Datenschutz im nichtöffentlichen Bereich

Zweiter Tätigkeitsbericht des Innenministeriums

2003

Baden-Württemberg
INNENMINISTERIUM

Inhaltsverzeichnis

Gesetzlicher Berichtsauftrag

Die Datenschutzaufsicht im Bereich der Wirtschaftsunternehmen und der sonstigen nicht-öffentlichen Stellen ist Aufgabe des Innenministeriums. Als Aufsichtsbehörde kontrolliert es die Ausführung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz. Nach § 39 des Landesdatenschutzgesetzes erstattet das Innenministerium dem Landtag zum 1. Juli jeden zweiten Jahres, erstmals 2001, einen Bericht über die Tätigkeit der Aufsichtsbehörde.

Dies ist der zweite Bericht nach Einführung der gesetzlichen Berichtspflicht. Der erste Tätigkeitsbericht (Landtagsdrucksache 13/40) enthielt grundlegende Ausführungen zu den Aufgaben und der Tätigkeit des Innenministeriums auf dem Gebiet des Datenschutzes im nichtöffentlichen Bereich. Der Bericht baut auf dem ersten Tätigkeitsbericht auf und beschränkt sich auf Neuerungen und Entwicklungen, die im Berichtszeitraum (1.7.2001 bis 1.7.2003) eingetreten sind.

A Entwicklung der Aufgaben seit 2001

1.1 Neues Bundesdatenschutzgesetz - neue rechtliche Rahmenbedingungen für die Aufsichtsbehörde

Im Jahr 2001 wurde das Bundesdatenschutzgesetz (BDSG) im Zuge der Anpassung an die EG-Datenschutzrichtlinie in zahlreichen Punkten geändert oder ergänzt. In einigen weiteren Punkten wurde es - insoweit über die EG-Datenschutzrichtlinie hinausgehend - modernisiert und fortentwickelt. Besonders hervorzuheben sind folgende Neuerungen:

- Bereits bei der Einrichtung von Datenverarbeitungsverfahren sind die Grundsätze der Datenvermeidung und Datensparsamkeit zu beachten.

- Die Videoüberwachung öffentlich zugänglicher Räume, der Einsatz von Chipkarten und automatisierte Einzelentscheidungen sind nur unter besonderen Voraussetzungen zulässig, weil sie erhebliche Risiken für das informationelle Selbstbestimmungsrecht der Betroffenen mit sich bringen.

- Für die Verarbeitung sog. besonderer Arten von personenbezogenen Daten, beispielsweise von Angaben über die ethnische Herkunft oder die Gesundheit, wurden besondere Schutzvorkehrungen vorgesehen. In bestimmten Fällen ist deshalb eine Vorabkontrolle durchzuführen, bevor ein automatisiertes Datenverarbeitungsverfahren zum Einsatz kommt.

Insgesamt ist das neue Bundesdatenschutzgesetz umfangreicher und zum Teil komplizierter geworden. In erster Linie sind hiervon die Wirtschaftsunternehmen und die sonstigen nichtöffentlichen Stellen betroffen. Betroffen ist aber auch die Aufsichtsbehörde, die bei ihrer tagtäglichen Arbeit - der Bearbeitung von Beschwerden Betroffener und der Beratung und Kontrolle der nichtöffentlichen Stellen - das Bundesdatenschutzgesetz zu Grunde legt. Es ist deshalb auch aus dem Blickwinkel der Aufsichtsbehörde zu begrüßen, wenn das Bundesdatenschutzgesetz in einer zweiten Stufe unter anderem mit der Zielsetzung überarbeitet werden soll, die rechtlichen Grundlagen des Datenschutzes zu vereinfachen und die Lesbarkeit der Vorschriften zu erhöhen.

Darüber hinaus enthält das neue Bundesdatenschutzgesetz eine Reihe von Neuerungen, die sich unmittelbar auf die Aufsichtsbehörde praktisch auswirken:

- Vollkontrolle statt Anlasskontrolle:

  Nach der Neuregelung ist es möglich, generell jederzeit Kontrollen durchzuführen. Im Rahmen ihres Ermessens wird die Aufsichtsbehörde in der Praxis auch künftig vorrangig in den Fällen tätig werden, in denen Anhaltspunkte für Datenschutzverstöße vorliegen.

- Ausdehnung der Ordnungswidrigkeiten-Tatbestände; Strafantragsrecht der Aufsichtsbehörde:

  Nunmehr hat die Aufsichtsbehörde auch die Möglichkeit, die unbefugte Verarbeitung personenbezogener Daten in den vom Gesetz genannten Fällen zu verfolgen und mit Bußgeld zu ahnden (§ 43 BDSG). Bei besonders schweren Verstößen hat die Aufsichtsbehörde - neben dem Betroffenen - ein Strafantragsrecht (§ 44 BDSG).

- Datenübermittlung in das Ausland:

  Die Übermittlung von personenbezogenen Daten an öffentliche oder nichtöffentliche Stellen in einem Mitgliedstaat der Europäischen Union wurde der Übermittlung zwischen Stellen im Inland gleichgestellt. Dies ist gerechtfertigt, da nach der Umsetzung der EU-Datenschutzrichtlinie durch die Mitgliedstaaten innerhalb der Gemeinschaft ein einheitliches Datenschutzniveau hergestellt worden ist. Für die Übermittlung an einen Empfänger in einem Staat außerhalb der Gemeinschaft („Drittland“) ist entsprechend der Richtlinie eine differenzierte Regelung vorgesehen (§§ 4b und 4c BDSG). Voraussetzung ist, dass bei der Stelle im Drittland, an die übermittelt werden soll, ein angemessenes Datenschutzniveau besteht. Ist dies nicht der Fall, ist eine Datenübermittlung nur zulässig, wenn einer der in § 4c Abs. 1 BDSG genannten Ausnahmetatbestände vorliegt. In Betracht kommt auch, dass die beteiligten Stellen ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte geben (§ 4c Abs. 2 BDSG). Auf Abschnitt B Nr. 3 wird verwiesen.

- Prüfung von Verhaltensregeln:

  Das Gesetz sieht vor, dass Berufs- und Wirtschaftsverbände Verhaltensregelungen zur Förderung der Durchführung von datenschutzrechtlichen Regelun-

gen erarbeiten sollen. Die Aufsichtsbehörde überprüft die Vereinbarkeit der ihr unterbreiteten Entwürfe mit dem geltenden Datenschutzrecht (§ 38a BDSG).

- Selbstkontrolle der Wirtschaft und der sonstigen nichtöffentlichen Stellen:

  Die zentrale Rolle des betrieblichen Datenschutzbeauftragten als Instrument der Selbstkontrolle ist im neuen Bundesdatenschutzgesetz noch stärker betont worden. Bei der Datenschutzkontrolle im Bereich der Unternehmen und sonstigen nichtöffentlichen Stellen steht nach dem Gesetz die Selbstkontrolle im Vordergrund, während der Aufsichtsbehörde die Aufgabe einer ergänzenden Fremdkontrolle zukommt. Nichtöffentliche Stellen sind zur Bestellung von Datenschutzbeauftragten verpflichtet, wenn sie personenbezogene Daten automatisiert verarbeiten und hiermit mindestens fünf Arbeitnehmer beschäftigen; erfolgt die Verarbeitung auf andere Weise, greift die Verpflichtung ab der Schwelle von 20 Personen. Bestimmte Stellen haben unabhängig von der Zahl der Personen einen Datenschutzbeauftragten zu bestellen (z. B. Auskunfteien). Der betriebliche Datenschutzbeauftragte hat insbesondere die Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden, zu überwachen. Er ist nach dem Gesetz auch zuständig für die Durchführung der Vorabkontrolle. Der damit verbundenen Verantwortung müssen sich die Unternehmen und sonstigen nichtöffentlichen Stellen bewusst sein.

2 Aufsicht in Zahlen

2.1 Datenschutzregister

Im Zuge der Novellierung des BDSG wurden auch die Bestimmungen über die Meldepflicht zum Datenschutzregister geändert. Zu dem von der Aufsichtsbehörde zu führenden Datenschutzregister sind nach § 4d BDSG nunmehr von den verantwortlichen Stellen grundsätzlich alle Verfahren automatisierter Verarbeitungen personenbezogener Daten vor deren Inbetriebnahme zu melden. Jedoch gibt es hiervon zahlreiche Ausnahmen, so dass die Meldung praktisch zur Ausnahme wird. Insbesondere besteht nach der Neuregelung keine Meldepflicht mehr für Stellen, die Daten für andere im Rahmen eines Auftragsverhältnisses verarbeiten (z. B. Dienstleistungsrechenzentren).

Bis zur Novellierung des BDSG im Mai 2001 waren 1369 meldepflichtige datenverarbeitende Stellen in dem bei der Aufsichtsbehörde geführten Register eingetragen. Nach der Umstellung auf die neue Rechtslage sind nur noch 72 Stellen mit

insgesamt 74 automatisierten Verfahren zum Datenschutzregister gemeldet. 43 dieser Verfahren dienen dem Zweck der Übermittlung von Daten (Auskunfteien und Adresshändler) und 31 der Verfahren dienen dem Zweck der anonymisierten Datenübermittlung (Markt- und Meinungsforschungsinstitute).

2.2 Anfragen, Eingaben und Anlassüberprüfungen

Tätigkeitsschwerpunkte der Aufsichtsbehörde sind die Bearbeitung von Beschwerden Betroffener, die Beratung und die Kontrolle. Dies spiegelt sich in folgenden Zahlen im Berichtszeitraum 2001 bis 2002 wider:

Schriftliche Anfragen		
- Sachfragen mit beratender Stellungnahme von datenverarbeitenden Stellen, betrieblichen Datenschutzbeauftragten und Betriebsräten	200	
- Eingaben Betroffener	667	
Abgabe wegen Unzuständigkeit/kein BDSG-Anwendungsbereich	96	
Beratung, Auskunft	225	
Anlassüberprüfung erforderlich	346	
Ergebnis: Verfahren korrekt		67%
Ergebnis: Empfehlung/Beanstandung		33%
Telefonische Anfragen	4000	

Erläuterungen zu der Tabelle:

2.2.1 Schriftliche Anfragen

Die schriftlichen Anfragen werden bei der Aufsichtsbehörde unterschieden in Anfragen zu Sachfragen, zu welchen die Aufsichtsbehörde eine beratende Stellungnahme abgibt, und in Eingaben von Bürgern, die sich wegen eines vermuteten datenschutzrechtlichen Verstoßes an die Aufsichtsbehörde wenden.

- Sachfragen mit beratender Stellungnahme

Rund 200 der schriftlichen Anfragen waren Sachfragen. Diese wurden überwiegend im Zusammenhang mit geplanten oder bereits anlaufenden Verarbeitungsvorhaben gestellt. Verantwortliche datenverarbeitende Stellen, betriebliche Datenschutzbeauftragte und Betriebsräte nutzten die Möglichkeit, sich von der Aufsichtsbehörde beraten zu lassen. Ein erhöhter Aufklärungsbedarf bestand insbesondere zur Position und Funktion des betrieblichen Datenschutzbeauftragten nach der entsprechenden Neuregelung in § 4g BDSG.

- Eingaben Betroffener

Insgesamt 667 der schriftlichen Anfragen waren Eingaben betroffener Bürger, die sich an die Aufsichtsbehörde wandten, weil sie im Umgang mit ihren personenbezogenen Daten einen Datenschutzverstoß annahmen. Gegenüber dem vorangegangenen Berichtszeitraum ist dies eine deutliche Zunahme (von gut 10 %). Die Steigerung ist zu einem erheblichen Teil auf die wachsende Kommunikation über E-Mail zurückzuführen.

In 96 Fällen war die Eingabe an andere Datenschutzaufsichtsbehörden abzugeben oder es war der Anwendungsbereich des BDSG nicht eröffnet, weil die Daten weder unter Einsatz von Datenverarbeitungsanlagen verarbeitet wurden noch in oder aus nicht automatisierten Dateien. In den verbleibenden 571 Fällen betrafen die Eingaben schwerpunktmäßig folgende Bereiche:

- in 65 Fällen Einzel-, Groß- und Versandhandel und Energieversorgungsunternehmen (die weit überwiegende Anzahl der Fälle betraf die Nutzung und Weitergabe von Daten für Werbezwecke und die Nichterfüllung des Auskunftsanspruchs über die Herkunft der für die Werbesendung verwendeten Adresse),
- in 62 Fällen Kreditinstitute, Banken und Bausparkassen,
- in 57 Fällen Unternehmen des Adresshandels sowie der Direktmarketing- und Werbebranche,
- in 56 Fällen Auskunfteien,
- in 42 Fällen Mediendiensteunternehmen,
- in 34 Fällen Versicherungsgesellschaften,
- in 34 Fällen den Datenschutz in Arbeitsverhältnissen,
- in 33 Fällen die Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA),
- in 32 Fällen das Gesundheitswesen,
- in 30 Fällen Teledienstunternehmen,
- in 29 Fällen Inkassounternehmen,
- in 23 Fällen Vereine, Parteien und sonstige Interessengemeinschaften,
- in 21 Fällen Vermieter, Hausverwaltungen und Mietervereine,

- in 5 Fällen Markt- und Meinungsforschungsinstitute,
- in 5 Fällen Berufe mit besonderer Schweigepflicht,
- in 5 Fällen Presse und Printmedien,
- übrige Fälle: sonstige Unternehmensbereiche.

2.2.2 Anlassüberprüfungen

In 346 Fällen waren auf Grund der Sachverhaltsschilderungen und der vorgelegten Unterlagen Anhaltspunkte für einen Verstoß gegen datenschutzrechtliche Bestimmungen gegeben. Die datenverarbeitenden Stellen wurden aus diesem Anlass schriftlich überprüft. Zu den häufigsten Mängeln zählten wie bereits im vorherigen Berichtszeitraum die Nichterfüllung des Auskunftsanspruchs über die Herkunft der verwendeten personenbezogenen Daten in Werbeangelegenheiten. Es kam auch zu Personenverwechslungen auf Grund nicht ausreichender Identifizierung und Prüfung der Angaben, beispielsweise im Bereich der Auskunfteien und Kreditschutzorganisationen. In einer Reihe von Fällen wurden die Betroffenen bei der Erhebung der Daten nicht ausreichend über den Zweck der weiteren Verarbeitung ihrer Daten aufgeklärt.

2.2.3 Telefonische Anfragen

Im Berichtszeitraum waren von den Mitarbeiterinnen und Mitarbeitern der Aufsichtsbehörde wieder rund 4000 telefonische Anfragen zu beantworten. Insbesondere wegen der Novellierung des BDSG war in zunehmendem Maße die Beratungsfunktion der Aufsichtsbehörde gefragt. In der weit überwiegenden Anzahl der Fälle war eine telefonische Information und Beratung über die Rechtslage ausreichend. In den restlichen Fällen wurde für eine Überprüfung und datenschutzrechtliche Bewertung eine schriftliche Vorlage unter Anschluss der entsprechenden Unterlagen erbeten.

2.3 Schwerpunktmäßige Sonderüberprüfungen

Im Rahmen schwerpunktmäßiger Sonderüberprüfungen wurden im Berichtszeitraum folgende Kontrollen durchgeführt:

Videoüberwachung in Kaufhäusern und Banken	5 (siehe Teil B Nr. 1)
private Rundfunkanbieter	20 (siehe Teil B Nr. 2)

private Fernsehanbieter	5 (siehe Teil B Nr. 2)
Telefon-Servicecenter bei Banken	2 (siehe Teil B Nr. 7.1)
Abrechnungsstellen medizinischer Leistungen	12 (siehe Teil B Nr. 9.1).

3 Ordnungswidrigkeitenverfahren

Im novellierten BDSG ist der Tatbestandskatalog der Ordnungswidrigkeiten erweitert worden. Zum einen wurden damit Sanktionsmöglichkeiten für die neuen Ge- und Verbote geschaffen, es wurde dabei aber auch der Grundtatbestand der bisherigen Strafvorschrift in einen Ordnungswidrigkeitentatbestand überführt, um eine flexiblere Handhabung durch die Aufsichtsbehörden zu ermöglichen.

So wurden im Berichtszeitraum gegen elf verantwortliche Stellen Ordnungswidrigkeitenverfahren eingeleitet. In vier dieser Fälle haben die verantwortlichen Stellen entgegen § 38 Abs. 3 Satz 1 BDSG der Aufsichtsbehörde gegenüber keine Auskunft erteilt. In drei Fällen sind die verantwortlichen Stellen trotz Aufforderung ihrer Meldepflicht zum Register nicht nachgekommen. Vier Fälle wurden von der Staatsanwaltschaft an die Aufsichtsbehörde übergeben, wobei in zwei Fällen kein Ordnungswidrigkeitentatbestand erfüllt war und ein Fall mangels Zuständigkeit an eine andere örtlich zuständige Aufsichtsbehörde abgegeben werden musste. Insgesamt wurde in drei Fällen ein Bußgeldbescheid erlassen. Die übrigen Verfahren wurden nach pflichtgemäßem Ermessen eingestellt.

B Einzelne Bereiche

1 Videoüberwachung

Die Anwendung der Videotechnik hat in vielen Bereichen des täglichen Lebens entsprechend der Weiterentwicklung der Technik auf diesem Gebiet stetig zugenommen. Der Gesetzgeber hat hierauf reagiert und im novellierten Bundesdatenschutzgesetz erstmalig eine Regelung zur Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) aufgenommen (§ 6b BDSG).

> Mit der Neuregelung hat sich die Aufsichtsbehörde in Form eines „Hinweises des Innenministeriums zum Datenschutz für private Unternehmen und Organisationen“ (Hinweis Nr. 40) eingehend auseinandergesetzt. Der Hinweis Nr. 40 befasst sich sowohl mit der Videoüberwachung durch eine Privatperson, namentlich im Zusammenhang mit der Zugangskontrolle zum Privatwohnhaus, als auch mit der Videoüberwachung im Bereich der Wirtschaft. Der Hinweis ist im Internet unter www.im.bwl.de (Rubrik Datenschutz/Hinweise) abrufbar.

Im Bereich der Wirtschaft hat die Aufsichtsbehörde die Überwachung bei Kaufhäusern und Banken näher unter die Lupe genommen. Dabei hat sich gezeigt, dass folgende drei Aspekte in der Praxis besonders bedeutsam sind:

- Zulässigkeit der Überwachung: Nach dem Gesetz ist die Videoüberwachung zulässig, wenn sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte für ein überwiegendes schutzwürdiges Interesse der Betroffenen bestehen.

