LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 4/1294**
4. Wahlperiode **18.08.2004**

UNTERRICHTUNG

durch die Landesregierung

Stellungnahme der Landesregierung zum Sechsten Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern für die Zeit vom 1. Januar 2002 bis 31. Dezember 2003 sowie Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörde

Zugeleitet mit Schreiben des Chefs der Staatskanzlei vom 13. August 2004 gemäß § 29 Absatz 1 Satz 2 des Datenschutzgesetzes des Landes Mecklenburg-Vorpommern; federführend ist das Innenministerium.

Einleitung

Mit Drucksache 4/1137 vom 27. April 2004 hat der Landesbeauftragte für den Datenschutz dem Landtag und der Landesregierung seinen Sechsten Tätigkeitsbericht vorgelegt, der den Berichtszeitraum vom 1. Januar 2002 bis 31. Dezember 2003 umfasst.

Zu diesem Bericht nimmt die Landesregierung gemäß § 33 Abs. 1 Satz 2 Datenschutzgesetz Mecklenburg-Vorpommern (DSG M-V) vom 24. Juli 1992, zuletzt geändert durch Artikel 4 des Gesetzes vom 12. Dezember 2003 (GVOBl. 2004, S. 2), wie folgt Stellung:

A. Allgemeines

Der Sechste Tätigkeitsbericht des Landesbeauftragten für den Datenschutz verdeutlicht, welchen hohen Stellenwert Ministerien und Behörden des Landes dem Datenschutz beimessen. In der Praxis wird dies auch durch die Tatsache unterstrichen, dass sich die verantwortlichen Stellen in Zweifelsfällen in zunehmendem Maße selbst an den Landesbeauftragten für den Datenschutz wenden, um dem Datenschutz gerecht zu werden.

Auf den über 120 Seiten Berichtstext, die sich mit der Situation des Datenschutzes in Mecklenburg-Vorpommern beschäftigen, berichtet der Landesbeauftragte für den Datenschutz von insgesamt lediglich fünf Fällen während dieses zweijährigen Berichtszeitraumes, in denen er förmliche Beanstandungen aussprechen musste. Nahezu in allen anderen Fällen konnte er mit den verantwortlichen Stellen Einvernehmen darüber erzielen, welche Maßnahmen zur Abhilfe von Schwächen oder zur Vermeidung von künftigen Datenschutzverletzungen erforderlich waren.

Mit Blick auf diese geringe Zahl von Beanstandungen beschränkt sich die Landesregierung auf grundsätzliche und ressortübergreifende Themen sowie auf Sachverhalte, die zwischen dem Landesbeauftragten für den Datenschutz und dem jeweils zuständigen Ressort zu erheblichen Meinungsverschiedenheiten geführt haben oder streitig geblieben sind. Von der Stellungnahme der Landesregierung werden nur diejenigen im Tätigkeitsbericht angesprochenen Themen erfasst, die in ihrer Zuständigkeit liegen.

B. Zu den Ausführungen des Berichts im Einzelnen

Zu Kapitel 1 - Situation des Datenschutzes und rechtliche Grundlagen

Dem Landesbeauftragten für den Datenschutz ist zuzustimmen, wenn er ausführt, sowohl der Datenschutz als auch die Sicherheit seien Grundbedürfnisse der Bürger. Aber gerade deshalb muss bei einem Aufeinandertreffen der Interessen besonders sorgfältig abgewogen werden. Es ist keinesfalls so, dass „die Sicherheitsbehörden“ leichtfertig mit den Persönlichkeitsrechten der Bürger umgegangen sind. Vielmehr beruhen die vom Landesbeauftragten vorgetragenen Kritikpunkte in einem Fall auf menschliches Versagen, im Übrigen jedoch auf unterschiedliche Rechtsauffassungen bzw. Zweckmäßigkeitseinschätzungen.

Der Datenschutz wird - wie der Landesbeauftragte für den Datenschutz feststellte - gelegentlich auch als „Störfaktor“ empfunden. Dies ist in der Praxis häufig dann der Fall - jedoch ohne das Erfordernis des Datenschutzes grundsätzlich in Frage zu stellen -, wenn es sich aus der Sicht der Verantwortlichen um bloße Formalien handelt, deren Nichtbefolgung zu keinen materiellen Beeinträchtigungen des Persönlichkeitsrechts Betroffener führen kann.

Zu dem vom Landesbeauftragten für den Datenschutz erwähnten Beispiel des Rundfunkgebühreneinzugs kann die Landesregierung nicht Stellung nehmen, da nach den Rundfunkstaatsverträgen die Anstalten ihre Wirtschaftsführung selbst regeln. Eine Verantwortung der Landesregierung besteht insoweit nicht.

Die vom Landesbeauftragten für den Datenschutz befürwortete Zusammenlegung der Zuständigkeiten für die Kontrolle des Datenschutzes im öffentlichen und nicht-öffentlichen Bereich befindet sich in der Vorbereitung. Der Landtag hat ein entsprechendes Gesetz zur Änderung des Landesdatenschutzgesetzes am 12. Mai 2004 in Erster Lesung behandelt und an den Innenausschuss und den Wirtschaftsausschuss überwiesen.

Es sei jedoch darauf hingewiesen, dass damit nicht jegliche Datenschutzkontrolle beim Landesbeauftragten für den Datenschutz liegen wird. Für den Datenschutz bei Behörden und öffentlichen Stellen des Bundes bleibt weiterhin der Bundesbeauftragte für den Datenschutz zuständig. Sonderregelungen gelten für die Rundfunkanstalten und die Religionsgemeinschaften. Sie nehmen aus verfassungsrechtlichen Gründen eine Sonderstellung ein. Der Datenschutz der Rundfunkanstalten ist wegen der grundgesetzlich garantierten Freiheit der Medien gesondert in Staatsverträgen geregelt und die Religionsgemeinschaften haben eigene Datenschutzgesetze im Kirchenrecht geschaffen. Beide Bereiche werden deshalb nicht vom Staat kontrolliert und haben eigene unabhängige Datenschutzbeauftragte.

Zu Abschnitt 2.1.5 - „Großer Lauschangriff“ im SOG M-V

Der Landesbeauftragte für den Datenschutz beschrieb in seinem Bericht die Argumente, die er in einer gemeinsamen Stellungnahme mit den Landesbeauftragten von Berlin, Bremen, Hamburg, Niedersachsen, Nordrhein-Westfalen und Schleswig-Holstein dem Bundesverfassungsgericht im Zusammenhang mit einer Verfassungsbeschwerde einiger Privatpersonen gegen die Einführung der akustischen Wohnraumüberwachung in Art. 13 Abs. 3 GG zusammengefasst hatte. Inzwischen ist das Verfahren mit Urteil vom 3. März 2004 - 1 BvR 2378/98 und BvR 1084/99 - (NJW 2004, S. 999 - 1022) teilweise erfolgreich abgeschlossen.

Bereits aufgrund des Urteils des Landesverfassungsgerichts Mecklenburg-Vorpommern vom 18. Mai 2000 - LVerfG 5/98 - (LKV 2000, S. 345 - 357) wurde eine Neufassung der Regelungen zur akustischen Wohnraumüberwachung im Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern (SOG M-V) notwendig. Während der damaligen Novellierung des SOG M-V fanden die vom Landesverfassungsgericht gesetzten Maßstäbe strikte Beachtung, so dass seitdem Maßnahmen der Wohnraumüberwachung auf Grundlage des SOG M-V nicht mehr zur vorbeugenden Bekämpfung von Straftaten, sondern nur noch dann zulässig sind, wenn es gilt, eine gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person abzuwehren. Die Regelungen zu Wohnraumüberwachungen wurden mithin schon zum damaligen Zeitpunkt weit eingeschränkt.

Nach dem Urteil des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung vom 3. März 2004 befasst sich derzeit eine gemeinsame Projektgruppe der vom Arbeitskreis II der Innenministerkonferenz eingesetzten Arbeitsgruppe Kripo, des Unterausschusses Führung, Einsatz, Kriminalitätsbekämpfung und des Unterausschusses Recht und Verwaltung mit der Frage, welche Auswirkungen das Urteil des Bundesverfassungsgerichts insgesamt - also nicht nur auf den Bereich der Strafverfolgung, sondern auch auf den Bereich der Gefahrenabwehr und damit auf die Polizeigesetze der Länder - hat. Erst nach Abschluss der Analysen dieser Projektgruppe wird eine Aussage getroffen werden können, ob und ggf. wie das SOG M-V zu ändern ist, um den Anforderungen des Bundesverfassungsgerichts zu entsprechen.

Maßnahmen des so genannten „Großen Lauschangriffs“ haben sowohl unter präventiven wie unter repressiven Gesichtspunkten in Mecklenburg-Vorpommern kaum eine praktische Bedeutung. So sind hier seit 1998 lediglich in zwei Fällen strafprozessuale Maßnahmen der akustischen Wohnraumüberwachung durchgeführt worden.

Das Bundesministerium der Justiz hat angekündigt, sämtliche heimliche Ermittlungsmaßnahmen, wozu auch der so genannte „Große Lauschangriff“ gehört, zu überprüfen. Die Auffassung der Datenschutzbeauftragten wird sowohl bei der Diskussion um dieses Vorhaben, als auch bei der dem späteren Gesetzgebungsverfahren Berücksichtigung finden. Auch die Landesregierung wird die Auffassung des Landesdatenschutzbeauftragten bei der Abgabe von Stellungnahmen im Bundesrat und seinen Ausschüssen berücksichtigen.

Zu Abschnitt 2.1.6 - DNA-Analyse - Erweiterung nur mit Augenmaß

Mit Blick auf mehrere Gesetzesinitiativen und politische Absichtserklärungen in der Vergangenheit, die zum Ziel hatten, die Nutzung der DNA-Analyse erheblich auszuweiten, haben die Datenschutzbeauftragten des Bundes und der Länder ihre Bedenken in einer Entschließung zusammengefasst.

Diese Auffassungen werden aus fachlicher Sicht nicht geteilt.

Der Arbeitskreis II der Innenministerkonferenz (AK II) hat sich in seiner Sitzung am 06./07.05.2004 mit der Verbreiterung der Anwendungsmöglichkeiten der DNA-Analyse befasst und einen durch eine Bund-Länder-Arbeitsgruppe erarbeiteten Bericht „Ausweitung der Anwendungsmöglichkeiten der DNA-Analyse“ (Stand: 11.04.2004) zur Kenntnis genommen.

In diesem Zusammenhang hat er ausdrücklich die dort enthaltene Empfehlung begrüßt, dass vor dem Hintergrund der überragenden Bedeutung, die die DNA-Identitätsfeststellung für die Kriminalitätsbekämpfung hat, eine Gleichstellung der DNA-Analyse im nicht codierten Bereich mit den sonstigen erkennungsdienstlichen Maßnahmen im Rahmen des § 81 b 2. Alternative StPO erfolgen sollte.

Die Landesregierung hält den Einsatz der DNA-Analyse als erkennungsdienstliche Maßnahme für ein hocheffizientes Mittel der Aufklärung von Straftaten, das in besonderer Weise auch dem Schutz der Bevölkerung vor neuen Straftaten dient. Alle Reformansätze haben die verfassungsmäßigen Rechte der Betroffenen, insbesondere das Recht auf informationelle Selbstbestimmung, zu achten. In diesem Rahmen wird die Landesregierung die Hinweise berücksichtigen.

Die Justizministerinnen und -minister haben auf der 75. Konferenz vom 17. - 18. Juni 2004 in Bremerhaven den Bericht des Strafrechtsausschusses der Justizministerkonferenz zu weiteren Anwendungsmöglichkeiten der DNA-Analyse im Strafverfahren zur Kenntnis genommen. Der Bericht des Strafrechtsausschusses spiegelt die fachliche Sicht der weit überwiegenden Mehrheit der Arbeitsgruppe des Strafrechtsausschusses und die Auffassung des Justizministeriums Mecklenburg-Vorpommern zu dieser Fragestellung wider. Danach ist es sinnvoll und zulässig auf den Anlasskatalog des § 81 g StPO vollständig zu verzichten, weil der verfassungsrechtliche Schwerpunkt dieser Norm nicht hier, sondern auf dem Tatbestandsmerkmal der qualifizierten Negativprognose liegt. Ein Richtervorbehalt im Sinne des § 81 f Abs. 1 StPO wird für entbehrlich gehalten, weil er auch aus verfassungsrechtlicher Sicht nicht zwingend ist, um die Rechte des Betroffenen zu wahren. Die überragende Mehrheit der Justizministerinnen und -minister ist der Auffassung, dass auf der Grundlage dieses Berichtes zu prüfen ist, ob und gegebenenfalls in welcher Weise die DNA-Analyse zum Zweck der Identifizierung im künftigen Strafverfahren entsprechend erkennungsdienstlicher Maßnahmen genutzt werden kann.

Zu Abschnitt 2.2.2 - Das neue Landesdatenschutzgesetz

Der Landesbeauftragte für den Datenschutz kritisierte, dass einige von ihm im Rahmen des Gesetzgebungsverfahrens zur Anpassung des Datenschutzgesetzes M-V an die EG-Datenschutzrichtlinie vorgetragene Änderungswünsche nicht berücksichtigt worden waren.

a) Zulässigkeit einer Datenverarbeitung, wenn eine Rechtsform sie „zwingend voraussetzt“

Die vom Landesbeauftragten für den Datenschutz gewünschte Einschränkung der Zulässigkeitsvoraussetzungen wurde nicht vorgenommen, weil es eine Reihe von allgemeinen Ermittlungsverpflichtungen von Behörden gibt, bei denen nicht im Voraus spezifiziert werden kann, welche Daten in jedem Einzelfall benötigt werden. Das Recht, Ermittlungen anzustellen, ist jeweils begrenzt auf die konkrete gesetzliche Aufgabenstellung. Die vom Landtag beschlossene Regelung hält die Landesregierung nicht für verfassungsrechtlich bedenklich. Mit Blick auf eine mögliche Überregulierung ist nicht vorgesehen, hier eine Änderung vorzunehmen.

b) Vorabkontrolle beim Einsatz von mobilen Verarbeitungssystemen und bei Videoüberwachung

Die generelle Vorabprüfung bei der Videoüberwachung wurde deshalb nicht in das Datenschutzgesetz M-V aufgenommen, da für kritische Einsatzfelder (z. B. im Polizeibereich) spezielle Vorschriften gelten und die Videoüberwachung von Arbeitnehmern der Mitbestimmung durch die Personalräte unterliegt.

