LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 3/1358**
3. Wahlperiode **16.06.2000**

UNTERRICHTUNG

durch die Landesregierung

Stellungnahme zum Vierten Tätigkeitsbericht des Landesbeauftragten für den Datenschutz gemäß § 29 Absatz 1 des Landesdatenschutzgesetzes von Mecklenburg-Vorpommern (DSG MV)

Zugeleitet mit Schreiben des Chefs der Staatskanzlei vom 15. Juni 2000; federführend ist das Innenministerium.

Stellungnahme der Landesregierung

zum

Vierten Tätigkeitsbericht des Landesbeauftragten

für den Datenschutz

Mecklenburg-Vorpommern

für die Zeit vom 01. Januar 1998 bis 31. Dezember 1999

Inhaltsverzeichnis

Seite

1. Einleitung

Der Vierte Tätigkeitsbericht des Landesbeauftragten für den Datenschutz bezieht sich auf die Zeit vom 1. Januar 1998 bis 31. Dezember 1999. Der Landesbeauftragte gibt darin einen exemplarischen Überblick über die im Berichtszeitraum von ihm geleistete Arbeit. Entsprechend seinem gesetzlichen Auftrag [§ 29 des Landesdatenschutzgesetzes von Mecklenburg-Vorpommern (DSG MV)] erstreckte sich diese von der Kontrolle und der Beratung in Einzelfällen über die kritische Begleitung von Bundes- und Landesgesetzen bis hin zu datenschutzrechtlichen Stellungnahmen im Zusammenhang mit neuen Entwicklungen der Technik und der Datensicherheit. Inhaltliche Schwerpunktthemen des Berichts sind neben der Darstellung von Einzelfällen, in denen es nach Auffassung des Landesbeauftragten zu Datenschutzverstößen durch die öffentliche Verwaltung gekommen ist, die Dringlichkeit der Novellierung des Landesdatenschutzgesetzes sowie die Datenschutzbelange neuer Techniken und Verfahren.

Im Hinblick auf die Novellierung des Landesdatenschutzgesetzes teilt die Landesregierung die Auffassung des Landesbeauftragten, dass eine den Vorgaben der EG-Datenschutzrichtlinie entsprechende Novellierung so bald wie möglich verabschiedet werden sollte. Die Dringlichkeit ergibt sich für die Landesregierung vor allem daraus, dass die Rechtslage im Datenschutz durch die mit Ablauf der Umsetzungsfrist am 24. Oktober 1998 eingetretene teilweise Direktwirkung der EG-Datenschutzrichtlinie außerordentlich unübersichtlich geworden ist. Seitdem ist es dem Bürger - und manchmal auch den Fachleuten - nur mit Schwierigkeiten möglich, seine konkreten Datenschutzrechte und -pflichten zu beurteilen. Die Landesregierung betrachtet die Novellierung des Landesdatenschutzgesetzes daher als ein vorrangiges Ziel. Zur Beschleunigung des Verfahrens hat sie den Landesbeauftragten von Anfang an in die Arbeiten einbezogen. Der erste Gesetzentwurf, der durch die Zusammenarbeit entstand, war im Rahmen der Ressortanhörung allerdings massivster Kritik ausgesetzt. Die Thematik wird unter 2.1 nochmals aufgegriffen.

Im Zusammenhang mit der Darstellung technischer und rechtlicher Aspekte neuer Technologien und Verfahren (z. B. DNA-Analyse, Lauschangriffe, elektronisches Grundbuch, Schleierfahndung, Asylcard, elektronische Steuererklärung, Chipkarte als Studentenausweis, Internetnutzung, Videoüberwachung) weist der Bericht auf die vielfältigen Gefahren für das Persönlichkeitsrecht hin, die sich aus ihrem Einsatz ergeben können. Insbesondere wird auf die Gefahr von Datenspuren und die daraus entstehende Gefahr des Missbrauchs und der Zusammenführung von Einzelinformationen zu komplexen Persönlichkeitsprofilen hingewiesen. Soweit sich der Bericht für die Beherrschbarkeit dieser Technologien und Verfahren durch größtmögliche Datenvermeidung, Anonymisierung, Pseudonymisierung, datenschutzfreundliche Hard- und Softwareprodukte sowie kryptographische Verfahren einsetzt, unterstreicht die Landesregierung die Bedeutung dieser Strategien für einen zeitgerechten und modernen Datenschutz.

Zu dem am 21. Oktober 1999 ergangenen Urteil des Landesverfassungsgerichts Mecklenburg-Vorpommern über die Verfassungsbeschwerde gegen § 29 Absatz 1 Satz 2 Nr. 5 des Sicherheits- und Ordnungsgesetzes (SOG M-V) (sog. Schleierfahndung) führen der Tätigkeitsbericht sowie eine Presseerklärung des Landesbeauftragten aus, das Gericht habe die verdachts- und ereignisunabhängigen Polizeikontrollen „im Wesentlichen für verfassungswidrig“ erklärt. Diese Darstellung entspricht nicht den Tatsachen. Vielmehr hat das Gericht das Konzept der Schleierfahndung, das auch in anderen Landespolizeigesetzen enthalten ist (sc. in Bayern, Baden-Württemberg, Berlin, Brandenburg, Niedersachsen, Sachsen, Thüringen), nicht beanstandet und dem Gesetzgeber ausdrücklich die Möglichkeit zugestanden, auch neue Wege der Verbrechensbekämpfung zu erproben. Lediglich die konkrete gesetzliche Ausgestaltung ist zum Teil auf gerichtliche Bedenken gestoßen, wie zum Beispiel die im Gesetz enthaltene Erlaubnis, Identitätsfeststellungen auf Durchgangsstraßen auch zur vorbeugenden Bekämpfung grenzüberschreitender Kleinkriminalität durchzuführen oder das Fehlen von sogenannten Eingriffsschwellen für Folgeeingriffe (vgl. LVerfG M-V vom 21.10.1999, NordÖR 99, 504 ff.).

Weshalb der Landesdatenschutzbeauftragte zu derart interpretierenden Darstellungen neigt, ist nicht nachvollziehbar. Diese Problematik zeigt sich auch bei zwei weiteren Punkten: Im Zusammenhang mit der Novellierung des Landesdatenschutzgesetzes heißt es in der Einleitung des Tätigkeitsberichtes, wegen der unterlassenen Umsetzung der Datenschutzrichtlinie sei inzwischen ein Verfahren vor dem Europäischen Gerichtshof eingeleitet worden. Gegenstand dieses Verfahrens sei unter anderem das Datenschutzrecht in den einzelnen Bundesländern, also auch die Situation in Mecklenburg-Vorpommern. Ein mögliches Urteil könne sein, dass Deutschland - und damit der Steuerzahler - für jeden Tag der Nichtumsetzung der Richtlinie „viel Geld“ an die Europäische Gemeinschaft zahlen müsse. Da auch der Bund sowie 12 Bundesländer die Richtlinie bisher nicht umgesetzt haben, erscheint die vom Landesbeauftragten nahegelegte Kausalitätsbeziehung zwischen der Nichtumsetzung in Mecklenburg-Vorpommern und einer möglichen Verurteilung der Bundesrepublik Deutschland überzeichnet. Auch in Frankreich, Irland, Luxemburg und den Niederlanden ist eine Richtlinienumsetzung bisher nicht gelungen. In zwei Presseerklärungen wird in unmittelbarer Nähe zur Nichtumsetzung der EG-Datenschutzrichtlinie und zur Verfassungsbeschwerde über die Schleierfahndung von der Umfrage eines Meinungsforschungsinstituts berichtet, wonach 69 % der Bürger im Lande mit dem Datenschutz unzufrieden seien. Eine Quelle für die Meinungsumfrage wird nicht genannt. Dadurch wird der Eindruck erweckt, es lägen wissenschaftlich fundierte Nachweise dafür vor, dass der Landesgesetzgeber nicht in ausreichendem Maße für den Schutz der personenbezogenen Daten seiner Bürger sorgt. In Wahrheit steht die zitierte Umfrage in keinem Zusammenhang mit dem Landesdatenschutz. Vielmehr handelt es sich bei ihr um eine vom Freizeit-Forschungsinstitut der British American Tobacco (Germany) GmbH vorgelegte Studie von Prof. Dr. Horst Opaschowski mit dem Titel „Der gläserne Konsument? Multimedia und Datenschutz“, die den bundesweiten Datenschutz im Multimediabereich als Verbraucherschutzproblem thematisiert. Im Hinblick auf die ermittelten Umfrageergebnisse hebt die Studie zudem ausdrücklich hervor: „Der subjektive Eindruck der Bevölkerung muss nicht mit der Realität übereinstimmen“ (S. 21).

In zumindest zwei Fällen sind Ministerien vom Landesbeauftragten aufgefordert worden, eine bereits gegenüber dem Bund geäußerte datenschutzrechtliche Bewertung einer Frage im Zusammenhang mit dem Bundesdatenschutzgesetz zurückzunehmen und „öffentlich zu widerrufen“, weil der Landesbeauftragte sich nicht in der Lage sah, die rechtliche Bewertung zu teilen. Das schriftliche Widerrufsansinnen wurde allen Bundes- und Landesdatenschutzbeauftragten zur Kenntnisnahme zugeleitet. Diese Form der „Datenschutzkontrolle“ wird von der Landesregierung zurückgewiesen.

Im Hinblick auf die Beachtung des Datenschutzes in der Praxis führt der Bericht zahlreiche Einzelfälle an, in denen nach Auffassung des Landesbeauftragten Datenverstöße festgestellt wurden. Nicht in jedem dieser Fälle kann dem Bericht gefolgt werden. Darüber hinaus schließen die Darstellungen des Berichtes in vielen Fällen mit der Feststellung, dass den Empfehlungen des Landesbeauftragten gefolgt wurde oder durch eine Dienstanweisung, Formulargestaltung, zukünftige Vorgehensweise usw. gefolgt werden wird. In diesen Fällen hat die Verwaltung ihre zustimmende Haltung gegenüber den Hinweisen des Landesbeauftragten bereits zum Ausdruck gebracht. Ferner beziehen sich einige dargestellte Fälle auf Vorhaben oder Verfahren, die im öffentlichen Bereich des Landes Mecklenburg-Vorpommern bisher nicht eingesetzt werden (z. B. 3.7 „Volkszählung 2004 - 2006“, 3.16.5 „Datawarehouse“, 3.16.11 „Kfz-Zulassung via Internet“), auf Vorschläge zu Gesetzgebungsvorhaben in Bundes- oder EG-Zuständigkeit (z. B. 3.1.1 „Täter-Opfer-Ausgleich“, 3.1.4 „Entwurf eines Untersuchungshaftvollzugsgesetzes“, 3.8.1 „Telekommunikations-Datenschutzverordnung“, 3.9.5 „Kein Konto ohne Ausweiskopie?“, 3.10.1 „Gesundheitsreform (GKV 2000) - neuer Ansatz für den Datenschutz“), auf rechtliche Einzelberatungen für Bürger und Abgeordnete, ohne dass der öffentlichen Verwaltung in diesem Zusammenhang ein Datenschutzverstoß zur Last fällt (z. B. 3.10.4 „Was das BAföG-Amt dem Antragsteller mitteilen darf“, 3.10.6 „Hausbesuch vom Sozialamt“, 3.11.3 „Krankenhaus informiert Ordnungsamt über fahruntüchtigen Patienten“, 3.11.5 „Prüfaufträge an den Medizinischen Dienst müssen korrekt sein“) oder auf Informationen über neue Entwicklungen der Datenverarbeitung und der Datensicherheit sowie die Zusammenarbeit der Datenschutzbeauftragten (3.16.4 „Neues zur Internetnutzung“, 3.16.6 „Prüfkriterien für datenschutzfreundliche Produkte (Common Criteria 2.0)“, 3.16.7 „Wer weiß schon noch, was in seinem Rechner passiert?“, 3.16.8 „Orten von Mobiltelefonen“, 3.16.10 „Orientierungshilfe für den Einsatz von Verzeichnisdiensten“, 3.16.12 „Neue Antragsverfahren für Ausweispapiere und Führerscheine“). In anderen Fällen müssen noch Stellungnahmen oder Gesetzesänderungen abgewartet werden, bevor den Hinweisen des Landesbeauftragten nachgegangen werden könnte (3.1.5 „Parlamentarische Kontrolle von Lauschangriffen“, 3.4.2 „Automatisierte Abrufverfahren in Gemeinden und Ämtern“). Ihre Zustimmung zu den Hinweisen des Landesbeauftragten hat die Landesregierung im Fall 3.4.2 bereits zum Ausdruck gebracht. Im Fall 3.1.5 war sie nicht betroffen.

Die Landesregierung ist deshalb der Auffassung, dass nicht zu jedem der angesprochenen Punkte Stellung genommen werden muss. Gleichwohl hat sie sich bemüht, möglichst viele Punkte aufzugreifen und aus ihrer Sicht zu behandeln. Mit den im Bericht angesprochenen Punkten haben sich die jeweiligen Ressorts selbst auseinandergesetzt.

2. Modernisierung des Datenschutzrechts

2.1 Zu „2.1 Novellierung des Datenschutzgesetzes längst überfällig“, „2.2 Novellierung des Bundesdatenschutzgesetzes“, „2.3 Neue Regelungen für moderne Technik“ und „3.16.9 Videoüberwachung“

Die Landesregierung teilt die Auffassung des Landesbeauftragten, dass eine Novellierung des Landesdatenschutzgesetzes, die die Vorgaben der EG-Datenschutzrichtlinie in Landesrecht umsetzt, erforderlich ist. Zur Beschleunigung des Novellierungsverfahrens hat sie den Landesbeauftragten von Anfang an in die Entwurfsarbeiten einbezogen. Den ihm dabei eröffneten Gestaltungsspielraum hat der Landesbeauftragte auch genutzt. Neben der Mitwirkung an der Umsetzung der EG-Datenschutzrichtlinie setzte er sich insbesondere für eine umfassende Modernisierung des Datenschutzrechtes nach Maßgabe der von den Arbeitskreisen der Datenschutzbeauftragten erzielten Ergebnisse sowie - da es sich um die erste Novellierung des Landesdatenschutzgesetzes handelte - für die Änderung von Vorschriften ein, die weder die Datenschutzrichtlinie noch die Modernisierung des Datenschutzrechts betrafen (z. B. § 2 Abs. 3 des Landesdatenschutzgesetzes von Mecklenburg-Vorpommern, der das sogenannte Rechtsprechungsprivileg enthält). Die Willensbildung der Landesregierung über die Novelle ist noch nicht abgeschlossen. Nach dem im Juni erwarteten Beschluss des Bundeskabinetts über die Novelle des Bundesdatenschutzgesetzes wird die Landesregierung über das Landesgesetz beschließen.

2.2 Zu „2.4 Direktwirkung der europäischen Datenschutzrichtlinie“

Die Landesregierung betrachtet die mit Ablauf der Umsetzungsfrist am 24. Oktober 1998 eingetretene Direktwirkung der EG-Datenschutzrichtlinie und die dadurch entstandene Unübersichtlichkeit und Kompliziertheit des Datenschutzrechts als maßgeblichen Grund für die Dringlichkeit einer Datenschutznovelle. Die Klage der Europäischen Kommission vor dem Europäischen Gerichtshof, die dem Gericht nach Auskunft des Bundesinnenministeriums bisher noch nicht vorliegt, sowie eine mögliche Geldstrafe für die Bundesrepublik Deutschland, zu der keinesfalls - wie im Bericht behauptet - für jeden Tag der Nichtumsetzung seit Ablauf der Umsetzungsfrist verurteilt würde, sondern allenfalls für jeden Tag der Nichtumsetzung ab Rechtskraft des Urteils, sind dagegen von nachrangiger Bedeutung. Angesichts des bundesweiten Umsetzungsstandes (vgl. Einleitung) liegt es nicht allein in der Hand der Landesregierung, die Klage abzuwenden. Um den Bürgern und nachgeordneten Behörden bis zum In-Kraft-Treten eines neuen Landesdatenschutzgesetzes eine Hilfestellung für die komplizierte Rechtslage zu geben, hat das Innenministerium „Hinweise zur unmittelbaren Wirkung der Richtlinie 95/46/EG“ veröffentlicht (AmtsBl. M-V 1999 S. 579) und darin erläutert, welche Bestimmungen der Richtlinie unmittelbar gelten und die entsprechenden Bestimmungen des Landesdatenschutzgesetzes verdrängen. Die Erstellung der Hinweise war mit der Schwierigkeit verbunden, dass über den Umfang der Direktwirkung zwischen Bund und Ländern unterschiedliche Auffassungen bestehen. Die Hinweise des Innenministeriums wurden in Abstimmung mit dem Landesbeauftragten nachträglich in einem Punkt berichtigt (AmtsBl. M-V 1999 S. 1203). Weitere Berichtigungsanregungen hat der Landesbeauftragte nicht geäußert. Die Landesregierung teilt den Standpunkt des Landesbeauftragten, dass das unbefriedigende Nebeneinander von Richtlinie und Landesdatenschutzgesetz durch die Novellierung des Landesdatenschutzgesetzes so bald wie möglich beendet werden muss.

