seiner anderweitigen Klage gegen die Behörde ohne seine Zustimmung in der von ihm bemängelten unbereinigten Form dem Verwaltungsgericht vorgelegt und somit Dritten - zumindest hinsichtlich der bemängelten Teile - unzulässigerweise zugänglich gemacht worden seien. Er bat mich, Einsicht in diese Personalakte zu nehmen und ihm bei der Bereinigung behilflich zu sein.

Leider kann ich ihm aus Rechtsgründen während des noch laufenden Verfahrens beim Verwaltungsgericht in eigener Kompetenz nicht weiterhelfen, da dem Landesbeauftragten für den Datenschutz als nicht am Verfahren Beteiligtem gem. § 2 Abs. 1 Bbg DSG eine Akteneinsichtnahme beim Verwaltungsgericht deshalb nicht zusteht, weil es sich bei der besagten Aktenanforderung nicht um eine Maßnahme der Justizverwaltung, sondern um eine solche handelt, die in den Bereich der richterlichen Unabhängigkeit fällt.

Zur Sache war zunächst festzustellen, daß Behörden gem. § 99 Abs. 1 Verwaltungsgerichtsordnung (VwGO)[186] verpflichtet sind, dem Gericht gemäß dessen Anforderung Urkunden oder Akten zur Verfügung zu stellen oder Auskünfte zu erteilen. Da Beschränkungen von diesem allgemeinen Grundsatz in § 99 VwGO abschließend genannt sind, kann aus § 61 LBG keine Verpflichtung für die Dienstbehörde abgeleitet werden, zuvor die Zustimmung des Betroffenen einzuholen. Vielmehr ist die Behörde verpflichtet, die angeforderten Teile vollständig vorzulegen, d. h. in der bis zu diesem Zeitpunkt vorliegenden Form. Da die Aktenanforderung keine Justizverwaltungsmaßnahme darstellt, sondern in den Bereich der richterlichen Unabhängigkeit fällt, muß ihr aufgrund der geltenden Rechtslage in dem vom Richter festgelegten Umfang entsprochen werden. In der Konsequenz bedeutet dies, daß hiervon ggf. auch Aktenbestandteile erfaßt sind, deren Zulässigkeit in der Personalakte zwar bestritten, deren Unzulässigkeit aber (noch) nicht rechtsverbindlich festgestellt (worden) ist.

---

[186] i. d. Fass. vom 19. März 1991, BGBl. I S. 686, zul. geänd. d. Art. 2 Magnetschwebebahngesetz vom 23. November 1994, BGBl. I S. 3480

Zur konkreten Vorgehensweise habe ich den Petenten auf die Möglichkeit verwiesen, durch seine Rechtsanwälte im Rahmen deren Einsichtsrechts nach § 100 Abs. 1 VwGO feststellen zu lassen, ob seine Personalakte vom Verwaltungsgericht uneingeschränkt (also auch mit den von ihm für unzulässig gehaltenen Vorgängen) oder lediglich in (anderen) Teilen angefordert worden ist. Im übrigen konnte ich ihm für den Fall, daß er nicht direkt im Rechtswege auch die Bereinigung seiner Personalakte von möglichen unzulässigen Vorgängen erwirken wollte, nur vorschlagen, daß ich nach Abschluß des laufenden Verwaltungsstreitverfahrens bei der ehemaligen Dienstbehörde Einsicht in die Personalakte nehmen und ggf. auf Bereinigung der Akte drängen werde.

13.2.3 Begrüßenswerte "Überprüfungs-Grundsätze" ...

In welchen Fällen zu welchem Zeitpunkt und zu welchen konkreten Zwecken die öffentlichen Arbeitgeber/Dienstherren von einer Anfrage beim Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU) Gebrauch machen und in welcher Weise diese mit den Überprüfungsergebnissen verfahren sollen, ist nicht vom Stasi-Unterlagen-Gesetz (StUG)[187] ableitbar. Bereits vom Zeitpunkt meines Amtsantrittes an habe ich immer wieder darauf hingewiesen, daß hierin lediglich die Befugnisnorm für die Auskunftserteilung gesehen werden kann, im übrigen aber die Landesgesetzgeber gehalten sind, normenklare gesetzliche Regelungen für ihre Bereiche zu schaffen[188].

Leider stehen solche gesetzlichen Regelungen auch in Brandenburg weiterhin aus, jedoch hat die Landesregierung in Umsetzung und auf der Grundlage zweier Landtagsbeschlüsse[189] Grundsätze der Landesregierung für die Überprüfung von Dienstkräften des Landes Brandenburg hinsichtlich einer Tätigkeit für das ehemalige Ministerium für Staatssicherheit/Amt für Nationale Sicherheit (MfS/AfNS)[190] geschaffen, die für die Beschäftigten des Landes Brandenburg unmittelbar gelten und deren entsprechende Anwendung den Gemeinden und Gemeindeverbänden anempfohlen ist. Hierzu konnte ich rechtzeitig meine datenschutzrechtlichen Anregungen und Vorschläge einbringen.

Auffällig war, daß bereits der vorgelegte Entwurf meine einschlägigen inhaltlichen Aussagen in den früheren Tätigkeitsberichten (s. o.) berücksichtigte. Auch wenn ich weiterhin darauf hinweisen mußte, daß die Regelungen in Form von Verwaltungsvorschriften grundsätzlich nicht datenschutzgerecht sein können, konnte ich doch mit Genugtuung feststellen, daß sie - unter dem Aspekt der Selbstbindung zumindest der Landesregierung - ihrem sachlichen Regelungsgehalt nach keinen datenschutzrechtlichen Bedenken begegnen, nachdem auf mein Betreiben hin insbesondere noch folgende Punkte eingefügt bzw. verdeutlicht wurden:

- "Die Antworten und Auskünfte des BStU und die im Zusammenhang mit dieser Anfrage entstandenen Vorgänge sind Bestandteil der Personalakte; sie sind als Teilakte zu führen und in einem geschlossenen Umschlag grundsätzlich räumlich getrennt von der Grundakte aufzubewahren."

- Bei den Personalverwaltungen (noch) eingehende Mitteilungen des BStU, die Personen betreffen, bei denen entsprechend den Überprüfungs-Grundsätzen die Anfrage zurückzuziehen ist/war, "sind - mit einem entsprechenden Vermerk versehen - dem

---

187 vom 20. Dezember 1991, BGBl. I S. 2272

188 s. 1. Tätigkeitsbericht unter 5.3.3 und 2. Tätigkeitsbericht unter 3.2.4

189 LT-Drs. 1/3098 vom 16. Juni 1994 "Mit menschlichem Maß die Vergangenheit bewerten" ; LT-Drs. 2/575-B vom 26. April 1995 "Weitere Verfahren der Anfrage beim Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes"

190 vom 10. Oktober 1995, ABl. S. 914

Bundesbeauftragten zurückzusenden".

Bei der genannten Rücksendepflicht an den BStU ist vermieden, daß grundsätzlich geheimzuhaltende Informationen losgelöst von der Erforderlichkeit und in einer für die Betroffenen nicht nachvollziehbaren Streuung unkontrollierbar und somit kaum justitiabel den gesetzlichen Festlegungen des StUG entzogen werden.

Mit der Feststellung, daß die mit der Anfrage in Zusammenhang stehenden Vorgänge Bestandteile der Personalakte sind, bestätigt auch die Landesregierung, daß es sich bei diesen Daten materiell um Personalaktendaten i. S. v. § 57 LBG mit den sich hieraus für die Betroffenen ergebenden Rechten handelt (s. hierzu auch unter 13.2.1).

Durch die räumliche Trennung der relevanten Vorgänge von der jeweiligen Personalgrundakte kann zusätzlich erreicht werden, daß nicht bereits im Rahmen der Aufbewahrung nicht öffnungsberechtigte Mitarbeiter/-innen aus dem Volumen des Umschlags vorurteilsbegründende Rückschlüsse ziehen können.

13.2.4 ... noch nicht ganz durchgedrungen

Mit Erstaunen erfuhr ich im Sommer des Berichtsjahres vom Personalrat eines Ministeriums, daß es den dortigen Beschäftigten nicht nur verwehrt werde, Kopien von den jeweils sie selbst betreffenden Überprüfungsbescheiden des BStU zu erhalten, sie darüber hinaus nicht einmal Einblick in diese Bescheide bekämen, ihnen das jeweilige Ergebnis lediglich mündlich vorgetragen würde.

Auf Befragen stützte das Ministerium auf die Aussage des BStU ab, daß die dort den Bescheiden zugesetzte Textstelle "Diese Mitteilung darf nicht an die betreffende Person herausgegeben werden, da sich die Mitteilung immer nur auf den bis dahin erschlossenen Bestand an Unterlagen bezieht und eine Berichtigung gem. § 4 Abs. 3 StUG nicht mehr gewährleistet werden könnte." weiterhin gültig sei, weil sich die rechtlichen Voraussetzungen im Überprüfungsverfahren nach den §§ 19 ff. StUG, die ihn ursprünglich zu diesem Verwendungshinweis veranlaßt hatten, nicht verändert hätten. Dabei hatte der BStU auf ausdrückliche Anfrage des Ministeriums lediglich auf die Möglichkeit nach §§ 12 ff. StUG aufmerksam gemacht, nach der die Beschäftigten "als Bürger" einen persönlichen Antrag auf Auskunft oder Akteneinsicht beim BStU stellen könnten, um bei ausdrücklichem Wunsch ggf. die Mitteilung zu erhalten, "daß unter den von ihnen eingereichten Daten keine Hinweise auf eine hauptamtliche oder inoffizielle Tätigkeit für den Staatssicherheitsdienst vorliegen".

Hinter dieser Aussage des BStU steht das Ziel zu vermeiden, daß vorläufige Bescheide als endgültige Bescheide angesehen und so von den Betroffenen verwendet werden könnten.

Zu vermuten ist, daß es aufgrund solcher Aussagen des BStU auch in anderen Bereichen der öffentlichen Verwaltung Brandenburgs - ungeachtet der Überprüfungs-Grundsätze der Landesregierung (s. unter 13.2.3) - zu Fehleinschätzungen und -entscheidungen kommt.

Tatsache ist, daß ein einschränkender Verwendungshinweis auch durch die bisherige Rechtslage nicht abgedeckt ist. Die Problematik der Einsichtnahme und der Anfertigung von Kopien von Mitteilungen des BStU wird durch das StUG nur insofern angesprochen, als die §§ 20, 21 jeweils Abs. 1 Nr. 6 der ersuchenden Stelle gebieten, der zu überprüfenden Person von dem Ersuchen "Kenntnis" zu geben. Dies begründet aber bereits aus dem StUG heraus den Anspruch der Betroffenen, in die Auskunft des BStU zumindest Einblick nehmen zu können.

Darüber hinaus werden durch diese Regelungen nicht die eindeutig und normenklar

geregelten Akteneinsichtsrechte aus § 60 LBG und Protokollnotiz zu § 13 Abs. 1 BAT-O[191] eingeschränkt. In Ziff. 6 Abs. 3 der Überprüfungs-Grundsätze der Landesregierung ist eindeutig bestätigt, daß die Antworten und Auskünfte des BStU und die im Zusammenhang mit dieser Anfrage stehenden Vorgänge Bestandteil der Personalakte sind.

Somit können grundsätzlich auch Kopien der Auskünfte des BStU angefertigt werden. In direkter bzw. analoger Anwendung von § 60 Abs. 3 LBG kann das Recht auf Fertigung bzw. Erhalt von Ablichtungen lediglich eingeschränkt werden, "soweit dienstliche Gründe nicht entgegenstehen". Dies jedoch kann nur im jeweiligen Einzelfall abgewogen und entschieden werden. Darüber hinaus dürfen Betroffene auf lediglich ein Auskunftsrecht entsprechend § 60 Abs. 4 LBG nur beschränkt werden, wenn mit einer Akteneinsichtnahme die Gefahr bestände, daß nicht oder nur mit großem Aufwand vermeidbar personenbezogene Daten Dritter zur Kenntnis gegeben würden. Dies dürfte aber in der überwiegenden Zahl der Auskunftsfälle ausgeschlossen sein, auf jeden Fall immer dann, wenn der BStU bestätigt, daß sich dort keine Hinweise auf eine inoffizielle oder hauptamtliche Zusammenarbeit mit dem Staatssicherheitsdienst ergeben haben.

An dieser Rechtslage können auch Überlegungen nichts ändern, mit der Weigerung der Herausgabe von Kopien von BStU-Auskünften verhindern zu wollen, daß vorläufige Bescheide als endgültige Bescheide angesehen und so von den Betroffenen verwendet werden könnten. Es ist vom Gesetzgeber eindeutig und normenklar geregelt, daß die Auskunft des BStU nur den Erkenntnisstand zum Zeitpunkt der Auskunft, der sich aus der Datierung seines Bescheides ergibt, ausweist. Für den Fall wichtiger neuer Erkenntnisse gilt die Nachberichtspflicht des § 4 Abs. 3 StUG.

Die Befürchtungen, überprüfte Mitarbeiter/-innen könnten die Kopien nutzen, um zu einem späteren Zeitpunkt einen Verstoß die besonderen Geheimhaltungsregelungen der Überprüfungs-Grundsätze vorzuhalten, könnten öffentliche Beschäftigungsstellen bzw. Dienstbehörden des Landes ggf. dadurch begegnen, daß sie sich den Empfang der Kopie jeweils auf dem dort verbleibenden und verschlossen aufzubewahrenden Original bestätigen lassen, um somit für den Eventualfall angemessen die Beweislast zu verändern.

13.3 Sonstiges

13.3.1 Gefahr der Ablesbarkeit automatischer Zeiterfassungssysteme

Welche Gefahren aus der Ablesbarkeit automatischer Zeiterfassungssysteme entstehen können und in welcher Weise ihnen begegnet werden kann, soll an folgendem Beispiel, das ich zu beurteilen hatte, deutlich werden:

In einer Dienststelle war ein automatisiertes Zeiterfassungssystem eingerichtet worden, bei dem die Mitarbeiter-bezogene Erfassung mittels eines individuellen Ausweises mit Magnetstreifen, der durch Kartenleser an den Dienstgebäudeausgängen gezogen werden muß, erfolgt. Auf dem Ausweis stand der jeweilige Vor- und Zuname für jeden lesbar aufgedruckt. Ohne weitere Zugriffssperren wie eine PIN oder ein zusätzliches Kennwort konnten mit dem Ausweis Informationen über Resturlaub der/des Beschäftigten, Zeitguthaben und geleistete Stunden außerhalb der Gleitzeit vom Zentralrechner abgerufen werden.

Bei einer solchen technischen Auslegung besteht das Hauptproblem darin, daß für den Fall

---

[191] Tarifvertrag zur Anpassung des Tarifrechts - Manteltarifliche Vorschriften (BAT-O) vom 10. Dezember 1990, GMBl. 1991 S.234, zul. geänd. am 4. November 1992, GMBl. 1993 S. 63

des Verlusts des lesbaren Ausweises unbefugte Dritte durch direktes Ablesen oder durch Abruf über die Kartenleser den Personenbezug herstellen, somit eine personenbezogene Information über die Tatsache des Verlusts und darüber hinaus beim Aufrufen des jeweiligen Datensatzes zusätzlich sehr eingehende, nur das Dienst- bzw. Arbeitsverhältnis betreffende Informationen erhalten können.

Zwar haben die hiermit verbundenen Gefahren die betroffenen Mitarbeiter/-innen insoweit selbst zu vertreten, als eine unmittelbare Preisgabe ihrer personenbezogenen Daten durch die Dienststelle nicht stattfindet. Jedoch hat diese, wenn sie personenbezogene Daten automatisiert verarbeitet, Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten geeignet sind, gem. § 10 Abs. 2 Nr. 2 Bbg DSG u. a. zu verhindern, daß Datenträger z. B. unbefugt gelesen werden können.

Nach § 29 Abs. 1 Bbg DSG kann zwar die Tatsache der Einführung eines automatisierten Zeiterfassungssystems und die Festlegung des Datenumfangs hierzu durch Dienstvereinbarung (mit dem jeweiligen Personalrat) für die Arbeitnehmer bestimmend festgelegt werden (bei Beamten könnte die Hinnahme eine allgemeine Dienstpflicht darstellen), jedoch ist dabei den sich aus § 10 Bbg DSG ersichtlichen Grundsätzen Rechnung zu tragen.

Um unangemessenen technischen und möglicherweise damit auch finanziellen Aufwand zu vermeiden, könnte es in Vergleichsfällen ausreichen, daß

- der auf dem Ausweis ausgedruckte Name durch eine Registriernummer ersetzt wird, die nur dem Betroffenen selbst bekannt ist und darüber hinaus nur von den zugriffsberechtigten Mitarbeitern zugeordnet werden kann,

- auch im Falle eines Abrufs durch unbefugte Dritte (eben bei Verlust des Ausweises) im Datensatz lediglich die für diese nicht personenbeziehbare Registriernummer angezeigt wird,

- für den Fall des Verlusts zusätzlich eine Zugriffssperre auf den jeweiligen Datensatz mit evtl. Neuvergabe einer Registriernummer vorgesehen wird.

13.3.2 Datenerhebung im Zusammenhang mit Honorarabrechnungen für Lehrbeauftragte

Im Zusammenhang mit seinem Honorarvertrag als Lehrbeauftragter einer Universität unseres Landes erhielt ein Berliner Diplomingenieur einen Fragebogen ausgehändigt, den die Zentrale Bezügestelle der Oberfinanzdirektion Cottbus (ZBB) üblicherweise gem. § 1 Abs. 1 Buchst. c BAT-O bei der Einstellung von Arbeitnehmern, die in einer der Rentenversicherungspflicht der Angestellten unterliegenden Beschäftigung tätig werden sollen, benötigt.

Den Vordruck befand ich zur Verwendung bei Honorarkräften nicht nur für ungeeignet, weil insbesondere die Fragen zur Ehepartnerin hinsichtlich des Orts- oder Sozialzuschlags, deren evtl. Beschäftigung im öffentlichen Dienst und Personalnummer, als auch Fragen zur eigenen Sozialversicherungsnummer, evtl. Krankenversicherungs- und Arbeitslosenversicherungspflicht für die Auszahlung des Honorars irrelevant sind. Der Vordruck mußte darüber hinaus bei Betroffenen auch noch den Eindruck erwecken, sie wären zur Abgabe sämtlicher Angaben verpflichtet. Insoweit war diese Form der Datenerhebung unerlaubt, weil sie für die Aufgabenerfüllung nicht erforderlich war.

Immerhin hatte ich es noch für zulässig erachtet, neben Namen und Vornamen, dienstliche und private Anschrift, Telefonverbindung (mit dem Hinweis auf Freiwilligkeit) und Bankverbindung auch noch den hauptberuflichen Arbeitgeber bzw. Dienstherrn und die

dortige Beschäftigung bzw. Position (Laufbahn) abzufragen, sofern die hauptberufliche Tätigkeit Relevanz für den Qualifizierungsnachweis und die Höhe des Honorars haben könnte.