Bei den übrigen Einsatzmöglichkeiten geht die Landesregierung davon aus, dass die Kontrolle durch die behördlichen Datenschutzbeauftragten ausreichend ist.

c) *Klarstellung, das sich das Kontrollrecht des Landesbeauftragten für den Datenschutz auch auf Daten erstreckt, die unter ein besonderes Berufs- oder Amtsgeheimnis fallen*

Auf diese vom Landesbeauftragten für den Datenschutz gewünschte Klarstellung wurde im Rahmen der Novellierung verzichtet, weil sich hierfür in der Vergangenheit bis auf einen einzigen Fall keine praktische Bedeutung ergeben hatte. Im Zuge der Deregulierungsbemühungen der Landesregierung würde eine derartige Regelung kontraproduktiv sein.

Hingegen ist die Landesregierung dem Interesse des Landesbeauftragten für die Zusammenlegung der Kontrolle des Datenschutzes im öffentlichen und nicht-öffentlichen Bereich mit ihrem Entwurf eines Gesetzes zur Änderung des Datenschutzgesetzes M-V nachgekommen. Dieser wurde vom Landtag in Erster Lesung am 12. Mai 2004 behandelt und an die zuständigen Ausschüsse überwiesen.

Zu Abschnitt 2.5.1 - Novellierung des Landesverfassungsschutzgesetzes

Der Landesbeauftragte für den Datenschutz führt in seinem Bericht seine Bedenken aus, die er in einer Stellungnahme zu einem Gesetzentwurf zur Änderung des Verfassungsschutzgesetzes vorgetragen hatte.

Das Gesetzgebungsverfahren wurde am 31. März 2004 damit abgeschlossen, dass der Landtag das Gesetz mit den Stimmen der Abgeordneten aller Fraktionen verabschiedete.

Der Landesbeauftragte für den Datenschutz hatte seine Einwände bei der Beratung des Gesetzentwurfs im Innenausschuss des Landtages vorgebracht. Der Ausschuss hatte sich jedoch der Auffassung des Innenministeriums angeschlossen.

Bei der Novellierung des Landesverfassungsschutzgesetzes war eine enge Anlehnung an das Bundesverfassungsschutzgesetz und der Verweis auf die entsprechenden Passagen dort sinnvoll und ausreichend. Dadurch wurde der klare Bezug zu den Regelungen im Bundesverfassungsschutzgesetz erkennbar, die Befristung an das Bundesverfassungsschutzgesetz geknüpft und dem Gedanken der Deregulierung Rechnung getragen.

In inhaltlicher Hinsicht ist den Bedenken des Landesbeauftragten insoweit Rechnung getragen, als das Gesetz die schriftliche Begründung bei Anträgen auf Datenerhebungen durch den Leiter der Verfassungsschutzbehörde gegenüber dem Innenminister vorsieht. Die Parlamentarische Kontrollkommission wird umfassend über die durchgeführten Maßnahmen unterrichtet.

Kapitel 2 - Einzelfälle

Zu Abschnitt 2.1.2 - Fahndungsausschreibung im INPOL nicht rechtzeitig gelöscht

Bei der versehentlich unterbliebenen Löschung in der Fahndungsliste der Polizei handelte es sich um einen Einzelfall, dem nach Feststellung unverzüglich abgeholfen worden ist.

Zu Abschnitt 2.1.4 - Zu viele Steuerdaten in der Akte?

Der Landesbeauftragte für den Datenschutz kritisierte, dass die Staatsanwaltschaft mehr Daten in der Akte gespeichert hatte, als für das Ermittlungsverfahren erforderlich gewesen wäre.

In der Sache besteht Einvernehmen, dass die Staatsanwaltschaft zur Prüfung des vom Petenten gegen eine Mitarbeiterin des Finanzamtes erhobenen Vorwurfs der Verletzung des Steuergeheimnisses berechtigt war, die Steuerakte des Petenten im Ermittlungsverfahren beizuziehen. Hierbei war es unvermeidbar, dass personenbezogene Daten des Petenten zur Kenntnis genommen wurden, die keinen unmittelbaren Bezug zum Sachverhalt hatten. Die Staatsanwaltschaft muss in einem solchen Fall prüfen können, welche Unterlagen aus der Steuerakte für ihre Entscheidung relevant sind. Auch ist sie berechtigt, diese Unterlagen in die Ermittlungsakten aufzunehmen.

Der Landesbeauftragte für den Datenschutz beanstandete indes, dass vorliegend auch Unterlagen aus der Steuerakte zu den Ermittlungsakten genommen worden seien, die ersichtlich keine Relevanz für den zu prüfenden Sachverhalt gehabt hätten und daher auszusondern gewesen wären.

Die Landesregierung schließt sich der Auffassung der Staatsanwaltschaft an, nach der es im Rahmen der gebotenen umfassenden Sachverhaltserfassung bei Eingang der beigezogenen Akten nicht möglich zu beurteilen war, welche Bestandteile der Steuerakten für die bei Abschluss der Ermittlungen zu treffende rechtliche Würdigung sich als erforderlich erweisen würden und welche nicht. Im konkreten Fall hatte der Petent gerade einen aus der Aktenführung der Finanzbehörde resultierenden Tatvorwurf zur Anzeige gebracht. Zudem hatte er auf Nachfrage der Staatsanwaltschaft ausdrücklich seine Einwilligung in die Beiziehung der Steuerakten zur Erforschung des Sachverhalts erklärt. Unter diesen Umständen erscheint in diesem Einzelfall die Sachverhaltserforschung im geschehenen Umfang gerechtfertigt.

Die Aufnahme wesentlicher Teile der Steuerakten als Sonderheft zu den Ermittlungsakten diente zudem der Dokumentation der getroffenen Sachentscheidung und sicherte sowohl die fachaufsichtliche Nachprüfung, die auf Beschwerde des Petenten durchzuführen war, als auch eine etwaige Wiederaufnahme des Verfahrens.

Im Übrigen war sowohl während der aktuellen Sachbearbeitung als auch bei der späteren Aufbewahrung der Akten gewährleistet, dass nur die im Rahmen ihrer sachlichen Zuständigkeit mit dem Verfahren befassten Bediensteten Zugriff auf die in dem Ermittlungsverfahren gespeicherten Daten nehmen konnten. Damit wird ebenso wie durch die Anlage eines Sonderheftes insbesondere der Beachtung des Steuergeheimnisses Rechnung getragen.

Zu Abschnitt 2.2.2 - Das neue Landesdatenschutzgesetz (Aufsicht über Notare)

Der Landesbeauftragte für den Datenschutz forderte bereits in seinem Vierten Tätigkeitsbericht, nachdem er einer konkreten gegen einen Notar gerichteten Beschwerde nachgegangen war, im Landesdatenschutzgesetz klarzustellen, dass sich seine Kontrolle auch auf personenbezogene Daten erstreckt, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Der Landtag fasste im Zusammenhang mit der Verabschiedung des neuen Landesdatenschutzgesetzes die Entschließung, nach der er davon ausgeht, dass Notare als Träger eines öffentlichen Amtes der Kontrolle durch den Landesdatenschutzbeauftragten unterliegen.

Das Justizministerium weist darauf hin, dass die zitierte Entschließung des Landtages im Widerspruch zum notariellen Amtsgeheimnis stehe. Die Kontrollbefugnis des Landesbeauftragten für den Datenschutz über Notare würde in unzulässiger Weise in dieses Recht eingreifen. Daneben würde es zu unverhältnismäßigen Doppelkontrollen führen. Denn die Notare unterliegen bereits der Aufsicht der Landesjustizverwaltungen und der Notarkammer. Diese Aufsichtsbefugnisse umfassen auch die Prüfung der Einhaltung der Amtspflichten der Notare, insbesondere auch der Verschwiegenheitspflicht und der sonstigen Pflichten nach dem Landesdatenschutzgesetz. Die Einhaltung dieser Pflichten wird bei den regelmäßig stattfindenden Geschäftsprüfungen der Notare überwacht. Die Landesjustizverwaltung und die Notarkammer unterliegen ebenfalls dem notariellen Amtsgeheimnis, sind aber in der Lage, Datenschutzverstöße intern und angemessen zu verhindern bzw. zu ahnden.

Soweit ersichtlich, haben die unterschiedlichen Auffassungen noch nicht zu einer gerichtlichen Entscheidung darüber geführt, ob die Notare der Aufsicht des Landesbeauftragten für den Datenschutz unterliegen oder nicht.

Zu Abschnitt 2.3.1 - Nutzung polizeilicher Auskunftssysteme zur Überprüfung von Bewerbern bei der Polizei

Der Landesbeauftragte für den Datenschutz bemängelte, dass im Rahmen des Auswahl- und Einstellungsverfahrens für den mittleren, gehobenen und höheren Polizeivollzugsdienst die Bewerber u. a. unter Nutzung polizeilicher Auskunftssysteme überprüft werden.

Die einstellende Behörde, die Verantwortung für ihre Entscheidung über die Zuverlässigkeit des künftigen Vollzugsbeamten übernehmen muss, kann auf diese Erkenntnisse nicht verzichten und nutzt auch Erkenntnisse aus nicht abgeschlossenen Vorgängen, die beispielsweise im Elektronischen Vorgangsassistenten (EVA) gespeichert sind. Für die Bewertung der Geeignetheit eines Bewerbers können diese Angaben von großem Belang sein.

Die Daten, als Bestandteil der Bewerberakte, werden fünf Jahre nach Beendigung des Bewerbungsverfahrens vernichtet, wenn der Bewerber nicht in den Polizeivollzugsdienst eingestellt wurde. Diese Frist wird zur umfassenden Information des Bewerbers in die zu unterzeichnende Einverständniserklärung aufgenommen.

Die Abfrage erfolgt sofort nach bestandener Auswahlprüfung. Zu Beginn des Auswahlverfahrens liegt in keinem Fall eine Mitteilung aus den Erkenntnisdateien vor. Bei positivem Ergebnis einer solchen Abfrage wird dies dem Bewerber als Grund seiner Ablehnung mitgeteilt.

Die Auskunftssysteme explizit zu nennen, erscheint nach Auffassung der Landesregierung nicht notwendig, zumal dies für die jugendlichen Bewerber wohl kaum Aussagekraft hätte.

Zu Abschnitt 2.3.3 - Rasterfahndung in Mecklenburg-Vorpommern ergebnislos

Der Landesbeauftragte für den Datenschutz äußerte grundsätzliche Bedenken gegen die Rasterfahndung, indem er feststellte, dass fast 10.000 Einwohner von Mecklenburg-Vorpommern „in einen gigantischen Datenabgleich geraten sind, ohne dass ein verdächtiger Einwohner ermittelt wurde“.

Der Datenabgleich im Rahmen der Rasterfahndung nach den Ereignissen vom 11. September 2001 erfolgte nach bundesweit abgestimmten Kriterien, die auch für Mecklenburg-Vorpommern bindend waren. Ziel der Maßnahme war es, potentielle so genannte „Schläfer“ ohne polizeiliche oder sonstige Erkenntnisse an Hand von tätergruppenspezifischen Rastermerkmalen zu erkennen. Der Auffassung des Landesbeauftragten für den Datenschutz, es habe sich bei Rasterfahndung um ein aufwändiges Experiment gehandelt, kann nicht gefolgt werden, zumal Erkenntnisse vorlagen, dass sich zwei der Attentäter vom 11. September 2001 Ende der 90er Jahre in Mecklenburg-Vorpommern aufgehalten hatten. Zum Zeitpunkt der Anordnung der Maßnahme musste davon ausgegangen werden, dass sich möglicherweise noch weitere bisher nicht identifizierte Personen in Mecklenburg-Vorpommern befinden, die jederzeit weitere vergleichbare Anschläge verüben könnten.

Der Umstand, dass in Mecklenburg-Vorpommern kein Verdächtiger ermittelt wurde, lässt nicht den Schluss zu, dass die Rasterfahndung prinzipiell ungeeignet ist, um terroristische Gewalttäter ausfindig zu machen. Soweit andere Maßnahmen keinen Erfolg versprechen, handelt es sich bei dieser Maßnahme grundsätzlich um ein geeignetes und sinnvolles Mittel bei der Kriminalitätsbekämpfung. Im Übrigen ist es dem Charakter einer Präventionsmaßnahme immanent, dass der Erfolg dieser Maßnahme im Vorfeld nicht feststeht.

Zu Abschnitt 2.9.1 - Abbau des Datenschutzes im Telekommunikationsrecht geplant

Die Entschließungen der Datenschutzbeauftragten des Bundes und der Länder mit dem Ziel, das Datenschutzniveau zu wahren, sind der Landesregierung bekannt. Sie wurden bei den bisherigen Gesetzgebungsvorhaben im Telekommunikationsrecht berücksichtigt und sollen auch künftig bei den Stellungnahmen der Landesregierung im Bundesrat berücksichtigt werden.

Zu Abschnitt 2.10.2 - Identifikationsnummer

Der Landesbeauftragte für den Datenschutz äußerte Bedenken gegen die geplante Einführung einer eindeutigen steuerlichen Identifikationsnummer, die bereits nach der Geburt vergeben werden soll.

Nach der Rechtsprechung des Bundesverfassungsgerichts zum Gleichheitssatz (Urteil vom 27. Juni 1991, BVerfGE 84, 239, „Zinsurteil“) hat der Gesetzgeber sicherzustellen, dass alle Steuerpflichtigen durch ein Steuergesetz rechtlich und tatsächlich gleich belastet werden.