3. Sorgen der Bürger, Einzelfälle, Beratungen, Kontrollen, Stellungnahmen

3.1 Zu „3.1.1 Täter-Opfer-Ausgleich“

Das Gesetz zur strafverfahrensrechtlichen Verankerung des Täter-Opfer-Ausgleichs ist inzwischen in Kraft getreten. Danach können gemäß § 155 b Abs. 1 StPO die Staatsanwaltschaft und das Gericht zum Zweck des Täter-Opfer-Ausgleichs oder der Schadenswiedergutmachung einer von ihnen mit der Durchführung beauftragten Stelle von Amts wegen oder auf deren Antrag die hierfür erforderlichen personenbezogenen Informationen übermitteln bzw. die Akten übersenden, soweit die Erteilung von Auskünften einen unverhältnismäßigen Aufwand erfordern würde. Der Gesetzgeber ist damit der Empfehlung des Landesbeauftragten für den Datenschutz nicht gefolgt. Hierfür hatte er auch gute Gründe. Aus der Tatsache, dass vor In-Kraft-Treten des o. g. Gesetzes in dem im Schlichtungsverfahren befindlichen Verfahren die überwiegende Mehrheit beider Beteiligter zu den ihnen übersandten vorbereiteten Einverständniserklärungen in die Weitergabe der personenbezogenen Daten an die Konfliktberater geschwiegen oder dieses abgelehnt haben, ergibt sich, dass ein wesentliches Hemmnis der Akzeptanz des Täter-Opfer-Ausgleichs durch die Beteiligten in der vom Datenschutzbeauftragten empfohlenen Sachbehandlung gelegen hat.

3.2 Zu „3.1.2 Maßvoller Umgang mit der DNA-Analyse“

Mit dem DNA-Identitätsfeststellungsgesetz vom 7. September 1998 ist eine Bestimmung in die Strafprozessordnung eingestellt worden (§ 81 g), nach der es möglich ist, zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren dem Beschuldigten, der einer Straftat von erheblicher Bedeutung, insbesondere eines Verbrechens oder Vergehens gegen die sexuelle Selbstbestimmung, einer gefährlichen Körperverletzung, eines Diebstahls in besonders schwerem Fall oder einer Erpressung verdächtig ist, Körperzellen zu entnehmen und zur Feststellung des DNA-Identifizierungsmusters molekulargenetisch untersuchen zu lassen. Der Sinn dieser Regelung besteht darin, bei der Tatortanalyse gewonnene DNA-Identifizierungsmuster mit solchen DNA-Identifizierungsmustern abzugleichen, die aus länger zurückliegenden Straftaten stammen, um auf diesem Wege die Straftat aufzuklären bzw. zukünftige Straftaten dieses Täters zu verhindern. Anlass dieser Rechtsänderung waren seinerzeit bundesweit aufsehenerregende Sexualstraftaten zum Nachteil von Kindern.

Nach § 81 a Abs. 2 StPO, auf den § 81 f StPO verweist, bedarf die Entnahme und molekulargenetische Untersuchung der Körperzellen der richterlichen Anordnung. Der Richter hat eine Prognoseentscheidung zu treffen, ob Grund zu der Annahme besteht, dass gegen den Täter künftig erneut Strafverfahren wegen einer der vorgenannten Straftaten zu führen sein werden. Einer richterlichen Anordnung und damit einer Prognoseentscheidung bedarf es allerdings nur, wenn der betreffende Beschuldigte nicht von sich aus bereit ist, Körperzellen zur Verfügung zu stellen und untersuchen zu lassen. Nur in diesem Falle bedarf es eines Beschlusses, der im Verweigerungsfalle mit Zwangsmitteln durchgesetzt werden kann.

Demgegenüber vermag die Auffassung des Landesdatenschutzbeauftragten, der in allen Fällen eine richterliche Anordnung zur Entnahme und Untersuchung des molekulargenetischen Materials fordert, nicht zu überzeugen. Es entspricht allgemeiner Auffassung und wird von niemandem bestritten, dass jeder Bürger, der in der Lage ist, seine Angelegenheiten eigenverantwortlich zu regeln, berechtigt ist, im Rahmen der guten Sitten einem Eingriff in seinen Rechtskreis zuzustimmen. Plastisches Beispiel für die Disponibilität persönlicher Rechtspositionen im Strafverfahrensrecht ist der § 81 a StPO. Dort ist geregelt, dass zur Feststellung von Tatsachen die Entnahme von Blutproben richterlich angeordnet werden darf. Niemand würde etwa bei einem unter Alkoholverdacht stehenden Verkehrsteilnehmer, der sich aus eigenen Stücken zur Blutentnahme bereit erklärt hat, auf den Gedanken kommen, zusätzlich eine richterliche Anordnung einzuholen, da Zweifel an der Zulässigkeit der Einverständniserklärung des Betroffenen bestehen. Warum also ein entsprechendes Einverständnis des Betroffenen in die Entnahme und Untersuchung seines zellkernenthaltenen Materials datenschutzrechtlich unzulässig sein soll, ist nicht ersichtlich; zumal dann nicht, wenn der Betroffene in schriftlicher Form umfassend vorab über die Tragweite seiner Entscheidung aufgeklärt worden ist.

Bis auf die Entscheidung des Landgerichtes Nürnberg-Fürth vom 22. Juli 1999, die im Bericht des Landesdatenschutzbeauftragten zitiert wird, haben alle Gerichte, die sich mit dieser Rechtsfrage zu befassen hatten, die oben dargestellte Rechtsauffassung vertreten [zuletzt Landgericht Berlin vom 5. November 1999 (Az.: 522 Qs 118/99), Landgericht Hamburg vom 17. und 24. November 1999 (Az.: 628 Qs 46/99 und 611 Qs 102/99)].

Neben diesen rechtlichen Gesichtspunkten sprechen auch praktische Überlegungen gegen die Auffassung des Landesbeauftragten für den Datenschutz. Würde man nur solche Daten erheben und in die Datei einstellen, die auf eine richterliche Anordnung zurückzuführen sind, wären empfindliche Lücken im Datenbestand und damit für die öffentliche Sicherheit zu befürchten. Beschuldigte könnten nämlich mit dem Ziel, eine richterliche Anordnung und damit eine Aufnahme in den Datenbestand zu verhindern, ihre Einwilligung erklären; der gleichwohl um einen entsprechenden Beschluss ersuchte Richter würde - jedenfalls in Mecklenburg-Vorpommern und in den meisten anderen Bundesländern - die Anordnung im Hinblick auf die erteilte Einwilligung ablehnen. An der bisher verfolgten Verfahrensweise sollte daher festgehalten werden.

3.3 Zu „3.1.3 Praxis der Telefonüberwachung“

Der Landesbeauftragte für den Datenschutz beklagt, dass die Zahl der Telefonüberwachungen in den letzten Jahren sowohl bundesweit als auch landesweit sprunghaft angestiegen ist. Soweit der Bericht auf das Forschungsvorhaben zum Thema „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, 100 b StPO“ zur Untersuchung der Ursachen dieses Trends verweist, ist Folgendes von Belang:

Das BMJ hat mit Schreiben vom 20. Juli 1999 über eine Ausschreibung eines rechtstatsächlichen Forschungsvorhabens informiert. Ziel dieses Forschungsvorhabens ist es, gesicherte empirische Erkenntnisse zur Rechtswirklichkeit der Ermittlungsmaßnahme der Telefonüberwachung im Hinblick auf die gesetzlichen Regelungen zum Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes in einer Wohnung zu benennen.

Der Staatssekretär im BMJ Dr. Geiger kündigte an, dass dieses Forschungsvorhaben durch eine umfangreiche Aktenanalyse bei den Staatsanwaltschaften in den jeweiligen Landesjustizverwaltungen zu speisen wäre. Mecklenburg-Vorpommern hat die Unterstützung dieses Vorhabens zugesagt. Mit dem Forschungsvorhaben wurde das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg beauftragt. Es ist geplant, die Landesjustizverwaltungen in das Forschungsprojekt durch die Einrichtung eines das Vorhaben begleitenden Beirats einzubinden. Die Konstituierung dieses Beirats wurde durch Mecklenburg-Vorpommern begrüßt, eine Mitarbeit in diesem Gremium wurde jedoch mangels personeller Ressourcen als nicht möglich bezeichnet. Der Beirat hat am 16. März 2000 getagt.

Im Protokoll der Sitzung heißt es u. a.: „Nach der Diskussion wurde zusammenfassend festgehalten, dass trotz der allseits anerkannten Bedeutung des Forschungsvorhabens die Vorbehalte gegen eine jetzige Durchführung im Zusammenhang mit der Aktenherausgabe überwiegen. Man kam darin überein, zunächst abzuwarten, bis eine Lösung in Form einer Rechtsgrundlage im Rahmen des StVÄG oder im Zusammenhang mit einer vorgezogenen Gesetzeslösung verwirklicht sei ... Herr Prof. Dr. Albrecht wurde gebeten, weiter schriftlich über den Fortgang der Untersuchung zu informieren und baldmöglichst das überarbeitete Forschungsdesign und den überarbeiteten Fragebogen den Beiratsmitgliedern zu übersenden.“

Soweit der Bericht des Landesbeauftragten für den Datenschutz über die Kontrolle stichprobenartig ausgewählter Akten bei der Staatsanwaltschaft Schwerin berichtet (S. 19 f.), wird ausgeführt, dass die Staatsanwaltschaft Schwerin die gegebenen Empfehlungen unverzüglich umgesetzt hat. Ein Eingehen auf die festgestellten Mängel erscheint daher entbehrlich.

3.4 Zu „3.1.4 Entwurf eines Untersuchungshaftvollzugsgesetzes“

Die von Seiten Mecklenburg-Vorpommerns in seinem Stimmverhalten im Bundesrat vertretene Auffassung stimmt weitgehend mit der des Landesbeauftragten für den Datenschutz überein. Ob ihr allerdings der Bundesgesetzgeber folgen wird, bleibt abzuwarten. Die Gegenäußerung der Bundesregierung zu der Stellungnahme des Bundesrates steht noch aus.

3.5 Zu „3.1.6 Welche Daten müssen bei Sparbuchverlust offenbart werden?“

Im Tätigkeitsbericht des Datenschutzbeauftragten wird nicht hinreichend genug zwischen einem von der Sparkasse selbst durchgeführten und einem gerichtlichen Aufgebotsverfahren zur Kraftloserklärung eines Sparkassenbuchs unterschieden.

Nach § 2 der Sparkassenverordnung für Mecklenburg-Vorpommern kann ein abhanden gekommenes oder vernichtetes Sparkassenbuch durch den Vorstand der Sparkasse für kraftlos erklärt werden. Dazu kann der Vorstand der Sparkasse auf Antrag des Berechtigten ein Aufgebot erlassen, das im Kassenraum der Hauptstelle der Sparkasse und der kontoführenden Zweigstelle auszuhängen sowie im Bekanntmachungsblatt der Sparkasse zu veröffentlichen ist. In diesem Zusammenhang genügt die Bezeichnung des Sparbuchs als solches und die Angabe der Kontonummer.

Für das gerichtliche Aufgebotsverfahren zum Zweck der Kraftloserklärung einer Urkunde, das daneben ebenfalls gewählt werden kann, gelten die einschlägigen Bestimmungen der Zivilprozessordnung. Als Verfahren im Rahmen der Rechtsprechung unterliegt es nicht der Kontrolle durch den Landesbeauftragten für den Datenschutz. Der inhaltliche Umfang der danach vorgeschriebenen Veröffentlichung hängt von dem aufgebotenen Recht ab. Name und Anschrift des Antragstellers des Verfahrens gehören zweifellos dazu. Im Übrigen hat das Gericht nach seinem Ermessen die Urkunde, deren Entkräftung mit dem Ausschlussurteil erstrebt wird, so genau wie möglich zu bezeichnen. Spezialgesetzliche Bestimmungen in der Prozessordnung gehen den Regelungen des allgemeinen Datenschutzrechts insoweit vor.

3.6 Zu „3.1.7 Wenn der Staatsanwalt zu Hause arbeitet“

Mit dem inzwischen erfolgten Abschluss des Projektes 3000 sind die technischen Voraussetzungen geschaffen worden, um die Musterdienstanweisung für den Datenschutz beim Umgang mit Verfahren und Geräten der Informationstechnik fertig zu stellen. Ein entsprechender Entwurf wird derzeit im Justizministerium erarbeitet. Dieser wird dem Landesbeauftragten für den Datenschutz zu gegebener Zeit zur Stellungnahme übersandt. Damit wird der Anregung des Landesdatenschutzbeauftragten entsprochen.

3.7 Zu „3.1.8 Elektronisches Grundbuch“

Zu den vom Landesbeauftragten für den Datenschutz hervorgehobenen zwei Teilaspekten nimmt das Justizministerium wie folgt Stellung:

Elektronische Unterschrift

Vorgehensweise und Form der Zusammenarbeit sind grundsätzlich zutreffend dargestellt. Der Bericht spart jedoch einige Besonderheiten aus, die zu einem falschen Bild der Projektarbeit führen könnten.

Das Justizministerium war und ist jederzeit offen für die Vorschläge des Landesbeauftragten und externer Dienstleister, hat jedoch gleichzeitig die technischen, organisatorischen und finanziellen Notwendigkeiten der Umsetzung entsprechender Hinweise zu prüfen und mit den fachlichen Anforderungen des jeweiligen Arbeitsbereiches in Einklang zu bringen. Die Einführung einer signaturgesetzkonformen Lösung zur Elektronischen Unterschrift ist nicht erforderlich - auch in anderen Bundesländern wird dies so gesehen und realisiert. Dass eine Anlehnung an die dort (SigG) beschriebenen Technologien notwendig und sinnvoll ist, wurde durch das Justizministerium jederzeit als Arbeitsgrundlage angenommen. Beim elektronischen Grundbuch handelt es sich jedoch um eine langfristige Datenarchivierung, die ausdrücklich nicht Einsatzziel des SigG ist (vgl. hierzu Amtliche Begründung zum Informations- und Kommunikationsdienste-Gesetz, BT-Drucksache 13/7385 vom 09.04.1997, S. 1). Eine personenbezogene Elektronische Unterschrift in einem Grundbuchblatt, welche mit Hilfe eines entsprechenden Zertifikates erzeugt wurde, verliert per Definition (auch des SigG) nach einer gewissen Zeit (3 bis 5 Jahre) ihre Funktion, da das benutzte Zertifikat abgelaufen bzw. die zugrunde liegenden Algorithmen schwach geworden sind.

Daher kann eine derartige Elektronische Unterschrift nach dieser Zeit nicht mehr verwendet werden, um die Unveränderheit und Gültigkeit des Grundbucheintrages nachzuweisen. Es müssen zusätzliche Sicherungsmaßnahmen ergriffen werden, die personenunabhängig und nachhaltig im zentralen Datenbestand des elektronischen Grundbuches die Anforderungen der §§ 126 GBO, 75 GBVfg. abdecken. Der geforderte Personenbezug zum Unterzeichner kann daher durchaus als Name in Klarschrift dem Eintrag hinzugefügt werden.

Das Gesamtpaket aus Eintragungstext und Name in Klarschrift ist dann nachhaltig durch geeignete Maßnahmen datentechnisch zu sichern und gegen Manipulation zu schützen. In diesem Sinne entspricht das Konzept des Justizministeriums aus dem Jahr 1998 mit einer softwaregestützten Signierung über dem Eintragungstext einschließlich Name des Unterzeichners in Klarschrift den gesetzlichen Vorgaben. Die Hinweise zur Absicherung gegen unberechtigten Systemverwalterzugriff wurden aufgenommen und sollen mit Hilfe organisatorischer Maßnahmen umgesetzt werden.

Im Rahmen der Projektarbeit und zusammen mit den anderen Beteiligten hat der Landesbeauftragte für den Datenschutz zu dem jetzt vorliegenden Realisierungskonzept (u. a. Einsatz eines personenbezogenen Zertifikats auf einer Smartcard) fachlich beigetragen.

Auftragsdatenverarbeitung

Die Rechtsauffassung des Justizministeriums hinsichtlich des Betriebs des elektronischen Grundbuchs im Hochsicherheitsrechenzentrum des Datenverarbeitungszentrums Mecklenburg-Vorpommern GmbH ist zutreffend dargestellt. Zutreffend wird auch auf mögliche Risiken hingewiesen, andererseits aber keine den hohen Anforderungen an Verfügbarkeit und Integrität des elektronischen Grundbuch entsprechende, wirtschaftlich vertretbare Alternative aufgezeigt, die auch den datenschutzrechtlichen Erfordernissen genügen würde.

Das derzeit in Abstimmung befindliche DVZ-Gesetz, auf das der Landesbeauftragte in anderem Zusammenhang in seinem Bericht hinweist (S. 106), könnte auch in diesem Bereich Rechtssicherheit schaffen.

3.8 Zu „3.1.9 Schuldnerverzeichnis bald öffentlich?“

In diesem Punkt werden primär die Industrie- und Handelskammern angesprochen. Von Seiten der Landesregierung sind zu diesem Punkt Bemerkungen nicht zu machen.

3.9 Zu „3.1.10 Notare in Mecklenburg-Vorpommern mit Sonderprivilegien“

Zu der der Petition zugrunde liegenden Rechtsfrage des Konkurrenzverhältnisses zwischen der Verschwiegenheitspflicht der Notare und dem Umfang der Kontrollbefugnisse nach dem Datenschutzgesetz in Mecklenburg-Vorpommern vertreten der Landesbeauftragte für den Datenschutz sowie das Justizministerium und die Notarkammer Mecklenburg-Vorpommern unterschiedliche Rechtsauffassungen. Der Landesbeauftragte für den Datenschutz geht von einem uneingeschränkten Vorrang der Kontrollbefugnis gegenüber der Verschwiegenheitspflicht des Notars aus.

Nach Auffassung des Justizministeriums und der Notarkammer ist das Konkurrenzverhältnis bisher in der Rechtsprechung nicht abschließend geklärt und ist im Einzelfall zu bestimmen (vgl. BGH NJW 1991, 558).

Unabhängig hiervon sind Notare öffentliche Stellen im Sinne des § 2 Abs. 1 des Datenschutzgesetzes und unterliegen dessen materiellen Bestimmungen. Die Notarkammer Mecklenburg-Vorpommern hat daher im Einvernehmen mit dem Landesbeauftragten für den Datenschutz ein Pflichtenheft für die Notare erlassen (z. B. zur Führung von Dateibeschreibungen, Geräteverzeichnissen etc.). In diesem Zusammenhang stehen dem Landesbeauftragten für den Datenschutz Kontrollmöglichkeiten zur Verfügung. Im Zuge der turnusgemäßen Geschäftsprüfung der Notare wird die Einhaltung dieser Pflichten zudem durch den für die Dienstaufsicht jeweils zuständigen Präsidenten des Landgerichts sichergestellt.