In schneller Umsetzung meiner Vorschläge hat mir die betreffende Universität bestätigt, daß sie in Abstimmung mit der ZBB zukünftig den Fragebogen ZBB (A) 01 für die Erstellung von Lehrbeauftragten nicht mehr verwenden werde. Ein neuentwickeltes Formblatt für diese Fälle beschränkt sich auf die Abfrage der von mir vorgeschlagenen Daten.

14 Aus der eigenen Behörde

Von allen schriftlichen, z. T. mit erheblichem Prüfungs- und Rechercheaufwand verbundenen Vorgängen im Berichtsjahr, nahmen die Bürgereingaben einen Anteil von fast 40 % ein. Damit hat sich die bereits im Vorjahr beobachtete Tendenz des permanenten Anstiegs von Bürgereingaben fortgesetzt, die nicht zuletzt darauf zurückzuführen sein dürfte, daß unterdessen über 13.500 "Datenscheckhefte" den Bürgern kostenfrei zur Verfügung gestellt werden konnten. Die nach wie vor anhaltende Nachfrage hatte jedoch zur Folge, daß im Berichtszeitraum aus Kostengründen die Herausgabe von weiteren Informationsschriften zurückgestellt werden mußte.

Aber auch aus der Verwaltung kommen vielfältige Hinweise und Anfragen. Diese beziehen sich überwiegend auf systematische Mängel oder darauf, daß Mitarbeiter befürchten, durch Einzel- oder Dienstanweisungen oder aus Unkenntnis zu unrechtmäßiger Bearbeitung personenbezogner Daten gezwungen sein könnten.

Nachdem ich gegen Ende des Berichtszeitraumes auch die beiden letzten noch offenen, im Vorjahr bewilligten Stellen bzw. Planstellen den Anforderungen angemessen besetzen konnte, hat meine Dienststelle den auf absehbare Zeit abgeschlossenen Stellenrahmen von 15 Mitarbeitern/-innen erreicht. Damit ist endlich auch der juristische Bereich voll besetzt. Die vorläufig verbindlichen Aufgabenzuweisungen und Zuständigkeiten sind der Anlage 14 zu entnehmen.

Mit der Besetzung aller Stellen und Planstellen sind allerdings die räumlichen Kapazitätsgrenzen in meiner Dienststelle erreicht. Ich bin froh, daß noch rechtzeitig vor Verabschiedung des Haushaltsplans 1996 Mittel für Umbaumaßnahmen in den Haushalt eingestellt werden konnten, so daß unter Verzicht auf ebenfalls wichtige Nebenräume demnächst ein zusätzlicher Büroraum geschaffen werden kann.

Unter Berücksichtigung der Tatsache, daß es einerseits in Brandenburg über 2.500 öffentliche Stellen der Landes- und Kommunalverwaltung gibt, und daß andererseits durch die Lage meiner Dienststelle zur Landeshauptstadt die ständig notwendigen Fahrten zum Landtag sowie den dortigen Landesbehörden unter Nutzung öffentlicher Verkehrsmittel artbeitsökonomisch mit einem unvertretbaren Zeitverlust verbunden sind, bin ich dankbar, daß durch eine einvernehmliche Unterstützung durch den Landtag, das Finanzministerium und die Landtagsabgeordneten meiner Dienststelle vom Haushaltsjahr 1996 an ein zweiter Dienstwagen bewilligt worden ist. Ich gehe davon aus, daß damit auch eine effizientere Erledigung meiner Kontrollaufgaben möglich sein wird.

Schließlich sei erwähnt, daß Mitarbeiter meiner Dienststelle im Berichtszeitraum wiederum zwei Fortbildungsveranstaltungen zu rechtlichen und technisch-organisatorischen Datenschutzfragen beim LDS gehalten haben. Eine Erweiterung solcher eigentlich dringend erforderlichen Schulungsangebote für Mitarbeiter der öffentlichen Verwaltung wird unter Beteiligung meiner Dienststelle auch künftig zu meinem Bedauern aus Kapazitätsgründen nicht möglich sein. Insofern habe ich die Initiative eines Amtsleiters zu einer Art "offenen Weiterbildungsveranstaltung" begrüßt, woran Bedienstete mehrerer benachbarter Ämter

teilnahmen und hierbei ihre Fragen zu den von ihnen (aktuell) zu bearbeitenden Vorgängen beantworten lassen konnten. Es stellte sich heraus, daß diese Vorgehensweise für beide Seiten offensichtlich nicht nur äußerst effektiv sein kann, sondern der eigenen Dienststelle u. U. ebenfalls einen Zuwachs von Erkenntnissen erbringt. Deshalb werde ich auch in Zukunft gegenüber solchen neuen Formen der Kommunikation mit Kommunalverwaltungen offen sein.

Kleinmachnow, den 3. Mai 1996

Dr. sc. Dietmar Bleyl
Der Landesbeauftragte für den Datenschutz

Rede des Landesbeauftragten für den Datenschutz vor dem Plenum des Landtages Brandenburg am 24. Januar 1996

Sehr geehrter Herr Präsident! Sehr geehrte Damen und Herren Abgeordnete! Erfreulicherweise ist bei vielen im dritten Tätigkeitsbericht meiner Behörde dargestellten Sachthemen zwischen der Landesregierung und dem Landesbeauftragten für den Datenschutz eine weitgehende Übereinstimmung festzustellen. Hervorzuheben ist z. B. das erzielte Einvernehmen in bezug auf die Arbeitsweise in den Wohngeldstellen. Das Beispiel wird Sie vielleicht verwundern, aber damit sind nicht nur Maßstäbe für diesen Bereich, sondern darüber hinaus für den praktizierten Datenschutz in allen Bereichen gesetzt worden, in denen Sozialdaten verarbeitet werden. Weil bekanntlich Ausnahmen die Regel bestätigen, komme ich allerdings nicht umhin, an dieser Stelle einige Punkte wegen ihrer Bedeutung noch einmal anzusprechen bzw. sogar zurückzuweisen. Ich fange mit letzterem an.

Erstens: Nach Ansicht der Landesregierung handelt es sich bei der Führung der Schuldnerverzeichnisse nicht um eine Verwaltungsaufgabe im Sinne des § 2 Abs. 1 des Brandenburgischen Datenschutzgesetzes, sondern um eine gerichtliche Tätigkeit. Dagegen sprechen mehrere Gründe. In das Schuldnerverzeichnis sind lediglich Personendaten nach den Bestimmungen der Zivilprozeßordnung und der Abgabenordnung als Datensammlung eingestellt. Mit der Einstellung von Daten in das Verzeichnis selbst wird keine einzige rechtliche Entscheidung getroffen. Das Verzeichnis kann auch bei einem anderen Gericht oder als zentrales Verzeichnis für die Gerichte mehrerer Bezirke geführt werden. Schließlich sind Auskünfte aus diesem Register sogar durch automatische Abrufe zulässig. Dies läßt nur den Schluß zu, daß die Führung eines Schuldnerverzeichnisses eine Verwaltungsaufgabe ist.

Zweitens: Die Landesregierung erachtet es nicht als erforderlich, den Landesbeauftragten für den Datenschutz bei der Erstellung von Staats-Kirchen-Verträgen zu beteiligen. In diesem Zusammenhang vertritt sie die Auffassung, daß der Landesbeauftragte für den Datenschutz eine Behörde des Landtages sei und daher nicht früher als der Landtag selbst über Verträge mit der Kirche zu informieren sei. Dem halte ich entgegen, daß eine bloße Information meiner Behörde, wie sie der Landtag im Zusammenhang mit bevorstehenden Abschlüssen gemäß Artikel 94 der Landesverfassung erhält, für die Beteiligung des Landesbeauftragten für den Datenschutz nicht ausreichend wäre, da anderenfalls die datenschutzrechtliche Begleitung der Vertragsgestaltung durch den Landesbeauftragten für den Datenschutz nicht möglich ist. Deshalb muß die Einbeziehung des Landesbeauftragten für den Datenschutz bereits früher erfolgen.

Drittens: In meiner Stellungnahme zum Gesetz zur Ausführung des Gesetzes zu Artikel 10 Grundgesetz im Land Brandenburg hatte ich angeregt, im Hinblick auf die jüngste Vergangenheit der Brandenburger Bürger mit verdeckten Überwachungsmethoden, bei den Regelungen zur Überwachung des Post-, Brief- und Fernmeldegeheimnisses die Kontrolle der damit verbundenen Daten durch den Landesbeauftragten für den Datenschutz ausdrücklich vorzusehen. Dazu kann man durchaus unterschiedliche Auffassungen vertreten. Die Landesregierung schließt aus meinen Ausführungen, daß hier der brandenburgische Verfassungsschutz der Stasi gleichgesetzt sei. Dies weist sie aber mit der Begründung zurück, daß derartige Vergleiche durch ein Hilfsorgan "des Landtages nicht geeignet seien, um das Vertrauen der Bürger in demokratische Strukturen zu stärken". Diese Bewertung, Hilfsorgan zu sein, steht nicht im Einklang mit § 22 des Brandenburgischen Datenschutzgesetzes. Dagegen wende ich mich entschieden.

Im übrigen sei darauf hingewiesen, daß jeder Erkenntnisgewinn erst durch den Vergleich des Neuen mit dem bereits Bekannten erfolgen kann. Erst wenn Bürger Brandenburgs ihre in der ehemaligen DDR gemachten Erfahrungen mit der Kontrolle des Post- und Telefonverkehrs mit denjenigen Maßnahmen vergleichen, die der brandenburgischen Verfassungsschutzbehörde durch die Anwendung des G10-Ausführungsgesetzes ermöglicht werden, können Sie den grundlegenden Unterschied erkennen, der sich durch die Anwendung nachrichtendienstlicher Mittel in einem Rechtsstaat mit einem Staat, den man nicht als Rechtsstaat bezeichnen kann, ergibt. Was die Landesregierung vermutlich zurückweisen wollte, war also nicht der "Vergleich", sondern vielleicht vielmehr die "Gleichsetzung". Eine solche Gleichsetzung ist im dritten Tätigkeitsbericht nicht vorgenommen worden. Das läge mir absolut fern.

Viertens: Problematisch ist nach wie vor die Datenverarbeitung im Auftrag. Von dieser Möglichkeit einer Verschlankung öffentlicher Verwaltung, der ich grundsätzlich aufgeschlossen gegenüberstehe, machen Kommunen nach eigenen Ermittlungen zu 73 % bei Lohn- und Gehaltszahlungen, zu 60 % bei Meldedaten, aber eben auch zu 36 % bei Sozialdaten und zu 42 % bei anderen Daten, die einem besonderen Amtsgeheimnis unterliegen, Gebrauch. Hervorzuheben ist dabei nicht nur die weitere Verbreitung einer Datenverarbeitung im

Auftrag, sondern es sind die konkreten Konstellationen, die inzwischen gewachsen sind und erst langfristig geändert werden können.

Dies betrifft einmal die Fälle, in denen die Satzungen kommunaler Datenzentralen, die als Zweckverbände nach dem Gesetz über kommunale Gemeinschaftsarbeit gegründet wurden, es zulassen, die mit der Datenverarbeitung betrauten Unternehmen als Mitglieder aufzunehmen. Diese bleiben ihrem Wesen nach Private und mutieren nicht etwa zu öffentlichen Stellen. Ich nenne diese Konstruktion Augenwischerei; denn es entsteht dadurch ein neues datenschutzrechtliches Problem. Die Datenverarbeitung im Auftrag ist zwar formal ersetzt, aber der neue Zustand unterscheidet sich nicht von dem alten. Der Landesregierung habe ich daher vorgeschlagen, durch eine Änderung des Gesetzes über kommunale Gemeinschaftsarbeit derartige rechtliche Gestaltungen von Satzungen künftig auszuschließen. Seit 1993 habe ich dieses Problem wiederholt gegenüber der Landesregierung angesprochen, ohne daß bisher hierzu eine Entscheidung gefallen ist.

Zum anderen geht es um die Fälle, in denen außerhalb Brandenburgs ansässige Auftragnehmer personenbezogene Daten im Auftrag für öffentliche Stellen des Landes verarbeiten. Die Datenschutzgesetze, so auch das brandenburgische, gelten nur innerhalb des jeweiligen Landes. Für die betroffenen Brandenburger ergeben sich bei der Vergabe solcher Aufträge an Nichtbrandenburger Nachteile dadurch, daß erstens die für sie zuständige Kontrollbehörde in dem jeweils anderen Bundesland schwer zu erreichen ist, zweitens ihr Auskunfts- und Akteneinsichtsrecht nicht ganz so weit wie in Brandenburg reicht und drittens - das ist der entscheidende Punkt - die Haftung gegenüber dem privaten Auftragnehmer wegen unrichtiger Datenverarbeitung nur durchzusetzen ist, wenn diesem eigenes Verschulden bei der Datenverarbeitung nachgewiesen werden kann.

Offensichtlich kann hier nur bundesweit eine Lösung herbeigeführt werden. Durch Staatsverträge oder eine andere geeignete Regelung muß dem Landesbeauftragten für den Datenschutz eine auf den konkreten Auftrag beschränkte Kontrollbefugnis beim Auftragnehmer eingeräumt werden. Die jeweilige öffentliche Stelle ist dazu zu verpflichten, bei der Vertragsgestaltung die Unterwerfung unter die Kontrollbefugnis des Landesbeauftragten für den Datenschutz festzulegen. Über die Ausgestaltung einer solchen Regelung wird gemeinsam mit der Landesregierung nachzudenken sein. Gegebenenfalls wäre die Umsetzung dieses Gedankens entweder durch eine Initiative im Bundesrat anzuregen oder bei der anstehenden Novellierung des Bundesdatenschutzgesetzes zu berücksichtigen.

Fünftens: Für den dritten Tätigkeitsbericht habe ich als eines der Schwerpunktthemen die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung des von der Verfassung garantierten Grundrechts auf informationelle Selbstbestimmung gewählt. Detaillierte Ausführungen hierzu hat die Landesregierung ausdrücklich begrüßt; denn den öffentlichen Stellen in Brandenburg liegt damit eine Art Checkliste vor, wie vorhandene DV-Technik zunächst einmal möglichst optimal genutzt werden kann. Die konsequente Fortsetzung dieses Gedankens, mit Hilfe von DV-Technik einen Grundrechtsschutz zu gewährleisten, verlangt in Zukunft, daß auch solche Systeme eingesetzt werden, die von vornherein grundrechtsschonend ausgelegt sind. Die Landesregierung ist in der Pflicht, hierzu Vorgaben zu erlassen. Das verdeutlicht der Versuch auf der A 555 zur Einführung der Autobahnmaut. Er ist unter anderem daran gescheitert, daß keines der getesteten Systeme die Forderung nach Fahren ohne Datenspuren erfüllen konnte. Ich gehe sogar soweit, zu behaupten, daß dieses Problem, in der Gesellschaft "ohne Datenspuren agieren zu können", generell bei der Akzeptanz neuer Technologien künftig eine Rolle spielen wird, indem eine datenschutzrechtliche Unbedenklichkeitserklärung eine Art Gütesiegel für Angebote in der Informationsgesellschaft darstellen wird. Denken Sie beispielsweise an die vieldiskutierten Fälle wie elektronische Geldbörse, die Patientenchipkarte, die Bahn-Card, Telekommunikationstechnik, Telefonverzeichnisse auf CD-ROM usw.

Gestatten Sie mir noch einen kurzen Ausblick:

Der Datenschutz, genauer formuliert, der für die Kontrolle der öffentlichen Stellen zuständige Landesbeauftragte für den Datenschutz, erlebte in den letzten Jahren sowohl eine ständig steigende Beachtung des Gewichts des Datenschutzes als auch eine schleichende Einschränkung seiner Zuständigkeit.

Erstens, also die Beachtung des Datenschutzes, zeigt sich darin, daß sich immer häufiger Bürger an den Landesbeauftragten für den Datenschutz wenden.

Letzteres, die Einschränkung seiner Kompetenzen, ergibt sich daraus, daß die Gemeinden und die Landkreise zunehmend dazu übergehen, Einrichtungen, vor allem der Daseinsvorsorge, in eine private Rechtsform zu überführen. Für so privatisierte Einrichtungen der öffentlichen Hand ist der Landesbeauftragte für den Datenschutz dann nicht mehr zuständig. Der Bürger wird diese Entwicklung nicht begrüßen!

Die Fragen der Aufgabenverteilung und des Gewichts des Datenschutzes wird sich allerdings in naher Zukunft erneut zur Beantwortung stellen; denn innerhalb der nächsten drei Jahre - darauf habe ich im dritten Tätigkeitsbericht bereits hingewiesen - muß die EU-Datenschutzrichtlinie vom 24. Oktober 1995 in nationales Recht, also auch Landesrecht, umgesetzt werden. Die Unterscheidung von öffentlichen und nichtöffentlichen Stellen wird dann sicherlich nicht mehr so getroffen werden können, wie das jetzt noch der Fall ist. Die Richtlinie stellt Weichen dazu. Zum einen sind die Kontrollen von solchen Stellen wahrzunehmen, die "die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen". Zum anderen werden öffentliche Stellen und nichtöffentliche Stellen in bezug auf den Datenschutz einheitlich und nicht mehr nach getrennten Maßstäben zu bewerten sein.

Im übrigen sind mittels weiterer Vorgaben der EU-Richtlinie Eckpunkte für ein fundamentaleres Datenschutzkonzept gefunden worden, die Privatheit und Autonomie des Bürgers

auch in einer Informationsgesellschaft ermöglichen sollen. Ich wäre dankbar, wenn Sie mir Gelegenheit geben würden, dies demnächst einmal ausführlicher darlegen zu können. - Ich danke Ihnen für die Aufmerksamkeit.

Kopenhagener Resolution der Konferenz der Datenschutzbeauftragten der Europäischen Union vom 8. September 1995

(1) Der Vertrag über die Europäische Union nimmt an zwei Stellen (Art. F Abs. 2 und Art. K.2 Abs. 2) ausdrücklich auf die Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten Bezug und garantiert darin die Achtung der in der Konvention festgeschriebenen Grundrechte. Damit ist auch Art. 8 der EMRK - Gebot der Achtung der privaten Sphäre - von der Garantie des Unionvertrages mit umfaßt.

Die Konferenz nimmt die für 1996 geplante Regierungskonferenz zum Anlaß, im Hinblick auf den europäischen Grundrechtsschutz im allgemeinen und auf das Recht auf informationelle Selbstbestimmung im besonderen eine weitergehende Änderung bzw. Ergänzung der Unions- und Gemeinschaftsverträge zu fordern. Sie unterstützt dabei die Bestrebungen zur Schaffung eines verbindlichen europäischen Grundrechtskatalogs und plädiert darüber hinaus für die Aufnahme eines europäischen Grundrechts auf Datenschutz in diesen Katalog, wodurch die Unionsorgane wie die nationalen Stellen gebunden werden und der Datenschutz den Bürgern in einklagbarer Form gewährt wird.

