Datenschutz im nichtöffentlichen Bereich

Dritter Tätigkeitsbericht des Innenministeriums nach § 39 des Landesdatenschutzgesetzes Baden-Württemberg

2005

Inhaltsverzeichnis

Berichtsauftrag

Die Datenschutzaufsicht im Bereich der Wirtschaftsunternehmen und der sonstigen nichtöffentlichen Stellen ist Aufgabe des Innenministeriums. Als Aufsichtsbehörde kontrolliert es die Ausführung des Bundesdatenschutzgesetzes (BDSG) sowie anderer Vorschriften über den Datenschutz. Nach § 39 des Landesdatenschutzgesetzes erstattet das Innenministerium dem Landtag seit 2001 zum 1. Juli jedes zweiten Jahres einen Bericht über die Tätigkeit der Aufsichtsbehörde.

Dies ist der dritte Bericht nach Einführung der gesetzlichen Berichtspflicht. Er baut auf den beiden ersten Tätigkeitsberichten (Landtagsdrucksachen 13/40 und 13/2200) auf und beschränkt sich auf Neuerungen und Entwicklungen, die im Berichtszeitraum (1. Juli 2003 bis 30. Juni 2005) eingetreten sind.

A Entwicklung der Aufgaben und des Datenschutzrechts seit 2003

1 Allgemeines zur Aufsichtstätigkeit

1.1 Eingaben, Anlasskontrollen

Eindeutiger Schwerpunkt der aufsichtsbehördlichen Tätigkeit war im Berichtszeitraum wieder die Bearbeitung von Beschwerden betroffener Bürger. 2003 und 2004 machten 914 Bürger von ihrem Recht Gebrauch, die Datenschutzaufsicht anzurufen. Gegenüber den vorangegangenen beiden Jahren stellt dies eine Steigerung um 37 % dar, die ohne personelle Verstärkung bewältigt werden musste. Jeweils mehr als 100 Eingaben betrafen Auskunfteien, Mediendiensteunternehmen sowie den Einzel-, Groß- und Versandhandel - zumeist wegen der Verarbeitung personenbezogener Daten für Werbezwecke und der Nichterfüllung des Auskunftsanspruchs über die Herkunft der für die Werbesendung verwendeten Adresse. Jeweils mehr als 50 Eingaben betrafen den Adresshandel selbst und die Direktmarketing- und Werbebranche samt Lotterien, die Kreditinstitute, die Banken und Bausparkassen sowie den Arbeitnehmerdatenschutz und jeweils mehr als 20 Eingaben Versicherungsunternehmen, das Gesundheitswesen, Markt- und Meinungsforschungsinstitute, die Videoüberwachung und Inkassounternehmen.

Die meisten Beschwerden konnten im schriftlichen Verfahren mit den betroffenen Unternehmen geklärt werden. Die Aufsichtsbehörde ist inzwischen jedoch verstärkt dazu übergegangen, bei möglicherweise schwerwiegenden Verstößen eines Unternehmens gegen datenschutzrechtliche Vorschriften den Sachverhalt durch eine - unter Umständen auch unangemeldete - Kontrolle vor Ort zu klären (**Anlasskontrollen**).

Es fällt auf, dass sowohl förmliche Beschwerden als auch sonstige Anfragen zunehmend per E-Mail gestellt werden. Leider wird darin der zu beurteilende Sachverhalt oftmals nur sehr unvollständig geschildert, auch fehlen häufig die für eine Überprüfung erforderlichen Angaben und Belege, die zumeist nicht elektronisch vorliegen. Dies macht Rückfragen erforderlich, die die Bearbeitung verzögern.

Zu den am häufigsten festgestellten Mängeln zählten wiederum die Nichterfüllung des Auskunftsanspruchs nach § 34 BDSG (insbesondere über die Herkunft der verwendeten personenbezogenen Daten in Werbeangelegenheiten) sowie der in Werbeschreiben fehlende bzw. unzureichende Hinweis auf die Möglichkeit, Widerspruch gegen die Nutzung der Daten für Werbezwecke einzulegen. Insbesondere bei den

Auskunfteien und Kreditschutzorganisationen kam es zu Personenverwechslungen auf Grund nicht ausreichender Identifizierung und Prüfung der Angaben. Einige Beanstandungen mussten auch wegen ungenauer Zweckbestimmung bei der Erhebung von Daten ausgesprochen werden.

1.2 Anlassunabhängige Kontrollen

Die Aufsichtsbehörde führte auch eine Reihe anlassunabhängiger Kontrollen durch, u.a. bei mehreren Auskunfteien, Internetdiensteanbietern, Adresshändlern, Direktmarketingbetrieben, bei einer Lotterie und in Krankenhäusern.

1.3 Beratung von Bürgern, Unternehmen und betrieblichen Datenschutzbeauftragten

Zusätzlich zu den förmlichen Beschwerden gab es 230 schriftliche und rund 4000 mündliche Anfragen von Bürgern zum Datenschutz im nichtöffentlichen Bereich.

Von der Aufsichtsbehörde beraten lassen sich auch betriebliche Datenschutzbeauftragte und Unternehmen. Einzelne Beispiele dafür finden sich auch in diesem Tätigkeitsbericht. Es fällt auf, dass betriebliche Datenschutzbeauftragte in aller Regel lediglich telefonisch an die Aufsichtsbehörde herantreten, nach unserem Eindruck vor allem deshalb, weil sie die schriftliche Kontaktaufnahme mit uns scheuen. Dies erschwert die Beratung, weil die zu beurteilenden Sachverhalte häufig doch komplexer Natur sind. Es sei deshalb daran erinnert, dass die betrieblichen Datenschutzbeauftragten nach dem BDSG ein Recht, teilweise sogar die Pflicht haben, sich in Zweifelsfällen an die Aufsichtsbehörde zu wenden. Die gesetzliche Regelung räumt ihnen einen breiten Ermessensspielraum ein, wann sie hiervon Gebrauch machen wollen. Die Aufsichtsbehörde misst der Beratung einen hohen Stellenwert bei. Vorbeugender Datenschutz ist der beste Datenschutz. Betriebliche Datenschutzbeauftragte und Unternehmen können daher nur dazu ermuntert werden, die Aufsichtsbehörde vor dem Einsatz neuer Formen der Datenverarbeitung oder bei Fragen zur Auslegung des BDSG um eine Beurteilung zu bitten.

1.4 Beratung eines Ministeriums bei einem Gesetzgebungsvorhaben

Die Aufsichtsbehörde berät das Sozialministerium bei der Neuordnung der Krebsregistrierung in Baden-Württemberg. Näheres dazu findet sich unter C 6.1.

1.5 Mitwirkung bei der Ausbildung betrieblicher Datenschutzbeauftragter

Die Aufsichtsbehörde misst der Arbeit der betrieblichen Datenschutzbeauftragten große Bedeutung bei, sofern diese ihre Aufgabe, auf die Einhaltung des BDSG und anderer Vorschriften über den Datenschutz hinzuwirken, ernst nehmen, und über die erforderliche Fachkunde und Zuverlässigkeit verfügen. Die Ausbildung der betrieblichen Datenschutzbeauftragten ist deshalb sehr wichtig. Das Angebot der Ausbildungsveranstalter ist groß, die Qualität unterschiedlich: neben sehr guten umfassenden Programmen zumeist langjährig etablierter Veranstalter finden sich auch Angebote, die schon deshalb nicht den Anforderungen genügen, weil die angehenden betrieblichen Datenschutzbeauftragten ausschließlich oder ganz überwiegend im technischen Datenschutz ausgebildet werden sollen. Nach Auffassung der Aufsichtsbehörde müssen sie mindestens in gleicher Weise im Datenschutzrecht unterwiesen werden. Um im Rahmen ihrer begrenzten personellen Ressourcen ihren Beitrag zu einer qualifizierten Ausbildung betrieblicher Datenschutzbeauftragter zu leisten, entschloss sich die Aufsichtsbehörde im November 2004, bei einem Ausbilder auf dessen Wunsch hin mitzuarbeiten und diesen auch hinsichtlich der Programmgestaltung zu beraten. Eine Empfehlung der Aufsichtsbehörde für dieses Angebot ist damit selbstverständlich nicht verbunden. Die Aufsichtsbehörde informiert bei diesen Veranstaltungen über ihre praktische Arbeit, aktuelle datenschutzrechtliche Themen sowie über ihre Aufgaben und Befugnisse, beleuchtet das Verhältnis zwischen betrieblichem Datenschutzbeauftragten und Aufsichtsbehörde und gibt Hinweise, die im Umgang mit ihr bei der Durchführung datenschutzrechtlicher Prüfungen oder im Rahmen von Bürgerbeschwerden beachtet werden sollten. Die Mitwirkung der Aufsichtsbehörde stieß auf eine positive Resonanz der Auszubildenden. Die Aufsichtsbehörde ist gerne bereit, auch andere Ausbilder konzeptionell zu beraten.

1.6 Herausgabe von Merkblättern, Hinweisen und Ähnlichem

Mit Hilfe von „Merkblättern“ und anderen im Internet bereitgestellten Informationen versucht die Aufsichtsbehörde, die Kenntnisse

- der Bürger über ihre Datenschutzrechte und
- der nichtöffentlichen Stellen über die von ihnen zu beachtenden datenschutzrechtlichen Vorschriften zu verbessern. Unter anderem wurde das Merkblatt „Datenschutz im Verein“ überarbeitet und um einige neue Fragestellungen, z.B. zu Veröffentlichungen im Internet, ergänzt. Es findet sich unter www.im.baden-wuerttemberg.de Rubrik Datenschutz, Weitere Infos, Infomaterial.

Im Behördenwegweiser von service-bw (www.service-bw.de) wurden die Zuständigkeiten der verschiedenen Datenschutzkontrollorgane dargestellt, in einzelnen Verfahrensbeschreibungen (beispielsweise zur Anrufung der Datenschutzkontrolle, zum betrieblichen Datenschutzbeauftragten und zur Meldung zum Datenschutzregister) werden weitere wichtige Informationen für Bürger und Unternehmen angeboten.

Hinweise (so genannte HIM´s) zur Beurteilung wichtiger, meist neuer datenschutzrechtlicher Fragestellungen gibt die Aufsichtsbehörde inzwischen seit mehr als 25 Jahren heraus. Adressaten sind vor allem die nichtöffentlichen Stellen als verantwortliche Stellen im Sinne des BDSG und die betrieblichen Datenschutzbeauftragten. Im Berichtszeitraum hat die Aufsichtsbehörde den HIM Nr. 41 veröffentlicht, der sich mit den Informationspflichten nach § 4 Abs. 3 BDSG, dem Einsatz biometrischer Verfahren im Handel und in der Gastronomie und der Verarbeitung von IP-Adressen durch Inhaltsanbieter im Internet befasst. Die Hinweise sind unter www.im.baden-wuerttemberg.de Rubrik Datenschutz/weitere Infos/Infomaterial im Internet abrufbar.
Die Ausführungen zu den Informationspflichten nach § 4 Abs. 3 BDSG haben in Fachkreisen ein lebhaftes Echo ausgelöst. Auf sie wird daher unter B 1 näher eingegangen.

1.7 Datenschutzregister

In dem von der Aufsichtsbehörde nach § 38 Abs. 2 BDSG zu führenden Datenschutzregister haben sich nur geringfügige Änderungen ergeben. Es sind insgesamt 71 Stellen mit 76 automatisierten Verfahren gemeldet. 46 dieser Verfahren dienen dem Zweck der Übermittlung personenbezogener Daten (Auskunfteien und Adresshändler) und 30 dem Zweck der anonymisierten Datenübermittlung (Markt- und Meinungsforschungsinstitute). Es ist allerdings davon auszugehen, dass nicht alle meldepflichtigen Verfahren auch tatsächlich zum Datenschutzregister gemeldet werden. Immer wieder wird die Aufsichtsbehörde auf meldepflichtige Verfahren aufmerksam und weist die betreffenden Firmen, die sich auf Unkenntnis der Vorschriften berufen, auf die bestehende Meldepflicht hin.

Für Meldungen zum Datenschutzregister wurden ein Merkblatt und entsprechende Formulare entwickelt. Die Unterlagen sind im Internet unter www.im.baden-wuerttemberg.de Rubrik Datenschutz/Organisation/Datenschutzregister und in service-bw (www.service-bwl.de) unter dem Stichwort „Datenschutz“ abrufbar.

1.8 Ordnungswidrigkeitenverfahren

Nach dem BDSG sind eine Reihe von Datenschutzverstößen bußgeldbewehrt. Die Aufsichtsbehörde macht von dieser Möglichkeit jedoch nur selten Gebrauch. Der Aufsichtsbehörde ist es wichtiger sicherzustellen, dass sich die ihrer Aufsicht unterliegenden Stellen künftig datenschutzgerecht verhalten als dass in der Vergangenheit liegende Datenschutzverstöße geahndet werden. In drei Fällen verhängte die Aufsichtsbehörde jedoch ein Bußgeld, weil die betreffenden nichtöffentlichen Stellen sich geweigert hatten, ihr die geforderten Auskünfte zu erteilen.

2 Rechtsentwicklung

2.1 Bundesdatenschutzgesetz

Das BDSG wurde im Berichtszeitraum nicht geändert. Die vom Deutschen Bundestag im Zusammenhang mit der Verabschiedung des Änderungsgesetzes 2001 ausgesprochene Erwartung, das BDSG werde bald umfassend modernisiert, hat sich nicht erfüllt. Das ist bedauerlich, da dieses Gesetz nach Meinung aller Datenschutzexperten dringend reformbedürftig ist. Der Deutsche Bundestag hat die Bundesregierung inzwischen in einer einstimmig gefassten Entschließung aufgefordert, die entsprechenden Arbeiten zügig fortzusetzen.

2.2 Änderung des Telekommunikationsrechts

Ende Juni 2004 ist das neue Telekommunikationsgesetz (TKG) in Kraft getreten. Neben Änderungen, die weitgehend die Telekom betreffen, wurden die Befugnisse der Sicherheitsbehörden erweitert. Das Telekommunikationsgesetz enthält jedoch keine Mindestspeicherfrist für Verkehrsdaten. Die Telekommunikations-Datenschutzverordnung wurde als Teil 7 in das TKG eingearbeitet. Die Datenschutzaufsicht über die Telekommunikationsdiensteanbieter verbleibt beim Bundesbeauftragten für den Datenschutz.

Eine wesentliche Rechtsänderung stellt die Zulassung der Inversauskunft (Rückwärtssuche) dar, bei der über die Rufnummer Auskunft zur Adresse des Anschlussinhabers erteilt wird. Diese Auskunft war nach früherem Recht unzulässig und damit datenschutzwidrig. Das Innenministerium hatte aus diesem Grund in seinem Hinweis Nr. 34 von 1996 das Vorhalten und Nutzen von Telefonauskunfts-CD mit Inverssuche für unzulässig erklärt.

Nach der Änderung des TKG informierte die Telekom - wie gesetzlich vorgeschrieben - die Kunden darüber, dass sie gegen die Auskunftserteilung über ihre Adresse Widerspruch einlegen können.

2.3 Änderung des Wettbewerbsrechts

Datenschutzrechtlich relevant ist die Änderung des Gesetzes gegen den unlauteren Wettbewerb (UWG) vom Juli 2004, da wettbewerbswidriger Umgang mit personenbezogenen Daten zugleich einen Verstoß gegen den Datenschutz darstellt.

Auf Grund der Änderung des § 7 UWG ist die unverlangte Telefon-, Telefax- und E-Mail-Werbung sowie jede Werbung an Empfänger, bei denen erkennbar ist, dass sie keine Werbung wünschen, eine unzumutbare Belästigung. **Ausnahmen** von dieser gesetzlichen Vermutung gibt es nur bei elektronischer Post, wenn der Versender der Werbung die Adresse des Kunden im Zusammenhang mit dem Verkauf von Waren und Dienstleistungen erhalten hat und er die Adresse zur Versendung von Direktwerbung für **eigene ähnliche** Waren oder Dienstleistungen verwendet. Der Kunde darf dieser Verwendung nicht widersprochen haben und er muss bei der Erhebung der E-Mail-Adresse auf sein jederzeitiges Widerspruchsrecht hingewiesen worden sein.

B Allgemeine Fragen des Bundesdatenschutzgesetzes (BDSG)

1 Unterrichtungspflichten bei der Datenerhebung (§ 4 Abs. 3 BDSG)

Die Aufsichtsbehörde hat sich in ihrem - vorwiegend an die betrieblichen Datenschutzbeauftragten, aber auch alle anderen Interessierten gerichteten - Hinweis Nr. 41 unter anderem mit den bisher wenig beachteten Unterrichtungspflichten bei der Datenerhebung befasst.

Das im Jahre 2001 auf Grund der EG-Datenschutzrichtlinie novellierte BDSG hat den Grundsatz der Direkterhebung der Daten beim Betroffenen besonders betont und sieht hierzu bestimmte Unterrichtungs-, Hinweis- und Aufklärungspflichten bei der Datenerhebung vor. Der Betroffene soll dadurch in die Lage versetzt werden, darüber zu entscheiden, ob er die Daten gegenüber der erhebenden Stelle bekannt geben will oder nicht. Diese Regelungen gelten für öffentliche wie für nichtöffentliche Stellen gleichermaßen. Von besonderer Bedeutung für den nichtöffentlichen Bereich ist § 4 Abs. 3 Satz 1 BDSG. Danach ist der Betroffene bei Erhebung der Daten von der verantwortlichen Stelle über die Identität der verantwortlichen Stelle, die Zweck-

bestimmungen der Erhebung, Verarbeitung oder Nutzung und die Kategorien von Empfängern der Daten zu unterrichten, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat. Über die Empfänger ist der Betroffene aber nur zu unterrichten, wenn er nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese Empfänger rechnen muss.

Hinsichtlich der Identität der verantwortlichen Stelle sind der Name und die Anschrift anzugeben. Der Hinweis auf den Zweck der Erhebung soll den Betroffenen darüber unterrichten, wozu die Daten benötigt werden, soweit die Zweckbestimmung nicht offensichtlich ist. Es sind dabei sämtliche Zwecke anzugeben. Deshalb ist, wenn die im Rahmen eines Vertragsverhältnisses mit dem Betroffenen verarbeiteten Daten auch für Werbezwecke verwendet werden sollen, auch dies anzugeben. Offenzulegen sind auch die Kategorien von Empfängern der Daten, zu denen im Einzelfall auch Stellen gehören können, die die Daten im Auftrag verarbeiten sollen.

Die Unterrichtungspflicht entfällt, wenn die betroffene Person bereits auf andere Weise Kenntnis von der Information erlangt hat. Die verantwortliche Stelle muss dies, wenn sie sich hierauf berufen will, allerdings nachweisen können.

Nur hinsichtlich der Empfänger der Daten genügt es, dass der Betroffene nach den Umständen des Einzelfalles hiermit rechnen musste. Dies ist jedoch nicht bereits dann der Fall, wenn die Datenübermittlung (beispielsweise eine Bonitätsanfrage bei einer Auskunftei) oder sonstige Datenweitergabe „branchenüblich“ ist; erforderlich ist auch, dass dies den Betroffenen bekannt ist. Es empfiehlt sich daher, den Betroffenen im Zweifelsfall zu unterrichten.

Zu der Frage, welche Rechtsfolgen die Nichtbeachtung der Unterrichtungspflicht nach sich zieht, enthält das BDSG keine spezielle Regelung, auch keinen Bußgeldtatbestand, der einen solchen Verstoß ausdrücklich sanktionieren würde. Zu berücksichtigen ist jedoch, dass die Informationspflicht in § 4 BDSG, der zentralen Vorschrift über die Zulässigkeit der Datenverarbeitung, verankert worden ist. Schutzzweck der Regelung ist, wie bereits eingangs ausgeführt, dem Betroffenen die Entscheidung zu ermöglichen, ob er die Daten angeben will oder nicht. Ein Verstoß gegen die Unterrichtungspflichten nach § 4 Abs. 3 Satz 1 BDSG wirkt sich deshalb in denjenigen Fällen auf die Zulässigkeit der Datenverarbeitung, aus, in denen durch die Nichtbeachtung der Informationspflichten der Grundsatz von Treu und Glauben verletzt wird. Ein Verstoß gegen Treu und Glauben ist bei der Prüfung der Zulässigkeit der Datenverarbeitung (§§ 28 und 29 BDSG) zu berücksichtigen. Eine unzulässige Datenerhebung hat dabei zur Folge, dass die Daten nicht weiterverwendet (verar-

beitet oder genutzt) werden dürfen und der Betroffene einen Anspruch auf Löschung der Daten hat. In diesem Fall liegt auch eine Ordnungswidrigkeit nach § 43 Abs. 2 Nr. 1 BDSG vor. Ob ein Verstoß gegen die Unterrichtungspflicht zur Unzulässigkeit der Datenerhebung führt, ist daher für jeden Einzelfall gesondert zu prüfen.

Beispielhaft sind folgende Fälle zu nennen:

- Beabsichtigt ein Unternehmen, das personenbezogene Daten des Betroffenen im Rahmen eines Kaufvertrags erhoben hat, diese auch zu Werbezwecken anderen Unternehmen zu übermitteln oder für diesen Zweck zu nutzen, muss es den Betroffenen nach § 4 Abs. 3 Satz 1 Nr. 2 BDSG auch auf diese Zweckbestimmung hinweisen. Es genügt nicht, dass er bei der werblichen Ansprache auf die Möglichkeit des Werbewiderspruchs hingewiesen wird. Mit einer solchen Datenübermittlung oder -nutzung muss der Betroffene zum Zeitpunkt des Abschlusses des Vertrages in der Regel nicht rechnen. Unterbleibt diese Unterrichtung, wird regelmäßig von der Unzulässigkeit der Datenverarbeitung auszugehen sein.

- Ein Unternehmen führt zur Gewinnung von Informationen für Zwecke der gezielten Werbung eine schriftliche oder mündliche Umfrage durch. Wird in diesem Fall nur von „Markt- und Meinungsforschung“ oder von der „Zusendung von Informationen“ gesprochen, ist dies keine zutreffende und klare Information über den Verwendungszweck, wenn in Wirklichkeit die Werbung für Produkte und Dienstleistungen einzelner Unternehmen beabsichtigt wird. Anzugeben ist in einem solchen Fall auch, an welche Stellen die Daten übermittelt werden sollen. Hierfür genügt aber die Nennung der Branchen, wie z.B. Nahrungsmittelhersteller, Autohändler, Versicherungsunternehmen oder Verlage.