Daraus ergibt sich, dass die Finanzbehörden aufgrund ihrer gesetzlichen Befugnisse in der Lage sein müssen, die Angaben des Steuerpflichtigen zu überprüfen. Die hierfür vorhandenen gesetzlichen Befugnisse reichen hierfür im Wesentlichen zwar aus, können aber derzeit nicht optimal ausgeschöpft werden. Die Finanzbehörden müssen auch organisatorisch und technisch fähig sein, die zulässigen Überprüfungen effizient vorzunehmen. Dazu ist eine enge Zusammenarbeit der Finanzbehörden erforderlich.

Wesentliche Voraussetzung hierfür ist die eindeutige Identifizierung des Steuerpflichtigen. Die gegenwärtige Zuweisung einer Steuernummer, die nicht dauerhaft vergeben wird und daher auch nicht eindeutig ist, ist für behördenübergreifende Zwecke wenig geeignet. Ein Steuernummersystem, das die Identifikation der Steuerpflichtigen ermöglichen soll, setzt voraus, dass jeder Steuerpflichtige nur eine Nummer erhält (Eindeutigkeit), die Nummer sich während der gesamten Dauer der Steuerpflicht nicht ändert und das gesamte System dauerhaft Bestand hat (Beständigkeit, Unveränderlichkeit).

Hierbei ist zu berücksichtigen, dass die Steuerpflicht nicht an ein bestimmtes Alter gebunden ist und bereits unmittelbar nach der Geburt z. B. durch Vermögensübertragungen einsetzen kann. Deshalb wird die Forderung nach Eindeutigkeit, Beständigkeit und Unveränderlichkeit des Identifikationsmerkmals natürlicher Personen für steuerliche Zwecke nur erfüllt, wenn die zentrale Vergabe ab Geburt erfolgt.

Zu Abschnitt 2.10.2 - Abruf von Kundendaten bei Kreditinstituten

Der Landesbeauftragte für den Datenschutz wandte sich gegen die Ausweitung des bestehenden Abrufverfahrens, das es den Finanzbehörden erlaubt, bei Kreditinstituten einzelne Daten abzurufen zu Zwecken der Steuerfestsetzung und -erhebung und zur Aufgabenerfüllung anderer Behörden, wenn das zu Grunde liegende Gesetz an Begriffe des Einkommensteuergesetzes anknüpft.

Mit dem Gesetz zur Förderung der Steuerehrlichkeit vom 23. Dezember 2003 soll Steuerflüchtigen die Rückkehr zur Steuerehrlichkeit durch eine strafbefreiende Erklärung bei gleichzeitiger günstiger „Nachversteuerung“ (pauschaler Steuersatz von 25 % bzw. 35 %) erleichtert werden. Diese Möglichkeit besteht befristet für die Zeit vom 1. Januar 2004 bis 31. März 2005. Gleichzeitig mit dieser Regelung für die Vergangenheit werden auch die Überprüfungsmöglichkeiten der Finanzbehörden ab 1. April 2005 verbessert, um Steuerhinterziehung in der Zukunft zu erschweren. Denn mit dem Gesetz wurden §§ 93 Absätze 7 und 8 und 93 b der Abgabenordnung neu eingeführt. Danach haben die Finanzbehörden zukünftig die Möglichkeit, unter bestimmten Voraussetzungen Kundendaten bei Kreditinstituten abzurufen.

Nach § 24c Abs. 1 Kreditwesengesetz ist bereits jedes Kreditinstitut verpflichtet, eine stets aktuelle Datei mit den bei ihm geführten Konten und Depots sowie den dazugehörigen persönlichen Angaben der Kunden zu führen. Nach § 93 b Abgabenordnung muss diese Datei nunmehr auch für Abrufe der Finanzbehörden geführt werden. Diese können bei den Kreditinstituten über das Bundesamt für Finanzen einzelne Daten abrufen, wenn

- dies zur Festsetzung oder Erhebung von Steuern erforderlich ist und ein Auskunftsersuchen an den Steuerpflichtigen nicht zum Ziele geführt hat oder keinen Erfolg verspricht (§ 93 Absatz 7 Abgabenordnung) oder

- ein anderes Gesetz an Begriffe des Einkommensteuergesetzes knüpft und eigene Ermittlungen der für das andere Gesetz zuständigen Behörde nicht zum Erfolg geführt haben.

Der Datenschutzbeauftragte kritisierte, dass es sich hierbei um Eingriffe
- in die Vertraulichkeit der Bankbeziehungen und
- in das Recht auf informationelle Selbstbestimmung der Bankkunden handelt.

Er forderte, dass die Kreditinstitute ihre Kunden über dieses Abrufverfahren informieren, um den Eingriff transparent zu machen.

Hierzu ist festzustellen:
Deutsche Steuerzahler haben in den letzten Jahrzehnten unversteuerte Gelder ins Ausland transferiert, um möglichen Kontrollen des deutschen Fiskus zu entgehen. Darüber hinaus haben viele Steuerpflichtige in der Vergangenheit ihre Zinsen und Spekulationsgewinne aus Wertpapiergeschäften nicht erklärt, da ihnen bekannt ist, dass das „Bankgeheimnis“ gemäß § 30 a Abgabenordnung eine Entdeckung nahezu unmöglich macht.

Das Bundesverfassungsgericht hat mit Urteil vom 9. März 2004 entschieden, dass die Besteuerung von Spekulationsgewinnen aus Wertpapiergeschäften für die Jahre 1997 und 1998 verfassungswidrig ist, weil der Steueranspruch mangels Kontrollmöglichkeiten der Finanzbehörden nicht durchsetzbar ist. In der Urteilsbegründung hat das Bundesverfassungsgericht sogar ursprüngliche Bestrebungen, das Bankgeheimnis abzuschaffen, positiv bewertet. Dagegen ist der neu eingeführte Abruf von Kundendaten bei Kreditinstituten ein wesentlich geringerer Eingriff. Er wird auch dadurch eingeschränkt, dass die Finanzbehörde nicht wahllos Daten abrufen kann. Sie muss sich grundsätzlich zunächst an den Steuerpflichtigen selbst wenden. Nur wenn dieses Auskunftsersuchen nicht zum Ziele führt oder keinen Erfolg verspricht, ist der Abruf bei Kreditinstituten gestattet.

Die Gleichmäßigkeit der Besteuerung hat gemäß Artikel 3 Absatz 1 Grundgesetz Verfassungsrang. Der Abruf von Kundendaten bei Kreditinstituten ist für die Durchsetzung der Gleichmäßigkeit der Besteuerung unerlässlich.

Zu Abschnitt 2.10.3 - Steuerberaterkammer ist keine Ermittlungsbehörde

Mit einem Schreiben vom 17. Dezember 2002 hat der Landesbeauftragte für Datenschutz Mecklenburg-Vorpommern dem Finanzministerium mitgeteilt, dass dem Vorstand der Steuerberaterkammer Mecklenburg-Vorpommern eine Beanstandung nach dem Landesdatenschutzgesetz (§ 32 Abs. 1 Satz 1 Nr. 3 DSG M-V) ausgesprochen wurde.

Der Landesbeauftragte für Datenschutz erhob zu Recht den Vorwurf, die Steuerberaterkammer habe in einem bestimmten Fall personenbezogene Daten nicht beim Betroffenen, bei einem Inserenten einer Chiffre-Anzeige in einer Zeitung, sondern bei einer anderen Stelle, der Anzeigenredaktion der Zeitung erhoben. Mit Schreiben vom 2. April 2002 hatte die Steuerberaterkammer in diesem Fall die Anzeigenredaktion der Zeitung gebeten, bei einer in der Zeitung geschalteten Chiffre-Anzeige Name und Anschrift des Inserenten zu nennen, da bei dieser Anzeige der Verdacht der unerlaubten Hilfeleistung in Steuersachen und berufswidrigen Werbung vorliege.

Steuerberaterkammern sind Träger der berufsständischen Selbstverwaltung der Steuerberater und Steuerbevollmächtigte. Als Selbstverwaltungskörperschaften nehmen die Kammern selbständig und frei von fachlichen Weisungen die ihnen durch das Steuerberatungsgesetz einzeln oder allgemein zugewiesenen Aufgaben wahr. Dabei werden sie u. a. auch in Erfüllung ihrer Aufgabe zivilrechtlich tätig.
Nach der im Steuerberatungsgesetz enthaltenen Generalklausel (§ 76 Abs. 1 StBerG), wonach die Steuerberaterkammer „die beruflichen Belange der Gesamtheit der Mitglieder zu wahren hat“, leiten sich Aufgabenbereiche in verschiedene Richtungen ab.

Zu der Wahrung der Belange der Gesamtheit der Mitglieder gehört u. a. auch die Bekämpfung von Verstößen gegen das Verbot der unbefugten Hilfeleistung in Steuersachen. In diesem Bereich ist die Steuerberaterkammer für Unterlassungserklärungen als Verbände im Sinne des Gesetzes gegen den unlauteren Wettbewerb aktiv legitimiert. Die Steuerberaterkammer Mecklenburg-Vorpommern war und ist im Rahmen der gesetzlich übertragenen Aufgaben bei der wettbewerbsrechtlichen Ahndung von Verstößen gegen das Verbot der unbefugten Hilfeleistung in Steuersachen seit 1993 mit mehr als 300 abgeforderten Unterlassungserklärungen intensiv tätig. Allein in den Jahren 2000 bis einschließlich 2002 wurden 206 Wettbewerbsverfahren eingeleitet. Im Ergebnis der Wettbewerbsverfahren konnten insgesamt 66 Unterlassungserklärungen gegenüber der Steuerberaterkammer Mecklenburg-Vorpommern eingefordert werden.

In der Regel wurde bzw. wird die Steuerberaterkammer Mecklenburg-Vorpommern erst dann tätig, wenn ihr durch Steuerberater oder Steuerpflichtige Hinweise auf Personen gegeben werden, die nicht nach dem Steuerberatungsgesetz zur Hilfeleistung in Steuersachen befugt sind.

Der Weg des Auskunftsersuchens der Kammer an die Anzeigenredaktion der Zeitung beschränkte sich nur auf ganz wenige Fälle. Dieser Weg ist (datenschutz-)rechtlich nicht zulässig. Der Vorwurf des Datenschutzbeauftragten, dass ohne Rechtsgrundlage geschützte personenbezogene Daten erhoben wurden, besteht zu Recht.

In Ausübung der Staatsaufsicht des Finanzministeriums gegenüber der Steuerberaterkammer wurden am 29.01.2003 auf einer gemeinsamen Beratung mit Vertretern der OFD Rostock und der Kammer unter Beachtung der Beanstandungen des Landesbeauftragen für den Datenschutz Festlegungen getroffen, die zukünftig die Erhebung von besonders geschützten personenbezogenen Daten ohne Rechtsgrundlage durch die Kammer ausschließen sollen. Danach sind u. a. in den Fällen, bei denen der Verdacht der unerlaubten Hilfeleistung in Steuersachen gegeben ist und diejenige Person oder Vereinigung nicht erkennbar oder bekannt ist - wie in Fällen von Chiffre-Anzeigen - der OFD Rostock die Verdachtsanzeige oder die zu diesem Zweck dienenden Unterlagen durch die Steuerberaterkammer zu übermitteln.

Die OFD leitet diese Unterlagen an die zuständige Bußgeld- und Strafsachenstelle weiter. Die Steuerberaterkammer wird, soweit sie ein begründetes Interesse an einer wettbewerbsrechtlichen Verfolgung bekundet, vom Ergebnis der jeweiligen Prüfung und Entscheidung der Bußgeld- und Strafsachenstelle des Finanzamtes unterrichtet. Der Mitteilung von Namen und Adresse durch das Finanzamt an die Steuerberaterkammer steht das Steuergeheimnis nach § 30 der Abgabenordnung nicht entgegen, da es sich hierbei nicht um Besteuerungsverfahren handelt.

In einem Erörterungsgespräch mit dem Datenschutzbeauftragten am 19.02.2003 haben sich beide Seiten darauf verständigt, das Finanzministerium als Aufsichtsbehörde über Verstöße gegen das Datenschutzgesetz zukünftig rechtzeitig in Kenntnis zu setzen, damit Beanstandungen vermieden werden können.

Zu Abschnitt 2.10.4 - PROfiskal - sicheres Update, aber wie?

Der Landesbeauftragte für den Datenschutz berichtete, dass er im Rahmen seiner Beratungstätigkeit dem Finanzministerium empfohlen hatte, bei Aktualisierung der Anwenderprogramme von PROfiskal die Anpassungsarbeiten nicht jedem Endanwender zu überlassen, sondern dafür nur speziell berechtigte Administratoren einzusetzen.

Bereits mit Einführung einer neuen Produktlinie von PROfiskal (P-Linie) in 2002 wurde von Seiten des Finanzministeriums an die Software-Entwicklungs-Firma der Auftrag erteilt, mit dem Standard eine automatisierte Aktualisierung der PROfiskal-Client-Versionen an den Endgeräten innerhalb eines Kontextes zu ermöglichen, um die Kosten für regelmäßig erforderliche Updates an den Clients zu minimieren. Diese beinhaltete Änderungen in einem besonderen Verzeichnis mit den Rechten, die jeder Nutzer des Verfahrens für PROfiskal benötigt.

Grundsätzlich ist anzumerken, dass im Rahmen des Verfahrens PROfiskal auf den Endgeräten keine Daten gespeichert werden, sondern lediglich die Ein-, Ausgabe- und Maskensteuerung auf den Endgeräten unterstützt wird, um das Antwort-Zeit-Verhalten im Online-Verfahren zu optimieren. Dies setzt ein Schreibrecht auf das Verzeichnis für die PROfiskal-Anwender voraus. Alle Verarbeitungsprozesse laufen auf der zentralen Anlage in der DVZ M-V GmbH.

Die Auftragnehmerin unterstützte die Anforderung seitens des Finanzministeriums und sicherte die Lieferung eines updatefähigen Clients bereits in 2002 zu. Eine termingerechte Bereitstellung durch die Auftragnehmerin erfolgte jedoch nicht.

