Landtag Brandenburg **Drucksache 3/2985**
3. Wahlperiode

Bericht
der Landesregierung

Neunter Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörde an den Landtag des Landes Brandenburg

Datum des Eingangs: 02.07.2001 / Ausgegeben: 04.07.2001

0. Einleitung

Der Bericht gibt einen Überblick über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörde im Land Brandenburg.
Die Berichterstattung erstreckt sich über den Zeitraum vom 1. Januar 2000 bis zum 31. Dezember 2000.

1. Übersicht über die Kontrolltätigkeit

1.1 Meldungen zum Register

Die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich führt das Register nach § 32 Abs. 2 Bundesdatenschutzgesetz (BDSG) .
Gemäß § 32 Abs. 1 BDSG haben Stellen, die personenbezogene Daten geschäftsmäßig

1. zum Zwecke der Übermittlung speichern (§ 29 BDSG),
   (z.B. Wirtschaftsauskunfteien, Detekteien)

2. zum Zwecke der anonymisierten Übermittlung speichern (§ 30 BDSG)
   (z.B. Markt- und Meinungsforschungsinstitute) oder

3. im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen (§ 11 BDSG),
   (z.B. Rechenzentren, Büros für Lohn- und Gehaltsabrechnungen, Datenträgervernichtungsfirmen)

sowie ihre Zweigniederlassungen und unselbständigen Zweigstellen die Aufnahme und Beendigung ihrer Tätigkeit der zuständigen Aufsichtsbehörde innerhalb eines Monats mitzuteilen.

Die Unternehmen unterliegen einer regelmäßigen Kontrolle durch die Aufsichtsbehörde gemäß § 38 Abs. 2 BDSG.

In diesem Berichtszeitraum haben sich insgesamt 35 Unternehmen erstmalig gemäß § 32 Abs. 1 BDSG zum Register angemeldet.

Bei den registrierten Firmen ist folgender Stand erreicht:

Gesamt:	163
Auskunfteien:	9
Markt- und Meinungsforschungsinstitute:	3
Dienstleistungsunternehmen:	151
davon:	
DV im Auftrag und Schreibbüros:	119
Datenträgervernichtungsfirmen:	24
Mikroverfilmer:	8

1.1.1 Änderung der Meldepflicht durch neues BDSG

Der Entwurf des BDSG sieht in §§ 4 d, 4 e einige Änderungen hinsichtlich der Meldepflicht vor. In Zukunft wird die Meldepflicht entfallen, wenn die verantwortliche Stelle einen Datenschutzbeauftragten bestellt hat. Auch wenn die Datenverarbeitung nicht von einem betrieblichen Datenschutzbeauftragten überwacht wird, hat dies nicht zwingend eine Meldepflicht zur Folge. Sie besteht nämlich nicht, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, damit höchstens vier Arbeitnehmer beschäftigt sind und entweder eine Einwilligung der Betreffenden vorliegt oder die Datenverarbeitung der Zweckerreichung eines Vertragsverhältnisses dient.
Eine Erleichterung soll auch für Unternehmen geschaffen werden, die personenbezogene Daten im Auftrag verarbeiten.
Hingegen sind Stellen, die personenbezogene Daten zum Zwecke der Übermittlung oder zum Zwecke der anonymisierten Übermittlung speichern (Adresshändler, Auskunfteien, Markt- und Meinungsforschungsinstitute) verpflichtet, die automatisierte Erhebung, Verarbeitung oder Nutzung personenbezogener Daten selbst dann zu melden, wenn sie einen Datenschutzbeauftragten bestellt haben oder weniger als fünf Arbeitnehmer beschäftigt sind.
Der Inhalt der Meldungen wird sich nicht wesentlich ändern.

1.2 Beschwerden und Anfragen

Im Berichtszeitraum gingen 37 schriftliche Beschwerden sowie 28 Informationsanfragen bei der Aufsichtsbehörde ein, welche dann ordnungsgemäß bearbeitet wurden.
Weitergeleitet an die betreffenden Bundesländer wurden die Beschwerden und Anfragen, die nicht in die Zuständigkeit der Aufsichtsbehörde Brandenburgs fielen.
Telefonisch eingegangene Anfragen wurden nicht gesondert erfasst.
Unter Ziffer 2.3 werden nähere Ausführungen zu einigen Beschwerden und Anfragen gemacht.

2. Kontrolltätigkeit der Aufsichtsbehörde

2.1 Übersicht über die geprüften Unternehmen

Im Berichtszeitraum hat die Aufsichtsbehörde bei 10 Unternehmen, die im Register eingetragen sind, Prüfungen nach § 38 Abs. 2 BDSG durchgeführt.
Neben einer Auskunftei gehörten die anderen Firmen zur Kategorie Auftragsdatenverarbeitung. Unter anderem waren dies zwei Archive und drei Schreibbüros.

2.1.1 Ergebnisse und Empfehlungen aus den Überprüfungen

Wie im zurückliegenden Berichtszeitraum konnten keine gravierenden Verstöße gegen Datenschutzbestimmungen festgestellt werden.

Bei einzelnen Unternehmen wurde auf die Vertragsgestaltung mit den Kunden hingewiesen. In diesem Zusammenhang wurde auf den § 11 Abs. 2 Satz 1 BDSG verwiesen.
Des Weiteren musste bei einer Firma darauf aufmerksam gemacht werden, dass die beschäftigte Angestellte auf das Datengeheimnis gem. § 5 BDSG nachträglich verpflichtet wird. Dies wurde umgehend nachgeholt.
Bei einem weiteren Unternehmen wurde festgestellt, dass der Geschäftsführer der Firma gleichzeitig der betriebliche Datenschutzbeauftragte ist. Hier wurde auf den § 36 Abs. 3 BDSG verwiesen.
Ein anderes Unternehmen hatte die Sicherheitsmaßnahmen des Büros, welches sich im Erdgeschoss befindet, nicht ausreichend realisiert. Seitens der Aufsichtsbehörde wurde empfohlen, Bewegungsmelder im Büro sowie Außenjalousien anzubringen. Gleichzeitig wurde angeregt, Liefer- und Begleitscheine zu verwenden, da der Transport zwischen dem Auftraggeber und Auftragnehmer durch eine Fremdfirma erfolgt.

Bei einer anderen Firma sind die Auftraggeber öffentliche Stellen und daher hat das private Unternehmen die Vorschriften des Brandenburgischen Datenschutzgesetzes (BbgDSG) zu beachten. Bei der Überprüfung des Unternehmens wurde das Fehlen von vertraglich geregelten Unterauftragsverhältnissen kritisiert. Die Vertreter des Unternehmens wurden darauf hingewiesen, dass mit den entsprechenden Firmen ebenfalls Verträge abzuschließen sind, die den Anforderungen des BbgDSG entsprechen müssen. Beim Vertrag mit einer Computerfirma zur Fernwartung ist vor allem § 11a BbgDSG mit seinen Anlagen zu beachten.

Als Hinweise wurden u.a. gegeben :
- die Verpflichtungen der Mitarbeiter gemäß § 5 BDSG nach Aufnahme der Geschäftstätigkeit vorzunehmen sowie
- die Bestellung eines Datenschutzbeauftragten nachzuholen (Verweis auf den § 36 Abs. 1 BDSG, wonach private Stellen, die personenbezogene Daten verarbeiten und mindestens 5 Mitarbeiter beschäftigen, innerhalb eines Monats nach Tätigkeitsaufnahme einen Beauftragten für den Datenschutz schriftlich zu bestellen haben. Das gleiche gilt, wenn personenbezogene Daten auf andere Weise verarbeitet werden und damit in der Regel mindestens 20 Arbeitnehmer beschäftigt sind).

2.2 Kontakte und Anfragen von betrieblichen Datenschutzbeauftragten

Im Berichtszeitraum ist z.B. die Handwerkskammer Postdam an die Aufsichtsbehörde mit der Bitte um Unterstützung bei der Einrichtung eines Prüfungsausschusses für die Prüfung zum "Datenschutzbeauftragten im Handwerk" herangetreten. In der Vergangenheit hatte das MI bereits bei der Erarbeitung der Rechtsvorschrift zur Fortbildung zum Datenschutzbeauftragten des Handwerks mitgewirkt. Aufgrund der Aufsichtsfunktion des MI wurde jedoch eine direkte Mitarbeit als Prüfer ausgeschlossen, gleichwohl aber die Mitarbeit bei der Vorbereitung der Tätigkeit der Prüfungsausschüsse zugesagt. Die Handwerkskammer wurde zur Gewinnung von Prüfern an die Gesellschaft für Datenschutz und Datensicherung e.V. verwiesen.

2.3 Schwerpunkte aus den Beschwerden und Anfragen

Die Bearbeitung von Beschwerden und Anfragen von Bürgern stellt einen Schwerpunkt der Tätigkeit der Aufsichtsbehörde dar. Wie bereits unter Ziffer 1.2 ausgeführt wurde, gingen auch in diesem Berichtszeitraum wieder mehrere Eingaben ein.

2.3.1 Beschwerden

Nachfolgend werden einige interessante Fälle aus Beschwerden kurz dargelegt.