Es zeigt sich, dass ein Verstoß gegen die Unterrichtungspflichten ein erhebliches rechtliches Risiko darstellt und nur deren konsequente Beachtung die Gewähr dafür bietet, dass die Erhebung und weitere Datenverarbeitung rechtmäßig ist.

Diese im Hinweis dargestellte Auffassung der Aufsichtsbehörde hat, wie bereits erwähnt, eine lebhafte Diskussion ausgelöst. Thematisiert wird dabei insbesondere die Frage, welche Rechtsfolgen die Nichtbeachtung der Unterrichtungspflicht nach sich zieht. Die Auffassung, dass bei einer im konkreten Einzelfall gegebenen Verletzung des Grundsatzes von Treu und Glauben von einer unzulässigen Datenerhebung auszugehen ist, wird jedoch geteilt.

2 Der betriebliche Datenschutzbeauftragte

2.1 Mindestanzahl an Arbeitnehmern als Voraussetzung für die Bestellung

Nach § 4f Abs. 1 BDSG ist ein Arbeitgeber, der mindestens fünf Arbeitnehmer mit der automatisierten oder mindestens zwanzig Personen auf andere Weise mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt, verpflichtet, einen betrieblichen Datenschutzbeauftragten zu bestellen. Damit wollte man Kleinstbetriebe von der Pflicht, einen betrieblichen Datenschutzbeauftragten zu bestellen, ausnehmen. In den letzten Jahren hat die EDV auch in Kleinunternehmen zunehmend Eingang gefunden. Diese steuern damit nicht nur den Produktionsprozess, sondern wickeln teilweise auch die Personal- und Kundenbetreuung und den Zahlungsverkehr mit Hilfe von EC- und Kreditkarten darüber ab. Dies hat dazu geführt, dass immer mehr kleinere Unternehmen einen betrieblichen Datenschutzbeauftragten bestellen müssen. Um dem Gesetz formal Genüge zu tun, wird dann häufig irgendein Mitarbeiter, der weder über die erforderlichen Datenschutzkenntnisse verfügt noch bereit und in der Lage ist, notfalls auch Konflikte mit dem Firmenchef auf sich zu nehmen und durchzustehen, zum betrieblichen Datenschutzbeauftragten bestellt. Dies ist nicht im Sinne des Datenschutzes. Es macht deutlich, dass die derzeit geltende Freistellungsgrenze nicht mehr zeitgemäß ist. Es soll deshalb die Gesetzesinitiative eines anderen Bundeslandes zur Änderung des BDSG unterstützt werden, die die maßvolle Anhebung der Arbeitnehmerzahl unter Beachtung der EG-Datenschutzrichtlinie vorsieht. Keinesfalls soll damit der Datenschutz zurückgefahren oder dem betrieblichen Datenschutzbeauftragten generell das Misstrauen ausgesprochen werden. Vielmehr soll die Eigenverantwortung der Unternehmensleitungen für die Einhaltung datenschutzrechtlicher Vorschriften betont werden.

Die Pflicht, unabhängig von der Zahl der Arbeitnehmer einen betrieblichen Datenschutzbeauftragten zu bestellen, wenn von dem Einsatz der automatisierten Verarbeitung besondere Risiken für die Rechte und Freiheiten der Betroffenen ausgehen, bleibt hiervon unberührt.

2.2 Bestellung eines externen Datenschutzbeauftragten und Geheimhaltungspflichten

§ 4f Abs. 2 Satz 2 BDSG erlaubt es, auch einer Person außerhalb der verantwortlichen Stelle die Aufgaben des betrieblichen Datenschutzbeauftragten zu übertragen (sog. externer Datenschutzbeauftragter). In der Praxis stellt sich die Frage, ob ein externer Datenschutzbeauftragter dieselben Rechte hat wie ein Beauftragter für den

Datenschutz, der in der verantwortlichen Stelle tätig ist oder ob sich der externe Datenschutzbeauftragte von der verantwortlichen Stelle oder den dort tätigen Personen die Geheimhaltungspflichten nach § 1 Abs. 3 Satz 2 BDSG, beispielsweise die ärztliche Schweigepflicht, entgegenhalten lassen muss.

Eine engere Auslegung hätte zur Folge, dass der externe Datenschutzbeauftragte bei der Wahrnehmung seiner Aufgaben Einschränkungen unterläge, beispielsweise bei der Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme, unter Umständen auch bei Beschwerden von Betroffenen. Um zu vermeiden, dass diese gesetzlich festgelegten Aufgaben des betrieblichen Datenschutzbeauftragten nicht erfüllt werden, müsste dann innerhalb der verantwortlichen Stelle eine weitere Person zur Unterstützung des externen Datenschutzbeauftragten bestellt werden.

Man kann aber auch die Auffassung vertreten, dass gegenüber externen Datenschutzbeauftragten nicht unbefugt offenbart wird, weil der Gesetzgeber die Verpflichtung zur Bestellung von betrieblichen Beauftragten für den Datenschutz unabhängig davon vorgesehen hat, ob den verantwortlichen Personen in der nichtöffentlichen Stelle Geheimhaltungspflichten obliegen oder nicht. Der Gesetzgeber selbst habe bestimmt, dass die Funktion des Datenschutzbeauftragten ohne Rücksicht auf die Geheimhaltungspflicht sowohl durch eine interne als auch externe Person wahrgenommen werden kann.

Um diese Diskussion ein für alle Mal zu beenden und es der verantwortlichen Stelle zu ermöglichen, sich für einen internen oder einen externen Datenschutzbeauftragten zu entscheiden, hat das Innenministerium vorgeschlagen, in die oben unter Nr. 2.1 erwähnte Initiative zur Änderung des BDSG eine eindeutige Regelung aufzunehmen.

2.3 Bestellung von Datenschutzbeauftragten in Rechtsanwaltskanzleien

Die Bundesrechtsanwaltskammer hat in einer Stellungnahme die Auffassung vertreten, Rechtsanwälte seien hinsichtlich mandatsbezogener Daten nicht verpflichtet, einen betrieblichen Datenschutzbeauftragten zu bestellen. Die entsprechenden Bestimmungen des BDSG seien gegenüber der Bundesrechtsanwaltsordnung (BRAO), welche einen betrieblichen Datenschutzbeauftragten nicht vorsieht, subsidiär. Nur dies entspreche dem nach der BRAO durch Unabhängigkeit, Interessenvertretung und Verschwiegenheit geprägten Berufsbild des Anwalts. Die Bestellung eines externen Datenschutzbeauftragten stehe darüber hinaus mit dem Berufsgeheimnis des

Anwalts nicht in Einklang. Bei der Verarbeitung von Personaldaten der Anwaltskanzlei sei hingegen das BDSG zu beachten mit der Folge, dass ein auf diesen Datenverarbeitungsbereich beschränkter Datenschutzbeauftragter zu bestellen sei, falls die gesetzlichen Voraussetzungen hierfür vorliegen.

Der Düsseldorfer Kreis, das Gremium der Obersten Datenschutzaufsichtsbehörden der Länder, ist demgegenüber der Auffassung, dass das BDSG auch auf mandatsbezogene Daten Anwendung findet. Lediglich soweit bereichsspezifische Datenschutzvorschriften bestünden, träten die entsprechenden Vorschriften des BDSG zurück. Die punktuellen Regelungen in der BRAO (Schweigepflicht, Handakten, allgemeine Kontrollbefugnisse der Kammern wegen Berufsverstößen) bewirkten nicht, dass das BDSG bei der mandatsbezogenen Verarbeitung nicht anwendbar sei.

Auch die Wahrung des strafrechtlich geschützten Berufsgeheimnisses stehe der Geltung des BDSG nicht entgegen. § 1 Abs. 3 Satz 2 BDSG bestimme lediglich, dass die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, unberührt bleibt. Sie sind deshalb neben den Vorschriften des BDSG zu beachten.

Der Bundesrechtsanwaltskammer wurde die Auffassung des Düsseldorfer Kreises mitgeteilt. Falls die mit der unter Nr. 2.1 dargestellten Gesetzesinitiative angestrebte Änderung des BDSG Gesetz würde, würde sich das Problem zumindest für die Mehrzahl der Rechtsanwaltskanzleien für die Zukunft erledigen.

2.4 Befristete Bestellung eines betrieblichen Datenschutzbeauftragten

Der Aufsichtsbehörde wurde die Frage gestellt, ob die Bestellung interner und externer Datenschutzbeauftragter befristet werden kann.

Sie vertritt hierzu folgende Auffassung: Das BDSG macht zur Dauer der Bestellung des Datenschutzbeauftragten keine Aussagen. Aus der Tatsache, dass das BDSG für den Fall, dass sich ein Datenschutzbeauftragter als ungeeignet erweist, den Widerruf der Bestellung wegen Vorliegens eines „wichtigen Grundes“ zulässt, folgt jedoch, dass sich der Gesetzgeber eine kontinuierliche Aufgabenwahrnehmung durch den betrieblichen Datenschutzbeauftragten vorgestellt hat. Dies ist, insbesondere bei externen Datenschutzbeauftragten, auch erforderlich, damit er die notwendige Erfahrung sammeln und sich Kenntnisse der betrieblichen Abläufe aneignen kann, und um sicherzustellen, dass er seine gesetzlichen Aufgaben in angemessener Weise wahr-

nimmt, seine Befugnisse voll ausschöpft und nicht mit Rücksicht auf eine Vertragsverlängerung von gebotenen Maßnahmen Abstand nimmt.

Ob eine Befristung generell ausscheidet, wie teilweise vertreten wird, kann dahingestellt bleiben. Den dargelegten Gesichtspunkten wird nach Auffassung der Aufsichtsbehörde jedenfalls nur dann Rechnung getragen, wenn ein betrieblicher Datenschutzbeauftragter für mindestens fünf Jahre bestellt wird. Für einen kürzeren Zeitraum ist eine Bestellung nur zulässig, wenn es dafür zwingende Gründe gibt.

2.5 Umfang der Tätigkeit eines betrieblichen Datenschutzbeauftragten

An die Aufsichtsbehörde wurde die Frage herangetragen, wie viel Zeit einem Datenschutzbeauftragten für die Erledigung seiner Aufgaben zugestanden werden muss.

Wir haben hierzu folgende Auffassung vertreten: Nach § 4f Abs. 5 BDSG haben nichtöffentliche Stellen den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. Im Rahmen dieser Unterstützungspflicht durch die Unternehmensleitung muss dem Datenschutzbeauftragten ausreichend Zeit für seine Tätigkeit im Bereich des Datenschutzes eingeräumt werden. Konkreter wird das BDSG nicht.

Das Arbeitsgericht Offenbach hat 1992 entschieden, dass für die Ausübung des Amts des betrieblichen Datenschutzbeauftragten in der Niederlassung eines Automobilherstellers mit weniger als 300 Beschäftigten weniger als zwanzig Prozent der Gesamttätigkeit genügen. Die Gesellschaft für Datenschutz und Datensicherung e.V. (GDD) hat 1996 im Rahmen einer Umfrage bei renommierten Firmen zur Datenschutzpraxis und zur Stellung des Datenschutzbeauftragten herausgefunden, dass in der Industrie bei einem Mitarbeiterbestand zwischen 1000 und 5000 Mitarbeitern ca. 74 Arbeitstage für die Erledigung der Aufgaben des betrieblichen Datenschutzbeauftragten angesetzt werden. Notwendig wären jedoch ca. 110 Arbeitstage.

Im Grunde genommen helfen solche Zahlenangaben jedoch nicht weiter. Weder die Anzahl der Beschäftigten noch die Anzahl der verwendeten Computer eignen sich dazu, Prozenttabellen aufzustellen, denen dann scheinbar exakt zu entnehmen ist, welchen Anteil der Gesamttätigkeit die Aufgaben des Datenschutzbeauftragten ausmachen. Entscheidend ist letztlich, wie viel Zeit ein Datenschutzbeauftragter für die angemessene Wahrnehmung der im BDSG im Einzelnen aufgezählten Aufgaben in

seinem Unternehmen benötigt. Dabei spielen Art, Umfang und Sensibilität der verwendeten personenbezogenen Daten, Zahl, Beschaffenheit, Neu- und Verschiedenartigkeit der eingesetzten Datenverarbeitungsverfahren, die mit der Verarbeitung konkret verfolgten Zwecke und die im Unternehmen anfallenden datenschutzrechtlichen und sicherheitsmäßigen Fragen eine Rolle. Immer wieder festgestellt wird von der Aufsichtsbehörde, dass für die Schulung der Mitarbeiter in Fragen des Datenschutzes zu wenig Zeit aufgewendet wird. Diese kann sich nicht in einer formalen Verpflichtung der Mitarbeiter auf das Datengeheimnis und einer wörtlichen Wiedergabe wichtiger Begriffe des BDSG erschöpfen. Ein „Vertrautmachen“ der Mitarbeiter mit den Vorschriften des BDSG sowie anderer Vorschriften über den Datenschutz - letztere bleiben meist völlig außer Betracht - und mit den jeweiligen besonderen Erfordernissen des Datenschutzes in einem Unternehmen, wie es § 4g Abs. 1 Satz 3 BDSG verlangt, ist dies nicht.

C Einzelne Tätigkeitsbereiche

1 Auskunfteien

1.1 Scoringverfahren

Die Aufsichtsbehörde prüft derzeit ein Scoringverfahren, das von einem Unternehmen mit Sitz in Baden-Württemberg betrieben wird, unter datenschutzrechtlichen Gesichtspunkten. Mit diesem Verfahren wird anhand mathematisch-statistischer Methoden eine Prognose über das zukünftige Zahlungsverhalten von Personen (-gruppen) erstellt und in einer Punktzahl (Score) ausgedrückt. Diese Scorewerte werden von Unternehmen aus den verschiedensten Bereichen (z. B. Versandhandel, Telekommunikation und Banken) als Entscheidungshilfe genutzt, wenn sie über keine Informationen zum Zahlungsverhalten eines Kunden verfügen.

Da der Scorewert einer konkreten Person (dem Kunden) zugeordnet wird, handelt es sich hierbei um ein personenbezogenes Datum, dessen Erhebung, Verarbeitung und Nutzung nach den Vorschriften des BDSG zu beurteilen ist. Dieses enthält jedoch keine ausdrückliche Regelung zur Frage, welche Merkmale bei der Bildung von Scorewerten berücksichtigt werden dürfen, wie das Verfahren dem Betroffenen gegenüber transparent gemacht werden kann und wie dieses insgesamt ausgestaltet werden muss, um datenschutzrechtlichen Anforderungen zu genügen. Beurteilungsmaßstab sind daher im wesentlichen die allgemeinen Zulässigkeitstatbestände des BDSG. Bei den Aufsichtsbehörden der Länder bestehen unterschiedliche Auffassungen darüber, wie danach Scoringverfahren zu beurteilen sind. Eine Arbeitsgruppe

des Düsseldorfer Kreises, die sich mit dem Thema Credit Scoring befasst und dabei auch die Anforderungen der Eigenkapitalübereinkunft Basel II berücksichtigt, die ab dem 31. Dezember 2006 stufenweise in Kraft tritt, bemüht sich derzeit darum, vorhandene Lösungsansätze zusammenzuführen. Deswegen und weil die datenschutzrechtliche Prüfung im vorliegenden Fall noch nicht abgeschlossen ist, beschränken wir uns im Folgenden auf einen Problemaufriss.

Als erstes stellt sich die Frage, welche einzelnen Merkmale in die Berechnung des Scorewertes einfließen dürfen: nur solche, die eine unmittelbare Aussagekraft zu Zahlungsverhalten, Einkommens- und Vermögensverhältnissen aufweisen wie etwa das monatliche Einkommen oder das Vorliegen von Einträgen im Schuldnerverzeichnis? Oder dürfen auch Daten einbezogen werden, die zwar keinen unmittelbaren Bonitätsbezug aufweisen, bei denen aber mittels eines wissenschaftlichen Standards entsprechenden statistischen Verfahrens ein gesicherter Zusammenhang zur Kreditwürdigkeit nachgewiesen wurde, wie etwa beim Alter oder beim Wohnumfeld des Betroffenen? Und wie ist es, wenn diese Daten (z.B. das Alter) geschätzt oder aus öffentlich zugänglichen Quellen hergeleitet werden (z.B. Herleitung des Familienstandes aus dem Telefonbucheintrag)? Geklärt werden muss auch, ob diese Fragen unterschiedlich zu beantworten sind, je nachdem, wozu der Scorewert verwendet wird (also etwa für die Frage der Kreditvergabe durch eine Bank anders als für die Festlegung der Zahlungsart im Versandhandel?).

Ein datenschutzrechtlich bedeutsamer Aspekt ist auch die Transparenz des Verfahrens. Der Betroffene muss bereits bei der Datenerhebung darüber informiert werden, dass die von ihm zur Verfügung gestellten Daten auch zur Bildung und anschließenden Übermittlung eines Scorewertes verwendet werden. So kann er entscheiden, ob er damit einverstanden ist oder von einem Vertragsschluss mit dem jeweiligen Unternehmen absieht bzw. sich für eine andere Art der Bezahlung (z.B. per Nachnahme) entscheidet.

Dem Betroffenen muss auch die Möglichkeit eingeräumt werden, der Bildung und Übermittlung von Scorewerten zu widersprechen bzw. seine Daten für diesen Zweck sperren zu lassen. Ihm ist Auskunft über den bei der verantwortlichen Stelle gespeicherten Scorewert sowie die Unternehmen, an die er weitergeben wurde, zu erteilen.

Ein Betroffener, dem die Gewährung einer Leistung (etwa bei der Bestellung bei einem Versandhändler) mit der Begründung versagt wird, „sein Scorewert sei zu schlecht“, muss jedenfalls die Möglichkeit haben, diese negative Prognose zu widerlegen, indem er seine persönliche Zahlungsfähigkeit und -willigkeit mittels entspre-

chender Belege nachweisen kann. Hierzu bedarf es aber zumindest der Information, welche Merkmale in seinem Fall zu der schlechten Bewertung geführt haben, damit er Korrekturansprüche geltend machen kann. Die zumindest wünschenswerte, zur Durchsetzung der Rechte des Betroffenen unter Umständen sogar gebotene Erteilung weitergehender Informationen etwa über die genaue Zusammensetzung des Scorewertes, die Gewichtung der einzelnen Merkmale und die eingesetzte Software steht möglicherweise im Widerstreit zu den Interessen des Scorewerte bildenden Unternehmens, das seine Geschäftsgeheimnisse selbstverständlich gewahrt wissen will. Dies macht es nicht gerade einfach, bei der Scorewertbildung den schutzwürdigen Belangen der Betroffenen ausreichend Rechnung zu tragen. Dass Grundlage für die Scorewertberechnung nur ein mathematisch-statistisches Verfahren sein kann, das anerkannt ist und aktuellen wissenschaftlichen Standards genügt, wird dabei als selbstverständlich vorausgesetzt.

Insgesamt erscheint es zweifelhaft, ob aus den sehr allgemein gehaltenen Vorschriften des BDSG den Interessen der Betroffenen gerecht werdende und von den Unternehmen akzeptierte Anforderungen an Scoringverfahren hergeleitet werden können. Möglicherweise wird hier der Bundesgesetzgeber tätig werden müssen.

1.2 Auskunftserteilung an den Betroffenen über die Zusammensetzung des Bonitätsindexes

Ein dem Scoring ähnliches Verfahren wird von Handels- und Wirtschaftsauskunfteien bei der Berechnung des sogenannten Bonitätsindexes angewandt. Dieser ist Bestandteil der jeweils erteilten Wirtschaftsauskunft und soll die schnelle und direkte Einschätzung der Bonität und des Ausfallrisikos eines Kunden ermöglichen. Er wird grundsätzlich nur für Unternehmen und nicht für Privatpersonen errechnet. In den Fällen, in denen der Bonitätsindex für Einzelkaufleute oder Gewerbetreibende ermittelt wird, handelt es sich um ein personenbezogenes Datum, dessen Erhebung, Verarbeitung und Nutzung den Regelungen des BDSG unterliegt. Der Wert setzt sich aus mehreren bonitätsrelevanten Informationen zusammen, wie etwa Rechtsform, Umsatz, Zahlungsweise, Unternehmensentwicklung oder Auftragslage. Diese Informationen werden einzeln bewertet, je nach ihrer Bedeutung unterschiedlich gewichtet und mittels einer mathematischen Formel in einer Zahl von beispielsweise 100 (sehr gute Bonität) bis 600 (Vorliegen harter Negativmerkmale) zusammengefasst. Bei jeder neuen Anfrage zu einem Datensatz wird der Bonitätsindex aktuell errechnet, da sich die Faktoren, die bei seiner Ermittlung zugrunde gelegt werden, ständig verändern können.

Begehrt der Betroffene, zu dessen Person ein solcher Bonitätsindex gebildet und an einen Vertragspartner der Auskunftei übermittelt wurde, Auskunft über die genaue Berechnung seines Wertes, etwa weil ihm der begehrte Kredit nicht eingeräumt wurde, verweigern die Auskunfteien diese in der Regel. Sie berufen sich dabei auf ihr Betriebs- bzw. Geschäftsgeheimnis, das eine Offenlegung der von ihnen angewandten Berechnungsmethode nicht zulasse. Dem Betroffenen wird lediglich eine allgemeine und nicht auf seinen Fall bezogene Informationsbroschüre zur Verfügung gestellt. Anhand dieser Unterlagen ist es für den Betroffenen jedoch nicht möglich, die Berechung des Bonitätsindexes in seinem Fall nachzuvollziehen.