(2) Gemeinschaftsrechtliche Regelungen verpflichten die Mitgliedsstaaten in immer größerem Maße zur Erhebung und Verarbeitung personenbezogener Daten, und gleichzeitig führen die europäischen Einrichtungen selbst zunehmend personenbezogene Datenbanken. Diese Einrichtungen sind jedoch nicht an die Grundsätze des Datenschutzes gebunden, insbesondere unterliegen sie keinem Datenschutzgesetz. Da der Datenschutz aber nicht mehr länger aus dem Wirken der Gemeinschafts- und Unionsorgane ausgeklammert bleiben kann, mahnt die Konferenz die Schaffung gemeinschaftsbezogener Datenschutzregelungen an.

Zwar war in dem von der Europäischen Kommission am 13.09.1990 vorgelegten Datenschutzpaket eine "Erklärung der Kommission betreffend der Anwendung der Grundsätze der Richtlinie zum Schutz von Personen bei der Verarbeitung personenbezogener Daten auf die Organe und Einrichtungen der EG" enthalten, die auf die Anwendung der Datenschutzrichtlinie auf EG-Institutionen abzielte. Dieses Vorhaben wurde indessen nicht weiterverfolgt. Die am 24.07.1995 verabschiedete Datenschutzrichtlinie richtet sich nur an die nationalen Gesetzgeber als Adressaten.

Um künftig sicherzustellen, daß den vielfältigen und umfangreichen Aktivitäten der Gemeinschaft die rechtzeitige und systematische Prüfung der datenschutzrechtlichen Auswirkungen zuteil wird, fordert die Konferenz für die Gewährleistung des Datenschutzes durch die Gemeinschaftsorgane und -einrichtungen die Schaffung rechtsverbindlicher Regelungen. Sie erinnert in diesem Zusammenhang an die Zusatzerklärung der Datenschutzbeauftragten der EG-Länder zur Berliner Resolution der Internationalen Konferenz der Datenschutzbeauftragten vom 30.08.1989 und ihren Vorschlag, wonach die Grundsätze der Europakonvention 108 durch entsprechende Rechtsakte der Europäischen Gemeinschaft für alle Mitgliedstaaten ebenso wie für die Institutionen der EG selbst verbindlich gemacht werden sollen.

(3) Nach wie vor fehlt es an einer unabhängigen und effektiven Datenschutzkontrollinstanz, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der Europäischen Union in seinen Rechten verletzt zu sein. Die Konferenz verweist auch in diesem Zusammenhang auf die Zusatzerklärung der Datenschutzbeauftragten der EG-Länder zur Berliner Resolution aus dem Jahre 1989 und ihren Vorschlag betreffend die Einrichtung einer unabhängigen Datenschutzkontrollinstanz. Diese sollte nicht nur Eingaben von Betroffenen entgegennehmen, sondern auch die Verarbeitung personenbezogener Daten innerhalb der Gemeinschaftseinrichtungen - nicht nur anlaßbezogen - kontrollieren, die Einrichtungen der Gemeinschaft in allen Datenschutzfragen beraten sowie mit den nationalen Datenschutzorganen zusammenarbeiten.

Entschließung

der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 09./10. November 1995 in Bremerhaven

zu

Forderungen an den Gesetzgeber zur Regelung der Übermittlung
personenbezogener Daten durch die Ermittlungsbehörden an die Medien
(außerhalb der Öffentlichkeitsfahndung der Ermittlungsbehörden)

1. Für die Übermittlung von personenbezogenen Daten durch Justiz und Polizei an die Medien sollte eine bereichsspezifische Rechtsgrundlage geschaffen werden. Die Regelung sollte für den betroffenen Bürger den Umfang des Eingriffs in sein Recht auf informationelle Selbstbestimmung erkennbar machen.

2. Die Übermittlung personenbezogener Daten an die Medien ist nur ausnahmsweise gerechtfertigt, wenn das Verfahren gerade im Hinblick auf die Person des Betroffenen oder die besonderen Umstände der Tat für die Öffentlichkeit von überwiegendem Interesse ist.

3. Bei der Entscheidung, ob und in welchem Umfang personenbezogene Daten an die Medien übermittelt werden, sind die schutzwürdigen Belange der Betroffenen zu berücksichtigen. Dazu zählen insbesondere die privaten und beruflichen Folgen für das Opfer, den Beschuldigten/Angeklagten und deren Angehörige sowie die Schwere, die Umstände und die Folgen des Delikts.

Bei der Übermittlung von personenbezogenen Daten über Beschuldigte/Angeklagte sind auch der Grad des Tatverdachts und der Stand des Verfahrens zu berücksichtigen. Vor Beginn der öffentlichen Hauptverhandlung ist ein besonders strenger Maßstab an das Vorliegen eines "überwiegenden Interesses" der Öffentlichkeit anzulegen.

Bis zur rechtskräftigen Verurteilung ist die Unschuldsvermutung zugunsten des Beschuldigten oder Angeklagten zu beachten. Zu unterlassen sind alle Auskünfte oder Erklärungen, die geeignet sind, die Unbefangenheit der Verfahrensbeteiligten zu beeinträchtigen. Akteneinsicht durch Medienvertreter kommt nicht in Betracht.

4. Grundsätzlich sind in Auskünfte und Erklärungen über das Ermittlungs- und Strafverfahren keine Namen und sonstige personenbezogene Angaben, die Opfer von Straftaten, Zeugen, Beschuldigte und Angeklagte bestimmbar machen, aufzunehmen. Vor allem bei Hinweisen auf den Wohnort, das Alter, den Beruf und die familiären Verhältnisse oder sonstigen sozialen Bindungen (z. B. Partei- oder Vereinsmitgliedschaft) ist zu prüfen, inwieweit dadurch eine Identifizierung des Betroffenen möglich wird.

5. Personenbezogene Daten dürfen nicht übermittelt werden, wenn besondere bundesgesetzliche oder landesgesetzliche Verwendungsregelungen entgegenstehen.

6. Ist die Bekanntgabe der Person des Beschuldigten oder Angeklagten wegen des überwiegenden öffentlichen Interesses gerechtfertigt, muß auch bei der Übermittlung sonstiger personenbezogener Daten abgewogen werden, ob diese Informationen für die Berichterstattung über die Tat selbst oder die Hintergründe, die zu der Tat geführt haben, erforderlich sind und in welchem Umfang der Betroffene dadurch in seinem Persönlichkeitsrecht beeinträchtigt wird.

7. Die Bekanntgabe von Vorstrafen ist nur ausnahmsweise zulässig. Sie setzt voraus, daß die frühere Verurteilung im Bundeszentralregister noch nicht getilgt und ihre Kenntnis für eine nachvollziehbare Berichterstattung über eine schwerwiegende Straftat - auch unter Berücksichtigung des Persönlichkeitsrechts des Betroffenen und des Resozialisierungsgedankens - erforderlich ist. Besondere Zurückhaltung ist bei Auskünften und Erklärungen über Sachverhalte geboten, die der früheren Verurteilung zugrunde liegen.

8. Wegen des überragenden Schutzes von Minderjährigen und Heranwachsenden ist bei Auskünften und Erklärungen über Verfahren gegen diesen Personenkreis besondere Zurückhaltung hinsichtlich der Bekanntgabe personenbezogener Daten zu wahren.

9. Opfer, Zeugen und Familienangehörige haben in der Regel keine Veranlassung gegeben, daß ihre persönlichen Lebensumstände in der Öffentlichkeit bekannt gemacht werden. Die Übermittlung personenbezogener Daten über diesen Personenkreis an die Medien kommt deshalb grundsätzlich nicht in Betracht.

10. Bildveröffentlichungen greifen wegen der damit verbundenen sozialen Prangerwirkung besonders tief in das Persönlichkeitsrecht des Betroffenen ein. Eine Bildherausgabe kommt daher für Zwecke der Medienberichterstattung nicht in Betracht.

Entschließung

der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 09./10. November 1995 in Bremerhaven

zu

Planungen eines Korruptionsbekämpfungsgesetzes

Derzeit gibt es Vorschläge, die Bekämpfung der Korruption durch Verschärfungen des Strafrechts und des Strafprozeßrechts mit weiteren Eingriffen in das Grundrecht auf informationelle Selbstbestimmung zu organisieren. Ein Beispiel dafür ist der Beschluß des Bundesrates vom 3. November 1995 zur Einbringung eines Korruptionsbekämpfungsgesetzes.

Nach dem vom Bundesrat beschlossenen Gesetzentwurf sollen Bestechlichkeit und Bestechung in den Kreis derjenigen Tatbestände aufgenommen werden, bei deren Verdacht die Überwachung des Fernmeldeverkehrs und der Einsatz technischer Mittel ohne Wissen des Betroffenen (§§ 100a, 100c StPO) angeordnet werden dürfen.

Die Datenschutzbeauftragten weisen demgegenüber darauf hin, daß es vorrangig um Prävention, nicht um Repression geht. Die Datenschutzbeauftragten treten für eine entschlossene und wirksame Bekämpfung der Korruption mit rechtsstaatlichen Mitteln unter strikter Beachtung der Freiheitsrechte ein.

Sie wenden sich zugleich gegen eine Rechtspolitik, welche - noch bevor sie sich darüber im klaren ist, was die bisherigen Verschärfungen und Eingriffe an Vorteilen und an Nachteilen gebracht haben - auf weitere Verschärfungen und Eingriffe setzt.

Gerade gegenüber der Korruption gibt es Möglichkeiten, welche Effektivität versprechen und gleichwohl die Privatsphäre der unbeteiligten und unschuldigen Bürgerinnen und Bürger nicht antasten:

- Rotation derjenigen Mitarbeiterinnen und Mitarbeiter einer Behörde, deren Position und Aufgaben erfahrungsgemäß für Bestechungsversuche in Betracht kommen;

- Vier- und Sechsaugenprinzip bei bestimmten Entscheidungen;

- Trennung von Planung, Überwachung und Ausführung, von Ausschreibung und Vergabe;

- Prüfverfahren und Innenrevision;

- Codes of Conduct (formalisierte "Ethikprogramme") im Bereich der Wirtschaft;

- verbesserte Transparenz von Entscheidungsprozessen in der Verwaltung.

Die in den Gesetzentwürfen vorgesehene weitere Einschränkung von Grundrechten, die mit einer abermaligen Erweiterung der Telefonüberwachung verbunden wäre, ist nur vertretbar, wenn sie nach einer sorgfältigen Güter- und Risikoabwägung zusätzlich zu den o. g. Verfahrens- und Verhaltensmaßregeln als geeignet und unbedingt erforderlich anzusehen wäre.

Die Datenschutzbeauftragten verlangen, daß vor einer zusätzlichen Aufnahme von Straftatbeständen in den Katalog der Abhörvorschrift des § 100a StPO diese Abwägung durchgeführt wird.

Die Datenschutzbeauftragten fordern weiterhin, daß eine Erweiterung des genannten Straftatenkataloges nur befristet vorgenommen wird, damit sich vor einer Verlängerung die Notwendigkeit stellt, auf der Grundlage einer sorgfältigen Erfolgs- und Effektivitätskontrolle erneut die Erforderlichkeit und Verhältnismäßigkeit einer solchen Erweiterung des Grundrechtseingriffs zu überprüfen.

Die Datenschutzbeauftragten verlangen, daß der Gesetzgeber vor weiteren Eingriffen in Freiheitsrechte eine sorgfältige Güter- und Risikoabwägung vornimmt und dabei insbesondere verantwortlich prüft, ob sich die innenpolitischen Ziele mit Mitteln erreichen lassen, welche die informationelle Selbstbestimmung der Bürgerinnen und Bürger schonen.

Schließlich gibt die anstehende erneute Erweiterung des Katalogs von § 100a StPO Veranlassung, den Umfang der darin genannten Straftaten sobald wie möglich grundlegend zu überprüfen.

Entschließung

der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 09./10. November 1995 in Bremerhaven

zu

Datenschutzrechtliche Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen

Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer 47. Konferenz am 09./10. März 1994 kritisch zum Einsatz von Chipkarten im Gesundheitswesen Stellung genommen. In dem Beschluß wird die Nutzung von Patientenkarten von mehreren Voraussetzungen zur Sicherung des Persönlichkeitsrechts abhängig gemacht.

Seitdem werden in mehreren Ländern Modellversuche und Pilotprojekte durchgeführt. Die Bandbreite reicht

- von allgemeinen Patientenkarten, die an möglichst viele Patienten/Versicherte ausgegeben werden, eine Vielzahl von Krankheitsdaten enthalten und von einem unbestimmten Kreis von Personen und Institutionen des Gesundheitswesens zu vielfältigen Zwecken verwendet werden können (z. B. Vital-Card der AOK Leipzig, Persönliche Patientenkarte Neuwied, BKK-Patientenkarte Berlin)

- bis zu krankheitsspezifischen Karten für bestimmte Patientengruppen mit reduziertem Datensatz und einer Definition der Verwendung (z. B. Dialyse-Card, Diab-Card, Krebsnachsorgekarte, Defi-Card).

Datenschutzrechtlich stellen sich vor allem folgende Probleme:

- Die massenhafte Einführung der Karten erzeugt einen sozialen Druck auf die Betroffenen, sie mitzuführen und vorzuzeigen. Diesen Erwartungen wird sich der Betroffene vielfach nur unter Befremden des Arztes oder sogar der Gefahr, daß dieser die Behandlung ablehnt, verweigern können.

- Die Verwendung von allgemeinen Patientenkarten bringt die Gefahr einer pauschalen Offenbarung von medizinischen Daten mit sich.

- Dem Patienten wird die Last aufgebürdet, für die Sicherheit seiner medizinischen Daten selbst zu sorgen.

Die Datenschutzbeauftragten fordern alle für Kartenprojekte im Gesundheitswesen Verantwortlichen in Politik, Industrie, Ärzteschaft, Wissenschaft und in den Krankenversicherungen auf, das Recht auf informationelle Selbstbestimmung der betroffenen Patienten bzw. Versicherten zu gewährleisten. Die 50. Konferenz hält folgende Voraussetzungen für elementar:

1. Besondere Schutzwürdigkeit medizinischer Daten

Medizinische Daten sind besonders schutzwürdig, unabhängig davon, welche Technologien eingesetzt werden, ob die Patientendaten beim Arzt gespeichert und versandt oder über ein Netz abgerufen werden oder ob der Patient die Daten auf einer Chipkarte bei sich hat. Es handelt sich oftmals um belastende, schicksalhafte Daten. Zudem geht es nicht nur um Daten des Patienten, sondern auch um fremde Einblicke in die ärztliche Tätigkeit.

2. Wirksame Entscheidung der Betroffenen über die Verwendung einer Karte

Die freie Entscheidung der Betroffenen (Patienten/Versicherten), eine Chipkarte zu verwenden, muß gewährleistet sein. Dies umfaßt die Entscheidung,

- ob Daten auf einer Chipkarte gespeichert werden,
- welche der Gesundheitsdaten auf die Karte aufgenommen werden,
- welche Daten auf der Karte wieder gelöscht werden,
- ob die Karte bei einem Arztbesuch bzw. einem Apothekenbesuch vorgelegt wird und
- welche Daten im Einzelfall zugänglich gemacht werden.

Ein Widerruf der Entscheidung muß ohne Nachteile für die Betroffenen möglich sein. Die gleiche Freiheit der Entscheidung für oder gegen die Verwendung der Chipkarte muß für Ärzte und Apotheker gewährleistet sein. Eine wirksame Entscheidung für oder gegen die Verwendung einer Chipkarte setzt eine schriftliche, objektive, vollständige und nachvollziehbare Information über Zweck, Art, Umfang und Beteiligte der Chipkarten-Kommunikation voraus. Das Gesamtkonzept des Chipkarteneinsatzes und der damit verbundenen Datenverarbeitung muß für die Betroffenen überschaubar sein.

Auf der Karte darf nicht der Datensatz der Krankenversichertenkarte nach § 291 Abs. 2 SGB V, insbesondere nicht die Krankenversicherung und die Krankenversicherungs-Nr., gespeichert werden, da andernfalls - zumal bei allgemeinen Patientenkarten mit hohem Verbreitungsgrad - die Krankenversichertenkarte verdrängt und deren Nutzungsbeschränkungen umgangen werden.

3. Freiheit der Entscheidung

Die uneingeschränkte Freiheit der Entscheidung der Betroffenen für oder gegen die Verwendung einer Chipkarte muß gewährleistet sein, denn der Einsatz von Chipkarten im Gesundheitswesen führt keineswegs zwangsläufig zu größerer Autonomie der Patienten. Neue Technologien können sich auch als Verführung erweisen, deren Preis erst langfristig erkennbar wird. Die individuelle Entscheidung des Bürgers über die Verarbeitung seiner Daten war und bleibt ein zentrales Recht gegenüber Eingriffen in seine Freiheitssphäre. Mit der Chipkarte können sich jedoch Situationen ergeben, in denen wirkliche Freiheit, tatsächliche Wahlmöglichkeit der Betroffenen nicht mehr gewährleistet sind und durch technische und organisatorische, rechtliche und soziale Rahmenbedingungen wiederhergestellt werden müssen.

Dem Staat kommt hier eine veränderte Rolle zu: Freiheitsrechte nicht einzuschränken, sondern sie zu sichern, wo Entwicklungen des Marktes und der Technologien sowie Gruppeninteressen die Entscheidungsfreiheit des Bürgers bedrohen. Die Technologie selbst kann für die Sicherung der Freiheitsrechte ein wertvolles Hilfsmittel sein. Darüber hinaus kommt der Informiertheit der Betroffenen ein zentraler Stellenwert zu. Ihre Kompetenz zur Entscheidung und zum praktischen Umgang mit der Karte muß gestärkt werden, damit sie auch langfristig die größtmöglichen Chancen haben, ihre Interessen durchzusetzen.

Mit der Ausstellung der Karte dürfen nur die Vorteile verknüpft werden, die sich unmittelbar aus den Nutzungspraktiken der Karte selbst ergeben. Die freie Entscheidung der Betroffenen, eine Karte zu nutzen oder dies abzulehnen, darf nicht durch einen Nutzungszwang oder eine Bevorzugung von Karten-Nutzern (z. B. durch Bonuspunkte) bzw. von Karten-Verweigerern eingeschränkt werden.

4. Keine Verschlechterung der Situation der Betroffenen

Durch die Einführung von Kommunikationssystemen mit Chipkarten dürfen die Betroffenen nicht schlechter gestellt werden als im konventionellen Verfahren. Die medizinische Versorgung, der Schutz der Gesundheitsdaten und die Mitentscheidungsrechte der Betroffenen müssen in Umfang und Qualität erhalten bleiben.

Das therapeutische Verhältnis Arzt/Patient darf sich durch den Einsatz von Chipkarten nicht verschlechtern. Freiheit und Vertrauen innerhalb des Arzt-Patienten-Verhältnisses sowie der Grundsatz der Abschottung der dem Arzt anvertrauten Informationen und der ärztlichen Erkenntnisse nach außen, gegen die Kenntnisnahme durch Dritte, müssen erhalten bleiben. Insbesondere muß der Gesetzgeber sicherstellen, daß die auf der beim Patienten befindlichen Chipkarte gespeicherten medizinischen Daten ebenso gegen Beschlagnahme und unbefugte Kenntnisnahme geschützt sind wie die beim Arzt gespeicherten Daten. Eine Kommunikation unter Vorlage der Karte mit Personen oder Stellen außerhalb des Arzt-Patienten-Verhältnisses, z. B. Arbeitgebern oder Versicherungen, muß vom Gesetzgeber untersagt werden.