"Datenübermittlung an privatärztliche Abrechnungsstelle ohne Einwilligung"

In einem Fall wurde Beschwerde darüber geführt, dass Patientendaten ohne Einwilligung an ein Abrechnungsbüro weitergegeben wurden.
Die Beschwerdeführerin ist Privatpatientin, das heißt, die Kosten von ärztlichen Behandlungen werden direkt zwischen Arzt und Patient abgerechnet. Im Zusammenhang mit einer ärztlichen Untersuchung wurde ihr eine "Datenschutz-Ermächtigungsklausel" bzgl. der Weitergabe der Patientendaten zu Abrechnungszwecken an ein Abrechnungsbüro vorgelegt. Die Beschwerdeführerin sollte darin einwilligen, dass ihre Daten zu Zwecken der Abrechnung an ein Dienstleistungsbüro übermittelt werden. Auf Nachfragen der Patientin konnte zunächst keine Auskunft über den Sitz dieses Büros gegeben werden. Die Patientin wurde vom Arzt behandelt und ein Folgetermin vereinbart, an dem auch Informationen über das Abrechnungsbüro gegeben werden sollten. Bei dem Folgetermin erfolgte die Informationen bzgl. des Abrechnungsbüro und die Patientin entschied sich, die "Datenschutz-Ermächtigungsklausel" nicht zu unterschreiben. Die Behandlung wurde abgebrochen. Vier Wochen später erhielt die Petentin eine Rechnung vom Abrechnungsbüro.

> Exkurs: Patientendaten/§ 203 StGB/Einwilligungserklärung/Folgen
> Das Arzt-Patienten-Geheimnis umfaßt alle Informationen, die im Zusammenhang mit einer ärztlichen Behandlung stehen. Dies beginnt bei der Tatsache, dass sich ein Patient überhaupt in ärztliche Behandlung befindet, umfaßt die Diagnosen und Therapien und endet mit der Abrechnung der Kosten gegenüber den Krankenkassen bzw. dem Patienten selbst.
> Das Arzt-Patienten-Geheimnis ist in der ärztlichen Berufsordnung verankert. Es hat im Rahmen der gesundheits- und sozialdatenschutzrechtlichen Bestimmungen eine herausragende Bedeutung. Eine Verletzung der ärztlichen Schweigepflicht stellt nach den arztberufsrechtlichen Vorschriften ein Berufsvergehen dar. Zudem ist die unbefugte Offenbarung eines fremden Geheimnisses (eines Patientendatums) durch Ärzte sowie andere Geheimnisträger nach § 203 StGB mit Strafe bedroht. Strafbar können sich insoweit nach Abs. 3 dieser Vorschrift unter anderem auch die sogenannten "berufsmäßig tätigen Gehilfen", also z.B. Sprechstundenhilfen, Laborbedienstete etc., machen. Eine befugte - und damit nicht strafbare - Offenbarung ist nur möglich, wenn der Patient in die Offenbarung eingewilligt hat oder eine gesetzliche Befugnis vorliegt.
> Bezüglich der Privatärztlichen Liquidation gilt, dass eine gesetzliche Befugnis zur Übermittlung der Abrechnungsdaten an eine Abrechnungsstelle nicht existiert. Die Übermittlung der Daten ist daher nur mit Einwilligung des Patienten erlaubt und damit straffrei.

Die Nachforschungen bei der betroffenen Einrichtung ergaben, dass die Arzthelferin, die Kenntnis davon hatte, dass eine Einwilligung der Patientin nicht vorlag, erkrankte und deshalb eine Sperrung der Daten für den Transfer zum Abrechnungsbüro nicht erfolgt ist.

Die betroffene Einrichtung bedauerte den Vorfall und nahm ihn zum Anlass, alle Praxen nochmals auf die Einhaltung des Datenschutzes hinzuweisen

"Einkauf mit EC-Karte"

Eine Petentin wandte sich mit folgendem Problem an die Aufsichtsbehörde.
Bei einem Einkauf in einem Kaufhaus bezahlte die Petentin mit EC-Karte und wurde von der Kassiererin aufgefordert, den Personalausweis vorzulegen. Anschließend notierte man sich auf einem losen Zettel die Personalausweisnummer, was seitens der Kundin Verwunderung hervorrief. Auf Nachfrage am Informationsstand, warum dies so gehandhabt wird, sagte man ihr, dass die schriftliche Erfassung lediglich der eigenen Sicherheit diene, da es in letzter Zeit häufig zum Missbrauch der EC-Karten gekommen sei.
Aus Sicht der Petentin blieb jedoch die Frage offen, was passiert mit dem Zettel, auf welchem die personenbezogenen Daten notiert wurden und wer kann Einsicht in diese nehmen.
Das Kaufhaus wurde diesbezüglich um Stellungnahme gebeten und es wurde auf zwei Vorschriften des BDSG aufmerksam gemacht.
Gemäß § 28 Abs. 1 Nr. 2 BDSG ist die Speicherung und Nutzung personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Personenbezogene Daten sind zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht erforderlich ist (§ 34 Abs. 2 Nr. 3 BDSG).
In der Stellungnahme des Kaufhauses wurde mitgeteilt, dass die angewandte Praktik zur Sicherheit der Kunden geschehen sei. Das Aufnehmen der Daten, die am selben Tag vom Bereichsverantwortlichen vernichtet wurden, dienten nur dem symbolischen Zweck, um Checkkartenbetrüger abzuschrecken. Die kurzfristige Verfahrensweise wurde sofort eingestellt und man versicherte, dass die schriftliche Erfassung der Daten 100%ig vernichtet und zu keinem anderen Zweck verwandt wurde.

"Vollstreckungsbescheid unter falschem Vornamen durch eine Möbelfirma"

Die Eheleute B. wurden im Februar 2000 von einem Gerichtsvollzieher aufgesucht. Zugrunde lag eine Forderung gegen einen Herrn Detlef B., obwohl der Petent Dieter B. heißt.
Nach den Ermittlungen der Eheleute B. war ein Herr Detlef B. unter deren Anschrift nicht gemeldet. Es wurde vermutet, dass möglicherweise das Einwohnermeldeamt aufgrund einer Namensverwechslung eine fehlerhafte Melderegisterauskunft erteilt haben könnte.
Die Ermittlungen des Landesbeauftragten für den Datenschutz und für das Recht auf Akten-

einsicht hatten inzwischen ergeben, dass seitens des Amtes ... keine Melderegisterauskunft an die Möbelfirma gegangen war.
Die Möbelfirma hatte beim Amtsgericht beantragt, Zwangsvollstreckungsmaßnahmen gegen den Herrn Detlef B. einzuleiten. Als vermeintliche Adresse des Herrn Detlef B. wurde die Anschrift des Petenten angegeben. Daraus musste geschlussfolgert werden, dass die Möbelfirma von Anfang an über eine falsche Anschrift des Herrn Detlef B. verfügt haben muss.
Seitens der Möbelfirma wurde zu diesem Fall folgende Stellungnahme abgegeben. Da die im Zeitraum 1997 bis Anfang 2000 erfolgten Einwohnermeldeamtsanfragen zum Schuldner Detlef B. negativ ausgingen, habe man bei einer Familie im Haus unter der vorhandenen Anschrift erfahren, dass bei dem Vermieter der Liegenschaft ein Herr Detlef B. abgemeldet sei und er seit 1997 in Berlin wohnhaft sei.
Da diese Auskunft zeitlich mit dem vorliegenden Mahn- bzw. Zwangsvollstreckungsverfahren übereinstimmte, wurde dann die Zwangsvollstreckungsmaßnahme unter der Berliner Anschrift beantragt. Der Obergerichtsvollzieher teilte jedoch der Möbelfirma mit, dass ein Herr Detlef B. unter der genannten Anschrift nicht wohnhaft sei, sondern ein Herr Dieter B. Die Zwangsvollstreckung wurde daraufhin eingestellt. Anfragen an das Landeseinwohnermeldeamt Berlin bestätigten, dass ein Herr Detlef B. unter dieser Anschrift nicht gemeldet war und auch nicht ist.

Seitens der Aufsichtsbehörde wurde nochmals telefonisch Rücksprache mit der Möbelfirma genommen. Zur Klärung der Angelegenheit hätte zuerst das Landeseinwohnermeldeamt befragt werden müssen, erst dann hätte man dem Gerichtsvollzieher den Vollstreckungsauftrag übergeben dürfen.
Dass die Angelegenheit so einen Verlauf genommen hat, wurde seitens der Möbelfirma bedauert und man wolle sich noch persönlich bei dem Petenten wegen der Vornamensverwechslung entschuldigen.

"Absetzen eines Faxes durch eine Rechtsanwaltskanzlei an den Dienstanschluß des Petenten"

Der Petent teilte mit, dass er gelegentlich Schriftwechsel mit seiner Rechtsanwältin über das Büro-Fax abwickelt. Jedoch sei keinesfalls die Anschlussnummer für Rückantworten autorisiert worden. Die Absenderkennung ließe auch keinen Zweifel, dass es kein Privatanschluss sei.
Nun hat die Rechtsanwältin in folgendem Fall, um dem Petenten schnell eine Antwort zukommen zu lassen, an den Faxabsender eine Rückantwort erteilt.
Der Petent war der Meinung, dass die Rechtsanwältin sich hier datenschutzwidrig verhalten hat.
Dem Petenten konnte mitgeteilt werden, dass nach Kontrolle der Anlagen (Fax an die Rechtsanwaltskanzlei sowie Rückantwort) kein Handlungsbedarf gegenüber der Rechtsanwältin besteht.
Auf dem abgesandten Fax des Petenten ist die Fax-Nummer angegeben, so dass für den

Empfänger nicht ersichtlich ist, ob es sich hier um einen dienstlichen oder privaten Anschluss handelt. In diesem Falle hätte der Petent dies deutlich für den Empfänger vermerken müssen.
Es gibt auch keine Regelung, die es untersagt, die angegebene Fax-Nummer zu benutzen. Nur wenn sich unmittelbar der Verdacht aufdrängt, Unbefugte könnten das Fax lesen bevor es in die Hände des Adressaten gelangt, kann ein Verstoß gegen § 9 BDSG und dessen Anlage (insbesondere dessen Nr. 2, wonach entsprechende Maßnahmen zu treffen sind, die je nach Art der zu schützenden personenbezogenen Daten geeignet sind, zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle)) angenommen werden. Aus einer Anlage zum Schreiben des Beschwerdeführers war auch nicht ersichtlich, dass das Schreiben per Fax an den Betrieb des Petenten gesandt wurde.
Obwohl sich der Petent mit der Antwort der Aufsichtsbehörde nicht zufriedengab und eine sachgerechte Bearbeitung seiner Beschwerde in Zweifel stellte, musste abschließend nochmals eingehend betont werden, dass der Petent ausdrücklich einer Rückantwort an seinen Arbeitgeber hätte widersprechen müssen.