So erging es auch dem Inhaber eines kleinen Gewerbebetriebs, der sich an die Aufsichtsbehörde gewandt hat. Er bat uns um Hilfe bei der Klärung, wie der zu seiner Person gebildete Bonitätsindex ermittelt wurde. Der ihm ausgehändigten Broschüre konnte er lediglich die beispielhafte Berechnung eines Bonitätsindexes mit den entsprechenden Risikomerkmalen, deren Einteilung in die Klassifikationsstufen und Gewichtung untereinander entnehmen. Da die Wirtschaftsauskunft zu dem Beschwerdeführer nicht zu allen in der Broschüre genannten Risikomerkmalen Angaben enthielt, wollte er wissen, welche Risikomerkmale in seinem Falle herangezogen und wie diese im Einzelnen bewertet und gewichtet wurden. Die Auskunftei hatte dazu lediglich dargelegt, dass nur die in der Wirtschaftsauskunft enthaltenen Angaben zur Berechnung des Bonitätsindexes herangezogen worden seien.

Nach Ansicht der Aufsichtsbehörde genügt es nicht, wenn einem Betroffenen auf die Anfrage nach der Ermittlung seines Bonitätsindexes lediglich eine allgemeine Erläuterung gegeben wird. Wir halten es in diesen Fällen für angebracht, dass dem Betroffenen zumindest die Risikomerkmale und die dazugehörigen Informationen, die in seinem Fall zur Bildung des Bonitätsindexes herangezogen wurden, mitgeteilt werden. Wünschenswert wäre es, wenn der Betroffene die Möglichkeit hätte, die Berechnung des zu seiner Person gebildeten Bonitätsindexes nachzuvollziehen, um so gegebenenfalls Korrekturansprüche - etwa, wenn unzutreffende Daten in die Berechnung eingeflossen sind - geltend zu machen. Dies jedenfalls dann, wenn das Ergebnis der Berechung für den Betroffenen negativ ausfällt. Ob bzw. in welchen Fällen der von den Auskunfteien gegen ein solches Auskunftsrecht vorgebrachte Einwand des entgegenstehenden Geschäftsgeheimnisses tatsächlich berechtigt ist, ist Gegenstand der derzeit von den Datenschutzaufsichtsbehörden mit den Auskunfteien geführten Diskussion. Es wäre wünschenswert, wenn hier für die Betroffenen eine Verbesserung im dargestellten Umfang erreicht werden könnte. Im konkreten Beschwerdefall konnte dem Betroffenen jedenfalls weitergeholfen werden.

1.3 Auskunftserteilung über Herkunft und Empfänger von Daten

Zu Problemen kommt es immer wieder, wenn ein Betroffener von einer Auskunftei wissen möchte, von welcher Stelle sie seine Daten erhalten und an welche Stellen sie diese weitergegeben hat. Das BDSG gewährt dem Betroffenen zwar einen Anspruch gegenüber der Auskunftei auf Erteilung von Auskünften sowohl über Empfänger als auch über die Herkunft von Daten. Dieser Anspruch besteht nach dem Gesetz aber nur, sofern das Interesse der Auskunftei an der Wahrung des Geschäftsgeheimnisses nicht überwiegt. Unter den Begriff des Geschäftsgeheimnisses kann grundsätzlich auch die Tatsache des Bestehens einer Geschäftsverbindung der Auskunftei zu einem Unternehmen fallen.

Die Auskunftei hat daher in jedem Einzelfall eine Abwägung der Interessen des Auskunftsbegehrenden an der Erteilung der Auskunft einerseits und ihrer eigenen Interessen an der Wahrung des Geschäftsgeheimnisses andererseits vorzunehmen. Kommt sie danach zu dem Ergebnis, dass ihre Geschäftsinteressen überwiegen, hat sie dies gegenüber dem Betroffenen zu begründen.

Da es bestimmte Branchen gibt, in denen die Einholung von Bonitätsauskünften üblich ist und der Betroffene damit rechnen muss, besteht in diesen Fällen kein Geheimhaltungsinteresse hinsichtlich der Daten empfangenden Stelle, so dass hier das Auskunftsinteresse überwiegt. Auch in bestimmten anderen Fällen kann in der Regel von einem überwiegenden Interesse des Betroffenen an der Auskunftserteilung ausgegangen werden.

Die Datenschutzaufsichtsbehörden der Länder und der Verband der Handelsauskunfteien haben sich daher in bezug auf die **Auskunftserteilung über Empfänger** von Daten auf eine generelle Vorgehensweise geeinigt. Eine Auskunftserteilung erfolgt danach stets in folgenden Fällen:

- Der Betroffene trägt begründete Zweifel an der Richtigkeit der Daten vor.
- Der Betroffene trägt vor, Schadenersatz- oder Richtigstellungsansprüche geltend zu machen, da einzelne Daten unzutreffend seien.
- Der Betroffene gibt an, der Auskunftsempfänger habe den Auskunftsdatensatz in unberechtigter Weise an Dritte weitergegeben bzw. ihn in der Weise missbräuchlich verwendet.
- Der Betroffene trägt vor, der Auskunftsempfänger könne unter keinen Umständen ein berechtigtes Interesse an der Auskunft gehabt haben.

In diesen Fällen hat der Betroffene die entsprechenden Voraussetzungen näher zu begründen und - falls möglich - auch zu belegen.

Über die genannten Fallgruppen hinaus erfolgt nach der getroffenen Absprache eine Auskunftserteilung über den Datenempfänger, wenn es sich dabei um ein Unternehmen aus folgenden Branchen handelt:

- Kreditversicherungen/Versicherungen,
- Versandhandel,
- Telekommunikation,
- Banken,
- Leasing-/Factoringgesellschaften oder
- Konzerngesellschaften.

In allen übrigen Fällen ist gleichwohl eine Interessenabwägung im Einzelfall vorzunehmen. Führt diese dazu, dass das Auskunftsinteresse überwiegt, hat der Betroffene einen entsprechenden Auskunftsanspruch. Andernfalls ist die Auskunftei berechtigt, die Erteilung einer Auskunft insoweit - allerdings mit entsprechender Begründung - abzulehnen.

Der Verband der Handelsauskunfteien hat gegenüber den Datenschutzaufsichtsbehörden mitgeteilt, dass seine Mitglieder diese Vereinbarung seit September 2004 umsetzen.

Ob zur **Herkunft der Daten** eine vergleichbare Regelung getroffen werden kann, ist derzeit noch offen. Es werden hierüber Gespräche mit dem Verband der Handelsauskunfteien geführt.

1.4 Schätzdaten und Kennzeichnungspflicht

Da ihnen tatsächliche Daten häufig nicht vorliegen, bedienen sich Wirtschaftsauskunfteien bei der Auskunftserteilung über Unternehmenszahlen häufig branchenüblicher oder statistisch ermittelter Durchschnittswerte. Statt echter Daten werden in diesen Fällen also Schätzdaten verwendet. Es handelt sich dabei meist um Informationen über den Jahresumsatz, die Anzahl der beschäftigten Mitarbeiter oder Bilanzzahlen (Aktiva/Passiva) von Unternehmen. Das BDSG ist in diesen Fällen anwendbar, wenn es sich um personenbezogene Angaben handelt, die z.B. einem Einzelhandelskaufmann oder dem Geschäftsführer einer Ein-Mann-GmbH zugeordnet werden können.

Die im Rahmen der Auskunftserteilung verwendeten Schätzdaten müssen auf einer soliden aussagefähigen Basis branchenüblicher und statistisch ermittelter Durchschnittswerte beruhen. Darüber besteht schon seit einiger Zeit Einigkeit zwischen den Datenschutzaufsichtsbehörden und dem Verband der Handelsauskunfteien.

Seit langem umstritten war dagegen die Frage, ob und in welchem Umfang die Verwendung von Schätzdaten von den Auskunfteien gekennzeichnet werden muss, um sowohl den Auskunftsempfänger als auch den Betroffenen selbst bei Erteilung einer Selbstauskunft darüber zu informieren, dass es sich hier nicht um auf Tatsachen beruhende Daten handelt. Wünschenswert wäre es aus Sicht der Aufsichtsbehörden, dass jedes einzelne geschätzte Datum gekennzeichnet wird. Im Ergebnis einigte man sich jedoch mit dem Verband der Handelsauskunfteien darauf, dass in jede Auskunft an geeigneter Stelle folgender Text deutlich sichtbar zu integrieren ist: „Bei den in den Auskünften enthaltenen Unternehmenszahlen kann es sich teilweise um auf Basis von Branchendurchschnittswerten geschätzte Angaben handeln“. Hierdurch werden sowohl die Interessen des Auskunftsempfängers als auch die des Betroffenen gewahrt. Letzterer hat so die Möglichkeit, entweder die geschätzten Daten durch tatsächliche Angaben zu ersetzen oder die geschätzten Daten sperren zu lassen.

Der Verband der Handelsauskunfteien hat mitgeteilt, dass die Kennzeichnung seit September 2004 vorgenommen und entsprechend Auskunft gegeben wird.

1.5 Entgelterhebung für die Selbstauskunft

Einige Auskunfteien machen die Erteilung einer Selbstauskunft von der Bezahlung eines Entgelts abhängig. Dies führt bei den Betroffenen immer wieder zu Unverständnis und entsprechenden Nachfragen bei der Aufsichtsbehörde.

Eine Selbstauskunft ist nach § 34 Abs. 5 BDSG unentgeltlich zu erteilen. Werden die personenbezogenen Daten jedoch geschäftsmäßig zum Zweck der Übermittlung gespeichert - wie etwa bei der Tätigkeit von Auskunfteien -, so kann ein Entgelt verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann, wobei insoweit die bloße Möglichkeit einer solchen Verwendung gegenüber Dritten ausreicht.

Die Entgelterhebung stellt jedoch nicht die Regel, sondern die Ausnahme dar. Auskunfteien sind nicht befugt, generell darauf zu verweisen, dass die Daten auch als

Selbstauskunft zu kommerziellen Zwecken verwendet werden könnten. Es muss für die Auskunftei vielmehr erkennbar sein, dass der Betroffene im konkreten Fall ihm ansonsten entstehende Kosten erspart.

Vor diesem Hintergrund ist nach Auffassung der Aufsichtsbehörde nicht ersichtlich, dass eine Selbstauskunft, die lediglich Negativmerkmale enthält oder die besagt, dass zu dem Betroffenen „keine Informationen“ vorliegen, von einem Betroffenen gegenüber Dritten zu wirtschaftlichen Zwecken genutzt werden kann. Mittels einer solchen Auskunft wird es ihm meist nicht gelingen, seine Bonität nachzuweisen. Es dürfte in der Regel so sein, dass ein Betroffener, der Dritten eine solche Selbstauskunft vorlegt, die von ihm gewünschte Leistung gerade nicht erhalten wird. Die Voraussetzung für eine Entgelterhebung liegen daher in diesem Fall nicht vor.

Ferner darf ein Entgelt nicht verlangt werden, wenn besondere Umstände die Annahme rechtfertigen, dass Daten unrichtig oder unzulässig gespeichert werden oder wenn die Auskunft ergibt, dass die Daten zu berichtigen oder wegen unzulässiger Speicherung zu löschen sind.

Liegen die Voraussetzungen für eine Entgelterhebung vor, so darf das Entgelt über die durch die Auskunftserteilung entstandenen direkt zurechenbaren Kosten nicht hinausgehen. Die Auskunftei hat in diesem Fall den Betroffenen aber die Möglichkeit einzuräumen, sich im Rahmen ihres Auskunftsanspruchs persönlich Kenntnis über die sie betreffenden Daten und Angaben zu verschaffen, etwa in einer Geschäftsstelle. Die Betroffenen sind darauf in geeigneter Weise hinzuweisen.

1.6 Auskunftei mit Datenpool für einen geschlossenen Benutzerkreis

Die Aufsichtsbehörde prüfte im Berichtszeitraum auch das Verfahren eines Unternehmens, das einerseits als Wirtschaftsauskunftei tätig ist, andererseits aber für einen geschlossenen Kreis von großen Industrieunternehmen aus den verschiedensten Bereichen einen sogenannten Datenpool betreibt und pflegt. In diesem Pool werden Daten über Unternehmen sowie Privatpersonen, die - wie z.B. Einzelhandelskaufleute - am Wirtschaftsleben teilnehmen, gespeichert, aktualisiert und bei konkreten Anfragen an die Poolteilnehmer weitergegeben. Bei diesen Daten handelt es sich einerseits um Stammdaten wie etwa Angaben zu Vor- und Nachnamen, Firmierung, Anschrift, Telefon- und Fax-Nummer. Darüber hinaus werden aber auch Informationen zum Zahlungsverhalten der Unternehmen wie etwa Einträge im Schuldnerverzeichnis, Angaben zum Zahlungsverzug und unbestrittene Inkassoforderungen, die von den Poolteilnehmern mitgeteilt werden, in dem Datenpool gespei-

chert. Zweck dieses Datenpools ist es, den angeschlossenen Poolteilnehmern einerseits den Administrationsaufwand für die Pflege ihrer Kundendaten zu ersparen und ihnen andererseits Informationen zum Zahlungsverhalten ihrer Kunden weiterzugeben.

Während für die Weitergabe der aktualisierten Stammdaten über das Bestehen einer Geschäftsverbindung keine besonderen Voraussetzungen erfüllt werden müssen, gilt dies für Informationen zum Zahlungsverhalten nicht. Die angeschlossenen Poolteilnehmer dürfen diese Informationen im Einzelfall nur abrufen, wenn sie insoweit ein berechtigtes Interesse haben. Das ist der Fall, wenn sie mit einem anderen Unternehmen ein Geschäft mit wirtschaftlichem Risiko abschließen, beispielsweise diesem einen Kredit gewähren wollen. Das andere Unternehmen kann ein Alt- oder ein Neukunde sein.

Die Aufsichtsbehörde hat von der Auskunftei verlangt, dass sie die einzumeldenden Daten klar definiert (z.B. wann liegt Zahlungsverzug vor?) und in den Verträgen mit den Poolteilnehmern die Einmeldung präziser regelt. Die Aufsichtsbehörde hält darüber hinaus eine Reihe von Maßnahmen für erforderlich, mit denen die Rechte der Betroffenen auf Benachrichtigung, Auskunftserteilung, Sperrung und Löschung gewahrt werden. Das Unternehmen wird die Forderungen umsetzen.

1.7 Warndatei „Diebstahl“

Ladendiebe werden in den meisten Fällen durch die Staatsanwaltschaft nicht verfolgt, wenn der entwendete Gegenstand geringwertig ist. Die Grenze liegt in der Regel bei 25 €. Dadurch können sogenannte Wanderdiebe nicht entdeckt werden. Das ist für die betroffenen Einzelhändler sehr ärgerlich. Eine Firma kam deshalb auf die Idee, mit dem Einzelhandel einen Interessenverbund gegen Ladendiebstahl zu gründen. Die betroffenen Einzelhändler sollten die Daten von Ladendieben in eine zentrale Datenbank einmelden. Erfasst werden sollten außer dem Wert des Diebesguts umfangreiche personenbezogene Daten des Ladendiebs. Auf diese Weise sollten Mehrfachtäter erkannt und mehrere Fälle des Diebstahls geringwertiger Gegenstände, bei denen zusammengenommen der Wert von 25 € überschritten wurde, von einer sogenannten „Klägergemeinschaft“ zur Anzeige gebracht werden.

Wir hielten dieses Vorhaben für datenschutzrechtlich bedenklich, da mit der systematischen Erfassung von Straftätern zur Ermittlung von Wiederholungstätern eine Kompetenz wahrgenommen würde, die einer privaten Vereinigung nicht zusteht. Sie würde damit auf dem Gebiet der Strafrechtspflege tätig, die der Polizei und der Staats-

anwaltschaft obliegt. Die Übermittlung der personenbezogenen Daten des Ladendiebs an eine zentrale Ladendiebstahls-Datenbank durch die jeweiligen Einzelhändler ist daher nicht mehr als ein Mittel zur Erfüllung eigener Geschäftszwecke anzusehen, das zur „Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist."

Erlaubt wäre hingegen, dass ein Einzelhändler, bei dem es zu einem Ladendiebstahl gekommen ist, die Daten des Ladendiebs speichert und nutzt, um ein ausgesprochenes Hausverbot zu überwachen oder um Ansprüche zivilrechtlicher Art geltend machen zu können.

1.8 Kaufkraftdaten und Risikoklassen privater Haushalte per CD

Bundesweit große Aufregung verursachte eine CD, die im Sommer 2004 auf den Markt kam und den Käufern Auskunft über statistische Kaufkraftdaten und Risikoklassen sämtlicher privater Haushalte in Deutschland versprach. Diese CD, die von einem Unternehmen mit Sitz in Nordrhein-Westfalen hergestellt wurde, ermöglichte es den Nutzern, Kaufkraft und Risikostruktur eines ausgewählten Straßenabschnitts festzustellen. Die CD wurde unter anderem mit folgendem Text beworben: "Wüssten Sie nicht auch gerne, wie es in Ihrer Nachbarschaft mit dem Geld aussieht? Oder im Wohngebiet von Kollegen und Bekannten? Sie werden überrascht sein!". Die zur Herstellung dieser CD erforderlichen Daten wurden von verschiedenen Unternehmen mit Sitz in Baden-Württemberg geliefert, weshalb sich die Aufsichtsbehörde in diesen Fall eingeschaltet hat.

Das auf der CD befindliche Programm zeigt bei einer Anfrage zu einem konkreten Straßenabschnitt jeweils die hierzu ermittelte Kaufkraft und das Zahlungsrisiko an. Zur Haushaltskaufkraft wird sowohl prozentual als auch absolut in Anzahl der Häuser des betreffenden Straßenabschnitts angegeben, ob die Kaufkraft in die Kategorie „sehr hoch" (Schulnote 1), „hoch" (Schulnote 2), „mittel" (Schulnote 3), „gering" (Schulnote 4) oder „sehr gering" (Schulnote 5) fällt. In ähnlicher Weise wird auch das Zahlungsrisiko für den betreffenden Straßenabschnitt ermittelt. Hier entspricht der Schulnote 1 ein sehr geringes Zahlungsrisiko, der Schulnote 5 ein sehr hohes Zahlungsrisiko. Beim Zahlungsrisiko findet eine Aufschlüsselung auf einzelne Häuser für den Nutzer abrufbar nicht statt. Vielmehr wird lediglich in einer optischen Anzeige, bezogen auf die Schulnoten 1-5, das Zahlungsrisiko mitgeteilt.

Die insoweit zuständige Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW) hat die CD datenschutzrechtlich bewertet. Danach

ist die mit dem Vertrieb der CD verknüpfte Übermittlung von Daten an Dritte bereits deswegen rechtswidrig, weil das Programm für bestimmte Kategorien die Information zur Verfügung stellt, dass alle Häuser einer Straße oder eines Straßenabschnitts bewertet wurden und dabei alle die gleiche oder eine ähnliche Note erhielten. Dies führt dazu, dass unabhängig von der Zahl der in einem Abschnitt zusammengefassten Häuser eine Aussage nicht nur über den Straßenabschnitt, sondern über ein konkretes Haus erfolgt. Jedenfalls soweit es sich um Einfamilienhäuser handelt, werden ohne Rechtsgrundlage personenbezogene Bewertungen über einen Haushalt oder dessen Mitglieder an eine unbestimmte Zahl von Dritten übermittelt. Die LDI NRW hat daher gegen das Unternehmen einen Bußgeldbescheid erlassen. Das betroffene Unternehmen hat inzwischen zugesichert, die CD nicht mehr zu vertreiben und auch von einer Neuauflage abzusehen.

Wir haben die Übermittlung der Kaufkraft- und Risikodaten durch die beteiligten baden-württembergischen Unternehmen an das nordrhein-westfälische Unternehmen zur Herstellung der CD ebenfalls als datenschutzrechtlich unzulässig beurteilt, da es hierfür keine Rechtsgrundlage gibt. Die von den hier ansässigen Unternehmen übermittelten Daten wurden entsprechend der zuvor getroffenen Vereinbarung zur Herstellung einer Auskunftssoftware verwendet, die grundsätzlich einem unbeschränkten Personenkreis zugänglich war. Der Nachweis eines berechtigten Interesses (wie z.B. der Abschluss eines Geschäfts mit wirtschaftlichem Risiko), den das BDSG in diesen Fällen fordert, erfolgte nicht. Bereits auf Grund des beabsichtigten Verwendungszwecks, der auch sogenannte Neugierauskünfte ermöglichte, sind hier schutzwürdige Interessen der Betroffenen am Ausschluss der Übermittlung dieser Daten an das die CD herstellende Unternehmen anzunehmen.

Die baden-württembergischen Unternehmen haben uns gegenüber bestätigt, dass der Vertrag mit der Herstellerfirma der CD zwischenzeitlich aufgelöst wurde. Sie haben darüber hinaus zugesagt, dass sie eine etwaige Neuauflage der CD oder andere ähnliche Produkte zukünftig nicht durch Datenlieferungen unterstützen werden.

Der Düsseldorfer Kreis hat in einem einstimmig gefassten Beschluss über den konkreten Fall hinaus zum Ausdruck gebracht, dass es vergleichbare, einem unbeschränkten Personenkreis zugängliche Produkte, die zum Zweck der Adress- oder Bonitätsbewertung statistische, mikrogeografische und/oder soziodemografische Klassifizierungen und Profile verwenden, sehr kritisch beurteilt.

1.9 „Waschabgleich“

Ein spezielles Angebot von Auskunfteien ist der sogenannte „Waschabgleich“. Dieser dient der Optimierung persönlich adressierter Werbeaussendungen und hat das Ziel, die richtige Zielgruppe ertragskräftiger Personen für das jeweils zu bewerbende Produkt zu ermitteln. Dieses Verfahren, das es in zwei verschiedenen Formen gibt, läuft wie folgt ab:

Ein Unternehmen übermittelt eine beliebige Anzahl von Adressen an die Auskunftei mit dem Auftrag, aus diesem Brutto-Adressbestand diejenigen „herauszuwaschen“, die bei der Auskunftei mit einem oder mehreren Negativmerkmalen (z.B. Einträge im Schuldnerverzeichnis) bekannt sind. Nach dem „Herauswaschen“ dieser Negativ-Adressen erhält das Unternehmen einen bereinigten Bestand zurückübermittelt. Dadurch soll erreicht werden, dass nur solche Personen Werbung erhalten, die bei einer Bonitätsprüfung im Fall einer Bestellung nicht wegen Zweifeln an der Zahlungsfähigkeit abgelehnt werden müssten.