Die in 2003 gelieferte Erst-Version des updatefähigen Client entsprach nach einem ersten Test in der Datenverarbeitungszentrum MECKLENBURG-VORPOMMERN GmbH (DVZ M-V GmbH) weder den Anforderungen des Finanzministeriums, noch denen der DVZ M-V GmbH. Die Update-Prozedur war zwar menügeführt, für den Anwender aber viel zu kompliziert. Für jeden Nutzer wäre eine Erweiterung der Zugriffsrechte für die Durchführung eines Updates unter dem jeweiligen Betriebssystem des Endgerätes notwendig gewesen. Der Updatevorgang war in Download und Installation geteilt. Fehleingaben und gesteuerte Eingriffe in den Installationsprozess durch den Anwender wären nicht auszuschließen gewesen.

Trotz der Mängel wurde in Absprache mit der DVZ M-V GmbH der Landesbeauftragte für Datenschutz zur Prüfung der Updateprozedur herangezogen. Mit der zeitnahen Einbindung des Landesbeauftragten für Datenschutz sollten weitere zeitliche Verzögerungen bezüglich der Lieferung einer überarbeiteten und produktionsreifen Version der Updateprozedur durch die Auftragnehmerin ausgeschlossen werden.

In Absprache mit dem Landesbeauftragten für Datenschutz wurde eine Liste mit den im Sechsten Tätigkeitsbericht des Landesbeauftragten für Datenschutz dargestellten Anforderungen an die Auftragnehmerin übergeben. Die Lieferung eines Prüfsummenverfahrens durch die Auftragnehmerin steht noch aus. Der Einsatz des updatefähigen Client ist aus diesem Grunde derzeit noch gesperrt. Eine Freigabe wird nur mit Einverständnis des Landesbeauftragten für Datenschutz erfolgen.

Die Sachverhalte bezüglich der Umsetzung des Konzeptes in größeren und kleineren Behörden sind im Sechsten Tätigkeitsbericht nicht immer zutreffend dargestellt. Für die kleineren Behörden, die ohne administrative Unterstützung vor Ort auskommen müssen, wurde eine Lösung auf Basis eines Terminalservers untersucht. Prinzipiell wäre diese Lösung in der Produktion einsetzbar. Lediglich die Kostenfrage ist noch zu klären. Eine Wirtschaftlichkeitsuntersuchung mit Vergleich beider Varianten (Terminalserver und automatisiertes Update) kann jedoch erst bei Vorlage der produktionsreifen Updateversion durch die Auftragnehmerin erfolgen.

Für größere Behörden, die in der Regel mit IT-Personal ausgestattet sind, ist ein automatisiertes Update durch den jeweiligen Administrator möglich. Deshalb sollte dem PROfiskal-Anwender die Möglichkeit des Updates nicht gestattet werden. Trotz des automatisierten Updates sind aufgrund der betriebssystemseitig eingeschränkten Rechte des PROfiskal-Anwenders weiterhin administrative Arbeiten an den Endgeräten durch berechtigtes Personal notwendig. Ein automatisierter Update-Prozess durch den PROfiskal-Anwender wird sich auf Versions-Stände beschränken, in denen man mit eingeschränkten Zugriffsrechten arbeiten kann. Es wird keine prinzipielle Freigabe eines automatisierten Update-Prozesses für den Anwender in PROfiskal geben.

Zu Abschnitt 2.10.5 - Notarielle Verschwiegenheit im steuerlichen Verfahren

Im Rahmen einer Betriebsprüfung des Finanzamts sah sich ein Notar aufgrund seiner Verschwiegenheitspflicht daran gehindert, dem Betriebsprüfer Ausgangsrechnungen, Kontoauszüge und sonstige betriebliche Unterlagen vorzulegen und Einsicht in das Kostenregister zu gewähren. Das Landgericht Rostock als Aufsichtsbehörde des Notars sah in der Offenbarung ebenfalls einen Verstoß gegen die Verschwiegenheitspflicht des Berufsträgers. Das Finanzamt berief sich indessen auf die Mitwirkungspflichten eines Steuerpflichtigen im Rahmen einer Außenprüfung und hatte die Vorlage der angeforderten Unterlagen verlangt.

Die Frage des Umgangs der Finanzverwaltung mit geheimhaltungspflichtigen Daten von Berufsträgern ist im Juni 2003 von den Referatsleitern für Abgabenordnung auf der Grundlage des Urteils des BFH vom 14.05.2002, IX R 31/00, BStBl. 2002 II S. 712 erörtert worden. Vor dem Hintergrund dieser Erörterung wird im Grundsatz die Rechtsauffassung des Landgerichts Rostock und des Landesbeauftragten für den Datenschutz geteilt.

Notare unterliegen zur Wahrung ihres Berufsgeheimnisses der Pflicht zur Verschwiegenheit (§ 18 BNotO). Diese Schweigepflicht bezieht sich auf alle Angelegenheiten, die dem Notar in seiner amtlichen Eigenschaft bekannt geworden sind. Dazu gehören auch (schon) die Identität des Beteiligten und die Tatsache, dass jemand zwecks Inanspruchnahme beim Notar vorgesprochen hat. Sie gilt gegenüber jedermann, es sei denn, ausdrückliche gesetzliche Vorschriften machen eine Bekanntgabe solcher Angelegenheiten (ausnahmsweise) zur Pflicht, die hier nicht ersichtlich ist. Für alle steuerbehördlichen Verfahren sieht die Abgabenordnung dementsprechend ein allgemeines Auskunftsverweigerungsrecht für Notare vor (§ 102 Abs. 1 Nr. 3 b AO). Dieses gilt sowohl in fremden als auch in eigenen Steuerangelegenheiten und ist unabhängig von der Frage, ob die Tatsachen ihrerseits geschützt sind (wie hier nach § 30 AO).

Der Notar ist folglich auch dann berechtigt, eine Auskunft über die der Verschwiegenheitspflicht unterliegenden Angelegenheiten Dritter abzulehnen, wenn er selbst als Steuerpflichtiger um Auskunft ersucht wird, also Beteiligter i. S. d. §§ 93, 78 AO ist.
Ungeachtet dessen bleibt die Mitwirkungspflicht, die den Notar in eigener Steuersache als Beteiligten trifft, hiervon unberührt (§ 90 AO). Die zulässige Berufung auf das Auskunftsverweigerungsrecht ist dabei als sog. neutrale Tatsache zu werten, aus der keine Schlüsse zu Ungunsten des Berufsträgers gezogen werden können, wobei andererseits die dem Geheimhaltungsrecht unterliegenden Tatsachen nicht per se als nachgewiesen gelten können. Verlangt also das Finanzamt im Rahmen einer Betriebsprüfung die Vorlage von Rechnungen, betrieblichen Bankbelegen und Einsicht in das Kostenregister, besteht eine Kollision mit der Verschwiegenheitspflicht des Notars, weil aus den Belegen auch der Name und ggf. weit reichende geheimhaltungspflichtige Beteiligtenverhältnisse erkennbar sind.

Verschwiegenheitspflicht (allgemeines Persönlichkeitsrecht) und Mitwirkungspflicht (Gleichmäßigkeit der Besteuerung) haben gemäß Artikel 1 Abs. 1 i.V.m. Art. 2 Abs. 1 bzw. Artikel 3 Abs. 1 GG Verfassungsrang und stehen sich deshalb gleichwertig gegenüber. Daher ist es notwendig, gemeinsam mit den Notaren nach einer Lösung zu suchen, die beiden Rechtspositionen zu maximalem Erfolg verhilft. Dem Notar müssen dabei Möglichkeiten eingeräumt werden, seine Besteuerungsgrundlagen auch ohne Gefahr des Verstoßes gegen seine Verschwiegenheitspflicht nachweisen zu können.

Im Falle der erbetenen Einsicht in gespeicherte Daten der Buchführung bieten bereits eine Reihe verschiedener Software-Hersteller Programme zur automatischen Trennung relevanter Daten an. Damit würde dem Finanzamt eine problemlose Umsetzung seines Datenzugriffsrechts (§ 147 Abs. 6 AO) und eine Prüfbarkeit digitaler Unterlagen ermöglicht.

Darüber hinaus muss der Notar zur Erfüllung seiner Mitwirkungspflichten besondere organisatorische Vorkehrungen treffen (z. B. getrennte Aufzeichnungen der offenbarungspflichtigen Tatsachen o. ä.). Soweit und solange solche Zugriffsbeschränkungen im Notariat (noch) keinen Einzug gefunden haben, muss das Finanzamt dementsprechend die Möglichkeit in Betracht ziehen, dass der Zugriff auf verschwiegenheitspflichtige Daten bzw. Unterlagen manuell verhindert wird, etwa durch Abdeckung der auf den Belegen befindlichen Namen anderer Steuerpflichtiger oder durch Anerkennung von Fotokopien mit entsprechenden „Schwärzungen“ (BFH-Urteil vom 14.05.2002, IX R 31/00). Im Bereich der Ausgangsrechnungen wären Drittschriften denkbar, d. h. Rechnungskopien, die zum Zwecke der Vorlage für die Finanzbehörde Namen und Anschrift des Urkundsbeteiligten nicht mehr enthalten.

Nur wenn dem Betriebsprüfer tatsächliche Anhaltspunkte vorliegen, die Zweifel an der Vollständigkeit und/oder Richtigkeit derartig aufbereiteter Unterlagen des Berufsträgers begründen und die Zweifel auch nicht auf andere Weise ausgeräumt werden können, wird eine Güterabwägung ergeben, dass die Berufung auf das Geheimhaltungsrecht des Berufsträgers nach den Regeln der Feststellungslast zur Versagung des Betriebsausgabenabzugs führt, bzw. Betriebseinnahmen durch die Finanzverwaltung im Schätzungswege zu ermitteln sind.

Im konkreten Fall wird das Finanzamt nach obigen Maßstäben alle rechtlichen und tatsächlichen Möglichkeiten ausschöpfen, um sowohl dem Auskunftsverweigerungsrecht als auch dem steuerlichen Prüfinteresse gerecht zu werden.

Zu Abschnitt 2.16 - E-Government

Der Sechste Tätigkeitsbericht des Landesbeauftragten für den Datenschutz für die Jahre 2002 und 2003 widmet sich unter anderem dem vom Kabinett am 27. Januar 2004 beschlossenen „Masterplan eGovernment - Strategie der Landesregierung“. Der Masterplan wurde auf der Grundlage des „Berichtes zur Analyse der Ausgangssituation für eGovernment in der Landesverwaltung“ (Kabinettsbeschluss vom 5. August 2003) unter anderem unter Mitwirkung des Datenschutzbeauftragten des Innenministeriums erarbeitet und beschreibt organisatorische Rahmenbedingungen und technische sowie Ablauf-Standards. Er trifft Aussagen zur Zusammenarbeit mit anderen Verwaltungsebenen, zu effektiven Controllingstrukturen sowie zu Auswirkungen des elektronischen Verwaltens auf das Personal. Darüber hinaus beschreibt der Masterplan 75 Verwaltungsprozesse und leitet daraus potentielle eGovernment-Projekte her. Er bildet die informationstechnische Säule des Beschlusses der Landesregierung zu den Zielen der Reform der öffentlichen Verwaltung im Land Mecklenburg-Vorpommern ab. Der eGovernment-Masterplan selbst ist mithin kein Umsetzungskonzept. Insofern finden grundsätzliche datenschutzrechtliche Fragen zwar Berücksichtigung, sie stehen an dieser Stelle aber nicht im Vordergrund. Ein weiterführendes Umsetzungskonzept wird gegenwärtig entsprechend dem Kabinettsbeschluss vom 27. Januar 2004 unter der Federführung des Innenministeriums erarbeitet.

Ziel der Umsetzungsplanung ist es, basierend auf detaillierten Projektbeschreibungen eine Grundlage für eine Entscheidung der Landesregierung über die Realisierung konkreter Einzelvorhaben zu schaffen. Kriterien werden Finanzierbarkeit, Wirtschaftlichkeit und Minimierung von Verwaltungsaufwand ebenso sein wie der Nutzwert für Bürger und Wirtschaft als Kunden der öffentlichen Verwaltung.

Die Landesregierung sieht im Anspruch der Mitarbeiter der Verwaltung und der Bürger auf den Schutz personenbezogener Daten und im Recht auf informationelle Selbstbestimmung ein Rechtsgut von unteilbarem Wert. Sie ist mit dem Landesbeauftragten für den Datenschutz der Auffassung, dass die Umsetzung des Masterplanes neben neuen Organisationsformen auch eine neue Qualität der automatisierten Verarbeitung personenbezogener Daten erfordert. Dem gemäß wird die Landesregierung entsprechend dem in § 33 Abs. 5 Landesdatenschutzgesetz verankerten Grundsatz den Landesbeauftragten für den Datenschutz über Verfahrensentwicklungen im Zusammenhang mit der automatisierten Verarbeitung personenbezogener Daten rechtzeitig und umfassend informieren. Bereits im Vorfeld der Realisierung potentieller eGovernment-Projekte hat die Landesregierung den Landesbeauftragten für den Datenschutz in die Vorüberlegungen zur Planung der Umsetzung einbezogen.

Beispiele hierfür sind die Erarbeitung des Sicherheitsrahmenkonzeptes, das Feinkonzept für die Einführung der IP-Telefonie, die Planungen zur Einführung der neuen Programmversion des elektronischen Personal-, Organisations- und Stellenverwaltungssystems EPOS 2.0 und die Einführung eines elektronischen Travelmanagement-Systems.

Mit der Reorganisation der Landesverwaltung auf dem Gebiet der Informationstechnik und der Bildung des Referates für ressortübergreifende Angelegenheiten der Informationstechnik einerseits und der beim Staatssekretär des Innenministeriums unmittelbar angebundenen zentralen IT-Controlling-Stelle andererseits sind grundlegende Voraussetzungen für eine Straffung von Verfahren zur Planung und Durchführung von IT-Projekten sowie für einen standardisierten und wirtschaftlichen Einsatz zeitgemäßer Informationstechnik geschaffen.