Das sich im Gespräch entwickelnde Vertrauensverhältnis zwischen Arzt und Patient darf nicht durch eine Chipkarten-vermittelte Kommunikation verdrängt werden. Verkürzte Darstellungen medizinischer Sachverhalte auf der Chipkarte - z. B. mit Hilfe von Schlüsselbegriffen - dürfen nicht zu einer Minderung der Qualität des therapeutischen Verhältnisses führen; das liegt auch im Interesse des Arztes. Der Patient muß auch weiterhin die Möglichkeit des

individuellen Dialogs wählen können. Dies schließt insbesondere die Freiheit des Betroffenen ein, eine Chipkarte im Einzelfall nicht vorzulegen, auf der Chipkarte nur einen begrenzten Datensatz speichern zu lassen oder zu entscheiden, welchem Arzt welche Informationen oder Informationsbereiche offenbart werden. Der Patient darf durch die Ausgestaltung und den Verwendungszusammenhang der Chipkarte nicht zur pauschalen Offenbarung seiner Daten gezwungen sein. So sind Daten auf der Chipkarte so zu ordnen, daß z. B. beim Zahnarzt die gynäkologische Behandlung geheim bleiben kann.

Es darf keine "Einwilligung" in Chipkarten und Chipkartensysteme mit verminderter Datensicherheit geben. Der Gesetzgeber muß die Patienten vor "billigen Gesundheitskarten" ohne ausreichende Sicherung vor einer Nutzung durch Dritte schützen.

5. Sicherstellung der Integrität und Authentizität der Daten

Zur Sicherstellung der Vertraulichkeit, Integrität und Authentizität der Daten auf Chipkarten im Gesundheitswesen und zur Differenzierung der Zugriffsmöglichkeiten nach dem Grundsatz der Erforderlichkeit in unterschiedlichen Situationen sind kryptographische Verfahren sowie geeignete Betriebssysteme zur Abschottung unterschiedlicher Anwendungsbereiche nach dem Stand der Technik in Chipkarten und Schreib-/Lese-Terminals zu implementieren. Eine Protokollierung der Lösch- und Schreibvorgänge auf der Karte ist unverzichtbar.

Darüber hinaus ist für das infrastrukturelle Kartenumfeld (Herstellung, Verteilung, Personalisierung,..., Rücknahme) sicherzustellen, daß ausreichende technische und organisatorische Maßnahmen Berücksichtigung finden. Für die zur Erstellung und Personalisierung von Gesundheits-Chipkarten dienenden Systeme sowie die informationstechnischen Systeme und Verfahren, mit denen Daten auf der Chipkarte gelesen, eingetragen, verändert, gelöscht oder verarbeitet werden, muß der gleiche hohe Sicherheitsstandard erreicht werden.

6. Keine neuen zentralen medizinischen Datensammlungen

Der Einsatz von Chipkarten im Gesundheitswesen darf nicht zur Entstehung neuer zentraler Dateien von Patientendaten bei Kassenärztlicher Vereinigung, Krankenkassen, Kartenherstellern oder sonstigen Stellen führen. Dies gilt auch für das Hinterlegen von Sicherungskopien der auf der Karte gespeicherten medizinischen Daten. Es steht in der freien Entscheidung der Betroffenen, ob sie dem Arzt ihres Vertrauens eine umfassende Pflege aller Chipkarten-Daten - einschließlich der Sicherungskopien - übertragen oder nicht.

7. Leserecht des Karteninhabers

Der Karteninhaber muß das Recht und die Möglichkeit haben, seine auf der Chipkarte gespeicherten Daten vollständig zu lesen.

8. Suche nach datenschutzfreundlichen Alternativen

Angesichts der aufgezeigten Gefährdungen der informationellen Selbstbestimmung im Gesundheitswesen muß die Suche nach datenschutzfreundlichen Alternativen zur Chipkarte fortgesetzt werden.

Vorstehende Kriterien sind der Maßstab für die datenschutzrechtliche Bewertung von Projekten für die Einführung von Chipkarten im Gesundheitswesen.

Die Datenschutzbeauftragten von Bund und Ländern fordern die Gesetzgeber auf, die dringend notwendigen Regelungen zur Sicherung der Rechte von Patienten und Ärzten zu schaffen. Ebenso ist durch die Gesetzgeber den Besonderheiten der Datenverarbeitung auf Chipkarten durch bereichsspezifische Regelungen Rechnung zu tragen.

Entschließung

der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 09./10. November 1995 in Bremerhaven

zur

Weiterentwicklung des Datenschutzes in der Europäischen Union

Die Konferenz der Datenschutzbeauftragten der Europäischen Union hat am 08.09.1995 in Kopenhagen in einer Resolution im Hinblick auf die für 1996 geplante Regierungskonferenz dafür plädiert, anläßlich der Überarbeitung der Unions- und Gemeinschaftsverträge in einen verbindlichen Grundrechtskatalog ein einklagbares europäisches Grundrecht auf Datenschutz aufzunehmen. Die Schaffung rechtsverbindlicher Datenschutzregelungen für die Organe und Einrichtungen der Union sowie die Schaffung einer unabhängigen und effektiven Datenschutzkontrollinstanz der EU werden angemahnt. Dieser Resolution schließt sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an. Sie hält angesichts der fortschreitenden Integration und des zunehmenden Einsatzes von Informations- und Kommunikationstechnologien in der EU eine Weiterentwicklung des Datenschutzes im Rahmen der EU für geboten.

Sie fordert die zuständigen Politiker und insbesondere die Bundesregierung auf, dafür einzutreten, daß im EU-Vertragsrecht ein Grundrecht auf Datenschutz aufgenommen wird, die materiellen Datenschutzregelungen in der EU verbessert werden, das Amt eines Europäischen Datenschutzbeauftragten geschaffen wird sowie eine parlamentarische und richterliche Kontrolle der Datenverarbeitung der im EU-Vertrag vorgesehen Instanzen sichergestellt wird.

Grundrecht auf Datenschutz

Bei einer Weiterentwicklung der Europäischen Union ist es unabdingbar, daß dem Grundrechtsschutz eine angemessene Bedeutung beigemessen wird. Dies sollte dadurch geschehen, daß die Verträge zur Europäischen Union mit einem Grundrechtskatalog ergänzt werden. Mit einer Entschließung vom 10.02.1994 hat das Europäische Parlament einen Entwurf zur Verfassung der Europäischen Union zur Erörterung gestellt, der u. a. folgende Aussagen enthält: "Jeder hat das Recht auf Achtung und Schutz seiner Identität. Die Achtung der Privatsphäre und des Familienlebens, des Ansehens (...) wird gewährleistet".

Die Konferenz der Datenschutzbeauftragten ist mit ihrer Entschließung vom 28.04.1992 dafür eingetreten, daß in das Grundgesetz nach dem Vorbild anderer europäischer Verfassungen ein Grundrecht auf Datenschutz aufgenommen wird. Sie hat hierfür einen Formulierungsvorschlag gemacht. Auf ihren Konferenzen am 16./17.02.1993 und 09./10.03.1994 bekräftigten die Datenschutzbeauftragten des Bundes und der Länder ihre Position. Diese Forderung wurde aber wegen des Nichterreichens der notwendigen qualifizierten Mehrheit durch den Gesetzgeber nicht umgesetzt.

In Wirtschaft, Verwaltung und Gesellschaft der Staaten der EU erhält der Dienstleistungs- und Informationssektor eine zunehmende Bedeutung. Dies hat zur Folge, daß mit hochentwickelten Informationstechnologien von privaten wie von öffentlichen Stellen verstärkt personenbezogene Daten verarbeitet und auch grenzüberschreitend ausgetauscht werden. Diese Entwicklung wird gefördert durch die Privatisierung und den rasanten Ausbau transeuropäischer elektronischer Telekommunikations-Netze. Dadurch gerät das Grundrecht auf informationelle Selbstbestimmung in besonderem Maße auf der überstaatlichen Ebene in Gefahr. Dieser Gefahr kann dadurch entgegengetreten werden, daß in einen in den überarbeiteten EU-Vertrag aufzunehmenden Grundrechtskatalog das Grundrecht auf Datenschutz und zu dessen Konkretisierung ein Recht auf unbeobachtete Telekommunikation aufgenommen werden. Dies hätte folgende positive Auswirkungen:

- Anhand einer ausdrücklichen gemeinsamen Rechtsnorm kann sich eine einheitliche Rechtsprechung zum Datenschutz entwickeln, an die sowohl die EU-Organe wie auch die nationalen Stellen gebunden werden.

- Ein solches Grundrecht wäre die Basis für eine Vereinheitlichung des derzeit noch sehr unterschiedlichen nationalen Datenschutzrechts auf einem hohen Niveau.

- Den Bürgerinnen und Bürgern wird deutlich erkennbar, daß ihnen in einklagbarer Form der Datenschutz in gleicher Weise garantiert wird wie die traditionellen Grundrechte.

- Das grundlegende rechtsstaatliche Prinzip des Datenschutzes wird dauerhaft, auch bei Erweiterung der EU, gesichert.

- Mit der rechtlichen Konkretisierung eines Rechts auf unbeobachtete Telekommunikation würde der zunehmenden Registrierung des Verhaltens der Bürgerinnen und Bürger in der multimedialen Informationsgesellschaft entgegengewirkt und der Schutz des Fernmeldegeheimnisses auch nach dem Abbau der staatlichen Monopole im Sprachtelefondienst sichergestellt.

Materielle Datenschutzregelungen

Mit der kürzlich verabschiedeten EU-Datenschutzrichtlinie wird ein großer Fortschritt für den Datenschutz auf europäischer Ebene erreicht. Dies darf aber nicht den Blick dafür verstellen, daß in einzelnen Bereichen spezifische, dringend nötige Datenschutzregelungen fehlen. Insbesondere sind folgende Bereiche regelungsbedürftig:

- Es bedarf eines für die EU-Institutionen verbindlichen eigenen Datenschutzrechts. Die datenschutzrechtliche Verantwortung der Mitgliedstaaten einschließlich ihrer Datenschutzkontrolle der Übermittlung von Daten an EU-Institutionen bleibt dabei unberührt.

- Die geplante ISDN-Datenschutzrichtlinie darf weder einer völlig falsch verstandenen Subsidiarität zum Opfer fallen noch in unzureichender Form verabschiedet werden.

- Die im Bereich der Statistik bestehenden datenschutzrechtlichen Defizite sind abzubauen.

- Es soll eine Technikfolgenabschätzung bei der Förderung und Einführung neuer Informationstechniken mit Personenbezug durch die EU obligatorisch eingeführt werden.

- In den Bereichen Inneres und Justiz sind aufeinander abgestimmte verbindliche Regelungen mit hohem Datenschutzstandard, die die Datenverarbeitung in Akten und die Sicherung der Datenschutzkontrolle mit umfassen, zu schaffen.

- Es bedarf der Harmonisierung des Arbeitnehmerdatenschutzes auf hohem Niveau in den Staaten der EU.

- Für das Personal der EU-Organe ist der Arbeitnehmerdatenschutz sicherzustellen, was z.B. bei der Durchführung von Sicherheitsüberprüfungen insbesondere unter Beteiligung von Behörden der Heimatstaaten von großer Bedeutung ist.

Es ist zu prüfen, inwieweit Informationszugangsrechte in weiteren Bereichen eingeführt werden sollen.

Europäischer Datenschutzbeauftragter

Die Konferenz der EU-Datenschutzkontrollinstanzen (25./26.05.1994, 08.09.1995) und die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (25.08.1994) haben darauf hingewiesen, daß es an einer unabhängigen und effektiven Datenschutzkontrollinstanz fehlt, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der EU in seinen Rechten verletzt zu sein. Aufgabe eines Europäischen Datenschutzbeauftragten sollte die Behandlung aller Datenschutzbelange der EU sein. Dazu gehört nicht nur die Bearbeitung von Betroffeneneingaben, sondern auch die datenschutzrechtliche Beratung der EU-Organe und -Einrichtungen sowie deren anlaßunabhängige Kontrolle, die Begleitung informationstechnischer EU-Projekte und der entsprechenden EU-Normsetzung sowie die Zusammenarbeit mit den nationalen Kontrollinstanzen. Wegen der teilweise anders gelagerten Aufgaben sollen die Funktionen des Europäischen Datenschutzbeauftragten und des Bürgerbeauftragten nach den EG-Verträgen nicht vermengt werden. Die Bundesregierung sollte im Rahmen der Vorbereitung der Regierungskonferenz 1996 darauf hinwirken, daß ein unabhängiger Europäischer Datenschutzbeauftragter in den Verträgen über die Europäische Union institutionell abgesichert wird.

Parlamentarische und richterliche Kontrolle

Bei der Zusammenarbeit der EU-Staaten in den Bereichen Justiz und Inneres muß mit Besorgnis festgestellt werden, daß eine ausreichende parlamentarische und richterliche Kontrolle im EUV derzeit nicht gewährleistet ist. Die geplante Europol-Konvention ist hierfür ein Beispiel. Mit unbestimmten Formulierungen werden einem fast völlig freischwebenden Europäischen Polizeiamt informationelle Befugnisse eingeräumt, einem Amt, das keiner parlamentarischen Verantwortlichkeit und nur einer unzureichenden (teils nur nationalen) Rechtskontrolle unterworfen wird. Zur Wahrung des Datenschutzes bei der Umsetzung gemeinsamer Maßnahmen in den Bereichen Justiz und Inneres muß daher - unbeschadet der Kontrolle durch die nationalen Datenschutzbehörden - auch eine im Rahmen ihrer jeweiligen Zuständigkeiten lückenlose Kontrolle durch die nationalen Parlamente und Gerichte sowie durch das Europäische Parlament und den Europäischen Gerichtshof sichergestellt werden.

Entschließung

der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 09./10. November 1995 in Bremerhaven

zum

Datenschutz bei der Neuordnung der Telekommunikation (Postreform III)

Mit der Postreform III soll die Neugestaltung des Telekommunikationssektors in Deutschland nach den Vorgaben des Liberalisierungskonzepts der Europäischen Union abgeschlossen werden. Entstehen wird ein riesiger Markt mit einer Vielzahl von großen und kleinen, teilweise auch grenzüberschreitend tätigen Netzbetreibern und Diensteanbietern. Die Akteure auf diesem Telekommunikationsmarkt werden zum größeren Teil als Privatunternehmen operieren, es werden aber auch öffentliche Stellen ihre Leistungen anbieten. Der gesetzgeberische Abschluß der Liberalisierung und der Privatisierung des TK-Sektors wird die rechtliche Grundlage bilden für den endgültigen Eintritt in das Zeitalter von weltweiter Vernetzung, Multimedia und interaktiven Diensten und damit für den rapiden Anstieg des Konsums von Angeboten der Telekommunikation, des interaktiven Rundfunks und der Datenverarbeitung.

Die Konsequenzen sind absehbar: Gegenüber der heutigen Situation werden unvergleichlich mehr personenbezogene Daten durch mehr Stellen registriert und ausgewertet werden. Betroffen sind alle, die fernsehen, telefonieren, fernkopieren, Texte und Dokumente über Datenleitung schicken oder Telebanking oder Teleshopping betreiben. Die Risiken für den einzelnen durch die vermehrten Möglichkeiten der Verhaltens- und Umfeldkontrolle oder der Ausforschung persönlicher Lebensgewohnheiten und Eigenschaften vergrößern sich entsprechend.

Der vom Bundesministerium für Post und Telekommunikation vorgelegte Referentenentwurf für ein Telekommunikationsgesetz (TKG-E, Stand: 06.10.95) macht es erforderlich, erneut die Realisierung der grundlegenden Rahmenbedingungen für eine datenschutzgerechte Gestaltung der künftigen Telekommunikationslandschaft - soweit die Gesetzgebungskompetenz des Bundes betroffen ist - anzumahnen.

Ein wirksamer Datenschutz muß - wie bereits jetzt gesetzlich fixiert -auch künftig gleichberechtigtes Regulierungsziel neben z. B. der Sicherstellung der flächendeckenden Grundversorgung mit Telekommunikationsdienstleistungen bleiben.

Kundenwünsche nach variablerer und komfortablerer Nutzung der technischen Möglichkeiten werden zunehmen. Gerade deshalb müssen die Prinzipien der Datenvermeidung und der strikten Begrenzung der Datenverarbeitung auf das erforderliche Ausmaß ihren Vorrang bei der Ausgestaltung der kommunikationstechnischen Infrastruktur behalten. Netzbetreiber und Diensteanbieter sollten verpflichtet werden, überall dort, wo dies technisch möglich ist, auch anonyme Zugangs- und Nutzungsformen für ihre Leistungen bereitzustellen. Für eine sichere Datenübertragung sind ohne prohibitive Zusatzkosten wirksame Verschlüsselungsverfahren bereitzustellen.

Das Recht auf informationelle Selbstbestimmung und das Fernmeldegeheimnis müssen für alle Netzbetreiber und Diensteanbieter ungeachtet ihrer Rechtsform und ihrer Kundenstruktur (z. B. sog. Corporate Networks) einheitlich auf einem hohen Niveau gesichert werden. Der bisherige Schutzstandard darf keinesfalls unter den durch die Postreform II erreichten Stand gesenkt werden. Ein hohes Datenschutzniveau ist als Grundversorgung unabdingbar; seine Gewährleistung sollte deshalb Teil der Universaldienstleistung sein. Die in Grundrechte eingreifenden Regelungen sind im Telekommunikationsgesetz selbst und nicht in Verordnungen zu treffen. Die untergesetzlichen, den Datenschutz betreffenden Normen gehören in eine einzige, nicht verstreut in mehrere Verordnungen.

Entscheidend für die Wirksamkeit des Grundrechtsschutzes ist die strikte Einhaltung der Zweckbindung der Verbindungs- und Rechnungsdaten. Das "Feststellen mißbräuchlicher Inanspruchnahme" oder die "bedarfsgerechte Gestaltung" von TK-Leistungen dürfen nicht als Anlaß für eine umfassende Auswertung dieser Angaben oder sogar der Nachrichteninhalte herangezogen werden.

Für den Kunden bzw. Teilnehmer ist es von größter Bedeutung, die Verarbeitungsvorgänge im TK-Bereich überschauen zu können. Er muß auch künftig über die Nutzungsrisiken bestimmter Kommunikationstechniken (z. B. Mobilfunk) ebenso wie über seine Widerspruchsmöglichkeiten umfassend aufgeklärt werden. Keinesfalls darf die Einwilligung des Betroffenen mißbraucht werden, um bereichsspezifischer Schutznormen oder effiziente Datensicherungsvorkehrungen zu umgehen.