- Transparenz der Überwachung: Für den Betroffenen muss erkennbar sein, dass und von wem er überwacht wird. Dies bedeutet, dass der Betroffene vor dem Eintritt in den überwachten Bereich entsprechend zu informieren ist.

- Löschung der Aufzeichnungen: Die Überwachungsaufnahmen sind unverzüglich zu löschen, wenn sie zum Erreichen des Überwachungszwecks nicht mehr erforderlich sind oder schutzwürdige

nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegen stehen.

1.1 Kaufhäuser

Die Überprüfung führte zu der Feststellung, dass die Voraussetzungen, unter denen eine Videoüberwachung nach § 6b Abs. 1 Nr. 2 und 3 BDSG zulässig ist, grundsätzlich eingehalten wurden. Die Videoüberwachung ist in diesen Fällen zur Wahrnehmung des Hausrechts und insbesondere zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke, d.h. zum Schutz vor Ladendiebstahl, erforderlich. Diese Rechtsauffassung kann sich auch auf ein Urteil des Landgerichts Stuttgart stützen, das die Videoüberwachung im Kaufhaus im „Sinne eines effektiven Eigentumsschutzes für geradezu geboten hält“.

Zu beanstanden war jedoch, wie mit den Aufzeichnungen umgegangen wurde. Meistens wurden die Aufnahmen eines Tages auf einer Videokassette aufgezeichnet und diese nach Ladenschluss in einem Schrank oder einer Schublade, mehr oder weniger geordnet, verwahrt. Soweit die Aufzeichnungen nicht als Beweismittel benötigt wurden, wurden sie irgendwann durch Überspielen gelöscht. Diese Verfahrensweise steht nicht mit dem Bundesdatenschutzgesetz in Einklang. Die Aufzeichnungen hätten, soweit sie nicht als Beweismittel benötigt wurden, unverzüglich gelöscht werden müssen. Dies ist im Gesetz klar geregelt. Bei einer vollständigen Aufzeichnung eines Geschäftstags (z.B. in einer Black Box) sind deshalb die Aufzeichnungen innerhalb von ein bis zwei Arbeitstagen auszuwerten und, wenn sie nicht als Beweismittel benötigt werden, zu löschen. Den betroffenen Kaufhäusern wurde eingehend dargelegt, wie in der Zukunft richtig zu verfahren ist.

Zu beanstanden war auch, dass die Videoüberwachung entgegen dem Gesetz nicht immer ausreichend erkennbar gemacht wurde. Die entsprechenden Hinweise fehlten teilweise oder waren versteckt angebracht. Diese Mängel sind in den von der Aufsichtsbehörde kontrollierten Häusern zwischenzeitlich abgestellt worden.

1.2 Banken

Banken setzen zum Schutz vor Straftaten üblicherweise optische Überwachungsanlagen ein. Hierzu gehören die gut sichtbar angebrachten Überfallkameras im

Kassenraum, Videoüberwachungsanlagen im öffentlich zugänglichen Bereich (Schalterhalle) und Überwachungskameras bei den Geldausgabeautomaten.

Die Überfallkameras, die üblicherweise erst bei einem Überfall durch Knopfdruck eines Mitarbeiters aktiviert werden, werden von der Aufsichtsbehörde nicht als Überwachungsanlage im Sinne des Bundesdatenschutzgesetzes qualifiziert, da sie durch die manuelle Aktivierung nur eine konkrete strafbare Handlung dokumentieren. Die Videoüberwachung der Räumlichkeiten, insbesondere des Vorraums, in dem sich der Geldausgabeautomat und der Kontoauszugsdrucker befinden, sowie die Überwachung der Geldausgabeautomaten fallen dagegen unter die erwähnte Vorschrift des Bundesdatenschutzgesetzes.

Problematisch war die Dauer der Speicherung der Aufnahmen der Überwachungskameras bei den Geldausgabeautomaten. Während bei der Videoüberwachung der Räumlichkeiten schnell feststeht, ob der Zweck der Überwachung erreicht ist, da ein Schaden im Regelfall immer sofort erkennbar ist, ist dies bei den Geldausgabeautomaten nicht sogleich möglich. Beispielsweise wird im Falle des Scheckkartenmissbrauchs am Geldausgabeautomaten eine unberechtigte Abhebung erst auf dem nächsten Kontoauszug des Geschädigten sichtbar und der Bank erst bekannt, wenn der Kunde sich meldet. In diesem Fall versucht dann die Bank, dem Auszahlungsvorgang die entsprechende Aufnahme der Überwachungskamera am Automaten zuzuordnen, um den Täter zu erkennen. Da der Zeitraum für die Erstellung eines Kontoauszugs je nach Art des Girokontovertrages unterschiedlich lang sein kann und der Kunde zudem noch eine Einspruchfrist hat, muss die Bank die Videoaufzeichnungen als mögliches Beweismittel über mehrere Wochen hinweg aufbewahren, bis sie für die Erreichung des Überwachungszwecks nicht mehr erforderlich ist. Bei der Auswahl und Einrichtung des Systems muss deshalb die Bank dafür sorgen, dass sie den unterschiedlichen Aufbewahrungsfristen Rechnung tragen kann.

2 Private Rundfunk- und Fernsehanbieter

Privaten Rundfunk- und Fernsehanbietern steht nach § 49 des Landesmediengesetzes - ebenso wie dem öffentlichrechtlichen Rundfunk und der Presse - das sog. Medienprivileg zu. Soweit sie personenbezogene Daten ausschließlich zu eigenen journalistisch-redaktionellen Zwecken verarbeiten, gelten deshalb nur einige wenige Datenschutzvorschriften wie beispielsweise die Bestimmung über das Datengeheimnis und die Bestimmung über technische und organisatorische Maßnahmen zur Sicherung der Daten. Zum Ausgleich hierfür sind private Rundfunk- und Fernsehanbieter gesetzlich verpflichtet, unabhängig von der

sehanbieter gesetzlich verpflichtet, unabhängig von der Zahl der mit der Datenverarbeitung beschäftigten Arbeitnehmer einen Beauftragten für den Datenschutz zu bestellen, der im journalistisch-redaktionellen Bereich die Einhaltung dieser Vorschriften überwacht. Außerhalb des journalistisch-redaktionellen Bereichs sind die Datenschutzvorschriften in vollem Umfang anzuwenden. Dies gilt beispielsweise für Hörerdaten, soweit solche erhoben werden.

Für die Aufsichtsbehörde besteht deshalb nur eine eingeschränkte Kontrollzuständigkeit bei privaten Rundfunk- und Fernsehanbietern. Hinsichtlich des journalistisch-redaktionellen Bereichs ist zu respektieren, dass die Überwachung des Datenschutzes dem betrieblichen Beauftragten für den Datenschutz obliegt. Um so wichtiger war es deshalb zu überprüfen, ob die privaten Anstalten ihrer Verpflichtung zur Einsetzung von Datenschutzbeauftragten in der Praxis auch nachkommen.

Die Überprüfung bei den insgesamt 25 Anbietern hat ergeben, dass nicht alle Anbieter ihrer Verpflichtung zur Bestellung eines Datenschutzbeauftragten ausreichend nachgekommen waren. Die betroffenen Anbieter zeigten sich jedoch einsichtig. Mit Abschluss der Überprüfung waren daher alle erforderlichen Datenschutzbeauftragten bestellt.

Hörerdaten wurden von den privaten Anbietern nur in geringem Umfang erhoben und gespeichert, beispielsweise im Zusammenhang mit Preisausschreiben. Der Umgang mit diesen Daten entsprach dem Gesetz; insbesondere wurden die Daten nach den Feststellungen der Aufsichtsbehörde nicht an Dritte weitergegeben.

3 Internationaler Datenverkehr

Erklärtes Hauptziel der EG-Datenschutzrichtlinie war es, ein einheitliches Datenschutzniveau in der EU herbeizuführen und damit die Voraussetzung für einen freien Datenverkehr in der Gemeinschaft zu schaffen. Daher war der innergemeinschaftliche Datenverkehr dem inländischen gleichzustellen. Nach dem neuen Bundesdatenschutzgesetz ist deshalb die Übermittlung an (öffentliche oder nichtöffentliche) Stellen eines anderen Mitgliedstaats unter den gleichen Voraussetzungen zulässig wie die Übermittlung zwischen Stellen im Inland. In diese Regelung sind neben den 15 Mitgliedstaaten auch die drei Staaten des europäischen Wirtschaftsraums (Liechtenstein, Norwegen und Island) sowie die Organe und Einrichtungen der Europäischen Gemeinschaft einbezogen.

Besondere Voraussetzungen gelten dagegen für die Übermittlung an öffentliche oder nichtöffentliche Stellen in einem Land außerhalb der EU („Drittland“). Hier sieht das neue Bundesdatenschutzgesetz entsprechend der Richtlinie eine differenzierte Regelung vor (§§ 4b und 4c BDSG). Voraussetzung ist, dass bei der Stelle im Drittland, an die übermittelt werden soll, ein angemessenes Datenschutzniveau besteht. Ist dies nicht der Fall, ist eine Datenübermittlung nur zulässig, wenn einer der in § 4c Abs. 1 BDSG genannten Ausnahmetatbestände vorliegt oder die übermittelnde Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist.

Die §§ 4b und 4c BDSG enthalten jedoch nur die zusätzlichen Voraussetzungen, die vorliegen müssen, wenn Daten in ein Drittland übermittelt werden sollen. Die in den §§ 28 und 29 BDSG geregelten allgemeinen Voraussetzungen für die Zulässigkeit einer Übermittlung müssen unabhängig hiervon - wie bei jeder anderen Datenübermittlung auch - ebenfalls gegeben sein.

Die Aufsichtsbehörde hat sich mit den Fragen des internationalen Datenverkehrs, die sich auf Grund der neuen Rechtslage ergeben, frühzeitig befasst, da hiervon in der Praxis viele in Baden-Württemberg ansässige Unternehmen betroffen sind. Bei der Datenübermittlung in ein Drittland sind - kurz gefasst - folgende Gesichtspunkte zu beachten:

3.1 Angemessenes Datenschutzniveau im Drittland

Die Verantwortung für die Zulässigkeit der Übermittlung trägt nach § 4b Abs. 5 BDSG die übermittelnde Stelle. Deshalb ist es ihre Aufgabe zu prüfen, ob bei der öffentlichen oder nichtöffentlichen Stelle im Drittland, an die übermittelt werden soll, ein angemessenes Datenschutzniveau gewährleistet ist.

Zu berücksichtigen ist, dass die Europäische Kommission nach der EG-Datenschutzrichtlinie für ein Drittland die Feststellung treffen kann, dass es auf Grund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen ein angemessenes Datenschutzniveau gewährleistet. Diese Feststellung ist für die Mitgliedstaaten verbindlich. Entsprechende Feststellungen hat die Kommission für die Schweiz, Ungarn und Argentinien getroffen. Für Kanada ist die Feststellung an das stufenweise Inkrafttreten des kanadischen Datenschutzgesetzes gebunden, das erst zum 1.1.2004 uneingeschränkte Anwendung findet.

Einen Spezialfall bilden die USA. US-Firmen können sich gegenüber dem US-Handelsministerium zur Einhaltung der „Grundsätze des sicheren Hafens zum Datenschutz (Safe Harbor)“ verpflichten. Diese Grundsätze, die zwischen der Europäischen Union und den USA vereinbart worden sind, stellen sicher, dass die an ein US-Unternehmen übermittelten Daten nur im Einklang mit den europäischen Datenschutz-Standards weiter verarbeitet werden. Soweit die „Safe-Harbor-Regelungen“ zur Anwendung kommen, hat die Europäische Kommission ebenfalls ein angemessenes Datenschutzniveau festgestellt. Nach einer Mitteilung der EU-Kommission waren zum 13.03.2003 insgesamt 310 Unternehmen mit Sitz in den USA zur Einhaltung der Safe-Harbor-Grundsätze verpflichtet und in der Liste des US-Handelsministeriums geführt.

3.2 Standardvertragsklauseln

Für den Fall, dass Daten in ein Drittland ohne ausreichendes Datenschutzniveau übermittelt werden sollen, sieht § 4c Abs. 1 BDSG verschiedene Ausnahmetatbestände vor. Die Ausnahmen sind weit gefasst, um den Wirtschaftsverkehr nicht unangemessen zu beeinträchtigen. Danach können Daten beispielsweise übermittelt werden zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen.

Kommt keiner der Ausnahmetatbestände zur Anwendung, können die Daten nur übermittelt werden, wenn die übermittelnde Stelle ausreichende Garantien hinsichtlich des Datenschutzes vorweisen kann.

Ausreichende Garantien können sich insbesondere aus Vertragsklauseln ergeben. Insoweit ist zu berücksichtigen, dass die Europäische Kommission nach der EG-Datenschutzrichtlinie darüber befinden kann, ob bestimmte Standardvertragsklauseln ausreichende Garantien bieten. Stellt sie dies fest, ist ihre Entscheidung für die Mitgliedstaaten verbindlich. Von dieser Möglichkeit hat die Kommission Gebrauch gemacht.

Erfolgt die Datenübermittlung in Drittländer auf der Grundlage der vertraglich vereinbarten Standardvertragsklauseln der Europäischen Kommission, bedarf die Datenübermittlung keiner zusätzlichen Genehmigung durch die Aufsichtsbehörde. Dies schließt jedoch nicht aus, dass die Aufsichtsbehörde im Rahmen ihrer Aufsichtstätigkeit die Vorlage der vereinbarten Standardvertragsklauseln zu Überprüfungszwecken verlangen kann.

3.3 Unternehmensregelungen

Für das Datenschutzrecht stehen rechtlich selbständige Unternehmen eines Konzerns untereinander im Verhältnis von Dritten. Sonderregelungen oder Erleichterungen für Konzerne gibt es nicht. Daher ist die Weitergabe von Daten zwischen den konzernangehörigen Unternehmen als Datenübermittlung einzustufen. Befindet sich das datenempfangende Unternehmen in einem Drittland, sind deshalb die besonderen Vorschriften der §§ 4b und 4c BDSG anzuwenden.

Auch in diesem Fall ist es grundsätzlich möglich, mit Vertragsklauseln, insbesondere den erwähnten Standardvertragsklauseln, zu arbeiten. Im Einzelfall kann es jedoch praktischer sein, mit einer Unternehmensregelung zum Datenschutz konzernintern ein angemessenes Datenschutzniveau herzustellen.

Die größte Gewähr dafür, dass Unternehmensregelungen ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweisen, besteht dann, wenn sie sich inhaltlich an den aus den Standardvertragsklauseln der Europäischen Kommission für die Übermittlung personenbezogener Daten in Drittländer ableitbaren datenschutzrechtlichen Standards orientieren. Inhaltliche Abweichungen von den Vorgaben der Standardvertragsklauseln können dann unschädlich sein, wenn sie durch sonstige verbindliche unternehmensinterne Regelungen und organisatorische Maßnahmen hinreichend kompensiert werden können.

Ausreichende Garantien können sich jedoch nur aus Unternehmensregelungen ergeben, die verbindlich, d.h. rechtlich durchsetzbar sind. Die Verbindlichkeit der unternehmensinternen Vorschriften muss dabei sowohl intern als auch gegenüber der Außenwelt, insbesondere gegenüber dem Betroffenen, gegeben sein. Welche Regelungsinstrumente die Unternehmen hierzu einsetzen, bleibt ihnen überlassen.

Für Datenübermittlungen in Drittländer auf der Grundlage verbindlicher Unternehmensregelungen ist nach Auffassung der Aufsichtsbehörde keine Genehmigung erforderlich, wenn die Unternehmensregelung bei der Daten empfangenden Stelle im Drittland ein „angemessenes Datenschutzniveau“ im Sinne von § 4b BDSG begründet. Diese Vorschrift ist offen formuliert. Danach sind bei der Beurteilung, ob bei der Daten empfangenden Stelle im Drittland ein angemessenes Datenschutzniveau vorhanden ist, alle Umstände zu berücksichtigen, also auch verbindliche Unternehmensregelungen.

Unternehmensregelungen, soweit sie rechtlich verbindlich und durchsetzbar sind, vermitteln keinen geringeren Datenschutzstandard als staatliche Rechtsvorschriften. Insoweit besteht eine Parallele zu den von der Europäischen Kommission anerkannten „Safe-Harbor-Regelungen“ der USA. Auch dort beruht das angemessene Datenschutzniveau letztlich auf rechtlich verbindlichen Selbstverpflichtungen der Daten empfangenden Unternehmen.

> Mit der Datenübermittlung in Drittländer hat sich die Aufsichtsbehörde in Form von „Hinweisen des Innenministeriums zum Datenschutz für private Unternehmen und Organisationen (Nr. 39 und Nr. 40)“ befasst. Die Hinweise sind im Internet unter www.im.bwl.de unter der Rubrik Datenschutz/Hinweise abrufbar.

4 Auskunfteien und Kreditschutzorganisationen

4.1 Verwendung von Inkassodaten für Zwecke einer Auskunftei

Viele Unternehmen wie beispielsweise Versandhäuser und Mobilfunkunternehmen fragen vor dem Vertragsschluss zur besseren Abschätzung des wirtschaftlichen Risikos bei einer Auskunftei nach. Aus der Sicht des Datenschutzes ist dabei entscheidend, mit welchen Informationen die Auskunftei handelt. Im Falle einer großen Auskunftei haben sich immer wieder Betroffene an die Aufsichtsbehörde gewandt, die nicht damit einverstanden waren, dass die Auskunftei die Information „außergerichtliches Mahnverfahren“ speicherte und weitergab. Im konkreten Fall arbeitete die Auskunftei in großem Stil mit mehreren Inkassounternehmen zusammen.

Auf Grund des Bundesdatenschutzgesetzes ist es den Auskunfteien erlaubt, Informationen über die Bonität (Zahlungsfähigkeit und Zahlungswilligkeit) der Betroffenen zu speichern und bei Vorliegen eines berechtigten Interesses zu übermitteln. Im Hinblick auf die gesetzlichen Vorgaben (§ 29 Abs. 1 Nr. 1 BDSG) kommen dabei aber nur Fakten in Betracht, aus denen zwingende negative Rückschlüsse auf die Zahlungswilligkeit und Zahlungsfähigkeit des Betroffenen gezogen werden können. Dies ist bei gerichtlichen Mahn- oder Vollstreckungsbescheiden der Fall. Im vorgerichtlichen Verfahren ist es aber zunächst so, dass der Gläubiger lediglich eine aus seiner Sicht bestehende Forderung geltend macht. Ein hinreichend sicherer Rückschluss auf die fehlende Zahlungsfähigkeit oder Zahlungswilligkeit des Schuldners ist hier nur möglich, wenn zusätzliche Umstände hinzukommen. Nur

wenn der Schuldner bei einer von ihm unbestrittenen Forderung nachweislich trotz entsprechender Mahnungen des Gläubigers und des Inkassounternehmens nicht reagiert, ist deshalb eine Speicherung durch die Auskunftei gerechtfertigt. Prüfen muss diese Voraussetzungen bereits das Inkassounternehmen, wenn es die Daten der Auskunftei übermittelt. Es darf daher beileibe nicht jede „offene Forderung“ oder jedes „außergerichtliche Mahnverfahren“ von der Auskunftei gespeichert werden.