"Angebot für eine Krankenversicherung"

In einer weiteren Beschwerde wurde ausgeführt, dass der Petent von einer Versicherungsgesellschaft ein Angebot für eine Krankenversicherung erhalten habe, ohne dieses beantragt zu haben. Der Petent habe sich gewundert, woher die Versicherung wusste, dass er sich privat krankenversichern möchte. Außerdem seien der Versicherung noch weitere persönliche Daten (Alter, Anschrift) bekannt gewesen. Der Petent erkundigte sich daraufhin bei der Versicherungsgesellschaft, woher sie seine personenbezogenen Daten hätten. Der Versicherungsvertreter hätte mitgeteilt, dass er eine Liste mit den "Besserverdienenden" erhalten und daraus die Daten entnommen hätte. Auf die Frage des Petenten, woher er diese Liste bezogen hätte, habe der Vertreter keine Auskunft gegeben, so dass die Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich eingeschaltet wurde.

Die Aufsichtsbehörde holte eine Stellungnahme vom Versicherungsvertreter ein, der als selbständiger Handelsvertreter, eigenverantwortlich für eine Versicherung tätig ist. Darin führte er aus, dass er auf einer privaten Feierlichkeit mit einem flüchtigen Bekannten ins Gespräch kam, in dem auch über seine berufliche Tätigkeit gesprochen worden sei. Kurz darauf habe er einen handschriftlichen Zettel bekommen. Der Adressenlieferant habe auf diesem Zettel nach seiner persönlichen, unverbindlichen Einschätzung "Besserverdienende" einer geschätzten Altersgruppe zwischen 40-55 Jahren notiert. Der Name sowie die Adresse des Adressenlieferanten seien dem Vertreter nicht bekannt. Ganz unverbindlich sei diesen Personen ein Beispielangebot unterbreitet worden, mit dem aus Sicht des Versicherungsvertreters positiven Hintergedanken, diesen Personen einen möglichen Vorteil aufzuzeigen. Da außer dem Petenten keine der

angeschriebenen Personen geantwortet habe, sei der handschriftliche Zettel der "Besserverdienenden" vernichtet worden.
Das BDSG dient dazu, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (§ 1 Abs. 1 BDSG). Davon ausgehend gilt das BDSG für die Verarbeitung und Nutzung personenbezogener Daten durch nicht-öffentliche Stellen, soweit sie Daten in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeiten oder nutzen (§ 1 Abs. 2 Nr. 3 BDSG). Der Versicherungsvertreter teilte mit, dass er keine dateimäßige Verarbeitung von personenbezogenen Daten vornehme. Danach käme das BDSG bei der Versicherungsvertretung nicht zur Anwendung.

Die Aufsichtsbehörde hat dem Versicherungsvertreter trotzdem Hinweise zur Zulässigkeit der Nutzung von Informationen aus privaten Quellen gegeben, denn bei dieser Frage ist § 28 Abs. 1 Satz 2 BDSG zu beachten. Danach müssen die Daten nach Treu und Glauben und auf rechtmäßige Weise erhoben werden. Im Hinblick auf das informationelle Selbstbestimmungsrecht ist daher zu empfehlen, das Daten grundsätzlich beim Betroffenen zu erheben sind.

"Datenschutz in Krankeneinrichtungen"

Weiterhin ging eine Beschwerde ein, in der der Petent ausführte, dass sich seine Frau einer Operation des Sprunggelenks unterziehen musste. Nach der Operation in Berlin sei die Behandlung durch einen niedergelassenen Arzt im Land Brandenburg erfolgt. Der Unfall würde durch die Verwaltungsberufsgenossenschaft in Schwerin bearbeitet. Diese Genossenschaft hatte nach Prüfung der häuslichen Verhältnisse hauswirtschaftliche Versorgung genehmigt. Eine Verlängerung der Maßnahme nach Entfernung des Gipses war in Aussicht gestellt und bedurfte der Beschreibung der noch vorhandenen Einschränkungen. Der Petent legte dar, dass diese Verordnung sowie weitergehende Rehabilitationsmaßnahmen seitens des behandelnden Arztes verweigert worden wäre. Daraufhin habe der Petent den Arzt aufgesucht, da er sich mit dieser Entscheidung nicht einverstanden erklären konnte. Der Petent habe außerdem dem Arzt geschrieben und gebeten, seine Entscheidung zu überdenken. Weiterhin habe er seine persönlichen Gefühle des Verletztsein über die Handlungsweise des Arztes geäußert. Diesen Brief hätte der Arzt ohne Einverständnis des Petenten an die Verwaltungsberufsgenossenschaft weitergereicht. Aus Sicht des Beschwerdeführers sei dieses Schreiben zur Entscheidungsfindung der Genossenschaft nicht notwendig gewesen und fiel nicht unter die Daten über die Heilbehandlung seiner Frau, die der Genossenschaft übermittelt werden durften.
Der Petent führte weiterhin aus, dass mit dem Datenschutz in der Praxis sehr großzügig umgegangen würde. So würde im Warteraum, der gleichzeitig Patientenanmeldung sei, u.a. am Telefon in Verbindung mit Namen für alle hörbar über Diagnosen gesprochen.

Auf Bitten der Aufsichtsbehörde übersandte der Arzt eine Stellungnahme. Der Arzt teilte mit, dass bei der Behandlung der Fußverletzung der Frau des Petenten Probleme entstanden wären. Die von der Berufsgenossenschaft (BG) geforderte optimale Therapie habe ein Mitziehen der Patientin verlangt und hier sehe er die Quelle der Konflikte. Im Weiteren führte er aus, dass wegen der weiteren Behandlung bereits Telefonate mit der BG stattgefunden hätten. Er habe der BG mitgeteilt, dass der Fuß wieder voll belastet werden solle und daher keine Haushaltshilfe mehr benötigt werde. Zur weiteren Zusammenarbeit habe er von der BG die Schreiben des Petenten erhalten und daraufhin habe er, um die Informationskette nicht zu brechen, den Brief des Petenten an die BG weitergegeben. Er sähe darin keine Verletzung des Datenschutzes, sondern die Mitteilung von behandlungsnotwendigen Informationen.

Das BDSG gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch nicht-öffentliche Stellen, soweit sie die Daten in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeiten und nutzen (§ 1 Abs. 2 Satz 1 Ziffer 3 BDSG). Im Bereich der Arztpraxen erfaßt das BDSG daher nur die Verarbeitung und Nutzung von Daten in oder aus Dateien. Dies können automatisierte "Computer-Dateien" oder nicht-automatisierte "Kartei-Dateien" sein. Vom BDSG regelmäßig nicht erfaßt werden z.B. Patientenunterlagen in Akten.
Niedergelassene Ärzte sind "nicht-öffentliche Stellen", für die das BDSG Anwendung findet. Das BDSG dient dazu, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (§ 1 Abs. 1 BDSG). Davon ausgehend gilt das BDSG für die Verarbeitung und Nutzung personenbezogener Daten durch nicht-öffentliche Stellen, soweit sie Daten in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeiten oder nutzen (§ 1 Abs. 2 Nr. 3 BDSG).
Für die Verarbeitung von Daten durch nicht-öffentliche Stellen für berufliche oder gewerbliche Zwecke oder für die geschäftsmäßige Datenverarbeitung sieht der 3. Abschnitt des BDSG Erlaubnistatbestände vor. Dieser Abschnitt des BDSG enthält Vorschriften zur Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen.
Im § 28 BDSG wird die Datenspeicherung, -übermittlung und -nutzung für eigene Zwecke geregelt. Nach § 28 Abs. 1 Satz 1 BDSG ist das Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig

1. im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen,
2. soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt,
3. wenn die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse

des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung offensichtlich überwiegt,

4. wenn es im Interesse der speichernden Stelle zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

Dieser Absatz stellt keine gesetzliche Grundlage für die Übermittlung der Daten des Petenten dar, keine der 4 Ziffern ist auf den Fall anwendbar.
Nach § 28 Abs. 2 BDSG ist eine Übermittlung auch zulässig, soweit es zur Wahrung berechtigter Interessen eines Dritten oder öffentlicher Interessen erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Mit dem schutzwürdigen Interesse ist das Persönlichkeitsrecht des Betroffenen gemeint (vgl. § 1 Abs. 1 BDSG). Die Weitergabe der Unterlagen lagen nicht im öffentlichen Interesse und außerdem war der Betroffene nicht mit der Übergabe einverstanden.