Um auch und gerade für das besonders schutzwürdige Fernmeldegeheimnis einen durchgängig hohen Schutzstandard zu sichern, braucht es eine unabhängige Kontrolle nach bundesweit einheitlichen Kriterien. Die Zuweisung dieser Überwachungsaufgabe an die im TKG-Entwurf vorgesehene Regulierungsbehörde ist wegen deren mangelhafter Unabhängigkeit und der von ihr wahrzunehmenden Regulierungsaufgaben, die mit Interessenkonflikten verbunden sein werden, nicht akzeptabel.

Deshalb sollte aufgrund seiner langjährigen fachlichen Erfahrung bei der Kontrolle der TELEKOM und seiner umfassenden Querschnittskenntnisse im TK-Bereich der Bundesbeauftragte für den Datenschutz eine zentrale Funktion für die Kontrolle im Telekommunikationsbereich erhalten. Die Aufgaben, die die Landesbeauftragten für den Datenschutz und die Aufsichtsbehörden im Rahmen ihrer Zuständigkeiten erfüllen, sind gesetzlich klar zu regeln.

Die Akzeptanz der Informationsgesellschaft der Zukunft hängt wesentlich ab von der Sicherung

des Grundrechts auf unbeobachtete Kommunikation. Das Telekommunikationsgesetz wird einen entscheidenden Baustein für die rechtliche Ausgestaltung der künftigen TK-Infrastruktur bilden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher dazu auf, die von ihr vorgeschlagenen Regelungen im weiteren Gesetzgebungsverfahren zu berücksichtigen und sich für ihre Umsetzung auch auf der europäischen Ebene (z. B. in der ISDN-Richtlinie) einzusetzen.

Entschließung

der 50. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 09./10. November 1995 in Bremerhaven

zum

Datenschutz bei elektronischen Geldbörsen und anderen kartengestützten Zahlungssystemen

Die Datenschutzbeauftragten des Bundes und der Länder halten es für dringend erforderlich, daß bei kartengestützten Zahlungssystemen, die zunehmend in Konkurrenz zum Bargeld treten, datenschutzfreundliche Verfahren eingesetzt werden. Dabei bietet es sich an, vor allem Guthabenkarten zu verwenden. Es sollten nur solche Clearingverfahren eingesetzt werden, die weder eine individuelle Kartennummer benutzen noch einen anderen Bezug zum Karteninhaber herstellen.

Sowohl im öffentlichen Personennahverkehr als auch bei der Deutschen Bahn AG können Fahrscheine bargeldlos erworben werden. Auch Autofahrer können auf Bargeld verzichten: Beim Parken, beim Tanken, künftig auch bei der Benutzung von Autobahnen wird verstärkt auf elektronisches Bezahlen zurückgegriffen. Immer mehr Telefone und Warenautomaten werden auf bargeldlose Zahlungsverfahren umgestellt, so daß viele Artikel des täglichen Bedarfs elektronisch bezahlt werden können. Von Kreditinstituten wird die Kombination verschiedener Anwendungen auf einer Karte angestrebt, z. B. mit einer Kombination der Bezahlung für den öffentlichen Nahverkehr, Parkgebühren und Benutzungsentgelte für öffentliche Einrichtungen.

Zum elektronischen Bezahlen werden entweder Kreditkarten, Debitkarten oder Guthabenkarten eingesetzt. Bei Kredit- und Debitkarten werden sämtliche Zahlungsbeträge verbucht, dem Käufer in Rechnung gestellt, auf den Kontoauszügen ausgedruckt und für mindestens 6 Jahre gespeichert. Dagegen wird bei Guthabenkarten im voraus ein Guthaben eingezahlt und bei jeder einzelnen Zahlung das Guthaben entsprechend herabgesetzt; die Zahlungsbeträge müssen keinem Käufer zugeordnet werden.

Beim elektronischen Bezahlen entstehen sehr unterschiedliche Datenschutzrisiken. Bei Kredit- und Debitkarten besteht die Gefahr, daß die aus Abrechnungsgründen gespeicherten personenbezogenen Daten ausgewertet und zweckentfremdet genutzt werden: Informationen über den Kauf von Fahrscheinen oder über die Nutzung von Autobahnen können zu den Bewegungsprofilen verdichtet werden. Das Konsumverhalten des einzelnen wird bis ins Detail nachvollziehbar, falls auch Kleineinkäufe am Kiosk nachträglich abgerechnet werden. Durch den Datenverkauf für Werbung und Marketing können sich weitere Risiken ergeben. Demgegenüber kann bei der Verwendung von Guthabenkarten auf das Speichern personen- oder kartenbezogener Daten aus erfolgten Zahlungen verzichtet werden.

Vor allem in Kleingeldbereichen ist die Nutzung von Debit- und Kreditkarten entbehrlich, da fälschungssichere Guthabenkarten auf der Basis von Chipkarten mit integriertem Verschlüsselungsbaustein zur Verfügung stehen. Falls größere Geldbeträge nachträglich per Kredit- oder Debitkarte bezahlt werden, ist darauf zu achten, daß die Abrechnung zunächst über Konten erfolgt, deren Inhaber dem Zahlungsempfänger nicht namhaft gemacht wird. Erst bei Zahlungsunregelmäßigkeiten ist es notwendig, den Bezug zum Kontoinhaber herzustellen.

Angesichts der Risiken, aber auch der von Chipkarten ausgehenden Chancen, fordern die Datenschutzbeauftragten die Kartenherausgeber und die Kreditwirtschaft dazu auf, kartengestützte Zahlungssysteme zu entwickeln, die möglichst ohne personenbezogene Daten auskommen, und deren Anwendung so zu gestalten, daß ein karten- und damit personenbezogenes Clearing nicht erfolgt. Der Gesetzgeber muß sicherstellen, daß auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher anonym zu bleiben.

Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet

**erstellt vom Arbeitskreis Technik
der Konferenz der Datenschutzbeauftragten des Bundes und der Länder**

1. Dezember 1995

Erarbeitet von Marit Köhntopp (LfD Schleswig-Holstein), Ulrich Kühn, HmbDSB, Ursula Meyer zu Natrup (BlnDSB), Peter Schaar (HmbDSB), Gabriel Schulz (LfD Mecklenburg-Vorpommern), Maren Thiermann (Lfd Hessen)

I. Einleitung

Seit einiger Zeit wächst in öffentlichen Stellen der Wunsch nach einem Zugang zu globalen Datennetzen, insbesondere zu dem Internet. Die Netzanbindung soll sowohl zur Informationsgewinnung als auch zur Bereitstellung eigener Informationen für andere dienen (zur Beschreibung des Internet und der wichtigsten Internetdienste vgl. Anlage 1).

Dabei ist der Anschluß an das Internet mit erheblichen Gefährdungen des Datenschutzes und der Datensicherheit verbunden. Die Risiken resultieren großenteils daraus, daß das Internet nicht unter Sicherheitsaspekten entwickelt wurde. Schwächen finden sich in den Protokollen für die Datenübertragung, in den Implementierungen und Installationen der Programme für die Internet-Dienste und in den angeschlossenen Rechnersystemen. So gibt es beispielsweise keine sicheren Mechanismen zur Identifikation und Authentisierung im Netz. Ohne besondere Schutzmaßnahmen kann sich ein Angreifer oft mit wenig Aufwand unter Ausnutzung der Sicherheitslücken unberechtigten Zugang zu fremden Rechnern verschaffen und dort Daten ausspähen oder sogar manipulieren oder zerstören. Dies ist besonders gravierend, weil angesichts von z. Zt. mehr als 40 Millionen Internet-Teilnehmern auch die Zahl der potentiellen Angreifer, die diese Sicherheitslücken ausnützen und somit die am Internet angeschlossenen Verwaltungsrechner bedrohen, sehr groß ist.

Die vorliegende Orientierungshilfe soll den für den Betrieb von Netzen der öffentlichen Verwaltung Verantwortlichen deutlich machen, mit welchen Risiken für die Sicherheit der „internen“ Netze bei einem Anschluß an das Internet zu rechnen ist und wie diese Risiken begrenzt werden können. Die Frage, ob und ggf. unter welchen Bedingungen Verwaltungen personenbezogene Daten über das Internet austauschen dürfen, ist nicht Gegenstand der Orientierungshilfe und muß jeweils konkret untersucht werden.

Die hier entwickelten Strategien zur Risikobegrenzung bedürfen im Einzelfall einer weiteren Konkretisierung, wobei neben den beschriebenen Firewall-Architekturen ggf. weitere Maßnahmen zu ergreifen sind, um eine Gefährdung personenbezogener Daten zu vermeiden (etwa Einsatz von Verschlüsselungsverfahren). Angesichts einer sich ständig verändernden Gefährdungslage infolge der „Entdeckung“ neuer unerwarteter Sicherheitsprobleme bleiben auch bei Einsatz von Firewall-Systemen erhebliche Restrisiken bestehen.

Der Anschluß an das Internet ist angesichts dieser Gefährdungslage aus Datenschutzsicht nur vertretbar, wenn zuvor eine eingehende Analyse und Bewertung der damit verbundenen Risiken erfolgt ist und die Gefahren durch technische und organisatorische Maßnahmen sicher beherrscht werden können. Die nachfolgenden Empfehlungen stellen ein Konzentrat aus den weiter unten angestellten eingehenderen Betrachtungen dar.

II. Empfehlungen

- Verwaltungsnetze dürfen an das Internet nur angeschlossen werden, wenn und soweit dies erforderlich ist. Die Kommunikationsmöglichkeiten haben sich am Kommunikationsbedarf zu orientieren. Dabei ist auch zu prüfen, inwieweit das Behördennetz in anschließbare, nicht anschließbare und bedingt anschließbare Teile segmentiert werden muß und ob die Aufgabe mit einem nicht in das Verwaltungsnetz eingebundenen Rechner erfüllt werden kann.

- Voraussetzung für die Anbindung eines Behördennetzes an das Internet ist das Vorliegen eines schlüssigen Sicherheitskonzepts und dessen konsequente Umsetzung. Die Internet-Anbindung darf nur erfolgen, wenn die Risiken durch technische und organisatorische Maßnahmen wirksam beherrscht werden können.

- Die Sicherheit des Verwaltungsnetzes und der Schutz von personenbezogenen Daten, die auf vernetzten Systemen verarbeitet werden, ist durch geeignete Firewall-Systeme sicherzustellen, die eine differenzierte Kommunikationssteuerung und Rechtevergabe unterstützen. Dabei sind die Anforderungen, die von den Firewall-Komponenten zu erfüllen sind, vorab zu definieren, wobei sich die Verwaltung ggf. auch externen Sachverstands bedienen sollte.

- Um der Gefahr von Maskeraden und der Ausforschung der Netzstrukturen des geschützten Netzes entgegenzuwirken, ist eine gesonderte interne Adreßstruktur zu verwenden. Die internen Adressen sind durch die zentrale Firewall auf externe Internet-Adressen umzusetzen.

- Der ausschließliche Einsatz einer zentralen Firewall-Lösung ist nur dann vertretbar, wenn eine Orientierung am höchsten Schutzbedarf erfolgt, auch wenn dies Nachteile für weniger sensible Bereiche mit sich bringt. Die Frage der Kontrolle interner Verbindungen bleibt bei einer solchen Lösung offen. Ferner ist eine ausschließlich zentrale Lösung mit der Maxime der lokalen Haltung und Verwaltung von sicherheitsrelevanten Daten (Pflege von Benutzerprofilen) schwer vereinbar. Werden

solche Daten nicht durch diejenigen verwaltet, die den verwalteten Bereich direkt überschauen können, besteht die Gefahr erheblicher Differenzen zwischen Realität und sicherheitstechnischem Abbild.

- Das Konzept gestaffelter Firewalls kommt den Datenschutzanforderungen an Verwaltungsnetze entgegen, die aus einer Vielzahl verschiedener Teilnetze bestehen, in denen Daten unterschiedlicher Sensibilität von unterschiedlichen Stellen für unterschiedliche Aufgaben verarbeitet werden und in denen dementsprechend jeweils unterschiedliche Sicherheitsanforderungen bestehen. Die mit gesonderten Firewalls abgesicherten Subnetze sollten jeweils einen definierten Übergang zu dem Gesamtnetz erhalten. Die Anbindung des Gesamtnetzes an das Internet sollte stets über ein zentrales Gateway erfolgen, das durch eine Firewall geschützt wird.

- Der personelle und sachliche Aufwand für Firewall-Lösungen ist generell hoch. Es ist gleichwohl unverzichtbar, hochspezialisierte Kräfte einzusetzen, um gegen mindestens ebenso spezialisierte Angreifer gewappnet zu sein. Dieser Aufwand ist jedoch stets dann gerechtfertigt, wenn Verwaltungsnetze an das Internet angeschlossen werden sollen, in denen sensible personenbezogene Daten verarbeitet werden.

- Der Betrieb von Firewall-Systemen muß klaren Richtlinien folgen. Diese Richtlinien müssen neben Zuständigkeitsregelungen auch Vorgaben über die Protokollierung, die Behandlung von sicherheitsrelevanten Ereignissen und Sanktionen bei Sicherheitsverstößen enthalten.

- Auch bei Einsatz von Firewalls bleiben Restrisiken bestehen, denen anwendungsbezogen begegnet werden muß. So bleibt es auch beim Einsatz von Firewalls notwendig, sensible Daten nur verschlüsselt zu übertragen; hierzu gehören neben besonders sensiblen personenbezogenen Daten auch Paßwörter und sonstige Authentifikationsdaten.

- Bei einem unvertretbaren Restrisiko muß auf einen Anschluß des jeweiligen Netzes an das Internet verzichtet werden. Der Zugriff auf Internet-Dienste muß in diesem Fall auf nicht in das Verwaltungsnetz eingebundene Systeme beschränkt werden, auf denen ansonsten keine sensiblen Daten verarbeitet werden.

- Firewall-Konzepte entlasten die dezentralen Verwalter von vernetzten Systemen nicht von ihrer Verantwortung zur Gewährleistung des Datenschutzes; vielmehr erhöhen sich mit der Vernetzung die Anforderungen an die lokale Systemverwaltung, da Administrationsfehler ungleich schwerwiegendere Konsequenzen haben könnten als bei stand alone betriebenen Rechnern.

III. Sicherheitsrisiken im Internet

Die nachfolgend dargestellten Sicherheitsrisiken spiegeln lediglich einen kleinen Ausschnitt der möglichen Angriffe auf Rechnersysteme mit Internet-Anschluß wider. Selbst wenn Gegenmaßnahmen gegen die bekannten Gefährdungen getroffen werden, läßt sich ein hundertprozentiger Schutz ohne Verzicht auf die Netzanbindung nicht realisieren. Sobald ein Computer Zugang zu einem Datennetz hat, ist er von anderen angeschlossenen Rechnern aus erreichbar. Damit wird das eigene System der Gefahr eines unberechtigten Gebrauches ausgesetzt. Es gibt jedoch eine Reihe von Schutzvorkehrungen, um das Sicherheitsrisiko zu minimieren.

1. Protokollimmanente Sicherheitsrisiken

Sowohl die Nutzerkennung als auch das Paßwort werden bei den gängigen Diensten im Klartext über das lokale Netz (z.B. Ethernet) und über das Internet übertragen. Mit Programmen, die unter dem Namen Packet Sniffer bekannt sind, kann der Datenverkehr im Netz bzw. auf den Netzknoten belauscht und nach interessanten Informationen durchsucht werden. So können diese Abhörprogramme zahlreiche Nutzerkennungen mit den zugehörigen Paßworten ausspähen, mit deren Hilfe sich ein Angreifer einen unberechtigten Zugriff auf andere Rechner verschaffen kann.

Datenpakete können nicht nur abgehört, sondern auch manipuliert werden. Da bei vielen Internet-Diensten die Authentisierung der Rechner lediglich über die IP-Nummer des Nutzers erfolgt, kann sich dies ein Angreifer zunutze machen, indem er IP-Pakete mit gefälschten Absenderadressen ans fremde Rechnersystem schickt (IP-Spoofing). Sofern das System die IP-Adresse für vertrauenswürdig hält, wird dem Eindringling ein Zugang, unter Umständen sogar mit Administratorrechten, gewährt. Ferner kann der Übertragungsweg bei dynamischem Routing geändert werden. Pakete können abgefangen werden, so daß sie nicht an ihrem Ziel ankommen; ein Angreifer kann sie durch eigene Pakete ersetzen. Weiterhin läßt sich die Kommunikation eines authorisierten Nutzers mitschneiden und später wiedereinspielen, wodurch sich der Angreifer bei vielen Diensten die Rechte des Nutzers verschafft (z. B. beim Festplattenzugriff über NFS (Network File System)).

2. Dienstspezifische Sicherheitsrisiken

E-Mail und Usenet-News:

Private Nachrichten können mitgelesen werden, sofern sie nicht verschlüsselt sind. E-Mails und News-Artikel ohne eine digitale Signatur lassen sich leicht verändern oder fälschen. Über den elektronischen Postweg können Programme und Textdokumente mit Viren ins System gelangen. Selbst ein automatisches Durchsuchen der Nachrichten nach Viren bietet keinen vollständigen Schutz.

Die Informationen über Datum und Uhrzeit der Erstellung einer Nachricht können zu einem Persönlichkeitsprofil des Absenders ausgewertet werden. Daneben forschen Adreßsammler nach

E-Mail- und Post-Adressen, um unaufgefordert Werbung zuzuschicken.

Sendmail, das auf UNIX-Rechnern am häufigsten eingesetzte Programm zum Verschicken elektronischer Post, weist zudem eine ganze Reihe von sicherheitsrelevanten Fehlern auf, die zu einer Zugangsmöglichkeit mit Administratorrechten führen können.

Zudem ist nicht sicherzustellen, daß eine email den Empfänger überhaupt erreicht und daß der Absender einen Nachweis der Zustellung erhält.

Telnet:

Ist der Telnet-Dienst nicht eingeschränkt, sondern von beliebigen Adressen aus zu beliebigen Ports auf dem eigenen Rechner möglich, wird die Zugangskontrolle gefährdet. Auch einem Angreifer, dem es nicht gelingt, sich einen Zugang mit Administratorrechten zu verschaffen, hat häufig die Möglichkeit, einen nichtprivilegierten Account auf dem Rechner zu nutzen. Dieser Account kann dann als Ausgangsbasis für den Angriff auf weitere Rechner verwendet werden.

FTP:

Schlecht gewartete FTP-Server stellen ein Risiko dar, da in älteren Versionen des FTP-Server-Programms (ftpd) Sicherheitslücken existieren, die zur Erlangung von Administratorrechten führen können. Besondere Vorsicht ist geboten, da viele Beschreibungen zur Installation und Konfiguration von Anonymous-FTP-Servern sicherheitsbedenkliche Fehler enthalten. Bei Fehlkonfigurationen kann es einem Angreifer gelingen, die Datei mit den verschlüsselten Paßwörtern aller Benutzer auf seinen Rechner zu laden und dort in aller Ruhe zu entschlüsseln. Läßt man zu, daß Benutzer eines FTP-Servers eigene Dateien in Verzeichnissen ablegen können, wo andere sie sich holen können, kann sich der FTP-Server schnell zu einem Umschlagplatz von Raubkopien entwickeln.