In der aufgezeigten Einzelsache sieht das Justizministerium weiterhin keinen Handlungsbedarf. Aus Anlass der Petition hat der für die Dienstaufsicht zuständige Präsident des Landgerichts den Sachverhalt geprüft. Nach dem Ergebnis der Prüfung liegt eine schuldhafte Amtspflichtverletzung des Notars im Hinblick auf die gerügte Grundbucheinsicht nicht vor. Auch die Weigerung gegenüber dem Landesbeauftragten für den Datenschutz, die weiterhin erbetene Mitteilung unter Hinweis auf die Verschwiegenheitspflicht zurückzuhalten, beinhaltet weder einen Verstoß gegen notarielle Dienstpflichten noch gegen die Bestimmungen des Datenschutzgesetzes. Die Schweigepflicht erstreckt sich grundsätzlich auf alle Tatsachen und Umstände, die dem Notar in Ausübung seines Amtes bekannt geworden sind. Mit Schreiben vom 16. Juli 1999 war der Landesbeauftragte für den Datenschutz über das Ergebnis der dienstaufsichtsrechtlichen Prüfung in Kenntnis gesetzt worden. Da das Ergebnis dem Petenten hätte mitgeteilt werden können, ist unklar, inwieweit die Petition einer abschließenden Bearbeitung nicht zugeführt werden konnte. Den Interessen des Petenten ist durch die vorbezeichnete dienstaufsichtsrechtliche Prüfung hinreichend Rechnung getragen worden.

3.10 Zu „3.1.11 Staatsanwälte löschen nicht“

Hier nimmt das Justizministerium zu den einzelnen Unterpunkten wie folgt Stellung:

Nutzung von Echtdaten für Testzwecke

Unmittelbar nach dem Kontrollbesuch des Landesbeauftragten für den Datenschutz sind die in der zu Testzwecken bei der Behörde des Generalstaatsanwalts installierten Datenbank des Anwendungssystems ARGUS-StA enthaltenen Daten von Verteidigern entfernt bzw. bis zur Unkenntlichkeit verändert worden.

Anmeldeverfahren

Mit der Neuausstattung der Gerichte und Staatsanwaltschaften mit neuen Computerarbeitsplätzen im Jahre 1999 sind die technischen Voraussetzungen dafür geschaffen worden, dass eine Hinterlegung der Passworte beim Systemadministrator entbehrlich ist. Eine entsprechende Regelung ist mit der Auslieferung der Neugeräte getroffen worden. Sie umfasst auch Vorgaben zur Passwortstruktur (Mindestlänge 6 Zeichen, wobei zumindest eine Zahl oder Sonderzeichen zu verwenden ist). Die Einführung des vorgeschlagenen Single-Sign-On-Verfahrens wird bei der Entwicklung der nächsten Generation der ARGUS-Software zu berücksichtigen sein.

Protokollierung; Löschen und Sperren von Daten; Zugriffs- und Organisationskontrolle

Die Einführung der verbesserten Protokollierung, des Löschens und Sperrens von Daten sowie der Zugriffs- und Organisationskontrolle im Anwendungssystem ARGUS-StA wird auch hier als unerlässlich betrachtet.

Im Ergebnis eines Vergleichs der verschiedenen in den Ländern eingesetzten Systeme mussten jedoch unterschiedliche Formen der Umsetzung dieser Anforderungen festgestellt werden. Auf Initiative des Justizministeriums Mecklenburg-Vorpommern hat die Bund-Länder-Kommission für Datenverarbeitung und Rationalisierung in der Justiz (BLK) deshalb in ihrer 62. Sitzung am 11. und 12.11.1997 eine Arbeitsgruppe, an der auch der Generalstaatsanwalt beteiligt ist, damit beauftragt, eine Bewertung der in der Vorlage der 53. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17. und 18.04.1997 erhobenen „Forderungen zum Einsatz von automatisierten staatsanwaltschaftlichen Informationssystemen“ vorzunehmen. Ziel ist es, aus diesen Forderungen einheitliche Grundsätze für alle eingesetzten Systeme unter Berücksichtigung der Erforderlichkeit der empfohlenen Maßnahmen aus fachlicher Sicht sowie der Realisierbarkeit entsprechender Maßnahmen und deren Aufwand aufzustellen. Zudem sind die Europäische Datenschutzrichtlinie sowie die Entschließung der 56. Konferenz der Datenschutzbeauftragten vom 05. und 06.10.1998 einzubeziehen.

Ein Entwurf des Arbeitsgruppenberichts ist bereits gefertigt. Der Abschlussbericht wird in Kürze der BLK vorgelegt werden. Der Bericht wird die sogenannten Geschäftsstellenautomationssysteme der Staatsanwaltschaften zum Gegenstand haben und datenschutzrechtliche Empfehlungen enthalten, die bei Neuentwicklungen oder im Zuge notwendiger Anpassungen bestehender Verfahren umgesetzt werden sollen.

Es ist vorgesehen, nach einer nochmaligen Beteiligung des Landesbeauftragten für den Datenschutz unverzüglich konkrete Programmieraufträge zur Ergänzung des Anwendungssystems ARGUS-StA auf der Grundlage des Arbeitsgruppenberichts zu erteilen. Der Generalstaatsanwalt ist beauftragt, die inhaltlichen Vorgaben aufzustellen, und hat bereits die entsprechenden vorbereitenden Arbeiten aufgenommen.

Weitere Softwareprodukte

Im Rahmen der Neuausstattung der Gerichte und Staatsanwaltschaften mit Computerarbeitsplätzen wurde aus Gründen der Datensicherheit einheitlich dafür Sorge getragen, dass grundsätzlich auch die mit anderen Standardsoftwareprodukten - insbesondere Textverarbeitung - erstellten Daten auf den Servern gespeichert werden. Schon aus Gründen der Speicherkapazität der Server sind die Systemverwalter gehalten, im Turnus von drei Monaten für eine Löschung von Dateien durch die Anwender zu sorgen.

Dienstanweisungen/Handbücher zum Verfahren ARGUS-StA

Das Anwendungssystem ARGUS-StA ist in den zurückliegenden Jahren im Wesentlichen unverändert geblieben, so dass eine Überarbeitung der entsprechenden Dienstanweisung des Generalstaatsanwalts und der Handbücher nicht veranlasst war. Mit der Einführung der Funktionalitäten zum Betrieb der Zentralen Staatsanwaltschaftlichen Verfahrensregister (ZStV) wird die Dienstanweisung eine Anpassung erfahren. Die Bereitstellung neuer Benutzerhandbücher ist vorgesehen.

3.11 Zu „3.1.12 Mitteilungen über Wahlrechtsausschlüsse nicht korrekt“

Nach § 3 Abs. 2 Nr. 1 LMG haben die Meldebehörden für die Vorbereitung und Durchführung von allgemeinen Wahlen und Abstimmungen die Tatsache zu speichern, dass der Betroffene vom Wahlrecht ausgeschlossen ist (Voraussetzung für die Prüfung vor Eintragungen in das Wählerverzeichnis sowie für Wählbarkeitsbescheinigungen). Mangels korrekter Mitteilungen an die zuständige Meldebehörde gemäß Nummer 12a Abs. 1 MiStra sind die Meldebehörden häufig nicht in der Lage, den Endtermin des Wahlrechtsausschlusses zu ermitteln.

Das Justizministerium ist der Auffassung, dass die Etablierung von sogenannten Folgemitteilungen unter anderem unverhältnismäßig ist, da diese die Justiz übermäßig belasten und die Verwaltungsbehörde im Bedarfsfall ein Führungszeugnis des Betroffenen anfordern kann, aus dem sich die zur Überprüfung des Sachverhalts erforderlichen Informationen entnehmen lassen (vgl. §§ 31, 12 Abs. 1 Nr. 7 Bundeszentralregistergesetz). Es hat deutlich gemacht, dass es Folgemitteilungen für Mecklenburg-Vorpommern nicht als notwendig erachtet.

Die Thematik soll auf der nächsten Sitzung des sogenannten MiStra-Ausschusses im Frühsommer dieses Jahres erörtert werden. Dies ist dem Landesbeauftragten für den Datenschutz inzwischen mitgeteilt worden. Nach der Befassung des Mistra-Ausschusses ist vorgesehen, das abschließende Ergebnis der Prüfung des Justizministeriums dem Landesbeauftragten für den Datenschutz zu übermitteln.

3.12 Zu „3.1.13 Datenschutz bei laufenden Ermittlungsverfahren?“

Zwischen dem Justizministerium und dem Landesbeauftragten für den Datenschutz liegen (bisher) unterschiedliche Auffassungen über die Reichweite der Kontrollrechte des Datenschutzbeauftragten in strafrechtlichen Ermittlungsverfahren vor.

In dem zugrunde liegenden Ausgangsfall hatte sich ein Petent an den Landesbeauftragten gewandt und die Vermutung vorgebracht, dass sein Telefonanschluss im Rahmen eines strafrechtlichen Ermittlungsverfahrens überwacht worden sei bzw. überwacht werde. Daraufhin bat der Beauftragte um Auskunft, ob und ggf. in welchem Zeitraum eine solche Maßnahme stattgefunden habe. Der Datenschutzbeauftragte erhielt zur Antwort, dass in der Vergangenheit - in abgeschlossenen Ermittlungsverfahren - von der Staatsanwaltschaft Telefonabhörmaßnahmen im Falle des Petenten nicht angeordnet worden sind. Zugleich wurde ihm der Hinweis erteilt, dass von der beanspruchten Kontrollkompetenz die Auskunft zu Vorgängen in noch laufenden Ermittlungsverfahren nicht umfasst sein könne.

Der Landesbeauftragte für den Datenschutz hat dieser Rechtsansicht widersprochen und angeführt, dass grundsätzlich gemäß §§ 26, 27 DSG MV von einem Auskunfts- und Akteneinsichtsrecht in strafrechtlichen Ermittlungsverfahren - unabhängig ob beendet oder noch laufend - ausgegangen werden müsse. Eine Einschränkung erfahre dieses Recht allein dahin, dass zwischen dem Kontrollrecht des Landesbeauftragten für den Datenschutz einerseits und der Mitteilung an den Petenten andererseits zu unterscheiden sei, da dem Petenten in Fällen laufender Ermittlungsverfahren über die durch den Datenschutzbeauftragten eingeholten Auskünfte keine Nachricht zu erteilen sei. Grundsätzlich habe der Datenschutzbeauftragte jedoch auch für laufende Verfahren selber zu prüfen, ob die Verfahrensvorschriften zum Schutz des Rechts auf informationelle Selbstbestimmung und des Datenschutzes im Übrigen gewahrt und eingehalten worden seien. Dies folge aus § 2 Abs. 3 1. Halbsatz DSG MV, der ausdrücklich die §§ 26, 27 DSG MV im Bereich der Staatsanwaltschaften für anwendbar erkläre. Insoweit finde sich im Gesetz kein Anhalt dafür, dass die Kontrolle des Datenschutzbeauftragten sich nur auf abgeschlossene Verfahren beziehe.

Das Justizministerium hat diese Rechtsmeinung zur Kenntnis genommen, jedoch keinen Anlass für eine vorschnelle und abschließende Klärung der Streitfrage gesehen, sondern stattdessen darauf verwiesen, dass diese Frage zum Gegenstand einer Behandlung im Zusammenhang mit den laufenden Novellierungsbestrebungen zum Bundes- und Landesdatenschutzgesetz genommen werden solle.

Die von dem Landesbeauftragten für den Datenschutz an dieser Vorgehensweise geübte Kritik, der meint, das Justizministerium habe es versäumt, bei der Bewertung von Sachverhalten das geltende Recht zur Anwendung zu bringen, vermag nicht zu verfangen. Wie der Beauftragte für den Datenschutz in seinem Bericht selbst darstellt, ist ihm auf die zum Fall des Petenten gestellte Anfrage umfassend Auskunft zuteil geworden.

Die - vom Petenten - vermutete Überwachung eines Fernmeldeanschlusses betraf einschlägig nur in der Vergangenheit gegen diesen geführte Ermittlungsvorgänge. In Anerkennung eines insoweit bestehenden Kontrollrechts des Datenschutzbeauftragten erhielt dieser durch das Justizministerium die von ihm erbetenen Informationen.

Hingegen war die weiter aufgeworfene Frage nach einer Kontrollkompetenz auch in laufenden strafrechtlichen Ermittlungsvorgängen - anlassbezogen betrachtet - nicht entscheidungserheblich. Von daher zeigte sich einerseits kein abschließender Klärungsbedarf. Dem Informationsverlangen des Petenten und des Datenschutzbeauftragten konnte auch bei Offenlassen der Streitfrage in Anwendung des geltenden Rechts Genüge getan werden. Andererseits ist die Frage des Datenschutzes im besonders sensiblen Bereich der Strafverfolgung und des auf diesem Gebiet miteinander in Konkordanz zu bringenden Schutzes unterschiedlicher Rechtsgüter von schwieriger und ganz grundsätzlicher Natur. Sie bildet deshalb - zu Recht - neben anderen Fragestellungen den Gegenstand der Diskussion über die anstehende Novellierung von Bundes- und Landesdatenschutzgesetz, wobei bisher weder die Frage eindeutig entschieden ist, ob schon das geltende Recht eine Kontrollkompetenz des Datenschutzbeauftragten im Feld aktueller Strafverfolgungsmaßnahmen gewährt, noch die weitere Frage, ob jedenfalls künftig eine solche Kontrollbefugnis gesetzlich verankert werden soll. Deshalb stellt es keine Verweigerung der Anwendung geltenden Gesetzesrechts dar, wenn der Landesbeauftragte für den Datenschutz durch das Justizministerium auf diesen noch laufenden Diskussionsprozess verwiesen worden ist. Im Gegenteil hätte es der Offenheit für die Aufnahme neuer Argumente in diesem Prozess widersprochen, wenn sich das Justizministerium vorschnell oder ohne Gebot in seiner Auffassung präjudiziert hätte, zumal auch ein darüber unter den Landesjustizverwaltungen in Gang gesetzter Meinungsaustausch noch nicht abgeschlossen ist.

3.13 Zu „3.2.1 INPOL-neu“

Zu den beiden Punkten, die der Landesbeauftragte für den Datenschutz im Hinblick auf die ins Auge gefasste Inkraftsetzung des „INPOL-neu-Systems“ kritisiert, ist Folgendes auszuführen:

Die Absicht, im Kriminalaktennachweis zukünftig die kriminelle „Karriere“ eines Straftäters in INPOL-neu insgesamt abzubilden, ist sowohl rechtlich zulässig als auch aus fachlichem Blickwinkel erforderlich, sobald nur eine Straftat des in Rede stehenden Straftäters die Schwelle des § 2 Abs. 1 Bundeskriminalamtgesetz (BKAG) erreicht und überschreitet.

Aus rechtlichem Blickwinkel ist diese Vorgehensweise unbedenklich, weil der Bundesgesetzgeber für die Zulässigkeit der Speicherung von Daten auf die Gesamtpersönlichkeit des Täters abgestellt hat und nicht nur einen einzelnen, isoliert zu betrachtenden Datensatz als gesetzliche Bedeutungsschwelle zugrunde legen wollte. Darüber hinaus besteht auch ein dringendes fachliches Bedürfnis, vollständige Informationen über einen Straftäter zu erhalten, um bei der Verfolgung von Straftaten länderübergreifender, internationaler oder erheblicher Bedeutung besondere Eigenschaften des Täters, wie Mehrfachtäterschaft, Wiederholungsgefahr oder das Gefährdungspotential der Einsatzkräfte polizeitaktisch rechtzeitig einschätzen zu können.

Zu der Frage, welches Recht bei gemeinsamen INPOL-Verbunddateien des Bundes und der Länder anzuwenden ist, wird die Auffassung vertreten, dass dem Bundeskriminalamtgesetz (§ 11 BKAG) unter Berücksichtigung der Festlegungen in den jeweiligen Errichtungsanordnungen der Vorzug zu geben ist. Der Frage erscheint insbesondere deshalb nur geringe Bedeutung beizukommen, weil datenschutzrechtliche Belange durch die Anwendung von Bundesrecht nicht beeinträchtigt werden dürften, denn der datenschutzrechtliche Standard des Bundeskriminalamtgesetzes ist dem der Landespolizeigesetze ebenbürtig.

3.14 Zu „3.2.2 Verfassungsgericht stoppt Schleierfahndung“

Mit seiner Entscheidung vom 21. Oktober 1999 hat das Landesverfassungsgericht Teile der Bestimmungen des Sicherheits- und Ordnungsgesetzes Mecklenburg-Vorpommern, die die verdachts- und ereignisunabhängige Kontrolle von Personen regeln, für verfassungswidrig erklärt.

Das Urteil bringt jedoch keineswegs das „Aus“ für die verdachts- und ereignisunabhängigen Personenkontrollen (vgl. Einleitung). Es bestätigt vielmehr ihre Zulässigkeit ohne zusätzliche gesetzliche Eingriffsschwellen, sofern die Kontrollmaßnahmen im Grenzgebiet, in den öffentlichen Einrichtungen des internationalen Verkehrs oder im Küstenmeer vorgenommen werden.

Das Urteil verlangt jedoch zusätzliche Gesetzesregelungen und höhere Eingriffsschwellen für alle Durchgangsstraßen außerhalb des Grenzgebiets, für alle über das bloße Anhalten und die Aufforderung sich auszuweisen hinausgehenden Einzelmaßnahmen („Folgeeingriffe“ wie Festhalten, Verbringen zur Dienststelle, erkennungsdienstliche Behandlung, Durchsuchung) sowie für die Verarbeitung und Nutzung der bei diesen Kontrollen erhobenen Daten.