Gemäß § 9 BDSG haben öffentliche und nicht-öffentliche Stelle, die personenbezogene Daten verarbeiten, technische und organisatorische Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG zu gewährleisten. Dazu werden in der Anlage zu § 9 Satz 1 BDSG die Anforderungen dargestellt.

Die Vertreter der Aufsichtsbehörde baten den Arzt den kritisierten Bereich (Patientenanmeldung=Warteraum) zu trennen bzw. so umzugestalten, so dass für unbefugte Dritte keine Möglichkeit des Mithörens von Gesprächen und der Kenntnisnahme von Daten mehr besteht. Der Arzt bestätigte die Veränderung in seiner Praxis und legte dar, dass die Patientenbefragungen gezielt in die Sprechzimmer verlegt würden.

"Offenbarung von Patientendaten Verstorbener an Bestattungsunternehmen"

In einer weiteren Beschwerde führte die Petentin aus, dass ihre Mutter in einem Krankenhaus verstorben sei. Nachdem sie über den Todesfall informiert wurde, habe die Petentin ein Bestattungsunternehmen ihrer Wahl mit der Beisetzung ihrer Mutter beauftragt.
Die Beschwerdeführerin war sehr verwundert, als sie von einem anderen Bestattungsunternehmen angerufen und ihr mitgeteilt worden sei, dass sie zur Besprechung der Beisetzung vorbei kommen könne.
Daraufhin brachte die Petentin in Erfahrung, das das andere Bestattungsunternehmen für das Klinikum die Überführung zum Haupthaus des Krankenhauses ausführte. Der Petentin war unklar, wie das andere Bestattungsunternehmen zu den Daten ihrer verstorbenen Mutter bzw. ihrer Telefonnummer gekommen sei.

Die Aufsichtsbehörde wandte sich aufgrund dieser Beschwerde an das betreffende Bestattungsunternehmen und bat um Mitteilung, wie das Unternehmen an die o.g. Daten gekommen sei und auf welcher rechtlichen Grundlage diese Daten für geschäftlichen Zwecke benutzt wurden.
Der mit der Vertretung des Bestattungsunternehmens beauftragte Rechtsanwalt wies in seinem Antwortschreiben den Vorwurf der vermuteten Verletzung datenschutzrechtlicher Vorschriften auf das Schärfste zurück. Die Aufsichtsbehörde hatte jedoch keinen Vorwurf erhoben, sondern wollte lediglich zur Sachverhaltsaufklärung einige Informationen zu bestimmten Fragen. Der Anwalt übersandte schließlich noch die gewünschten Auskünfte.

Der Anwalt betonte, dass sein Mandant ein seriöses Bestattungsunternehmen führe und dessen Leistungen bisher nie Anlass zu Beanstandungen gegeben hätten. Er verwies auf die langjährigen Erfahrungen der im Unternehmen tätigen Mitarbeiter.
Weiterhin führte er aus, dass sein Mandant sowie seine Mitarbeiter vom Namen der Petentin zum ersten Mal aus dem Schreiben der Aufsichtsbehörde Kenntnis erhalten hätten.
Außerdem legte der Anwalt dar, dass der Leichentransport von der Außenstelle zum Haupthaus des Klinikums auf der Grundlage eines Vertrages zwischen dem Klinikum und dem Bestattungsunternehmen erfolge. Er führte aus, dass seinem Mandanten und den Mitarbeitern des Unternehmens unter Beachtung der Regelungen des Vertrages folgende Daten bekannt seien :

- Vorname, Name des/der Verstorbenen,
- Datum/Uhrzeit der Anforderung zum Transport
- Abholadresse und
- Name des/der Anfordernden

Weitere Angaben würden dem Unternehmen nicht bekannt.
Es würden sich wohl auch andere Bestattungsunternehmen unter dem Namen seines Mandanten melden. Ob dies hier der Fall war, konnte nicht überprüft werden.

Die Ausführungen des Anwalts des Bestattungsunternehmens ließen keine Zweifel an der Richtigkeit der Aussagen zu. Es ließ sich kein Verstoß gegen datenschutzrechtliche Vorschriften erkennen.

"Beschwerden zur Arbeitsweise eines Telekommunikationsunternehmens"

Aufgrund dessen, dass einige Beschwerden zur Arbeitsweise eines Telekommunikationsunternehmens mit Sitz im Land Brandenburg eingingen, fand ein Gespräch zwischen Vertretern des Unternehmen und der Aufsichtsbehörde zu allgemeinen datenschutzrechtlichen Fragen statt. In dem Gespräch wurde zu Beginn das Unternehmen kurz vorgestellt. Anschließend wurden Ausführungen zur Bonitätsprüfung gemacht, die das Unternehmen vor Abschluß eines Vertrages

durchführt bzw. durchführen lässt. Die Bonitätsprüfung erfolgt in zwei Stufen. Auf der zweiten Stufe wird dabei auch ein Scoring-Verfahren durchgeführt.
Der potentielle Kunde schreibt einen Kundenauftrag aus und willigt nach der Darstellung des Unternehmens mit seiner Unterschrift in die Bonitätsprüfung sowie in die Erhebung seiner Ausweisdaten ein. Daraufhin erfolgt eine Anfrage bei der SCHUFA. Liegen der örtlichen SCHUFA keine Informationen vor, wird eine weitere Anfrage an eine in den AGB genannten Wirtschaftsauskunfteien gestartet. Es erfolgt eine Risikoananlyse anhand der auf dem Kundenauftrag vorgegebenen personenbezogenen Informationen in Wechselbeziehung mit sozidemographischen (nicht personenbezogenen) Daten im Auftrag und nach konkreten Vorstellungen des Unternehmens.
Bei erhöhten Risiken für die Telekommunikationsfirma werden die Verträge nicht bestätigt. Der Interessent erhält ein pauschales Schreiben, dass das Auftragsverhältnis nicht bestätigt werden kann. Der Händler, bei dem der Auftrag abgegeben wurde, kann dazu keine Aussage treffen. In vielen Fällen rufen die Interessenten die Hotline des Unternehmens an, deren Mitarbeiter nach Ansicht des Unternehmens aus datenschutzrechtlichen Gründen keine telefonischen Auskünfte erteilen dürfen und eine qualifizierte Auskunft zu diesem Thema auch nicht abgeben können. Rückfragen der Betroffenen können nur schriftlich beantwortet werden.
In diesen Antwortschreiben erklärt das Unternehmen, dass es sich im Rahmen seiner Prüfung verschiedener Wirtschaftsauskunfteien bedient, die das Unternehmen bei der Entscheidung über die Anträge unterstützen. Sind diese Auskünfte für den Betroffenen nicht ausreichend, teilt ein Vertreter des Unternehmens auf Nachfrage bzw. Berufung auf § 34 BDSG mit, welche Auskunfteien befragt wurden sowie welcher Grund zur Ablehnung geführt hat. Des weiteren wird eine Einzelfallprüfung angeboten. Bei weiteren Nachfragen wird das Scoring-Verfahren allgemein erläutert.

Im Zusammenhang mit der Bearbeitung einer Beschwerde (Registrierung mehrerer vorauszahlbarer Karten, sogenannter prepaid-Karten, auf den Namen der Petentin) fragten die Vertreter der Aufsichtsbehörde nach, in wieweit eine Prüfung der Personalien bei der Registrierung von solchen Karten durchgeführt wird. Die Vertreter vom Unternehmen führten aus, dass eine Identitätprüfung erfolge. Die Händler dürfen zur Vermeidung von Betrugsfällen in der Regel nur eine definierte Menge an Einzelpersonen abgeben, es sei jedoch nicht auszuschließen, dass in Einzelfällen Händler hiervon aus Eigenmotivation abweichen. Der zugrunde liegende Sachverhalt war im konkreten Fall nicht mehr vollständig zu rekonstruieren.

Außerdem wurde die Abgrenzung der Zuständigkeiten diskutiert. Der Bundesbeauftragte für den Datenschutz (BfD) ist nach dem Telekommunikationsgesetz für Beschwerden, die das Kerngeschäft des Unternehmens betreffen, zuständig. Die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich ist für Fälle, die z.B. das Service-Center oder die Arbeit der eingeschalteten Auskunfteien betreffen, zuständig.

2.3.2 Anfragen

Auch in diesem Berichtszeitraum gingen mehrere Anfragen bei der Aufsichtsbehörde ein. So wurden einige Fragen zur Veröffentlichung im Internet an die Aufsichtsbehörde herangetragen. Nachfolgend sind einige interessante Probleme zusammengestellt.

"Warndatei im Online-Verfahren"

Es wurde folgendes Vorhaben zur datenschutzrechtlichen Prüfung an die Aufsichtsbehörde herangetragen:
Es soll eine Datenbank im Online-Verfahren errichtet werden. Die Datenbank soll Angaben über Kunden von Handwerksbetrieben enthalten. Abfrageberechtigt sind die der Datei vertraglich angeschlossenen Handwerksbetriebe, die auch einzutragende Daten melden.
Dies soll eine Auskunftsdatei sein, in der Angaben über Auftraggeber und Vertragspartner von Handwerksbetrieben der Baubranche gespeichert sind und die den angeschlossenen Unternehmen zur Beurteilung der Kreditwürdigkeit von Kunden übermittelt werden.