In einem weiteren Schritt werden die IT-Regelwerke grundlegend überarbeitet. Die Ressortabstimmung zu dem Entwurf der an die neuen Organisationsstrukturen angepassten IT-Richtlinien mit klar verteilten Aufgaben und Kompetenzen innerhalb der Landesverwaltung steht vor dem Abschluss. Der IT-Strukturrahmen wird gegenwärtig zu einem IT-Handbuch fortentwickelt und künftig neben der Festlegung verbindlicher Standards für Hard- und Software auch Abläufe für Planung und Umsetzung von IT-Vorhaben festlegen und durch ein Sicherheitsrahmenkonzept ergänzt werden. Dies gewährleistet einen Grundschutz auf einheitlichem Niveau.

Einen weiteren Schwerpunkt sieht die Landesregierung in der Entwicklung und Einführung der Basiskomponenten. Sofern im Ergebnis dieser Planungen weitere über die in der Innenministerkonferenz beschlossenen Rahmenbedingungen zur Einführung von elektronischen Signaturen hinausgehende organisatorische Festlegungen erforderlich werden, ist eine diesbezügliche Abstimmung im interministeriellen Ausschuss für Organisationsfragen (AfO) vorgesehen.

Das Corporate Network der Landesverwaltung wird noch im Kalenderjahr 2004 einer Überprüfung durch das Bundesamt für Sicherheit in der Informationstechnik mit dem Ziel einer Grundschutz-Zertifizierung unterzogen werden. In diesem Zusammenhang ist darauf hinzuweisen, dass die zentrale Firewall bereits im Oktober 2000 durch das BSI geprüft wurde. Zur weiteren Erhöhung der Sicherheit kann der Einsatz von Terminalservern beitragen. Dies kann durch jede Dienststelle realisiert werden. Die Landesregierung prüft, ob eine landeseinheitliche, zentrale Lösung etabliert wird.

Die Landesregierung begrüßt die ausdrücklich erklärte Bereitschaft des Landesbeauftragten für den Datenschutz, die Modernisierung der Verwaltung datenschutzrechtlich zu begleiten. Die Empfehlungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die teilweise unter Mitwirkung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erarbeitet wurden, sieht die Landesregierung als weiteren wertvollen Ratgeber auf dem Weg, datenschutzgerechte und datenschutzfreundliche IT-Verfahren im Land Mecklenburg-Vorpommern zu implementieren.

Zu Abschnitt 2.18.1 - Gütesiegel für datenschutzfreundliche Produkte

Der Landesbeauftragte für den Datenschutz kritisierte, dass im Land noch keine Regelungen für ein sog. Datenschutz-Audit geschaffen wurde.

Die Situationsbeschreibung des Landesbeauftragten für den Datenschutz trifft auch heute noch zu. Die Landesregierung hält ihre abwartende Haltung nicht für bedenklich. Es ist durchaus hinnehmbar, dass mit dem Auditieren von informationstechnischen Produkten gewartet wird, bis bundeseinheitliche Standards festgelegt worden sind. Die vom LfD für bedenklich befundene abwartende Haltung wird in nahezu allen Bundesländern eingenommen. Das Land Schleswig-Holstein ist das einzige Bundesland, das eine entsprechende Rechtsverordnung vorhält.

Viel problematischer ist aus Sicht der Landesregierung die Tatsache, dass ein Bundesland für verschiedene Unternehmen gutachterlich tätig wird, für die es örtlich nicht zuständig ist, denn damit wird der Entscheidungsspielraum der örtlich zuständigen Landes-Aufsichtsbehörden wesentlich eingeengt.

Zu Abschnitt 2.20.6 - Polizeifunk - und immer noch hören alle zu

Im Bericht des Landesbeauftragten für den Datenschutz werden Ausführungen zum „Polizeifunk“ getätigt, die auf dem Stand 2002 basieren.

Im Mai 2002 wurde durch die Zentralstelle für die Vorbereitung und Einführung eines bundesweit einheitlichen digitalen Sprech- und Datenfunksystems - Digitalfunk (ZED) die Auswertung des durchgeführten Interessenbekundungsverfahrens veröffentlicht. Aufgrund der hier dargestellten möglichen Gesamtkosten für das Digitalfunknetz (ca. 5.400 Mio. € ohne Endgeräte) wurde die Innenministerkonferenz (IMK) beauftragt, die Anforderungen an ein Digitalfunksystem konkret zu benennen. In der 170. Sitzung der IMK im Juni 2002 wurde die ZED beauftragt, einen Bericht über die abschließende Beschreibung der grundlegenden Leistungsmerkmale und damit den erforderlichen Mindeststandard des geplanten Digitalfunknetzes zur Herbst-IMK vorzulegen.

Innerhalb kürzester Zeit wurde durch die „Gruppe Anforderungen an das Netz (GAN)“, die sich aus Vertretern der Länder, des Bundes und der ZED zusammensetzte, ein Papier (GAN-Papier) erstellt, das als Grundlage für ein Vergabeverfahren dienen soll. Die Kosten belaufen sich nach GAN auf ca. 3.060 Mio. € ohne Endgeräte. Darüber hinaus wurden drei mögliche Anbieter eines Digitalfunksystems in der Modifikation für Behörden und Organisationen mit Sicherheitsaufgaben (BOS) ermittelt. Auf den nachfolgenden Sitzungen der Innen-, Finanzminister- und der Ministerpräsidenten-Konferenzen wurden weitere Schritte zur Einführung des Digitalfunks beschlossen.

Im Land Mecklenburg-Vorpommern wurde Anfang 2003 die Landesprojektgruppe Digitalfunk MECKLENBURG-VORPOMMERN eingerichtet, die sich aus Vertretern der nichtpolizeilichen und der polizeilichen BOS, des Sozialministeriums und des Finanzministeriums unter Leitung des Abteilungsleiters der Polizeiabteilung des Innenministeriums zusammensetzt. Diese Projektgruppe gliedert sich in die Arbeitsgruppen Technik, Taktik, Haushalt und Recht.

Im Januar 2004 wurde im Bundesinnenministerium die Gruppe „netzwerk“-BOS eingerichtet, die die ZED ablöst und mit den Aufgaben der Planung und Durchführung des Aufbaus eines bundesweit einheitlichen Digitalfunks betraut ist.

Anfang 2004 wurde durch den Innenminister des Landes Mecklenburg-Vorpommern, nach Zustimmung durch das Kabinett, die „Dachvereinbarung zur Regelung der Zusammenarbeit beim Aufbau und Betrieb eines bundesweit einheitlichen Digitalfunksystems“ unterzeichnet.

Am 19. Mai 2004 wurden durch das Bundesbeschaffungsamt bereits Vorinformationen zum Vergabeverfahren veröffentlicht. Es ist beabsichtigt, und dies wird in der Pressemitteilung des Bundesministers des Innern vom 27. Mai 2004 nochmals unterstrichen, den Beginn des förmlichen Vergabeverfahrens zum Abschluss eines Rahmenvertrages im 4. Quartal mit der Eröffnung des Teilnehmerwettbewerbs zu starten. Darüber hinaus wurde durch den Bundesinnenminister mitgeteilt, dass mit einer funktionsfähigen Inbetriebnahme von Teilnetzen zur Fußballweltmeisterschaft im Sommer 2006 nicht mehr zu rechnen sei.

Derzeit werden die Unterlagen für das Vergabeverfahren in Zusammenarbeit zwischen der Projektgruppe „netzwerk“-BOS, dem Bund und den Ländern erstellt bzw. abgestimmt.

Zur 15. Anlage - Elektronische Signatur im Finanzbereich

Der Landesbeauftragte für den Datenschutz gab eine Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wieder, die eine Reihe von Empfehlungen enthielt.

Nach § 3 Abs. 1 Abgabenordnung haben die Steuerbehörden dafür zu sorgen, dass die Steuern gleichmäßig von allen Steuerpflichtigen erhoben werden. Die Massenverfahren des heutigen Besteuerungssystems können im Sinne dieses Anspruchs nur bewältigt werden, wenn alle technischen und organisatorischen Möglichkeiten die moderne Medien bieten nicht nur auf Seiten der Steuerverwaltung, sondern bereits von den Steuerpflichtigen genutzt werden, um Medienbrüche zu vermeiden. Hierfür ist es erforderlich, Hemmschwellen abzubauen und die Steuerbürger so einfach und schnell wie möglich an die Nutzung dieser Medien in der Kommunikation mit Steuerbehörden heranzuführen.

Ein mit zusätzlichen Kosten für die Anschaffung von Chipkarten und Lesegeräten verbundenes Verfahren würde dieser Zielrichtung entgegenstehen.

Gerade in der Öffnungsphase für neue technische Verfahren ist es notwendig, möglichst viele Teilnehmer zu erreichen und hierfür auf bekannte und bewährte Sicherheitsstandards zurückzugreifen, die sich wie die qualifizierte Signatur mit Einschränkungen im Bankenbereich beim Umgang mit sensiblen Daten bereits bewährt haben.

Kapitel 3 - Fortsetzung von Themen früherer Berichte

Zu Abschnitt 3.1 - Auslegung von Wählerverzeichnissen bei Kommunalwahlen

Um Missverständnisse zu vermeiden, wird darauf hingewiesen, dass im Jahre 2001 die öffentliche Auslegung der Wählerverzeichnisse bei Landtagswahlen durch eine beschränkte Möglichkeit der Einsichtnahme abgelöst wurde. Danach hat jeder Wahlberechtigte innerhalb der Frist zur Einsichtnahme das Recht, die Richtigkeit oder Vollständigkeit der zu seiner eigenen Person im Wählerverzeichnis eingetragenen Daten zu überprüfen. Darüber hinaus besteht auch ein Recht auf Überprüfung der Daten anderer Personen - dies jedoch nur, wenn Tatsachen glaubhaft gemacht werden, dass das Verzeichnis unrichtig oder unvollständig sein kann.

Zu Abschnitt 3.2 - Noch immer rechtswidrige Datenerhebungen bei der Hochbaustatistik

Die angesprochene Rechtsverordnung ist im Entwurf bereits dem Kabinett vorgelegt worden und soll nach Abschluss der derzeitigen Verbandsanhörung noch in diesem Jahr erlassen werden.

Bericht der Landesregierung

über die Tätigkeit der für den

Datenschutz im nicht-öffentlichen Bereich

zuständigen Aufsichtsbehörde

Berichtszeitraum: 23. Mai 2001 bis 31. Dezember 2003

Inhaltsverzeichnis

1. Einleitung

2.1 Übersicht über die Tätigkeit der Aufsichtsbehörde
2.2 Meldungen zum Register
2.3 Beschwerden
2.4 Beratung betrieblicher Datenschutzbeauftragter
2.5 Sonstige Anfragen und Beratungen
2.6 Überprüfungen vor Ort
2.7 Bußgeldverfahren
2.8 Prüfung von Verhaltensregeln

3. Einzelfälle aus der aufsichtsbehördlichen Praxis
3.1 Handels- und Wirtschaftsauskunfteien
3.2 Identifikationspapiere bei Kauf per EC-Lastschriftverfahren
3.3 Herkunft einer Anschrift für eine Werbung zur PKW-Hauptuntersuchung
3.4 Vorsicht bei Preisausschreiben
3.5 Umgang mit Mitgliederdaten eines Vereins
3.6 Anruf von einem Markt- und Meinungsforschungsinstitut oder einem Call-Center - wieso ist die Geheimnummer bekannt?
3.7 Bekanntgabe von Fehlzeiten durch Aushang - Prangerwirkung
3.8 Verbrauchsdatenablesung per Funk
3.9 Bildungsträger
3.10 Abschlussberichte von Reha-Kliniken

4. Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz

5. Zusammenarbeit mit den Datenschutzaufsichtsbehörden der Länder

6. Öffentlichkeitsarbeit (Broschüren, Faltblätter)

7. Stand der Novellierung des Datenschutzrechts

1. Einleitung

Die Landesregierung legt dem Landtag erstmalig einen Bericht über die Tätigkeit der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich vor.

Diese Berichterstattung aller für den Datenschutz zuständigen Kontrollstellen ist in der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten vorgesehen und wurde mit Gesetz vom 18. Mai 2001 (BGBl. I S. 904) durch die Einfügung des § 38 Abs. 6 in das Bundesdatenschutzgesetz (BDSG) in nationales Recht übernommen.

Grundlage für diese Aufsichtstätigkeit ist das BDSG, das die Zulässigkeiten für die Datenverarbeitung, die Rechte der Betroffenen und die Aufsicht über den Datenschutz im nicht-öffentlichen Bereich regelt. Mit Landesverordnung vom 11. Juli 1991 hat die Landesregierung die Zuständigkeit für diese Aufsicht dem Innenministerium übertragen.

Der vorliegende Bericht gibt einen Überblick über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörde im Land Mecklenburg-Vorpommern. Die Berichterstattung erstreckt sich über den Zeitraum vom 23. Mai 2001 bis zum 31. Dezember 2003. Der vorgeschriebene Berichtszeitraum von zwei Jahren wurde ausnahmsweise verlängert, weil er so an den Zeitraum für den Tätigkeitsbericht des Landesbeauftragten für den Datenschutz angeglichen werden konnte. Es ist vorgesehen, dem Landtag diesen Bericht jeweils gemeinsam mit der Stellungnahme der Landesregierung zum Tätigkeitsbericht des Landesbeauftragten für den Datenschutz vorzulegen.

Die Aufgaben dieser Aufsichtsbehörde nach § 38 BDSG werden im Land Mecklenburg-Vorpommern vom Referat II 220 des Innenministeriums wahrgenommen.
Dieses Referat ist gleichzeitig für alle Grundsatzfragen im Datenschutz zuständig.
In dieser Funktion bereitete es den Regierungsentwurf eines Gesetzes zur Änderung datenschutzrechtlicher Vorschriften vor, das vom Landtag am 13. März 2002 beschlossen wurde und nach seiner Verkündung im Gesetz- und Verordnungsblatt M-V 2002, S. 153 am 18. April 2002 in Kraft getreten ist. Das Innenministerium ist zudem federführend zuständig für die Stellungnahme der Landesregierung zum Tätigkeitsbericht des Landesbeauftragten für den Datenschutz.