Bei der erwähnten Auskunftei ist es mehrfach vorgekommen, dass Daten aus Inkassoverfahren in den Datenbestand der Auskunftei übernommen worden sind, obwohl die genannten Voraussetzungen nicht vorlagen. Die Fehlerquelle lag bei den Inkassounternehmen, deren Mitarbeiter trotz interner Anweisungen, wie in diesen Fällen zu verfahren ist, Daten an die Auskunftei übermittelt haben. Die Auskunftei kann sich jedoch nicht mit dem Hinweis auf fehlerhafte Übermittlungen entlasten, da sie als verantwortliche Stelle dafür sorgen muss, dass nur korrekte Daten von ihr verarbeitet werden. Die Auskunftei muss daher - gemeinsam mit den einmeldenden Stellen - alle erforderlichen Maßnahmen ergreifen, um die ordnungsgemäße Datenverarbeitung sicherzustellen. Sie wird daher mit mehr Nachdruck als bisher auf die Schulung der Mitarbeiter des Inkassounternehmens hinwirken müssen. Die Effektivität dieser Maßnahme wird daran abzulesen sein, ob die Zahl der entsprechenden Beschwerden zurückgeht.

4.2 Berechtigtes Interesse an einer Auskunft und dessen Darlegung

Um von einer Auskunftei Daten über eine dort gespeicherte Person übermittelt zu bekommen, muss der Anfragende ein berechtigtes Interesse an der Kenntnis der Daten haben.

In einem Fall hat ein Versandhaus bei einer Auskunftei auf Grund einer Bestellung des Betroffenen, in welcher dieser als Zahlungsart „Barzahlung bei Lieferung“ angegeben hatte, eine Auskunft angefordert. Bei der Überprüfung durch die Aufsichtsbehörde hat sich herausgestellt, dass es sich bei der Bestellung um ein höherwertiges Wirtschaftsgut gehandelt hat, das für den Betroffenen erst hergestellt werden musste.

Das vom Gesetz geforderte „berechtigte Interesse“ liegt vor, wenn zwischen dem Anfragenden und dem Betroffenen Geschäfte mit einem kreditorischen oder wirtschaftlichen Risiko abgeschlossen werden sollen, also beispielsweise ein Kauf auf Rechnung oder gegen Ratenzahlung. Im Zusammenhang mit Bestellungen per

Nachnahme oder - wie im oben genannten Fall - per Barzahlung bei Lieferung wird das berechtigte Interesse an der Kenntnis der bei der Auskunftei gespeicherten Daten von den Aufsichtsbehörden grundsätzlich verneint. Ausnahmsweise ist allerdings ein berechtigtes Interesse in den Fällen anzunehmen, in denen mittel- und hochwertige Güter, insbesondere Sonderanfertigungen, bestellt werden oder in denen hohe Transportkosten anfallen, da dann ein wirtschaftliches Risiko des Unternehmens zu Grunde liegt.

Im Rahmen einer Anfrage muss der Anfragende sein berechtigtes Interesse an der Kenntnis der Daten gegenüber der Auskunftei darlegen. Die Auskunfteien haben dazu für ihre Vertragspartner sogenannte Anfragemerkmale geschaffen, die pauschaliert ausdrücken sollen, welches berechtigte Interesse an der Kenntnis der Daten vorliegt. Solche Anfragemerkmale lauten beispielsweise „Kreditgewährung“ oder „Geschäftsanbahnung“. Es wird jedoch teilweise auch das Anfragemerkmal „Bonitätsprüfung“ verwendet und von einzelnen Auskunfteien zur Darlegung des berechtigten Interesses akzeptiert. So geschehen in dem obengenannten Fall.

Das Anfragemerkmal „Bonitätsprüfung“ drückt aber lediglich den Zweck der Anfrage aus, aber niemals das berechtigte Interesse an der Kenntnis der Daten. Für die Darlegung des berechtigten Interesses müsste der Begriff „Bonitätsprüfung“ stärker differenziert und in Form von Fallgruppen konkretisiert werden. Die Aufsichtsbehörde wird gemeinsam mit den Aufsichtsbehörden der anderen Länder versuchen, über den Verband der Handelsauskunfteien auf eine Verbesserung hinzuwirken.

4.3 Stichprobenregelung

Auskunfteien haben für ihre Vertragspartner in der Regel die Möglichkeit geschaffen, Auskünfte in einem automatisierten Verfahren abzurufen. Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt in einem solchen Fall der Abrufende. Die Auskunftei prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlass besteht. Sie hat aber zu gewährleisten, dass die Zulässigkeit der Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann. Die Handelsauskunfteien haben sich bereits vor Jahren in Gesprächen mit den obersten Aufsichtsbehörden bereit erklärt, jährlich zwei Promille aller Anfragen über Privatpersonen daraufhin zu überprüfen, ob für die Auskunftseinholung tatsächlich ein berechtigtes Interesse vorlag. Für eine solche Stichprobenüberprüfung wird möglichst zeitnah die Vorlage eines Dokumentes gefordert, aus dem die für die Anfrage relevanten wirtschaftlichen Vorgänge erkenn-

bar sind, insbesondere die Angaben, die belegen, dass es sich dabei um ein Geschäft mit einem kreditorischen oder wirtschaftlichen Risiko handelt. In Betracht kommt beispielsweise ein Vertrag oder ein Kreditantrag.

Eine große Auskunftei begnügte sich bei der stichprobenweisen Überprüfung des berechtigten Interesses damit, sich von den Auskunftsempfängern den Anfragegrund auf einem Formblatt nochmals ankreuzen zu lassen. Sinn und Zweck der Stichprobenprüfung wurden damit ersichtlich verfehlt. Die Auskunftei wurde deshalb aufgefordert, sich an die getroffenen Absprachen zu halten und von den Auskunftsempfängern die Vorlage eines zentralen Dokuments zu verlangen.

4.4 Wahrung des Geschäftsgeheimnisses bei Auskunftsersuchen des Betroffenen

Ein heikler Punkt für Auskunfteien ist es, wenn der Betroffene nicht nur wissen will, welche Daten über ihn gespeichert, sondern auch an welche Stellen sie übermittelt worden sind.

In der letzten BDSG-Novelle wurde das Auskunftsrecht des Betroffenen neu geregelt; die Rechte des Betroffenen sollten damit gestärkt werden. Jedoch kann der Betroffene auch nach der Neuregelung von Stellen, die personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung speichern, Auskunft über Herkunft und Empfänger seiner Daten nur verlangen, sofern nicht das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt. Es ist daher grundsätzlich in jedem Einzelfall eine Interessenabwägung vorzunehmen zwischen dem Auskunftsinteresse des Betroffenen und dem Interesse an der Wahrung des Geschäftsgeheimnisses der Auskunftei. Hierzu muss der Betroffene sein Auskunftsinteresse zumindest stichwortartig darlegen.

Die Abwägung muss in jedem Fall zugunsten des Betroffenen ausgehen, wenn er entsprechend der bisherigen Gesetzesfassung begründete Zweifel an der Richtigkeit der Daten geltend machen kann. Regelungen in den Verträgen zwischen den Auskunfteien und ihren Vertragspartnern, wonach deren Geschäftsbeziehungen als Geschäftsgeheimnis behandelt werden sollen, reichen für sich allein nicht aus, ein grundsätzliches Überwiegen der Interessen der Auskunftei an der Wahrung des Geschäftsgeheimnisses zu begründen. In Fällen, in denen die Auskunft an Unternehmen erteilt wurde, bei denen der Kunde davon ausgehen muss oder sogar darauf hingewiesen wird, dass der Vertrag erst nach einer Bonitätsprüfung abgeschlossen wird, sind jedoch grundsätzlich keine schutzwürdigen Geheimhal-

tungsinteressen zu erkennen. Dies trifft beispielsweise für Telekommunikationsunternehmen, Versandhändler, Banken oder Versicherungen zu. Daher ist es in diesen Fällen auch nicht erforderlich, dass der Betroffene sein Auskunftsinteresse besonders begründet. Über die Umsetzung der neuen Regelung werden mit dem Verband der Handelsauskunfteien noch Gespräche geführt.

4.5 Die SCHUFA und die Auskunft „Bestrittene Daten in Prüfung“

Personenbezogene Daten sind nach dem BDSG zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt. Die Handhabung dieser Bestimmung führt in der Praxis zu Fragen, die an die Aufsichtsbehörde herangetragen werden. So hatte die SCHUFA im Falle einer Auskunft an eine Bank die bestrittenen Daten zwar nicht mehr genannt, jedoch darauf hingewiesen, dass „Bestrittene Daten in Prüfung“ vorhanden seien.

Im Ergebnis war dieses Verfahren nicht zu beanstanden. Wie sich zeigte, prüft die SCHUFA sofort nach Bestreiten der Daten, ob die erhobenen Einwendungen begründet sind. Während dieser Prüfungsfrist, die in der Regel höchstens zwei Wochen beträgt, wird Anfragenden die Auskunft „Bestrittene Daten in Prüfung“ erteilt. Je nach Ergebnis der Prüfung werden die Daten entweder weiter gespeichert, berichtigt oder gelöscht und der Betroffene hiervon unterrichtet.

Die Erteilung der Auskunft „Bestrittene Daten in Prüfung“ während einer angemessenen, maximal zweiwöchigen Prüfungszeit ist mit dem Bundesdatenschutzgesetz noch vereinbar. Der Betroffene wird durch diese Praxis während einer relativ kurzen Prüfungszeit auch nicht unverhältnismäßig beeinträchtigt. Lässt sich jedoch der umstrittene Sachverhalt innerhalb der Zweiwochenfrist nicht aufklären, sind die entsprechenden Daten entweder zu löschen oder aber zu sperren, wobei im letzteren Fall spätere Auskünfte keinen Hinweis auf die Tatsache der Sperrung enthalten dürfen.

Obwohl das von der SCHUFA praktizierte Verfahren im Ergebnis nicht zu beanstanden war, wurde von der Aufsichtsbehörde darauf hingewiesen, dass in jedem Einzelfall eine Abwägung der Interessen vorzunehmen ist und gegebenenfalls auf den Hinweis „Bestrittene Daten in Prüfung“ völlig zu verzichten ist, wenn schutzwürdige Interessen des Betroffenen entgegenstehen.

4.6 SCHUFA- Scoringverfahren

Gegenstand von Beschwerden ist immer wieder das Scoringverfahren der SCHUFA. Mit diesem Verfahren wird anhand statistisch-mathematischer Methoden eine Prognose über das zukünftige Zahlungsverhalten von Personengruppen ermittelt und in einer Punktzahl (Score) ausgedrückt.

Im Berichtszeitraum konnten die Aufsichtsbehörden hier einige Verbesserungen für die Betroffenen erreichen. So erklärte sich die SCHUFA - nach entsprechender Kritik der Aufsichtsbehörden - bereit, die Anzahl der von den Betroffenen eingeholten Selbstauskünfte nicht mehr in die Berechnung des Scorewertes einfließen zu lassen. Die technische Umsetzung erfolgte Mitte 2002.

Kontrovers diskutiert wurde die Frage der Auskunftserteilung über den Scorewert an den Betroffenen. Nach Auffassung der SCHUFA lässt die gegenwärtig genutzte Software die Speicherung des übermittelten Scorewertes nicht zu, weshalb auch eine Auskunftserteilung nicht möglich sei. Eine Änderung der genutzten Software mit dem Ziel, den Scorewert zu speichern, sei mit wirtschaftlich vertretbarem Aufwand nicht möglich. Die Aufsichtsbehörden sind allerdings der Meinung, dass die Speicherung und Auskunftserteilung des übermittelten Scorewertes für deutlich mehr Transparenz des Verfahrens gegenüber den Betroffenen sorgen würde und warben für eine Änderung des Verfahrens. Man konnte sich darauf einigen, dass die Vertragspartner der SCHUFA - also insbesondere Banken - angehalten werden, den Betroffenen - soweit möglich - den ihnen übermittelten Scorewert auf Anfrage mitzuteilen. Überdies erklärte die SCHUFA, dass die nächste Softwaregeneration (Pilotphase voraussichtlich 2004) die Speicherung des Scorewertes und somit eine entsprechende Auskunftserteilung an den Betroffenen ermöglichen wird.

Die SCHUFA erklärte sich ebenfalls bereit, den Betroffenen - gegen entsprechenden Kostenersatz - eine tagesaktuelle Scorewertberechnung anzubieten. Dieser Scorewert - der sich allerdings von bereits zu früheren Zeitpunkten durch Dritte eingeholten Scorewerten unterscheiden kann - kann auch ohne eine umfassende Selbstauskunft erfragt werden.

Die Aufsichtsbehörden erreichten auch, dass die SCHUFA dem Betroffenen nunmehr ermöglicht, der Ermittlung des Scorewertes zu widersprechen. Dieser Widerspruch muss nicht begründet werden. Bei eingelegtem Widerspruch informiert die SCHUFA den Betroffenen noch einmal über das Scoreverfahren und die Folgen einer Nichtermittlung des Scorewertes. Erst wenn der Betroffene auf diese Information hin seinen Widerspruch aufrechterhält, wird tatsächlich kein Scorewert er-

mittelt. Intern wird bei der SCHUFA das Merkmal „Betroffener widerspricht Scorewertermittlung“ gespeichert, während in Auskünften an Vertragspartner der SCHUFA der Text „Über die angefragte Person erfolgt keine Scorewertermittlung“ übermittelt wird. Dieses ist notwendig, um die anfragenden Vertragspartner darüber zu informieren, weshalb zu einem Betroffenen, zu dem keine Negativdaten vorliegen, kein Scorewert ermittelt wird. Die Aufsichtsbehörden haben diesen Filtertext als nicht diskriminierend beurteilt und das Verfahren gebilligt.

Die SCHUFA hat die wesentlichen Informationen zum Thema Scorewert in einer neugefassten Verbraucherinformation „SCHUFA Score-Verfahren ASS“ zusammengestellt.

4.7 Neustrukturierung der SCHUFA

Seit dem 1. Januar 2002 besteht die SCHUFA nur noch aus einer Aktiengesellschaft mit Sitz in Wiesbaden.

Zuständige Datenschutz-Aufsichtsbehörde ist damit grundsätzlich allein das Regierungspräsidium Darmstadt. Im Interesse der Bürgernähe und der rationelleren Verwaltung haben sich das Regierungspräsidium Darmstadt und die übrigen Aufsichtsbehörden jedoch darauf geeinigt, dass einfache Anfragen von Bürgern und Standardfälle nach wie vor von den für die örtliche SCHUFA-Niederlassung zuständigen Aufsichtsbehörden bearbeitet werden, da sich einfach gelagerte Fälle in der Regel rascher vor Ort klären lassen. Treten im Einzelfall Meinungsunterschiede mit der SCHUFA auf oder geht es um grundsätzliche Fragen, wird der Fall an das Regierungspräsidium Darmstadt abgegeben, das die Sache dann mit der Zentrale der SCHUFA in Wiesbaden weiter verhandelt und die abschließende Entscheidung trifft.

Diese Verfahrensweise hat sich nach Auffassung der Aufsichtsbehörden bewährt.

Berührungspunkte mit der SCHUFA bestehen jedoch für die Aufsichtsbehörde auch weiterhin. Die Arbeitsweise dieser Kreditschutzorganisation beruht auf dem Prinzip gegenseitiger Informationen. Der Verpflichtung der Organisation, Auskünfte zu erteilen, steht die Verpflichtung der Vertragspartner, namentlich der angeschlossenen Banken, gegenüber, Informationen für den Datenbestand zur Verfügung zu stellen. Da die Vertragspartner nur einmelden dürfen, was die SCHUFA speichern darf, wird die Aufsichtsbehörde auch künftig mit Fragen der SCHUFA-Datenverarbeitung befasst sein.

5 Adresshandel und Werbung

Zahlreiche Beschwerden richten sich alljährlich gegen die Zusendung persönlich adressierter Werbung. Dabei geht es den Betroffenen in erster Linie darum, von der werbetreibenden Stelle keine Werbung mehr zu erhalten und zu erfahren, woher diese Stelle ihre Anschrift erhalten hat. Die fehlende Transparenz der Arbeitsweise in der Direktwerbebranche macht es vielen Betroffenen schwer, sich selbst durchzufinden, um ihre Rechte gegenüber den letztendlich verantwortlichen Stellen geltend machen zu können.

Auffällig war im Berichtszeitraum die Häufung von Fällen, in denen sich Betroffene an die Aufsichtsbehörde wandten, nachdem sie eine als „Gewinnmitteilung“ aufgemachte Werbung erhalten hatten, in denen sie für eine Gewinnanforderung zur telefonischen Kontaktaufnahme unter einer kostenpflichtigen 0190-er Nummer aufgefordert wurden. Mit den Mitteln des Datenschutzes ist diesen Praktiken nicht beizukommen. Die Verwendung von personenbezogenen Daten für Werbezwecke ist grundsätzlich zulässig, es sei denn, der Betroffene hat Widerspruch gegen die Verwendung seiner Daten für Werbezwecke eingelegt, was in den vorgelegten Fällen nicht zutraf. Nach den Feststellungen der Aufsichtsbehörde haben diese Firmen jeweils aus dem benachbarten Ausland agiert. Bei den angegebenen Absenderadressen im Inland handelte es sich lediglich um Postfachadressen. Einige dieser Fälle wurden an die Aufsichtsbehörden im benachbarten Ausland abgegeben, einzelne Fälle wegen Betrugsverdacht auch über die Polizei an die Staatsanwaltschaft.