Die Formulierung im Bericht des Landesdatenschutzbeauftragten ist daher missverständlich, wonach das Gericht Zwangsmaßnahmen im Grenzgebiet bis zu einer Tiefe von 30 km, in Einrichtungen des internationalen Verkehrs und im Küstenmeer, die über das Anhalten einer Person und das an sie gerichtete Verlangen, Angaben zur Person zu machen und Ausweispapiere vorzulegen, hinausgehen, eine deutliche Absage erteilt habe. Wie dargelegt ist dem Urteil nur zu entnehmen, dass es für solche weitergehenden Maßnahmen gegenwärtig keine hinreichende gesetzliche Grundlage gibt.

Zur erfolgreichen Bekämpfung grenzüberschreitender sowie Organisierter Kriminalität wird nicht auf das Instrument der verdachts- und ereignisunabhängigen Kontrolle verzichtet. Die Landesregierung beabsichtigt, dem Landtag unter Beachtung der verfassungsrechtlichen Vorgaben ein entsprechendes Änderungsgesetz zum Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern vorzulegen.

3.15 Zu „3.2.3 Polizeiliche Zusammenarbeit mit der Russischen Föderation“

Am 3. Mai 1999 wurde in Moskau das Abkommen zwischen den Regierungen der Bundesrepublik Deutschland und der Russischen Föderation über die Zusammenarbeit bei der Bekämpfung von Straftaten von erheblicher Bedeutung unterzeichnet. Sofern künftig organisierte Strukturen bei der Tatplanung oder -begehung erkennbar werden, sollen die zuständigen Behörden der Vertragstaaten zusammenarbeiten, insbesondere bei der Bekämpfung von Betäubungsmittelkriminalität, Terrorismus, Menschenhandel, Erpressung, Eigentumskriminalität und Geldwäschedelikten.

Artikel 6 des Abkommens enthält dezidierte Bestimmungen zum Umgang mit personenbezogenen Daten. So hat beispielsweise jede Vertragspartei das Recht, Auskunft über die Verwendung der übermittelten Daten bei der anderen Vertragspartei zu erhalten. Darüber hinaus enthält Artikel 6 eine Regelung zur Zweckbindung der Daten, denn der Empfänger ist nur berechtigt, die Daten zu dem im Abkommen bezeichneten Zweck zu nutzen. Schließlich - und das ist besonders wichtig - hat jede Vertragspartei das Recht, die Übermittlung erbetener Daten zu unterlassen, wenn Grund zu der Annahme besteht, dass dadurch gegen den Zweck eines innerstaatlichen Gesetzes verstoßen würde oder schutzwürdige Interessen der betroffenen Personen beeinträchtigt würden.

Mit Blick auf die in der Russischen Föderation vorkommende Korruption und die dort operierenden mafiosen Organisationen sind die Bedenken, die der Landesbeauftragte für den Datenschutz gegenüber diesem Abkommen vorträgt, nicht vollständig von der Hand zu weisen. Auch wenn dem Bundeskriminalamt keine Anhaltspunkte vorliegen, kann sicherlich niemand mit letzter Sicherheit ausschließen, dass übermittelte Daten an kriminelle Organisationen weitergegeben werden.

Wollte man hingegen nur mit solchen Staaten im Polizeibereich zusammenarbeiten, die einen den deutschen Bestimmungen entsprechend hohen Datenschutzstandard aufweisen - bei denen demzufolge jeder auch nur denkbare Missbrauch von Daten ausgeschlossen erscheint -, würde man der globalen Herausforderung der grenzüberschreitenden Kriminalität nicht gerecht werden. Im Zielkonflikt zwischen den Risiken von Informationsübermittlung und den Chancen internationaler polizeilicher Zusammenarbeit muss unter Wahrung eines gemeinsam erreichbaren Höchstmaßes an Datenschutz der zur Bekämpfung des Kriminalitätsgeschehens erforderliche Datenaustausch mit der Russischen Föderation ermöglicht werden.

3.16 Zu „3.2.4 Täterlichtbildsystem“

Das Projekt Täterlichtbildsystem (TLBS) wird nach einer europaweiten Ausschreibung seit dem 15. September 1999 realisiert. Das Täterlichtbildsystem ist ein dv-gestütztes System zur Realisierung von

- Zeugeneinsichtnahmen in Lichtbildvorzeigebestände (Standorte KPI’en u. LKA)
- Wahllichtbildvorlagen (Standorte KPI’en u. LKA)
- Täterübersichten (Standorte KPI’en u. LKA)
- der Erstellung von Phantombildern (Standorte KPI’en u. LKA)

Das System stellt einen erheblichen Fortschritt gegenüber der bisherigen konventionellen Arbeitsweise dar. Es ermöglicht die Aufnahme, die Speicherung und das Vorhalten sowie Vorzeigen von Täterlichtbildern. Da es auch Personendaten und Personenbeschreibungen enthält, werden Recherchen vereinfacht. Mehrfacherfassungen gleicher Daten für die verschiedenen Vordrucke entfallen. Die aufgenommenen Täterlichtbilder können sofort einer Qualitätskontrolle unterzogen werden. Sie stehen nach der Abspeicherung im System unmittelbar (tagaktuell) landesweit zur Verfügung. Zur Erstellung von Wahllichtbildvorlagen und Täterübersichten wird nicht mehr der „lange Weg“ über das Fotolabor benötigt, sie können sofort am Rechner erstellt und ausgedruckt werden. Hierzu stellt das System vielfältige Werkzeuge zur Auswahl der Lichtbilder mittels Recherchen zur Verfügung.

Die Anwendung des Systems soll alle Aktivitäten zur erkennungsdienstlichen Behandlung (ohne Fingerabdrucknahme) und der Auswertung des ED-Materials, speziell der Personenbeschreibung, unterstützen. Hierzu wurden die Funktionen des Systems im Pflichtenheft detailliert festgelegt und zur Realisierung an die auftragnehmende Firma übergeben.

Der Landesbeauftragte für den Datenschutz begleitet die Realisierung des Vorhabens TLBS von Beginn an. Die von den Mitarbeitern des Landesbeauftragten für den Datenschutz in Arbeitsbesprechungen gegebenen Hinweise wurden berücksichtigt. So wurden u. a. die als kritisch erachteten „unbestimmten Datenfelder“ (Freitextfelder) nicht in die Datenstruktur integriert. Infolgedessen wurde die Datenstruktur überarbeitet und enthält nunmehr keine „unbestimmten Datenfelder“ mehr.

Die rechtlichen Grundlagen, der Zweck sowie die Prüffristen werden in der Errichtungsanordnung (EAO) TLBS beschrieben. Dieses Dokument befindet sich in Bearbeitung und wird gem. § 47 Abs. 3 Satz 2 SOG M-V nach Fertigstellung dem Landesbeauftragten für den Datenschutz übersandt.

3.17 Zu „3.2.5 Erkennungsdienstliche Behandlung eines Zeugen - volles Programm“

In den beiden vom Landesbeauftragten für den Datenschutz geschilderten Fällen haben Polizeibeamte im Zuge erkennungsdienstlicher Maßnahmen gegenüber einem Zeugen bzw. Beschuldigten den Umfang der Behandlung über das gebotene Maß hinaus ausgedehnt. Dabei wurde jeweils die Verfügung der sachleitenden Staatsanwaltschaft nicht mit der erforderlichen Genauigkeit beachtet und demzufolge rechtswidrig gehandelt.

Nach Auffassung des Innenministeriums handelt es sich um zwei nicht verallgemeinerungsfähige Einzelfälle mit eher geringen Auswirkungen auf das Persönlichkeitsrecht der Betroffenen, die gleichwohl Anlass gegeben haben, die handelnden Beamten zu einer genaueren Beachtung datenschutzrechtlicher Bestimmungen anzuhalten.

3.18 Zu „3.2.6 Unschuldig - aber mehrfach verdächtigt“

Im Zusammenhang mit drei Tötungsdelikten zum Nachteil junger Mädchen wurde der Petent im Jahre 1996 mehrfach durch Polizeibeamte überprüft. Die Überprüfungen ergaben jedoch, dass er mit den Mordtaten nichts zu tun hatte. Die Hinweise, die dazu führten, dass der Petent wiederholt in das Blickfeld der Strafverfolgungsorgane gelangte, stammten in zwei von drei Fällen nicht aus dem Polizeibereich. In zwei Fällen haben Bürger des Landes aufgrund eines veröffentlichten Phantombildes bzw. einer über die Medien ausgestrahlten Stimmprobe Kontakt mit der Polizei aufgenommen. Im dritten Fall hat ein Polizeibeamter aufgrund einer durch ihn festgestellten Ähnlichkeit zwischen dem Petenten und eines im Bundeskriminalblatt abgedruckten Phantombildes einer anderen Polizeibehörde auf der Grundlage von § 163 StPO die entsprechenden Daten übermittelt.

Auch wenn es im Zusammenhang mit der Bearbeitung dieser Fälle nicht zu den zunächst befürchteten schwerwiegenden Verstößen gegen Datenschutzbestimmungen durch Mitarbeiter der Landespolizei gekommen war - die Überprüfungen des Petenten haben zu keinem Zeitpunkt den Straftatbestand des § 344 StGB (Verfolgung eines Unschuldigen) erfüllt - ist festzuhalten, dass die Bearbeitung der Fälle eine ganze Reihe von Mängeln im Umgang mit persönlichen Daten offenbart hat.

Unbeschadet der Verpflichtung, auch bei der Bearbeitung derartiger Angelegenheiten die Bestimmungen des Datenschutzrechts genau zu beachten, ist auf der anderen Seite darauf hinzuweisen, dass die Polizei bei medienwirksamen Kapitalverbrechen einem erheblichen öffentlichen Aufklärungsdruck ausgesetzt ist. In solchen Situationen offenbart sich das nicht immer spannungsfreie Nebeneinander von Strafverfolgung einerseits und der Beachtung der Vorgaben des Datenschutzrechts andererseits. In der verständlichen Absicht, möglichst schnell alles zur Aufklärung der Straftat und zur Festnahme des Täters zu versuchen, treten unzutreffenderweise die Belange des Datenschutzes gelegentlich in den Hintergrund. Dabei wird oftmals nicht beachtet, dass gerade die Vielzahl derjenigen, die im Rahmen der Ermittlungen unverschuldet in das Blickfeld der Strafverfolgungsbehörden gelangt sind und sich einer Überprüfung ihres Alibis unterziehen müssen, eines besonderen Schutzes ihrer Daten bedürfen.

Der durch den Landesbeauftragten für den Datenschutz durchgeführte Kontrollbesuch bei der zuständen Polizeibehörde hat - so der übereinstimmende Eindruck der dortigen Mitarbeiter - nachhaltig dazu beigetragen, offene Fragen zu beantworten und durch Wissensdefizite hervorgerufene Missverständnisse zu beseitigen.

3.19 Zu „3.2.7 Leichtfertiger Umgang mit DDR-Flüchtlingsakten“

Nach einem Erlass über das Archiv- und Schriftgutwesen in der Landespolizei vom 31. Mai 1996 ist es Aufgabe der Zentralstelle für Technik und Beschaffung der Landespolizei, das dienstliche Archiv- und Schriftgut der ehemaligen Volkspolizei der Bezirke Neubrandenburg, Rostock und Schwerin aufzuarbeiten. Hierbei handelt es sich um eine umfangreiche, den Zeitraum von mehreren Jahren in Anspruch nehmende Aufgabe, da die Aktenbestände gesichtet, zusammengeführt, bewertet und schließlich über den Verbleib der Akten entschieden werden muss (Archivierung vor Ort, im Zentralen Polizeiarchiv oder in den Archiven des Landes; Übergabe an die zuständigen Behörden; Vernichtung).

Im vorliegenden Fall hat die Zentralstelle für Technik und Beschaffung Altaktenbestände der Volkspolizei aus dem Bereich der Bezirksdirektion Neubrandenburg an die Meldebehörde der Stadt Neubrandenburg übergeben. Es handelte sich dabei um Akten der Volkspolizeikreisämter, die in den dortigen Abteilungen „Pass- und Meldewesen“ entstanden waren. Die zweifelsfreie Zuordnung der Akten zum Bereich „Pass- und Meldewesen“ ergibt sich zum einen aus den vorhandenen Aktenübergabelisten und wird darüber hinaus durch Strukturerkenntnisse bestätigt, denn die in jedem Volkspolizeikreisamt eingerichteten Sachbereiche „Rückkehrer und Zuzieher“ waren organisatorisch den Abteilungen für „Pass- und Meldewesen“ zugeordnet.

Der Vorwurf des Landesbeauftragten für den Datenschutz, es handele sich bei der Aktenübergabe um eine unzulässige Datenübermittlung, geht fehl. Die Übergabe der Akten findet ihre Rechtsgrundlage in § 34 Abs. 1 Satz 1 Landesdatenschutzgesetz von Mecklenburg-Vorpommern (DSG MV). Dort ist festgelegt, dass personenbezogene Daten ehemaliger Einrichtungen derjenigen öffentlichen Stelle zustehen, auf die die Aufgaben dieser Einrichtungen übergegangen sind. Demzufolge wurden zutreffenderweise Aktenbestände, die in den Abteilungen „Pass- und Meldebehörden“ der Volkspolizeikreisämter entstanden waren, an das nunmehr für das Pass- und Meldewesen zuständige Ordnungsamt der Stadt Neubrandenburg übergeben.

Der vom Landesbeauftragten für den Datenschutz geltend gemachte Einwand, die Erfassung der „Rückkehrer und Zuzieher“ habe in keinem sächlichen Zusammenhang zu den Aufgaben des Pass- und Meldewesens gestanden, sondern vielmehr originär volkspolizeilichen Zwecken zur Überwachung und Strafverfolgung gedient, hat auf die Frage der ordnungsgemäßen Zuordnung der Altakten keinen Einfluss.
§ 34 Absatz 1 Satz 1 DSG MV knüpft für die Rechtsnachfolge erkennbar nicht an Gesichtspunkte sächlicher Zuständigkeit für eine konkrete Aufgabe an, sondern legt als Ausgangspunkt für die Frage der Zuordnung alter Aktenbestände die tatsächliche funktionsbezogene Rechtsnachfolge zwischen der „ehemaligen Einrichtung“ und „der Stelle, auf die die Aufgaben dieser Einrichtung übergegangen sind“, zugrunde. Richtigerweise ist demzufolge nicht danach zu fragen, wer nach heutiger Rechtslage für „Rückkehrer und Zuzieher“ zuständig wäre, sondern danach, wer Rechtsnachfolger der Einrichtung ist, die zu Zeiten der ehemaligen DDR diesen Aufgabenbereich wahrgenommen hat.

Auch der Landesbeauftragte für den Datenschutz stellt letztlich nicht in Frage, dass diese Aufgabe - unbeschadet der Überlegung, dass dieser Sachbereich nach heutiger Auffassung weder im Bereich des Meldewesens noch in einer sonstigen staatlichen Stelle zutreffend angesiedelt werden könnte - zu damaliger Zeit ausschließlich den Abteilungen „Pass- und Meldewesen“ der Volkspolizei der ehemaligen DDR zugeordnet war. Die Voraussetzungen der Aktenübernahmepflicht der Meldebehörde als Ausdruck einer Funktionsnachfolge liegen demzufolge vor. Die Tatsache, dass sich die Art der Aufgabenerfüllung geändert hat, Teilaufgaben entfallen oder hinzugekommen sind, ändert an der grundsätzlichen Zuständigkeit der Pass- und Meldebehörden für diese Akten nichts.

Darüber hinaus verdeutlicht ein weiterer Gesichtspunkt, dass die Übergabe der Akten an die Ordnungsbehörde der Stadt Neubrandenburg rechtsfehlerfrei erfolgt ist. Die Meldebehörden haben sich nämlich die ihnen von der Landespolizei übergebenen „Rückkehrer- und Zuzieherakten“ zu Nutze gemacht, um mit den Angaben über frühere Wohnsitze der betroffenen Personen ihre eigenen Unterlagen zu vervollständigen. Hätte demgegenüber die Landespolizei die Akten sogleich an die Landesarchive gegeben - wie es der Landesbeauftragte für den Datenschutz fordert -, wäre eine Nutzung der Daten durch die Meldebehörden ausgeschlossen worden. Der Sinn des § 34 DSG MV, die abschließende Entscheidung über den Verbleib der Altakten (Archivierung oder Vernichtung) der Stelle zu überlassen, die in einem funktionalen Sinne Rechtsnachfolger der ehemaligen Behörde geworden ist, wäre verfehlt worden.

Nach der Beanstandung hat die Landesregierung veranlasst, dass alle an die Stadt Neubrandenburg übergebenen Akten der Volkspolizeikreisämter, die Auslöser für die Beanstandung waren, teilweise den Kreisarchiven und teilweise dem Landeshauptarchiv zur Aufbewahrung zugeleitet werden. Darüber hinaus wurden die Kommunen mit Schreiben vom 29. Februar 2000 gebeten, im Falle des Auffindens weiterer Altakten der Polizei über Rückkehrer/Zuziehende diese unverzüglich den kommunalen Archiven zu übergeben.

3.20 Zu „3.3 Das Nachrichtendienstliche Informationssystem der Verfassungsschutz-behörden“

Im August 1998 wurde durch den Landesdatenschutzbeauftragten der Umgang mit personenbezogenen Daten im Nachrichtendienstlichen Informationssystem der Verfassungsschutzbehörden des Bundes und der Länder (NADIS) geprüft.

In einigen Fällen wurde festgestellt, dass

- das Erkenntnisdatum (EK-Datum) nicht richtig eingegeben worden war,
- der Bearbeitungsstand der jeweiligen Fälle sich nur aus der Personenarbeitsdatei (PAD) und nicht aus der Akte ergab, sowie
- Sperrvermerke noch nicht vor die Akten geheftet waren, in denen sich zu sperrende Personendaten befanden.