WWW:

Gefährdungen entstehen bei WWW-Servern durch fehlerhafte Software oder Konfigurationen. Ohne den Einsatz von SSL (Secure Socket Layer) läßt sich die Kommunikation abhören. Außerdem weisen CGI (Common Gateway Interface)-Skripte häufig Sicherheitslücken auf. Zur Zeit sind WWW-Browser in der Entwicklung, die das Ablegen von Dateien auf dem Server erlauben. Dies kann zu weiteren Sicherheitsproblemen führen. Beim Nutzen des World Wide Web können zahlreiche Daten über den Anwender und sein Verhalten (was hat wer wann aufgerufen und wie lange gelesen?) protokolliert werden, so daß ein umfassendes Persönlichkeitsprofil erstellt werden kann.

Finger:

Die Daten, die der Finger-Dienst ausgibt, können einem Angreifer Informationen über die Nutzerkennungen auf dem System liefern, die gezielt für einen Angriff verwendet werden können. Berühmt geworden ist dieser Dienst 1988 durch den sogenannten Internet-Wurm. Dabei handelte es sich um ein Angriffsprogramm, das ausnutzte, daß die beim Aufruf von Finger übergebenen Parameter in einen Puffer fester Länge geschrieben wurden. Die Daten, die nicht mehr in den Puffer paßten, überschrieben den Stack im Arbeitsspeicher, wo sie als Programmcode behandelt und ausgeführt wurden. Bei geschickter Wahl der übergebenen Zeichenreihe kann so beliebiger Code zur Ausführung kommen. Ähnliche Programmfehler finden sich auch heute noch in vielen anderen Serverprogrammen. Zum Beispiel ist gerade Ende 1995 ein weiterer solcher Fehler im Programm Sendmail bekannt geworden. Der Protokollierbefehl Syslog und manche WWW-Browser (auch für MS-Windows) enthalten ebenfalls Fehler dieser Art.

IV. Kommunikationsanalyse

Bevor eine öffentliche Stelle Zugang zum Internet bekommt, muß sie eine Analyse des Kommunikationsbedarfs durchführen. Bei der Beurteilung der Erforderlichkeit eines Internet-Anschlusses ist ein strenger Maßstab anzulegen. Auch wenn die Erforderlichkeit bejaht wird, ist zu prüfen, ob der Verwendungszweck nicht schon durch den Anschluß eines isolierten Rechners erreicht werden kann.

Die Art des zu realisierenden Zugangs hängt wesentlich davon ab, welche Dienste des Internet genutzt werden sollen. Dabei ist zu unterscheiden zwischen Diensten, die von lokalen Benutzern im Internet abgerufen werden, und Diensten, die von lokalen Rechnern für Benutzer im Internet erbracht werden. Diese Kommunikationsanforderungen müssen auf Grund der unterschiedlichen Aufgaben sowohl für den zentralen Zugang zum Internet als auch für jeden einzelnen Rechner analysiert werden. Es dürfen nur die IP-Pakete weitergeleitet werden, die für den zu nutzenden Dienst bezogen auf den nutzungsberechtigten Rechner notwendig sind.

Wird bei der Analyse des Kommunikationsbedarfs festgestellt, daß die Anbindung an das Internet auf IP-Ebene notwendig ist, das TCP/IP-Protokoll also in seiner vollen Funktionalität genutzt wird, müssen weitere Sicherheitsbetrachtungen durchgeführt werden, die Voraussetzung für die Planung und Realisierung von Sicherheitskonzepten sind. Ausgangspunkte einer derartigen Risikoanalyse sind der Schutzbedarf der zu verarbeitenden Daten und die Sicherheitsziele der öffentlichen Stelle.

In Anlehnung an die Empfehlungen des BSI-Grundschutzhandbuches sind zur Feststellung des Schutzbedarfs folgende Fragen zu beantworten:

- Welche Datenpakete dürfen auf der Grundlage welchen Protokolls bis zu welchem Rechner im Netz weitergeleitet werden?

- Welche Informationen sollen nicht nach außen gelangen?

- Wie können z.B. die interne Netzstruktur und Benutzernamen nach außen unsichtbar gemacht werden?

- Welche Authentisierungsverfahren sollen benutzt werden; sind benutzerspezifische Authentisierungsverfahren notwendig?

- Welche Zugänge werden benötigt (z.B. nur über einen Internet-Service-Provider)?

- Welche Datenmengen werden voraussichtlich übertragen?

- Welche Rechner mit welchen Daten befinden sich im Netz, die geschützt werden müssen?

- Welche Nutzer gibt es im Netz, und welche Dienste sollen dem einzelnen Nutzer zur Verfügung gestellt werden?

- Welche Aktivitäten im Netz sollen protokolliert werden? (Dabei werden ggf. Fragen des Arbeitnehmerdatenschutzes tangiert)

- Welche Dienste sollen auf keinen Fall genutzt werden?

- Wird sichergestellt, daß nur die Dienste genutzt werden können, die ausdrücklich freigegeben worden sind (was nicht erlaubt ist, ist verboten)?

- Welcher Schaden kann im zu schützenden Netz verursacht werden, wenn Unberechtigte Zugang erhalten?

- Welche Restrisiken verbleiben, wenn die vorgesehenen Schutzmaßnahmen realisiert wurden?

- Welche Einschränkungen würden Benutzer durch den Einsatz von Schutzmaßnahmen akzeptieren?

Um im Rahmen der empfohlenen Kommunikationsanalyse beurteilen zu können, welche Dienste von welchem Nutzer an welchem Rechner tatsächlich benötigt werden, sollten die jeweiligen Stellen zunächst versuchen, genaue Kenntnisse über die Möglichkeiten und Gefährdungen der angebotenen Kommunikationsmöglichkeiten zu erlangen (etwa durch entsprechende Tests mit an das Internet angeschlossenen Einzelplatz-PC).

V. Firewalls

Soll ein Verwaltungsnetz an das Internet angeschlossen werden, so kann dies entweder durch einen zentralen Zugang oder durch mehrere dezentrale erfolgen. Aus Sicherheitsgründen ist ein zentraler Zugang vorzuziehen. Ist das Verwaltungsnetz erst einmal an das Internet angeschlossen, so lassen sich die durch die Anbindung hervorgerufenen Sicherheitsrisiken durch Einsatz einer Firewall reduzieren.

Unter einer Firewall (“Brandschutzmauer”) wird eine Schwelle zwischen zwei Netzen verstanden, die überwunden werden muß, um Systeme im jeweils anderen Netz zu erreichen. Die Hauptaufgabe einer Firewall besteht darin, zu erreichen, daß jeweils nur zugelassene netzübergreifende Aktivitäten möglich sind und daß Mißbrauchsversuche frühzeitig erkannt werden. Üblicherweise wird dabei davon ausgegangen, daß die Teilnehmer des internen Netzes (hier: des Verwaltungsnetzes) vertrauenswürdiger sind als die Teilnehmer des externen Netzes (hier: des Internet). Gleichwohl sind Firewall-Lösungen auch geeignet, die “grenzüberschreitenden” Aktivitäten der internen Nutzer, d.h. den Übergang zwischen verschiedenen Teilnetzen (z.B. Ressortnetze) innerhalb eines Verwaltungsnetzes zu begrenzen.

Firewalls weisen die folgenden Charakteristika auf:

- die Firewall ist die definierte und kontrollierte Schnittstelle zwischen dem zu schützenden und dem nicht vertrauenswürdigen Netz;

- im internen Netz besteht jeweils ein einheitliches Sicherheitsniveau; eine weitere Differenzierung nach Sicherheitsstufen geschieht - zumindest auf der Ebene des Netzes - nicht;

- die Firewall setzt eine definierte Sicherheitspolitik für das zu schützende Netz voraus; in diese müssen die Anforderungen aller vernetzten Stellen einfließen;

- es besteht die Notwendigkeit einer firewallbezogenen Benutzerverwaltung derjenigen internen Teilnehmer, die mit Rechnern in dem externen Netz kommunizieren dürfen.

Die Stärke der Firewall hängt wesentlich von der eingesetzten Technik und ihrer korrekten Administration ab; entscheidend für die Sicherheit sind jedoch auch die Staffelung und die organisatorische Einbindung von Firewalls in die IuK-Infrastruktur.

Von besonderer Relevanz ist der Aspekt, daß für den von einer Firewall geschützten Bereich das erforderliche Schutzniveau definiert wird. Diese Anforderung kann mit drei Lösungsvarianten erfüllt werden:

- einheitlich hohes Schutzniveau im internen Netz, d.h. Orientierung am höchsten vorhandenen Schutzbedarf;

- einheitlich niedriges Schutzniveau, d.h. Orientierung am niedrigsten vorhandenen oder einem insgesamt geringen oder mittleren Schutzbedarf;

- einheitlich niedriges Schutzniveau sowie Durchführung zusätzlicher Maßnahmen zum Schutz von Netz-Komponenten mit höherem Schutzbedarf.

Die Varianten 1 und 2 entsprechen am ehesten zentralen Firewall-Lösungen, wobei angesichts der Sensibilität der in der Verwaltung verarbeiteten Daten allein Variante 1 mit den Anforderungen des Datenschutzrechts vereinbar sein dürfte. Variante 3 führt zur Lösung gestaffelter Firewalls, d.h. zu einer Konstellation, bei der neben einer zentralen, den mittleren Schutzbedarf abdeckenden Firewall (die u.a. die interne Netzstruktur nach außen sichert) bereichsbezogen und bedarfsorientiert Firewall-Anschlüsse mit unterschiedlichem Sicherheitsniveau implementiert werden können. Allerdings können selbst bei einheitlich hohem Schutzniveau im Gesamtnetz gestaffelte Firewalls sinnvoll sein, um den möglichen Schaden, der mit Sicherheitsverletzungen verbunden ist, auf ein Netzsegment zu begrenzen. Dies gilt insbesondere auch für die Abwehr von internem Mißbrauch.

1. Zentrale Firewalls

Rein zentrale Firewall-Lösungen (vgl. Abb.1) sind durch folgende Aspekte charakterisiert:

- die zentrale Firewall bildet die einzige Schnittstelle zwischen dem kompletten zu schützenden Verwaltungsnetz und dem übrigen Internet;

- innerhalb des Verwaltungsnetzes besteht ein einheitliches Sicherheitsniveau, eine weitere Differenzierung nach Sicherheitsstufen erfolgt nicht;

- eine Kontrolle der internen Verbindungen durch die Firewall ist nicht möglich;

- die zentrale Firewall setzt eine definierte Sicherheitspolitik für das gesamte Verwaltungsnetz voraus; abweichende Sicherheitspolitiken für besonders schützenswerte Bereiche sind auf Netzebene nicht durchsetzbar;

- es besteht die Notwendigkeit einer zentralen Benutzerverwaltung. Für jeden Teilnehmer muß sowohl auf Dienstebene als auch bezogen auf die zugelassenen Adressen die zulässige Kommunikation festgelegt werden.

Da eine zentrale Firewall eine Differenzierung nach Teilnetzen nicht unterstützt und dementsprechend ein einheitliches Sicherheitsniveau für das gesamte Verwaltungsnetz voraussetzt, muß sich der Grad des gewährleisteten Schutzes nach den sensibelsten Daten richten und ist dementsprechend hoch. Dies hat jedoch für Verwaltungsbereiche mit weniger sensiblen Daten den Nachteil, unnötig hohe Schranken zu errichten. Daraus ergibt sich die Gefahr, daß von diesen Stellen zusätzliche Internet-Zugänge mit geringeren Restriktionen geschaffen werden, wodurch der gesamte Zweck der Firewall ad absurdum geführt wird.

Ein weiterer Nachteil zentraler Firewalls besteht in dem - auch aus dem Großrechnerbereich bekannten - Problem, daß eine Benutzerverwaltung, die fernab von dem jeweiligen Fachbereich erfolgt, häufig zu Abweichungen zwischen der Realität von Benutzerrechten und deren Abbildung in Form von Accounts führt.

Da sich Firewall-Lösungen primär zum Schutz gegen Zugriffe von außen eignen, sekundär auch zum Schutz gegen Zugriffe von innen nach außen, jedoch nicht zur Kontrolle der rein internen Zugriffe, besteht bei rein zentralen Lösungen die Gefahr, daß das gesamte Verwaltungsnetz als eine Einheit betrachtet wird und insofern nur die Zugriffe von oder nach außen restringiert werden. Dieser Aspekt ist zwar nur mittelbar Teil des Themas "Internetanbindung", muß bei einer Gesamtbetrachtung von Netzwerksicherheit jedoch unbedingt einbezogen werden.

Der Einsatz einer alleinigen zentralen Firewall ist allenfalls dann vertretbar, wenn alle angeschlossenen Teilnetze über ein gleiches Sicherheitsbedürfnis bzw. -niveau verfügen und zudem nicht die Gefahr des internen Mißbrauchs besteht. Davon kann in behördenübergreifenden Verwaltungsnetzen mit einer Vielzahl angeschlossener Rechner jedoch nicht ausgegangen werden.

2. Gestaffelte Firewalls (Voraussetzungen, Einsatzmöglichkeiten, Forderungen)

Gestaffelte Firewall-Lösungen (vgl. Abb.2) sind durch folgende Aspekte charakterisiert:

- es handelt sich um eine Kombination zentraler und dezentraler Komponenten, wobei durch eine zentrale Firewall ein Mindestschutz für das Gesamtnetz gegenüber dem Internet realisiert wird und dezentrale Firewalls in Subnetzen mit besonderem Schutzbedarf ein angemessenes Schutzniveau sicherstellen;

- innerhalb des jeweiligen geschützten Subnetzes besteht jeweils ein einheitliches Sicherheitsniveau;

- eine Kontrolle der verwaltungsinternen Verbindungen ist möglich, sofern die Kommunikation den durch dezentrale Firewalls geschützten Bereich überschreitet;

- auch ein gestaffeltes Firewall-System setzt eine definierte Sicherheitpolitik für das Gesamtnetz voraus; in diese müssen insbesondere die Anforderungen an einen zu

garantierenden Grundschutz einfließen; darüber hinaus sind für die Subnetze gesonderte Sicherheitsanforderungen zu definieren;

- die Benutzerverwaltung kann weitgehend dezentralisiert werden. Allerdings sind einheitliche Regeln festzulegen, nach denen Benutzer das Recht haben, über die zentrale Firewall mit Systemen im Internet in Verbindung zu treten.

Für die dezentralen Firewalls bieten sich prinzipiell die gleichen Mechanismen wie bei einer zentralen Firewall an. Die Kombination zentraler und dezentraler Schutzmechanismen erlaubt die Realisierung des Prinzips eines autonomen Schutzes; bei sorgfältiger Konfiguration bleiben besonders geschützte Subnetze auch dann gesichert, wenn die zentrale Firewall durch einen Eindringling überwunden wurde.

Mit gestaffelten Firewalls kann – anders als bei zentralen Lösungen – das datenschutzrechtlich bedeutsame Prinzip der informationellen Gewaltenteilung abgebildet werden, mit dem es nicht zu vereinbaren wäre, wenn die Verwaltung als informatorisches Ganzes betrachtet würde. Die Teilnetze können sowohl gegen Angriffe von außen – aus dem Internet – als auch untereinander abgeschottet werden.

Da gestaffelte Lösungen besser als ausschließlich zentrale Firewalls die Anforderungen der Benutzer abbilden können, ist auch die Gefahr der Umgehung der kontrollierten Schnittstellen durch Schaffung „wilder“ Internetzugänge geringer. Zudem würden sich die Folgen derartiger Verstöße gegen die festgelegte Sicherheitspolitik besser isolieren lassen.

Auch gestaffelte Firewalls sind mit einem insgesamt hohen Administrations- und Pflegeaufwand für verbunden, der jedoch auf die zentrale Firewall und jeweiligen Bereiche verteilt ist. Die Festlegung der individuellen Benutzerrechte kann dabei im wesentlichen den anwendernäheren dezentralen Firewalls zugeordnet werden.

Anlage 1: Dienste im Internet

Das Internet ist ein weltumspannender Zusammenschluß vieler lokaler Computernetze. Die Zahl der Benutzer wird auf etwa 40 Millionen geschätzt (Stand: Ende 1995). Bisher wurde das Internet hauptsächlich von wissenschaftlichen Einrichtungen wie Universitäten genutzt. Inzwischen hat sich der Nutzerkreis ausgeweitet, und es ist eine fortschreitende Nutzung für kommerzielle Zwecke zu beobachten. Der Datenübertragung im Internet liegen die einheitlichen TCP/IP-Protokolle (Transmission Control Protocol/Internet Protocol) zugrunde.

Jeder Rechner im Internet erhält eine eindeutige numerische Adresse, die IP-Adresse. Die zu übertragenden Daten werden in Pakete zerlegt, die u.a. mit der Absender- und der Empfänger-IP-Adresse versehen werden. Die Datenpakete werden über zumeist eine Vielzahl von Zwischenstationen weitergeleitet, die den Weg zum Zielrechner aufgrund der Adreßinformationen bestimmen (Routing). Die Zwischenstationen tauschen die Daten über Wähl- oder Standverbindungen im Telefonnetz (per Kabel oder Satellit) aus.

Die wichtigsten Dienste, die das Internet bietet, werden im folgenden beschrieben.

E-Mail: Electronic Mail (kurz E-Mail) ist der am weitesten verbreitete Internet-Dienst. E-Mail ermöglicht das Verschicken von "elektronischen Briefen" zwischen mehreren Computerbenutzern. Die Nachrichten können aus Texten, Programmen, Grafiken oder Tönen bestehen. Sender und Empfänger müssen jeweils eine eindeutige E-Mail-Adresse besitzen (Form: Name@Anschrift), die ähnlich der postalischen Anschrift funktioniert. Um E-Mails in andere Datennetze zu verschicken oder von dort zu empfangen, werden Gateways benötigt, die den Übergang von einem System zum anderen handhaben. E-Mail kann außerdem für eine indirekte Inanspruchnahme von anderen Diensten (z.B. FTP, WWW) genutzt werden.

Usenet-News: Öffentliche Nachrichten werden im Internet in thematisch gegliederten Diskussionsforen (Newsgroups) ausgetauscht. Dieser News-Dienst wird auch als Usenet (Kurzform von Users´ Network) bezeichnet. Er gleicht einer riesigen Zeitung mit Fachartikeln, Leserbriefen und Kleinanzeigen. Zur Zeit gibt es etwa 10.000 verschiedene Newsgroups, in denen pro Monat rund 3,2 Millionen Artikel mit einem Datenvolumen von ca. 14 GB geschrieben werden (Stand: August 1995). Die Artikel werden auf zentralen Rechnern (Newsservern) in Datenbanken gehalten; der Zugriff erfolgt über Newsreader-Programme.

Telnet: Mit Hilfe von Telnet ist es möglich, auf einem entfernten Rechner eine Terminalsitzung aufzubauen (Remote Login) und textorientierte Anwendungen zu nutzen. Dazu benötigt man einen Account (Nutzerkennung und Paßwort) oder einen öffentlichen Zugang auf dem entfernten Rechner. Über Telnet sind zum Beispiel Informationssysteme wie Datenbanken oder Bibliotheken nutzen. Telnet wird ebenfalls häufig für die Fernwartung von Rechnern eingesetzt.