5.1 Änderungen für die Werbebranche durch das novellierte Bundesdatenschutzgesetz

Ein Werbetreibender bedient sich oftmals mehrerer Stellen, um an die Adressen seiner Zielgruppen zu gelangen. In der Regel werden die Adressen dem Werbetreibenden nicht unmittelbar vom Adresseigner zur Verfügung gestellt, sondern über mehrere sogenannte Listbroker vermittelt, so dass der Werbetreibende bisher dem Betroffenen oft zum Schluss nicht mehr sagen konnte, wer letztendlich Adresseigner der für seine Werbezwecke genutzten Adresse ist. Neu in das BDSG aufgenommen wurde deswegen die Regelung, wonach die Stelle, die solche personenbezogenen Daten für Zwecke der Werbung und der Markt- und Meinungsforschung nutzt, die bei einer ihr nicht bekannten Stelle gespeichert sind, sicherzu-

stellen hat, dass der Betroffene Kenntnis über die Herkunft seiner Daten erhalten kann.

Die Praxis sieht aber häufig anders aus. Typisch ist folgender, an die Aufsichtsbehörde herangetragene Fall: Der Betroffene, der ein Werbeschreiben erhalten und sich beim Werbetreibenden nach der Herkunft seiner Anschrift erkundigt hatte, wurde vom werbenden Unternehmen an ein Listbroking-Unternehmen verwiesen, das dem Betroffenen gegenüber als Adressherkunft wiederum ein weiteres Listbroking-Unternehmen benannte. Dieses weitere Listbroking-Unternehmen hat sich allerdings auf den Standpunkt gestellt, nicht auskunftspflichtig zu sein, da dort keine Daten zum Betroffenen gespeichert, sondern nur vermittelt worden waren. Der Auskunftsanspruch des Betroffenen ist damit ins Leere gelaufen. Nach der Neuregelung hätte bereits der Werbetreibende gegenüber dem Betroffenen den Adresseigner benennen oder aber sicherstellen müssen, dass zumindest das von ihm benannte Listbroking-Unternehmen dieser Auskunftsverpflichtung nachkommt.

Weitere Neuregelungen wurden in Bezug auf das Widerspruchsrecht der Betroffenen getroffen. Zwar hatte ein Betroffener schon bisher das Recht, bei der verantwortlichen Stelle Widerspruch gegen die Nutzung und Übermittlung seiner Daten für Zwecke der Werbung und der Markt- und Meinungsforschung einzulegen. Nunmehr aber muss der Betroffene von der verantwortlichen Stelle bei der Ansprache zum Zweck der Werbung oder der Markt- oder Meinungsforschung auf dieses Widerspruchsrecht ausdrücklich hingewiesen werden.

Auch ist es in der Vergangenheit immer wieder vorgekommen, dass auf der Werbesendung nicht erkennbar war, wer die werbetreibende Stelle ist. Der Gesetzgeber hat deshalb vorgesehen, dass die für die Werbesendung verantwortliche Stelle auf der Werbesendung konkret - also mit der vollständigen Anschrift - genannt wird.
Ein Verstoß gegen diese Hinweispflichten stellt eine Ordnungswidrigkeit nach § 43 BDSG dar.

Diese neuen Vorschriften werden bei den Unternehmen nur sehr zögerlich umgesetzt. Es bleibt zu hoffen, dass ein vom Deutschen Direktmarketingverband e.V. herausgegebener Leitfaden zur Umsetzung der neuen Vorschriften (vgl. Ziff. 5.2) daran etwas ändern wird.

5.2 Verhaltensregeln der Werbewirtschaft

Den Aufsichtsbehörden wurde im Herbst 2001 vom Deutschen Direktmarketingverband e.V. (DDV) mit Sitz in Wiesbaden ein Leitfaden „BDSG 2001 - Auswirkungen auf das Direktmarketing“ zur Kenntnisnahme und der Bitte um Äußerung übersandt. In diesem Leitfaden werden den Unternehmen, die dem Verband angeschlossen sind, Hinweise zur Umsetzung der neuen Vorschriften des Bundesdatenschutzgesetzes gegeben. Auch wenn der neue Ansatz positiv zu bewerten ist, entsprechen die im Leitfaden gegebenen Hinweise nach Auffassung der Aufsichtsbehörden in mehreren Punkten noch nicht den datenschutzrechtlichen Neuregelungen. Das Gespräch mit dem Verband soll deshalb fortgesetzt werden.

5.3 Nichtbeachtung des Werbewiderspruchs

In einem Fall war auf den Bestellkarten eines Versandhandelsunternehmens für die Kunden die Möglichkeit gegeben, durch Ankreuzen auszuwählen, ob sie mit der Weitergabe ihrer Daten für Werbezwecke einverstanden waren oder nicht. Die eingegangene Beschwerde berichtete von mehreren Kunden, die ihr Kreuz bei „nein, nicht einverstanden“ gemacht, aber danach trotzdem Werbung erhalten hätten.

Bei der Nichtbeachtung des Werbewiderspruchs handelt es sich um einen Verstoß gegen § 28 Abs. 4 BDSG, der nach § 43 Abs. 2 Nr. 1 BDSG eine Ordnungswidrigkeit darstellt. Das Versandhandelsunternehmen führte die Nichtbeachtung des Werbewiderspruches auf einen Fehler im EDV-System zurück. Es hat auf unser Betreiben hin das Verfahren zur Erfassung und Befolgung der Widersprüche geändert. Seither sind keine Beschwerden mehr eingegangen. Von der Einleitung eines Ordnungswidrigkeitenverfahrens wurde abgesehen.

In einem anderen Fall wurde ebenfalls von einem Betroffenen vorgebracht, dass er trotz eingelegtem Widerspruch erneut Werbung von einem Unternehmen erhalten habe. Die Überprüfung ergab, dass bei dem werbenden Unternehmen zwar eine Werbesperrdatei geführt wird, bei einer neuen Werbeaktion ein Abgleich mit dieser Datei aber immer manuell veranlasst, im vorgelegten Fall aber unterlassen wurde. Die Beanstandung der Aufsichtsbehörde hat dazu geführt, dass bei dem Unternehmen der Abgleich nunmehr automatisiert erfolgt.

5.4 Unverlangte elektronische Werbung

Immer häufiger ist zu beobachten, dass sich Unternehmen neuer Medien und neuer Formen der Kundenansprache bedienen. Das unverlangte Herantreten an die Kunden per Telefon, Telefax, SMS und E-Mail führte in einer beachtlichen Anzahl von Fällen zu Anfragen und Beschwerden bei der Aufsichtsbehörde.

Aus der Sicht des Datenschutzes stellt bereits die Rufnummer einer Person ein personenbezogenes Datum im Sinne des BDSG dar. Ruft jemand bei einer Person an, so handelt es sich nach der Systematik des BDSG um eine Nutzung des personenbezogenen Datums „Rufnummer“. Für die Zulässigkeit dieser Nutzung kommt es nach § 28 Abs. 1 Satz 1 Nr. 2 und 3 BDSG darauf an, ob der Betroffene ein überwiegendes berechtigtes Interesse am Ausschluss der Nutzung hat. Im Zusammenhang mit der Telefonwerbung hat der Bundesgerichtshof entschieden, gestützt auf das Wettbewerbsrecht, dass eine Telefonwerbung gegenüber Privatkunden eine nicht hinzunehmende Beeinträchtigung der Privatsphäre darstellt, die nur dann zulässig ist, wenn der Angerufene zuvor ausdrücklich oder stillschweigend sein Einverständnis gegeben hat, zu Werbezwecken angerufen zu werden. Wird eine Person ungebeten angerufen, bedeutet dies ein Eindringen in ihre Privatsphäre und eine belästigende oder zumindest unerwünschte Störung, insbesondere dann, wenn die Anrufe durch dafür extra geschultes Personal von Fremdfirmen durchgeführt werden. Andere Gerichte haben bei unverlangten Telefax-, SMS- und E-Mail-Sendungen entsprechend entschieden. Diese Grundsätze sind auf das Datenschutzrecht übertragbar.

Die Praxis sieht jedoch anders aus, da die Versender dieser Art von Werbung regelmäßig im Ausland sitzen, meist außerhalb der EU und damit auch außerhalb des Einwirkungsbereichs der Aufsichtsbehörde. Jedoch sind auch Ermittlungen im Inland nicht immer erfolgversprechend, da die Aufsichtsbehörde nach den Telekommunikations- und Teledienstevorschriften - anders als die Strafverfolgungsbehörden - keinen Anspruch auf Auskunft über den Inhaber einer Rufnummer oder E-Mail-Adresse hat.

Überhand nimmt derzeit das Versenden unverlangter Massen-Werbe-E-Mails. Allerdings ist es insbesondere bei Massenwerbemails (sogenannte Spam-Mails) für elektronisch abrufbare Angebote kaum möglich, den Versender der Werbe-E-Mail zu ermitteln, da durch die weltweite Verbindungsmöglichkeit des Internets der Versender der Werb-E-mail beispielsweise in der Karibik und der Anbieter der Dienstleistung in Osteuropa registriert sein kann. Wenn sich manchmal Ansatzpunkte dafür finden, dass doch ein Verantwortlicher im Inland zu ermitteln sein könnte, stellt sich dies regelmäßig als unzutreffend heraus.

So ist die Aufsichtsbehörde einem Fall von Massen-Werbe-E-Mail nachgegangen, bei der als Absender eine Partnervermittlung aus Stuttgart angegeben war. Die Nachforschungen zeigten aber schon bald, dass weder der Name noch die Anschrift des Absenders stimmten. Auch führte die Suche mit der E-Mail-Absenderadresse zu keinem Erfolg. Bei den verschiedenen der Aufsichtsbehörde bekannten Absenderadressen handelte es sich durchweg um Fälschungen. Hierbei ist anzumerken, dass eine E-Mail-Absenderadresse auf Grund der Funktionsweise der Internet-E-Mail manipulierbar ist. Die Suche nach dem Anbieter des Angebots führte schließlich zu einer Gesellschaft in Bulgarien. Somit musste die Untersuchung nach der Herkunft der Werbe-E-Mail und der zu Grunde liegenden Adressen erfolglos eingestellt werden.

Als geradezu tückisch erweist sich in diesem Zusammenhang der scheinbar datenschutzfreundliche Hinweis in manchen dieser E-Mails auf die Möglichkeit des Werbewiderspruchs. Die genutzten E-Mail-Adressen sind meist mittels spezieller Suchprogramme aus dem Internet gesammelt oder elektronisch, d.h. durch Zeichenkombinationen, generiert worden und führen nur zufällig zu einer tatsächlich vorhandenen Person. Mit dem Werbewiderspruch wird dann aber die Existenz der Adresse bestätigt. Damit wird die Adresse für den Absender wertvoller. Der Betroffene muss in diesem Fall damit rechnen, dass seine Daten künftig für weitere Werbung genutzt werden.

6 Markt- und Meinungsforschung

6.1 Haushaltsbefragungen nach dem neuen BDSG

Werbemaßnahmen haben nur dann Erfolg, wenn die potenziellen Verbraucher möglichst zielgenau beworben werden können. Das führt dazu, dass in der Werbebranche die Nachfrage nach sogenannten qualifizierten Adressen ständig zunimmt. Die Beschaffung dieser qualifizierten Adressen geschieht über Konsumentenbefragungen mit zum Teil mehrseitigen Fragebögen, entweder für eigene Werbezwecke, aber vielfach zum Zweck der Übermittlung an andere Werbetreibende oder Listbroker, die die Adressen für eine Werbung nach Vorgaben der Unternehmen zusammenstellen. Firmen, die sich darauf spezialisiert haben, Haushaltsbefragungen mit mehrseitigen Fragebögen durchzuführen, die alle möglichen Lebensumstände erfassen, müssen wegen der Vielzahl der Fragen und der dadurch möglichen personenbezogenen Auswertungen die neuen Vorschriften des BDSG ganz besonders beachten und umsetzen. Dies gilt insbesondere dann, wenn die unterschiedlichsten Daten aus vielen Lebensbereichen (z.B. aus den Lebensberei-

chen Medien, Computer, Haus und Heim, Hobbys, Auto, Urlaub, Finanzen) erfragt werden.

Im Zuständigkeitsbereich der Aufsichtsbehörde befindet sich ein Unternehmen, das derartige Umfragen durchführt. Mit Vertretern dieses Unternehmens wurde der Anpassungsprozess in mehreren Gesprächen durchgeführt. Dabei wurde insbesondere erreicht, dass die verantwortliche Stelle den Betroffenen schon bei der Befragung über ihre Identität, über den Zweck der Erhebung und der nachfolgenden Verarbeitung sowie über die Kategorien von Empfängern informiert. Weiter wurde auf den Hinweis Wert gelegt, dass die Ausfüllung des Fragebogens freiwillig ist. Werden besondere Arten personenbezogener Daten (z.B. über den Gesundheitsbereich) erhoben, verarbeitet und genutzt, so muss der Betroffene ausdrücklich darin einwilligen. Damit soll dem höheren Schutzbedürfnis von Personen in besonderen Lebenszusammenhängen Rechnung getragen werden. Ausserdem sind schon bei der Erhebung der Daten die Zwecke, für welche die Daten verarbeitet oder genutzt werden, konkret festzulegen.

Das betroffene Unternehmen hat die Fragebögen entsprechend geändert.

6.2 Customer Relationship Management (CRM) - Kundenbindungsprogramme

In letzter Zeit haben sich neue Geschäftspraktiken zum Sammeln von qualifizierten Daten über Kunden zu Werbezwecken, das sogenannte Customer Relationship Management (CRM), am Markt etabliert. Dabei kommt eine Kundenkarte zum Einsatz. Der Kunde bekommt beim Kauf von Waren oder der Nutzung von Dienstleistungen Rabattpunkte gutgeschrieben. Damit der Kunde möglichst viele Rabattpunkte sammeln und individuell eintauschen kann, haben sich Firmen zu sogenannten Partnerunternehmen zusammengeschlossen. Gibt der Kunde seine Kundenkarte zur Gutschrift ab, werden u.a. die Kundennummer, das Datum des Einkaufs, die Kennung des Unternehmens, die Warengruppe und der Betrag erhoben und an das Kundenbindungsprogramm weitergegeben. Kundenbindungsprogramme werden von hierauf spezialisierten Unternehmen angeboten. Diese führen die Rabattkonten der Kunden. Auf der Basis dieser Daten werden die Kunden nach ihren individuellen Bedürfnissen und Wünschen beworben. Die Ziele, die damit verfolgt werden, sind, die Kundenzufriedenheit zu erhöhen und die Kunden enger an das Unternehmen zu binden. Eine Übermittlung der Daten an Dritte, die nicht Partnerunternehmen sind, findet nicht statt.

Die Unternehmen, die bisher solche Kundenbindungsprogramme anbieten, befinden sich außerhalb unserer Zuständigkeit. Da sie aber bundesweit agieren, wurden diese Fälle im Düsseldorfer Kreis, dem Zusammenschluss der obersten Datenschutzaufsichtsbehörden, besprochen. Hierbei wurden insbesondere die Fassungen der Datenschutzhinweise und der Einwilligungserklärungen abgestimmt. Bei der Einwilligungserklärung wurde Wert darauf gelegt, dass der Kunde auf die erweiterte Nutzung seiner Daten für Werbung und Marketingzwecke aufmerksam gemacht wird und der Kunde diese Nutzung untersagen kann.

6.3 Datenerhebung bei Minderjährigen - Schülerbefragungen

Die Aufsichtsbehörde wurde von einem Vater informiert, dass ein Markt- und Meinungsforschungsinstitut auf dem Schulhof seinen vierzehnjährigen Sohn und andere Schüler aufgefordert habe, an einer Studie teilzunehmen, und dass die Kinder etwas hätten unterschreiben müssen. Die Überprüfung der Aufsichtsbehörde ergab, dass ein Markt- und Meinungsforschungsinstitut von einem Jugend-Verlag beauftragt worden war, eine Studie bei Jugendlichen zwischen 14 und 18 Jahren durchzuführen. Zu diesem Zweck hatte sich das Markt- und Meinungsforschungsinstitut von den Jugendlichen die schriftliche Einwilligung in die Verarbeitung ihrer Daten geben lassen. Zugleich wurden sie darauf hingewiesen, dass die Einwilligung jederzeit widerrufen werden kann.

Damit eine erforderliche Einwilligung wirksam ist, muss diese freiwillig sein. Dem Betroffenen muss der Umfang der Verarbeitung der Daten hinreichend dargelegt werden, so dass die Verwendung der Daten für ihn durchschaubar ist. Dies war vorliegend erfüllt. Eine wirksame Einwilligung setzt aber auch voraus, dass hinsichtlich der Person des Betroffenen eine ausreichende Einsichtsfähigkeit in die Tragweite seiner Entscheidung vorhanden ist. Da sich die Einwilligung auf tatsächliche Handlungen - nämlich den Eingriff in das Persönlichkeitsrecht - bezieht und keinen rechtsgeschäftlichen Charakter hat, ist für eine wirksame Einwilligung nicht die Geschäftsfähigkeit des Betroffenen erforderlich. Wirksame Einwilligungen können daher auch von Jugendlichen gegeben werden, soweit davon ausgegangen werden kann, dass sie die mit der Herausgabe ihrer persönlichen Daten verbundenen Folgen im konkreten Fall überschauen können. Auch davon hat das Markt- und Meinungsforschungsinstitut ausgehen dürfen, denn die befragten Jugendlichen waren alle über 14 Jahre alt und zudem Gymnasiasten. Ein Verstoß gegen datenschutzrechtliche Bestimmungen lag daher nicht vor.

7 Kreditwirtschaft

7.1 Prüfung von Telefon-Servicecentern bei Banken

Im Tätigkeitsbericht des Jahres 2001 wurde über die schwerpunktmäßige Sonderüberprüfung von Telefon-Servicecentern, die im Auftrag von Banken tätig sind, berichtet. Im Zuge dieser schwerpunktmäßigen Sonderüberprüfungen fehlte noch die Überprüfung von bankeigenen Telefon-Servicecentern. Eine zur Vorbereitung der Sonderüberprüfung durchgeführte Umfrage ergab, dass lediglich fünf Banken mit Sitz in Baden-Württemberg ein eigenes Telefon-Servicecenter unterhalten. Zwei Banken mit verschiedenen Ansätzen für das Telefon-Servicecenter wurden für die Prüfung ausgesucht. Gegenstand der Prüfung war insbesondere, inwieweit bei der persönlichen Identifikation des Kunden gegenüber der Bank die datenschutzrechtlichen Bestimmungen eingehalten werden.