Da die Durchführungsbestimmungen zu § 8 Abs. 7 NADIS-Richtlinien eine Aktualisierung des EK-Datums vorsehen, ist die Kritik zu Punkt 1 dem Grunde nach berechtigt. Es wurde daher veranlasst, dass die mit der Speicherung befassten Sachbearbeiter auf das Erfordernis der Aktualisierung des EK-Datums bei jeder Zuspeicherung eindringlich hingewiesen wurden.

Der Landesdatenschutzbeauftragte wurde allerdings darauf aufmerksam gemacht, dass die festgestellte Abweichung zwischen dem im NADIS vorhandenen EK-Datum und dem an sich zutreffenden (späteren) Erkenntnisdatum weder in den konkret geprüften Fällen noch potentiell zu datenschutzrechtlichen Beeinträchtigungen der gespeicherten Personen geführt hat. In den meisten Fällen konnte anhand des betreffenden PAD-Auszuges schlüssig nachvollzogen werden, dass die Weiterspeicherung über den regelmäßigen Fünfjahreszeitraum hinaus aufgrund zwischenzeitlich angefallener neuer Erkenntnisse zur betreffenden Person fachlich geboten und rechtlich zulässig war.

Im Übrigen ist in diesem Zusammenhang auch darauf hinzuweisen, dass der Verfassungsschutz unseres Landes zugunsten des Betroffenen abweichend von der gesetzlichen Option (§ 11 Abs. 3 Satz 2 LVerfSchG), die eine fünfjährige Überprüfungsfrist für gespeicherte Daten vorsieht, bei Erstspeicherung generell bereits nach zwei Jahren prüft, ob eine Weiterspeicherung erforderlich ist. Die fällige Überprüfung der Datensätze wird bis zu sechs Monate vorher durch interne Hinweise der PAD-Sachbearbeiter oder durch die NADIS-Ausdrucke des BfV beim jeweiligen Sachbearbeiter angezeigt. Darüber hinaus wird der Datensatz bei jeder Einzelfallbearbeitung auf seine Notwendigkeit überprüft.

Wenngleich der Mangel zu Punkt 2 durch interne Arbeitsumorganisation seit Mitte 1996 für die neueren Fälle abgestellt wurde und die Sperrvermerke (Punkt 3) bereits geschrieben, jedoch durch Verzögerungen im Schreibdienst noch nicht eingeheftet worden waren, sind die Beanstandungen des Landesdatenschutzbeauftragten dem Grunde nach berechtigt.

Seinen Empfehlungen wurde gefolgt, soweit sie sich nicht durch eigene Arbeitsumstellungen bereits erledigt hatten.

3.21 Zu „3.4.1 Elektronische Überwachung von Asylbewerbern geplant“

Schon die vom Datenschutzbeauftragten gewählte Überschrift „Elektronische Überwachung von Asylbewerber geplant“ ist unzutreffend. Bei dem geplanten Einsatz einer Chipkarte geht es um die Harmonisierung der Verwaltungsabläufe im Asylverfahren.

Auf der Karte sollen neben den Personalien und dem digitalisierten Fingerabdruck weitere Daten des Asylbewerbers, wie Verfahrens- und Statusdaten oder Leistungsdaten enthalten sein. Sie soll also die Behörden in die Lage versetzen, einen Asylbewerber eindeutig zu identifizieren und die für die Bearbeitung notwendigen Daten sofort zur Verfügung zu haben. Gleichzeitig soll sie als Ausweis dienen. In dieser Funktion würde die Chipkarte der bisherigen Aufenthaltsgestattung entsprechen. Behörden könnten damit Daten speichern oder ablesen, die bisher in Papierform vorhanden sind. Durch die Chipkarte wird also nicht mehr gespeichert als zum gegenwärtigen Zeitpunkt in den Akten bei den verschiedenen Behörden bereits gespeichert ist. Lediglich die Art der Datenübermittlung, die bereits umfassend gesetzlich geregelt ist, würde sich ändern.

Jede Verwaltung soll aber nur auf die Daten ihres Bereichs Zugriff erhalten. Insofern ist auch die Aussage des Datenschutzbeauftragten, dass die Chipkarte „Daten aus sämtlichen Lebensbereichen zusammenführen“ soll, nicht den Tatsachen entsprechend.

Die Vorteile der Einführung einer Chipkarte wären u. a.:

- erhebliche Erleichterung der Identifizierung eines Asylbewerbers,
- Verkürzung der Kommunikationswege, z. B. zum aktuellen Stand des Asylverfahrens, der für jede Behörde, die am Asylverfahren beteiligt ist, von grundlegender Bedeutung ist,
- bei Inanspruchnahme von Leistungen sofortige Feststellungsmöglichkeit, ob die betreffende Person anspruchsberechtigt ist (Begrenzung des Leistungsmissbrauchs),
- Verhinderung von mehrfachen Erfassungen des Asylbewerbers bei verschiedenen Behörden und somit Entlastung von zusätzlichen Identitätsprüfungen.

Neben den Vorteilen für die Behördenseite könnte die Einführung der Chipkarte auch wesentliche Verbesserungen für den Asylbewerber mit sich bringen, z. B. eine schnellere Bearbeitungszeit für von ihm gestellte Anträge oder die sofortige Entkräftung von nicht begründeten Verdächtigungen. Daher hat die Innenministerkonferenz am 18./19. November 1999 in Görlitz den Bundesminister des Innern gebeten, dass er mit allem Nachdruck die Einführung einer Chipkarte im Asylverfahren betreibt und die Weichen für eine möglichst rasche Einführung der Chipkarte stellt.

Der datenschutzrechtlich gebotene Vorrang der Datenerhebung beim Betroffenen wird durch den Technikeinsatz nicht verdrängt. Natürlich würden die Daten auch weiterhin bei dem Asylbewerber selbst erhoben werden müssen. Entbehrlich wäre lediglich eine Datenerhebung beim Betroffenen, wenn dies bereits eine andere Behörde getan hat. Dabei ist es unerheblich, ob die Datenerhebung nun aus der Asyl-Card gelesen oder Einsicht in die Akte der anderen Behörde genommen wird. Eine „Entpersönlichung“ der Datenerhebung gegenüber der bisher praktizierten Verfahrensweise ist daher in keiner Weise erkennbar. Das Gleiche gilt für den vom Landesdatenschutzbeauftragten angenommenen Verlust an Transparenz für den Betroffenen. Er könnte sich im Falle der Einführung der Chip-Karte bei den Behörden über den Stand der von ihm erhobenen Daten informieren.

Bei der bisherigen Beurteilung stand selbstverständlich der Zweckbindungsgrundsatz im Vordergrund. Ein Informationsbedürfnis einzelner Verwaltungsbereiche darüber hinaus besteht nicht und wäre auch nicht zulässig. Wenn also die Erforderlichkeit der in der Studie vorgesehenen Datensätze und der Umfang der zu übermittelnden Daten in Frage gestellt wird, sollte der Landesdatenschutzbeauftragte konkret mitteilen, wo er den Grundsatz der Verhältnismäßigkeit im Sinne des Verfassungsrechts als nicht gegeben ansieht. Das von ihm genannte Beispiel des Datenzugriffs von Polizeibeamten entspricht dem Zweckbindungsgrundsatz. Natürlich ist gerade für die Polizei die Identität des Asylbewerbers, dessen Status zur Überprüfung der Legalität, die Arbeitsberechtigung oder die räumliche Beschränkung der Aufenthaltsgestattung für die von ihr zu erledigenden Aufgaben von Interesse, um sofort überprüfen zu können, ob ein Verstoß gegen die Bestimmungen des Asylverfahrensgesetzes, des Ausländergesetzes, des Arbeitsförderungsgesetzes oder anderer Vorschriften, die Straftatbestände oder Regelungen zur Ahndung einer Ordnungswidrigkeit enthalten, gegeben ist.

Daneben ist die Polizei, wie auch die Ausländerbehörden, für die Zurückschiebung, die Durchsetzung der Verlassenspflicht bei räumlicher Beschränkung der Aufenthaltsgestattung des Asylbewerbers, die Durchführung der Abschiebung und, soweit es zur Vorbereitung und Durchführung dieser Maßnahmen erforderlich ist, die Festnahme und Beantragung der Haft zuständig. Der Polizei den gleichen Datenzugriff wie den Ausländerbehörden zu geben, entspricht somit durchaus dem Zweckbindungsgrundsatz. Unnötige Verzögerungen, z. B. bei einer Festnahme, könnten entfallen, wenn die Polizei nicht erst die erforderlichen Daten bei den Ausländerbehörden erfragen muss. Gerade an Wochenenden und Feiertagen sowie in den Nachtstunden wäre dies von besonderer Bedeutung und letztendlich auch im Interesse der Betroffenen.

Da von der Bundesregierung lediglich eine sehr eingeschränkte Einführung der Asylcard mitgetragen würde, ist eine Einführung derzeit nicht mehr aktuell.

3.22 Zu „3.4.2 Automatisierte Abrufverfahren in Gemeinden und Ämtern“

In Gemeinden und Ämtern wird auf die Meldebehörden dahingehend verstärkt Druck ausgeübt, die Melderegister für automatisierte Abrufverfahren anderen Verwaltungseinheiten zu öffnen. Es wurden mit dem Landesdatenschutzbeauftragten Gespräche zu dem Themenkomplex geführt. Es besteht Einvernehmen darüber, dass die geltende Rechtslage eine solche Verfahrensweise nicht zulässt. In Übereinstimmung mit dem Landesdatenschutzbeauftragten ist beabsichtigt, nach erfolgter Novellierung des Melderechtsrahmengesetzes (zurzeit in Arbeit) und des Landesdatenschutzgesetzes darauf abgestimmte Änderungen im Landesmeldegesetz vorzunehmen, die die rechtlichen Rahmenbedingungen für die Zulassung eines automatisierten Abrufverfahrens regeln.

3.23 Zu „3.4.3 Widerspruchsrecht bei Übermittlung von Meldedaten unzureichend“

<u>Widerspruchsrecht gegen Datenübermittlungen aus dem Melderegister</u>

Gemäß § 22 Abs. 1 Melderechtsrahmengesetz (MRRG) sieht die bundesrechtliche Regelung im Falle von Bundestags- und Europawahlen lediglich die Möglichkeit des Widerspruchs vor. § 35 Abs. 1 LMG M-V beinhaltet ebenfalls die Widerspruchslösung. Die Normierung der Einwilligungslösung im LMG - wie vom Landesdatenschutzbeauftragten gewünscht - wurde bisher vom Gesetzgeber abgelehnt.

Gerade bei gleichzeitiger Durchführung von Wahlen auf Bundes- und Landesebene, wie sie in M-V in den letzten Jahren stets erfolgte, ist eine ausschließlich für die auf Landesebene stattfindenden Wahlen geltende Einwilligungslösung rechtlich nicht möglich. Da die in M-V wohnenden, zur Wahl auf Landesebene wahlberechtigten Personen auch zur Wahl auf Bundesebene wahlberechtigt sind, würde eine zulässige Herausgabe von Meldedaten der zu den Bundeswahlen Wahlberechtigten indirekt eine Melderegisterauskunft über die zur Wahl auf Landesebene Wahlberechtigten auch dann beinhalten, wenn eine Einwilligung der Betroffenen hierfür nicht vorliegt. Die Verankerung der Einwilligungslösung im LMG ist solange problematisch, wie die Widerspruchslösung im MRRG normiert ist.

Ob im MRRG die Widerspruchslösung durch die Einwilligungslösung ersetzt werden sollte, ist weniger aus melde- und datenschutzrechtlicher Sicht als vielmehr aus politischer Sicht zu beantworten. Entscheidend kommt es darauf an, wie hoch das Interesse der Wahlvorschlagsträger an den Meldedaten zum Zwecke ihrer Wahlwerbung ist. In ihrer praktischen Ausführung bedeutet die Einwilligungslösung, dass die Parteien und die anderen Wahlvorschlagsträger keine oder nur sehr wenige Meldedaten von Wahlberechtigten erhalten werden. Es dürfte davon auszugehen sein, dass die Bürger - sei es aus Bequemlichkeit, Gleichgültigkeit, politischem Desinteresse o. ä. - von sich aus keinen Kontakt mit der Meldebehörde aufnehmen werden, um ihr ausdrückliches Einverständnis für die Weitergabe ihrer personenbezogenen Daten aus dem Melderegister an die Wahlvorschlagsträger zu erklären. Darüber hinaus muss, selbst wenn in § 22 Abs. 1 MRRG die Einwilligungslösung normiert werden sollte, auch eine Änderung der zurzeit noch unter Widerspruchsvorbehalt stehenden Melderegisterauskünfte an Adressbuchverlage sowie an Mandatsträger, Presse und Rundfunk über Alters- und Ehejubiläen vorgenommen werden. Eine differenzierte Regelung zwischen Einwilligungslösung für die Wahlen einerseits und Widerspruchslösung für Adressbuchverlage sowie Alters- und Ehejubiläen andererseits ist nicht verwaltungspraktisch, insbesondere aber für den Bürger nicht verständlich.

Im Übrigen ermöglicht gerade das Widerspruchsrecht, auf das die Einwohner sowohl bei der Anmeldung als auch mindestens einmal jährlich durch öffentliche Bekanntmachung hingewiesen werden, dem Betroffenen die freie Entscheidung darüber, ob er die Weitergabe seiner Daten hinnehmen will. Über ihr Widerspruchsrecht sind die Bürger, von Einzelfällen abgesehen, auch informiert und sie machen Gebrauch davon. Die Anzahl der eingetragenen Widersprüche allein in den kreisfreien Städten verdeutlicht, dass die Bürger sehr genau zwischen Melderegisterauskünften an Wahlvorschlagsträger einerseits und Melderegisterauskünften an Adressbuchverlage andererseits differenzieren. Selbst als anlässlich der letzten Landtagswahlen die DVU eine sehr offensive Werbekampagne betrieb und fast landesweit Meldedaten bei den Meldebehörden abgefordert hatte und dies auch in den Medien eine ausführliche Berichterstattung nach sich zog, sind die Widerspruchszahlen nach Aussage der kreisfreien Städte nur unbedeutend gestiegen.

Gegenwärtig sind Arbeitsgruppen mit der Vorbereitung einer Novellierung des MRRG befasst. Dabei ist auch die Einwilligungslösung wieder in der Diskussion. Das Ergebnis ist abzuwarten.

Gebührenpflichtige Auskunftssperre

Im Rahmen der Änderung der Verordnung über die allgemeinen Verwaltungsgebühren im Geschäftsbereich des Innenministeriums ist im Bereich des Einwohnerwesens unter der Tarifstelle 2.1.2.7 eine Gebühr in Höhe von 20,-- DM für die Errichtung einer Auskunftssperre nach § 34 Abs. 5 und 6 LMG mit Wirkung vom 24. Juli 1997 eingeführt worden. Mit Schreiben vom 26. Mai 1998 hat sich der Landesdatenschutzbeauftragte gegen die in der Verordnung festgelegte Gebühr mit der Begründung ausgesprochen, dass durch die Auskunftssperre hochrangige Rechtsgüter wie Leben, Gesundheit oder persönliche Freiheit geschützt werden sollten und es von daher unbillig wäre, eine Gebühr für eine Auskunftssperre zu erheben.

Daraufhin wurde dem Landesdatenschutzbeauftragten mit Schreiben des Innenministers vom 15. Juli 1998 dargelegt, dass die Verwaltungsgebühr insbesondere im Hinblick auf den hohen Verwaltungsaufwand gerechtfertigt sei und eine Aufhebung der Tarifstelle nicht in Erwägung gezogen werde. Ein weiteres Schreiben des Landesdatenschutzbeauftragten vom 22. Dezember 1998 war erneut vom Innenminister zum Anlass genommen worden, sich noch einmal bei den kreisfreien Städten, die immerhin einen Bestand von ca. 580 000 Einwohnern verwalten, nach der Notwendigkeit und den Auswirkungen der Gebührenregelung zu erkundigen. Nach Auskunft der zuständigen Amtsleiter der kreisfreien Städte gibt es in der Praxis bei der Umsetzung der Gebührenregelung keinerlei Probleme; Fälle des versuchten Missbrauchs konnten verhindert werden. In sozialen Härtefällen wird die Gebührenbefreiung sehr großzügig zugunsten der Betroffenen angewendet.

Angesichts des mit einer Antragstellung verbundenen hohen Verwaltungsaufwandes hat der Innenminister die Gebührenerhebung für gerechtfertigt angesehen. Jeder Einzelfall bedarf, wie bereits im Schreiben vom 15. Juli 1998 dargelegt wurde, einer gründlichen Prüfung und wird in einem ausführlichen Gespräch oder Schriftwechsel bearbeitet. Vielfach besteht bei den Antragstellern zudem eine völlig unzutreffende Vorstellung darüber, unter welchen engen Voraussetzungen eine Auskunftssperre überhaupt in das Melderegister eingetragen werden darf. In diesen Fällen ist eine intensive Aufklärungsarbeit erforderlich. Angesichts des hohen Verwaltungsaufwandes hat der Städte- und Gemeindetag in seiner Stellungnahme vom 21. März 1997 zu dem Entwurf der Kostenverordnung sogar eine Gebühr in Höhe von 40,-- DM angeregt. Gerade mit Blick auf den hohen Stellenwert der zu schützenden Rechtsgüter ist letztlich eine Gebühr in Höhe von nur 20,-- DM in die Verordnung aufgenommen worden. Angesichts dieses geringen Betrages wird das Recht auf informationelle Selbstbestimmung nicht beeinträchtigt. Entsprechend wird im Übrigen auch in anderen Ländern verfahren, wie z. B. in Sachsen, wo sogar eine Gebühr in Höhe von 30,-- DM für die Einrichtung einer Auskunftssperre erhoben wird.

Mit Schreiben vom 14. Januar 1999 hat der Innenminister dem Landesdatenschutzbeauftragten mitgeteilt, dass er aus o. g. Gründen auch weiterhin von einer Aufhebung der Tarifstelle absehen wird.