Manche Unternehmen bedienen sich zur Durchführung von Werbeaktionen hingegen eines Direktmarketingunternehmens oder eines Adressbrokers. Dieser zwischengeschaltete Dienstleister übernimmt zumeist sämtliche Tätigkeiten im Rahmen der Werbeaktion bis hin zur Versendung der Werbematerialien. In diesem Fall liegt eine Datenverarbeitung im Auftrag durch den Dienstleister vor.

Nach Auffassung der Aufsichtsbehörde ist die Durchführung des Waschabgleichs in der ersten Variante unzulässig. Der Adresseigner kann hier nämlich rekonstruieren, welche Adressen selektiert wurden. Für diese Datenübermittlung an den Adresseigner fehlt es an dem erforderlichen berechtigten Interesse. Ein solches besteht nur beim bevorstehenden Abschluss eines Geschäfts mit wirtschaftlichem Risiko, nicht aber bei der Zusendung von Werbung.

Datenschutzrechtlich zulässig ist hingegen der Waschabgleich nach der zweiten Variante, weil hier der Adresseigner selbst nicht rekonstruieren kann, welche Adressen selektiert wurden.

2 Werbung und Adresshandel

2.1 Hinweis auf Werbewiderspruch, Informationspflichten nach § 4 Abs. 3 BDSG bei der Coupon- und Verbundwerbung

Nach § 28 Abs. 4 BDSG kann ein Betroffener der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung gegenüber der verantwortlichen Stelle widersprechen mit der Folge, dass die Nutzung seiner Daten für diese Zwecke unzulässig ist. Auf dieses Widerspruchsrecht ist der Betroffene bei der Ansprache zum Zwecke der Werbung hinzuweisen. Wir müssen jedoch leider feststellen, dass diese Vorschriften noch immer vielen werbetreibenden Unternehmen nicht bekannt sind und uns vorgelegte Werbemittel entweder überhaupt keinen oder keinen dem Gesetz genügenden Hinweis enthalten, obwohl es zu diesem Thema inzwischen ausreichend Informationsmaterial gibt.

Häufig nicht beachtet werden im Bereich der Werbung auch die Informationspflichten bei der Datenerhebung (vgl. dazu oben B. 1). Eine leicht modifizierte Verfahrensweise haben wir für die sogenannte Coupon- und Verbundwerbung zugelassen, um deren Besonderheiten Rechnung zu tragen.

Bei der Couponwerbung handelt es sich entweder um ein Heft, das mehrere Anforderungs- oder Bestellkarten für Kataloge oder Waren unterschiedlicher Unternehmen enthält, oder um Bestellvordrucke bzw. -abschnitte aus Werbeanzeigen in Zeitschriften. Die Coupons sind in der Regel bereits an die werbenden Unternehmen adressiert. Die Werbung mit einem Couponheft kann adressiert oder als Postwurfsendung erfolgen.

Bei der Verbundwerbung werben mehrere Unternehmen gemeinsam und der Betroffene kann beispielsweise durch Ankreuzen auf einer Postkarte von verschiedenen Unternehmen Informationsmaterial oder Waren bestellen. Die Postkarte wird an den Versender der Verbundwerbung zurückgesandt. Dieser gibt die angegebenen Daten an die einzelnen Unternehmen zum Versand der Informationsmaterialien oder der Waren weiter. In all diesen Fällen werden die Daten der Betroffenen den werbenden Unternehmen erst mit der Anforderung oder Bestellung durch den Betroffenen selbst bekannt gegeben.

Damit, dass die Daten der Besteller bei dem werbenden Unternehmen zumindest für die Versandabwicklung der bestellten Artikel gespeichert werden, damit dürfte heutzutage jeder Betroffene rechnen, so dass eine diesbezügliche Unterrichtung nicht

erforderlich ist. Sollen die Daten aus dem Bestellvorgang aber für einen anderen Zweck, beispielsweise für Werbezwecke weiterverwendet werden, müsste im Grunde genommen auf jedem Coupon, auch wenn es sich z.B. um einen Bestellabschnitt aus einer Zeitschrift handelt, ein Hinweis nach § 4 Abs. 3 BDSG angebracht werden. Oftmals ist dies jedoch auf Grund der Größe der Coupons nicht praktikabel. Die Aufsichtsbehörde hat sich daher damit einverstanden erklärt, dass in den Fällen, in denen das Couponheft mit einem persönlich adressierten Anschreiben zugesandt wird, lediglich in dieses ein Hinweis nach § 4 Abs. 3 BDSG aufgenommen wird. Wird ein Couponheft mittels Postwurfsendung versandt, kann der Hinweis entweder im gegebenenfalls beigefügten Anschreiben oder aber auf dem Deckblatt des Couponheftes angebracht werden. Bei der Verbundwerbung gilt Entsprechendes.

Für Coupons aus Zeitschriften ohne einen entsprechenden Hinweis gilt, dass die Daten zunächst nur für die konkrete Bestellabwicklung verarbeitet werden dürfen. Sollen die Daten aber auch für Werbezwecke verwendet werden, ist der Betroffene spätestens im Rahmen der Ausführung der Bestellung darauf hinzuweisen.

2.2 Werbung durch Kooperationspartner

Es ist zunehmend festzustellen, dass Unternehmen einen Kooperationspartner damit beauftragen, für ihr Produkt zu werben. Früher haben in der Regel die Kooperationspartner dem Unternehmen, welches das Produkt vertreibt, ihre Kundendaten für Werbezwecke zur Verfügung gestellt. Inzwischen kommt es immer häufiger vor, dass zwischen dem Unternehmen und dem Kooperationspartner vertraglich geregelt wird, dass der Kooperationspartner selbst für das Produkt des Unternehmens wirbt und dazu die Daten seiner eigenen Kunden nutzt. Die Werbemaßnahme durch den Kooperationspartner erfolgt sowohl auf telefonischem als auch auf schriftlichem Weg.

Bei schriftlicher Werbung wird das Unternehmen, welches das Produkt vertreibt, in den Werbeschreiben regelmäßig nicht genannt. Vielfach wird darin aber für die Kontaktaufnahme eine Postfachadresse oder eine Telefonnummer angegeben, unter der das Produkt bestellt werden kann. Eingehende Post an die Postfachadresse wird direkt an das Unternehmen, welches das Produkt vertreibt, weitergeleitet. Hinter der genannten Telefonnummer befindet sich in der Regel ein Call-Center des Unternehmens, welches das Produkt vertreibt. Den Betroffenen wird meistens erst bei der telefonischen Kontaktaufnahme oder sogar erst beim Vertragsschluss bewusst, dass es sich um ein Produkt eines anderen Unternehmens handelt.

Bei telefonischer Werbung sichert der Kooperationspartner dem Unternehmen, für dessen Produkt er wirbt, vertraglich zu, nur solche Kunden telefonisch zu kontaktieren, von denen ihm eine Einwilligung in die telefonische Werbung vorliegt. In den Gesprächen wird erfahrungsgemäß in der Regel das Unternehmen genannt, welches das Produkt vertreibt und mit welchem dann auch ein Vertrag zustande kommt.

Datenschutzrechtlich verantwortliche Stelle für die Werbung ist zumindest bei einem Teil der an uns herangetragenen Fälle der Kooperationspartner, der auch die Datenschutzrechte der Betroffenen zu wahren hat. Das Unternehmen, dass das Produkt vertreibt, erfährt die Daten des Betroffenen regelmäßig erst, wenn dieser auf die Werbung reagiert, also beispielsweise unter der angegebenen Telefonnummer anruft bzw. unter der Postfachadresse bestellt oder aber beim Kooperationspartner im Rahmen des telefonischen Werbegesprächs das Produkt bestellt und dieser die Daten zum Vertragsschluss an das Unternehmen weiterleitet.

Bei den schriftlichen Werbemaßnahmen haben sich die Betroffenen in der Regel an die Aufsichtsbehörde gewandt, als sie bemerkten, dass es sich bei dem Vertragspartner nicht um das Unternehmen handelt, bei welchem sie schon Kunde sind, sondern um ein völlig anderes Unternehmen. Sie fühlten sich getäuscht.

Die Aufsichtsbehörde hat sich in den vorgelegten Fällen insbesondere bei den Kooperationspartnern dafür eingesetzt, dass die Rechte der Betroffenen gewahrt werden. Sie hat nach dem BDSG darauf hingewirkt, dass bei schriftlicher Werbung in den Werbeschreiben die erforderlichen Hinweise auf die verantwortliche Stelle und die Möglichkeit, der Nutzung der Daten für Werbezwecke zu widersprechen, an deutlich erkennbarer Stelle angebracht werden. Die Aufsichtsbehörde hat auch darauf gedrängt, in den Werbeschreiben auf die Kooperation hinzuweisen, denn der Betroffene kann auf Grund seiner Kundenbeziehung zum werbenden Unternehmen nicht davon ausgehen, dass bei der Bestellung eines Produkts ein anderes, ihm womöglich bis dahin fremdes Unternehmen Vertragspartner wird.

Über telefonische Werbemaßnahmen beschweren sich Betroffene immer wieder mit der Begründung, darin nicht eingewilligt zu haben. Hier war bei den Überprüfungen zumeist festzustellen, dass sich die Kooperationspartner externer Call-Center bedient hatten, die wiederum die Telefonnummern für die telefonische Werbung angemietet hatten. Die Vermieter bestätigten den Call-Centern in der Regel, dass es sich nur um solche Telefonnummern handelt, für die entsprechende Einwilligungen in die telefonische Werbung vorliegen. Die Einwilligungen selbst lagen den Call-Centern regelmäßig nicht vor.

Bei diesem Geflecht von Beteiligten ist es für den Betroffenen selbst beinahe unmöglich, herauszufinden, auf Grund welcher Einwilligung in eine telefonische Werbung er angerufen wurde. Zum einen ist es nicht ungewöhnlich, dass bei Vertragsabschlüssen in die „telefonische Werbung auch von Vertragspartnern“ eingewilligt wird, wobei die Vertragspartner allerdings häufig in einer Weise benannt werden, die datenschutzrechtlichen Erfordernissen nicht genügt, so dass die Einwilligung unwirksam ist. Zum anderen werden aber auch Formulierungen wie beispielsweise „anbei meine Telefonnummer für die telefonische Gewinnbenachrichtigung“ von einzelnen Datenhändlern als Einwilligung in die telefonische Werbung angesehen, was selbstverständlich nicht der Fall ist.

Insgesamt ist dieser Bereich nicht sehr transparent. Deshalb wird man die weitere Entwicklung sorgfältig beobachten müssen. Dies ist mühsam, weil in zahlreichen Fällen die Akteure über das ganze Bundesgebiet verteilt sind, so dass mehrere Datenschutzaufsichtsbehörden zuständig sind. Geboten erscheint uns auch eine enge Kooperation mit den Verbraucherschutzverbänden, da der Problematik nur zum Teil mit den Mitteln des Datenschutzes beizukommen ist.

2.3 Unverlangt zugesandte elektronische Werbung

Nach wie vor beziehen sich viele Beschwerden auf die unverlangte Zusendung von Werbung per E-Mail und Telefax. Während die datenschutzrechtliche Beurteilung unverändert blieb (vgl. dazu den zweiten Tätigkeitsbericht Nr. 5.4, Seite 56), hat sich die wettbewerbsrechtliche Grundlage geändert. Wie unter A 2.3 dargestellt, bestimmt der neue § 7 UWG, dass unverlangte elektronische Werbung eine unzumutbare Belästigung im Sinne des § 3 UWG sein kann. Damit hat der Gesetzgeber Klarheit geschaffen. Eine wettbewerbswidrige Nutzung eines personenbezogenen Datums, wie E-Mailadresse oder Rufnummer, ist immer auch datenschutzrechtlich unzulässig, da die schutzwürdigen Interessen des Betroffenen gegenüber einer wettbewerbswidrigen Nutzung und Verarbeitung immer überwiegen.

2.4 Zielgruppenbildung bei einem Direktwerbeunternehmen und Praxis der Auskunftserteilung

Beschwerden von Bürgern, die sich über ihre Einbeziehung in eine Direktwerbeaktion beklagt hatten und von uns wissen wollten, woher ihre Daten stammen und weshalb sie ausgewählt wurden, waren für uns Anlass, ein Direktwerbeunternehmen zu überprüfen. Gegenstand der Prüfung waren insbesondere Datenerhebung,

-speicherung und Zielgruppenbildung sowie die Praxis der Auskunftserteilung. Erstere waren nicht zu beanstanden, letztere muss in einigen Punkten verbessert werden.

Die Werbebranche bevorzugt die direkte Ansprache potentieller Kunden, da so wesentlich besser auf deren Wünsche und Bedürfnisse eingegangen werden kann und kein Werbematerial an mutmaßlich nicht Interessierte versandt wird. Eine der wesentlichen Voraussetzungen für ein gut funktionierendes Direktmarketing ist die Bildung von Zielgruppen, bei denen davon ausgegangen werden kann, dass sich deren Angehörige höchstwahrscheinlich für das angebotene Produkt interessieren.

Erste Feststellung im Rahmen der Prüfung war, dass das Unternehmen nicht - wie viele meinen - über „fertige“ Zielgruppen - beispielsweise Haushalte nach Kaufkraft, nach Wohnsituation usw. - samt zugehöriger Anschriften verfügt, sondern diese je nach Kundenwunsch des Auftraggebers aus verschiedenen Datenbanken zusammenstellt, die teilweise personenbezogene, teilweise aber auch mikrogeografische, soziodemografische und statistische Daten ohne Personenbezug enthalten.

Beschafft werden diese Daten zum einen über Konsumenten- und Haushaltsbefragungen mittels mehrseitiger Fragebögen, an denen die Betroffenen freiwillig teilnehmen. Sofern die Betroffenen in gehöriger Form über die Verwendung ihrer Daten informiert werden und in die Datenverarbeitung eingewilligt haben, ist dagegen nichts einzuwenden. Zum anderen werden die Daten allgemein zugänglichen Quellen, z. B. Zeitungen, Zeitschriften, Telefonbüchern, Rundfunk- und Fernsehsendungen, dem Internet sowie Publikationen entnommen und gespeichert, was ebenfalls zulässig ist. Allgemein zugänglich sind auch Daten von Wohngebäuden (z. B. deren Alter und Zustand) und Wohngegenden, die im Rahmen sogenannte Wohngebietsbegehungen erhoben werden, sowie Statistikdaten.

Wenn daraus dann Haushalte nach der Kaufkraft oder nach der Wohnsituation zusammengestellt werden, mag dies bei Außenstehenden den Eindruck erwecken, als lägen dem konkrete Informationen zur Einkommenssituation zugrunde, tatsächlich sind es jedoch die genannten Daten verbunden mit der Einschätzung, dass die Lebensverhältnisse aller Bewohner eines bestimmten Wohngebiets im Großen und Ganzen ähnlich sind. Eine solche Verwendung der aufgeführten Ausgangsinformationen **für Zwecke der Werbung** ist nach Auffassung der Aufsichtsbehörde mit § 28 Abs. 1 Satz 1 Nr. 3 BDSG vereinbar. Dies gilt auch für die Weitergabe der Zielgruppendaten samt zugehöriger Adressen an Unternehmen zur Durchführung von Werbemaßnahmen (sogenannte Lettershops), wenn die Adressdaten - wie üblich - nach der Werbeaussendung gelöscht werden. An dieser Stelle sei darauf hingewiesen,

dass die Veröffentlichung von Kaufkraftdaten und Risikoklassen privater Haushalte per CD als unzulässig beurteilt wird (vgl. C 1.8).

In mehrfacher Hinsicht verbessert werden muss die Praxis der Auskunftserteilung an Betroffene (§ 34 BDSG):

- Verlangt ein Betroffener Auskunft über die zu seiner Person gespeicherten Daten, ist ihm, falls keine Daten über ihn gespeichert sind, eine entsprechende Auskunft zu erteilen.

- Die Auskunftserteilung darüber, ob Daten in eigenen Dateien des Unternehmens gespeichert sind, kann nicht davon abhängig gemacht werden, dass der Auskunftssuchende nähere Angaben zur Werbesendung macht, über die er sich beschwert und die ihn zu seinem Auskunftsverlangen veranlasst hat. Zwar soll der Betroffene nach dem Gesetz die Art der personenbezogenen Daten, über die er Auskunft begehrt, näher bezeichnen, um bei der speichernden Stelle unnötigen Aufwand zu vermeiden. Für die Auskunftserteilung darüber, ob Daten gespeichert sind, ist diese Angabe jedoch nicht erforderlich.

- Dem Auskunftssuchenden müssen **alle über ihn gespeicherten Daten konkret, also auf seine Person bezogen**, mitgeteilt werden. Eine allgemeine Beschreibung der gespeicherten Daten genügt nicht, erst recht nicht eine Beschränkung auf die aus allgemein zugänglichen Quellen entnommenen Daten. Sind zu einer Anschrift weitere Daten zum Wohnumfeld gespeichert, wie z. B. Kaufkraft der Region oder Angaben zum Wohnumfeld, und werden diese im Rahmen einer Zielgruppenbildung dem Betroffenen zugeordnet, muss sich die Auskunft auch hierauf erstrecken. Mitgeteilt werden müssen auch gesperrte Daten, beispielsweise wenn der Betroffene in einer Sperrdatei erfasst ist, da er keine Werbung erhalten möchte. Die Auskunft muss auch die genaue Bezeichnung der Datei angeben, in der die Daten gespeichert sind.

- Anzugeben ist auch der Zweck der Datenverarbeitung, es sei denn, der Betroffene schränkt sein Auskunftsverlangen ein.

- Der Betroffene kann auch Auskunft über die Herkunft seiner Daten und die Datenempfänger beanspruchen. Im ersteren Fall muss ihm mitgeteilt werden, welchen Quellen die Daten **entnommen werden**. Die Angabe, welchen Quellen sie entnommen werden können, genügt nicht. Die Auskunft muss sich auch insoweit auf

alle Daten beziehen. Die Datenempfänger sind zumindest der Kategorie nach zu bezeichnen.

2.5 Adressübermittlung an die Gebühreneinzugszentrale zur Ermittlung von Schwarzhörern und -sehern

Die Gebühreneinzugszentrale (GEZ) erwirbt im Auftrag der Rundfunkanstalten regelmäßig Anschriften beim Adresshandel. Sie nutzt die Daten für Briefaktionen, mit denen Schwarzhörer und -seher zur Anmeldung ihrer Rundfunkgeräte bewegt werden sollen. In einem ersten Schreiben werden die Empfänger aufgefordert, zu überprüfen, ob sie ihrer gesetzlichen Verpflichtung zur Anmeldung von Rundfunkgeräten nachkommen. Die Empfänger werden unter Fristsetzung aufgefordert, auch dann zu antworten, wenn sie keine Rundfunkgeräte anzumelden haben. Sie ersparen sich dadurch eine „Erinnerung“. Wer nicht antwortet, erhält einen Monat später eine „freundliche Erinnerung“, wiederum verbunden mit einer Frist für die Beantwortung. Wer auch diese Frist verstreichen lässt, erhält eine „letzte Erinnerung“, die den Hinweis enthält, dass eine Verletzung der Anmeldepflicht mit einer Geldbuße geahndet werden könne. Durch eine fristgemäße Antwort ließen sich Unannehmlichkeiten vermeiden.

Bei den Aktionen werden zwangsläufig viele Personen angeschrieben, die bereits Gebührenzahler sind oder keiner Gebührenpflicht unterliegen. Es ist daher nicht verwunderlich, dass sich Betroffene mit Beschwerden an die Datenschutzkontrollorgane wenden. Teilweise wenden sie sich auch an die Aufsichtsbehörde, weil sie in Erfahrung gebracht haben, dass die GEZ die Daten von privaten Adresshändlern erhält.

Datenschutzrechtlich ist dazu Folgendes zu sagen:

Für die Erhebung der Daten durch die GEZ wurde inzwischen eigens eine Rechtsgrundlage im Rundfunkgebührenstaatsvertrag geschaffen. Sie erlaubt es der GEZ, zur Feststellung, ob ein Rundfunkteilnehmerverhältnis besteht, „entsprechend § 28 BDSG personenbezogene Daten zu erheben und zu verarbeiten“. Ob eine solche Regelung mit ihrer Bezugnahme auf eine für nichtöffentliche Stellen geltende Vorschrift sachgerecht ist und damit alle datenschutzrechtlichen Probleme auf der Erhebungsseite gelöst sind - eine Abweichung vom Grundsatz der Direkterhebung beim Betroffenen sieht die Regelung nicht vor -, mögen die für die Kontrolle der Rundfunkanstalten zuständigen Datenschutzbeauftragten (in Baden-Württemberg ist dies der Rundfunkbeauftragte für den Datenschutz beim SWR, in anderen Ländern sind es zum Teil die Landesbeauftragten für den Datenschutz) beurteilen. Eine andere Frage

ist es, ob die Adresshändler die Daten an die GEZ übermitteln dürfen. Ein Adresshändler in Baden-Württemberg und der GEZ nennen als Rechtsgrundlage hierfür § 29 Abs. 2 Satz 1 Nr. 1b BDSG. Danach dürften listenmäßig zusammengefasste Daten für Zwecke der Werbung übermittelt werden, wenn keine schutzwürdigen Interessen der Betroffenen beeinträchtigt werden. Die GEZ selbst schreibt in der uns vorliegenden Antworten auf Auskunftsersuchen Betroffener, dass die Anschrift von der GEZ „für rein werbliche Nutzung“ zur Information über möglicherweise bestehende Gebührenpflichten genutzt werde. Unter „Werbung“ werden nach der üblichen Begriffsdefinition Maßnahmen verstanden, die die Menschen auf **freiwilliger Basis** zu einem bestimmten Verhalten veranlassen sollen. In den Schreiben der GEZ, für die die Adressdaten übermittelt werden, wird jedoch unter Hinweis auf die Folgen eines Untätigbleibens (Verhängung eines Bußgelds) Druck auf die Adressaten ausgeübt, der gesetzlich bestehenden Verpflichtung zur Anmeldung eines Rundfunkgeräts nachzukommen. Werbung im Sinne des BDSG stellt dies nach Auffassung der Aufsichtsbehörde nicht dar. Die Übermittlung der Adressbestände kann daher nicht auf die oben genannte Vorschrift gestützt werden. Eine datenschutzrechtlich befriedigende Lösung des Problems steht noch aus.