Bei der einen Bank wurden unter dem Begriff „Telefon-Servicecenter“ sowohl die Möglichkeit der Kunden, ihre Bankgeschäfte telefonisch abzuwickeln (Telefon-Banking), als auch die telefonische Kundenansprache (Telefon-Marketing) verstanden. Das Telefon-Banking wird dort ausschließlich nur für eigene Kunden angeboten. Dabei können die Kunden
Überweisungen tätigen und Kontostände sowie Umsätze abfragen. Darüber hinaus waren u.a. die telefonische Erteilung von Wertpapieraufträgen, das Abwickeln von Daueraufträgen, das Anfordern von Schecks und die Bestellung von EC- oder Kreditkarten möglich.

Für die Teilnahme am Telefon-Service muss der Kunde ein Antragsformular unterschreiben und an die Bank zurücksenden. Danach erhält der Kunde die Sonderbedingungen zur Teilnahme am Telefon-Service und die erforderliche PIN (Persönliche Identifikationsnummer) zugesandt. Erst nachdem er den Empfang gegenüber der Bank schriftlich bestätigt hat, wird der Zugang zum Telefon-Banking freigeschaltet. Nimmt ein Kunde die Dienste des Telefonservice-Center in Anspruch, erfolgt die Identifizierung mittels der Kontonummer und der PIN. Bei der Identifizierung kann der Kunde zwischen der Eingabe durch Sprache und durch Tonwahl (über das Tastaturfeld) wählen. Die Überprüfung auf Richtigkeit erfolgt mittels einer Quersumme, die sich aus der Kontonummer und der PIN ergibt, so dass die PIN seitens der Bank nicht aufgezeichnet werden muss. Nach der erfolgten Freischaltung hat der Kunde die Auswahl, welche Bankgeschäfte er abwickeln möchte. Dabei werden Dienste wie z.B. Überweisungsaufträge, Abfragen von Kontoständen und Änderung und Sperrung der PIN per Sprachcomputer erledigt. Wertpapieraufträge, die Einrichtung von Daueraufträgen und sonstige Beratungen im Bankbereich werden hingegen von Mitarbeitern/-innen der Bank erledigt. Alle Eingaben,

sowohl des Sprachcomputers als auch bei der persönlichen Betreuung durch die Mitarbeiter-/innen, werden aufgezeichnet.

Diese Aufzeichnung ist datenschutzrechtlich nicht zu beanstanden, da sie zum Nachweis der Bank gegenüber ihren Kunden dient, dass der erteilte Auftrag auch richtig ausgeführt wurde. Die Aufbewahrungsfrist der aufgezeichneten Gespräche von sechs Monaten wurde aber als zu lang bemängelt. Die Bank hat daraufhin die Speicherfrist auf 120 Tage verkürzt. Zudem wurden nach unserer Empfehlung die Antragsformulare um eine Einverständnisklausel zur Durchführung der telefonischen Kundenansprache ergänzt.

Bei der anderen überprüften Bank wird der Telefon-Service ebenfalls nur für eigene Kunden angeboten. Hierbei wird, im Unterschied zur vorhergehenden Bank, auf den Einsatz eines Sprachcomputers verzichtet und der Telefon-Service ausschließlich über die Mitarbeiter/-innen der Bank abgewickelt. Die Identifizierung des Kunden geschieht nicht durch die Kontonummer und die PIN, sondern durch Fragen zu Details, die nur der Kunde, aber kein Dritter, kennen kann (z.B. Fragen nach personen- oder kontenspezifischen Daten). Kann der Anrufer die gestellten Fragen nur unvollständig beantworten, so wird die Auskunft schriftlich an die gespeicherte Kundenadresse gesendet. Bei Rückrufen durch das Telefon-Servicecenter wird die Identifizierung des Kunden analog durchgeführt. Die Anleitungen zur Identifizierung des Kunden sind im Organisations-Handbuch hinterlegt. Zusätzlich wurde eine Kurzanleitung (Checkliste) angefertigt.

7.2 Offenlegung der PIN (Persönliche Identifikationsnummer)

Im Zug der Zeit werben viele Banken dafür, dass die Kunden ihre Bankgeschäfte von zu Hause aus erledigen, sogenanntes Homebanking. Nicht immer ist die Handhabung für die Kunden einfach, müssen sie doch neben der PIN auch noch für jede Transaktion die zugehörige Transaktionsnummer (TAN) zur eindeutigen Identifizierung eingeben. In dem hier geschilderten Fall hatte der Kunde ein Problem damit, über das Internet auf sein Online-Konto zuzugreifen. Da der Online-Zugang nach mehrfachen Versuchen immer noch nicht funktionierte, nahm der Betroffene mit seiner Bank Kontakt auf. Dabei wurde von den Mitarbeitern der Bank dargelegt, dass das Problem nur durch Offenlegung seiner PIN gelöst werden könnte. Er wurde deshalb aufgefordert, die PIN anzugeben.

Da er der Sache misstraute, wandte er sich an die Aufsichtsbehörde. Nach einer Klärung mit der betroffenen Bank war klar, dass der Anruf intern an die Stelle hätte weitergeleitet werden müssen, die über Berechtigungen zur Unterstützung des

Kunden verfügt. Hier bedarf es nicht der Offenlegung der PIN oder TAN. Auch gab es interne Regelungen, wonach das Personal auf keinen Fall nach der PIN fragen darf. Dies wurde zum Anlass genommen, die entsprechenden Mitarbeiter nochmals darauf aufmerksam zu machen. Der Kunde misstraute zu Recht den „Anweisungen“ des Bankmitarbeiters.

Nach § 9 Satz 1 BDSG und der Anlage hierzu ist die PIN unter die Zugriffs- und Eingabekontrolle einzuordnen. Mit der Zugriffskontrolle soll sichergestellt werden, dass nur in dem Umfang auf personenbezogene Daten zugegriffen wird wie eine Zugriffsberechtigung besteht. Durch die Eingabekontrolle soll gewährleistet werden, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Geldbewegungen verursacht wurden. Um diese Schutzmechanismen nicht zu unterlaufen, darf die PIN und bei Homebanking auch die TAN in keinem Fall anderen offengelegt werden, auch nicht den Bankmitarbeitern.

7.3 Nutzung des Kontoauszugsdruckers ohne PIN

Bei einigen Banken musste in der Vergangenheit bei der Nutzung des Kontoauszugdruckers die Bankkarte eingeführt und zusätzlich die PIN des Kontoinhabers eingegeben werden. Zum Jahreswechsel 2001/2002 wurden diese Kontoauszugdrucker auf den Betrieb ohne PIN-Eingabe umgestellt. Dies führte zu mehreren Anfragen besorgter Bürger bei der Aufsichtsbehörde, die darin einen verringerten Schutz ihrer Kontodaten sahen.

Wie die Überprüfung ergab, musste im Zuge der Umstellung des Zahlungsverkehrs auf den Euro auch die Software vieler Kontoauszugsdrucker geändert werden. Da vorgesehen ist, in den nächsten Jahren die PIN zu erweitern, hätte die Software dann wieder erneut geändert werden müssen. Um sich diese zusätzliche Änderung zu sparen, wurde mit der Anpassung der Software auf den Euro auf ein Beibehalten der PIN-Abfrage verzichtet. Hierbei ist jedoch anzumerken, dass die Mehrzahl der Banken seit je her am Kontoauszugdrucker auf die PIN-Abfrage verzichtet haben.

Ein Kontoauszug enthält personenbezogene Daten. Datenschutzrechtlich gesehen handelt es sich beim Druck eines Kontoauszugs um eine durch den Kontoinhaber veranlasste Nutzung seiner personenbezogenen Daten. Beim bisherigen Verfahren mit EC- beziehungsweise Bankkarte und PIN war weitgehend sichergestellt, dass Karteninhaber und Kontoinhaber übereinstimmten. Eine Datenübermittlung an Dritte konnte somit nicht erfolgen. Bei dem vereinfachten Verfahren ohne PIN werden

im Falle des Kartenverlusts die personenbezogenen Daten des Kontoinhabers auch an einen unberechtigten Dritten
übermittelt, wenn dieser in den Besitz der Bankkarte gelangt ist. Dies war der Grund für die Bedenken der Anfrager.

Das vereinfachte Verfahren bewirkt in der Summe betrachtet zwar einen geringeren Schutz der personenbezogenen Daten des Kunden. Es kann aber datenschutzrechtlich nicht beanstandet werden, da die Quelle der Unsicherheit, nämlich der Verlust der Karte, im Verantwortungsbereich des Kunden liegt.

7.4 Weitergabe der Adresse des Kontoeigentümers

Einer Inhaberin eines Girokontos wurde die EC-Karte gestohlen. Den Diebstahl meldete sie sofort ihrer Bank und ließ die Karte sperren. Die Kartensperrung wurde von der Bank schriftlich bestätigt. Um sicher zu gehen, ließ die Kontoinhaberin zusätzlich noch das Girokonto löschen. Einige Wochen später erhielt sie von mehreren unbekannten Firmen Zahlungsaufforderungen wegen nicht einlösbarer Lastschriften. Ihre Anfrage bei den Firmen, wie sie zu ihrer Adresse gekommen waren, ergab, dass diese die Adresse von der Bank der Kontoinhaberin erhalten hatten.

Die Übermittlung der Adresse des Kontoinhabers an Dritte ist datenschutzrechtlich nur mit seiner schriftlichen Einwilligung zulässig. Bei dem im Handel gebräuchlichen Lastschriftverfahren willigt deshalb der Kunde auf dem Lastschriftbeleg mit seiner Unterschrift darin ein, dass seine Bank im Falle des Nichteinlösens der Lastschrift seine Adresse an den Gläubiger weitergeben darf.

Da die Unterschrift auf dem Beleg vom Kartendieb gefälscht worden war, lag im vorliegenden Fall eine wirksame Einwilligung nicht vor. Nachdem der Bank der Diebstahl der EC-Karte zum Zeitpunkt der Anfrage bereits bekannt war, konnte sie nicht davon ausgehen, dass die Kontoinhaberin den Lastschriftbeleg und damit die Einwilligung unterschrieben hatte. Die Bank hätte zumindest Zweifel anmelden und den Beleg zur Kontrolle der Unterschrift anfordern oder gegebenenfalls bei der Kontoinhaberin nachfragen müssen.

Die Nachprüfung ergab, dass im Grunddatenbestand des Girokontos nach Eingang einer Verlustmitteilung ein Sperrvermerk angebracht wird, um eine Auskunftserteilung zu verhindern. Wie sich herausstellte, führte die Auflösung des Girokontos dazu, dass damit zugleich der Sperrvermerk gelöscht wurde. Bei den nachfolgenden Auskunftsersuchen konnte die Bank dann nicht mehr erkennen,

dass die Karte gestohlen war. Dieser organisatorischer Fehler bei der Kontoverwaltung der Bank war zu beanstanden. Die Bank hätte dafür Sorge tragen müssen, dass der Sperrvermerk auch nach der Kontoauflösung erkennbar bleibt, da es nicht ungewöhnlich ist, dass auch noch zu einem späteren Zeitpunkt Anfragen eingehen.

7.5 Ausweiskopie und Geldwäschegesetz

Etliche Anfragen betrafen wieder das Problem, dass Kreditinstitute Kopien des Ausweises (Personalausweis oder Reisepass) verlangen und sich dabei auf die im Geldwäschegesetz geregelten Identifizierungs- und Dokumentationspflichten berufen.

Bis zur Änderung des Geldwäschegesetzes im August 2002 wurde den Betroffenen mitgeteilt, dass die Identifizierungspflicht nach dem Geldwäschegesetz erst eingreift, wenn das Kreditinstitut Bargeld in Höhe von 15.000 EURO oder mehr annimmt oder abgibt. Die Feststellungen zur Identifikation waren dann, soweit möglich, durch Kopie des vorgelegten Ausweises zu dokumentieren. Die bloße Eröffnung eines Girokontos löste dagegen noch keine Pflicht zur Anfertigung einer Ausweiskopie aus.

Nunmehr hat ein Kreditinstitut auch bei Abschluss eines Vertrages zur Begründung einer auf Dauer angelegten Geschäftsbeziehung den Vertragspartner entsprechend den Bestimmungen des Geldwäschegesetzes zu identifizieren. Dies betrifft die Eröffnung eines Girokontos, aber auch sonstige Geschäfte wie die Überlassung eines Schließfachs.

Bei der Dokumentation hat das Kreditinstitut nach der Neuregelung einen größeren Handlungsspielraum. Es kann wählen, ob es die für die Identifizierung erforderlichen Daten dem vorgelegten Ausweis entnimmt und aufzeichnet, z.B. im EDV-Datenbestand, oder ob es eine Kopie des Personalausweises oder Reisepasses anfertigt; dabei muss es sich jedoch auf diejenigen Seiten beschränken, welche die erforderlichen Identifizierungsdaten enthalten. Eine Einwilligung des Betroffenen ist nach diesen Bestimmungen nicht erforderlich.

Erfahrungsgemäß machen die Kreditinstitute seither in aller Regel von der nunmehr gesetzlich eingeräumten Möglichkeit Gebrauch, eine Ausweiskopie zum Nachweis der erfolgten Identifizierung zu fertigen. Begründet wird dies hauptsäch-

lich damit, dass dadurch mögliche Fehler beim Abschreiben der Angaben aus dem Ausweis vermieden werden und das Verfahren auch weniger zeitaufwändig ist.

Unverändert blieb die Bestimmung des Geldwäschegesetzes, wonach diese Aufzeichnungen nur für die Verfolgung einer Straftat herangezogen und verwendet werden dürfen.

7.6 Verwendung von Girokontodaten zu Werbezwecken

Ein Betroffener wandte sich an die Aufsichtsbehörde, nachdem er ein Werbeschreiben seiner Bank erhalten hatte, in welchem er unverblümt danach gefragt wurde, weshalb er immer noch Monat für Monat Miete zahle. Zugleich wurden die finanziellen Vorteile des Eigentumserwerbs angepriesen und eine persönliche Beratung hinsichtlich einer Baufinanzierung angeboten. Auf eine entsprechende Anfrage des Kunden teilte ihm die Bank mit, dass sie seine Kontobewegungen analysiert und dabei bemerkt habe, dass der Kunde Mieter war.

Da für die gezielte Auswertung des Überweisungsverkehrs keine Einwilligung des Kunden erteilt worden war, beurteilte sich die Zulässigkeit des Vorgehens der Bank anhand einer - vom Bundesdatenschutzgesetz geforderten - Interessenabwägung. Gegenüberzustellen waren das berechtigte Interesse der Bank, bei ihren Kunden für die von ihr angebotenen Produkte zu werben und das schutzwürdige Interesse des Kunden am Ausschluss dieser Nutzung.

Die Aufsichtsbehörde war hier zwar der Auffassung, dass die Bank durchaus ein berechtigtes Interesse zur Nutzung der Daten zum Zwecke der Werbung hatte, diesem Interesse jedoch ein überwiegendes schutzwürdiges Interesse des Kunden gegenüberstand.

Die Kunden einer Bank, die dort einen Girokontovertrag abgeschlossen haben, bringen dieser Bank ein besonderes Vertrauen entgegen, das sich insbesondere auch auf einen besonderen Schutz hinsichtlich des Umgangs mit Kundendaten bezieht. Die Bank, bei der in aller Regel die einzige Girokontoverbindung besteht, erhält durch die vielfältigen unterschiedlichen Kontobewegungen Kenntnis von den konkreten Lebensumständen des Betroffenen wie sonst kaum ein anderes Unternehmen. Die Bankkunden erwarten, dass die Bank die im Rahmen eines Girokontovertrags bekannt werdenden Daten gleich welchen Inhalts ausschließlich zum Zweck der Durchführung der Girokontotransaktionen und zu keinem anderen Zweck verwenden. Damit ist eine Datennutzung nicht vereinbar, bei welcher der

Kunde - wie im vorliegenden Fall - den Eindruck haben muss, dass er gezielt beobachtet wird und gleichsam unter Rechtfertigungsdruck kommt.

Das schutzwürdige Interesse des Kunden an dem Ausschluss der Nutzung seiner Girokontodaten zu Analysezwecken, um zielgerichtet Werbung betreiben zu können, wird auch nicht durch einen zwischen Kunden und Bank etwa abgeschlossenen übergreifenden Bankvertrag aufgehoben, der die Bank zu derartigen Analysen berechtigen würde. Mit einem Girokontovertrag ist ein derartig umfassendes Bankvertragsverhältnis, das auch eine Vermögensberatung beinhaltet, nicht verbunden. Es geht dem Kunden hier lediglich um eine korrekte Durchführung der in Auftrag gegebenen Transaktionen.

Auch der Verweis auf ein bestehendes Widerspruchsrecht des Kunden hinsichtlich einer derartigen Nutzung der Daten führt zu keiner anderen Beurteilung, da ein solches Widerspruchsrecht (auf das die Kunden im übrigen hätten hingewiesen werden müssen) eine zulässige Datennutzung bereits voraussetzt. Gerade dies war aber nicht der Fall. Eine unzulässige Datennutzung wird aber nicht durch einen fehlenden Widerspruch zulässig.

Für eine gezielte Kundenwerbung und die Erschließung neuer Geschäftsmöglichkeiten bedarf es im Übrigen nicht unbedingt einer gezielten Auswertung von Girokonto-Transaktionen der einzelnen Bankkunden. Eine Werbeansprache ist als abstrakte Information auch ohne eine konkrete Bezugnahme auf die individuelle Situation des Betroffenen durchführbar.

Die Aufsichtsbehörde wies die Bank auf diese Rechtslage hin und forderte sie auf, zukünftig auf derartige Kontoanalysen zum Zwecke gezielter Werbemaßnahmen zu verzichten.

7.7 Datenerhebung bei Konten von Wohnungseigentümergemeinschaften (WEG)

Anlässlich der Umschreibung eines WEG-Kontos auf den neuen Verwalter verlangte ein Kreditinstitut vom neuen Verwalter die Vorlage einer vollständigen Eigentümerliste.
Nach § 154 der Abgabenordnung, der eine Legitimation der Kontoinhaber fordert, sind alle Namen, Anschriften und Geburtsdaten der Kontoinhaber in den Unterlagen festzuhalten.