2. Übersicht über die Tätigkeit der Aufsichtsbehörde

2.1 Rechte der Aufsichtsbehörde

Die Rechte der Datenschutz-Aufsichtsbehörde im Rahmen ihrer Aufgaben nach dem Bundesdatenschutzgesetz (BDSG) sind mit Blick auf die Privatautonomie der Bürger im Rechtsverkehr bewusst eingegrenzt, weil dem Staat im Verhältnis der Bürger untereinander keine weitgehenden Eingriffsrechte eingeräumt werden. Das gilt erst dann nicht mehr, wenn generelle Auswirkungen auf die Gesellschaft zu erwarten wären oder aber, wie beim Datenschutz, um dem Bürger in besonderen Situationen eine Hilfestellung zu bieten, da seine Grundrechte betroffen sein können.

Der Betroffene muss seine Rechte gegenüber einer für die Datenverarbeitung verantwortlichen privatrechtlichen Stelle zunächst selbst geltend machen.

In Fragen der Zulässigkeit einer einzelnen Datenverarbeitung oder -nutzung hat die Aufsichtsbehörde keine direkten Eingriffsmöglichkeiten. Sie kann - auch nach Prüfungen - entweder unverbindliche Empfehlungen aussprechen, die keinen Verwaltungsakt darstellen, weil nicht konkret regelnd eingegriffen wird. Sie kann, wenn sie der Überzeugung ist, es liegt eine unzulässige Datenverarbeitung vor, ein Ordnungswidrigkeitenverfahren einleiten (§ 43 Abs. 2 BDSG) oder sogar einen Strafantrag stellen (§ 44 Abs. 2 BDSG).

Die Aufsichtsbehörde kann jedoch - ähnlich wie in einem vorgerichtlichen Verfahren - den Sachverhalt aufklären und eine unverbindliche rechtliche Wertung vornehmen. Mit dieser Äußerung hat der Petent oft schon gute Argumente, die die Daten verarbeitende Stelle einlenken lassen. Die Stellungnahme der Aufsichtsbehörde kann auch z. B. im Gerichtsverfahren wie ein Gutachten verwendet werden.

Von wesentlicher Bedeutung sind deshalb die Beratung und die Sensibilisierung für den Datenschutz.

Die Datenschutzkontrolle der Aufsichtsbehörde gliedert sich in zwei Bereiche.

Sie überwacht allgemein die Datenverarbeitung bei allen nicht-öffentlichen Stellen im Lande. Ferner wird sie tätig nach Beschwerden von Betroffenen oder nach anderen Hinweisen.

Im Rahmen ihrer Prüfungstätigkeit kann die Aufsichtsbehörde
- Auskünfte verlangen (§ 38 Abs. 3 BDSG),
- Geschäftsräume zu Prüfungen und Besichtigungen betreten, Einsicht in Unterlagen nehmen, vor allem in die Übersicht des Datenschutzbeauftragten (§ 38 Abs. 4 BDSG),
- bei nicht ausreichenden Datensicherungsmaßnahmen kann sie
  a) anordnen, dass Mängel beseitigt werden,
  b) bei schwerwiegenden Mängeln kann sie u. U. Zwangsgelder festsetzen oder sogar den Einsatz einzelner Verfahren untersagen (§ 38 Abs. 5 BDSG),
- die Abberufung des betrieblichen Datenschutzbeauftragten verlangen, wenn ihm Fachkunde und Zuverlässigkeit fehlen (§ 38 Abs. 5 letzter Satz BDSG).

Anders ist die Situation in Fragen der Angemessenheit von Datensicherungsmaßnahmen (§ 38 Abs. 5 BDSG). Hier kann die Aufsichtsbehörde regelnd eingreifen, wenn sie Mängel feststellt. Gegen einen solchen anordnenden Bescheid sind der Widerspruch und ein weiteres Verwaltungsgerichtsverfahren möglich.

2.2 Meldungen zum Register

Für einige Unternehmen besteht eine Meldepflicht gegenüber der Aufsichtsbehörde. Sie bezieht sich auf Verfahren automatisierter Verarbeitung personenbezogener Daten durch nichtöffentliche Stellen, die geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung (Handelsauskunfteien und andere Auskunftsdienste) oder der anonymisierten Übermittlung speichern (Markt- und Meinungsforschungsinstitute).

Die Aufsichtsbehörde führt ein Register, in dem die nach § 4 d BDSG meldepflichtigen automatisierten Verarbeitungen erfasst werden. Es dient der Transparenz und kann von jedermann eingesehen werden.

Da diese Unternehmen bereits nach altem Recht einer Meldepflicht unterlagen, mussten die vorhandenen Angaben lediglich entsprechend der neuen Meldepflicht ergänzt bzw. angepasst werden. Insgesamt waren am Ende des Berichtszeitraumes 9 Unternehmen registriert, darunter 4 Auskunfteien, 3 Markt- und Meinungsforschungsinstitute und 2 sonstige Unternehmen.

Die Anmeldungen entsprachen größtenteils den inhaltlichen Anforderungen des § 4 e BDSG; nur geringfügige Nachbesserungen waren erforderlich gewesen.

Eines der Marktforschungsinstitute hatte auf die Aufforderung, seine Verfahrensbeschreibung zu melden, jedoch zunächst überhaupt nicht reagiert. Nach einem Hinweis auf die Möglichkeit eines Bußgeldverfahrens wurden die Angaben dann nachgereicht.

2.3 Beschwerden

Nach § 38 Abs. 1 Satz 7 i. V. m. § 21 Abs. 1 Satz 1 BDSG kann sich jedermann an die Aufsichtsbehörde wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch nicht-öffentliche Stellen in seinen Rechten verletzt worden zu sein.

Im Berichtszeitraum gingen rund 150 schriftliche Eingaben ein - zunehmend auch per E-Mail. Einige Beschwerden wurden zuständigkeitshalber an andere Bundesländer, an andere Stellen in der Landesregierung oder an den Landesbeauftragten für den Datenschutz abgegeben.

Inhaltlich reichten sie von schlichten Anfragen oder Hinweisen bis zu konkreten Beschwerden über den Umgang mit den Daten im Einzelfall.

Die Aufsichtsbehörde erreichten mehrere Meldungen von Aktenfunden. Meistens waren Betriebe betroffen, die nicht mehr existierten. Aber auch Unterlagen aus einer Arztpraxis und einem ambulanten Pflegedienst wurden gefunden. Dies ist besonders bedenklich, da durch die Verletzung des Arztgeheimnisses ein Straftatbestand erfüllt sein kann. In diesen Fällen wurde mit Hilfe der Polizei der Verursacher gefunden, der für die sichere Aufbewahrung oder sichere Vernichtung gesorgt hatte.

Die wesentlichen Problemschwerpunkte, die aufgrund von Beschwerden sichtbar geworden sind, werden unter Punkt 3 dieses Berichtes näher erläutert.

In nur wenigen Fällen waren die Beschwerden begründet und führten zu rechtlichen Bewertungen, die mit dem Hinweis auf einen möglichen Strafantrag abschlossen. Zu Strafverfahren kam es indes in keinem Fall.

Die Beschwerden betrafen vor allem Handels- und Wirtschaftsauskunfteien, aber auch die Kreditwirtschaft und den Handel. In jüngster Zeit häuften sich Beschwerden über die vermeintlich unzulässige Beobachtung durch Videokameras.

2.4 Beratung betrieblicher Datenschutzbeauftragter

Nicht-öffentliche Stellen, die personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen, haben grundsätzlich die Pflicht, einen betrieblichen Beauftragten für den Datenschutz zu bestellen (§ 4 f Abs. 1 BDSG). Dieser Beauftragte hat nach § 4 g Abs. 1 BDSG die grundsätzliche Aufgabe, auf die Einhaltung der Datenschutzregelungen in seinem Betrieb hinzuwirken. Damit er dieser Aufgabe gerecht werden kann, ist er nicht nur gemäß § 4 f Abs. 3 Satz 2 BDSG auf dem Gebiet des Datenschutzes weisungsfrei, sondern hat auch das Recht, sich in Zweifelsfällen direkt an die beim Innenministerium eingerichtete Aufsichtsbehörde zu wenden (§ 4 g Abs. 1 Satz 2 BDSG).

Zur Fortbildung der betrieblichen Datenschutzbeauftragten unterstützte die Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD) in Deutschland die Einrichtung von regionalen Erfahrungsaustauschkreisen. Auch in Mecklenburg-Vorpommern treffen sich bis zu 60 betriebliche Datenschutzbeauftragte aus Betrieben des Landes; zusätzlich beteiligen sich auch einige Vertreter von Behörden und öffentlichen Stellen. Seit Einrichtung der Aufsichtsbehörde im Jahr 1992 ist es gute Übung, die Aufsichtsbehörde zu diesen zwei bis dreimal im Jahr stattfindenden Treffen einzuladen. Auch zu den jährlichen Datenschutz-Fachtagungen ist die Aufsichtsbehörde regelmäßig eingeladen.

Die Aufsichtsbehörde wurde im Berichtszeitraum in vielen Fällen um Beratung gebeten. Diese Beratungswünsche wurden schriftlich und elektronisch, aber im Wesentlichen telefonisch vorgetragen. Im direkten Gespräch ließen sich viele Fragen datenschutzrechtlich korrekt und in der Umsetzung praktikabel lösen.

Einzelne der Aufsichtsbehörde auf diesem Wege bekannt gewordene Problemstellungen werden unter Punkt 3 dieses Berichtes näher erläutert.

2.5 Sonstige Anfragen und Beratungen

Zweimal haben verantwortliche Stellen darum gebeten, vor Ort eine Unterweisung für die Mitarbeiter durchzuführen. Dies musste abgelehnt werden, weil dies eine originäre Aufgabe des betrieblichen Datenschutzbeauftragten ist. Bei der Vermittlung von Informationsmaterial ist die Aufsichtsbehörde gern behilflich, auch kann sie auf aktuelle Seminare oder andere Fortbildungsmöglichkeiten verweisen.

2.6 Überprüfungen vor Ort

Die Prüftätigkeit musste sich aus Kapazitätsgründen beschränken auf die Beschwerdefälle, in denen die Sachverhaltsaufklärung anderweitig nicht möglich war. Das waren im Wesentlichen Beschwerden über eine vermutete unzulässige Videoüberwachung.

Nach § 6 b BDSG ist die Überwachung öffentlich zugänglicher Räume durch private Stellen nur zulässig, wenn sie
- zur Aufgabenerfüllung öffentlicher Stellen,
- zur Wahrnehmung des Hausrechts oder
- zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

In einem Beschwerdefall ging es darum, dass eine Videokamera in einem Garten von einem Mast aus schräg von oben auf das Eingangstor und den Briefkasten gerichtet war. Nachbarn hatten Sorge, dass der gesamte Bereich der Straße überwacht würde. Es stellte sich heraus, dass die Kamera fest installiert und so eingestellt war, dass zwar auch ein kleiner Teil des Fußweges vor dem Grundstück beobachtet werden konnte, aber von vorübergehenden Personen der Oberkörper oder gar der Kopf nicht gesehen werden konnte. Die Geräteausstattung ließ eine Aufzeichnung der Bilder nicht zu. Diese Art der Beobachtung zur Absicherung des Eigentums war nicht zu beanstanden.

2.7 Bußgeldverfahren

Mit der Änderung des BDSG wurde auch der Katalog der Ordnungswidrigkeiten verändert. Heute sind nicht nur die Verstöße gegen formale Vorschriften mit einem Bußgeld von bis zu 25.000,- € bewehrt, sondern auch Verstöße gegen materielles Datenschutzrecht. Eine unzulässige Datenverarbeitung kann mit einem Bußgeld von bis zu 250.000,- € bedroht sein.

Im Berichtszeitraum musste die Aufsichtsbehörde in keinem Fall ein Bußgeldverfahren einleiten.

2.8 Prüfung von Verhaltensregeln

Verhaltensregeln nach § 38 a BDSG sind Regelwerke, die sich insbesondere Berufsverbände, aber auch verbundene Unternehmen zur Förderung der Durchführung von datenschutzrechtlichen Vorschriften geben können. Sie dienen der Anpassung der gesetzlichen Regelungen an die speziellen Erfordernisse der vertretenen bzw. betroffenen Firmen sowie der freiwilligen branchenspezifischen Erhöhung der Schutzniveaus beim Umgang mit personenbezogenen Daten.

Die Aufsichtsbehörde war über die Zusammenarbeit im Düsseldorfer Kreis (s. u. Nr. 5) an einer intensiven Prüfung eines Entwurfs einer Verhaltensregel nach § 38 a BDSG beteiligt, bei der ein bundesweit tätiges Unternehmen betroffen war.

In eigener Zuständigkeit wurden keine Entwürfe geprüft.

3. Einzelfälle aus der aufsichtsbehördlichen Praxis

3.1 Handels- und Wirtschaftsauskunfteien

Oft wird die Aufsichtsbehörde gefragt, ob die Tätigkeit der Handels- und Wirtschaftsauskunfteien mit dem Datenschutzrecht vereinbar sei.

Handels- und Wirtschaftsauskunfteien bestehen seit mehr als hundert Jahren und haben ihre wirtschaftliche Berechtigung. Ihre Befugnisse sind durch das Bundesdatenschutzgesetz reglementiert, ihre Tätigkeit ist aber nicht gänzlich verboten.

Anstoß für diese Frage ist häufig die Mitteilung einer Auskunftei an einen Bürger, sie hätte Informationen über ihn gespeichert. Mit dieser Benachrichtigung kommt die Auskunftei ihrer Verpflichtung aus § 32 Abs. 1 BDSG nach. Denn das Wissen um das Vorhandensein von Daten ist Voraussetzung für die Wahrnehmung der weiteren Rechte durch den Betroffenen. Er kann Auskunft und ggf. Berichtigung, Sperrung oder Löschung verlangen.

Wer nun diese Selbstauskunft erhalten hat, stellt häufig die Frage nach den Empfängern dieser Wirtschaftsauskunft.

Grundsätzlich dürfen nur solche Stellen eine Auskunft erhalten, die ein berechtigtes Interesse haben. Dieses ist bei jeder Anfrage zu begründen. Betroffen sind also hauptsächlich Geschäftsleute. Der größte Teil des Auskunftsverkehrs betrifft ohnehin Firmen, die sich über andere Unternehmen oder Freiberufler erkundigen.