3.24 Zu „3.4.4 Wohnsitzwechsel - Kopie des Mietvertrages zu den Akten der Meldebehörde?“

Die dargelegte Verfahrensweise einer Meldebehörde war durch das LMG nicht gedeckt. Es bestand Einvernehmen darüber zwischen dem Landesdatenschutzbeauftragten und dem fachlich zuständigen Referat. Die Meldebehörde ist den Empfehlungen des Landesdatenschutzbeauftragten zur erforderlichen Aktenführung gefolgt, so dass in diesem Punkt die Rechtmäßigkeit wieder hergestellt werden konnte.

3.25 Zu „3.6 Datenübermittlung in Planfeststellungsverfahren“

Das Landesamt für Straßenbau und Verkehr ist Anfang 1999 in dieser Angelegenheit an den Datenschutzbeauftragten des Wirtschaftsministeriums herangetreten. Dieser hat sich bemüht, zu einer praxisnahen Lösung zu kommen, die allen betroffenen Interessen ausreichend Rechnung tragen sollte. Er hat deshalb in Abstimmung mit dem Landesamt mit Schreiben vom 20.05.1999 an den Landesbeauftragten für den Datenschutz wie folgt Stellung genommen:

„1. Die Einwilligung kann vom Einwender folgendermaßen konkludent erklärt werden: Der Einwender reicht seine Einwendungen schriftlich auf eine Bekanntmachung ein, in der er nach Maßgabe des Datenschutzrechts über den Umgang mit seinen personenbezogenen Daten aufgeklärt worden ist, ferner darüber, dass die Einreichung der Einwendungen als Einwilligung im Sinne des DSG MV gilt. Er wird in der Bekanntmachung darüber unterrichtet, dass er der Weiterleitung bei Einreichung widersprechen kann und dass die eingereichten Unterlagen in diesem Fall anonymisiert werden.

2. Liegt die Einwilligung des Einwenders vor, so kommt es für den Umgang mit den Daten auf das Vorliegen weiterer Voraussetzungen (etwa der Erforderlichkeit) aus Vorschriften des DSG MV oder anderer Gesetze nicht mehr an; die Einwilligung steht gleichrangig als Zulässigkeitsvoraussetzung neben der Erlaubnis auf Grund des DSG MV oder einer anderen Rechtsvorschrift (vgl. Bergmann/Möhrle/Herb, BDSG, § 4, Rdnr. 27).

   Die Form der Einwilligung steht im Einklang mit § 7 DSG MV. Zwar ist im Regelfall die Schriftform gefordert, eine andere Form (auch die Einwilligung durch schlüssiges Handeln, Schaffland/Wiltfang, BDSG, § 4, Rdnr. 8) ist jedoch zulässig, wenn sie wegen besonderer Umstände angemessen ist (§ 7 Satz 1 DSG MV). Solche Umstände liegen hier vor. Die Daten, um die es sich handelt (Name, Adresse), sind vielfach schon dem Telefonbuch zu entnehmen; sie sind keinesfalls sensibel. Im weiteren Verlauf des Verfahrens - bei Identifizierung des Einwenders im Erörterungstermin - werden sie dem Vorhabenträger ohnehin bekannt. Für die Behörde wäre mit einer Anonymisierung aller Einwendungen in einem Massenverfahren ein unverhältnismäßiger Aufwand verbunden.“

Der Landesbeauftragte für den Datenschutz hat mit Schreiben vom 20.08.1999 dieser Auffassung widersprochen und - ebenso wie im Tätigkeitsbericht - die Auffassung vertreten, das entscheidende Kriterium der Datenübermittlung sei die Erforderlichkeit. Dem kann auch mit Blick auf das vom Landesbeauftragten in seinem Schreiben herangezogene Volkszählungsurteil des Bundesverfassungsgerichts (BVerfGE 65, 1) nicht gefolgt werden. Aus dem Urteil ergibt sich Nichts dafür, dass bei vorliegender Einwilligung des Betroffenen noch die Erforderlichkeit der Datenübermittlung geprüft werden muss. Das Gericht hat vielmehr festgestellt, dass das Recht auf informationelle Selbstbestimmung „die Befugnis des Einzelnen (gewährleistet), grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“ (BVerfGE 65, 43). Zwar muss „der Einzelne Einschränkungen seines Rechts ... im überwiegenden Allgemeininteresse hinnehmen“ (BverfGE 65, 44); keine Rede ist aber davon, dass der Einzelne zu seinem Schutz daran gehindert sein soll, seine Daten an andere weiterzuleiten oder weiterleiten zu lassen, obwohl er die Weiterleitung wünscht oder mit ihr einverstanden ist. Auch das Landesdatenschutzgesetz lässt sich nicht in diesem Sinne verstehen.

Eine (nochmalige) Antwort an den Landesbeauftragten ist unterblieben, weil die Auffassungen in fernmündlichen und schriftlichen Kontakten ausgetauscht waren und für das Wirtschaftsministerium ein hinreichender Grund zur Änderung seiner Position nicht erkennbar war.

3.26 Zu „3.7 Volkszählung“

Gemäß des Beschlusses der Innenministerkonferenz vom 19./20. November 1998 wird der Methodenwechsel von einer primärstatistischen Vollerhebung zu einer hauptsächlich registergestützten Datengewinnung angestrebt. Dabei spielt die Nutzung des Melderegisters eine entscheidende Rolle.

Der Entwurf eines Gesetzes zur Erprobung eines registergestützten Zensus wird derzeit vom BMI erarbeitet. Da den Ländern noch kein Gesetzentwurf zugeleitet wurde, kann derzeit nicht eingeschätzt werden, ob datenschutzrechtliche Belange berührt werden.

3.27 Zu „3.9.1 Detektiv verfolgt Hund“

Die Auffassung des Landesbeauftragten für den Datenschutz kann nicht in vollem Umfang geteilt werden. Die zu diesem Thema mit Schreiben des Innenministeriums vom 30. November 1999 aufgrund einer entsprechenden Anfrage des Landesbeauftragten für den Datenschutz vom 12. Oktober 1999 abgegebene Stellungnahme ist bei der Abfassung des Tätigkeitsberichtes erkennbar nicht gewürdigt worden.

Einigkeit bestand mit dem Landesbeauftragten für den Datenschutz darüber, dass Hundebestandsaufnahmen privater Dienstleistungsunternehmen als „Umgang mit personenbezogenen Daten im Auftrag“ gem. § 4 DSG MV anzusehen seien. Sie unterlägen daher grundsätzlich den Beschränkungen dieses Gesetzes, soweit nicht besondere Vorschriften i. S. d. § 2 Abs. 3 DSG MV vorgingen.

Dem Landesbeauftragten für den Datenschutz wurde mitgeteilt, dass die gem. § 8 DSG MV geforderten Voraussetzungen für das Erheben entsprechender Daten auch ohne ausdrückliche Regelung in der Hundesteuersatzung der jeweiligen Stadt oder Gemeinde vorlägen. Derzeit sei eine Neufassung der bestehenden Mustersatzung aus dem Jahre 1996 nicht beabsichtigt und aus datenschutzrechtlicher Sicht auch nicht erforderlich.

Weiter wurde darauf hingewiesen, dass auf die Erhebung der Hundesteuer gem. § 12 KAG die Vorschriften der Abgabenordnung (AO) in der jeweiligen Fassung entsprechende Anwendung fänden, soweit nicht das KAG oder andere Gesetze besondere Vorschriften enthielten. Insbesondere die §§ 90 und 93 AO verpflichteten die Steuerpflichtigen (Beteiligten) zur Mitwirkung und Auskunft. Letzteres schließe ausdrücklich auch „andere Personen“ ein (§ 93 Abs. 1 Satz 1 AO). Gemäß § 85 AO hätten die abgabeberechtigten Städte und Gemeinden die Steuer nach Maßgabe der Gesetze gleichmäßig festzusetzen und zu erheben. Insbesondere hätten sie u. a. sicherzustellen, dass Steuern nicht verkürzt würden. Es handele sich hierbei um besondere Rechtsvorschriften i. S. d. § 2 Abs. 3 DSG MV, die damit den Vorschriften dieses Gesetzes vorgingen.

In diesem Zusammenhang wurde auf § 88 a AO aufmerksam gemacht, der es den steuerberechtigten Behörden erlaube, zur Sicherstellung einer gleichmäßigen Festsetzung und Erhebung der Steuern Daten auch für Zwecke künftiger Verfahren zu sammeln und zu verwenden.

Es wurde deutlich gemacht, dass die Frage, inwieweit die Einbeziehung privater Dienstleistungsunternehmen zulässig sei, nicht einheitlich beurteilt werde. Nicht zuletzt aus diesem Grunde sehe die Mustersatzung auch keine Regelung zur Durchführung von Hundebestandsaufnahmen durch private Dritte vor. Abweichungen von der Mustersatzung bedürften gem. § 2 Abs. 2 Satz 1 KAG der Genehmigung der Rechtsaufsichtsbehörde. Bislang seien ausschließlich Genehmigungen zu von der Mustersatzung dbzgl. abweichenden Satzungen erteilt worden, die eine von der Stadt durchzuführende Hundebestandsaufnahme vorsehen.

Darüber hinaus wurde dem Landesbeauftragten für den Datenschutz unter Hinweis auf aktuelle Rechtsprechung mitgeteilt, dass seine Auffassung, für Private könnten keine Befugnisse zur Durchsetzung einer Auskunftspflicht vorgesehen werden, von hier aus geteilt wird.

3.28 Zu „3.9.3 Haushalts-, Kassen- und Rechnungswesen“

Datenschutz und IT-Sicherheitskonzept

Am 07.04.2000 fand zu der im Bericht angeführten Problematik eine Beratung statt, an der Vertreter des Landesdatenschutzbeauftragten, Mitarbeiter der DVZ M-V GmbH und des Finanzministeriums teilnahmen. Diese Arbeitsgruppe arbeitet kontinuierlich an der Verfeinerung und Anpassung des Konzeptes zu Datenschutz und Datensicherheit an die neuesten Anforderungen und technischen Standards. Das Konzept zu Datenschutz und Datensicherheit konnte in Übereinstimmung aller Beteiligten am o.g. Termin überarbeitet werden. Ein Exemplar der aktuellen Version ist an den Landesbeauftragten für Datenschutz übergeben worden.

Es wurde weiterhin beschlossen, einen Teil über die Anforderungen an die Endgerätesicherheit in das Konzept aufzunehmen. Es wird eine Einteilung der Arbeitsplätze nach Arbeitsplatztypen erfolgen, für die die Mindestanforderungen an die Endgeräte in Abstimmung mit dem Landesdatenschutzbeauftragten definiert werden. Dieser Teil wird allen Profiscal anwendenden Dienststellen zur Kenntnis gegeben. Das Finanzministerium wird einen Entwurf anfertigen. Eine Abstimmung zwischen Finanzministerium und DVZ M-V GmbH soll in der 20. Kalenderwoche erfolgen. Der überarbeitete Entwurf wird dann dem Landesdatenschutzbeauftragten übergeben. Die Einarbeitung dieses Teiles in das Konzept soll sowohl eine Durchsetzung der Mindestanforderungen in den Dienststellen des Landes als auch die Kontrollmöglichkeiten gegen Verstöße für den Landesdatenschutzbeauftragten sowie für das Finanzministerium erleichtern.

Test mit Echtdaten

Der Test mit Echtdaten ist aus Sicht des Finanzministeriums Mecklenburg-Vorpommern unverzichtbar. Er wird unter Beachtung der im 3. Tätigkeitsbericht (Drucksache 2/3531 vom 16.02.1998) gesetzten engen Grenzen durchgeführt.

Einführung der elektronischen Kassenanordnung

Die Einführung der digitalen Signatur und modernen Methoden der Nutzerindentifikation wird für die neue Entwicklungslinie von Profiscal frühestens für das Jahr 2002 angestrebt. Bis zu diesem Zeitpunkt sind schriftliche Kassenanordnungen mit den notwendigen Unterschriften zu versehen. Der Landesdatenschutzbeauftragte wird in die Planungen und Entwicklungen einbezogen.

3.29 Zu „3.9.4 Muss man bei Sterbefällen Vermögensangaben machen?“

Bei der im o. g. Bericht dargestellten Thematik handelt es sich um ein Problem, das nicht nur in Mecklenburg-Vorpommern, sondern im gesamten Bundesgebiet existierte.

In Absprache mit dem Bundesministerium des Innern wurden die vom Landesdatenschutzbeauftragten vorgetragenen Beanstandungen zum Anlass genommen, das Verfahren zu ändern und den Standesämtern die in dem Bericht des Landesbeauftragten für den Datenschutz aufgeführten Hinweise zu erteilen.

3.30 Zu „3.9.5 Kein Konto ohne Ausweiskopie?“

Die im Referentenentwurf eines Gesetzes zur Bereinigung von steuerlichen Vorschriften (Steuerbereinigungsgesetz 1999) vorgesehene Änderung des § 154 Abs. 2 Abgabenordnung (AO) wurde im Gesetzgebungsverfahren aus dem Entwurf herausgenommen. Anlass dafür war, dass das Erfordernis einer Identifizierung aufgrund eines amtlichen Ausweisdokumentes primär aus Gründen der Geldwäschebekämpfung und nicht aus steuerrechtlichen Beweggründen erfolgt.

Das Geldwäschegesetz (GWG) enthält keine Regelung zur Identifizierungspflicht bei Aufnahme der Geschäftsbeziehung. Eine explizite Umsetzung der Vorgaben des Artikels 3 Abs. 1 der EU-Geldwäscherichtlinie zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche im Geldwäschegesetz ist bisher unterblieben, weil in § 154 Abs. 2 AO bereits eine bewährte Vorschrift zur Identifizierung bei Einrichtung eines Kontos enthalten war. Daher hat der Gesetzgeber von einer Regelung im Geldwäschegesetz abgesehen. Durch die nunmehr vorgesehene Änderung des § 9 Abs. 1 Satz 1 des GWG soll sichergestellt werden, dass die zur Identifizierung vorgelegten Dokumente abgelichtet und die Ablichtungen aufbewahrt werden dürfen. So können datenschutzrechtliche Bedenken gegen die Fertigung von Kopien ausgeräumt werden. Das Finanzministerium ist für die Änderung des GWG nicht zuständig.

Die im Bericht angesprochene Thematik und die an das Finanzministerium gerichtete Bitte, im Gesetzgebungsverfahren ein Kopieren der Ausweise von der Zustimmung der Betroffenen abhängig zu machen, hat sich durch die Änderung des Entwurfs im Gesetzgebungsverfahren erledigt.

3.31 Zu „3.9.6 Zweitwohnungssteuer“

Der Landesbeauftragte für den Datenschutz zeigt anhand einer konkreten Zweitwohnungssteuersatzung einer Kommune datenschutzrechtliche Bedenken auf. Die Angelegenheit ist der Kommunalabteilung des Innenministeriums bekannt. Die in Rede stehende Satzung ist bis heute nicht in Kraft getreten. Da diese Satzung nicht nur aus datenschutzrechtlicher Sicht auf Bedenken stieß, überdenkt die betreffende Kommune z. Z. eine Überarbeitung dieser Satzung.

Dem Landesbeauftragten für den Datenschutz wird zugestimmt, dass einer Zweitwohnungssteuersatzung die Rechtsgrundlage fehlt, soweit sie Mitwirkungspflichten regelt, die über das nach dem KAG M-V und der AO zulässige Maß hinausgehen.

3.32 Zu „3.9.7 Elektronische Steuererklärung“

Schaffung einer Rechtsgrundlage für die Abgabe der Elektronischen Steuererklärung (ELSTER)

Zu der Frage, nach welchen Grundsätzen Steuererklärungen und Steuererklärungsdaten verwendet werden dürfen, haben sich der Bund und die Länder in zwei BMF-Schreiben vom 27.12.1999, BStBl. I S. 1049 ff., geäußert. Hieraus wird deutlich, dass sich auch nach Einführung des EDV-Verfahrens ELSTER an den Grundsätzen zur Abgabe einer Steuererklärung nichts geändert hat. Steuererklärungen sind wie bisher nach amtlich vorgeschriebenem Vordruck im Sinne des § 150 Abs. 1 AO abzugeben. Die elektronische Übermittlung der Steuererklärungsdaten ersetzt diese Abgabe nicht. Auch werden durch das bloße Bereitstellen der Steuererklärungsdaten die Fristen zur Abgabe einer Steuererklärung nicht berührt.

Insoweit wird in den Grundsätzen für die elektronische Übermittlung von Steuererklärungsdaten unmittelbar auf § 150 Abs. 1 AO Bezug genommen, so dass es einer Rechtsverordnung nach § 150 Abs. 6 AO derzeit noch nicht bedarf. Diese wäre jedoch ab dem Zeitpunkt zu schaffen, wenn auf die Abgabe einer Steuererklärung in der nach § 150 Abs. 1 AO vorgeschriebenen Form verzichtet werden würde.

Wie bereits im Berichtsentwurf festgestellt, wird für die Schlüsselerzeugung bei der OFD Rostock ein stand-alone-PC eingesetzt.

Projekt zur Elektronischen Lohnsteuerkarte EloKa

Im Grobkonzept EloKa VO.2 wird u. a. auch die Sozialversicherungsnummer als eindeutiger, unveränderbarer Ordnungsbegriff für die elektronische Lohnsteuerkarte in Betracht gezogen, deren Verwendung jedoch aus Gründen des Datenschutzes ausgeschlossen ist.

Weitere mögliche Ordnungsbegriffe sind eine Electronik-Taxpayer-Identifikation-Nummer (eTIN), eine Lohnsteuerkartennummer, eine Arbeitnehmer Identifikations-Nummer (AIN) und die AIN variabel (pro Arbeitgeber). Im Ergebnis der Untersuchung schlägt die mit der Aufgabe betraute Arbeitsgruppe beim Bundesministerium der Finanzen vor, eine lebenslang gültige eTIN - in Anlehnung an ein in Italien gültiges System - als Ordnungsbegriff für die elektronische Lohnsteuerkarte zu verwenden. Eine endgültige Entscheidung ist noch nicht getroffen worden.