3 Kreditwirtschaft

3.1 Offenlegung der wirtschaftlichen Verhältnisse nach § 18 KWG

Mehrere Bürger wandten sich an die Aufsichtsbehörde, nachdem sie von ihrer Bank unter Hinweis auf das Kreditwesengesetz (KWG) eine Aufforderung zur Vorlage bestimmter Unterlagen - meist Einkommensteuererklärung, Einkommensteuerbescheid und Vermögensaufstellung - erhalten hatten. Den Betroffenen war unklar, ob und gegebenenfalls in welchem Umfang sie danach verpflichtet waren, die gewünschten Unterlagen vorzulegen. Sie äußerten auch die Befürchtung, dass sie weit mehr Daten preisgeben müssten, als das Kreditinstitut tatsächlich benötige.

Nach § 18 KWG sind Kreditinstitute gesetzlich dazu verpflichtet, sich bei einer Kreditgewährung von mehr als 250.000 € die wirtschaftlichen Verhältnisse des Kreditnehmers, insbesondere durch Vorlage der Jahresabschlüsse, offen legen zu lassen. Das Kreditinstitut soll über die mit dem Kreditengagement verbundenen Risiken stets informiert sein, um bei etwa eintretenden Verschlechterungen geeignete Maßnahmen ergreifen zu können.

Da das Gesetz keine Vorgaben zur Qualität und zur Zeitnähe der notwendigen Unterlagen enthält, hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) bzw.

vormals das Bundesaufsichtsamt für das Kreditwesen die Anforderungen der Vorschrift in mehreren Rundschreiben inhaltlich konkretisiert, um sicherzustellen, dass die Kreditinstitute die Kreditwürdigkeit ihrer Kreditnehmer in ausreichendem Maße überprüfen. Danach haben die Kreditinstitute durch angemessene organisatorische Vorkehrungen dafür zu sorgen, dass ihre Kreditnehmer ihnen geeignete, die wirtschaftlichen Verhältnisse widerspiegelnde Unterlagen vorlegen.

Hinsichtlich bilanzierender Kreditnehmer hat sich das jeweilige kreditgewährende Institut daher innerhalb bestimmter Fristen turnusgemäß mindestens den zeitlich letzten Jahresabschluss vorlegen zu lassen. Diese Vorgaben gelten entsprechend für die Offenlegung bei Krediten an nicht bilanzierende Kreditnehmer, d.h. auch Privatpersonen. Da diese jedoch ihre wirtschaftlichen Verhältnisse nicht mittels Bilanzen dartun können, muss sich das Kreditinstitut die Vermögenslage und Einkommensverhältnisse des Kreditnehmers durch andere geeignete Unterlagen wie den Einkommensteuerbescheid, die Einkommensteuererklärung oder eine Vermögensaufstellung, die Angaben etwa zu den monatlichen Einnahmen und Ausgaben, Grundvermögen, Guthaben, Wertpapieren, Lebensversicherungen und bestehenden Verbindlichkeiten enthält, nachweisen lassen.

Die BaFin hat den Kreditinstituten jedoch bei der Anforderung der Einkommensteuererklärung und der Vermögensaufstellung einen im Einzelfall auszuübenden Beurteilungsspielraum eingeräumt. Das Kreditinstitut kann danach auf die Heranziehung der Einkommensteuererklärung im Einzelfall verzichten, wenn aus dieser Unterlage keine weiteren Nachweise über die wesentlichen Einkünfte des Kreditnehmers vorliegen. Bei der - in jedem Fall vorzulegenden - Vermögensaufstellung kann das Institut im Einzelfall auf die Angabe einzelner Vermögenswerte verzichten, sofern sämtliche Verbindlichkeiten sowie etwaige Beteiligungen des Kreditnehmers angegeben sind und die dargelegten Vermögenspositionen im übrigen ein hinreichend verlässliches Bild über die Vermögenssituation des Kreditnehmers vermitteln.

Die BaFin weist auch darauf hin, dass es dem Kreditnehmer nicht verwehrt ist, einzelne Daten in den von ihm vorgelegten Unterlagen unkenntlich zu machen. Allerdings darf dadurch die Prüfung der Kreditwürdigkeit nicht beeinträchtigt werden. Das Kreditinstitut hat danach - unter Wahrung der Persönlichkeitsrechte der Kunden und datenschutzrechtlicher Bestimmungen - zu prüfen, ob die Angaben, welche den vom Kreditnehmer eingereichten Unterlagen zu entnehmen sind, für die Offenlegung der wirtschaftlichen Verhältnisse ausreichen.

Nach Auffassung der Aufsichtsbehörde müsste aus datenschutzrechtlicher Sicht grundsätzlich im Einzelfall geprüft werden, welche Unterlagen das Kreditinstitut konkret zur Durchführung der Prüfung nach § 18 KWG benötigt. Nur so kann letztlich vermieden werden, dass das Kreditinstitut ein Zuviel an Daten erhält. Lediglich in den Fällen, in denen eine Heranziehung der Steuerklärung bzw. einer kompletten Vermögensaufstellung zur Durchführung der Prüfung tatsächlich erforderlich ist, darf die Vorlage dieser Unterlagen auch vom Kunden verlangt werden. Ein derartiges Prüfungsverfahren würde jedoch auf Grund der Vielzahl der betroffenen Fälle zu einem nicht unerheblichen Arbeitsaufwand bei den Kreditinstituten führen.

Ein aus Sicht der Aufsichtsbehörde erster Schritt zur Sicherstellung der datenschutzrechtlichen Anforderungen könnte daher so aussehen, dass das Kreditinstitut seine Kunden im Aufforderungsschreiben auf die Möglichkeit hinweist, dass sie den Umfang der für die Prüfung nach § 18 KWG erforderlichen Daten mit ihrem Kundenberater vorab klären können. Das Anschreiben sollte zudem einen Hinweis darauf enthalten, dass insbesondere bei Steuerbescheiden oder Steuererklärungen solche persönlichen Daten unkenntlich gemacht werden können, die für die Prüfung des Kreditinstituts offensichtlich ohne Bedeutung sind, wie etwa die Konfession oder Adressaten von Parteispenden. So hätten alle angeschriebenen Kunden die Möglichkeit, den Umfang der Datenerhebung in ihrem Fall auf das erforderliche Maß zu reduzieren. Diese Anregung wurde auch bereits von einem größeren Kreditinstitut aufgegriffen. Andere werden diesem Beispiel folgen.

Die BaFin hat vor kurzem mitgeteilt, dass sie zukünftig auf detaillierte Auslegungsregelungen zu § 18 KWG verzichten wolle. Die bisher zu dieser Vorschrift veröffentlichten Rundschreiben seien mit sofortiger Wirkung aufgehoben. Ab sofort sei es Sache der Kreditinstitute, selbst auf der Grundlage ihrer Geschäftstätigkeit Kriterien zur Sicherstellung der umfassenden Beurteilung der Ausfallrisiken bei den von ihnen vergebenen Krediten zu entwickeln und hierfür auch die erforderlichen organisatorischen Vorkehrungen zu treffen.

Durch die Streichung der detaillierten aufsichtsrechtlichen Vorgaben wird den Kreditinstituten die eigenverantwortliche Wahrnehmung der sich aus § 18 KWG ergebenden Pflichten übertragen. An der Beachtung der dargestellten datenschutzrechtlichen Anforderungen bei der Prüfung nach § 18 KWG ändert dies jedoch nichts. Die weitere Entwicklung in diesem Punkt bleibt abzuwarten.

3.2 Übermittlung von Spenderdaten

Verschiedene wohltätige Organisationen rufen immer wieder über die Medien dazu auf, für bestimmte Zwecke, wie z.B. die Flutkatastrophe in Asien, zu spenden. Dabei kommt es vor, dass Spender auf dem Überweisungsträger, mit dem sie den entsprechenden Betrag überweisen, ihren Namen und ihre Anschrift nicht angeben oder eine Zuordnung der gespendeten Summe zu ihrer Person aus anderen Gründen nicht möglich ist. In diesen Fällen hat die Organisation, die den Spendenaufruf gestartet hat, keine Möglichkeit, mit dem Spender in Kontakt zu treten, um diesem zu danken, eine Spendenbescheinigung auszustellen oder für zukünftige Spendenaktionen zu werben.

Diesem Problem wollte ein Marketingunternehmen abhelfen und trat mit einer Geschäftsidee an die Aufsichtsbehörde heran. Die wohltätige Organisation sollte danach die zu dem Spender bekannten Bankdaten (Bankleitzahl, Kontonummer) an ein externes Unternehmen (z. B. ein großes Energieversorgungsunternehmen) geben, dem selbst ein umfangreicher Bestand an Daten zu einem großen Personenkreis zur Verfügung steht. Dieses sollte dann die bekannten Daten zu dem Spender mit den vorhandenen Daten abgleichen, einem Namen und einer Anschrift zuordnen und dies der Organisation mitteilen. Diese wäre dann in der Lage, Kontakt zu dem Spender aufzunehmen.

Die Aufsichtsbehörde hielt dieses Vorhaben für datenschutzrechtlich unzulässig. Bereits für die Übermittlung personenbezogener Daten von der Organisation an das eingeschaltete externe Unternehmen gibt es keine Rechtsgrundlage. Es war hier eine Abwägung der berechtigten Interessen der wohltätigen Organisation auf der einen Seite und der schutzwürdigen Interessen der Spender andererseits vorzunehmen, die im Ergebnis zu Gunsten der Spender ausfiel.

Als berechtigte Interessen der Organisation kamen die gewünschte Kommunikation mit dem Spender, die Möglichkeit, diesem zu danken, die Betreuung des Spenders auch im Hinblick auf die zukünftige Spendenbereitschaft sowie die Kostenersparnis eines solchen Verfahrens im Vergleich zum Vorgehen mittels eines Nachforschungsauftrags bei der Bank in Betracht. Als überwiegende schutzwürdige Interessen des jeweiligen Spenders hingegen wurden sein Interesse, der Organisation seinen Namen und seine sonstigen Daten nicht mitzuteilen und somit als Spender anonym bleiben zu können, sowie der Wunsch, von der Organisation nicht regelmäßig beworben zu werden, angesehen. Ein Spender hätte andernfalls keine Möglichkeit mehr, einer Organisation eine anonyme Spende zukommen zu lassen, da er stets

damit rechnen müsste, dass seine persönlichen Daten von ihr ermittelt werden können. Wünscht ein Spender dagegen die Kontaktaufnahme durch die Organisation, so hat er die Möglichkeit, seinen Namen samt Adresse auf dem Überweisungsträger anzugeben oder aber sich unmittelbar an die Organisation zu wenden, um so gegebenenfalls eine Spendenbescheinigung zu erhalten.

Das Ergebnis der datenschutzrechtlichen Bewertung wurde dem anfragenden Unternehmen mitgeteilt, das seine Geschäftsidee danach nicht weiterverfolgte.

3.3 Datenübermittlung aus Bausparverträgen

Überrascht war der Kunde einer Bausparkasse, als er von einem Immobilienbüro ein Angebot erhielt, die Verwaltung seiner Wohnung zu übernehmen. Wie sich herausstellte, hatte die Bausparkasse dem Immobilienbüro Name und Anschrift ihres Kunden sowie Ort und Größe der ihm gehörenden Wohnung mitgeteilt, die sich in einer Wohnanlage mit mehreren Wohnungen befand.

Die Bausparkasse hatte diese Daten ohne Zustimmung der Bewohner der Wohnanlage weitergegeben, da sie ein Interesse daran hatte, dass das Immobilienbüro die Wohnungsverwaltung übernahm. Hintergrund hierfür war, dass die dort befindlichen Wohnungen als Sicherheiten für durch sie finanzierte Darlehen bestellt worden waren. Die Darlehensverträge enthielten überdies eine Verpflichtung des Darlehensnehmers, einer Mieteinnahmegemeinschaft (Mietpool) beizutreten.

Um die Gefahr ausbleibender Mieten bei Leerstand von Wohnungen zu verringern, mussten die Eigentümer die Mieteinnahmen in einen Pool einbringen. Dieser wurde von einem Verwalter betreut, der die Einnahmen zunächst sammelte und dann anschließend entsprechend der Größe der einzelnen Wohnungen auf alle Mietpoolteilnehmer verteilte. Eine wesentliche Aufgabe des Mietpoolverwalters war es auch, dafür zu sorgen, dass die im Bestand des Pools befindlichen Wohnungen möglichst vollzählig und gut vermietet waren, da dies die Ausschüttungsquote des Mietpools verbesserte.

Da die Bausparkasse mit der bisherigen Mietpoolverwaltung schon seit längerem unzufrieden war und damit ein anderes Unternehmen betrauen wollte, gab sie die Daten der betroffenen Wohnungseigentümer an das Immobilienbüro weiter, damit dieses an die Eigentümer herantreten konnte.

Die Bausparkasse übermittelte zu Unrecht Daten der Kunden an das Immobilienbüro. Sie hatte diese Daten ursprünglich zum Zweck der Durchführung des Bausparvertrags erhoben und gespeichert. Die Datenweitergabe an das Immobilienunternehmen geschah aber zu dem Zweck, die Verwaltung des Mietpools einem neuen Unternehmen zu übertragen. Die Datenübermittlung war damit nicht mehr vom ursprünglichen Zweck der Datenerhebung und Datenspeicherung gedeckt. Auch auf eine andere Rechtsgrundlage konnte sich die Bausparkasse hier nicht stützen. Insbesondere eine vom BDSG geforderte Abwägung der berechtigten Interessen der Bausparkasse einerseits und der schutzwürdigen Interessen des Kunden andererseits ergab, dass letztere hier überwogen. Zwar war das Interesse der Bausparkasse an der Sicherung der Zahlungsfähigkeit seiner Vertragspartner anzuerkennen. Zweifelhaft war jedoch, ob die Übermittlung der Daten erforderlich war, um das beabsichtigte Ziel zu erreichen. Dies war nach unserer Auffassung hier nicht der Fall, da sich die Bausparkasse ohne großen zeitlichen Aufwand selbst an ihre Kunden hätte wenden und diese entsprechend informieren sowie deren Einverständnis zur Datenweitergabe an das Immobilienbüro einholen können. Nach der eigenen Darstellung der Bausparkasse bestand die Unzufriedenheit mit der bisherigen Hausverwaltung bereits seit längerer Zeit. Hätten sich die Kunden gegen eine Datenweitergabe entschieden, hätte eine solche nicht erfolgen dürfen. In diesem Fall wäre aber auch ein Anschreiben des Immobilienbüros mit der Bitte um Übertragung der Hausverwaltung erfolglos gewesen. Im Übrigen konnten hier auch schutzwürdige Interessen der Kunden der Bausparkasse angenommen werden. Die Kunden vertrauen in aller Regel darauf, dass Daten, die im Rahmen eines Vertragsverhältnisses erhoben werden, nicht für andere Zwecke verwendet und insbesondere nicht an Dritte weitergegeben werden. Es ist auch nicht davon auszugehen, dass ein Kunde mit einer Datenübermittlung zu einem anderen als dem ursprünglichen Vertragszweck ohne weiteres einverstanden ist.

Wir haben der Bausparkasse unsere datenschutzrechtliche Bewertung mitgeteilt und sie aufgefordert, zukünftig in gleich gelagerten Fällen datenschutzrechtlich korrekt vorzugehen, d.h. vor etwaigen Datenübermittlungen eine Einwilligung des Betroffenen einzuholen. Die Bausparkasse hat dies zugesagt.

3.4 Sicherheit beim Telefonbanking

Ein Kunde einer Bank wandte sich an die Aufsichtsbehörde, nachdem seine Bank beim Telefonbanking das sichere Zugangsverfahren mit PIN (**P**ersönliche **I**dentifikations-**N**ummer) und deren Überprüfung mittels Sprachcomputer abgeschafft hatte. Am Telefon wurden von den Kunden zur Identitätsfeststellung nur noch Kontonummer, Adresse und das Geburtsdatum erfragt. Grund für die Verfahrensänderung war die

geringe Akzeptanz der Kunden, sich auch noch eine Telefon-PIN merken zu müssen. Da Kontonummer, Adresse und Geburtsdatum oftmals einem größeren Personenkreis zugänglich sind, bestand bei diesem Verfahren die Gefahr, dass sich Dritte Kenntnis von den Zugangsdaten verschaffen und dann über das Konto unbefugt verfügen können. Ein vom Betroffenen selbst initiierter Test verlief „erfolgreich“.

Bei der Datenverarbeitung in der Bank werden personenbezogene Daten automatisiert verarbeitet. Nach § 9 Satz 1 BDSG hat die Bank die Maßnahmen zu treffen, die erforderlich sind, um zu verhindern, dass ihre Datenverarbeitungssysteme von Unbefugten genutzt werden. Daher muss die Bank dafür Sorge tragen, dass ein unberechtigter Zugriff Dritter, der bei dem gewählten System ohne Zutun des Betroffenen erfolgen kann, unterbleibt.

Nach längeren Verhandlungen mit der Bank konnte erreicht werden, dass jeder Kunde ein geheimes, durch ihn änderbares Kennwort verwenden muss. Die Kennwörter werden in der Datenverarbeitungsanlage so gespeichert, dass die mit dem Telefonbanking betrauten Mitarbeiter nicht darauf zugreifen können, sondern bei der Eingabe nur erfahren, ob das Kennwort stimmt oder nicht. Ferner schließt die Bank mit den Kunden eine Vereinbarung über das Telefonbanking ab, in dem diese über die verbleibenden Risiken aufgeklärt werden und in das Verfahren schriftlich einwilligen müssen. Der sicherste Weg zur Identifizierung bleibt jedoch weiterhin das PIN-Verfahren unter Einsatz eines Sprachcomputers.

4 Versicherungswirtschaft

4.1 Schweigepflichtentbindungserklärung in der privaten Krankenversicherung

Der bei einer privaten Krankenversicherung Versicherte tritt in den meisten Fällen in Vorleistung und bezahlt die an ihn gerichteten Arzt-, Krankenhaus- und Apothekenrechnungen zunächst selbst. Danach reicht er diese Rechnungen bei seiner Versicherung ein und bittet um Erstattung der von ihm verauslagten Beträge. In der ganz überwiegenden Anzahl der Fälle werden diese von der Versicherung auch umgehend erstattet. In Einzelfällen kommt es jedoch vor, dass nach Auffassung der Krankenversicherung im Rahmen der Beurteilung ihrer Leistungspflicht eine Rückfrage bei dem behandelnden Arzt oder dem Krankenhaus erforderlich ist, dessen Rechnung erstattet werden soll. Es geht hier zumeist um Fragen der medizinischen Notwendigkeit der durchgeführten ärztlichen Behandlung.

Beantwortet der angefragte Arzt bzw. das Krankenhaus derartige Rückfragen, werden Gesundheitsdaten des Versicherten weitergegeben, die vom Gesetzgeber als besonders schützenswert angesehen werden und deren Erhebung, Verarbeitung und Nutzung besonders strengen Regelungen unterliegen.

Um derartige Anfragen durchführen zu dürfen, lassen sich die Krankenversicherungen bereits bei Abschluss des Versicherungsvertrags vom Versicherten eine entsprechende Schweigepflichtentbindungserklärung erteilen, mit der der behandelnde Arzt, andere Angehörige von Heilberufen oder Krankenanstalten, die in den vom Versicherten vorgelegten Unterlagen genannt sind oder die an der Heilbehandlung beteiligt waren, von ihrer (ärztlichen) Schweigepflicht entbunden werden. Durch Abgabe dieser Erklärung wird zugleich die Weitergabe der betreffenden Gesundheitsdaten an die Versicherung legitimiert. Diese Erklärung wird jedoch vom Versicherten nur einmalig und zwar im Rahmen der Antragstellung auf Abschluss eines Versicherungsvertrags abgegeben, hat aber nach bisheriger Praxis während des Bestehens des gesamten Vertragsverhältnisses Geltung. Nach dem Text der bislang verwendeten Schweigepflichtentbindungserklärung hat die Geltendmachung eines Leistungsanspruchs die Bedeutung einer Schweigepflichtentbindung für den Einzelfall. Vor einer Rückfrage bei einem Arzt oder Krankenhaus holt die Versicherung in aller Regel keine weitere Schweigepflichtentbindungserklärung ein.

Aus Sicht der Datenschutzaufsichtsbehörden ist bei diesem Verfahren insbesondere problematisch, dass der Versicherte im Moment der Abgabe der Schweigepflichtentbindungserklärung noch nicht überblicken kann, zu welchem Zeitpunkt welche Gesundheitsdaten von welcher Stelle (Arzt, Krankenhaus) an seine Krankenversicherung weitergegeben werden. Bei Abschluss des Vertrags ist dem Versicherten in aller Regel nicht bekannt, in welchem Umfang zukünftig ärztliche Behandlungen erforderlich sein werden.

Um das Verfahren im Rahmen der Leistungsprüfung der privaten Krankenversicherung datenschutzfreundlicher zu gestalten, hält eine deutliche Mehrheit der Mitglieder des Düsseldorfer Kreises, darunter auch das Innenministerium Baden-Württemberg, eine Änderung der Vorgehensweise für geboten. Künftig soll für jede Rückfrage von Krankenversicherungen bei Ärzten, anderen Angehörigen von Heilberufen oder Krankenanstalten wegen der Erstattung von Rechnungen die Einwilligung des Patienten eingeholt werden.

Dies wurde der Bundesärztekammer, der Bundeszahnärztekammer sowie dem Gesamtverband der Deutschen Versicherungswirtschaft (GDV) mitgeteilt. Letzterer teilt

die Auffassung der Datenschutzaufsichtsbehörden jedoch nicht und hält im Grundsatz an dem bisherigen Verfahren fest. Die weitere Entwicklung bleibt abzuwarten.