Über Privatpersonen werden relativ wenig Auskünfte erteilt - für diese interessiert sich vor allem der Versandhandel. Daneben fragen aber auch Hypothekenbanken, Handels- und Kaufhäuser, Heizöl-Lieferanten oder andere Firmen an, die Kontakte mit Privatkunden haben. Sie können eine Auskunft erhalten, wenn ein konkretes berechtigtes Interesse vorliegt. In der Regel ist dies ein Kauf, für den die Rechnung erst später erstellt wird. Für diese Auskunftsempfänger ist es in erster Linie wichtig zu wissen, dass es diese Person tatsächlich gibt und ob sie an der angegebenen Adresse wohnt; ihnen liegt oftmals nur daran, bereits bekannte Angaben bestätigt zu sehen. Außerdem interessieren sie sich dafür, ob Eintragungen im öffentlichen Schuldnerregister vorhanden sind.

Die Frage nach dem tatsächlichen Empfänger muss eine Auskunftei nur beantworten, wenn ihr eigenes Interesse an der Wahrung eines Geschäftsgeheimnisses nicht überwiegt. Zwar gehen die Auskunfteien fast immer davon aus, es gibt jedoch eine Fülle von Situationen, in denen das Geschäftsgeheimnis gar keine oder nur eine untergeordnete Rolle spielt. Im Zweifelsfall kann eine entsprechende Beschwerde bei der Aufsichtsbehörde weiterhelfen.

In einem konkreten Beschwerdefall meinte ein Betroffener, nachdem er die vorgeschriebene Benachrichtigung über die Speicherung seiner Daten erhalten hatte, hier müsse es sich um eine unzulässige Anfrage gehandelt haben, denn er sei in der letzten Zeit keinerlei Vertragsverhältnis eingegangen, die mit einem Bonitätsrisiko verbunden wären.

Die Auskunftei musste sich ihrerseits erst wieder bei ihrem Kunden über den Hintergrund der Anfrage informieren. Dabei stellte sich heraus, dass Ursache nicht der Petent selbst, sondern sein Sohn war, der nach dem Auszug aus einer Wohnung eine Restschuld nicht beglichen hatte.

In dem zugrunde liegenden Mietvertrag aber hatte sein Vater sich als Bürge zur Verfügung gestellt. Nachdem der Sohn mehrfach umgezogen und nicht mehr auffindbar war, wollte der Vermieter auf den Vater als Bürgen zurückgreifen. Insofern waren weder die Anfrage bei der Auskunftei noch die Auskunftserteilung zu beanstanden. Letztlich bedankte sich der Petent für die Aufklärung.

3.2 Identifikationspapiere bei Kauf per EC-Lastschriftverfahren

Die Datenerhebung und -nutzung ist grundsätzlich zulässig, soweit sie im Rahmen eines Vertragsabschlusses erforderlich ist oder soweit ein berechtigtes Interesse besteht. Diese ist jedoch sorgfältig abzuwägen gegen die mögliche Beeinträchtigung schutzwürdiger Belange der betroffenen Person.

Das Lastschriften-Einzugsverfahren ohne Einsatz einer PIN-Nummern-Prüfung ermöglicht eine zügige und nahezu problemlose Zahlung. Der vereinbarte Geldbetrag wird vom Konto abgebucht, ohne dass der Kunde etwas unternehmen muss. Hierbei vertraut das Kreditinstitut auf die Erklärung des abbuchenden Handelsunternehmens, ihm läge eine eindeutige Zustimmung des Kunden zu diesem Verfahren vor. Die vom Kunden unterschriebene Erklärung wird nicht weitergeleitet.

Da das Abbuchen so einfach ist, ermöglichen die Allgemeinen Geschäftsbedingungen der Kreditinstitute es den Kunden, derartige Lastschriften, von denen sie meinen, sie seien unberechtigt, ohne Angabe von Gründen zurückzubuchen. Ein Händler hat nur dann eine Möglichkeit, das ihm zustehende Geld vom Kunden erneut zu verlangen, wenn er weiß, mit wem er es zu tun hatte.

Zwar wird mit der Erklärung zur Einwilligung in das Lastschriften-Verfahren meistens auch eine zusätzliche Befreiung des Kreditinstituts vom Bankgeheimnis unterschrieben, die es dem Kreditinstitut erlaubt, dem Handelsunternehmen die Anschrift des Kunden bekannt zu machen. Nur - manche Institute verweigern dies, weil sie zu dieser zusätzlichen Dienstleistung nicht verpflichtet sind.

Außerdem gab es in der Vergangenheit erheblichen Missbrauch - vor allem mit entwendeten EC-Karten.

So bleibt dem Handel bei dieser Art der Bezahlung nichts anderes übrig, als sich beim Kauf zunächst von der Identität des Kunden zu überzeugen, aber auch sicherheitshalber seine Anschrift festzuhalten. Dies geschieht allerdings nicht bei kleinen Kaufsummen.

Da geänderte Anschriften auf dem Personalausweis nur per Aufkleber angebracht und relativ leicht zu entfernen sind, notieren einige Handelsunternehmen auch die Nummer des Personalausweises und die ausstellende Behörde.

Diese Angaben werden üblicherweise auf der Rückseite des Lastschrift-Beleges vermerkt. Diese Belege werden chronologisch gesammelt und sicher verwahrt. Die erhobenen Daten werden im Einzelfall nur dann noch genutzt, wenn tatsächlich eine Lastschrift zurückgebucht wird. Jede weitere Verwendung dieser Daten wäre unzulässig.

Unter diesen Umständen wird die Erhebung von Namen und Anschriften beim Kauf per EC-Karte ohne Verwendung der PIN-Nummer für zulässig gehalten. Das Interesse des Handelsunternehmens und das Interesse desjenigen, dem eine EC-Karte entwendet worden ist, ist als durchaus berechtigt anzuerkennen. Die Beeinträchtigung beim Kauf hingegen, wenn Name und Anschrift festgehalten werden, ist hinnehmbar, wenn ein Mindestmaß an Diskretion gewahrt bleibt.

Allerdings muss - zumindest auf Nachfrage - dem Kunden mitgeteilt werden, was mit seinen Daten geschieht. In § 4 Abs. 3 des Bundesdatenschutzgesetzes ist ausdrücklich geregelt, dass der Betroffene bei der Erhebung seiner Daten zu unterrichten ist über
- die Identität der verantwortlichen Stelle,
- die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und
- die Kategorien von Empfängern, wenn mit einer folgenden Datenübermittlung zu rechnen ist.

An diesem Punkt gab es offenbar mehrfach Mängel, weil das Kassenpersonal nicht genau informiert war. Der in einem Fall beteiligte betriebliche Datenschutzbeauftragte des Unternehmens sagte zu, in einem Rundschreiben auf diese Pflicht zur Unterrichtung noch einmal gesondert hinzuweisen.

3.3 Herkunft einer Anschrift für eine Werbung zur PKW-Hauptuntersuchung

Ein Bürger fragte an, wie einer werbenden Firma sein Name, seine Anschrift und die Tatsache bekannt werden konnte, dass sein PKW zu einer bestimmten Zeit zur Hauptuntersuchung dem TÜV vorgeführt werden musste.

Die Nachforschungen haben ergeben, dass der Firmenzentrale in Hessen die verwendeten Anschriften von einem der großen Adressenvermittler zu einer einmaligen Nutzung überlassen worden waren. Es stellte sich heraus, dass der Bürger selbst die zusätzlichen konkreten Daten dorthin geliefert hatte. Das geschah auf dem Wege einer sog. life-style-Befragung, die dieser Adressenvermittler von Zeit zu Zeit in großem Stil durchführt. Dabei wird in einem umfangreichen Fragebogen nach einer ganzen Reihe von Verbrauchergewohnheiten gefragt und gleichzeitig eine Verlosung angeboten. Unter anderem war auch nach der Anschaffung des genutzten PKW gefragt, woraus sich der nächste Termin für die Hauptuntersuchung leicht ableiten ließ.

Dieser Fall mag ein Beispiel dafür sein, dass jederzeit genau überlegt werden sollte, wem man zu welchem Zweck seine Daten übermittelt und was möglicherweise mit diesen Daten geschehen kann. Aber selbst, wenn die Daten bereits bei einer anderen Stelle sind, kann man sich noch wehren: Die weitere Verwendung einer Adresse zu Werbezwecken kann man unterbinden, indem man sich in die sog. Robinsonliste aufnehmen lässt.

Diese Robinsonliste wird vom Deutschen Direkt-Marketing-Verband geführt, an den man sich telefonisch (07156 - 95 10 10) oder schriftlich (Postfach 1401, 71243 Ditzingen) wenden kann. Die Verbandsmitglieder - das ist ein großer Teil der gesamten Branche - gleichen Adressen, die sie von anderen übernommen haben, mit dieser Robinsonliste ab, um sie herauszuselektieren und nicht zu verwenden.

3.4 Vorsicht bei Preisausschreiben

Ein heute nicht mehr existierendes Unternehmen hatte in der Weise für seine Dienstleistungen geworben, dass es „Gewinnmitteilungen“ an eine Vielzahl von Empfängern im ganzen Bundesgebiet versandt hatte. In einer ganzen Reihe von Beschwerden wurde vorgetragen, unaufgefordert Angebote erhalten zu haben. Offen war die Frage, woher diese Anschriften stammten. Beanstandet wurde auch, dass das Unternehmen auf Auskunfts- und Löschungsbegehren nicht reagierte.

Die Werbung war so gestaltet, dass die Verbraucherzentrale grundsätzlich und öffentlich geraten hatte, auf diese Werbung nicht zu reagieren.

Bei einem Kontrollbesuch erläuterte der Geschäftsführer, die Anschreiben würden nur dazu verwendet, die Interessenten mit Hilfe eines Agenten an ein Reiseunternehmen weiter zu vermitteln. Die genutzten Adressen hätte er von einem der großen Adressenverlage auf der Grundlage der marktüblichen Verträge zur einmaligen Nutzung erhalten. Er sei davon ausgegangen, dass diese Adressen vorher mit der sog. Robinsonliste abgeglichen worden sind. In den Fällen, in denen sich jemand gegen die Nutzung seiner Adresse gewandt hatte, hätte er diese sofort gelöscht und seinen Adressenlieferanten davon informiert.

Die Überprüfung vor Ort ergab, dass die Daten aller Beschwerdeführer tatsächlich im Datenbestand nicht mehr vorhanden waren.

Da ein Gewerbeuntersagungs-Verfahren ohnehin kurz vor seinem Abschluss stand, wurden seitens der Aufsichtsbehörde keine weiteren Maßnahmen erforderlich.

3.5 Umgang mit Mitgliederdaten eines Vereins

Einige Beschwerden bezogen sich auf die Übermittlung von Adressen durch Vereine an werbende Unternehmen.

Dazu ist anzumerken, dass eine Datenübermittlung zu Werbezwecken durch das BDSG zwar erleichtert ist, aber nicht völlig am Willen des Betroffenen vorbei vorgenommen werden sollte. In § 28 Abs. 3 Nr. 3 BDSG wird trotz einer generellen Zweckbindung von erhaltenen Mitgliederdaten erlaubt, Anschriften zu Werbezwecken zu übermitteln, ohne dass der Betroffene seine Zustimmung dazu geben muss. Diese Übermittlung hat nach dieser Vorschrift zu unterbleiben, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss dieser Übermittlung hat. Eine konkrete Prüfung ist demnach nicht erforderlich. Deshalb wird in der Werbewirtschaft üblicherweise davon ausgegangen, der Betroffene hätte keine Einwände. Tatsächlich hat jeder nach § 28 Abs. 4 BDSG die Möglichkeit, bei allen Stellen, die seine Anschrift speichern, einen Widerspruch gegen die Übermittlung und Nutzung für die Werbung auszusprechen. Dieser Widerspruch bedeutet, dass ihre Anschrift nicht mehr weitergegeben werden darf.

Da dieses Widerspruchsrecht relativ unbekannt ist, wird es kaum genutzt.

3.6 Anruf von einem Markt- und Meinungsforschungsinstitut oder einem Call-Center - wieso ist die Geheimnummer bekannt?

Ein Bürger beklagte sich darüber, von einem Call-Center keine ihm zustehende Selbstauskunft erhalten zu haben.

Eine Recherche beim Datenschutzbeauftragten des Unternehmens ergab, dass in diesem Falle die Telefonnummer nicht aus einem Verzeichnis entnommen worden war, sondern durch ein Computerprogramm per Zufallsgenerator entstanden war. Dieses Verfahren wird von den großen Markt- und Meinungsforschungs-Instituten vermehrt eingesetzt, um möglichst alle subjektiven Einflüsse auszuschalten. Da über diesen Bürger persönlich keine Daten bekannt oder gar gespeichert waren, konnte man ihm auch die gewünschte Auskunft nicht erteilen.

Eine Verletzung von Datenschutzvorschriften war demnach nicht festzustellen.

3.7 Bekanntgabe von Fehlzeiten durch Aushang - Prangerwirkung

Von einer Mitarbeiterin eines Betriebes wurde die Aufsichtsbehörde darüber informiert, dass eine Übersicht an einem Informationsbrett angebracht worden war, aus der hervorging, welche/r Mitarbeiter/in wann wegen Krankheit fehlte. Dieses Informationsbrett konnte auch von Außenstehenden gelesen werden.

Der Geschäftsleitung wurde mitgeteilt, dass in diesem Aushang eine Datenübermittlung an eine Vielzahl von unbekannten Empfängern zu sehen war, die nach § 28 Abs. 1 Nr. 1 BDSG nur zulässig wäre,
- wenn ein Gesetz sie zuließe,
- wenn sie im Rahmen eines Vertragsverhältnisses mit den Betroffenen erforderlich wäre oder
- wenn die betroffenen Personen dazu die Einwilligung gegeben hätten.