Die Aufsichtsbehörde hat dazu einige Ausführungen zur Rechtslage den Datenschutz betreffend übersandt.
Das BDSG dient dazu, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (§ 1 Abs. 1 BDSG). Davon ausgehend gilt das BDSG für die Verarbeitung und Nutzung personenbezogener Daten durch nicht-öffentliche Stellen, soweit sie Daten in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeiten oder nutzen (§ 1 Abs. 2 Nr. 3 BDSG).
§ 4 BDSG regelt die Zulässigkeit der Datenverarbeitung und -nutzung. Danach sind die Verarbeitung personenbezogener Daten und deren Nutzung nur zulässig, wenn das BDSG oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat (§ 4 Abs. 1 BDSG). Der Vorschrift kommt grundsätzliche Bedeutung zu. Sie unterwirft die Datenverarbeitung einschließlich der Nutzung einem Gesetzesvorbehalt. Es handelt sich um ein sogenanntes Verbot mit Erlaubnisvorbehalt. Für die Verarbeitung von Daten durch nicht-öffentliche Stellen für berufliche oder gewerbliche Zwecke oder für die geschäftsmäßige Datenverarbeitung sieht der 3. Abschnitt des BDSG entsprechende Erlaubnistatbestände vor.
Der 3. Abschnitt des BDSG enthält Vorschriften zur Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen.
Im § 28 BDSG wird die Datenspeicherung, -übermittlung und -nutzung für eigene Zwecke geregelt. § 28 BDSG wurde bereits in der Beschwerde "Datenschutz in Krankeneinrichtungen" (Seite 12) näher ausgeführt. Darauf soll an dieser Stelle verwiesen werden.
Der Vorschrift (§ 28 BDSG) unterliegen die Verarbeitung sowie die Nutzung für bestimmte -

berufliche oder gewerbliche- Zwecke. Eine Datenverarbeitung für eigene berufliche Zwecke liegt vor, wenn die Datenverarbeitung in irgendeinem Zusammenhang mit einer beruflichen Tätigkeit steht. Darunter fällt z.B. die Verarbeitung personenbezogener Daten von Kunden, Mandanten, Interessenten, Arbeitnehmern, freien Mitarbeitern usw. Die gewerblichen Zwecke sind weitestgehend nur ein Unterfall der beruflichen Zwecke. Nach dem vorgelegten Konzept sollen Daten aus einem Vertragsverhältnis an die Auskunftei übermittelt werden. Hinsichtlich der Zulässigkeit kommt hierfür § 28 Abs.1 Nr. 2 und Abs. 2 Nr. 1 Buchst. a BDSG oder die Einwilligung der Betroffenen in Betracht.

Ist der Geschäftszweck der Stelle das Speichern und Verändern personenbezogener Daten zum Zwecke der Übermittlung kommt § 29 BDSG zur Anwendung.
Im § 29 BDSG ist die geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung geregelt. Adressaten dieser Vorschrift sind u.a. Auskunfteien, Detekteien und Kreditinformationsdienste. Danach ist das geschäftsmäßige Speichern oder Verändern personenbezogener Daten zum Zwecke der Übermittlung zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Speicherung oder Veränderung hat, oder
2. die Daten aus allgemein zugänglichen Quellen entnommen werden können, oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Speicherung oder Veränderung offensichtlich überwiegt.

Mit dem schutzwürdigem Interesse ist das Persönlichkeitsrecht und damit das informationelle Selbstbestimmungsrecht des Betroffenen gemeint.
Durch § 29 Abs. 2 BDSG wird die Übermittlung personenbezogener Daten im Rahmen der geschäftsmäßigen Datenverarbeitung für die Fälle erlaubt, in denen keine Einwilligung des Betroffenen vorliegt. Die Zulässigkeit einer Übermittlung kann sich u.a. daraus ergeben, dass der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat. In diesem Fall ist die Übermittlung nur zulässig, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.
Das berechtigte Interesse umfasst weniger als ein rechtliches Interesse, weshalb auch ein wirtschaftliches oder ideelles Interesse darunter fällt. Berechtigt können nur Interessen sein, die im Zusammenhang mit der konkret beabsichtigten Verarbeitung stehen und sich auf die dabei zu verwendenden Daten beziehen. Dem berechtigten Interesse der speichernden Stelle stehen die schutzwürdigen Interessen der Betroffenen gegenüber. Es ist also eine Interessenabwägung vorzunehmen.
Des weiteren muss der Empfänger das Interesse glaubhaft dargelegt haben. Die Glaubhaftmachung setzt voraus, dass ein Sachverhalt vorgetragen wird, der dann gedanklich nachvollzogen werden kann und für den nach allgemeiner Lebenserfahrung eine ausreichende Wahrscheinlichkeit besteht. Zur glaubhaften Darlegung gehört auch, dass die Identität des Empfängers nach-

prüfbar ist. Bei der Einsicht im Online-Verfahren bedarf es hinsichtlich der Identität des Empfängers sowie der Glaubhaftmachung des berechtigten Interesses besonderer Vorkehrungen, wie Paßwortvergabe o.Ä., damit bei einem Angebot über das Internet die Daten nicht für jedermann zur freien Verfügung abrufbar sind.
Offen gelassen wurde die Frage, in wieweit auch das Teledienstedatenschutzgesetz zu beachten ist.

"Veröffentlichung im Internet"

Ein Bürger (Stadtverordneter) fragte an, ob auf seiner privaten Homepage das Ortsrecht seiner Stadt darstellen kann. Er wollte die im Ortsrecht als Satzungen und Verordnungen veröffentlichten Daten, die veröffentlichten Namen von Stadtverordneten, Ausschussmitgliedern, Fraktionen, Fraktionsmitglieder sowie Mitgliedern von Beiräten sowie die veröffentlichten Telefonnummern der voran genannten Personen im Internet publizieren.

Auch bei dieser Anfrage wurden allgemeine Informationen zum Datenschutzrecht gegeben, z.B. zu § 1 und § 4 BDSG. Des weiteren wurde geprüft, in wieweit der § 28 BDSG Anwendung findet. An dieser Stelle wird auf die Ausführungen zu § 28 BDSG aus Seite 12 verwiesen. Danach findet § 28 BDSG in diesem Fall keine Anwendung.
Ist dagegen der Geschäftszweck der Stelle das Speichern und Verändern personenbezogener Daten zum Zwecke der Übermittlung kommt § 29 BDSG zur Anwendung, wobei das Einstellen von Daten ins Internet eine Übermittlung der Daten von Seiten des Anfragenden an die Internet-Nutzer darstellt.
Der Frage war zu entnehmen, dass der Anfragende bereits veröffentlichte Namen und Telefonnummern im Internet publizieren möchte. Nach § 29 Abs. 1 Nr. 2 BDSG wäre dies zulässig, wenn die Daten aus allgemein zugänglichen Quellen entnommen werden können, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Speicherung oder Veränderung offensichtlich überwiegt. Mit dem schutzwürdigem Interesse ist das Persönlichkeitsrecht und damit das informationelle Selbstbestimmungsrecht des Betroffenen gemeint.
Es ist also eine Interessenabwägung vorzunehmen, bei der zu berücksichtigen ist, dass die Veröffentlichung von Informationen im Internet eine Verbreitung und Vervielfältigung der Quellen weltweit bedeutet. Damit können bestimmte Risiken verbunden sein und die Tatsache der weltweiten Verbreitung kann ebenfalls die Privatsphäre oder die körperliche Unversehrtheit beschädigen.
In diesem Fall kann davon ausgegangen werden, dass bereits eine Interessenabwägung vorgenommen wurde und einer Veröffentlichung zugestimmt wurde, da die Daten auf der Internetseite der Stadt veröffentlicht sind.
Gemäß § 2 Abs. 2 Nr. 2 Teledienstegesetz (TDG) sind Teledienste im Sinne von Absatz 1

insbesondere Angebote zur Information oder Kommunikation, soweit nicht die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht (Datendienste, z.B. Verkehrs-, Wetter-, Umwelt- und Börsendaten, Verbreitung von Informationen über Waren und Dienstleistungsangebote). Auch dieser Aspekt war für dieses Vorhaben zu untersuchen. Da die Thematik noch relativ neu ist, fehlen noch entsprechende Erfahrungen.
Daher wurde angeraten, nach den oben gemachten Ausführungen zum BDSG zu verfahren.

"Videoüberwachung in öffentlichen Verkehrsmitteln"

Die Aufsichtsbehörde war mehrfach mit der Frage des Einsatzes von Kameras in öffentlichen Verkehrsmitteln befasst. Das derzeitig noch gültige BDSG enthält keine spezielle Regelung zur Videoüberwachung. Zwingende Voraussetzung für die Anwendung des BDSG im privaten Bereich ist jedoch der Dateibegriff, der nicht erfüllt ist, wenn keine Aufzeichnung der Bilder erfolgt. Nur eine digitale Aufzeichnung von Bildern würde diese Voraussetzung erfüllen.
In der derzeit laufenden Änderung des BDSG ist eine Regelung zur Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen in der Diskussion. Das geänderte Gesetz tritt jedoch erst Mitte des Jahres in Kraft. Wenn der Entwurf des § 6 b neue Fassung des BDSG so übernommen wird, wäre eine Videoüberwachung unter bestimmten Bedingungen zulässig.