Die Erhebung von Daten der einzelnen Wohnungseigentümer bei WEG-Konten basiert auf einer entsprechenden Forderung des ehemaligen Bundesaufsichtsamts für das Kreditwesen (BAKred - jetzt BAFin). Ursprünglich hatte das BAKred von den Kreditinstituten mit Schreiben vom 13.08.1997 bei WEG-Konten die Vorlage von Grundbuchauszügen gefordert. Auf entsprechende Einwände der Kreditwirtschaft hat das BAKred dann aber wieder von der Einreichung dieser für die WEG sehr aufwändig zu beschaffenden Unterlagen Abstand genommen und mit Schreiben vom 23.06.1999 und 25.11.1999 nur noch eine jährlich zu aktualisierende Eigentümerliste verlangt. Regelungen bezüglich der Führung von WEG-Konten sind auch in einem mit dem BAKred abgestimmten und für alle Kreditinstitute maßgebenden „Leitfaden zur Bekämpfung der Geldwäsche" enthalten, der vom Zentralen Kreditausschuss, dem Zusammenschluss der Bankenverbände, herausgegeben wurde. Seitdem die endgültige Forderung des BAKred bezüglich der Verfahrensweise bei WEG-Konten feststeht, wird bei allen WEG-Kontoneuanlagen und -umschreibungen eine Eigentümerliste verlangt. Die WEG wird außerdem verpflichtet, das Kreditinstitut über künftige Veränderungen in der Eigentümergemeinschaft zu unterrichten. Die Eigentümerliste ist jährlich vom Verwalter zu überprüfen und eine aktualisierte Fassung beim Kreditinstitut einzureichen.

Datenschutzrechtlich ist gegen die Forderung des Kreditinstituts nach Überlassung einer aktuellen Eigentümerliste nichts einzuwenden. Die Datenerhebung ist zur Erfüllung der gesetzlich vorgeschriebenen Aufgaben des Kreditinstituts erforderlich. Die Übermittlung der Daten der Eigentümer an das Kreditinstitut dient der Zweckbestimmung des Vertragsverhältnisses zwischen dem Verwalter und den Eigentümern und ist damit nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG zulässig.

8 Versicherungswirtschaft

In der Versicherungsbranche waren im Berichtszeitraum sowohl unzureichende technische und organisatorische Maßnahmen (§ 9 BDSG) zu bemängeln als auch Datenschutzverletzungen, die durch persönliches Fehlverhalten einzelner Mitarbeiter verursacht wurden wie beispielsweise das Beifügen von falschen Unterlagen beim manuellen Kuvertieren oder die Übergabe einer Liste, in welcher die Außenstände von anderen Versicherungsnehmern aufgeführt waren, durch einen Versicherungsvertreter an den Versicherten.

8.1 Datenerhebung im Rahmen von Versicherungsanträgen

Ein Thema, das auch in den Gesprächen zwischen den Aufsichtsbehörden für den Datenschutz und dem Gesamtverband der Deutschen Versicherungswirtschaft besprochen wurde, war die Datenerhebung im Rahmen von Kraftfahrtversicherungen.

In einem Fall hat ein Versicherungsunternehmen in seinen Vordrucken für eine Angebotserstellung Daten wie Geburtsdatum, ausgeübter Beruf, derzeitiger Arbeitgeber, Wohneigentum und Garage erhoben, ohne die Betroffenen über den Zweck der Erhebung dieser detaillierten Daten sowie die anschließende Verarbeitung und Nutzung zu informieren. Das Versicherungsunternehmen war der Auffassung, dass nach der damaligen gesetzlichen Regelung im alten BDSG keine Verpflichtung bestand, die Betroffenen über den genauen Zweck der Datenerhebung zu informieren.

Diese Auffassung trifft nicht zu. Da die Daten zum Zwecke der Angebotserstellung gespeichert wurden, war eine Datenerhebung erforderlich, die nach Treu und Glauben und auf rechtmäßige Art und Weise erfolgt ist (§ 28 Abs. 1 Satz 2 BDSG a.F.). Der Forderung nach einer ausführlichen Information der Betroffenen bereits bei der Datenerhebung wurde in der Neufassung des BDSG in § 4 Abs. 3 Ausdruck verliehen.

Um sicher zu stellen, dass die Betroffenen in Kenntnis der Verwendungszwecke der Daten darüber entscheiden können, ob sie die Daten bekannt geben, müssen sie klar und verständlich über die Zwecke der Erhebung und die anschließende Speicherung informiert werden. Die Aufsichtsbehörde hat das Versicherungsunternehmen aufgefordert, bereits in dem Vordruck deutlich darauf hinzuweisen, dass die erhobenen Daten tarifrelevant sind und über die Angebotserstellung hinaus solange gespeichert werden, bis für die Versicherung erkennbar ist, dass es nicht zum Abschluss einer Versicherung kommt. Im Sinne einer umfassenden Aufklärung ist auch auf die Löschfrist hinzuweisen, die von der Versicherung auf sechs Monate ab der Speicherung festgelegt wurde, was im übrigen von der Aufsichtsbehörde als Obergrenze angesehen wurde.

In einem anderen Fall ergab sich im Rahmen der Übertragung eines Schadensfreiheitsrabatts von einem Versicherungsnehmer auf einen anderen das Problem, dass ein Versicherungsunternehmen die Gewährung des Rabatts von der Vorlage einer Führerscheinkopie abhängig machte. Der Führerschein enthält aber neben dem für die Rabattgewährung erforderlichen Ausstellungsdatum personenbezogene Daten, deren Kenntnis für die Versicherung nicht notwendig ist, wie etwa Inhaber mehrerer Führerscheinklassen oder Brillenträger. Von dem Versicherungsun-

ternehmen wurde es als nicht ausreichend angesehen, wenn der Versicherungsvertreter die Angaben aus einem ihm vorgelegten Führerschein bestätigt. Zwischen den Aufsichtsbehörden für den Datenschutz und der Versicherungswirtschaft konnte Einvernehmen erzielt werden, dass für die Feststellung der Voraussetzungen für die Gewährung des Rabatts auch eine Bestätigung der Führerscheinstelle ausreichend ist. Alternativ kann auch eine Kopie des Führerscheins unter Schwärzung der für die Versicherung irrelevanten Angaben vorgelegt werden. Die Versicherungsnehmer sind im Bedarfsfall über beide Möglichkeiten zu informieren.

8.2 Herausgabe von Arztberichten durch die Versicherung

Immer wieder werden der Aufsichtsbehörde Fälle vorgetragen, die im Zusammenhang mit der Ablehnung von Versicherungsverträgen und der darauf hin geforderten Überlassung der Arztberichte oder sonstigen ärztlichen Unterlagen stehen.

So wurde beispielsweise einer Versicherung im Rahmen von Verhandlungen über eine private Krankenhauszusatzversicherung von einem Betroffenen die Erlaubnis erteilt, sich bei dem ihn behandelnden Arzt über seinen Gesundheitszustand zu erkundigen. Auf Grund des Arztberichts war die Versicherung aber nur bereit, einen eingeschränkten Versicherungsschutz zu gewähren. Als der Betroffene um Überlassung des Arztberichtes bat, wurde er von der Versicherung an seinen Arzt verwiesen. Da keine Versicherung zustande kam, wünschte der Betroffene zudem die sofortige Löschung seiner Daten bei der Versicherung.

Die Verweisung an den behandelnden Arzt war datenschutzrechtlich nicht zu beanstanden. Hierfür war maßgeblich, dass die Betroffenen von den vielfach hoch sensiblen Gesundheitsdaten häufig keine Kenntnis haben und diese Daten deshalb auch nicht von der Versicherung gegenüber den Versicherungsnehmern offengelegt werden dürfen. Letztlich respektiert die Versicherung in diesen Fällen nur das Vertrauensverhältnis zwischen Arzt und Patient.

Zur Löschung seiner Daten wurde dem Betroffenen folgende Auskunft gegeben: Nach § 35 Abs. 2 Nr. 3 BDSG sind personenbezogene Daten, die für eigene Zwecke verarbeitet werden, zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, was bei einem nicht zustande gekommenen Vertrag grundsätzlich anzunehmen ist. Nach § 35 Abs. 3 Nr. 1 BDSG tritt jedoch an die Stelle einer Löschung der Daten deren Sperrung, wenn einer Löschung u.a. gesetzliche Aufbewahrungsfristen entgegenstehen. Bei den

Antragsunterlagen handelt es sich um Handelsbriefe, für die handels-, steuer- und aufsichtsrechtliche Aufbewahrungspflichten und -fristen gelten. Insbesondere § 257 des Handelsgesetzbuchs und § 147 der Abgabenordnung regeln die Aufbewahrungspflicht und -frist geschäftlicher Unterlagen. Danach gilt, dass Handels- und Geschäftsbriefe – und als solche sind auch die Unterlagen bezüglich abgelehnter Anträge anzusehen – für die Dauer von mindestens sechs Jahren aufzubewahren sind. Da die Antragsunterlagen bei der Versicherung noch nicht elektronisch gespeichert werden, bedarf es für den Nachweis der ordnungsgemäßen dv-gestützten Buchführung der Originalbelege. Folglich unterliegen sowohl die gespeicherten als auch die in Papierform vorliegenden Daten der Aufbewahrungspflicht. Im Fall des Betroffenen waren die zu seiner Person gespeicherten Daten daher zwar nicht zu löschen, aber nach § 35 Abs. 3 Nr. 1 BDSG zu sperren. Hierzu wurde die Versicherung von der Aufsichtsbehörde aufgefordert.

8.3 Vorlage vertraulicher Unterlagen bei Gericht im Rahmen eines Rechtsstreits

Die Aufsichtsbehörde war mit einigen Fällen befasst, in denen es um die Zulässigkeit der Vorlage von vertraulichen Unterlagen - insbesondere Arztbriefe oder ärztliche Gutachten - im Rahmen von Gerichtsprozessen ging. So etwa befand sich ein Beschwerdeführer im Rechtsstreit mit seiner privaten Versicherung wegen der Zahlung einer Berufsunfähigkeitsrente. Die beklagte Versicherung hatte dem Gericht verschiedene Unterlagen vorgelegt, darunter auch Briefe von Ärzten, bei denen der Betroffene in Behandlung gewesen war.

Die Verwendung „sensitiver“ Daten wie beispielsweise der Angaben über die Gesundheit ist nach dem Gesetz ausdrücklich zugelassen, wenn dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Nutzung überwiegt. Daran gemessen war im geschilderten Fall das Vorgehen der Versicherung zulässig. Überwiegende schutzwürdige Interessen des Betroffenen am Ausschluss der Verwendung waren nicht erkennbar. Zum einen musste ihm bereits bei Klageerhebung bewusst gewesen sein, dass die Versicherung die bei ihr vorhandenen und rechtmäßig erlangten Unterlagen über seinen Gesundheitszustand bei Gericht zum Zwecke der Abwehr eines ihr gegenüber geltend gemachten Anspruchs vorlegen würde. Im Übrigen wäre es auch widersprüchlich, wenn ein Versicherungsnehmer mit einer Klage gegenüber seiner Versicherung Leistungen aus dem Versicherungsvertrag geltend macht, zugleich aber verhindern möchte, dass Unterlagen, die für die Beurteilung der An-

spruchsvoraussetzungen entscheidend sind, in das Gerichtsverfahren eingeführt werden.

8.4 Widerrufene Einwilligung in Datenübermittlung an Wagnisdatei

Verwundert war ein Beschwerdeführer, als er erfuhr, dass sein Antrag auf Abschluss einer Lebens- und Berufsunfähigkeitsversicherung mit dem Hinweis auf einen Eintrag in einer zentralen Wagnisdatei abgelehnt wurde. In dieser Datei, die vom Gesamtverband der Deutschen Versicherungswirtschaft geführt wird und dazu dienen soll, Missbrauch und Betrug sowie Fälle von Doppelversicherung zu Lasten der Versichertengemeinschaft zu verhindern, können Versicherungsunternehmen Kundendaten einmelden. Fragt ein anderes Versicherungsunternehmen - etwa vor Abschluss eines Versicherungsvertrages oder vor Auszahlung einer beantragten Leistung - dann bei der Wagnisdatei an, wird ihr mitgeteilt, dass zu der angefragten Person Daten gespeichert sind und welche Versicherung diese Daten eingemeldet hat. Konkrete Informationen erhält sie jedoch erst auf entsprechende Nachfrage bei der einmeldenden Versicherung.

Der Beschwerdeführer hatte ein Jahr zuvor bei einer anderen Versicherungsgesellschaft ebenfalls einen Antrag auf Abschluss einer Lebens- und Berufsunfähigkeitsversicherung gestellt, der jedoch aus versicherungsmedizinischen Gründen abgelehnt worden war. Die Versicherung hatte seinerzeit das Merkmal „Erschwernis im Bereich Lebens- und Berufsunfähigkeitsversicherung“ an die zentrale Wagnisdatei gemeldet und zwar aufgrund einer datenschutzrechtlichen Einwilligung, die der Beschwerdeführer im Rahmen des Antrags auf Abschluss der gewünschten Versicherungsverträge erteilt hatte. Die Einwilligung umfasste insbesondere die Übermittlung von Daten aus den Antragsunterlagen und der Vertragsdurchführung an Rückversicherer zur Beurteilung des Risikos und zur Abwicklung der Rückversicherung sowie an den Gesamtverband der Deutschen Versicherungswirtschaft zur Weitergabe der Daten an andere Versicherungsgesellschaften. Die Einwilligung galt unabhängig vom Zustandekommen des Vertrages und war nur wirksam, nachdem der Unterzeichnende vom Inhalt des Merkblatts zur Datenverarbeitung, das alle wesentlichen Informationen insoweit enthielt, Kenntnis erlangt hatte.

Später jedoch widerrief der Beschwerdeführer die von ihm abgegebene Einwilligungserklärung. Ein Widerruf hat aber nur Wirkung für die Zukunft. Die bereits - zulässigerweise - erfolgte Übermittlung der Daten an die zentrale Wagnisdatei wird durch den Widerruf nicht in Frage gestellt. Die dort vorhandenen Daten dürfen von der Wagnisdatei weiterhin auf der Grundlage des Bundesdatenschutzgesetzes (§

28 Abs. 1 Satz 1 Nr. 2 und Abs. 3 Satz 1 Nr. 1) gespeichert und auch an anfragende Versicherungsunternehmen übermittelt werden. Ein eventuelles Interesse des Betroffenen an dem Ausschuss der Speicherung ist nicht schutzwürdig, da der Betroffene die vorvertragliche Pflicht hat, risikoerhebliche Umstände anzuzeigen.

9 Gesundheitswesen

9.1 Überprüfung von Abrechnungsstellen medizinischer Leistungen

Überprüft wurden alle der Aufsichtsbehörde mit Sitz in Baden-Württemberg bekannten Abrechnungszentren medizinischer Leistungen. Dort können Ärzte und medizinische Dienstleister Rechnungen für Leistungen, die nicht direkt mit den gesetzlichen Krankenkassen abgerechnet werden können, erstellen und einziehen lassen. Dies trifft insbesondere bei Abrechnungen mit Privatpatienten zu.

Der Schwerpunkt der Überprüfung war die Einholung der Einwilligung des Patienten. Sie ist Voraussetzung, wenn der Arzt oder medizinischer Dienstleister Patientendaten an die externe Abrechungsstelle zur Verarbeitung weitergeben will. Die Notwendigkeit der Einwilligung ergibt sich aus der Schweigepflicht nach § 203 StGB sowie aus § 28 Abs. 6 BDSG, der Vorschrift über „besondere Arten personenbezogener Daten“, zu denen auch die Patientendaten gehören. Sind Patientendaten ohne Einwilligung an eine Abrechnungsstelle übermittelt worden, dürfen sie von der Abrechungsstelle nicht gespeichert werden, da der Rechtsverstoß dadurch fortgesetzt würde. Es ist daher die eigene Pflicht der Abrechnungsstelle, sicherzustellen, dass die Einwilligung vom behandelnden Arzt rechtzeitig vor der Übermittlung der Daten eingeholt wird. Hiervon muss sich die Abrechnungsstelle durch geeignete Mittel, zumindest stichprobenweise, vergewissern.

Die Überprüfungen ergaben, dass die datenschutzrechtlichen Anforderungen im Wesentlichen beachtet wurden. Allerdings mussten drei Abrechnungsstellen einer Firmengruppe erst durch die Einleitung eines Ordnungswidrigkeitenverfahrens zur Auskunftserteilung veranlasst werden.

9.2 Weitergabe von Patientendaten an eine Selbsthilfegruppe

Eine Patientin eines Krankenhauses, die dort in privatärztlicher Behandlung war, erhielt nach ihrer Entlassung ein Informations- und Werbeschreiben einer Selbsthilfegruppe zugeschickt. Wie die Ermittlung der Aufsichtsbehörde ergab, hatte die behandelnde Krankenhausärztin die Adresse der Patientin für das

behandelnde Krankenhausärztin die Adresse der Patientin für das Schreiben genutzt. Die Ärztin war zugleich Vorsitzende der Selbsthilfegruppe, deren Tätigkeit sich auf die Krankheit erstreckte, die bei der Patientin festgestellt worden war.

Die für die Behandlung und Abrechung erforderlichen Patientendaten sind personenbezogene Daten. Die Krankenhausärztin hatte die Patientenadresse zur Privatliquidation erhalten. Die Nutzung der Adressen für einen anderen Zweck, auch wenn es ein anderer eigener Geschäftszweck ist, ist nach § 28 Abs. 6 BDSG nur mit der Einwilligung des Betroffenen zulässig. Die Aufsichtsbehörde hat der Ärztin geraten, das Informationsschreiben den betreffenden Patienten schon während des Krankenhausaufenthalts auszuhändigen oder ihr Einverständnis für eine spätere Zusendung einzuholen.

9.3 Heimverträge für Senioren

Die Pflege von älteren Menschen findet heutzutage immer mehr in einem Heim statt. Deshalb erreichen uns auch Anfragen, die sich auf die datenschutzrechtliche Beurteilung von Heimverträgen beziehen. In dem hier geschilderten Fall ging es darum, ob es zulässig ist, dass sich der Heimträger in einem Heimvertrag die Berechtigung einräumen lässt, den Pflegekassen bzw. dem Medizinischen Dienst der Krankenkassen die über den Heimbewohner geführte Pflegedokumentation zugänglich zu machen, und ob der Heimträger den Pflegekassen bzw. dem Medizinischen Dienst der Krankenkassen Mitteilung über den jeweiligen Gesundheitszustand des Heimbewohners machen darf.

Für die datenschutzrechtliche Bewertung des Heimvertrags sind die Vorschriften des Sozialgesetzbuchs (SGB) und hier insbesondere das Elfte Buch (XI) „Soziale Pflegeversicherung“ (SGB XI) anzuwenden.

Nach § 104 SGB XI, der die Pflichten des Leistungserbringers (hier des Heimträgers) regelt, ist der Leistungserbringer berechtigt und verpflichtet, die erforderlichen Angaben über die Versicherungsleistungen aufzuzeichnen und an die Pflegekassen zu übermitteln.