4.2 Datenweitergabeklauseln in Versicherungsverträgen

Vor dem Hintergrund der 2001 erfolgten Novellierung des BDSG führen die Datenschutzaufsichtsbehörden der Länder unter Mitwirkung des Innenministeriums Baden-Württemberg derzeit Verhandlungen mit dem GDV über eine Neufassung der 1994 zwischen den obersten Datenschutzaufsichtsbehörden und ihm abgestimmten Datenweitergabeklausel in Versicherungsverträgen sowie die Änderung des bisher praktizierten Verfahrens.

Mittels dieser Klausel willigt der Versicherungsnehmer bei Antragstellung in verschiedene Datenverarbeitungsvorgänge ein: In die Datenübermittlung an Rückversicherer sowie an andere Versicherer bzw. den GDV im Rahmen zentraler Warn- und Hinweissysteme, die Datenverarbeitung in gemeinsamen Datensammlungen in der Versicherungsgruppe, die Datenweitergabe an Vermittler sowie die Nutzung der Daten durch den Vermittler auch für die Beratung und Betreuung in sonstigen Finanzdienstleistungen. Die jeweiligen Datenverarbeitungsvorgänge werden in einem „Merkblatt zur Datenverarbeitung“ erläutert, das jedem Versicherungsnehmer ausgehändigt werden muss.

Ziel der Verhandlungen soll es sein, die Einwilligungsklausel für den Betroffenen so transparent zu gestalten, dass er bezogen auf jeden Sachverhalt überblicken kann, welche Konsequenzen mit der Erklärung verbunden sind. Die Klausel soll trotzdem möglichst knapp und klar gefasst sein. Das Verfahren zur Aushändigung des „Merkblatts zur Datenverarbeitung“ soll verbessert und das Merkblatt selbst in einzelnen Punkten verständlicher gefasst werden. Es bleibt zu hoffen, dass dieses Ziel in absehbarer Zeit erreicht werden kann.

4.3 Weitergabe von Gesundheitsdaten an den Versicherungsvermittler

Verärgert war eine Frau, als der sie betreuende Versicherungsvermittler sie anrief und versuchte, sie unter Hinweis auf die bei ihr diagnostizierte chronische Krankheit zum Abschluss eines neuen Krankenversicherungsvertrags zu bewegen. Vorausgegangen war ein von ihrem bisherigen Versicherer erklärter Rücktritt vom Versicherungsvertrag aufgrund einer Anzeigepflichtverletzung nach dem Versicherungsvertragsgesetz. Als Grund hierfür wurde eine chronische Krankheit genannt, die von der

behandelnden Ärztin der Frau festgestellt wurde und die bereits vor Abschluss des Vertrags bestand, bei Antragstellung von ihr aber nicht angegeben worden war.

Die Versicherung teilte der Frau in einem Schreiben den Rücktritt vom bestehenden Vertrag unter Angabe von Gründen mit. Ausdrücklich erwähnt wurde darin auch, um welche chronische Krankheit es sich handelt. Dieses Schreiben wurde in Kopie vollständig (d.h. ohne Schwärzung) an den Versicherungsvermittler der Frau weitergegeben. Dieser konnte so Kenntnis von der ärztlichen Diagnose erlangen.

Das Versicherungsunternehmen hatte hier - vom Gesetzgeber als besonders schützenswert erachtete - Gesundheitsdaten an den Versicherungsvermittler weitergegeben. Dies war datenschutzrechtlich unzulässig.

Diese Datenübermittlung konnte nicht auf die von der Versicherungsnehmerin bei Abschluss des Versicherungsvertrags erteilte datenschutzrechtliche Einwilligungserklärung gestützt werden. Darin heißt es: „Gesundheitsdaten dürfen nur an Personen - und Rückversicherer übermittelt werden; an Vermittler dürfen sie nur weitergegeben werden, soweit es zur Vertragsgestaltung erforderlich ist.“ Der entsprechende Passus im erläuternden „Merkblatt zur Datenverarbeitung“ lautet: „Ausschließlich zum Zweck von Vertragsanpassungen in der Personenversicherung können an den zuständigen Vermittler auch Gesundheitsdaten übermittelt werden.“

Grund für die Datenübermittlung war hier die Mitteilung der Beendigung des Vertragsverhältnisses mit der Versicherungsnehmerin und nicht eine erforderliche Anpassung ihres Versicherungsvertrags. Die Datenübermittlung war auch nicht zur Vertragsgestaltung erforderlich. Es hätte hier ausgereicht, wenn die Versicherung den Versicherungsvermittler über den Rücktritt vom Versicherungsvertrag und den Grund hierfür (Verletzung der Anzeigepflicht) informiert hätte. Die Information, welche Krankheit bei der Versicherungsnehmerin diagnostiziert wurde, war für die Tätigkeit des Versicherungsvermittlers unerheblich. Auch auf eine andere Rechtsgrundlage als die Einwilligung konnte die Datenübermittlung nicht gestützt werden.

Wir haben der Versicherung unsere datenschutzrechtliche Bewertung in dieser Angelegenheit mitgeteilt und sie aufgefordert, zukünftig sicherzustellen, dass bei der Übermittlung von Gesundheitsdaten an Vermittler die datenschutzrechtlichen Vorgaben beachtet werden. Die Versicherung hat dies bestätigt und eine Löschung der Gesundheitsdaten beim Vermittler veranlasst.

4.4 Sperrung von Daten wegen Rücknahme eines Versicherungsantrags

Eine Frau hatte ihren ursprünglichen Antrag auf Abschluss einer Berufsunfähigkeitsversicherung zurückgenommen und verlangte nun, da kein Vertrag zustande gekommen war, von der Versicherung die Löschung der zu ihrer Person gespeicherten Daten. Dabei handelte es sich insbesondere um einen von ihr ausgefüllten Fragenbogen zu ihrem Gesundheitszustand. Da die Versicherung die von ihr begehrte Löschung nicht vornahm, wandte sie sich an die Aufsichtsbehörde.

Da ein Versicherungsvertrag in diesem Fall nicht zustande gekommen ist, bestand grundsätzlich ein Anspruch auf Löschung der personenbezogenen Daten der Betroffenen. An die Stelle einer Löschung tritt jedoch eine Sperrung der Daten, soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen. Eine Löschung wäre dann sogar unzulässig. Im vorliegenden Fall war eine gesetzliche Aufbewahrungsfrist aus dem Handelsgesetzbuch zu wahren. Danach ist jeder Kaufmann dazu verpflichtet, u.a. die empfangenen Handelsbriefe für die Dauer von sechs Jahren aufzubewahren. Dazu gehören Schriftstücke, die die Vorbereitung, den Abschluss, die Durchführung oder die Rückgängigmachung eines Handelsgeschäfts zum Gegenstand haben. Diese gesetzlich vorgeschriebene Aufbewahrung der Unterlagen dient der Dokumentation und erlaubt Nachprüfungen, Beweissicherungen und Beweisführungen. Weitere gesetzliche Aufbewahrungsfristen enthält z.B. die Abgabenordnung.

Die Versicherung war daher im konkreten Fall verpflichtet, sämtliche Unterlagen aufzubewahren bzw. die Daten zu speichern, die hinsichtlich des von der Betroffenen gestellten und später zurückgenommenen Antrags auf Abschluss einer Berufsunfähigkeitsversicherung dort vorlagen. Diese Daten waren jedoch zu sperren und entsprechend zu kennzeichnen. Nach Ablauf der Aufbewahrungsfrist müssen sie gelöscht werden.

Die Versicherung bestätigte uns gegenüber, dass die Daten zur Betroffenen gesperrt wurden und damit nur noch eingeschränkt, nämlich für Zwecke der externen Kontrolle durch Finanzbehörden, verwendet werden dürfen. Zugesagt wurde uns auch, dass die Daten nach Ablauf der gesetzlichen Aufbewahrungsfrist in der Versicherungsdatenbank gelöscht werden.

4.5 Datenerhebung bei Reiserücktrittsversicherung

Ein Arzt wandte sich an die Aufsichtsbehörde, weil ihn eine Patientin darum gebeten hatte, die Diagnose der Krankheit, die zum Nichtantritt der geplanten Reise geführt hatte, in eine Bescheinigung für die Reiserücktrittskostenversicherung einzutragen.
Die Versicherung hatte dies von ihr verlangt. Nach Auffassung des Arztes war dieses Ansinnen der Versicherung mit dem Datenschutz nicht vereinbar. Ausreichend sei es in diesen Fällen, wenn der Arzt bescheinige, dass der Patient sich in einem Krankheitszustand befindet, in dem er die gebuchte Reise nicht antreten kann. Die Mitteilung der exakten Diagnose sei nicht erforderlich.

In der Reiserücktrittskostenversicherung entsteht die Leistungspflicht des Versicherers dann, wenn infolge eines wichtigen Grundes entweder die Reiseunfähigkeit des Versicherten nach allgemeiner Lebenserfahrung zu erwarten ist oder ihm der Antritt der Reise nicht zugemutet werden kann. Solche wichtigen Gründe sind: Tod, schwerer Unfall oder unerwartete schwere Erkrankung des Versicherten bzw. naher Angehöriger. Dem Versicherer muss die Prüfung seiner Leistungspflicht ermöglicht werden. Ob die Voraussetzungen im Einzelnen vorliegen, kann der Versicherer in der Regel nicht lediglich anhand der Aussage des behandelnden Arztes, „dass der Patient sich in einem Krankheitszustand befindet, der eine Reise nicht ermöglicht“, entscheiden. Erforderlich ist ein ärztliches Attest, dem der Versicherer entnehmen kann, ob es sich typischerweise um eine unerwartete Erkrankung handelt, die einen gewissen Schweregrad erreicht hat und bis zum Antritt der Reise dauern wird. Um Zweifelsfragen direkt durch Rückfragen beim Arzt klären zu können, ist eine vom Patienten erteilte Schweigepflichtentbindungserklärung erforderlich.

Der insoweit bedeutsame Teil der mit den Datenschutzaufsichtsbehörden abgestimmten Schweigepflichtentbindungserklärung in Schadensfällen bei der Reiserücktrittskostenversicherung lautet wie folgt: „Mir ist bekannt, dass der Versicherer zur Beurteilung seiner Leistungspflicht Angaben überprüft, die ich zur Begründung meines Anspruchs mache. Zu diesem Zweck befreie ich die Angehörigen von Heilberufen oder Krankenanstalten, die in den von mir vorgelegten Unterlagen genannt sind oder die an der Heilbehandlung beteiligt waren, von ihrer Schweigepflicht - und zwar auch über meinen Tod hinaus.“

Die Pflicht zur Offenbarung von Gesundheitsdaten geht damit - wie im vorliegenden Fall - möglicherweise über das von dem jeweils behandelnden Arzt für richtig gehaltene Maß hinaus. Das Informationsverlangen der Versicherung muss jedoch vom Gegenstand und vom Umfang her den Erforderlichkeitsgrundsatz beachten. Tut es

das nicht, ist der befragte Arzt gehalten, beim Patienten abzuklären, ob dessen Daten an die Versicherung übermittelt werden dürfen.

4.6 Hinweissystem der Rechtsschutzversicherer

Damit Rechtsschutzversicherer die Möglichkeit haben, die Angaben zu Vorversicherungen bei der Antragstellung zu überprüfen, wurde beim GDV ein zentrales Hinweissystem der Rechtsschutzversicherer eingerichtet. Folgende Tatbestände führen dazu, dass durch den Rechtsschutzversicherer eine Meldung in dieses zentrale Hinweissystem erfolgt:

- vorzeitige Kündigung und Kündigung zum normalen Vertragsablauf durch den Versicherer nach mindestens zwei Versicherungsfällen innerhalb von 12 Monaten, oder
- Kündigung zum normalen Vertragsablauf durch den Versicherer nach mindestens drei Versicherungsfällen innerhalb von 36 Monaten, oder
- vorzeitige Kündigung und Kündigung zum normalen Vertragsablauf bei konkret begründetem Verdacht einer betrügerischen Inanspruchnahme der Versicherung.

Bei Vorliegen eines dieser Tatbestände werden von dem kündigenden Versicherungsunternehmen nur Name, Anschrift, Geburtsdatum und die Nummer des Versicherungsscheins in das zentrale Hinweissystem gemeldet, nicht jedoch die einzelnen Versicherungsfälle. Diese Eintragungen werden im zentralen Hinweissystem fünf Jahre nach der Einspeicherung gelöscht. Wenn nun eine Versicherung zu einem Antrag eine Risikoprüfung durchführen will, erhält sie aus dem zentralen Hinweissystem nur die Information, ob zu dem Antragsteller eine Eintragung vorhanden ist und wenn ja, wer der Vorversicherer war. Die Angaben, die im Rahmen der Risikoprüfung erforderlich sind, werden daraufhin in der Regel telefonisch beim Vorversicherer erfragt.

Immer wieder wird der Aufsichtsbehörde vorgetragen, dass der Vorversicherer im Rahmen der Risikoprüfung alle während des gesamten Versicherungsverlaufs angefallenen Versicherungsfälle an den Nachversicherer bekannt gegeben habe. Von den beteiligten Versicherern wurde dies regelmäßig als zutreffend eingeräumt. Auf Grund des telefonischen Verfahrens wurde aber bisher nicht festgehalten, wer an wen eine Auskunft erteilt hat und in welchem Umfang Daten übermittelt wurden. Die beteiligten Versicherungsunternehmen wurden aufgefordert, dies zukünftig nachvollziehbar festzuhalten.

Zur Datenübermittlung des Vorversicherers an andere Versicherer ist festzustellen, dass die Betroffenen in der Regel über die Datenschutzklausel im Versicherungsvertrag unter anderem darin eingewilligt haben, dass der Versicherer Daten, die sich aus der Vertragsdurchführung (Versicherungsfälle) ergeben, zur Beurteilung des Risikos im erforderlichen Umfang an andere Versicherer übermittelt. Zur Wahrung berechtigter Interessen der Versichertengemeinschaft des Nachversicherers ist es zweifellos erforderlich, bei Antragstellung die Angaben zur Vorversicherung zu überprüfen und dazu vom Vorversicherer bestimmte Daten zu dem potentiellen Neukunden zu erhalten. Die Datenübermittlung ist jedoch nur im erforderlichen Umfang zulässig. Dieser ist durch die schutzwürdigen Interessen des Betroffenen begrenzt. Die Aufsichtsbehörde ist der Auffassung, dass zumindest hinsichtlich der Daten, die eine Einmeldung in das zentrale Hinweissystem bewirken, kein schutzwürdiges Interesse eines Betroffenen vorliegt. Bei Datenübermittlungen, die darüber hinausgehen, weil die Kenntnis der Daten für den Nachversicherer zur Risikobeurteilung erforderlich ist, dürfen jedoch keine Umstände zur Grundlage einer Risikobeurteilung gemacht werden, die keine Aussagekraft mehr haben. Die Speicherdauer von fünf Jahren im zentralen Hinweissystem wird von den Aufsichtsbehörden für den Datenschutz sowohl für die Interessenlage der Nachversicherer als auch der Betroffenen als ausreichend und angemessen angesehen. Daher dürften die in den zurückliegenden fünf Jahren angefallenen Daten für die Auskunftserteilung zur Risikobeurteilung durch den Nachversicherer grundsätzlich ausreichen. Im Einzelfall kann auch noch weiter zurückliegenden Daten eine Aussagekraft beigemessen werden. Mehr als zehn Jahre dürfen die Daten jedoch auf keinen Fall zurückreichen.

4.7 Fusion innerhalb einer Versicherung

Ein Versicherungsunternehmen kam im Jahr 2004 auf die Aufsichtsbehörde zu und bat um Beratung im Vorfeld einer Fusion. Zwei bislang regional ausgerichtete konzernangehörige Unternehmen sollten insgesamt zu einer Aktiengesellschaft verschmolzen werden. Dadurch ergaben sich auch datenschutzrechtliche Fragen. Die in den bestehenden Verträgen enthaltene Einwilligungsklausel musste an die neuen Unternehmensverhältnisse angepasst und aktualisiert werden. Dies betraf insbesondere den Teil der Klausel, der die „Datenübermittlung zur Beratung und Betreuung in sonstigen Finanzdienstleistungen“ zum Gegenstand hat. Mittels dieser 1995 im Grundsatz zwischen den Datenschutzaufsichtsbehörden der Länder und dem GDV abgestimmten Klausel willigt der Versicherungsnehmer - allerdings bei jederzeitiger freier Widerrufsmöglichkeit - darin ein, dass ein Vermittler, aber auch etwaige Partnerunternehmen aus dem Verbund, die allgemeinen Antrags-, Vertrags- und Lei-

stungsdaten (z.B. Personalien und bestimmte Daten über Versicherungsverträge) für die Beratung und Betreuung auch in sonstigen Finanzdienstleistungen nutzen dürfen.

Weil der Text der ursprünglich bei Vertragsschluss erteilten Einwilligung und des der Erläuterung dienenden „Merkblatts zur Datenverarbeitung“ geändert werden musste, war eine Vielzahl bestehender Versicherungsverträge betroffen. Es stellte sich nun die Frage, ob in sämtlichen Fällen erneut eine ausdrückliche schriftliche Einwilligung der Versicherungsnehmer hinsichtlich der genannten Datenübermittlungen eingeholt werden musste oder ob hier mit einer Widerspruchslösung gearbeitet werden konnte.

Die Aufsichtsbehörde erachtete in diesem Fall - ebenso wie bereits in früheren Fällen - wegen der besonderen Umstände eine Ausnahme vom Grundsatz der Schriftlichkeit der datenschutzrechtlichen Einwilligung für angemessen (§ 4a Abs. 1 Satz 3 BDSG). Es genügte, dass die Versicherung ihren Versicherungsunternehmern mitteilte, dass für den Versicherungsbestand eine einheitliche Einwilligungserklärung gelten soll und ihnen hiergegen ein Widerspruchsrecht einräumte.

Angesichts der Vielzahl der betroffenen Verträge beeinträchtigt die gewählte Widerspruchslösung nach Auffassung der Aufsichtsbehörde die Betroffenen nicht in unangemessener Weise. Wir forderten jedoch von dem Unternehmen, dass es den Versicherungsnehmern die sich durch die Fusion ergebenden Änderungen auch in datenschutzrechtlicher Hinsicht transparent darstellt und erläutert. Die textlichen Änderungen im „Merkblatt zur Datenverarbeitung“ sollten im einzelnen optisch hervorgehoben werden. Besonders wichtig war uns, dass die Betroffenen deutlich auf ihr Widerspruchsrecht und die Möglichkeit, etwaige Widersprüche auch telefonisch einlegen zu können, hingewiesen werden.

Sämtliche Forderungen wurden umgesetzt. Das Unternehmen hat sich auch verpflichtet, eingehende Widersprüche im jeweiligen Datensatz des Versicherungsnehmers zu vermerken und allen Versicherungsnehmern, die einen Widerspruch eingelegt haben, eine Bestätigung darüber zukommen zu lassen.

Positiv zu bemerken ist, dass trotz der Vielzahl betroffener Versicherungsnehmer die Zahl der bei der Aufsichtsbehörde eingegangenen Beschwerden über diese Vorgehensweise vergleichsweise gering war. Dies spricht dafür, dass sich die Beratung durch die Aufsichtsbehörde in diesem Fall sowohl für das Versicherungsunternehmen als auch für die betroffenen Kunden gelohnt hat.

5 Internet und Medien

5.1 Speicherung von Nutzerdaten durch Internetinhaltsanbieter

Im Wege der anlassunabhängigen Aufsichtsprüfung wurde eine größere Anzahl von Internetinhaltsanbietern von der Aufsichtsbehörde überprüft. Es handelte sich sowohl um Tele- als auch um Mediendienste.

Neben der Überprüfung des Umgangs mit den Bestands- und Nutzungsdaten der Kunden (Nutzer) lag der Schwerpunkt bei der Kontrolle, ob die IP-Adresse des Nutzers über die Verbindung hinaus gespeichert wird. Die IP-Adresse ist die „Anschlussnummer“ eines jeden Internetnutzers. Auch wenn dem Nutzer vom Zugangsanbieter bei jeder Einwahl eine neue IP-Adresse zugeteilt wird (sogenannte dynamische Adressierung), ist diese ein personenbeziehbares Datum, da der Zugangsanbieter mit Hilfe seiner Protokolldateien feststellen kann, welche IP-Adresse er wann welchem Nutzeranschluss zugeteilt hat.

Nutzungsdaten fallen beim Bewegen im Internet oftmals zwangsläufig an und werden teilweise auch benötigt, um den laufenden Internetverkehr aufrechtzuerhalten. Nach den Datenschutzbestimmungen des Teledienste- und Mediendiensterechts dürfen die Nutzungsdaten, wozu auch die IP-Adresse gehört, über das Ende des Nutzungsvorgangs hinaus nur zu

- Zwecken der Abrechnung des Tele- oder Mediendienstes, sowie bei
- Verdacht auf Entgeltverkürzung bei der Nutzung des Tele- oder Mediendienstes,

ferner nach dem BDSG

- zur Gewährleistung der Datensicherheit, wenn die Erforderlichkeit in einer Datenschutzkonzeption begründet wird,

gespeichert werden.

Nutzungsdaten, die für diese Zwecke nicht benötigt werden, sind sofort zu löschen. Nutzungsdaten, die für diese Zwecke zulässigerweise gespeichert werden, sind für eine Verwendung zu anderen Zwecken zu sperren. Werden dagegen Nutzungsdaten gespeichert, um mit ihrer Hilfe die Bezahlung von über das Internet gemachten Bestellungen abzusichern, geht dies über das Teledienstrecht hinaus. Es ist dazu die Einwilligung des Betroffenen erforderlich.

Ergebnis der Überprüfung war, dass sich die Anbieter zwar bemühen, den Datenschutz einzuhalten, keiner jedoch völlig fehlerfrei arbeitet. Festgestellt wurde ferner,

dass die IP-Adressen der Nutzer von jedem Anbieter zumindest in Protokolldateien gespeichert wurden, wobei einige Anbieter von der Speicherung gar nichts wussten, da ihr DV-System von einem Systemhaus eingerichtet und gewartet wird. Nicht bekannt war zum Teil, dass auch eine Speicherung in einer Protokolldatei eine echte Datenspeicherung ist.