Die oberste Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich des Landes Brandenburg vertritt zu der angesprochenen Problematik generell folgende Position:

- Zweck der Videobeobachtung ist die sichere Beförderung der Fahrgäste oder die Verhinderung von Eigentumsdelikten - mithin die Wahrnehmung des Hausrechtes durch das jeweilige Unternehmen. Die Videobeobachtung muss zu diesem Zweck erforderlich sein und darf das Recht auf informationelle Selbstbestimmung der Fahrgäste nicht unverhältnismäßig beeinträchtigen.
- Die mit Überwachungsanlagen ausgestatteten Fahrzeuge sind mit Hinweisschildern zu versehen, die auf die Tatsache der Videobeobachtung bzw. -aufzeichnung und Speicherung der gewonnenen Daten aufmerksam machen und konkrete Angaben (z.B. Telefonnummer und weitere Angaben) u.a. über die verantwortliche und speichernde Stelle enthalten.
- Die Speicherung der Aufzeichnung erfolgt so lange, bis das Fahrzeug routinemäßig auf Sachbeschädigungen hin überprüft ist. Wird keine solche Sachbeschädigung festgestellt, ist das Aufzeichnungsband sofort zu löschen. Die Auswertung von Aufzeichnungen erfolgt nur entsprechend des Zwecks ihrer Erstellung und nur durch dazu befugte Personen. Bei dem Verdacht auf das Vorliegen einer Straftat müssen die Strafverfolgungsbehörden die Möglichkeit haben, entsprechend den für sie geltenden Rechtsvorschriften, die Herausgabe der Aufzeichnungen als Beweismittel zu verlangen.

- Die Videoüberwachung, gleich welcher Variante, sollte in jedem Falle mit klaren und eindeutigen technischen, organisatorischen und personellen Maßnahmen verbunden werden. So sollte z.B. ein schriftliches Sicherheits- bzw. Einsatzkonzept erarbeitet sowie gegebenenfalls eine Betriebsvereinbarung abgeschlossen werden. Darin wäre der Einsatz der Überwachungsanlage detailliert zu beschreiben und zu regeln. Das betrifft z.B. die Festlegung des zulässigen Gebrauchs, die Hinweise an die Betroffenen, Regelungen zur Aufbewahrung und Vernichtung der Videobänder sowie die Festlegung des berechtigten Personenkreises für die damit verbundenen Teilaufgaben.
  Denkbar wäre auch die Erstellung einer Betriebsanweisung, die Bestandteil des Datenschutzkonzeptes des Unternehmens sein sollte.
- Es wird empfohlen, die Videobeobachtung schrittweise einzuführen und dabei die Datenschutzvorkehrungen kontinuierlich zu überprüfen und zu bewerten. In regelmäßigen Zeitabständen sollte erneut festgestellt werden, ob die Videoüberwachung noch erforderlich ist.

Auch die Datenschutzbeauftragten vertreten die Auffassung, dass die Videoüberwachung in öffentlichen Verkehrsmitteln nicht zu beanstanden ist, wenn bestimmte Voraussetzungen erfüllt sind.

3. Zusammenarbeit zwischen den Datenschutzaufsichtsbehörden der Länder

3.1 Schwerpunkte aus der Sitzung der Arbeitsgruppe "Auskunfteien" in Potsdam/ Stuttgart

Sitzungen der Arbeitsgruppe fanden am 19./20.06.2000 in Postdam und am 07./08.12.2000 in Stuttgart statt. Dabei wurden folgende Schwerpunkte behandelt:

- SCHUFA:
Negative Beeinflussung des Score-Wertes durch Selbstauskünfte
Im Zusammenhang mit dem von der SCHUFA angewendeten Scoring-Verfahren zur Beurteilung der Bonität von Personen kam es in der Vergangenheit zu Beschwerden darüber, dass die Einholung einer Selbstauskunft gemäß § 34 Abs. 2 BDSG in die Berechnung des Score-Wertes einfließt und zu einer Verschlechterung der Bonitätsbeurteilung führt. Die Aufsichtsbehörden vertreten hierzu die Auffassung, dass die Wahrnehmung eines Rechtes nicht zu einer Verschlechterung der Beurteilung des Betroffenen führen darf. Dies würde einem Verbot gleichkommen. Gespräche mit der SCHUFA haben dazu geführt, dass die Einholung einer Selbstauskunft zukünftig nicht mehr in die Berechnung des Score-Wertes einfließen wird.
- Auskunfteien

Verflechtung von Inkasso- und Auskunfteibereich

Eine deutschlandweit tätige Auskunftei hat zwei Geschäftszweige. Zum einen ist dies der klassische Auskunfteibereich und zum anderen wird ein Inkassobüro betrieben. Beide Geschäftszweige sind datenschutzrechtlich als selbständige Bereiche einzuordnen. Bei diesem Unternehmen ist das Problem aufgetaucht, dass eine Verflechtung zwischen diesen beiden an sich getrennten Bereichen besteht. So kann der Mitarbeiter des Auskunfteibereiches auf bestimmte Daten (offene Inkassoverfahren) des Inkassobereiches zugreifen. Dieses Verfahren ist rechtlich unzulässig, weil hier möglicherweise der Mitarbeiter von nicht nur sogenannten "harten Negativmerkmalen " sondern auch von jeglichen bestehenden Inkassoverfahren Kenntnis erlangen kann. Einer solchen Datennutzung i.S.v. § 28 Abs.2 BDSG stehen jedoch die schutzwürdigen Interessen der Betroffenen am Ausschluss der Übermittlung/Nutzung ihrer personenbezogenen Daten entgegen.

Die Aufsichtsbehörden haben gegenüber dem Unternehmen ihre rechtlichen Bedenken vorgetragen und eine Änderung des Verfahrens verlangt. Diese Angelegenheit wird in der Zukunft weiter verfolgt werden.

Verwendung von Schätzdaten

Eine weit verbreitete Praxis ist die Verwendung von Schätzdaten durch Auskunfteien. Dabei werden Personen oder Firmen statistische Daten zugeordnet und an Auskunftsuchende ohne Kennzeichnung weitergegeben. Diese Daten stimmen jedoch regelmäßig nicht mit den tatsächlichen Daten überein, da es sich lediglich um Durchschnittswerte handelt. Deshalb vertreten die Aufsichtsbehörden die Auffassung, dass eine Übermittlung von Schätzdaten nur zulässig ist, wenn diese Daten auch als solche gekennzeichnet werden. Diese Auffassung wird mittlerweile auch durch ein Gerichtsurteil eines Oberlandesgerichtes gestützt. Die Diskussion mit der betroffenen Auskunftei führte bislang noch nicht zu einem befriedengenden Ergebnis. Aufgrund des derzeitigen Standes der Diskussion und des mittlerweile existierenden Gerichtsurteils wird jedoch davon ausgegangen, dass die Rechtsauffassung der Aufsichtsbehörden durchgesetzt werden kann.

Es gilt, die Kennzeichnung von Schätzdaten als solche durchzusetzen.

Auskunftsrechte des Betroffenen nach § 34 BDSG

In der Vergangenheit kam es immer wieder zu Beschwerden von Betroffenen, weil sie gemäß § 33 Abs.1 BDSG darüber informiert wurden, dass ihre personenbezogenen Daten übermittelt wurden, aber nicht der Empfänger der Daten mitgeteilt wurde. Auch auf Nachfrage wurde der Empfänger der Daten durch die jeweilige Auskunftei nicht bekanntgegeben.

Gemäß § 34 Abs.2 BDSG kann der Betroffene in diesen Fällen nur Auskunft über den Empfänger verlangen, wenn er begründete Zweifel an der Richtigkeit der Daten geltend macht. Da diese im Normalfall nicht geltend gemacht werden (können), erhält der Betroffene auch keine Auskunft über den Empfänger.

Dies ist für die Betroffenen unverständlich und unbefriedigend. Im Gesetzgebungsverfahren zur BDSG-Novelle konnte keine Änderung dieses Verfahrens, wie dies von den Aufsichtsbehörden gewünscht wurde, erreicht werden.

3.2 Besondere Beratungsthemen des Düsseldorfer Kreises

3.2.1 Datenschutz in Call-Centern

Eingangs sollen einige allgemeine Bemerkungen zur Rechtsnatur von Call-Centern gemacht werden.
Ausgehend von den vielfältigen Ausgestaltungen und Entwicklungsstufen von Call-Centern ist festzustellen, dass das BDSG in seiner jetzigen Form und nach erfolgter Umsetzung der EU-Datenschutzrichtlinie in nationales Recht entsprechend novelliert die Grundsatznorm für die Tätigkeit der Call-Center hinsichtlich der Daten sowohl der Anrufer als auch der Mitarbeiter darstellt.

Dazu gehören insbesondere die z.Zt.. geltenden Bestimmungen zur Zulässigkeit der Datenverarbeitung (§ 4 BDSG), zum Datengeheimnis (§ 5 BDSG), zu notwendigen technischen und organisatorischen Maßnahmen (§ 9 BDSG, Anlage), zur Verarbeitung personenbezogener Daten im Auftrag (§ 11 BDSG; im Falle von Outsourcing) und zur Datenspeicherung, -übermittlung und -nutzung für eigene oder fremde Zwecke (§§ 28, 29 BDSG).

Lediglich in den seltenen und bei der Aufsichtsbehörde Brandenburg nicht bekannten Fällen, in denen Call-Center zusätzlich geschäftsmäßig bzw. gewerblich nachhaltig Telekommunikationsdienste bzw. -dienstleistungen erbringen, würden ergänzend die Vorschriften des Telekommunikationsgesetzes und der Telekommunikationdatenschutzverordnung (TDSV) zur Anwendung kommen.