FTP: FTP steht für File Transfer Protocol und dient dem Übertragen von Dateien zwischen Rechnern mit Hilfe eines normierten Befehlssatzes. Auf dem eigenen Rechner läuft der FTP-Client, der die Befehle an den entfernten FTP-Server weiterleitet. Voraussetzung für die Nutzung sind Accounts auf beiden Rechnern oder eine öffentliche Zugriffsmöglichkeit auf dem FTP-Server durch "Anonymous FTP", wodurch ein eingeschränkter Zugriff auf bestimmte Dateien des entfernten Rechners ermöglicht werden kann. Weltweit gibt es Tausende Anonymous-FTP-Server, die Programme, Texte, Grafiken oder Tondateien bereithalten.

Archie: Archie ist ein mächtiger Dienst für die weltweite Suche nach Dateien auf FTP-Servern. Der Zugriff erfolgt über Telnet, E-Mail oder einen eigenen Archie-Client. Als Suchergebnis liefert Archie entweder Server-, Verzeichnis- und Dateinamen oder eine Kurzbeschreibung zu gesuchten Dateien.

WWW: Der jüngste Internet-Dienst WWW (World Wide Web) kann nahezu alle anderen Dienste integrieren. Durch einen multimediafähigen Hypertext-Mechanismus wird eine einfache Bedienbarkeit erreicht. Der Kommunikation zwischen dem WWW-Client und dem WWW-Server, der die multimedialen Daten anbietet, liegt das Protokoll HTTP (HyperText Transport Protocol) zugrunde. Die WWW-Dokumente werden mit der Definitionssprache HTML (HyperText Markup Language) erstellt. Für die Generierung interaktiver WWW-Seiten können CGI (Common Gateway Interface)-Skripte installiert werden.

Gopher: Gopher ist ein menü-orientiertes Werkzeug zur Recherche, das unabhängig davon eingesetzt werden kann, auf welchem Rechner die gesuchten Informationen zu finden sind, in welchem Format sie vorliegen und welche Zugriffsmöglichkeiten (FTP, Telnet, WAIS usw.) existieren. Jeder Gopher-Server ist öffentlich zugänglich. Benutzer können mit ihrem Gopher-Client nur lesend auf die angebotenen Daten zugreifen. Gopher ist im WWW integriert.

WAIS: WAIS (Wide Area Information Server) ermöglicht eine Volltextsuche in einer Vielzahl von Datenbanken ohne Kenntnis komplizierter Abfragesprachen. WAIS-Abfragen können mit Telnet, E-Mail, einem eigenen WAIS-Client oder über WWW durchgeführt werden.

Finger: Finger ist ein Werkzeug zur Suche nach Informationen über Personen und Rechner, die an der Kommunikation im Internet beteiligt sind. Es können sowohl personenbezogene Daten (Name, E-Mail-Adresse, Telefonnummer, Arbeitszeit, öffentliche Schlüssel usw.) als auch sicherheitsrelevante Informationen über angeschlossene Rechner in Erfahrung gebracht werden.

WhoIs: WhoIs wurde speziell zur Recherche nach personenbezogenen Daten von im Internet registrierten Nutzern entwickelt. Das Vorhaben, eine Datenbank mit weltweit allen Internet-Nutzern aufzubauen, konnte nicht realisiert werden. Zur Zeit existiert eine Vielzahl von einzelnen WhoIs-Servern, auf die mit Telnet oder mit besonderer Client-Software zugegriffen werden kann.

Anlage 2: Beispielhafte Darstellung von Firewall-Architekturen

Eine Firewall kann durch durch verschiedene Konzepte realisiert werden. Im wesentlichen unterscheidet man folgende Grundkonzepte:

- Packet Filter (packet screen, screening router)

- Application Gateway (dual-homed-gateway)

Ein Packet Filter ist ein Router der IP-Pakete zur Unterscheidung zwischen der erlaubten und unerlaubten Nutzung von Kommunikationsdiensten filtert. Packet Filter können nach Quell- und Zieladresse sowie nach Quell- und Zielport filtern. Damit ist einerseits einschränkbar, welche Rechner an der Kommunikation beteiligt sein dürfen, sowohl im zu schützenden als auch im unsicheren Netz und andererseits, welche Kommunikationsdienste erlaubt sind.

Ein Application Gateway ist ein speziell konfigurierter Rechner über den die gesamte Kommunikation zwischen dem zu schützenden und dem unsicheren Netz stattfindet. Ein Application Gateway arbeitet, anders als ein Packet Filter, auf Anwendungsebene, d.h., die Kontrolle der Kommunikationsbeziehungen findet auf Anwendungsebene statt. Hierbei besteht z.B. die Möglichkeit ausführliche Protokolle (Audis) zu führen und eine benutzerbezogene Authentisierung für die unterschiedlichen Dienste durchzuführen.

Die Kombination der Grundkonzepte wird als screened Gateway bezeichnet und erhöht die Sicherheit der Firewall erheblich. Die Anordnung der beteiligten Komponenten kann variieren und erlaubt die individuelle Realisierung eines Firewall-Konzeptes.

Abbildung 1: Zentrale Firewall-Anordnung

Abb. 2: Gestaffelte Firewall-Anordnung

	VORTEILE	**NACHTEILE**
PACKET FILTER Router oder Rechner mit spezieller Software	leicht realisierbar: einfache Installation und Administration leicht erweiterbar Router auf dem Markt verfügbar Preis	IP-Spoofing möglich alle Dienste, die erlaubt und erreicht werden können , müssen sicher sein komplexe Filterregeln keine ausreichende Protokollierungsmöglichkeiten es ist nicht möglich, Dienste nur für bestimmte Benutzer zu zulassen
DUAL-HAMIT-GATEWAY Applikations-Gateway mit zwei Netz-Interfaces	kein Paket kann ungefiltert passieren umfangreiche Protokollierung möglich interne Netzstruktur wird verborgen	keine Transparenz für den Benutzer Probleme bei neuen Diensten Übernahme des Applikations- Gateway durch einen Angreifer führt zu einen vollständigen Verlust der Sicherheit Preis
SCREENED SUBNET Anordnungen aus Applikation Gateway mit einem oder zwei Packet-Filter-bilden Teilnetze	kein direkter Zugang zum Gateway möglich die Struktur der internen Netze wird verdeckt vereinfachte Regeln durch zweiten Filter durch Einsatz mehrerer Gateways läßt sich die Verfügbarkeit steigern umfangreiche Protokollierung möglich	wenn Packet Filter manipuliert werden, ist eine direkte Verbindung unter Umgehung des Gateways möglich keine Transparenz für den Benutzer Preis

Abb. 3: Vorteile und Nachteile von verschiedenen Firewall Typen

Abb. 4: Screened Subnet mit Dual-Hamit Gateway

Abb. 5: Anordnung der Mail-Server

Abb. 6: Anordnung der DNS-Server

Entschließung

der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 14./15. März 1996 in Hamburg

zur

Modernisierung und europäische Harmonisierung des Datenschutzrechts

Die Datenschutzrichtlinie der Europäischen Union vom Oktober 1995 verpflichtet alle Mitgliedstaaten, ihr Datenschutzrecht binnen drei Jahren auf europäischer Ebene zu harmonisieren. Die Richtlinie geht zu Recht von einem hohen Datenschutzniveau aus und stellt fest: "Die Datenverarbeitungssysteme stehen im Dienste des Menschen".

Die Datenschutzbeauftragten begrüßen diesen wichtigen Schritt zu einem auch international wirksamen Datenschutz. Sie appellieren an den Gesetzgeber in Bund und Ländern, die Umsetzung der Richtlinie nicht nur als Beitrag zur europäischen Integration zu verstehen, sondern als Aufforderung und Chance, den Datenschutz fortzuentwickeln. Die Datenschutzbeauftragten sprechen sich für eine umfassende Modernisierung des deutschen Datenschutzrechts aus, damit der einzelne in der sich rapide verändernden Welt der Datenverarbeitung, der Medien und der Telekommunikation über den Umlauf und die Verwendung seiner persönlichen Daten soweit wie möglich selbst bestimmen kann.

Die wichtigsten Ziele sind:

1. Weitgehende Vereinheitlichung der Vorschriften für den öffentlichen und privaten Bereich mit dem Ziel eines hohen, gleichwertigen Schutzes der Betroffenen, beispielsweise bei der Datenerhebung und bei der Zweckbindung bis hin zur Verarbeitung in Akten

2. Erweiterung der Rechte der Betroffenen auf Information durch die datenverarbeitenden Stellen über die Verwendung der Daten, auf Auskunft, auf Widerspruch und im Bereich der Einwilligung

3. Verpflichtung zu Risikoanalyse, Vorabkontrolle, Technikfolgenabschätzung und zur Beteiligung der Datenschutzbeauftragten bei der Vorbereitung von Regelungen mit Auswirkungen auf den Datenschutz

4. Verbesserung der Organisation und Stärkung der Befugnisse der Datenschutzkontrolle unter den Gesichtspunkten der Unabhängigkeit und der Effektivität

5. Einrichtung und effiziente Ausgestaltung des Amtes eines internen Datenschutzbeauftragten in öffentlichen Stellen

6. Weiterentwicklung der Vorschriften zur Datensicherheit, insbesondere im Hinblick auf Miniaturisierung und Vernetzung

Darüber hinaus machen die Datenschutzbeauftragten folgende Vorschläge:

7. Erweiterung des Schutzbereichs bei Bild- und Tonaufzeichnungen und Regelung der Video-Überwachung

8. Stärkere Einbeziehung von Presse und Rundfunk in den Datenschutz; Aufrechterhaltung von Sonderregelungen nur, soweit dies für die Sicherung der Meinungsfreiheit notwendig ist

9. Sonderregelungen für besonders empfindliche Bereiche, wie den Umgang mit Arbeitnehmerdaten, Gesundheitsdaten und Informationen aus gerichtlichen Verfahren

10. Sicherstellung der informationellen Selbstbestimmung bei Multimedia-Diensten und anderen elektronischen Dienstleistungen durch die Pflicht, auch anonyme Nutzungs- und Zahlungsformen anzubieten, durch den Schutz vor übereilter Einwilligung, z.B. durch ein Widerrufsrecht, und durch strenge Zweckbindung für die bei Verbindung, Aufbau und Nutzung anfallenden Daten

11. Besondere Regelungen für Chipkarten-Anwendungen, um die datenschutzrechtliche Verantwortung aller Beteiligten festzulegen und den einzelnen vor unfreiwilliger Preisgabe seiner Daten zu schützen

12. Schutz bei Persönlichkeitsbewertungen durch den Computer, insbesondere durch Beteiligung des Betroffenen und Nachvollziehbarkeit der Computerentscheidung

13. Verstärkung des Schutzes gegenüber Adressenhandel und Direktmarketing

14. Verbesserung des Datenschutzes bei grenzüberschreitender Datenverarbeitung; Datenübermittlung ins Ausland nur bei angemessenem Datenschutzniveau

Entschließung

der 51. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
vom 14./15. März 1996 in Hamburg

zum

Transplantationsgesetz

Bei der anstehenden gesetzlichen Regelung, unter welchen Voraussetzungen die Entnahme von Organen zur Transplantation zulässig sein soll, werden untrennbar mit der Ausformung des Rechts auf Selbstbestimmung auch Bedingungen des Rechts auf informationelle Selbstbestimmung festgelegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder betont hierzu, daß von den im Gesetzgebungsverfahren diskutierten Modellen die "enge Zustimmungslösung" - also eine ausdrückliche Zustimmung des Organspenders - den geringsten Eingriff in das Recht auf informationelle Selbstbestimmung beinhaltet. Sie zwingt niemanden, eine Ablehnung zu dokumentieren. Sie setzt auch kein Organspenderegister voraus.

Mit einer engen Zustimmungslösung ist auch vereinbar, daß der Organspender seine Entscheidung z. B. einem nahen Angehörigen überträgt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt nachstehende Grundsätze für eine notwendige gesetzliche Regelung der öffentlichen Fahndung in Strafverfahren auf Basis der Vorlage des AK Justiz zustimmend zur Kenntnis.

Diese Grundsätze sollen schon jetzt soweit wie möglich bei der öffentlichen Fahndung beachtet werden (z.B. in den Fällen des § 131 StPO).

Grundsätze für die öffentliche Fahndung im Strafverfahren

Bei den an die Öffentlichkeit gerichteten Fahndungsmaßnahmen nach Personen (Beschuldigten, Verurteilten, Strafgefangenen und Zeugen) wird stets das Recht des Betroffenen auf informationelle Selbstbestimmung eingeschränkt. Es bedarf daher nach den Grundsätzen des Bundesverfassungsgerichts im Volkszählungsurteil vom 15.12.1983 für alle Maßnahmen der öffentlichen Fahndung nach Personen einer normenklaren und dem Grundsatz der Verhältnismäßigkeit entsprechenden gesetzlichen Regelung, die bisher fehlt.

1. Der Gesetzgeber hat zunächst die Voraussetzungen der öffentlichen Fahndung zu regeln und dabei einen sachgerechten Ausgleich zwischen dem öffentlichen Strafverfolgungsinteresse und dem Recht auf informationelle Selbstbestimmung des Betroffenen zu treffen.

   Die öffentliche Fahndung sollte nur bei Verfahren wegen Verletzung bestimmter vom Gesetzgeber zu bezeichnender Straftatbestände und bei Straftaten, die aufgrund der Art der Begehung oder des verursachten Schadens ein vergleichbares Gewicht haben, zugelassen werden.

   Sie soll nur stattfinden, wenn weniger intensive Fahndungsmaßnahmen keinen hinrei chenden Erfolg versprechen.

   Der Grundsatz der Erforderlichkeit mit der gebotenen Beschränkung des Verbreitungsgebiets ist auch bei der Auswahl des Mediums zu berücksichtigen.

2. Bei der öffentlichen Fahndung nach unbekannten Tatverdächtigen, Beschuldigten, Angeschuldigten, Angeklagten einerseits und Zeugen andererseits erscheint es geboten, die Entscheidung, ob und in welcher Weise gefahndet werden darf, grundsätzlich dem Richter vorzubehalten ; dies gilt nicht bei der öffentlichen Fahndung zum Zwecke der Straf- oder Maßregelvollstreckung gegenüber Erwachsenen.

   Bei Gefahr in Verzug kann eine Eilkompetenz der Staatsanwaltschaft vorgesehen werden; dies gilt nicht bei der öffentlichen Fahndung nach Zeugen. In diesem Falle ist unverzüglich die richterliche Bestätigung der Maßnahme einzuholen.

   Die öffentliche Fahndung nach Beschuldigten setzt voraus, daß ein Haftbefehl oder Unterbringungsbefehl vorliegt, bzw. dessen Erlaß nicht ohne Gefährdung des Fahndungserfolges abgewartet werden kann.

3. Eine besonders eingehende Prüfung der Verhältnismäßigkeit hat bei der Fahndung nach Zeugen stattzufinden.

   Eine öffentliche Fahndung nach Zeugen darf nach Art und Umfang nicht außer Verhältnis zur Bedeutung der Zeugenaussage für die Aufklärung der Straftat stehen. Hat ein Zeuge bei früherer Vernehmung bereits von seinem gesetzlichen Zeugnis- oder Auskunftsverweigerungsrecht Gebrauch gemacht, so soll von Maßnahmen der öffentlichen Fahndung abgesehen werden.

4. In Unterbringungssachen darf eine öffentliche Fahndung mit Rücksicht auf den Grundsatz der Verhältnismäßigkeit nur unter angemessener Berücksichtigung des gesetzlichen Zwecks der freiheitsentziehenden Maßregel, insbesondere der Therapieaussichten und des Schutzes der Allgemeinheit angeordnet werden.

5. Die öffentliche Fahndung zur Sicherung der Strafvollstreckung sollte zur Voraussetzung haben, daß

   - eine Verurteilung wegen einer Straftat von erheblicher Bedeutung vorliegt und

   - der Verurteilte, der sich der Strafvollstreckung entzieht, (noch) eine Restfreiheitsstrafe von in der Regel mindestens einem Jahr zu verbüßen hat, oder ein besonderes öffentliches Interesse, etwa tatsächliche Anhaltspunkte für die Begehung weiterer Straftaten von erheblicher Bedeutung, an der alsbaldigen Ergreifung des Verurteilten besteht.

6. Besondere Zurückhaltung ist bei internationaler öffentlicher Fahndung geboten. Dies gilt sowohl für Ersuchen deutscher Stellen um Fahndung im Ausland als auch für Fahndung auf Ersuchen ausländischer Stellen im Inland.

7. Öffentliche Fahndung unter Beteiligung der Medien sollte in den Katalog anderer entschädigungspflichtiger Strafverfolgungsmaßnahmen des § 2 Abs. 2 StrEG aufgenommen werden.

   Durch Ergänzung des § 7 StrEG sollte in solchen Fällen auch der immaterielle Schaden als entschädigungspflichtig anerkannt werden.

   Der Gesetzgeber sollte vorsehen, daß auf Antrag des Betroffenen die Entscheidung über

die Entschädigungspflicht öffentlich bekanntzumachen ist.

4.1 Die vier Stufen des Verfahrens

Das Verfahren besteht aus vier Stufen, die in der folgenden Abbildung dargestellt sind:

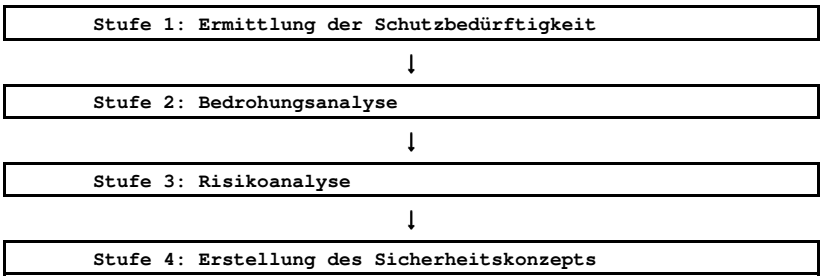

Abbildung 3: Die Vier Stufen des Verfahrens

In der **Stufe 1** wird aus der Sicht der Nutzer des IT-Systems ausgewählt und abgegrenzt, was Gegenstand der weiteren Untersuchungen ist. Dazu wird festgelegt, welche IT-Anwendungen aufgrund ihres Wertes schutzbedürftig sind.

In der **Stufe 2** werden alle vorstellbaren Bedrohungen ermittelt, die den in Stufe 1 ausgewählten IT-Einsatz gefährden können. Dabei sind die Schwachstellen des IT-Systems zu untersuchen.

In der **Stufe 3** wird bewertet, wie schädlich sich die Bedrohungen auf den IT-Einsatz auswirken können, das heißt, welche Risiken aktuell bestehen. Zusätzlich wird festgelegt, welche Risiken tragbar und welche untragbar sind.