Die datenschutzrechtliche Bewertung der Überprüfungen fand Eingang in den Hinweis Nr. 41 des Innenministeriums vom 28. Juni 2004 (www.im.baden-wuerttemberg.de Rubrik: Datenschutz/weitere Infos/Infomaterial).

5.2 Ahnenforschung im Internet

Immer wieder kommt es im Bereich der Ahnenforschung zu Eingaben. Vielfach sind es Ahnenforscher, die wissen wollen, was sie veröffentlichen dürfen. Manchmal beschweren sich jedoch auch Betroffene, die eine Veröffentlichung ihrer Daten oder von Daten ihrer Vorfahren nicht wünschen. Zumeist geht es um die Veröffentlichung von Daten im Internet.

Hier ist zunächst zu klären, ob der Ahnenspiegel einer Familie oder die Ortschronik überhaupt personenbezogene Daten enthält. Soweit es um Daten Verstorbener geht, ist dies zu verneinen. Zwar ist die Würde des Menschen (Art. 1 Abs. 1 GG) auch nach seinem Tod zu respektieren, auch gelten einzelne spezialgesetzliche Bestimmungen, z.B. das Arztgeheimnis, über den Tod hinaus. Das Persönlichkeitsrecht (Art. 2 Abs. 1 GG) erlischt jedoch mit dem Tod. Daher ist auch eine Ausdehnung des BDSG über den Tod hinaus nicht gerechtfertigt.

Ist jedoch eine lebende Person durch sie beschreibende Merkmale, beispielsweise Vorname, Nachname, Wohnort, aber auch über Vorfahren, identifizierbar, handelt es sich um personenbezogene Daten. Diese dürfen veröffentlicht werden, wenn sie allgemein zugänglich sind. Das sind beispielsweise Daten, die dem Telefonbuch, dem Adressbuch oder der Presse entnommen oder von jedermann ohne Zugangsvoraussetzung aus einem Register erhoben werden können. Name, Vorname und Anschrift einer Person können ohne weiteres im Wege einer sogenannten einfachen Melderegisterauskunft bei der Meldebehörde erfragt werden, sind also allgemein zugänglich. Weitere Daten können aus dem Melderegister oder aus Personenstandsbüchern hingegen nur bei Vorliegen eines berechtigten oder gar eines rechtlichen Interesses in Erfahrung gebracht werden. Gleiches gilt beispielsweise für das Grundbuch.

Allgemein zugängliche Daten dürfen jedoch dann nicht veröffentlicht werden, wenn das schutzwürdige Interesse des Betroffenen an der Nichtveröffentlichung das berechtigte Interesse des Ahnenforschers offensichtlich überwiegt. Davon ist bei einer Veröffentlichung im Internet auszugehen, weil hier die Daten durch den Einsatz von Suchmaschinen weltweit abrufbar und beliebig auswertbar und verarbeitbar sind. Die Daten lebender Personen dürfen daher nur mit deren Einwilligung im Internet veröffentlicht werden.

Hingegen ist die Veröffentlichung einer Ortschronik in Buchform zulässig, wenn die personenbezogenen Daten allgemein zugänglich sind oder die Betroffenen eingewilligt haben.

5.3 PHISHING

Dass das Internet ein für jedermann offenes Netz ist, bemerkt man spätestens, wenn man selbst im Internet surft. Dort tummeln sich neben seriösen Anbietern auch solche, die versuchen, Schaden anzurichten. Sie löschen, verändern oder missbrauchen geschützte Datenbestände oder Programme.

Viele PC-Anwender sind sich der Gefahren, die tagtäglich im Internet, beim E-Mail-Verkehr oder auch beim Einlegen einer fremden Diskette oder CD-ROM auftreten können, gar nicht oder zu wenig bewusst. Ein Antivirus-Programm allein reicht oftmals nicht mehr aus, um den PC und das PC-Netzwerk ausreichend und wirkungsvoll zu schützen. Angefangen von hinterlassenen Surfspuren über Cookies bis hin zu Spionage-Attacken aus dem Internet - die Angriffsmöglichkeiten sind ausgesprochen raffiniert und vielfältig. Vor allem Privatanwender sowie kleinere und mittlere Betriebe mit unzureichenden Sicherheitsvorkehrungen sind gefährdet. Die Angriffe nehmen immer mehr zu. Deshalb ist es wichtig, den PC oder das PC-Netzwerk, der bzw. das mit dem Internet verbunden ist, zumindest mit einer Virensoftware und einer Firewall zu betreiben und diese regelmäßig auf dem aktuellsten Stand zu halten. In unserem ersten Tätigkeitsbericht haben wir ausführlich Maßnahmen zum Schutz vor Angriffen aus dem Internet dargestellt (vgl. dort S. 30 ff.).

Es gibt aber auch Bedrohungsarten, die nicht durch eine Virensoftware oder Firewall behoben werden können. Hierzu gehört beispielsweise das PHISHING. Der Begriff kommt aus dem Englischen und bedeutet übersetzt so viel wie „nach Passwörtern oder Zugangsdaten fischen“. Der PHISHING-Betrüger erstellt eine E-Mail, die so echt gestaltet ist, dass der Empfänger der Auffassung ist, diese komme von seiner Bank oder einem ihm bekannten Unternehmen. Der Betrüger fordert mit dieser so getarn-

ten E-Mail den Betroffenen auf, seine Daten zu aktualisieren bzw. zu verifizieren. Dafür ist in der E-Mail gleich der Link der entsprechenden Internet-Seite mit angegeben. Ein Klick darauf und schon ist man auf einer gefälschten Internet-Seite. Diese ist wie die E-Mail so echt gestaltet, dass der Kunde den Eindruck gewinnt, er befinde sich auf der Internet-Darstellung seiner Hausbank oder des ihm bekannten Unternehmens. Hinter diesem Link verbirgt sich aber eine ganz andere Internet-Adresse, in der Regel eine Internet-Adresse, die nicht in Deutschland oder der EU registriert ist. Auf den ersten Blick erscheint aber alles wie gewohnt. Gibt der Kunde jetzt wie gefordert seine Kreditkartennummer, seine EC-Geheimnummer, sein Passwort und andere Kontendaten ein, freut sich der „Angler“ am anderen Ende. Auf diese Weise kann er beispielsweise das Bankkonto des Kunden mit Hilfe eines Überweisungsauftrags an eine fremde Bank oder durch Abheben leer räumen. Den finanziellen Schaden hat der Kunde, weil er ja seine PIN- bzw. TAN-Nummer eingegeben hat. Eine Rücküberweisung ist in den meisten Fällen nicht möglich, da das fremde Konto nur für eine kurze Zeit eröffnet wird und dazu unter einem fremden Namen.

Man kann deshalb nur zu größter Vorsicht mahnen. Derartige per E-Mail eingehende Ansinnen sollten sofort gelöscht werden. Banken und seriöse Unternehmen werden ihre Kunden auf keinen Fall über das Internet nach geheimen Zugangsdaten fragen.

6 Gesundheitswesen

6.1 Neuordnung der Krebsregistrierung in Baden-Württemberg

Neben dem Landesbeauftragten für den Datenschutz berät die Aufsichtsbehörde, die für die niedergelassenen Ärzte und die Krankenhäuser in Privatrechtsform zuständig ist, das Sozialministerium bei der Neuordnung der Krebsregistrierung in Baden-Württemberg. Diese ist notwendig, weil das bisherige epidemiologische Krebsregister keine verwertbaren Daten geliefert hat. Gründe dafür sind eine unbefriedigende Meldequote der meldeberechtigten Ärzte und Krankenhäuser von unter 50 % und Doppelmeldungen, die als solche nicht erkannt wurden. Das Krebsregister soll deshalb so umgestaltet werden, dass es für die Kliniken und Ärzte von unmittelbarem Nutzen ist. Es soll eine Verlaufs- und Erfolgskontrolle von Krebstherapien und Aussagen dazu ermöglichen, welche Behandlungsformen bei welchen Tumoren und Erkrankungsstadien die besten Ergebnisse für die Patienten zur Folge haben (sog. Klinisches Krebsregister). Die meldenden Ärzte und Kliniken sollen künftig eine Rückmeldung der Erkenntnisse erhalten. Dies soll langfristig zu einer Verbesserung der Überlebenschancen und der Lebensqualität der Krebspatienten führen. Erreicht werden

soll dies dadurch, dass Ärzte und Kliniken künftig gesetzlich verpflichtet sein sollen, Krebserkrankungen an das klinische Krebsregister zu melden. Die erste Konzeption dafür sah vor, dass die Daten der Krebspatienten unverschlüsselt an das klinische Krebsregister übermittelt und dort mit vollem Personenbezug während der Dauer der Erkrankung, also möglicherweise lebenslang, gespeichert werden; der Krebspatient sollte der Verarbeitung seiner Daten lediglich widersprechen können. Die Kombination von Widerspruchslösung und Klardatenspeicherung trägt der Tatsache, dass es sich bei Daten über Krebserkrankungen um sensitive Daten handelt, nicht hinreichend Rechnung. Die Aufsichtsbehörde setzte sich deshalb dafür ein, dass die Patientendaten verschlüsselt beispielsweise an eine (oder mehrere) Vertrauensstelle(n) übermittelt werden, die sie pseudonymisiert an ein (oder mehrere) klinische(s) Krebsregister weiterübermittelt (weiterübermitteln). Inzwischen zeichnet sich eine entsprechende Lösung ab; die Einzelheiten müssen allerdings noch geklärt werden.

6.2 Führung und Aufbewahrung von Patientenakten

6.2.1 - in der Arztpraxis, Aktenaussonderung

In der Patientenakte dokumentiert der Arzt die Befunde und die Behandlung des Patienten. Zu der Patientenakte gehören auch Facharztbriefe, Röntgenbilder und Operationsberichte und zwar unabhängig davon, in welcher Form diese vorliegen. Die Patientenakten unterliegen nach § 3 Abs. 9 BDSG und auf Grund der ärztlichen Schweigepflicht einem besonderen Schutz. Daraus folgt, dass sie stets sicher aufbewahrt werden müssen. Sie müssen in der Arztpraxis vor unbefugter Kenntnisnahme geschützt werden, was nicht immer beachtet wird, sei es, dass die Patientenkartei offen in einem Behandlungszimmer aufbewahrt wird, in dem sich zeitweilig unbeaufsichtigt Patienten aufhalten, sei es, dass der Inhalt der elektronischen Akte des zuvor behandelten Patienten für den nachfolgenden Patienten lesbar auf dem Bildschirm angezeigt wird, während sich der Arzt noch in einem anderen Behandlungszimmer aufhält.

Besondere Vorsicht ist auch bei der Entsorgung von Patientenakten aus Arztpraxen angebracht. Dagegen wird - trotz wiederholter Hinweise auch der Standesvertretung an die niedergelassenen Ärzte - immer wieder verstoßen. So wurden Patientenakten zur Altpapiersammlung am Straßenrand abgelegt, auf dem Schrottplatz in nicht vollständig geleerten alten Metallschränken einer Arztpraxis aufgefunden oder in einem offenen, allen Mietern zugänglichen Altpapiercontainer eines großen Geschäftsgebäudes entdeckt. Die dafür verantwortlichen Ärzte wurden von uns eingehend über die ordnungsgemäße Beseitigung solcher Unterlagen belehrt. In zwei Fällen sahen

wir die Verstöße jedoch als so schwerwiegend an, dass wir die Strafverfolgungsbehörden einschalteten. Ein Verfahren wurde inzwischen gegen Zahlung einer Geldbuße eingestellt, das andere Verfahren ist noch anhängig.

6.2.2 - nach Praxisaufgabe, bei Insolvenz und nach dem Tod eines Arztes

An die Aufsichtsbehörde wurden mehrere Fälle herangetragen, in denen es um die Aufbewahrung von Patientenakten und die Auskunftserteilung an Patienten
- nach Praxisaufgabe (mit und ohne Nachfolge),
- dem Tod eines Arztes und
- bei Insolvenz und Flucht eines Arztes ins Ausland

ging.

Praxisaufgabe

Gibt ein Arzt seine Praxis auf, übernimmt im Regelfall der Nachfolger die Patientenunterlagen insgesamt, muss sie aber absondern und darf sie erst nutzen, wenn der Patient zum Ausdruck bringt, dass er vom Nachfolger weiterbehandelt werden will.

Hat ein Arzt keinen Nachfolger, bleibt er nach der Berufsordnung der Landesärztekammer (andere Kammern haben eine vergleichbare Regelung getroffen) verpflichtet, die Patientenunterlagen insgesamt 10 Jahre lang selbst aufzubewahren oder dafür Sorge zu tragen, dass sie solange in gehörige Obhut kommen.

Tod eines Arztes

Ist der Arzt verstorben, ist danach zu unterscheiden, ob Erben vorhanden sind oder nicht: **Sind Erben vorhanden**, haben sie, obwohl sie nicht der ärztlichen Berufsordnung unterliegen, den einem Arzt obliegenden Aufbewahrungs- und Obhutspflichten zu genügen und die Patientenunterlagen entweder selbst zu verwahren oder in gehörige Obhut zu geben, wofür es keiner Einwilligung der Patienten bedarf. Auch müssen die Erben oder der Beauftragte Einsicht in Patientenunterlagen gewähren bzw. Auskunft daraus erteilen. Entsprechende Nebenpflichten aus dem Behandlungsvertrag zwischen Arzt und Patienten sind auf die Erben übergegangen.

Patienten können von den Erben in solchen Fällen verlangen, dass diese Kopien der gesamten Patientenakten an ihren neuen Hausarzt übergeben. Dies bestätigte das vom Innenministerium beteiligte Sozialministerium in einem Fall, in dem eine Be-

zirksärztekammer den zur Mitwirkung bereiten Erben eine gegenteilige Rechtsauskunft gegeben hatte.

Mitunter fällt es den Erben aber auch schwer, ihre neue Aufgabe zu erfüllen, sei es, dass sie nicht über geeignete Räume zur Aufbewahrung der Patientenunterlagen verfügen, sei es, dass sie sich als medizinische Laien außer Stande sehen, Einsichts- bzw. Auskunftsverlangen der Patienten zu entsprechen. Eine Erbin brachte uns gegenüber zum Ausdruck, dass sie froh wäre, wenn sie dabei von der Ärztekammer unterstützt würde. Die Aufsichtsbehörde würde es daher begrüßen, wenn die Kammern für solche Fälle ein Angebot bereithielten, sei es dass die Unterlagen von den Kammern aufbewahrt werden, sei es, dass die Kammern einen anderen Arzt mit der Aufbewahrung von Patientenunterlagen und der Auskunftserteilung beauftragen können. Die Bundesrechtsanwaltsordnung enthält für vergleichbare Fälle bei Rechtsanwälten bereits eine entsprechende Regelung.

Sind **keine Erben vorhanden** oder wird die **Erbschaft ausgeschlagen**, hat der Staat für die Aufbewahrung der Unterlagen und die Auskunftserteilung während der vorgeschriebenen Aufbewahrungszeit zu sorgen. Das Sozialministerium hat in einem mit dem Innenministerium abgestimmten Schreiben klargestellt, dass in diesen Fällen die Gemeinden als Ortspolizeibehörden verpflichtet sind, den polizeiwidrigen Zustand zu beseitigen, d.h., also die Akten bei sich aufzubewahren. Die Gemeinden wehren sich dagegen jedoch aus nachvollziehbaren Gründen: Weder gehören solche Akten ins Rathaus, noch sollte die Einsichtsgewährung bzw. Auskunftserteilung Sache nicht ärztlich ausgebildeter gemeindlicher Bediensteter sein. Nach Auffassung des Innenministeriums sollte das Kammergesetz in solchen Fällen die Kammern zum Tätigwerden verpflichten.

Insolvenz

Die Dringlichkeit einer entsprechenden Gesetzesänderung unterstreicht ein weiterer Fall: Eine Praxisgesellschaft war insolvent geworden. Der Arzt selbst hatte sich ins Ausland abgesetzt. Sämtliche Patientendaten lagen ausschließlich auf den Festplatten des Datenservers. Der Insolvenzverwalter sah sich weder dazu berufen noch in der Lage, die Festplatten zu sichern und den Patienten, von denen sich einzelne auch an uns gewandt hatten, Auskunft über ihre ausschließlich elektronisch gespeicherten Daten zu geben. Da sich alle in Betracht kommenden Stellen weigerten, tätig zu werden, baute schließlich die Aufsichtsbehörde mit Zustimmung des Insolvenzverwalters und des Pfandrechtinhabers die Festplatten aus dem Server aus und lagerte sie bei der Ärztekammer ein, um zu verhindern, dass sich Unbefugte Zugang

zum ungesicherten Server verschaffen und die Patientendaten bei einer Verwertung der Rechneranlage im Insolvenzverfahren in fremde Hände fallen. „Auf der Strecke“ blieb das Einsicht- bzw. Auskunftsrecht der Patienten, da es nicht möglich war, die ausschließlich elektronisch gespeicherten Daten sichtbar zu machen und die Ärztekammer sich im Übrigen auch nicht für verpflichtet hielt, Auskünfte über die gespeicherten Patientendaten zu erteilen. Auch für solche Fälle bedürfte es einer gesetzlichen Verpflichtung der Ärztekammer zum Tätigwerden. Das Sozialministerium zeigte sich in einem Gespräch mit dem Innenministerium aufgeschlossen, das Kammergesetz entsprechend zu ändern.

Der zuletzt geschilderte Fall macht noch ein weiteres Problem deutlich: Da immer mehr Patientendaten ausschließlich elektronisch gespeichert werden, muss für die Zukunft sichergestellt werden, dass diese während der gesamten Aufbewahrungszeit auch im Falle einer längeren Abwesenheit des Arztes von dazu Verpflichteten gelesen und beauskunftet werden können.

6.3 Datenschutz beim Internetzugang und interne Vernetzung in Arztpraxen

Auf Wunsch der Ärzteorganisation nahm die Aufsichtsbehörde Stellung zur Frage des Internetzugangs vom Praxiscomputer aus und zur Vernetzung der Praxis-PC durch ein Funk-Netzwerk (Wireless local Network,WLAN) innerhalb einer Arztpraxis.

6.3.1 Internetzugang vom Praxiscomputer aus

Bei jedem Computer, der mit dem Internet verbunden ist, besteht grundsätzlich die Möglichkeit, dass Dritte versuchen, unbemerkt eine Verbindung aufzubauen, um Schaden stiftende Programme dort zu installieren oder den Datenbestand auszuspähen oder zu verändern. § 9 BDSG und die Anlage hierzu gebieten, dagegen Vorkehrungen zu treffen.

Einen wirkungsvollen Schutz vor unrechtmäßigen Handlungen bietet nur eine professionelle, regelmäßig gewartete und aktualisierte Firewall. Ob sich jede kleinere Arztpraxis eine solche Firewall leisten kann, erscheint fraglich. Als pragmatische Lösung wurde daher empfohlen, den Internetzugriff von einem extra aufgestellten, nicht vernetzten PC, auf dem sich keine Patientendaten befinden, durchzuführen.

6.3.2 Funk-Netzwerk (WLAN)

Beim Einsatz von WLAN sind nach der Anlage zu § 9 BDSG Maßnahmen zu treffen, die gewährleisten, dass personenbezogene Daten bei ihrer elektronischen Übertragung nicht unbefugt gelesen werden können. Das standardmäßig im WLAN zur Übertragung verwendete Sicherheitsprotokoll „WEP“ wird allgemein als nicht sicher im datenschutzrechtlichen Sinn angesehen. Die auf der Funkstrecke damit übertragenen Daten können abgehört und entschlüsselt werden. Aus diesem Grund halten wir den Einsatz eines WLAN, über das Patientendaten versendet werden, nur dann für datenschutzgerecht, wenn die Daten zusätzlich noch verschlüsselt werden, beispielsweise durch Einbetten in eine Sicherungsschicht eines VPN (Virtual Private Network).

6.4 Vernetzung der niedergelassenen Ärzte

Die Kassenärztliche Vereinigung betreibt seit geraumer Zeit ein Projekt, das die elektronische Kommunikation zwischen den niedergelassenen Ärzten ermöglichen soll, um Überweisungen und Befundberichte elektronisch zu übermitteln. Anlass für dieses Projekt ist die elektronische Gesundheitskarte 2006. Damit die Rechte der Patienten von Anfang an gewahrt werden, wurden der Landesbeauftragte für den Datenschutz und die Aufsichtsbehörde für den Datenschutz um Beratung gebeten.

6.5 Versand von Laborunterlagen per Telefax

Ein Bürger wandte sich empört an uns, nachdem ihm ein Labor ein Meldeformular über den Nachweis des Hepatitis-B-Virus bei einem namentlich bezeichneten Patienten zugefaxt hatte. Die Überprüfung ergab, dass das Fax für das Staatliche Gesundheitsamt am Ort bestimmt war. Das Labor trug zur Entschuldigung folgendes vor: Es sei nach dem Infektionsschutzgesetz verpflichtet, bestimmte Befunde von Infektionskrankheiten unter Angabe der betroffenen Person innerhalb von 24 Stunden dem zuständigen Gesundheitsamt zu melden. Ein Versand per Post scheidet daher aus. Anhand eines Programms werde zum jeweiligen Einsender des Materials das zuständige Gesundheitsamt ermittelt und eine Meldung erstellt. Nach Durchsicht der so erstellten Befunde würden diese automatisch gefaxt. Grund für die fehlerhafte Übermittlung sei ein Fehler in einem Tool des zuständigen Bundesinstituts gewesen, das dieses Tool ärztlichen Labors für entsprechende Meldungen zur Verfügung stellt. In dem Tool seien die Faxnummern aller Gesundheitsämter in Deutschland verzeichnet; im vorliegenden Fall sei die Faxnummer des zuständigen Gesundheitsamts in der Version 2001 falsch angegeben gewesen.

Wir wiesen das Labor unter Angabe weiterführender Literatur darauf hin, dass sensible Daten grundsätzlich nicht per Fax versandt werden sollten. Auf jeden Fall dürfe nur mit eingespeicherten Faxnummern gearbeitet werden, deren Richtigkeit zuvor mit einem Testfax festgestellt wurde. Das Labor richtete darauf hin Testfaxe an alle Gesundheitsämter. Deren Antworten machten weitere Korrekturen des Faxnummerverzeichnisses erforderlich. Nach Eingabe der Änderungen wurde ein weiterer Test durchgeführt.