Überwiegend werden die Call-Center im Auftrag eines anderen Unternehmens tätig. Die dem jeweiligen Call-Center übertragenen Aufgaben des Auftraggebers stellen eine Auftragsdatenverarbeitung im Sinne des § 11 BDSG dar.
Daraus ergeben sich für den Auftraggeber folgende Verpflichtungen:

- sorgfältige Auswahl des Auftragnehmers unter besonderer Berücksichtigung der von ihm getroffenen Schutzmaßnahmen,
- schriftliche Erteilung von Aufträgen mit vorgegebenen Inhaltskriterien,
- Weitergabe von personenbezogenen Daten an den Auftragnehmer nur in dem Umfang, wie es zur Aufgabenerfüllung erforderlich ist (z.B. sind für Terminvereinbarungen Name, Anschrift, Telefonnummer, evtl. Geburtstag zur Identifizierung in Zweifelsfällen sowie das Merkmal für eine vorliegende Telefonmarketing-Erklärung des Kunden erforderlich),

- der Auftraggeber ist auch weiterhin verantwortlich für die Einhaltung der Datenschutzvorschriften,
- Regelung für Unterauftragnehmer (z.B. Überlauffunktion in ein anderes Call-Center, wenn das Anrufvolumen beim beauftragten Call-Center nicht zu bewältigen ist).

Für das Call-Center als Auftragnehmer ergeben sich folgende Konsequenzen:

- die erhaltenen Daten dürfen nur entsprechend den Weisungen des Auftraggebers verarbeitet und genutzt werden,
- alle Mitarbeiter des Call-Centers müssen auf das Datengeheimnis verpflichtet werden, wobei besonders bei der Verarbeitung sensibler Daten die Anforderungen des Auftraggebers an die Qualifikation und den Einsatz des Personals beachtet werden müssen,
- es sind technische und organisatorische Maßnahmen zu ergreifen, die den Schutz der Daten sicherstellen (§ 9 BDSG und die Anlage zu § 9 BDSG),
- das Call-Center muss sich als Auftragsdatenverarbeiter bei der zuständigen Aufsichtsbehörde (§ 38 BDSG) zum Register nach § 32 BDSG melden und unterliegt deren Aufsicht,
- das Call-Center hat bei Vorliegen der Voraussetzungen des § 36 BDSG einen Datenschutzbeauftragten zu bestellen,
- wird das Call Center für mehrere Auftragnehmer tätig, erfordert dies vertragliche Vereinbarungen mit jedem einzelnen Auftraggeber entsprechend der vorgenannten Kriterien und eine Trennung der Daten nach Auftraggebern,
- die Kontaktaufnahme per Telefon ist grundsätzlich im Namen des Auftraggebers durchzuführen.

Der "Düsseldorfer Kreis" als das Beratungsgremium der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich hat sich im Mai 2000 und die Arbeitsgruppe "Telekommunikation, Tele- und Mediendienste" des "Düsseldorfer Kreises" im März und Oktober 2000 insbesondere mit der speziellen Problematik der Zulässigkeit des Mithörens und Aufzeichnens von Telefongesprächen zwischen Mitarbeitern von Call-Centern und Kunden durch die jeweilige Geschäftsleitung beschäftigt.
Die Call-Center machen diesbezüglich geltend, die Qualität der Kundenbetreuung auf diese Weise überprüfen zu können.
Die Aufsichtsbehörden waren sich insoweit einig, dass eine Aufzeichnung von Gesprächen nur nach vorheriger Einwilligung des Kunden in Betracht kommt. Ohne eine solche Einwilligung wäre eine Aufzeichnung gemäß § 201 Strafgesetzbuch (StGB) als Verletzung der Vertraulichkeit des Wortes grundsätzlich strafbar.
Beim Mithören eines Kundengespräches wird ebenfalls regelmäßig eine Information des Kunden hierüber für notwendig erachtet. Auch gegenüber dem Mitarbeiter des Call-Centers wäre ein heimliches Mithören von Gesprächen grundsätzlich unzulässig. Wenn der Arbeitgeber z.B. in der Probezeit oder stichprobenartig Gespräche seiner Mitarbeiter mithören möchte, muss er sie vorher darüber informieren.

Die Thematik wird jedoch sowohl in der o.g. Arbeitsgruppe als auch im "Düsseldorfer Kreis" selbst unter Berücksichtigung der noch nicht all zu umfangreichen Erfahrungen der Aufsichtsbehörden auf diesem Gebiet weiterhin diskutiert.

3.2.2 Versicherungen im Internet

Angesichts der steigenden Zahl immer neuer Anbieter von Informationen und Angeboten zum Bezug von Waren und Dienstleistungen im Internet und einer stetig wachsenden Zahl von Internetnutzern, sind aus der Sicht der Aufsichtsbehörden Aspekten des Datenschutzes und der Datensicherheit bei der Nutzung des Internets erhöhte Aufmerksamkeit zu schenken.
In der Versicherungswirtschaft z.B. besteht ein starkes Interesse daran, Versicherungsverträge im Internet sowohl anzubieten als auch abzuschließen. Vor diesem Hintergrund wurde eine "ad hoc" Arbeitsgruppe gebildet, der je drei Vertreter der Aufsichtsbehörden und der Versicherungswirtschaft angehören. Die Aufsichtsbehörde aus Brandenburg ist ebenfalls Mitglied dieser Arbeitsgruppe. Zweck dieser Arbeitsgruppe ist es, einen Kriterienkatalog für einen datenschutzgerechten Internetauftritt von Versicherungsunternehmen zu erarbeiten.
Dieser Katalog wurde in der November-Sitzung des "Düsseldorfer Kreises" von Vertretern der Arbeitsgruppe "Versicherungswirtschaft" vorgestellt und im Kreise der Aufsichtsbehörden erörtert. Dabei musste konstatiert werden, dass zwischen den Aufsichtsbehörden und den Vertretern der Versicherungswirtschaft keine Einigung über das Schriftformerfordernis für die Einwilligungsklausel zum Datenschutz und ein Formerfordernis für die Abgabe der Schweigepflichtsentbindungserklärung erzielt werden konnte.
Die Aufsichtsbehörden im "Düsseldorfer Kreis" waren sich darüber einig, dass auch bei Abschluß eines Versicherungsvertrages im Internet für die Unterzeichnung der Einwilligungserklärung zur Verarbeitung der jeweiligen personenbezogenen Daten gem. § 4 Abs. 2 Satz 2 BDSG die Schriftform einzuhalten ist. Erst mit Vorliegen aller rechtlichen und praktischen Voraussetzungen wird die schriftliche Form durch eine elektronische Form z.B. eine digitale Signatur ersetzt werden können.
Darüber hinaus haben die Datenschutzaufsichtsbehörden Bedenken gegen die formlose Abgabe der Schweigepflichtsentbindungerklärung im Internet. Die Entbindung von der Schweigepflicht durch bloßes Anklicken stellt nicht sicher, dass die Schweigepflichtsentbindungserklärung nur durch Befugte abgegeben wird.
Einigkeit mit der Versicherungswirtschaft konnte u.a. zu Aussagen über Anbieterkennzeichnung, Datenschutzpolitik, Grundsatz der Datensparsamkeit bzw. Datenvermeidung und Verwendung von personenbezogenen Daten bei Informationsangeboten im Internet erreicht werden.

3.3 Teilnahme an den Sitzungen der Arbeitsgruppe "Internationaler Datenverkehr"

Die Arbeitsgruppe "Internationaler Datenverkehr", in der auch die Aufsichtsbehörde Brandenburg vertreten ist, befasste sich im Berichtszeitraum u.a. mit solchen besonderen Themenstellungen wie den Verhandlungen zwischen der Europäischen Kommission und der US-Regierung über die Vorsaussetzungen des Transfers personenbezogener Daten in die USA und den Vorentwurf einer Entscheidung der Europäischen Kommission zu Standardvertragsklauseln für die Datenübermittlung in Länder außerhalb der Europäischen Union.
Grundlage beider Themenschwerpunkte ist die in Kapitel IV der EU-Datenschutzrichtlinie geregelte Übermittlung personenbezogener Daten in Staaten außerhalb der EU, die grundsätzlich nur zulässig ist, wenn dort ein angemessenes Datenschutzniveau existiert.
Im Hinblick auf die Datenübermittlung in die USA wurden auf Grund einer langen und schwierigen Diskussion die sogenannten"Safe-Harbor"- Prinzipien vereinbart. Diese Prinzipien des "Sicheren Hafens" sehen vor, dass das Handelsministerium der USA ein Verzeichnis derjenigen Firmen führt, die sich öffentlich zur Einhaltung dieser Safe-Harbor-Prinzipien verpflichtet haben. An Hand dieser auch im Internet veröffentlichten Liste können z.B. europäische Unternehmen feststellen, an welche US-Unternehmen personenbezogene Daten übermittelt werden können, ohne dass zusätzliche Garantien verlangt werden müssen.
Die vereinbarten Prinzipien beinhalten folgende wesentliche Voraussetzungen für einen Datentransfer:

- Informationspflichten über die Art der Daten und der Erhebung, den Zweck, die Art der Empfänger und die Wahlmöglichkeiten hinsichtlich der Begrenzung der Nutzung und Übermittlung,
- Wahlrecht hinsichtlich der Nutzung der Daten,
- Wahlrecht hinsichtlich der Weiterübermittlung der Daten an Dritte,
- Angemessene Maßnahmen zur Sicherheit der Datenverarbeitung,
- Erforderlichkeit, Richtigkeit, Vollständigkeit und Aktualität der Daten im Rahmen ihrer den Prinzipien entsprechenden Zweckbestimmung,
- Recht auf Auskunft,
- Effektive Durchsetzung der Prinzipien.

