**Bericht der Landesregierung**

über die Tätigkeit der für den

**Datenschutz im nicht-öffentlichen Bereich**

zuständigen Aufsichtsbehörde

an den Landtag des Landes

Mecklenburg-Vorpommern

Berichtszeitraum: 23. Mai 2001 bis 31. Dezember 2003

**Gliederung**

## 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 Aufsichts-

behörde kann auch z.B. im Gerichtsverfahren wie ein Gutachten verwendet werden.

Von wesentlicher Bedeutung ist 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 nicht-öffentliche 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 wurde 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 Einhal-

tung 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 betrieblichen 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 § 6b 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 hatte 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 ggfs. Berichtigung, Sperrung oder Löschung verlangen.

Wer nun diese Selbstauskunft erhalten hat, stellt häufig die Frage nach dem 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 zugrundeliegenden 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 werbende 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. Robinson-Liste 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 seien 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 Betroffenen 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.

Meine 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 Vertragverhältnisses 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 Nrn. 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 arbeitsamtsgefördeten 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 nicht-öffentliche Stellen betroffen waren und in Bereichen, in denen im öffentlichen wie im nicht-öffentlichen 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 Kon-

trolltätigkeit 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 z.Zt. 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. zweite 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 der 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 zur Zeit noch an.