Alle drei Voraussetzungen dürften nicht erfüllt gewesen sein. Die Zulässigkeitsvoraussetzungen nach § 28 Abs. 1 Nr. 2 und 3 schieden ebenfalls aus, denn dem Interesse des Betroffenen kommt jeweils ein höheres Gewicht zu. Deshalb lag offenbar eine unzulässige Datenübermittlung vor, die ein Ordnungswidrigkeiten-Verfahren nach sich ziehen könnte (§ 43 Abs. 2 Nr. 1 BDSG). Es stellte sich sehr schnell heraus, dass dieses Vorgehen nicht im Interesse der Geschäftsleitung lag und hier offenbar eine Mitarbeiterin „übers Ziel hinausgeschossen war“. Da die Geschäftsleitung sofort für die Entfernung gesorgt hatte, waren keine weiteren förmlichen Schritte erforderlich.

3.8 Verbrauchsdatenablesung per Funk

Zwischen einer Wohnungsbaugenossenschaft und einer Firma wurde ein Service-Vertrag geschlossen, mit dem Ziel, die Ablesungen vorzunehmen und die Verbrauchsdaten für die Abrechnung mit den Mietern vorzubereiten. Die Verbrauchsdaten sollten zweimal im Monat abgelesen und bei der Servicefirma intern gespeichert werden.

Dazu wurde vorher jedem Mieter eine Nutzernummer zugeteilt - und nur diese sollte mit den Verbrauchszahlen auf dem Funkwege der Servicefirma übermittelt werden. Erst dort sollten die abgelesenen Verbrauchszahlen einem bestimmten Mieter zugeordnet werden können.

Zur Jahresabrechnung sollten die Daten an die Wohnungsbaugenossenschaft geliefert werden. Vorbereitend sollten die zwischenzeitlichen Mieterwechsel gemeldet werden, damit die Verbrauchszahlen korrekt dem ausgezogenen und dem neuen Mieter zugeordnet werden können.

Datenschutzrechtlich von Bedeutung war nur, dass die Mieter genau über das Verfahren und die beteiligten Stellen informiert werden, bevor sie einer entsprechenden Vereinbarung zustimmen.

Nach der Heizkostenverordnung ist der Vermieter gehalten, ein einheitliches Mess- und Abrechnungsverfahren einzusetzen. Er ist jedoch nicht auf die Zustimmung aller einzelnen Mieter angewiesen. Es genügt, wenn er allen Mietern die Veränderungen unter Angabe der durch die Umstellung entstehenden Kosten mitteilt und nicht mehr als die Hälfte der Mieter dem Verfahren widersprechen.

Unter diesen Voraussetzungen bestehen keine Bedenken gegen den Einsatz des Ablese- und Meldeverfahrens mit Hilfe der Funkanlage.

3.9 Bildungsträger

Von einem privaten Träger der arbeitsamtsgeförderten beruflichen Bildung wurde den Teilnehmern ein Fragebogen ausgehändigt, der sich nicht nur mit der Vorbildung oder den Zukunftsvorstellungen beschäftigte, sondern auch mit der Familie und der Wohnsituation.

Die Mutter eines Teilnehmers wandte sich an die Aufsichtsbehörde und meinte, durch diese Befragung „hinter dem Rücken“ in ihrem informationellen Selbstbestimmungsrecht beeinträchtigt zu sein.

Eine Rückfrage beim Bildungsträger ergab, dass dieser Fragebogen den begleitenden Sozialpädagogen und Praktikumsbetreuern ausgehändigt würde, damit sie die erforderlichen Einzelgespräche zur Feststellung der persönlichen Situation und der Neigungen und Interessen besser vorbereiten könnten. Eine weitere Verarbeitung dieser Angaben sei ausgeschlossen, da sie unter die Schweigepflicht der Sozialpädagogen falle. Es hätte sich aber herausgestellt, dass die Fragen zur familiären Situation nur eine geringe Bedeutung haben. Deshalb würden diese Angaben nicht mehr verwendet werden.

Mit dieser Auskunft konnte der Petentin geholfen werden.

3.10 Entlassungsberichte von Reha-Kliniken

Ein Patient einer privatrechtlichen Reha-Klinik beschwerte sich darüber, dass der Entlassungsbericht dem Medizinischen Dienst der Krankenkassen weitergegeben worden war, obwohl er dieser Absicht eindeutig widersprochen hatte.

Auf Anforderung der Aufsichtsbehörde beschrieb die Datenschutzbeauftragte der Klinik zusätzliche Einzelheiten über die technische Verarbeitung von Patientendaten. Sie erläuterte, dass bei der Aufnahme eines Patienten seine Grunddaten erfragt und in den Rechner eingegeben würden. Dabei handele es sich um Namen, Geburtsdatum, Anschrift, Krankenkasse, Versicherungsnummer, Aufnahmedatum, ein (vorläufiges) Entlassungsdatum und eine hausinterne Patientennummer.

Neben dem Abrechnungsverfahren mit den Krankenkassen würden alle Vorgänge über die Patienten nur in den Patientenakten festgehalten. Hierin befänden sich auch über sie die o. g. Erklärung, die Abforderung vom Medizinischen Dienst der Krankenkassen und der Entlassungsbericht.

Da die Anwendung des Bundesdatenschutzgesetzes eingeschränkt ist auf Daten, die in automatisierten Verfahren oder in manuellen Dateien verarbeitet werden, lag eine Ordnungswidrigkeit oder ein Straftatbestand nach §§ 43 und 44 des Bundesdatenschutzgesetzes nicht vor.

Daneben ist jedoch festzustellen, dass es andere Auskunftsrechte gibt. So ist z. B. in der Berufsordnung für die Ärztinnen und Ärzte in Mecklenburg-Vorpommern in § 10 Abs. 2 festgeschrieben, dass der Arzt dem Patienten grundsätzlich Einsicht in die Krankenakten zu gewähren hat. Auf Verlangen sind ihm - gegen Kostenerstattung - Kopien herauszugeben. Ausnahmen können nur gelten, wenn konkrete Gründe für eine Selbstgefährdung des Patienten bestehen.

Verstöße gegen die Berufsordnung werden von der Ärztekammer Mecklenburg-Vorpommern verfolgt.

4. Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz

Die Abstimmung zwischen dem Landesbeauftragten für den Datenschutz und der Aufsichtsbehörde in Bereichen, in denen von einer Beschwerde zugleich öffentliche und nichtöffentliche Stellen betroffen waren und in Bereichen, in denen im öffentlichen wie im nichtöffentlichen Bereich parallele Fragestellungen zu bearbeiten sind, war im Berichtszeitraum von vertrauensvoller Zusammenarbeit geprägt.

Mit der Änderung des Landesdatenschutzgesetzes (DSG M-V) wurde zur Zuständigkeit des Landesbeauftragten für den Datenschutz in der Vorschrift des § 2 Abs. 2 DSG M-V klargestellt, dass alle von öffentlichen Stellen beherrschten juristischen Personen oder sonstigen Vereinigungen des privaten Rechts, soweit sie Aufgaben der öffentlichen Verwaltung wahrnehmen, selbst auch als öffentliche Stellen zu betrachten sind und damit auch in den Anwendungsbereich des Landesdatenschutzgesetzes fallen. Dieser Umstand wurde nicht auf Anhieb von allen betroffenen Stellen, vor allem nicht von städtischen Wohnungsbaugesellschaften verstanden, die in der Rechtsform einer GmbH geführt wurden.

5. Zusammenarbeit mit den Datenschutzaufsichtsbehörden der Länder

Die Aufsichtsbehörden aller Bundesländer für den Datenschutz im nicht-öffentlichen Bereich arbeiten seit vielen Jahren erfolgreich im „Düsseldorfer Kreis“ zusammen, um eine möglichst gleiche Anwendung des Bundesdatenschutzgesetzes in den Ländern zu erreichen. Hierbei handelte es sich ursprünglich um einen Unterausschuss des Arbeitskreises II der Innenministerkonferenz. Seit aber in den Bundesländern vermehrt die Aufgabe der Aufsichtsbehörden auf die Landesbeauftragten übertragen worden sind, ist wegen der besonderen Stellung der Landesdatenschutzbeauftragten der Status nicht mehr eindeutig.
Die Referenten der Länder-Datenschutz-Aufsichtsbehörden treffen sich jährlich zweimal, um die wichtigsten Fachfragen der Datenschutzaufsicht im nicht-öffentlichen Bereich zu diskutieren und abgestimmte Lösungen zu entwickeln. Dies ist insbesondere dann von Bedeutung, wenn sich die Beratungs- und Kontrolltätigkeit der Aufsichtsbehörden auf länderübergreifend handelnde Wirtschaftsunternehmen oder eine ganze Branche bezieht.

Mecklenburg-Vorpommern ist zusätzlich beteiligt an der „Arbeitsgruppe SCHUFA/Handels- und Wirtschaftsauskunfteien“ des Düsseldorfer Kreises, die sich ebenfalls zweimal jährlich trifft.

Die weiteren Arbeitsgruppen befassen sich mit der Versicherungswirtschaft, der Kreditwirtschaft, der Telekommunikation, den Tele- und Mediendiensten, dem internationalen Datenschutz.

6. Öffentlichkeitsarbeit (Broschüren, Faltblätter)

Auf die Erstellung eigener Broschüren oder Faltblätter hat das Innenministerium verzichtet; es sind aber zurzeit folgende Broschüren von anderen Stellen verfügbar:

- Merkblatt zum Adressenhandel,
- Merkblatt über Handels- und Wirtschaftsauskunfteien,
- BfD - Info 1 (Text und Erläuterungen zum Bundesdatenschutzgesetz).

Bestelladresse:
Innenministerium Mecklenburg-Vorpommern
19048 Schwerin

Darüber hinaus können Materialien bei anderen Stellen über das Internet unter www.datenschutz.de, vor allem beim Bundesbeauftragten für den Datenschutz bestellt werden. Eine spezielle Suchmaschine hilft, gezielte Informationen zu vielen Themen zu finden.

7. Stand der Novellierung des Datenschutzrechts

Nachdem die EU-Datenschutzrichtlinie 95/46/EG vom 24. Oktober 1995 nunmehr sowohl im Bund als auch in allen Ländern umgesetzt worden ist, arbeitet die Bundesregierung bereits an der sog. zweiten Stufe der Novellierung des Bundesdatenschutzgesetzes.

In Vorbereitung dieser zweite Stufe der Novellierung des Bundesrechtes wurde am 12. November 2001 ein Gutachten „Modernisierung des Datenschutzrechts“ vorgelegt, das von Prof. Roßnagel, Prof. Pfitzmann und Prof. Garstka im Auftrag des Bundesministeriums des Innern erstellt worden war.

Dieses Gutachten kommt zum Ergebnis, dass das Datenschutzrecht einer umfassenden Modernisierung bedarf, da es an überkommenen Formen der Datenverarbeitung orientiert, stärker auf den öffentlichen als auf den privaten Bereich gerichtet, überreguliert, uneinheitlich und schwer verständlich ist.

Ein modernes Datenschutzrecht sollte bereichsunabhängig ein Mindestschutzniveau festlegen und der betroffenen Person Kontroll- und Mitwirkungsmöglichkeiten anbieten. Es sollte auf einer einfachen Struktur von Erlaubnistatbeständen aufbauen. Ein genereller Erlaubnistatbestand sollte die Datenverarbeitung immer dann für zulässig erklären, wenn offenkundig keine Beeinträchtigung der betroffenen Person zu erwarten ist.

Die Einwilligung, der Vertrag und der Antrag sollen zum vorrangigen Legitimationsgrund für die Datenverarbeitung werden. Dabei muss das Datenschutzrecht die Freiwilligkeit der Einwilligung sichern.

Im nicht-öffentlichen Bereich sollte Datenverarbeitung ohne Einwilligung des Betroffenen nur in gesetzlich eng umgrenzten Fällen möglich sein.

Im öffentlichen Bereich soll die Datenverarbeitung wie bisher dann zulässig sein, wenn sie erforderlich ist, um gesetzliche Aufgaben der Verwaltung zu erfüllen. Im nicht gesetzlich gebundenen Bereich tritt die Einwilligung hinzu.

Ein modernes Datenschutzrecht sollte auf einem allgemeinen Gesetz gründen, das bereichsspezifischen Regelungen vorgeht.

Dieses soll einheitliche Grundsätze für den öffentlichen und nicht-öffentlichen Bereich sowie Regelungen zur Technikgestaltung, zur Datensicherung, zur Datenschutzorganisation, zur Datenschutzkontrolle und zur Selbstregulierung enthalten.
Spezialregelungen in bereichsspezifischen Gesetzen sollen nur noch Ausnahmen von den allgemeinen Regelungen enthalten.

Zusätzlich wurden weitere Empfehlungen ausgesprochen:
- Das jeweilige technisch-organisatorische System soll nur zu der Datenverarbeitung in der Lage sein, zu der es rechtlich auch ermächtigt ist (Systemdatenschutz).
- Die technisch-organisatorischen Verfahren sind so zu gestalten, dass - soweit möglich - auf die Verarbeitung von Daten verzichtet wird oder die zu verarbeitenden Daten keinen Personenbezug aufweisen und den Betroffenen muss Gelegenheit gegeben werden, anonym oder pseudonym zu handeln (Datenvermeidung und präventiver Datenschutz).
- Den Betroffenen sind einfach zu bedienender Tools bereitzustellen für den Schutz vor Ausspähung von Daten (Selbstdatenschutz).

Damit soll das Datenschutzrecht insgesamt eine umfassende Modernisierung erfahren. Neben einer grundsätzlichen Neustrukturierung zur Förderung der Verständlichkeit und damit der Anwendbarkeit des Datenschutzrechts soll auch den in den letzten Jahren eingetretenen grundlegenden Veränderungen der technischen Rahmenbedingungen Rechnung getragen werden.

Eine solche inhaltliche und formale Neustrukturierung des Bundesrechts auf dem Gebiet des Datenschutzes wird auch Änderungsbedarf im landesrechtlichen Bereich nach sich ziehen. Eine nächste Novellierung auch des Landesdatenschutzgesetzes ist damit vorgezeichnet.

Da der Datenschutz nahezu alle Lebensbereiche berührt, sind viele bereichsspezifische Regelungen in Gesetzen und Verordnungen aller Ressorts des Bundes betroffen. Die Vorbereitungen beim Bund dauern zurzeit noch an.