Dies gilt sinngemäß auch für den Medizinischen Dienst, der nach § 97 SGB XI personenbezogene Daten für Zwecke der Pflegeversicherung erheben, verarbeiten und nutzen darf, soweit dies für Prüfungen, Beratungen und gutachterliche Stellungnahmen nach den §§ 18 (Verfahren zur Feststellung der Pflegebedürftigkeit),

40 (Pflegehilfsmittel und technische Hilfen) und 80 SGB XI (Maßstäbe und Grundsätze zur Sicherung und Weiterentwicklung der Pflegequalität) erforderlich ist.

Die Regelung im Heimvertrag war daher datenschutzrechtlich nicht zu beanstanden.

10 Handel und Dienstleistungen

10.1 Fingerabdruckverfahren zur Identifizierung des Kunden

Eine Software-Firma präsentierte der Aufsichtsbehörde ein Vorhaben, bei dem ein Warenwirtschaftssystem um ein Fingerabdruckverfahren zur Identifizierung der Kunden erweitert werden sollte. Das Warenwirtschaftssystem dient u.a. der Fakturierung (Rechnungs-, Lieferscheinerstellung, Berechnung des Rabatts) von Waren, die beispielsweise von einem Großhändler an seine Kunden (Einzelhändler, Handwerker) abgegeben werden. Um den Nachweis zu führen, wer wann welche Ware bezogen hat, kommen bisher vielfach Kundenkarten zur Anwendung. Mit dem geplanten Fingerabdruckverfahren sollte dieser Nachweis noch einfacher und zugleich sicherer werden.

Das Fingerabdruckverfahren ist ein Verfahren, das mittels biometrischer Merkmale eine
Identifikation und eine Authentifikation einer Person durchführt. Dabei entstehen personenbezogene Daten. Werden diese personenbezogenen Daten automatisiert verarbeitet, so sind nach § 1 Abs. 2 Nr. 3 BDSG die Vorschriften des Bundesdatenschutzgesetzes (BDSG) zu beachten.

Die Aufsichtsbehörde wies darauf hin, dass bei der Auswahl der einzusetzenden Verfahren nach § 3a BDSG der Grundsatz der Datenvermeidung und Datensparsamkeit zu beachten ist. Danach haben sich Gestaltung und Auswahl von Datenverarbeitungssystemen an dem Ziel auszurichten, keine oder so wenig wie möglich personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen. Es gibt mehrere technische Realisierungsmöglichkeiten des Fingerabdruckverfahrens. Eine Variante setzt die zentrale Speicherung der biometrischen Merkmale voraus. Als Alternative kommt in Betracht, dass die zu identifizierende Person die gemessenen biometrischen Daten der Fingerabdrücke mit sich führt (z. B. als Chip-Karte) und im Identifikationssystem lediglich die Übereinstimmung dieser Daten mit den gemessenen biometrischen Daten der Kunden überprüft wird. Bei diesem Verfahren bleibt die Kontrolle über die biometrischen Merkmale, mittels dezentralem Daten-

träger, bei den betroffenen Kunden. Eine Verknüpfung der personenbezogenen biometrischen Daten und der im Warenwirtschaftssystem vorhandenen personenbezogenen Daten (Anschrift und Name) ist mit diesem Verfahren nicht möglich. Der Software-Firma wurde deshalb mitgeteilt, dass im Hinblick auf den Grundsatz der Datenvermeidung und Datensparsamkeit die zweite Variante vorzuziehen ist.

10.2 Barkauf von Waren nur in Verbindung mit Angabe persönlicher Daten

Eine Firma mit mehreren Filialen in Deutschland, die Computerzubehör sowie Soft- und Hardware vertreibt, bestand darauf, dass bei Barverkäufen Namen und Anschrift der Kunden erhoben und gespeichert wurden. Widerstrebenden Kunden wurde mitgeteilt, dass dies in allen Filialen so üblich sei. Auf Nachfrage wurde der Aufsichtsbehörde mitgeteilt, dass die Erhebung und Speicherung der personenbezogenen Daten auch von Barzahlern insbesondere aus Gründen des Marken- und Urheberrechts zwingend erforderlich sei.

Nach einer intensiven Erörterung mit dem Unternehmen stand für die Aufsichtsbehörde fest, dass für einen Computerhändler Auskunftspflichten nach dem Marken- und Urheberrecht allenfalls über Namen und Adressen von Herstellern, Lieferanten und anderen Vorbesitzern in Betracht kommen. Es bestand daher kein Grund, von Letztverbrauchern bei Barkäufen den Namen und die Anschrift zu fordern.

Das Unternehmen teilte daraufhin mit, dass die Angabe des Namens und der Anschrift bei Barkäufen freiwillig und ohne Einfluss auf das Zustandekommen des Kaufvertrages sein sollte. Die erhobenen Daten sollten ausschließlich zur Rechnungsstellung verwendet und der Kunde auf diesen ausschließlichen Verwendungszweck hingewiesen werden. Zu guter Letzt hat sich das Unternehmen dann aber doch entschlossen, ganz auf die Erhebung von Kundendaten bei Bar-Verkäufen an private Endverbraucher zu verzichten.

10.3 Kundenkarten im Einzelhandel

Die Kundin eines Einzelhändlers bemerkte, dass ihre neue Kundenkarte über eine Lastschriftfunktion verfügte, obwohl sie dies gar nicht beantragt hatte. Im Kundenkartenantrag hatte sie die Frage nach der Bankverbindung bewusst nicht ausgefüllt, da sie nur in den Genuss des mit der Karte verbundenen Rabatts kommen wollte.

Bei der Nachprüfung durch die Aufsichtsbehörde stellte sich heraus, dass die Kundin bei dem Einzelhändler einmal mit ihrer Bankkarte bezahlt und zugleich wegen der Rabattpunkte ihre Kundenkarte vorgelegt hatte. Bei dieser Gelegenheit wurde die Bankverbindung (Kontonummer und Bankleitzahl) automatisch im Kundenkartenkonto gespeichert. Der Kundin sollte damit ermöglicht werden, beim nächsten Einkauf mit der Kundenkarte im Lastschriftverfahren zu bezahlen, ohne die Bankkarte vorlegen zu müssen, da das Kassensystem automatisch auf die im Kundenkartenkonto bereits gespeicherte Bankverbindung zurückgreifen kann.

Die Bankverbindung ist ein personenbezogenes Datum des Kunden. Falls der Kunde beim Kundenkartenantrag seine Bankverbindung angegeben hat, darf dieses Datum gespeichert und zum Zweck des Lastschrifteinzugs genutzt werden, in den der Kunde ohnehin auf dem Lastschriftbeleg noch gesondert einwilligen muss.

Die heimliche Speicherung der Bankverbindung im Kundenkartenkonto war jedoch datenschutzrechtlich unzulässig und von der Aufsichtsbehörde zu beanstanden.

10.4 Elektronische Fahrkarten im Linienbus

Bei einem privaten Verkehrsunternehmen wurde der Einsatz elektronischer Fahrscheine überprüft. Bei den Fahrscheinen handelt es sich um Kärtchen mit Magnetstreifen, auf denen die gelöste Fahrstrecke gespeichert werden kann. Bei Mehrfahrtenkarten kann der Fahrschein mit einem Guthaben aufgeladen werden. Es wird für jede Fahrt ein eigener Datensatz angelegt. In den Fahrzeugen werden die Daten der gelösten Fahrstrecke ausgelesen und zusammen mit einer eventuellen Barzahlung gespeichert. Damit können Abrechnungs- und Bewegungsdaten der Fahrgäste erfasst und für die Abrechnung mit den öffentlichen Stellen (Fördermittel ÖPNV), für die Abrechnung der Fahrerkassen, für die betriebliche Rechnungslegung, für die Optimierung des Fahrzeugeinsatzes und eine bedarfsabhängige Fahrplangestaltung, sowie zur Missbrauchskontrolle ausgewertet werden. Datenschutzrechtlich gesehen, bergen solche Systeme erhebliche Gefahren in sich, da sie die Möglichkeiten bieten, Nutzungs- und Bewegungsprofile der Fahrgäste anzulegen. Die Aufsichtsbehörde hielt daher eine Überprüfung vor Ort für erforderlich.

Bewegungsdaten, die einer bestimmten Person zugeordnet werden können, sind personenbezogene Daten. Das Unternehmen musste daher bei der Realisierung des Systems besonderen Wert darauf legen, dass möglichst jeglicher Personenbezug vermieden wird. Dies wurde mit der Ausgabe mit Bargeld aufladbarer Inha-

berkarten gelöst. Schülerkarten, deren Kosten mit den kommunalen Stellen abzurechnen sind, werden über die Schulen ausgegeben und zwar in einer Weise, die für das Verkehrsunternehmen keinen nachträglichen Personenbezug ermöglicht. Lediglich bei der Variante der Monatskarte mit Abbuchung vom Girokonto ist ein Personenbezug technisch möglich. Durch den Einsatz eines eigenen Rechnersystems zur Abbuchung, das technisch von dem Fahrkartensystem getrennt ist, und durch organisatorische Maßnahmen wird eine Verknüpfung der verschiedenen Daten vermieden. Nur die Information, dass die Fahrkarte für den aktuellen Zeitraum bezahlt ist, wird aus dem Abbuchungssystem in das Fahrkartensystem übernommen.

Das System kann im Übrigen die Manipulation einer Karte erkennen. Ein konkreter Personenbezug entsteht in diesem Fall jedoch erst dann, wenn der Nutzer einer manipulierten Karte gefasst wird. Die Verarbeitung der Daten hier für ist nach § 28 Abs. 1 Nr. 1 BDSG zulässig. Zur Datenverarbeitung im Rahmen der Zweckbestimmung eines Beförderungsvertragsverhältnisses gehört auch die Prüfung, ob die Zahlung tatsächlich erfolgt ist. Entgegenstehende überwiegende Interessen des Betroffenen sind nicht ersichtlich.

Insgesamt wurde das elektronische Fahrscheinsystem von der Aufsichtsbehörde für datenschutzgerecht befunden.

10.5 Verarbeitung biometrischer Daten in einer Videothek

Neben herkömmlichen Videotheken, in denen die Ausleihe an einem Schalter durch Ausleihpersonal erfolgt, gibt es auch Automaten-Videotheken. Der Kunde identifiziert sich hier mit einer Kundenkarte. Damit die Karte nicht an einen anderen, beispielsweise an einen Minderjährigen, weiter gereicht werden kann, wird vom Karteninhaber eine elektronische Kontrolle seines Daumenabdruckes verlangt. Anschließend gibt er seine Auswahl in einen Automaten ein und erhält von dort die Videokassette; das Entgelt wird automatisch abgebucht. Personal des Verleihers ist nicht anwesend. Somit entfällt die Kontrollfunktion, die ansonsten das Personal im Hinblick auf den Jugendschutz innehat. Die Kundin einer Automaten-Videothek mit jugendgefährdenden Angeboten beschwerte sich über die Kontrolle des Daumenabdrucks.

Im Zuge der Überprüfung durch die Aufsichtsbehörde stellte sich heraus, dass der Betreiber der Automatenvideothek durch gerichtlichen Beschluss verpflichtet worden war, ein sogenanntes „Finger-Print-System“ (System zum Erkennen der Zu-

gangsberechtigung mittels Vergleichs des Daumenabdrucks) und eine Videoüberwachung mit kontinuierlicher Bildaufzeichnung der eintretenden Personen einzusetzen. Dieser Gerichtsbeschluss basierte auf der ständigen Rechtsprechung, nach der Automaten-Videotheken mit jugendgefährdeten Inhalten nur dann betrieben werden dürfen, wenn die zutrittsberechtigten Personen sich mittels biometrischer Erkennung identifizieren. Ferner muss im Verleihraum eine Videokontrolle durchgeführt werden, um sicherzustellen, dass zutrittsberechtigte Personen nicht weitere Personen durch die Schleuse schmuggeln.

Es stellt sich heraus, dass der Daumenabdruck nur für die Identifizierung beim Zugang genutzt wurde, d.h. zur Überprüfung, ob der Karteninhaber mit der eintretenden Person identisch ist. Das Videoband der Überwachungsanlage wurde täglich auf Missbrauch kontrolliert, danach wurde es unverzüglich gelöscht.

Unter diesen Voraussetzungen wurde die Erhebung der biometrischen Daten für zulässig erachtet. Der Kunde muss zudem bei der Erfassung selbst mitwirken.

10.6 Erfassung der Besucherdaten bei einer Fachmesse

Ein Messebesucher informierte die Aufsichtsbehörde davon, dass die Messegesellschaft beim Verkauf von Eintrittskarten für eine Fachmesse von den Besuchern auf einem Fragebogen zahlreiche personenbezogene Daten erhob. Die Angaben wurden in einer Datenbank gespeichert. Bei Einlass erhielt jeder Besucher ein Namensschild, das mit seinem Namen und einem Barcode versehen war. Der Barcode wies auf den Datensatz des Besuchers in der Datenbank hin. Die Aussteller konnten an ihren Ständen die Standbesucher über den Barcode auf dem Namensschild erfassen und damit die Daten der Standbesucher aus der Datenbank abrufen. Darüber hinaus sollte die Adressdaten der Besucher für eigene Werbezwecke der Messegesellschaft genutzt werden.

Als Rechtsgrundlage für die Erhebung und Verarbeitung der Daten kam im vorliegenden Fall nur eine Einwilligung in Betracht. Wirksam ist nach § 4a Abs. 1 BDSG aber nur eine „informierte Einwilligung“. Der Messebesucher muss deshalb in dem Fragebogen darauf hingewiesen werden, für welche Zwecke die Daten erhoben werden, an wen die Daten übermittelt und wann sie gelöscht werden. Daran fehlte es im konkreten Fall. Darüber hinaus muss eine Einwilligung, um wirksam zu sein, auf der freien Entscheidung des Betroffenen beruhen. Die Messegesellschaft stellte hierzu klar, dass die Besucher auch ohne Ausfüllung des Fragebogens eingelassen würden, was allerdings nicht den Erfahrungen entsprach, von denen der

eingangs erwähnte Messebesucher der Aufsichtsbehörde berichtete. Die Messegesellschaft wurde deshalb aufgefordert, den Besucher im Fragebogen darauf hinzuweisen, dass die Angaben freiwillig sind, und auch ihre Mitarbeiter entsprechend zu instruieren.

10.7 Datenschutzwidrige Verwendung von Druckerdaten

Die Aufsichtsbehörde wurde gefragt, ob es zulässig ist, dass ein neues Druckermodell eines bestimmten Herstellers Verbrauchsdaten per Internet an den Hersteller schickt. Die Überprüfung ergab, dass bei der Installation des Druckertreibers im PC zugleich ein Programm installiert wird, das Verbrauchsdaten des Druckers sammelt und in Abständen an den Hersteller schickt. Beim Installationsvorgang wird der Kunde zwar gefragt, ob er diese Funktionalität deaktivieren will, beachtet er die Frage jedoch nicht und klickt bei der Installation auf „weiter“, so werden zukünftig Daten übermittelt. Den Vorgang kann er jedoch auch später jederzeit abschalten. Die Daten werden über das Internet direkt vom PC des Kunden an die Datenbank bei einem anderen Konzernunternehmen des Hersteller geschickt, wo sie für statistische Zwecke des Herstellers und für druckerbezogene Auswertungen, die nur der Kunde dort selbst abrufen kann, gespeichert werden. Mit den Verbrauchsdaten wird auch die Seriennummer des jeweiligen Druckers gespeichert. Ferner wird die IP-Adresse des Absenders in einer Protokolldatei gespeichert.

Über die IP-Adresse und die Seriennummer sind die Verbrauchsdaten personenbeziehbare Daten. Die IP-Adresse ist nach allgemeiner Auffassung der Datenschutzaufsichtsbehörden ein personenbeziehbares Datum. Die Seriennummer ist ebenfalls ein personenbeziehbares Datum, da der Druckerkäufer die Möglichkeit hat, sich aus anderen Gründen beim Hersteller selbst zu registrieren.

Für die Datenübermittlung ist der Hersteller datenschutzrechtlich verantwortlich. Voraussetzung für eine rechtmäßige Übermittlung ist eine datenschutzrechtlich wirksame Einwilligung des Betroffenen, die hier nicht vorliegt. Die fehlende wirksame Einwilligung wurde gegenüber dem Hersteller beanstandet. Dieser wird zukünftig die Einwilligung und die Information datenschutzgerecht gestalten und ferner die Speicherung der IP-Adresse unterlassen.

11 Verarbeitung von Arbeitnehmerdaten

11.1 Bekanntgabe des Beratungshonorars eines freien Mitarbeiters vom ehemaligen Arbeitgeber an eine Rechtsanwältin

Scheidungs- und Unterhaltsverfahren sind in den meisten Fällen für beide Betroffenen mit Unannehmlichkeiten verbunden. Im konkreten Fall hatte die Rechtsanwältin der Ehefrau ein Auskunftsersuchen an die Firma gerichtet, für die der Ehemann tätig war, und um Mitteilung der an den Ehemann gezahlten Beratungshonorare gebeten. Die Firma gab der Rechtsanwältin darauf hin die gewünschte Auskunft, ohne den betroffenen Ehemann davon in Kenntnis zu setzen oder gar um Einwilligung zu bitten. Die Rechtsanwältin hatte sich bei ihrem Ersuchen an das Unternehmen auf §§ 1580 (Auskunftspflicht der Ehegatten untereinander) und 1605 BGB (Auskunftspflicht über Einkommen und Vermögen) berufen. Danach seien nach § 1605 Abs. 1 Satz 2 BGB wegen der Unterhaltspflicht des Betroffenen auf Verlangen Belege über die Höhe der Einkünfte, insbesondere Bescheinigungen des Arbeitgebers, vorzulegen.

Das Unternehmen hat mit der Erteilung der Auskunft an die Rechtsanwältin gegen das BDSG verstoßen. Die von der Rechtsanwältin angeführten Rechtsvorschriften (§§ 1580 und 1605 BGB) können die Übermittlung der Daten nicht rechtfertigen, da sie nur die Auskunftspflicht zwischen den Eheleuten regeln. Der Anspruch auf Auskunft über das Beratungshonorar hätte von der Rechtsanwältin direkt an den betroffenen Ehemann gerichtet werden müssen und nicht an die Firma. Im Übrigen wäre das Familiengericht zur Festlegung der Unterhaltszahlungen auf die Firma zugekommen. Gegenüber dem Gericht wäre die Firma unmittelbar zur Auskunft verpflichtet gewesen.