Darüber hinaus arbeitet die Europäische Kommission an sogenannten Standardvertragsklauseln, bei deren Vereinbarung eine Datenübermittlung an Drittstaaten zulässig sein soll, da sie ausreichende Datenschutzgarantien beinhalten. Bis zum jetzigen Zeitpunkt liegt jedoch immer noch nur ein Entwurf dieser Klauseln vor. Mit einer baldigen Entscheidung der Kommission hierüber ist zu rechnen. Sie wäre im Interesse der Rechtssicherheit insbesondere der Wirtschaft auch wünschenswert.

3.4 Teilnahme an den Sitzungen der Arbeitsgruppe "Telekommunikation, Tele- und Mediendienste"

Im Berichtszeitraum nahm auch wieder ein Vertreter Brandenburgs an den regelmäßigen Sitzungen der Arbeitsgruppe "Telekommunikation, Tele- und Mediendienste" teil. Ein wesentliches Beratungsthema ist oben schon unter Ziffer 3.2.1 (Datenschutz in Call-Centern) erörtert worden. Auf die Ausführungen darf verwiesen werden. Ansonsten beschäftigte sich die Arbeitsgruppe unter anderem mit der aktuellen Rechtsentwicklung (Änderung der Telekommunikations-Datenschutzverordnung und dem Entwurf für eine Rechtsverordnung nach § 88 Telekommunikationsgesetz -Telekommunikations-Überwachungsverordnung). Auch wurde der Arbeitsgruppe Versicherungswirtschaft hinsichtlich des Internetauftritts von Versicherungen (siehe Ziffer 3.2.2) zugearbeitet.

4. Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht (LDA)

Wie bereits in den vorangegangenen Jahren fanden wieder Gespräche zwischen dem LDA und Vertretern der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich statt. In diesen Gespräche wurden Themen erörtert, die beide Institutionen betreffen. Zu bestimmten Problemen kann keine einheitliche Meinung erlangt werden und die unterschiedlichen Rechtsauffassung bleiben bestehen (siehe Ziffer 4.1).
In den meisten Fällen kann jedoch ein Konsens gefunden werden. Die Zusammenarbeit mit dem LDA verläuft auf einer sachlichen Ebene und kann als gut eingeschätzt werden. Unter Ziffer 4.2 wird kurz über eine gemeinsame Überprüfung eines Unternehmens berichtet.

4.1 Abrechnungen Apothekenrechenzentren

Im Rahmen der Tätigkeit der Aufsichtsbehörde wurde bekannt, dass es (und ähnlich in etlichen anderen Bundesländern) in Brandenburg seit Dezember 1997 eine Vereinbarung u.a. zwischen mehreren Apothekenrechenzentren und der Kassenärztlichen Vereinigung (KV) gab, die die Lieferung von Informationen zu Arznei- und Verbandmittelverordnungen der Vertragsärzte im Land Brandenburg an die KV zum Inhalt hat und sich damit außerhalb der in § 296 Abs. 3, § 297 Abs. 3 i.V.m. § 106 SGB V geregelten Voraussetzungen für derartige Datenlieferungen bewegt. Als Grund für den Abschluß einer solchen Vereinbarung wurde angeführt, dass die entsprechenden Daten von den Krankenkassen nicht quartalsweise (§ 296 Abs. 3 SGB V) sondern nur mit einem großen zeitlichen Rückstand an die KV übermittelt würden und diese dadurch ihre Beratungspflichten insbesondere gem. § 305 a SGB V nicht bzw. nicht wirkungsvoll genug wahrnehmen könne.

Die Vereinbarung betraf die Übermittlung solcher Daten, auf die die KV auf der Grundlage des § 296 Abs. 3, § 297 Abs.3 SGB V i.V.m. § 106 SGB V gegenüber den Krankenkassen einen Anspruch hat.
Ausweislich der Kopie der der Aufsichtsbehörde vorliegenden Vereinbarung wurde der KV quartalsbezogen ein Datensatz übermittelt, der folgende Informationen enthielt:

- Abrechnungsmonat,
- Arztnummer,
- Kassenart,
- Status,
- Zuzahlung,
- Bruttobetrag.

Die geschilderte Verfahrensweise erfolgte sowohl ohne Kenntnis und vertragliche Einbindung der Krankenkassen als auch ohne Zustimmung der betroffenen Ärzte.

Der LDA Brandenburg hatte in seiner Zuständigkeit gegenüber der KV die Vereinbarung als Übergangslösung bis zum Funktionieren des gesetzlich vorgeschriebenen Datenübermittlungsweges akzeptiert.

Die Aufsichtsbehörde vertrat die Auffassung, dass die in Rede stehende Vereinbarung keine ausreichende rechtliche Grundlage darstelle, um die Datenübermittlung von den Apothekenrechenzentren an die KV zu rechtfertigen.

Adressat der §§ 296 Abs. 3 und 297 Abs. 3 SGB V sind die Krankenkassen. Diese waren aber in das ganze Prozedere nicht eingebunden. Bei Einbeziehung der Krankenkassen in diese Vereinbarung, hätte das Ganze als rechtlich unbedenklich angesehen werden können.
Die Apothekenrechenzentren werden auf der Grundlage des § 300 SGB V tätig.
Nach der ab dem 01.01.2000 geltenden Rechtslage sind die von den Apotheken in Anspruch genommenen Rechenzentren befugt, gem. § 300 Abs. 2 SGB V die Daten für im SGB bestimmte Zwecke zu verarbeiten (wozu auch das Übermitteln gehört) und zu nutzen, **"soweit sie von einer berechtigten Stelle beauftragt worden sind"**. Die KV war nach Auffassung des Ministeriums des Innern keine solche berechtigte Stelle.
Da mit dem LDA, mit dem die Aufsichtsbehörde auf Grund seiner Zuständigkeit für die KV an der Problematik zusammenarbeitete, keine einheitliche Rechtsauffassung in dieser Frage zu erreichen war, hat sich das Ministerium des Innern an das für diese Rechtsmaterie zuständige Bundesministerium für Gesundheit (BMG) mit der Bitte um Stellungnahme zu der Rechtsfrage gewandt.
Das BMG hat in Abstimmung mit dem Bundesbeauftragten für den Datenschutz letztlich die Rechtsauffassung der Aufsichtsbehörde bestätigt.
Die in Rede stehende Vereinbarung ist zwischenzeitlich ausgelaufen und nicht mehr erneuert worden.

4.2 Gemeinsame Überprüfung eines Unternehmens

Die Aufsichtsbehörde führt, wie unter Ziffer 2.1 ausgeführt wird, regelmäßig Überprüfungen von Unternehmen durch, die im Register der Aufsichtsbehörde gemeldet sind. Unternehmen, die im Auftrag von öffentlichen Stellen Datenverarbeitung im Land Brandenburg durchführen, haben sich gemäß § 11 Abs. 1 Satz 3 Brandenburgisches Datenschutzgesetz der Kontrolle des LDA zu unterwerfen. So fand in diesem Berichtszeitraum eine Überprüfung eines Unternehmens statt, an der ein Vertreter des LDA, ein Vertreter des Berliner Beauftragten für Datenschutz und Akteneinsicht, ein Vertreter der Aufsichtsbehörde für den nicht-öffentlichen Bereich im Land Brandenburg teilnahmen.
Vor Ort wurde das Unternehmen vorgestellt. Des weiteren wurden Fragen zur Struktur des Unternehmens, zum betrieblichen Datenschutzbeauftragten sowie zur Verpflichtung der Mitarbeiter auf das Datengeheimnis erörtert. Den Schwerpunkt der Prüfung bildeten die vom Unternehmen getroffenen technisch-organisatorischen Maßnahmen. Die vorgefundenen Bedingungen wurden in einem Protokoll zusammengefasst.

Die vorgefundenen Bedingungen sowie die Auskünfte der Vertreter des Unternehmens ließen keine Verstöße gegen datenschutzrechtliche Regelungen erkennen.

5. Stand der Novellierung des BDSG

Das Bundeskabinett hat am 14. Juni 2000 den Entwurf für ein neues Bundesdatenschutzgesetz beschlossen. Das Gesetz hat mittlerweile den Bundestag und den Bundesrat passiert. Auf eine Darstellung des Gesetzgebungsverfahrens wird an dieser Stelle verzichtet. Wesentliche Aufgabe der Aufsichtsbehörde wird es nun sein, dem sicherlich bei den datenverarbeitenden Stellen vorhandenen Beratungsbedarf zu befriedigen und sich selbst mit den neuen Regelungen vertraut zu machen. Einige in den Vorjahren an dieser Stelle dargestellte Erwartungen an das neue Gesetz sind erfüllt worden. So wird es zukünftig eine Regelung zum Einsatz von Chip-Karten durch nicht-öffentliche Stellen geben. Außerdem enthält das Gesetz eine Regelung zur Videobeobachtung durch private Stellen (und auch öffentliche Stellen des Bundes). Zudem erfolgte eine Neukonzipierung der Straf- und Bußgeldvorschriften. Wie sich das Gesetz in der Praxis bewährt, bleibt abzuwarten.