3.33 Zu „3.10.4. Was das BaföG-Amt dem Antragsteller mitteilen darf“

Im Bericht wird festgestellt, dass im BAföG-Verfahren die Interessen des Unterhaltsberechtigten und Unterhaltsverpflichteten berücksichtigt und hinsichtlich der Angaben über die Einkommensverhältnisse eines Elternteils im Förderungsbescheid interessengerecht abgewogen werden. Insoweit hat sich die Regelung des § 50 Abs. 2 Satz 3 BAföG aus datenschutzrechtlicher Sicht bewährt.

3.34 Zu „3.11.1 Meldungen an das Krebsregister“

Der Landesbeauftragte für den Datenschutz bemängelt in erster Linie den Ausschluss des Widerspruchsrechts des Patienten durch § 2 des Krebsregisterausführungsgesetzes (vom 29. Mai 1998). Dies war eine Entscheidung des Landesgesetzgebers, die die Landesregierung nicht kommentieren muss.

Für die daneben verlangte Prüfung, ob aufgrund der Erfahrungen anderer Bundesländer mit einem Widerspruchsrecht dies nicht auch in Mecklenburg-Vorpommern wieder eingeführt werden könnte, ist die Zeit noch nicht reif, weil in mehreren Bundesländern die Krebsregister erst 1998 oder 1999 ihre Arbeit aufgenommen haben. Schon jetzt kann aber darauf hingewiesen werden, dass in neuerer Zeit mehrere Bundesländer (Hessen, Niedersachsen) eine das Widerspruchsrecht einschränkende modifizierte Meldepflicht neu eingeführt haben. Ein Vergleich mit dem Erfassungsgrad beim Deutschen Kinderkrebsregister ist nicht möglich, weil dieses in erster Linie ein klinisches Register ist. Die Erfassung von Daten dient also nicht nur der epidemiologischen Forschung, sondern auch der Behandlung des jeweiligen Patienten.

3.35 Zu „3.11.2 Ärztliche Schweigepflicht im Bestattungsgesetz“

Die Frage, an wen die vom Arzt ausgestellte Todesbescheinigung zu senden ist, wird zusammen mit weiteren Detailfragen in der in § 6 Abs. 5 des Bestattungsgesetzes vorgesehenen Rechtsverordnung geregelt werden. Die Befürchtung des Landesbeauftragten für den Datenschutz bei Ablichtung von Todesbescheinigungen könnten auch für den Einzelfall nicht erforderliche Daten übermittelt werden, ist nach dem Wortlaut des § 6 Abs. 4 des Bestattungsgesetzes unbegründet. Denn danach dürfen Auskünfte nur „im erforderlichen Umfang“ erteilt und Ablichtungen nur „insoweit“ ausgehändigt werden. Daten, die der Antragsteller nicht für einen berechtigten Zweck benötigt, wären vor der Aushändigung der Ablichtung unkenntlich zu machen.

3.36 Zu „3.11.3 Krankenhaus informiert Ordnungsamt über fahruntüchtige Patienten“

Den Ausführungen des Landesbeauftragten für den Datenschutz wird insoweit zugestimmt, dass eine Information der Ordnungsbehörde immer nur das letzte Mittel sein darf und dass vorrangig ein Gespräch mit dem Patienten zu führen ist. Gewinnt der Arzt bei diesem Gespräch aber die Überzeugung, dass der Patient trotz seiner gesundheitlichen Beeinträchtigung ein Kraftfahrzeug führen wird, dann kann es für die Information an die Ordnungsbehörde nicht darauf ankommen, ob der Patient eine Fahrerlaubnis hat oder nicht. Ergänzend wird darauf hingewiesen, dass die Einhaltung der Verschwiegenheitspflicht zu den ärztlichen Berufspflichten gehört, deren Überwachung nicht der Landesregierung, sondern der Ärztekammer Mecklenburg-Vorpommern obliegt.

3.37 Zu „3.11.4 Notrufe werden aufgezeichnet“

Ob die Aufzeichnung von Gesprächen, die über die Notrufnummern 110 und 112 bei Polizei und Rettungsleitstellen eingehen, überhaupt einer rechtlichen Grundlage bedarf, ist zweifelhaft.

Durch Artikel 2 Absatz 1 des Grundgesetzes, durch § 201 des Strafgesetzbuches sowie durch die Bestimmungen der Datenschutzgesetze ist nämlich nur das „nicht-öffentlich“ gesprochene Wort ein persönliches Datum und demzufolge gesondert geschützt. Das öffentlich gesprochene Wort kann hingegen ohne gesonderte rechtliche Grundlage auf Tonträger aufgezeichnet werden.

Dem über eine Notrufnummer geführten Telefonat kommt unbeschadet des möglicherweise persönlichen Inhalts kein „nicht-öffentlicher“ Charakter zu, denn der Anrufer misst dem Gesprächsinhalt in aller Regel keine Vertraulichkeit bei. Er will vielmehr durch den Anruf auf das Vorhandensein einer Not- und Gefahrenlage und die Notwendigkeit fremder Hilfe aufmerksam machen. Ebensowenig wie bei nicht über Telefon geäußerten Hilferufen (etwa mittels Rufen oder durch Gesten) steht allein die Alarmierung von Hilfskräften, nicht aber die Übermittlung persönlicher Daten im Vordergrund.

Der Umstand, dass sich der Anrufer telefonisch an die Polizei als Teil der Öffentlichkeit wendet, macht den Hilferuf nicht zur vertraulichen Angelegenheit; die Nutzung des Anschlusses 110 anstelle einer anderen Art des Hilferufs geschieht in der Regel nur deshalb, weil kein anderer erfolgversprechender Weg zur Verfügung steht. Jedenfalls kann ein etwa durch Herbeirufen von Personen geäußertes Hilfeverlangen an die allgemeine Öffentlichkeit nicht dadurch vertraulichen Charakter erhalten, dass mit der gleichen Absicht über den Notruf 110 die Polizei um Hilfe gebeten wird.

Anders ist die Situation selbstverständlich dann zu beurteilen, wenn über einen allgemeinen Amtsanschluss Kontakt mit einer Polizeidienststelle aufgenommen wird. In diesem Falle steht das vertraulich gesprochene Wort im Vordergrund, so dass eine Aufzeichnung des Telefonats mangels spezialgesetzlicher Rechtsgrundlage ausgeschlossen ist.

Zweifel an der Notwendigkeit einer gesonderten Rechtsgrundlage ergeben sich auch noch aus einem anderen Blickwinkel. Die Aufzeichnung des Gesprächsinhalts und der Verbindungsdaten erfolgt nämlich vornehmlich im Interesse und zum Schutz des Anrufers, denn ihm soll die Hilfe zuteil werden. Ist etwa der Gesprächsinhalt nur teilweise verständlich oder bricht das Gespräch ab, besteht die Möglichkeit, das Band nochmals abzuhören oder über die Verbindungsdaten den Anschluss zu ermitteln und dem Anrufer zur Hilfe zu eilen. Dieser Gesichtspunkt führt zu der Überlegung, ob nicht bei einem Anrufer, der sich in einer lebensbedrohenden Situation befindet, davon ausgegangen werden muss, dass er in die Aufzeichnung des Gesprächs unter der Telefonnummer 110 konkludent eingewilligt hat und schon deshalb in diesem Falle keine gesonderte Rechtsgrundlage erforderlich ist.

Schließlich - unterstellte man einmal die Vertraulichkeit im Zuge von Notrufen übermittelter Daten - ist nicht nachvollziehbar, weshalb neben den vorhandenen rechtlichen Grundlagen eine zusätzliche Spezialvorschrift erforderlich sein soll.
§§ 27, 36 und 38 SOG M-V erlauben bereits den erforderlichen Datenumgang zum Zwecke der Gefahrenabwehr.

Die vom Innenministerium im Schreiben an den Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern vom 18. November 1999 und 20. Januar 2000 vertretene Rechtsauffassung findet breite Zustimmung, insbesondere bei namhaften Kommentatoren des Strafgesetzbuches, die ebenfalls in einem Notruf einen allgemeinen Hilferuf erblicken, der nur der Alarmierung der Öffentlichkeit dient. Auch der Umstand, dass bisher lediglich ein Bundesland eine spezielle Rechtsgrundlage für das regelmäßige Aufzeichnen von Notrufen in sein Polizeigesetz aufgenommen hat, ist ein Hinweis darauf, dass auch andernorts die Aufzeichnung von Notrufen nicht als regelungsbedürftig erachtet wird.

3.38 Zu „3.11.5 Prüfungsaufträge an den Medizinischen Dienst müssen konkret sein“

Nachdem eine alle Seiten zufrieden stellende Regelung gefunden worden ist, kann dieser Punkt als erledigt angesehen werden und bedarf keiner weiteren Stellungnahme.

3.39 Zu „3.12.1 Was die Polizei von Bewerbern wissen will“

Die Einstellungsstelle der Landespolizei Mecklenburg-Vorpommern verwendet zurzeit einen Vordruck, der bereits inhaltlich überarbeitet wurde. Eine Verwendung des neuen Vordrucks ist nicht möglich, weil dieser noch nicht gedruckt ist und ca. 14.000 Exemplare der „alten“ Vordrucke existieren. Die inhaltlichen Änderungen wurden auf einem Merkblatt zusammengefasst und werden den Bewerbern zusammen mit dem alten Vordruck ausgehändigt.

Es handelt sich dabei um folgende Änderungen:

- Telefonnummer: entfällt im neuen Vordruck
- Geburtsname/Geburtsdatum des Ehepartners: entfällt im neuen Vordruck
- Name, Vorname, Beruf, Wohnung der Eltern: freiwillige Angabe, entfällt im neuen Vordruck
- Angaben über gerichtliche Bestrafungen, Erhebung über finanzielle Verpflichtungen oder Schulden: freiwillige Angabe im alten Vordruck; entfällt im neuen Vordruck.

Einzelne Fragen zur gesundheitlichen Vorgeschichte des Bewerbers werden auf dem Formular „Ärztliches Gutachten“ gestellt.

Dieses Formular ist integraler Bestandteil der die Beurteilung der Polizeidiensttauglichkeit von Bewerbern bundesweit regelnden Polizeidienstvorschrift (PDV) 300. In der einleitenden Erklärung erklärt sich der Bewerber bereit, dem untersuchenden Arzt alle Umstände zu offenbaren, die für die Beurteilung seines Gesundheitszustandes bedeutsam sein können. Weiterhin nimmt der Bewerber zur Kenntnis, dass das Verschweigen bestehender Beschwerden und früherer Krankheiten die Entlassung aus dem Polizeidienst nach sich ziehen kann. Die Angaben zur Vorgeschichte (Anamnese) sind in der Form einer schriftlichen Eigenauskunft vom Bewerber zu erbringen (Teil 1 des Formulars „Ärztliches Gutachten“).

Auf dieses schriftliche anamnestische Verfahren im Vorfeld der eigentlichen ärztlichen Einstellungsuntersuchung kann wegen der Vielzahl der zu bearbeitenden Bewerbungen (in Mecklenburg-Vorpommern > 4000/Jahr) nicht verzichtet werden. Im Rahmen der Einstellungsuntersuchung sprechen aber auch in der Landespolizei Mecklenburg-Vorpommern die untersuchenden Polizeiärztinnen/-ärzte den anamnestischen Teil 1 des Formulars „Ärztliches Gutachten“ mit dem Bewerber durch, um eventuelle Fehlangaben zu korrigieren oder Missverständnisse des Bewerbers auszuräumen.

In Bezug auf die Angaben zu Suizidversuchen bei nahen Verwandten wie Onkel und Tante wurde festgestellt, dass angesichts ihrer geringen Aussagekraft für die Beurteilung der gesundheitlichen Eignung des Bewerbers derartige Fragen verzichtbar sind.

3.40 Zu „3.12.2 Praxis der Stasi-Überprüfung noch zeitgemäß?“

Nach den Regelungen der Anlage I Kapitel XIX, Sachgebiet A Abschnitt III Nr. 1 Absatz 5 des Einigungsvertrages wurde als ein wichtiger Grund für eine außerordentliche Kündigung im öffentlichen Dienst gesehen, wenn es sich um frühere Mitarbeiter des MfS/AfNS handelt und im Einzelfall aus diesem Grunde ein Festhalten am Arbeits- oder Beamtenverhältnis unzumutbar erscheint. Nach der aktuellen Regelung des § 8 Abs. 4 Nr. 2 Landesbeamtengesetz Mecklenburg-Vorpommern (LBG M-V) kann Beamter nicht werden, wer für das frühere MfS/AfNS tätig war und aus diesem Grunde bestehende Zweifel an seiner Eignung nicht ausräumt. Durch diese gesetzliche Vorgabe ist insoweit weiterhin die Frage der Zusammenarbeit mit dem MfS/AfNS bei der Einstellung von Bewerbern in den öffentlichen Dienst zu beachten.

Hiervon ausgehend, aber auch in Anbetracht der Tatsache, dass die praktische Bedeutung dieser Materie nachgelassen hat, hat die Landesregierung im Februar 1999 einen Beschluss zur Überprüfung der Eignung von Bewerbern für den öffentlichen Dienst gefasst. Danach geht die Landesregierung unverändert davon aus, dass ehemalige Mitarbeiter des früheren MfS/AfNS nicht im öffentlichen Dienst tätig sein dürfen, sofern im Einzelfall aus diesem Grunde ein Festhalten am Arbeits-/Beamtenverhältnis unzumutbar erscheint. Es wurde festgelegt, dass bei der gebotenen Einzelfallüberprüfung und Beurteilung der Eignung des Betroffenen die maßgeblichen Gesamtumstände zu berücksichtigen und abzuwägen sind. Insbesondere erfolgt nach wie vor eine Überprüfung bei

- tatsächlichen Anhaltspunkten für eine Zusammenarbeit mit dem MfS/AfNS,
- Einstellungen in den höheren Dienst oder Begründung vergleichbarer Angestelltenverhältnisse und
- der Berufung für sicherheitsempfindliche Aufgaben.

Darüber hinaus soll eine Anfrage nur erfolgen, wenn die herausgehobene Position oder die besondere Vertrauensstellung des übertragenen Amtes es ausnahmsweise erfordern.

Dieser Beschluss wurde durch die Landesregierung unverzüglich umgesetzt. Auch dadurch hat die Stasi-Überprüfung gegenüber der früheren Praxis an Relevanz deutlich abgenommen. Nur in den genannten Ausnahmefällen, z. B. bei Tätigkeiten in den Reihen der Landespolizei Mecklenburg-Vorpommern, die die Bearbeitung von sicherheitsempfindlichen Aufgaben umfassen, wird bei Neueinstellungen in der Regel nach wie vor eine Überprüfung auf frühere Tätigkeiten beim MfS/AfNS durchgeführt.

Zur Illustrierung dessen sei angemerkt, dass es im Jahre 1999 insgesamt 87 Neueinstellungen in die Landespolizei Mecklenburg-Vorpommern gab, davon waren 60 Polizeimeister-Anwärter, 20 Polizeikommissars-Anwärter und 7 Tauschversetzungen. Des Weiteren wurden im vergangenen Jahr 19 Angestellte und 2 Arbeiter neu in die Landespolizei Mecklenburg-Vorpommern eingestellt. Es wurden im Bereich der Landespolizei Mecklenburg-Vorpommern im vergangenen Jahr 22 Regelanfragen beim BStU gestellt, insgesamt sind bis zum 31. Dezember 1999 99,82 % aller Anfragen durch den BStU beantwortet und von hier aus abschließend bearbeitet worden.

Für die restlichen neu eingestellten Bediensteten in der Landespolizei Mecklenburg-Vorpommern wurden keine Regelanfragen beim BStU gestellt, weil sie vor dem 12.01.1990 das 18. Lebensjahr noch nicht vollendet hatten und damit eine Regelanfrage entbehrlich war. Daher ist zusammenfassend festzustellen, dass Einzelfallprüfungen im Zusammenhang mit einer früheren Tätigkeit für das MfS/AfNS von Mitarbeitern der Landespolizei Mecklenburg-Vorpommern nur noch eine untergeordnete Rolle spielen.

3.41 Zu „3.12.3 Was darf in die Personalakte aufgenommen werden?“

Als einschlägige Vorschriften zu Personalakten sind die §§ 100 bis 107 LBG M-V mit den dazu erlassenen Verwaltungsvorschriften vom 13. Oktober 1994 - II 240 b - 0310-11 - zu nennen. Unter Nr. 3.18 der Richtlinien über die Führung von Personalakten (VV zu §§ 100 bis 107 LBG M-V) ist geregelt, dass es für die Personalakten von Beamten genügt, dass Ehescheidungen durch Vorlage einer Scheidungsurkunde (nur Tenor) oder beglaubigten Abschrift vom Familienbuch mit Scheidungsvermerk nachgewiesen werden. Es ist nicht zulässig, von Beamten die Vorlage des vollständigen Scheidungsurteils mit Gründen zu verlangen.

Zur Frage der Mitgliedsbescheinigungen der Krankenkassen für Beamte und deren Aufnahme in die Personalakte ist Folgendes anzumerken:

Fürsorgeangelegenheiten, wie Beihilfen es sind, werden in einer Teilakte, die zur Personalakte gehört, geführt.

Zur Abrechnung der Beihilfen ist es erforderlich, dass der Beamte gemäß § 15 der Beihilfevorschriften des Bundes i. V. m. den Hinweisen des BMI zu § 15 beim ersten Beihilfeantrag einen Krankenversicherungsnachweis erbringt. Dieser wird zur Teilakte genommen und verbleibt dort. Darüber hinaus werden keine Nachweise, die Angaben zur Krankenversicherung der Beamten enthalten, zur Personalakte genommen.