11.2 Ärztliches Zeugnis bei Bewerbungen

„Muss ich wirklich all diese Daten offen legen?“, fragte sich ein Beschwerdeführer, der sich bei einer Akademie für den Ausbildungslehrgang zum Psychotherapeuten bewerben wollte und zu diesem Zweck auch ein sehr umfangreiches ärztliches Zeugnis vorlegen sollte. In diesem ärztlichen Zeugnis sollte der Arzt insbesondere zu folgenden Punkten Angaben über den Bewerber machen: Gewicht, Größe, frühere Krankheiten und Operationen, Zustand der Sinnes-, Bewegungs- und Inneren Organe, dem Nervensystem, dem psychischen Verhalten, etwaigen Anfallsleiden, erforderlicher Schonung während der Menstruation, Schwangerschaft und Rausch- bzw. Betäubungsmittelmissbrauch. Abschließend musste der Arzt beurteilen, ob bei dem Bewerber Anhaltspunkte für das Vorliegen von Anlagefehlern oder Erkrankungen vorliegen, die den Untersuchten für den Beruf des Psychotherapeuten ungeeignet machen würde oder nicht. Das mit Stempel und Unterschrift des Arztes versehene Zeugnis musste dann mit den anderen Bewerbungsunterlagen bei der Akademie eingereicht werden.

Gegen die Vorlage eines ärztlichen Zeugnisses bestehen im Kern keine datenschutzrechtlichen Bedenken, zumal auch das „Gesetz über die Berufe in der Psychotherapie“ für den Zugang zur Ausbildung zum Psychotherapeuten die gesundheitliche Eignung des Bewerbers zur Ausübung des Berufes voraussetzt. Dies bedeutet jedoch nicht, dass jede denkbare Frage im Zusammenhang mit dem Gesundheitszustand des Bewerbers zulässig ist. Es dürfen nur solche Fragen gestellt werden, die Aufschluss über die gesundheitliche Eignung des Bewerbers geben können und für diese Beurteilung auch notwendig sind. Als datenschutzrechtlich unzulässig - weil nicht erforderlich - wurden Fragen zur jetzigen oder früheren Berufstätigkeit, nach dem Bestehen einer Schwangerschaft oder nach Menstruationsbeschwerden angesehen. Fragen nach früheren Krankheiten sind auf solche Fälle zu beschränken, bei denen noch aktuell fortwirkende Folgen bestehen. Es ist insgesamt zweifelhaft, ob es überhaupt erforderlich ist, derartig umfangreiche Angaben zu verlangen, um die gesundheitliche Eignung des Bewerbers beurteilen zu können. Die Aufsichtsbehörde machte der Akademie daher den Vorschlag, zukünftig lediglich das vom untersuchenden Arzt bestätigte Ergebnis der Untersuchung für die Bewerbung ausreichen zu lassen. Der Arzt müsste dann nur noch bescheinigen, ob der Bewerber gesundheitlich zur Ausübung des Berufs des Psychotherapeuten geeignet ist oder nicht.

Die Akademie erklärte, dass sie zukünftig auf die Vorlage des ärztlichen Zeugnisses verzichten und die bloße Erklärung des Arztes zur gesundheitlichen Eignung

des Bewerbers als ausreichend anerkennen würde. Den Bedenken der Aufsichtsbehörde wurde somit Rechnung getragen.

11.3 Fragebogen bei Bewerbung für ein Arbeitsverhältnis

Eine Beschwerdeführerein war auf Veranlassung des Arbeitsamtes zu einem Bewerbungsgespräch bei einer Zeitarbeitsfirma eingeladen worden. Bevor sie jedoch Informationen über die zu besetzende Stelle erhielt, wurde sie aufgefordert, einen Personalfragebogen auszufüllen. Dieser enthielt teilweise sehr weitgehende Fragen etwa nach Vorstrafen, dem letzten Verdienst oder der Bankverbindung. Die Aufsichtsbehörde hat den Fragebogen unter dem Blickwinkel des Datenschutzrechts geprüft und das Ergebnis der Zeitarbeitsfirma mitgeteilt.

Dem Arbeitgeber steht im Rahmen eines Vorstellungsgespräches ein umfangreiches Fragerecht zu, das allerdings auch Beschränkungen unterliegt. So dürfen etwa Fragen nach dem Bestehen einer Schwangerschaft, der Religions- oder Parteizugehörigkeit in der Regel nicht gestellt werden. Darüber hinaus dürfen aus datenschutzrechtlicher Sicht Daten beim Betroffenen nur erhoben werden, soweit die Erhebung erforderlich ist. Insoweit ist auch der Grundsatz der Datenvermeidung und Datensparsamkeit zu beachten.

Im Beschwerdefall war es nach Auffassung der Aufsichtsbehörde zum Zeitpunkt der Vorstellung der Bewerberin unzulässig, nach der Bankverbindung und der Krankenkasse zu fragen. Die Beantwortung dieser Fragen spielt für die Entscheidung des Arbeitgebers, ob ein Bewerber für die Besetzung einer bestimmten Arbeitsstelle in Betracht kommt, keine Rolle. Beide Fragen müssen erst dann beantwortet werden, wenn das Arbeitsverhältnis auch tatsächlich begründet wird. Die Frage nach dem letzten Verdienst der Bewerberin wurde ebenfalls als unzulässig angesehen, jedenfalls soweit der bisherige Verdienst für die zu besetzende Stelle keine Aussagekraft hat und die Bewerberin diesen Verdienst nicht von sich aus als Mindestvergütung für die neue Stelle fordert. Die Frage nach etwaigen Vorstrafen ist nur dann zulässig, wenn und soweit die zu besetzende Stelle oder die zu leistende Arbeit dies erfordert. Es muss sich um eine bezogen auf die Arbeitsstelle einschlägige Vorstrafe handeln. So kann es als zulässig angesehen werden, etwa einen Kraftfahrer nach Vorstrafen aufgrund von Verkehrsdelikten oder eine Kassiererin nach solchen aus Vermögensdelikten zu fragen. Zudem beschränkt sich das Fragerecht auf Vorstrafen, die im Bundeszentralregister noch nicht gelöscht sind.

Der Fragebogen musste daher von der Zeitarbeitsfirma entsprechend abgeändert werden. Die wahrheitswidrige Beantwortung der als unzulässig beurteilten Fragen hätte allerdings für die Bewerberin keine nachteiligen Folgen haben dürfen.

11.4 Bewerbungsunterlagen

Die Aufsichtsbehörde ist immer wieder mit Fällen befasst, in denen Bewerber ihre bei Firmen eingereichten Bewerbungsunterlagen nach Abschluss des Bewerbungsverfahrens trotz entsprechender Bitten nicht zurückerhalten.

Das Bundesdatenschutzgesetz findet auf diese Fälle nur dann Anwendung, wenn die in den Unterlagen enthaltenen Daten unter Einsatz von Datenverarbeitungsanlagen oder in oder aus nicht automatisierten Dateien (strukturierten Datensammlungen wie beispielsweise Karteien) verarbeitet, genutzt oder dafür erhoben werden.

Diese Merkmale sind bei Bewerbungsunterlagen in vielen Fällen nicht erfüllt, so dass es für eine Herausgabe derartiger Unterlagen keine datenschutzrechtliche Grundlage gibt. In diesen Fällen muss die Herausgabe im Streitfall auf dem Zivilrechtsweg erreicht werden. Die Aufsichtsbehörde kann hier nicht weiterhelfen. Grundsätzlich gilt jedoch, dass Unterlagen von Bewerbungen, die nicht zu einer Einstellung geführt haben, den Betroffenen unverzüglich zurückzusenden sind. Zu beachten ist zudem, dass nur entsprechend autorisierte Beschäftigte Zugang zu Bewerbungsunterlagen haben, weshalb diese Unterlagen entsprechend zu sichern sind.

Sofern das Bundesdatenschutzgesetz Anwendung findet, haben die Betroffenen einen Anspruch auf Löschung der personenbezogenen Daten, wenn der Bewerbungsvorgang abgeschlossen ist. Dann dürfen die Personaldaten eines abgelehnten Bewerbers nicht mehr gespeichert werden, d.h. ein zwecks der Bewerbung ausgefüllter Personalfragebogen ist zu vernichten, sonst gespeicherte Bewerberdaten müssen gelöscht werden.

11.5 Insolvenzverfahren und Datenschutz

„Was passiert eigentlich mit meinen personenbezogenen Daten, nachdem gegen meinen Arbeitgeber ein Insolvenzverfahren eröffnet wurde?“ Die Firma, bei welcher der Betroffene bis vor kurzem gearbeitet hatte, war insolvent, ein Insolvenz-

verwalter war bestellt worden. Zwei Firmen hatten den Betrieb übernommen, jedoch nur insgesamt einen Teil der bisherigen Belegschaft. Beide Erwerberfirmen hatten zunächst - neben dem Insolvenzverwalter - Zugriff auf sämtliche personenbezogene Daten der Mitarbeiter des übernommenen Betriebes wie etwa Zeugnisse, Personallisten, Personalkorrespondenz und Zeiterfassungsdaten.

Nach Auffassung der Aufsichtsbehörde war diese Verfahrensweise nicht mit dem Bundesdatenschutzgesetz vereinbar. Die personenbezogenen Daten der Mitarbeiter hätten nur jeweils in dem Umfang zur Verfügung gestellt werden dürfen, in dem dies für die jeweilige übernehmende Firma auch tatsächlich erforderlich war. So gab es keinen Grund, den Erwerberfirmen personenbezogene Daten von ausgeschiedenen Miterbeitern oder solchen Mitarbeitern zur Verfügung zu stellen, die beim jeweils anderen Betrieb weiterbeschäftigt wurden. Anders fällt die Beurteilung hinsichtlich des Insolvenzverwalters aus. Dieser benötigt die vorhandenen Personaldaten der Mitarbeiter des insolventen Unternehmens in der Regel noch für die Abwicklung des Insolvenzverfahrens. Solange sie hierfür gebraucht werden, dürfen sie vom Insolvenzverwalter gespeichert werden. Sobald sie aber nicht mehr für Zwecke der Abwicklung des Insolvenzverfahrens benötigt werden, sind die Daten zu löschen.

Nachdem die Aufsichtsbehörde sowohl den Insolvenzverwalter als auch die beiden übernehmenden Firmen über die Rechtslage informiert hatte, wurden die Daten von den Firmen entsprechend gelöscht. Der Insolvenzverwalter sagte zu, dies nach Abschluss des Insolvenzverfahrens zu veranlassen.

12 Tele- und Mediendienste, Internetprovider

Das Internet ist nach wie vor ein sich rasant entwickelndes Medium, das immer neue Nutzungsmöglichkeiten elektronischer Dienste hervorbringt. Daraus resultieren entsprechende Risiken für das Persönlichkeitsrecht des Einzelnen. Für die Datenschutzaufsicht im nichtöffentlichen Bereich stellt dies eine besondere Herausforderung dar, die in technischer und rechtlicher Hinsicht vielfach mit schwierigen Fragestellungen verbunden ist. Diese Fragen werden die Aufsichtsbehörde in Zukunft voraussichtlich verstärkt beschäftigen.

Für die Informations- und Kommunikationsdienste des Internet gelten die besonderen Datenschutzbestimmungen des Teledienstedatenschutzgesetzes (TDDSG) und des Mediendienste-Staatsvertrags. Teledienste sind Dienste, die eine interaktive Nutzung ermöglichen, beispielsweise die Bestellung angebotener Waren. Me-

diendienste sind Informationsdienste, die an die Allgemeinheit gerichtet sind, beispielsweise eine Homepage oder eine elektronische Zeitung. Die besonderen Datenschutzbestimmungen regeln das Verhältnis zwischen Anbietern und Nutzern und die Verarbeitung der dabei anfallenden Dienstedaten.

Das Teledienstedatenschutzgesetz wurde im Zusammenhang mit dem Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz -EGG- vom 14.12.2001, BGBl I S. 3721) weiterentwickelt. Geändert wurde unter anderem die als unpraktikabel empfundene Vorschrift über die elektronische Einwilligung des Nutzers in die Nutzung seiner Daten, die nur mit Hilfe der kaum verbreiteten elektronischen Signatur erteilt werden konnte. Nach der Novellierung ist für eine wirksame Einwilligung erforderlich, dass sie durch eine eindeutige und bewusste Handlung des Nutzers erfolgt, der Inhalt der Einwilligung protokolliert wird und jederzeit vom Nutzer abgerufen werden kann.

Die Länder haben in einem Änderungsstaatsvertrag zum Mediendienstestaatsvertrag (MDStV) die Änderungen des TDDSG übernommen. Er trat am 01.07.2002 in Kraft.

12.1 Veröffentlichung von Schuldnern im Internet

Von mehreren Beschwerdeführern wurden die Aufsichtsbehörde auf eine Internet-Seite hingewiesen, die Schuldner im Internet öffentlich anprangerte. Dem Anbieter dieses Mediendienstes wurde die Rechtslage erläutert. Da die Datenschutzvorschriften des Mediendienste-Staatsvertrags nur im Verhältnis zwischen Nutzern und Anbietern von Mediendiensten gelten, hier aber der Inhalt des Angebots zu beurteilen ist, kommt das BDSG zur Anwendung. Eine Veröffentlichung personenbezogener Schuldnerdaten im Internet stellt datenschutzrechtlich eine Datenübermittlung dar.

Bei allem Verständnis dafür, dass ein Gläubiger seine offenen Forderungen beglichen sehen will, so ist doch zu berücksichtigen, dass eine Übermittlung und damit Veröffentlichung von Schuldnern im Internet besondere Risiken für das Persönlichkeitsrecht mit sich bringt. Vor allem ist eine Speicherung zeitlich nicht begrenzbar, da die Daten von jedermann abgerufen und anderweitig gespeichert werden können. Dies kann dazu führen, dass Dritte die Daten auch nach Begleichung der Schuld speichern und diese über längere Zeit für sich nutzen können, und zwar für alle möglichen anderen Zwecke und dies weltweit. Darin liegt eine Verletzung

schutzwürdiger Interessen. Die Firma hat daraufhin auf die Veröffentlichung der Schuldner im Internet verzichtet.

12.2 Speicherung von Nutzungsdaten (IP-Adressen) durch einen Telediensteanbieter

Die Aufsichtsbehörde wird immer wieder gefragt, ob ein Telediensteanbieter die IP-Adressen von Besuchern seiner Webseiten speichern darf.

Eine IP-Adresse ist, vereinfacht ausgedrückt, die „Telefonnummer“ des mit dem Internet verbundenen Computers. Diese wird dem Internetnutzer vom Internet-Zugangsdienst-Anbieter in der Regel dynamisch, d.h. nur für die Zeit der Nutzung, zugeteilt und wird datenschutzrechtlich grundsätzlich als ein personenbeziehbares Datum angesehen. Die IP-Adresse eines Besuchers auf einer Webseite ist damit in erster Linie ein Nutzungsdatum. Der Diensteanbieter darf nach § 6 Abs. 4 TDDSG Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus verarbeiten und nutzen, soweit sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind (Abrechnungsdaten). Eine darüber hinausgehende Speicherung von Nutzungsdaten ist nicht zulässig. Sie sind sofort zu löschen.

Das bedeutet, dass eine IP-Adresse grundsätzlich sofort nach dem Ende des Nutzungsvorgangs zu löschen ist. Bei kostenpflichtigen Angeboten kann es erforderlich sein, die IP-Adresse zum Nachweis der Inanspruchnahme des Angebots und damit zur Abrechnung mit dem Nutzer zu speichern. Die Datenspeicherung ist in diesem Fall bis zum Ablauf der Einspruchsfrist gegen die Abrechnung zulässig.

Von einem Telediensteanbieter wurde die Speicherung der IP-Adressen der Besucher seiner Webseite damit begründet, dass er nach den strafrechtlichen Vorschriften zur Auskunft an die Strafverfolgungsbehörden verpflichtet sei. Hierbei übersah der Anbieter, dass ein Unterschied besteht zwischen der Herausgabe bereits gespeicherter Daten und der Speicherung von Daten, die eventuell einem Herausgabeanspruch unterliegen können. Die rechtlichen Möglichkeiten der Strafverfolgungsbehörden verpflichten den Diensteanbieter zur Herausgabe gespeicherter Daten. Sie schaffen nach derzeitiger Rechtslage jedoch keine eigene Grundlage zur Speicherung von Nutzungsdaten über das TDDSG hinaus. Die Aufsichtsbehörde forderte den Anbieter zum Unterlassen der Speicherung der IP-Adressen auf.

12.3 Teledienst nur gegen Registrierung

Einige Beschwerden richteten sich dagegen, dass die volle Nutzung des Teledienstes erst nach einer Registrierung möglich war. Die Betroffenen wurden auf der Internetseite darauf hingewiesen, dass sie damit zugleich in die Weitergabe ihrer Daten an andere Firmen für Zwecke der Beratung, Werbung und Marktforschung einwilligten. Bei einer Firma stand der Hinweis auf die Weitergabe in den Allgemeinen Geschäftsbedingungen, die der Nutzer per Klickbox annehmen musste.

Der Diensteanbieter darf nach § 3 Abs. 4 TDDSG die Erbringung von Telediensten nicht von einer Einwilligung des Nutzers in eine Verarbeitung oder Nutzung seiner Daten für andere Zwecke abhängig machen, wenn dem Nutzer ein anderer Zugang zu diesen Telediensten nicht oder in nicht zumutbarer Weise möglich ist.

In einem Fall war es so, dass die vollumfängliche Nutzung des Dienstes zwar kostenlos war, aber durch die Weitergabe von Daten an Kooperationspartner eine Refinanzierungsmöglichkeit offengehalten werden sollte. Das Unternehmen erklärte sich jedoch von sich aus bereit, die Basisdienste (u.a. einfache Routenplanung) auch ohne Registrierung anzubieten. Nur die vollumfängliche Nutzung sollte erst nach der Registrierung möglich sein. Dabei kann der Nutzer zwischen einer kostenfreien Nutzung und der Weitergabe seiner Daten an Dritte für Werbezwecke oder einer kostenpflichtigen Nutzung ohne Weitergabe seiner Daten an Dritte wählen. Da die angebotenen Services einer vollumfänglichen Nutzung finanziert werden müssen, hat die Aufsichtsbehörde in den beiden Wahlmöglichkeiten keinen Widerspruch zu § 3 Abs. 4 TDDSG gesehen.

In den anderen Fällen haben die Unternehmen entweder ganz auf die Übermittlung an Dritte für Werbung verzichtet oder den Betroffenen die Möglichkeit eingeräumt, der Werbung zu widersprechen.