In der **Stufe 4** werden Maßnahmen gegen die Bedrohungen ausgewählt und ihre Wirkungen beurteilt. Dabei muß entschieden werden, welche Maßnahmen angemessen sind und welches Restrisiko tragbar ist.

Zum **Abschluß jeder Stufe** muß das verantwortliche Management über die Ergebnisse informiert werden und die Ergebnisse mittragen. Insbesondere muß das IT-Sicherheitskonzept nach der Stufe 4 abschließend akzeptiert werden, bevor es realisiert wird.

Beschäftigtenverzeichnis der Dienststelle

Tel.: 033203/356-0
Fax: 033203/356-49

Name, Vorname	Stellenzeichen	App.	Name, Vorname	Stellenzeichen	App.
Berndt, Gabriela	- Be -	12	Müller, Veikko	- Mü -	32
Dr. sc. Bleyl, Dietmar	- LfD -	10	Objartel, Christine	- Obj -	10
Bultmann, Martin	- Bu -	21	Peschenz, Gabriele	- Pe -	22
Burghardt, Susann	- Bg -	44	Schraut, Lena	- Schr -	41
Franzen, Marie-Luise	- Fr -	20	Thiele, Udo	- Th -	33
Groß, Manfred	- Gr -	40	Urban, Kurt	- Ur -	30
Kern, Christel	- Ke -	43	Weber, Marion	- We -	44
Leunig, Ursel	- Leu -	42	Wiener, Ulrich	- Wie -	31

Aufgabenzuweisungen und Zuständigkeiten (in Klammern: Verantwortliche für technisch-organisatorische Angelegenheiten)

Herr Dr. Bleyl — Landesbeauftragter für den Datenschutz

Frau Berndt — Schreibarbeiten, Teilaufgaben der automatisierten Vorgangsverwaltung, Registrierung von Meldungen gem. § 6 Abs. 4 SchuVVO, Bearbeitung von Anforderungen von Informationsmaterial

Herr Bultmann — Geschäftsbereiche Datenschutzrecht: MdF (Herr Thiele), MWMT (Herr Wiener), MSWV (Herr Thiele - Stadtentwicklung und Wohnen; Herr Urban - Verkehr)

Frau Burghardt — Geschäftsbereiche Datenschutzrecht: MELF (Herr Wiener), MUNR (Herr Müller)

Frau Franzen — Geschäftsbereiche Datenschutzrecht: Grundsatzfragen des Datenschutzrechts, Internationales Datenschutzrecht, MdJBE (Herr Urban), MI, insbesondere Verfassung, Kommunalrecht, Körperschaften/Stiftungen/Anstalten des öffentlichen Rechts, LRH (Herr Wiener);
Koordinierung rechtlicher Aufgaben

Herr Groß — Geschäftsbereiche Datenschutzrecht: MI, insbesondere Personal, Melderecht, Personenstandsrecht, Wahlen (Herr Wiener), Bürgerberatung, Öffentlichkeitsarbeit;
Koordinierung interner Personal- und Verwaltungsaufgaben;
Beauftragter des Haushalts - BdH -

Frau Kern — Schreibarbeiten, Bibliotheksarbeit, Literaturbeschaffung, Mailboxkommunikation mit BfD und LfD, Bearbeitung von Anforderungen von Informationsmaterial;
Gleichstellungsbeauftragte der Behörde

Frau Leunig — Büroleitungsaufgaben, Haushaltsangelegenheiten, Dienstreiseangelegenheiten, Materialbeschaffung

Herr Müller — Geschäftsbereiche Technik: insbesondere UNIX-Systeme, Vernetzte Systeme, Online-Dienste, Kommunikationsnetze, Sicherheitsprodukte, Kartentechnologien, Magnetische und optische Datenträger

Frau Objartel — Vorzimmer des Landesbeauftragten für den Datenschutz, Sekretariat

Frau Peschenz — Geschäftsbereiche Datenschutzrecht: MBJS (Herr Thiele), MWFK (Herr Müller)

Frau Schraut — Geschäftsbereiche Datenschutzrecht: MI, insbesondere Polizei, Verfassungsschutz (Herr Urban), Ordnungswidrigkeiten (Herr Thiele), Ausländer (Herr Wiener), Bürgerberatung, Pressearbeit

Herr Thiele — Geschäftsbereiche Technik: insbesondere Dateienregister, Gebäudesicherung, Datenträgerentsorgung, Isolierte und vernetzte PC, Systemverwalter der betriebsinternen DV-Anlage

Herr Urban — Führung der Geschäfte bei Abwesenheit des LfD gem. § 22 Bbg DSG;
Geschäftsbereich Medien/Telekommunikation
Technik: insbesondere technisch-organisatorische Grundsatzfragen, Landesverwaltungsnetz, Geographische Informationssysteme AS400, ISDN;
Koordinierung technischer Aufgaben

Frau Weber — Geschäftsbereiche Datenschutzrecht: MASGF (Herr Müller)

Herr Wiener — Geschäftsbereich Statistik
Technik: insbesondere Großrechner, Datenbanksysteme, Laptops, Organisations-/Dienstanweisungen, kryptographische Verfahren;
Personalrat der Behörde

Stichwortverzeichnis:

(Berichtszeitraum der Jahresberichte: I = März bis Dezember 1992; II = bis März 1994; III = bis März 1995; IV = bis März 1996 /Seitenangabe)

Abkürzungsverzeichnis

1. SKWPG	=	Ersten Gesetzes zur Umsetzung des Spar-, Konsolidierungs- und Wachstumsprogramms
1. SRG	=	Erstes Schulreformgesetz für das Land Brandenburg
2. MeldDÜÄV	=	Zweite Verordnung zur Änderung der Verordnung über regelmäßige Datenübermittlungen der Meldebehörden
2. SGBÄndG	=	2. Gesetz zur Änderung des Sozialgesetzbuches
a. F.	=	alte Fassung
ABl.	=	Amtsblatt
Abs.	=	Absatz
Abschn.	=	Abschnitt
ADV	=	Automatische Datenverarbeitung
AFIS	=	Automatisierte Fingerabdruck-Identfizierungssystem
AfNS	=	Amt für Nationale Sicherheit
AG	=	Ausführungsgesetz
AGE	=	Autobahngebührenerfassungssystem
AgrStaG-DVO	=	Verordnung über die Durchführung des Agrarstatistikgesetzes
AGTierSGBbg	=	Gesetz zur Ausführung des Tierseuchengesetzes
ALK	=	Automatisierte Liegenschaftskarte
AMG	=	Arzneimittelgesetz
Änd.	=	Änderung
Anl.	=	Anlage
AO	=	Abgabenordnung
AO-GS	=	Ausbildungsordnung der Grundschule im Land Brandenburg
AOK	=	Allgemeine Ortskrankenkasse
APOmJD	=	Ausbildungs- und Prüfungsordnung mittlerer Justizdienst
Art.	=	Artikel
Ärzte-ZV	=	Zulassungsordnung für Vertragsärzte
ATKIS	=	Amtliches topographisch-kartographisches Informationssystem
Aufl.	=	Auflage
AufnV	=	Verordnung über die Aufnahme in weiterführende Schulen des Landes Brandenburg
AuslG	=	Ausländergesetz
AV	=	Allgemeine Verfügung
AVA	=	Automatisierten Vorgangstagebuchs
AWMF	=	Arbeitsgemeinschaft der Wissenschaftlichen Medizinischen Fachgesellschaften
AZV	=	Abfallzweckverband
BAföG	=	Bundesausbildungsförderungsgesetz
BauGB	=	Baugesetzbuch
Bbg DSG	=	Brandenburgisches Datenschutzgesetz
Bbg.	=	Brandenburgisch(es)
BbgArchivG	=	Brandenburgisches Archivgesetz
BbgBO	=	Brandenburgische Bauordnung
BbgGDG	=	Brandenburgisches Gesundheitsdienstgesetz
BbgKita-Gesetz	=	Brandenburgisches Kindertagesstättengesetz
BbgMeldeG	=	Brandenburgisches Meldegesetz
BbgPAuswG	=	Brandenburgischen Personalausweisgesetz
BbgPolG	=	Brandenburgisches Polizeigesetz
BbgPsychKG	=	Brandenburgisches Psychisch-Kranken-Gesetz
BbgRAVG	=	Brandenburgisches Rechtsanwaltsversorgungsgesetz
BbgSchulG	=	Brandenburgisches Schulgesetz
BbgVerf	=	Brandenburgische Verfassung
BbgVerfSchG	=	Brandenburgisches Verfassungsschutzgesetz
BDSG	=	Bundesdatenschutzgesetz
BdVP	=	Bezirksdirektionen der Volkspolizei
BGB	=	Bürgerliches Gesetzbuch
BGBl.	=	Bundesgesetzblatt
BKA	=	Bundeskriminalamt
BKAG	=	Bundeskriminalamtgesetz
BKAG-E	=	Bundeskriminalamtgesetz-Entwurf
BKGG	=	Bundeskindergeldgesetz
BlnDSG	=	Berliner Datenschutzgesetz
BLVS	=	Landesamt für Verkehr und Straßenbau Brandenburg
BND	=	Bundesnachrichtendienst
BR-Drs.	=	Bundesrats-Drucksache
BSI	=	Bundesamt für Sicherheit in der Informationstechnik
BSS	=	Basisstationen
BSeuchenG	=	Bundesseuchengesetz
BStatG	=	Bundesstatistikgesetz
BStU	=	Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR
BT-Drs	=	Bundestags-Drucksache
Buchst.	=	Buchstabe
Bundes-SISY	=	bundesweites staatanwaltschaftliches Informationssystem
BVerfGE	=	Bundesverfassungsgerichtsentscheidung
BZR	=	Bundeszentralregister
BZRG	=	Bundeszentralregistergesetz
bzw.	=	beziehungsweise

ca.	=	circa
CD-ROM	=	Compact Disc Read Only Memory
CERT	=	Computer Emergency Response Team
CSIS	=	Centrales Schengener Informationssystem
DAV	=	Verwaltungsvorschrift über die Errichtung und Benutzung dienstlicher Telekommunikationsanlagen für die Verwaltung des Landes Brandenburg
DDR-GBl.	=	DDR-Gesetzblatt
DES	=	Data Encryption Standard
d. h.	=	das heißt
DIN	=	Deutsches Institut für Normung
DORA	=	Dialogorientertes Recherche- und Auskunftssystem
DV	=	Datenverarbeitung
DVO	=	Durchführungsverordnung
e. V.	=	eingetragener Verein
ed-Behandlung	=	erkennungsdienstliche Behandlung
EDU	=	European Drug Unit
EG	=	Europäische Gemeinschaft
EUROPOL	=	Europäisches Polizeiamt
EuWG	=	Europawahlgesetz
FDGB	=	Freier Deutscher Gewerkschaftsbund
ff.	=	folgende
FrauFöV	=	Frauenförderungsverordnung
GastVO	=	Verordnung zur Ausführung des Gaststättengesetzes
geänd.	=	geändert
GEK	=	Kohortenstudie "Gesundheit, Ernährung, Krebs"
gem.	=	gemäß
GewAnzVwV	=	Allgemeine Verwaltungsvorschrift zur Durchführung der Gewerbeordnung
GewO	=	Gewerbeordnung
GEZ	=	Gebühreneinzugszentrale
GG	=	Grundgesetz
GGG	=	Gesetz über die gesellschaftlichen Gerichte der DDR
GIS	=	Geographische Informationssysteme
GKG	=	Gesetz über kommunale Gemeinschaftsarbeit im Land Brandenburg
GMBl.	=	Gemeinsames Ministerialblatt
GO	=	Gemeindeordnung
GVBl.	=	Gesetz- und Verordnungsblatt
GWG	=	Geldwäschegesetz
G 10	=	Gesetz zu Artikel 10 Grundgesetz
G 10 AG Bbg	=	Gesetz zur Ausführung des Gesetzes zu Art. 10 Grundgesetz im Land Brandenburg
HebBOBbg	=	Berufsordnung für Hebammen und Entbindungspfleger im Land Brandenburg
HeilBerG	=	Heilberufsgesetz
hrsg.	=	herausgegeben
i. d. Fassung	=	in der Fassung
IHK	=	Industrie- und Handelskammern
IHK-G	=	IHK-Gesetz
INPOL	=	Informationssytem der Polizei
InVeKoS	=	Integriertes Verwaltungs- und Kontrollsystem
ISO	=	International Organization for Standardization
i. S. v.	=	im Sinne von
ISVB	=	Informationssystem für Verbrechensbekämpfung Berlin
i. V. m.	=	in Verbindung mit
ISDN	=	Integrated Services Digital Network (dienste-integrierendes Digitalnetz)
JMBl.	=	Justizministerialblatt
JVA	=	Justizvollzugsanstalt
KA	=	Kriminalakte
KAG	=	Kommunalabgabengesetz
KAN-BB	=	Kriminalaktennachweis Land Brandenburg
Kap.	=	Kapitel
KBA	=	Kraftfahrt-Bundesamt
KHDsV	=	Verordnung zum Schutz von Patientendaten im Krankenhaus
KitaBKVO	=	Kindertagesstätten-Betriebskosten Verordnung
KJHG	=	Kinder- und Jugendhilfegesetz
KKO	=	Konfliktkommissionsordnung
KOVVfG	=	Gesetzes über das Verwaltungsverfahren der Kriegsopferversorgung
KRG	=	Krebsregistergesetz
LAG	=	Landesarbeitsgruppe
LAN	=	Local Area Network
LBG	=	Landesbeamtengesetz
LDS	=	Landesamt für Datenverarbeitung und Statistik
LELF	=	Landesamt für Ernährung, Landwirtschaft und Flurneuordnung
LfD	=	Landesbeauftragter für den Datenschutz
LfV	=	Landesamt für Verfassungsschutz
LGG	=	Landesgleichstellungsgesetz
LHO	=	Landeshaushaltsordnung
LKA	=	Landeskriminalamt

LKGBbg = Krankenhausgesetz des Landes Brandenburg
LSPV = Lehrerstellen- und Personalverwaltung
LT-Drs. = Landtags-Drucksache
MAC = Medium Access Control
MASGF = Ministerium für Arbeit, Soziales, Gesundheit und Frauen
MBJS = Ministerium für Bildung, Jugend und Sport
MdF = Ministerium der Finanzen
MdJBE = Ministerium der Justiz und für Bundes- und Europaangelegenheiten
MDK = Medizinischen Dienst der Krankenkassen
MeldDÜÄV = Änderung der Verordnung über regelmäßige Datenübermittlungen der Meldebehörden
MeldDÜV = Verordnung über regelmäßige Datenübermittlungen der Meldebehörden
MELF = Ministerium für Ernährung, Landwirtschaft und Forsten
MESTA = Mehrländer-Staatsanwaltschaft-Automation
MfS = Ministerium für Staatssicherheit
MI = Ministerium des Innern
MiStra = Anordnung über Mitteilungen in Strafsachen
MOD = Magneto-optische Datenträger
MSWV = Ministerium für Stadtentwicklung, Wohnen und Verkehr
MUNR = Ministerium für Umwelt, Naturschutz und Raumordnung
MWFK = Ministerium für Wissenschaft, Forschung und Verkehr
MWMT = Ministeriums für Wirtschaft, Mittelstand und Technologie
NASISTE = Nachrichtensammelstelle
n. F. = neue Fassung
Nr. = Nummer
NSIS = Nationales Schengener Informationssystem
OEG = Opferentschädigungsgesetz
ORB = Ostdeutscher Rundfunk Brandenburg
OWiG = Gesetz über Ordnungswidrigkeiten
PAK = Personenarbeitskartei
PaßG = Paßgesetz
PAuswG = Personalausweisgesetz
pB = Polizeiliche Beobachtung
PC = Personalcomputer
PersVG = Landespersonalvertretungsgesetz
PflRi = Pflegebedürftigkeits-Richtlinien
PHW = personenbezogener Hinweis
PolG = Polizeigesetz
POLIKS BB/BR = Polizeiliches Informations- und Kommunikationssystem Brandenburg/Berlin
PO-Nsch = Nichtschülerprüfungsordnung
PStG = Personenstandsgesetz
RAK = Referatsarbeitskartei
RSA-Algorithmus = nach den Entwicklern Rivest, Shamir und Adleman
RTK = Rasterdaten topographischer Karten
RVO = Reichsversicherungsordnung
S. = Seite
s. = siehe
Sachgeb. = Sachgebiet
SchG = Schiedsstellengesetz
SCHUFA = Schutzgemeinschaft für allgemeine Kreditsicherung GmbH
SchuVVO = Verordnung über das Schuldnerverzeichnis
SchwbG = Schwerbehindertengesetz
SDÜ = Schengener Durchführungsübereinkommen
SGB = Sozialgesetzbuch
SIS = Schengener Informationssystem
SopV = Verordnung über Unterricht und Erziehung für junge Menschen mit sonderpädagogischem Förderbedarf
StA = Staatsanwaltschaft
StGB = Strafgesetzbuch
StPO = Strafprozeßordnung
StUG = Stasi-Unterlagen-Gesetz
StVG = Straßenverkehrsgesetz
StVollzG = Strafvollzugsgesetz
StVZO = Straßenverkehrszulassungsordnung
TB = Tätigkeitsbericht
TDSV = Telekom-Datenschutzverordnung
TFH = Technische Fachhochschule Wildau
TierSchG = Tierschutzgesetz
TK = Telekommunikation
TSK = Tierseuchenkasse
u. a. = unter anderem
UAG = Untersuchungsausschußgesetz
UIG = Umweltinformationsgesetz
u. U. = unter Umständen
UWG = Gesetz gegen den unlauteren Wettbewerb
VDMA = Verband Deutscher Maschinen- und Anlagenbau e.V
VersammlG = Versammlungsgesetz

vgl.	=	vergleiche
VGO	=	Vollzugsgeschäftsordnung
VGPolGBbg	=	Vorschaltgesetz zum Polizeigesetz des Landes Brandenburg
VPKÄ	=	Volkspolizeikreisämter
VV	=	Verwaltungsvorschrift
VV-Hauunt	=	Verwaltungsvorschriften über die Durchführung von Hausunterricht
VV-WissU	=	Verwaltungsvorschrift über wissenschaftliche Untersuchungen an Schulen
VwGO	=	Verwaltungsgerichtsordnung
VwVfGBbg	=	Verwaltungsverfahrensgesetz
VZR	=	Verkehrszentralregister
WildÜV	=	Wildhandelsüberwachungsverordnung
WoBelegG	=	Gesetz über die Gewährleistung von Belegungsrechten im kommunalen und genossenschaftlichen Wohnungswesen
WoBindG	=	Wohnungsbindungsgesetz
WoGG	=	Wohngeldgesetz
WoGSoG	=	Wohngeldsondergesetz
WORM	=	Write Once Read Many
WoStatG	=	Wohnungsstatistikgesetz
WWW	=	World Wide Web
ZBB	=	Zentrale Bezügestelle des Landes Brandenburg
Ziff.	=	Ziffer
ZPO	=	Zivilprozeßordnung
zul.	=	zuletzt
z. Z.	=	zur Zeit