Eine Meldepflicht des Dienstherrn gegenüber der Krankenkasse besteht nicht.

3.42 Zu „3.13.1 Chipkarte als Studentenausweis“

Der Studentenausweis wurde erstmalig zum Wintersemester 1999/2000 als Chipkarte ausgestellt. Die Chipkarte ist eine Multifunktionskarte, die gegenwärtig den Studienausweis, den Bibliotheksausweis, die bargeldlose Zahlungsfunktion für Kopiergeräte und in den Einrichtungen des Studentenwerkes in einer Karte vereint.

Gemäß § 123 des Landeshochschulgesetzes sind Studienbewerber und Studierende verpflichtet, personengebundene Daten über Hochschulzugang, Studium und Studiumsverlauf anzugeben. Einzelheiten zu den Mitteilungspflichten des Studierenden und der Datenerhebung hierzu regeln die §§ 21 und 22 der Immatrikulationsordnung der Hochschule Wismar vom 30.04.1998.

Am 23.02.2000 wurde durch die Hochschule Wismar die Beitragsordnung für die Chipkarte als Anlage zur Immatrikulationsordnung der Hochschule Wismar vom 30.04.1998 mit der Bitte um Genehmigung im Bildungsministerium eingereicht. Bei der Ausgabe der Chipkarte ermächtigt der Studierende schriftlich die Hochschule zum Lastschrifteinzug und zur Adressenweitergabe bei Nichteinlösung der Lastschrift oder Widerspruch gegen die Lastschrift.

Den Studierenden werden in jedem Fall wahlweise durch andere Geldkarten (in den Einrichtungen des Studentenwerkes), den Bibliotheksausweis (in der Hochschulbibliothek), die Zahlung mit Bargeld (für Kopiergeräte, Semesterbeitrag) oder mittels Überweisungsauftrag (für Semesterbeitrag) Alternativen geboten, bei Kartenverzicht gleiche Leistungen in Anspruch nehmen zu können, ohne dadurch benachteiligt zu werden. Der Studierende kann jederzeit Auskunft über die auf seiner Chipkarte aktivierten Funktionen erhalten.

Die Chipkarte dient lediglich zur Identifizierung an einem Computer. Die auf den Kartenkörper aufgedruckte Matrikelnummer ist das einzige eindeutige identifizierende Datum für den Studenten. Eine Trennung beim Aufdruck von Matrikelnummer und Namen der Person war auf bisher bestehenden Medien des Studienausweises (z. B. „Leporello“ an anderen Hochschuleinrichtungen) nicht gegeben bzw. wurde nicht beanstandet. Die Mitteilung der Matrikelnummer an jeden einzelnen Studierenden erfolgt persönlich bei der Immatrikulation in „Einzelabfertigung“. Somit ist das Datum „Matrikelnummer“ nur den zuständigen Mitarbeitern des Dezernates Studentische und Akademische Angelegenheiten im Rahmen ihrer Tätigkeit bekannt. Es sei denn, der Studierende gibt seine Matrikelnummer mündlich bzw. seine Chipkarte an Dritte weiter. Der Studienausweis ist Eigentum des Studierenden. Damit liegt es in seiner Verantwortung, seine Daten nur an berechtigte Personen weiterzuleiten. Des Weiteren ist es in anderen Branchen ebenfalls üblich, ein eindeutiges Datum (z. B. Kontonummer) in Verbindung mit dem Namen des Karteninhabers auf den Kartenkörper aufzudrucken.

Mit der Einführung der Chipkarte haben sich keine Änderungen in Art und Ort der Datenerhebung und Datenhaltung ergeben. Die Schaffung einer zusätzlichen Schnittstelle ermöglicht dem Studierenden, direkt und auch nur auf seine in der Datenbank gespeicherten Daten zuzugreifen. Eine interaktive Handlung der Studierenden ist nur möglich, nachdem sich der Karteninhaber fälschungssicher gegenüber der Karte identifiziert hat. Die Identifizierung erfolgt durch die vom Studierenden frei wählbare und durch ihn jederzeit änderbare 5-stellige persönliche Identifizierungsnummer (PIN). Bei Verlust der Chipkarte wird diese mit schriftlicher Einwilligung des Studierenden gesperrt.

Es besteht keine Möglichkeit des Missbrauchs oder des Ausspähens der Daten durch Dritte. Das Auslesen und Ändern der Chipkartendaten ist nur über ein Terminalhochsicherheitsmodul möglich.

Die Daten auf der Chipkarte werden durch die im Sicherheitskonzept der Sparkassenorganisation festgeschriebenen Maßnahmen geschützt:

- Das Aufbringen studentischer Daten auf der Chipkarte ist ohne vorherige Zulassung der Sparkassenorganisation nicht möglich (kryptographische Absicherung). Alle kryptographischen Schlüssel sind für den Transport und die Speicherung vor unbefugter Kenntnisnahme und Manipulation geschützt (möglich: kryptopgraphische Absicherung; Schlüsseltransport in Sicherheitsmodulen; organisatorische Maßnahmen).
- Die Freischaltung der Chipkarte erfolgt ausschließlich über das Terminalhochsicherheitsmodul und ist ohne Einwilligung des Karteninhabers nicht möglich (kryptographische Absicherung und organisatorische Maßnahmen).
- Die Anwendung studentischer Daten kann nur dann durchgeführt werden, wenn die eingesetzte Chipkarte authentisch ist (kryptographische Absicherung).
- Das Duplizieren, Manipulieren oder Fälschen von studentischen Daten wird wirksam verhindert (kryptographische Absicherung).
- Gestohlene und gefundene Terminalhochsicherheitsmodule können nicht unbefugt benutzt werden (Terminalhochsicherheits-PIN; Aktionen „Freischalten“ und „Sperren“).
- Das Duplizieren, Manipulieren oder Fälschen von Terminalhochsicherheitsmodulen wird wirksam verhindert (kryptographische Absicherung).
- Das Durchführen unkorrekter Transaktionen am Akzeptanzterminal wird erkannt (kryptographische Absicherung; insbesondere werden Transaktionsdatensätze im Terminal mit MAC gesichert; Zählerstände im Terminalhochsicherheitsmodul).

Der Datenverkehr zwischen Chipkarte und Terminal sowie zwischen Terminal und Datenbank findet nur im internen Hochschulnetz statt. Jeglicher Datenverkehr zwischen den Standorten der Hochschule Wismar außerhalb des hochschulinternen Netzes aufgrund der Zugriffe der jeweiligen Studierenden erfolgt verschlüsselt. Die Abschirmung des gesamten betroffenen Netzteiles durch eine Firewall befindet sich im Aufbau. Zum Schutz des Hochschulnetzes und zur Gewährleistung der Authentizität des studentischen Datenbestandes läuft die Kommunikation zwischen Terminal und Datenbank über einen vorgeschalteten Kommunikationsrechner. Somit wird ein kontrollierter Zugriff auf die Datenbank sichergestellt.

Die beschriebenen Maßnahmen belegen, dass aus hiesiger Sicht den datenschutzrechtlichen Bestimmungen entsprochen wird.

3.43 Zu „3.13.2 Anfrage bei der Sekteninformationsstelle - nicht vertraulich?“

Die Feststellung des Landesbeauftragten für den Datenschutz, es sei davon auszugehen, dass sich infolge der Belehrung der betreffenden Mitarbeiter ein solcher Vorgang nicht wiederhole, ist zutreffend und insoweit nicht ergänzungsbedürftig.

3.44 Zu „3.13.3 Schüler im Fokus der Forschung“

Der Sachverhalt wird im Tätigkeitsbericht des Landesbeauftragten für den Datenschutz zutreffend wiedergegeben. Die Übersendung der Unterlagen durch das Ministerium für Bildung, Wissenschaft und Kultur unterblieb zunächst deshalb, weil das Max-Planck-Institut für Bildungsforschung mitgeteilt hatte, dass die datenschutzrechtliche Prüfung durch den Datenschutzbeauftragten des Bundeslandes Hessen stellvertretend und in Abstimmung mit den anderen Datenschutzbeauftragten für alle anderen Bundesländer durchgeführt würde. Aus diesem Grunde übersandte das Ministerium für Bildung, Wissenschaft und Kultur die Unterlagen zunächst nicht. Diese wurden dem Datenschutzbeauftragten auf dessen Nachfrage hin zur Verfügung gestellt.

Das Ministerium wird zukünftig bei derartigen Erhebungen den Datenschutzbeauftragten sofort nach Bekanntwerden der Maßnahme (in der Planungsphase) einbeziehen. Die datenschutzrechtlichen Probleme wurden auch mit dem Max-Planck-Institut erörtert. Das Institut sagte zu, dass die Datenschutzbeauftragten künftig bereits in der Planungsphase einbezogen werden sollen. Vor diesem Hintergrund kann davon ausgegangen werden, dass zukünftig den datenschutzrechtlichen Bestimmungen durch die rechtzeitige Einbeziehung der Datenschutzbeauftragten Rechnung getragen wird.

3.45 Zu „3.15.1 Daten für Abwasseranschluss an privates Unternehmen“

Mit Schreiben vom 22. März 1999 wurde dem Landesbeauftragten für den Datenschutz auf seine Anfrage hin mitgeteilt, dass sich Zweckverbände zur Erfüllung der ihnen übertragenen Aufgaben der Wasser- und Abwasserentsorgung nach § 40 Abs. 4 und § 43 Abs. 2 LWaG Dritter bedienen könnten. Soweit die Verbandssatzung eine entsprechende Regelung enthalte, stünden einer Übertragung der Aufgabenwahrnehmung und -erfüllung des Zweckverbandes an einen privaten Dritten grundsätzlich keine kommunalverfassungsrechtlichen Bedenken entgegen.

Es wurde darauf hingewiesen, dass der zwischen dem Zweckverband und dem privaten Unternehmen zu schließende Vertrag datenschutzrechtliche Belange hinreichend zu berücksichtigen habe, was jedoch einer Einzelfallprüfung vorbehalten bliebe.

Da die Anfrage des Landesbeauftragten für den Datenschutz (auch nach telefonischer Nachfrage) weder den Namen des nicht der Rechtsaufsicht des Innenministeriums unterliegenden Zweckverbandes noch den Sachverhalt zweifelsfrei offenzulegen vermochte, konnte die Rechtmäßigkeit der Verbandssatzung und deren Auslegung seinerzeit nicht abschließend bewertet werden.

Auf weitere Nachfrage des Landesbeauftragten für den Datenschutz wurde diesem telefonisch mitgeteilt, dass sich der Umfang der Aufgabenübertragung an private Dritte durch den Vorbehaltskatalog nach § 157 Abs. 2 i. V. m. § 22 Abs. 3 und 4 KV M-V (Wahrnehmung wichtiger Aufgaben durch die Verbandsversammlung des Zweckverbandes) einschränken ließe.

Insoweit ist dieser Zusammenhang in den Ausführungen des Landesbeauftragten für den Datenschutz in den Absätzen 2 und 3 nur ungenau wiedergegeben.

3.46 Zu „3.16.1 Sichere Vernetzung der Landesverwaltung noch in den Kinderschuhen“

Die in der Staatskanzlei betriebene Kopfstelle für elektronische Post (X.400) ist derzeit über einen Grenzrouter, der eine Paketfilterung und somit Firewall-Funktionalitäten vornimmt, mit dem TESTA-Overlaynetzwerk verbunden. Ein entsprechender Basisschutz ist somit bei der Kommunikation mit den Ländern und dem Bund gewährleistet. Die Anbindung des Ressortverbundnetzwerkes an LAVINE erfolgt ebenfalls über einen Router. Nach Zertifizierung der Firewall durch das BSI wird die X.400-Kopfstelle über diese an TESTA angebunden werden.

In TESTA wird zudem noch dieses Jahr eine Leitungsverschlüsselung implementiert.

Die Frage der Verschlüsselung im landesweiten Corporate Network ist Gegenstand des derzeit in Erarbeitung befindlichen Feinkonzepts.

3.47 Zu „3.16.2 Verschlüsselung künftig ein Standardmerkmal?“

Die Auffassung des Landesdatenschutzbeauftragten, dass es Aufgabe der LKSt sei, möglichst landeseinheitliche Empfehlungen für den Einsatz kryptographischer Verfahren zu geben, wird geteilt. Die LKSt verfolgt entsprechende Entwicklungen auf Bundesebene und in den anderen Ländern. Exemplarisch sei diesbezüglich auf das noch laufende Pilotprojekt „Sphinx“ verwiesen. Aufgrund der zunehmenden Vernetzung der Verwaltungsnetze untereinander - TESTA-D und TESTA-EU - ist darauf zu achten, dass die im Land eingesetzten Kryptographieverfahren mit denen anderer Länder oder des Bundes kompatibel sind. Bei entsprechenden Bedarfen wird die LKSt ihrer Aufgabenstellung entsprechend handeln.

Hinsichtlich der Verschlüsselung im Bereich der Personaldatenverarbeitung erscheint die Forderung des Landesdatenschutzbeauftragten zum gegenwärtigen Zeitpunkt nicht zwingend. Eine Übertragung von Personaldaten zwischen den Behörden des Landes, z. B. mit dem LBesA, findet derzeit nicht über Netzwerkverbindungen statt. Darüber hinaus können Personaldaten nur durch autorisiertes Personal bearbeitet werden. Die entsprechenden Datenbanken befinden sich zudem auf separaten Servern, die ihrerseits nur für eine dezidierte Personengruppe zugänglich sind.

3.48 Zu „3.16.3 Braucht das Land ein eigenes Trustcenter?“

Die Frage der Einrichtung eines eigenen Trustcenters für das Land kann nur vor dem Hintergrund nationaler und internationaler Entwicklungen beantwortet werden. So hat z. B. das BSI im Rahmen von TESTA angeboten, als Root-Certification Authority zu fungieren, um ein bundesweit einheitliches Schlüsselmanagement und somit eine Kompatibilität der Schlüssel zu gewährleisten. In Mecklenburg-Vorpommern und in den anderen Ländern würde sich hierdurch der Investitionsaufwand reduzieren.

Darüber hinaus ist gegenwärtig noch fraglich, ob das Signaturgesetz in seiner gegenwärtigen Fassung auch zukünftig Bestand haben wird. Das Signaturgesetz wird durch einige Bundesländer, insbesondere von Bayern kritisiert, weil es mit seinen Anforderungen über den internationalen Standards läge und somit die Bundesrepublik Schlüssel anderer Staaten nicht akzeptieren könne.

3.49 Zu „3.16.4 Neues zur Internetnutzung“

Unter Federführung des Justizministeriums ist bereits eine Zentrale Firewall mit Viruswall für die gesamte Landesverwaltung bei der DVZ GmbH zur Sicherung des Datenverkehrs der Behörden über das Landesdaten- und Informationsnetz (LAVINE) errichtet worden. Der Landesbeauftragte für den Datenschutz begleitete von Beginn an die Entwicklung und den Aufbau der technischen Lösung bis hin zum abschließend gemeinsam erarbeiteten Sicherheitskonzept. Das Bundesamt für Sicherheit in der Informationstechnik konnte sich Anfang des Jahres 2000 in verschiedenen Tests von der Zuverlässigkeit der Zentralen Firewall überzeugen.

Neben dem Justizministerium nutzen bereits die Landtagsverwaltung und die Fraktionen des Landtages, das Umweltministerium und das Ministerium für Arbeit und Bau die Firewall. Die Anbindung des Finanzministeriums als weiterer Nutzer ist in Vorbereitung.

3.50 Zu „3.16.13 Bundesweite Behördenvernetzung mit TESTA“

Auf der Sitzung der AG „TESTA“ des KoopA ADV am 17. Februar 2000 wurde die Einführung der Leitungsverschlüsselung in TESTA empfohlen. Die Fa. T-Data, eine Tochtergesellschaft der DTAG, hat ein entsprechendes Konzept vorgestellt und wurde aufgefordert, bis Ende März einen Realisierungsplan einschließlich der zu erwartenden Mehrkosten vorzulegen.

Der KoopA ADV konnte auf seiner Sitzung am 10./11. April 2000 nicht über den Realisierungsplan entscheiden, da das ursprünglich vorgesehene Produkt für die Leitungsverschlüsselung nicht im TESTA-Overlaynetzwerk eingesetzt werden kann. Für das nunmehr vorgesehene Produkt „radguard“ wurde beim BSI die Zertifizierung beantragt, die für den Einsatz in TESTA unverzichtbar ist. Aus diesem Grunde verzögert sich die Einführung der Leitungsverschlüsselung. Auf der in Rede stehenden Sitzung wurde darüber hinaus ein Konzept zur sicheren Kommunikation zwischen Verwaltungsnetzen zur Kenntnis genommen, auf dessen Grundlage durch die AG „TESTA“ ein Sicherheitskonzept für das TESTA-Overlaynetzwerk erarbeitet werden soll. Das auf der Sitzung verabschiedete Konzept sollte auch bei der Planung von Sicherheitsmaßnahmen für das landesweite CN berücksichtigt werden. In diesem Zusammenhang sei auch noch einmal auf die vorstehenden Ausführungen zu einem eigenen Trustcenter verwiesen.

Die LKSt teilt die Auffassung des Landesdatenschutzbeauftragten, dass die Anbindung an TESTA über die Firewall in der DVZ M-V GmbH erfolgen soll. Nicht geteilt wird hingegen die Aussage des Landesdatenschutzbeauftragten, dass die DVZ M-V GmbH hierfür noch präzisierte Anforderungen von der LKSt erhalten müsste. Die Anforderungen der LKSt sind dort bereits bekannt.

Gegenwärtig steht lediglich die Zertifizierung durch das BSI aus, die aus Sicht der LKSt Voraussetzung für die Nutzung der in Rede stehenden Firewall ist. Es muss ausgeschlossen werden, dass durch das CN des Landes Mecklenburg-Vorpommern eine Kompromittierung des TESTA-Overlaynetzwerkes verursacht werden kann.