6.6 Weitergabe von Patientendaten an externe Abrechnungsstellen

Ein Bürger beschwerte sich bei der Aufsichtsbehörde darüber, dass er nach einer privaten Arztbehandlung die Rechnung nicht vom Arzt selbst, sondern von einer externen, privatwirtschaftlich tätigen Abrechnungsstelle erhalten hatte. Die datenschutzrechtliche Überprüfung beim Arzt und bei der Abrechnungsstelle führte zu folgendem Ergebnis:

Der Arzt hatte die Abrechnungsstelle beauftragt, die Rechnungen für seine Privatpatienten zu erstellen und ihr dazu Patienten- und Behandlungsdaten übermittelt. Um die Patienten in den Vorgang einzubinden, hatte die Abrechnungsstelle dem Arzt einen Aushang zur Verfügung gestellt, mit dem er in seinen Praxisräumen auf die Weitergabe der Patientendaten und die Erstellung der Rechnung durch die Abrechnungsstelle hinwies.

Die Vorgehensweise des Arztes war unzulässig, die der Abrechnungsstelle möglicherweise. Gibt ein Arzt oder ein Krankenhaus Patientendaten aus privatärztlicher Behandlung an einen Dritten weiter, ist hierfür die schriftliche und freiwillige Einwilligung des Patienten erforderlich. Der Patient muss vor der Behandlung darüber informiert werden, welche Daten an wen und zu welchem Zweck übermittelt werden. Dies kann mittels eines Vordrucks erfolgen. Eine datenschutzrechtliche Grundvoraussetzung für die Wirksamkeit der Einwilligung ist jedoch die Unterschrift des Patienten.

Abrechnungsstellen dürfen die Patientendaten nur dann verarbeiten, wenn sie sicher gehen können, dass die Einwilligung des Patienten beim Arzt oder beim Krankenhaus vorliegt. Sie müssen deshalb behandelnde Ärzte, die über sie abrechnen lassen, auf das richtige Vorgehen hinweisen und durch Stichprobenkontrollen überprüfen, ob die schriftliche Einwilligung der Patienten vorliegt. Auf diese Rechtslage haben Ärztekammer und Aufsichtsbehörde wiederholt hingewiesen. Ob die Abrech-

nungsstelle sie beachtet hat, wird von ihr und dem Arzt unterschiedlich dargestellt. Der Arzt hat sich, nachdem ihm das richtige Verfahren aufgezeigt wurde, sofort bereiterklärt, künftig die schriftliche Einwilligung seiner Patienten einzuholen.

6.7 Verwendung von Apotheken-Abrechnungsdaten für andere Zwecke

Die Apotheken sind nach dem Sozialgesetzbuch verpflichtet, die unter die gesetzliche Krankenversicherung fallenden Verordnungen (Kassenrezepte) elektronisch abzurechnen. Sie dürfen sich hierzu externer Rechenzentren bedienen. Da die Verordnungen und damit auch die Namen der Patienten, für die sie ausgestellt sind, in den Apotheken im Regelfall nicht erfasst werden, erstellen die Rechenzentren für jede Apotheke, die dies wünscht, monatlich eine Abrechnungs-CD, auf der in einer Datenbankstruktur die Verordnungsdaten der von ihr abgegebenen Medikamente personenbezogen enthalten sind.

Nach § 300 Abs. 2 des Fünften Buchs des Sozialgesetzbuchs dürfen die Daten von den Rechenzentren nur für Zwecke des SGB und nur in einer auf diese Zwecke ausgerichteten Verarbeitung verarbeitet und genutzt werden. Der Düsseldorfer Kreis ist ganz überwiegend der Auffassung, dass die Erstellung von **Zuzahlungsbescheinigungen** für Patienten, die Möglichkeiten der **Rezeptrecherche** für Patienten, Ärzte und Krankenkassen sowie die Nachvollziehbarkeit der Berechtigung einer **Retaxation** im Sozialgesetzbuch festgelegte Zwecke sind und die Herstellung und Verwendung von Abrechnungs-CD für diese Zwecke zulässig ist. Bei Anwendungen, die darüber hinausgehen, ist von Anfang an die informierte Einwilligung des Betroffenen einzuholen. Anzumerken ist, dass bei einer arztbezogenen Nutzung zudem die Einwilligung des Arztes erforderlich ist.

Wir haben die berührten Stellen über unsere Rechtsauffassung unterrichtet.

6.8 Übermittlung von Gesundheitsdaten an einen Arzneimittelhersteller

Ein Arzneimittelhersteller vertreibt ein Medikament, für das die Krankenkassen einen Höchsterstattungsbetrag (sogenannter Festbetrag) festgesetzt haben. Die Firma hat den Abgabepreis für ihr Medikament jedoch nicht gesenkt. Das hatte zur Folge, dass Versicherte bei der ärztlichen Verordnung dieses Medikaments seit 1. Januar 2005 den Differenzbetrag zwischen Festbetrag und Abgabepreis selbst tragen müssen. Die Firma bot deshalb Patienten, die wegen Überschreitung der Belastungsgrenze von 2 % ihrer jährlichen Bruttoeinnahmen von der Zuzahlung befreit sind, sowie Sozialhilfeempfängern an, ihnen in der Zeit vom 1. Januar bis 31. Dezember 2005 den

Differenzbetrag zum Festbetrag zu erstatten. Voraussetzung dafür war die Übersendung eines von den Patienten ausgefüllten Datenerhebungsbogens und einer Reihe von Nachweisen, beispielsweise der ärztlichen Verordnung, der Zahlungsquittung der Apotheke, einer Bescheinigung der Krankenkasse über die Befreiung von der Zuzahlung als 2 %-Patient bzw. falls die Krankenkasse dies ablehnt, des entsprechenden Ablehnungsschreibens, des Sozialhilfebescheids sowie der regulären Befreiungsbescheinigung. Mehrere Organisationen wandten sich wegen datenschutzrechtlicher Bedenken gegen diese Verfahrensweise an uns.

Wir wiesen den Arzneimittelhersteller daraufhin, dass er die Betroffenen, die nach § 3 Abs. 9 BDSG besonders geschützte Daten preisgeben, nicht nur über die Freiwilligkeit ihrer Angaben informieren muss - allerdings verbunden mit dem Zusatz, dass ohne diese Angaben eine Entscheidung über die Erstattung der Zuzahlung nicht möglich ist -, sondern auch darüber, welche Daten wie und für welche Zwecke verarbeitet werden. Ferner mussten wir ihm sagen, dass der Grundsatz der Datensparsamkeit (§ 3a BDSG) es gebietet, auf die Vorlage einer Reihe von Nachweisen zu verzichten bzw. andere Nachweise zuzulassen. Beispielsweise genügt es, anstelle der ärztlichen Verordnung die Bestätigung einer Apotheke zu übersenden, dass ihr eine ärztliche Verordnung vorlag. Damit wird vermieden, dass die Daten des Arztes und möglicherweise weitere auf dem Rezept enthaltene Angaben an die Arzneimittelfirma übermittelt werden. Nicht gefordert werden kann auch die Vorlage des Sozialhilfebescheids, da dieser zahlreiche Informationen enthält, die für die Erstattung der Zuzahlung nicht benötigt werden. Es genügt hier, dass das Sozialamt bestätigt, dass der Antragsteller Sozialhilfeempfänger ist, zumindest müssen die Antragsteller jedoch darauf hingewiesen werden, dass sie bei Vorlage des Sozialhilfebescheids für den Empfänger nicht erforderliche Daten schwärzen können. Da das Unternehmen die Anträge der Patienten von einem Dienstleister verarbeiten lässt, wiesen wir es darauf hin, dass es die Datenerhebung, -verarbeitung und -nutzung und die technischen und organisatorischen Maßnahmen in einem schriftlichen Auftrag im einzelnen festlegen muss (vgl. § 11 Abs. 2 Satz 2 BDSG), was bisher nicht geschehen war.

Nach einer längeren kontroversen Diskussion erklärte sich das Arzneimittelunternehmen schließlich bereit, den Forderungen der Aufsichtsbehörde „ohne Anerkennung einer Rechtspflicht“ Rechnung zu tragen.

7 Handel- und Dienstleistungen

7.1 Kundenbindungsprogramme

Im Berichtszeitraum baten einige Unternehmen, in der Mehrzahl Zeitungsverlage, um eine datenschutzrechtliche Beratung bei der Einführung ihres Kundenbindungssystems. Dessen Abwicklung war in allen Fällen einer Fremdfirma als Dienstleister übertragen.

Die zu beurteilenden Kundenbindungssysteme sehen vor, dass Kunden, beispielsweise Abonnenten der Zeitungsverlage, bei Einkäufen in Partnerunternehmen oder Inanspruchnahme von Dienstleistungen eines Partnerunternehmens Nachlässe gewährt werden. Dieser Bonus kann mittels einer Kundenkarte, welche bei dem Partnerunternehmen vorgezeigt wird, eingelöst werden. Die Kundenkarte ist personenbezogen. Beim Einlösen werden die Umsatzdaten des getätigten Geschäftes und die auf der Karte gespeicherte Kartennummer an das Auftragsunternehmen übermittelt. Dort erfolgt die Gutschrift der Boni für den jeweiligen Kunden. Ab einem bestimmten Betrag werden diese von der verantwortlichen Stelle ausgezahlt. Diese holt sich die geleisteten Boni von den Partnerunternehmen zurück. Der Einsatz der Kundenkarte soll der Kundenbindung dienen.

Für die Teilnahme am Kundenbindungsprogramm ist ein Aktivierungsantrag auszufüllen. Mit diesem werden auch die Teilnahmebedingungen übersandt. Im ersten Teil des Aktivierungsantrags werden die sogenannten Stammdaten (Vorname, Name, Titel, Straße/Hausnummer, PLZ und Ort) erhoben. Diese werden nach den Teilnahmebedingungen nur für den Zweck der Bonusgewährung und -abrechnung, also zur Verwaltung des Kundenbindungsprogramms genutzt. Dafür werden auch die notwendigen Umsatzdaten (Partnernummer, Kartennummer, Datum und Umsatz) jedes Einkaufs erfasst und an die verantwortliche Stelle, die das Kundenbindungssystem durchführt, übermittelt, wo sie weiterverarbeitet werden. Eine Erhebung und Verarbeitung von Angaben zur gekauften Ware oder Dienstleistung erfolgt nicht. Datenschutzrechtlich ist diese Vorgehensweise nicht zu beanstanden.

In einem weiteren Abschnitt des Aktivierungsantrags werden zusätzliche Daten (vollständiges Geburtsdatum, Telefonnummer, Mobilnummer, Fax- und E-Mail-Adresse) erhoben. Diese Angaben stehen zwar unter der Überschrift „freiwillige Angaben“; jedoch wird der Kunde, außer bei der E-Mail-Adresse, nicht darüber aufgeklärt, für welche Zwecke diese Angaben benötigt werden. Wir haben darauf hingewiesen, dass nach § 4 Abs. 3 BDSG der Betroffene bei der Erhebung über die Zweckbe-

stimmung der Erhebung, Verarbeitung oder Nutzung der zu erhebenden Daten zu unterrichten ist. Darüber hinaus ist der Grundsatz der Datenvermeidung und Datensparsamkeit (§ 3a BDSG) zu beachten. Der Betroffene kann die Tragweite seiner Angaben nur überschauen, wenn er weiß, für welche Zwecke diese Daten erhoben, verarbeitet oder genutzt werden.

Wenn die zusätzlich erhobenen Daten nicht nur zur Erledigung der Verwaltung der Kundenkarte (Gutschrift und Auszahlung der Boni), sondern darüber hinaus auch für die werbliche Ansprache genutzt werden sollen, ist für die Zulässigkeit der Erhebung, Verarbeitung und Nutzung dieser personenbezogenen Daten eine eindeutige und unmissverständliche Einwilligung des Betroffenen nach § 4a BDSG erforderlich. Die Aktivierungsanträge und die Teilnahmebedingungen wurden dementsprechend geändert. Der Kunde kann jetzt genau erkennen, dass die freiwilligen Angaben für werbliche Zwecke genutzt werden. Er hat jederzeit die Möglichkeit, der weiteren Nutzung dieser Daten für werbliche Zwecke gegenüber der verantwortlichen Stelle zu widersprechen.

7.2 Identifikation anhand des Personalausweises, Anfertigen von Ausweiskopien

Nach § 4 Abs. 1 des Gesetzes über Personalausweise (PAuswG) können der Personalausweis und der vorläufige Personalausweis auch im nichtöffentlichen Bereich als Ausweis- und Legitimationspapiere benutzt werden. Das PAuswG verbietet lediglich, die Seriennummern der Ausweise so zu verwenden, dass mit ihnen ein Abruf personenbezogener Daten aus Dateien oder eine Verknüpfung von Dateien möglich ist.

Im Berichtszeitraum sind der Aufsichtsbehörde mehrere Fälle vorgetragen worden, in denen Unternehmen unter Angabe von verschiedensten Gründen von ihren Kunden die Vorlage von Ausweispapieren forderten bzw. eine Leistung von der Zustimmung zur Fertigung einer Kopie der Ausweispapiere abhängig machten. Stein des Anstoßes war für die Betroffenen die Tatsache, dass der erhebenden Stelle durch die Kopie der Ausweispapiere Daten bekannt wurden, die für den jeweils genannten Zweck nicht erforderlich waren.

7.2.1 Ausweiskopie für das Finanzamt

Mehrere Metallhändler erhielten von ihrem Finanzamt im Rahmen einer Betriebsprüfung die Empfehlung, zur Vermeidung steuerlicher Nachteile ihre Lieferanten identitätsmäßig zu erfassen und hierzu Kopien der Personalausweise zu fertigen. Als

Rechtsgrundlage wurde von den Finanzämtern § 160 der Abgabenordnung und ein Urteil des Bundesfinanzhofes (BFH) aus dem Jahr 1999 genannt. Nach dieser Vorschrift muss ein Steuerpflichtiger gegenüber der Finanzbehörde die Empfänger von Ausgaben benennen, wenn er die Ausgaben steuerlich geltend machen will. Nach der Entscheidung des BFH muss sich der Steuerpflichtige, um steuerliche Nachteile für sich abzuwenden, im Rahmen einer ordnungsgemäßen Geschäftstätigkeit über Namen und Adressen der Lieferanten anhand von Ausweispapieren, etwa durch Einsichtnahme in den Personalausweis, Pass oder Führerschein vergewissern. Dieser Entscheidung ist nicht zu entnehmen, dass der Steuerpflichtige zu diesem Zweck eine Fotokopie des Personalausweises fertigen muss. Die Aufsichtsbehörde hält es für ausreichend, wenn sich der Steuerpflichtige die Daten, die er für eine eindeutige Benennung des Lieferanten gegenüber dem Finanzamt benötigt, aus den vorgelegten Ausweispapieren notiert. Die Fertigung einer Ausweiskopie, in der auch Daten enthalten sind, die das Finanzamt nicht benötigt, ist nicht erforderlich und ohne datenschutzrechtlich wirksame Einwilligung des Betroffenen unzulässig. Die betreffenden Finanzämter wurden gebeten, ihre Empfehlung entsprechend zu ändern.

7.2.2 Ausweiskopie im Falle einer Barauszahlung bei Reklamation

In einem anderen Fall wurde von einem Kunden, der von seinem Rückgaberecht in einem Ladengeschäft Gebrauch machte, verlangt, dass er wegen der Barauszahlung des Erstattungsbetrags seinen Personalausweis kopieren lassen müsse. Als Begründung wurde gegenüber dem Kunden angegeben, dass das Finanzamt diese Daten für die Rückerstattung der Umsatzsteuer benötige. Auf Nachfragen der Aufsichtsbehörde hieß es hingegen, es sei bei Barauszahlungen im Rahmen von Reklamationen üblich, den Personalausweis der Kunden zu kopieren. Näher begründet wurde dies nicht. Es wurde jedoch versichert, dass die über die Ausweiskopien erhobenen Daten nicht gespeichert, sondern die Kopien nach Prüfung durch die Buchhaltung umgehend vernichtet worden seien. Das Unternehmen hat versichert, künftig keine Ausweiskopien mehr zu fertigen.

7.2.3 Ausweiskopie für Rechnungsstellung

In einem weiteren Fall wurde einem Kunden beim Kauf von Ersatzteilen der Wunsch nach Barzahlung abgelehnt und für die Erstellung einer Rechnung zu Beweiszecken eine Kopie des Personalausweises verlangt. Die Firma versicherte, die Ausweiskopie nach Bezahlung der Rechnung zu vernichten. Sie wurde darauf hingewiesen, dass für die genannten Zwecke die Vorlage von Ausweispapieren und ein Aufzeichnen der erforderlichen Daten aus dem Ausweis genügt.

7.2.4 Anforderung und Prüfung des Ausweises für Handyvertrag

Der Abschluss von Handyverträgen wurde von einem Vertriebspartner eines Service-/Netzproviders in mehreren Fällen von der Vorlage einer Kopie des Personalausweises abhängig gemacht. Als Begründung wurde gegenüber der Aufsichtsbehörde angegeben, dass in den betreffenden Fällen die Identität des potentiellen Vertragspartners ansonsten nicht zweifelsfrei hätte festgestellt werden können. Zur Anforderung und Prüfung des Personalausweises ist der Vertriebspartner des Service-/Netzproviders in solchen Fällen nach § 95 Abs. 4 des Telekommunikationsgesetzes berechtigt.

7.2.5 Ausweiskopie wegen § 24c KWG

In einem weiteren Fall hat ein Kreditinstitut von einer Betroffenen die Vorlage einer Ausweiskopie des Kontobevollmächtigten gefordert, weil dessen Geburtsdatum nicht bekannt war. Die Betroffene empfand diese Forderung als völlig überzogen.

Nach dem neuen § 24c Abs. 1 Satz 1 Nr. 1 und 2 KWG müssen Kreditinstitute neben der Kontonummer, dem Tag der Errichtung des Kontos und gegebenenfalls dem Tag der Auflösung des Kontos auch Name und Geburtstag des Kontoinhabers und gegebenenfalls des Kontobevollmächtigten in einer zentralen Datei speichern. Kreditinstitute müssen deshalb fehlende Daten von Kontoinhabern und Kontobevollmächtigten nacherheben. Ein bundesweit tätiges Kreditinstitut hat dazu die betroffenen Kunden aufgefordert, die Angaben zu vervollständigen und diese durch die Vorlage einer Ausweiskopie nachzuweisen. Eine bloße Mitteilung sei kein Nachweis. Das Kreditinstitut räumte auf Nachfrage ein, es genüge selbstverständlich, wenn der Kontobevollmächtigte seinen Ausweis in einer Filiale vorlegt, damit die erforderlichen Angaben abgeschrieben werden können. Das Kreditinstitut wurde gebeten, den Betroffenen künftig sämtliche in Frage kommenden Möglichkeiten aufzuzeigen.

7.2.6 Ausweiskopie an der Kasse als Stichprobe beim Lastschrifteinzugsverfahren

Viele Anfragen gab es zum bargeldlosen Bezahlen an den Kassen des Handels. Insbesondere war von Interesse, ob sich die Händler Daten aus dem Personalausweis abschreiben oder diesen sogar fotokopieren dürfen.

Beim dem im Handel vielfach angewandten Lastschriftverfahren wird aus der EC-Karte des Kunden lediglich die Bankverbindung ausgelesen und damit die Abbuchung vom Kundenkonto veranlasst. Da die Bezahlung der Ware jedoch erst dann erfolgt ist, wenn die Bank den Rechnungsbetrag auf dem Konto des Händlers gutgeschrieben hat, der Kunde die Ware aber sofort mitnehmen möchte, erhält er vom Händler die Ware auf der Grundlage eines Warenkredits. Der Händler hat jedoch ein berechtigtes Interesse zu wissen, wem er einen Warenkredit einräumt. Aus diesem Grund darf er die Anschrift des Kunden erheben und ein Personaldokument einsehen.

Es ist jedoch zur Kreditsicherung nicht erforderlich, den Ausweis zu fotokopieren, da dieser mehr Daten enthält, als der Händler zur Sicherung seines Zahlungsanspruchs benötigt. Daher ist hier das Anfertigen einer Kopie datenschutzrechtlich unzulässig.

7.2.7 Erhebung und Speicherung von Personalausweisdaten von Fahrern von Gefahrguttransporten

Eine in Baden-Württemberg ansässige Firma für Ausweislesegeräte hat bei uns nachgefragt, ob es erlaubt sei, zur Identifizierung der Fahrer von Gefahrguttransporten die maschinenlesbaren Seriennummern des Personalausweises auszulesen und zu speichern. Das System solle zur Reduzierung von Risiken bei der Beförderung gefährlicher Güter durch Überprüfung des Fahrers anhand der amtlichen Dokumente dienen. Diese Überprüfung solle automatisch durchgeführt werden. Die Firma hat in diesem Zusammenhang auf ein Schreiben des Bundesministeriums für Verkehr, Bau- und Wohnungswesen vom Oktober 2001 verwiesen. Darin wird auf Grund des Terroranschlags in den USA am 11. September 2001 von allen Beteiligten eine besondere Sorgfalt bei der Beförderung gefährlicher Güter gefordert. Insbesondere bei der Übergabe gefährlicher Güter für den Straßenverkehr sollten Absender bzw. Verlader dafür sorgen, dass die einschlägigen Vorschriften strikt eingehalten werden. Im Rahmen dieser Überprüfung solle auch die Übereinstimmung der Daten des Fahrers mit den amtlichen Personaldokumenten überprüft werden.

Das System war bei einer Firma im ostdeutschen Raum kurz im Einsatz und wurde dann abgeschaltet, da es nach Auffassung der zuständigen Datenschutzaufsichtsbehörde und des Rechtsberaters der Firma nicht § 4 PAuswG entsprach, nach dem der Personalausweis nicht zur automatisierten Speicherung personenbezogenen Daten verwendet werden darf. Das Gesetz will damit verhindern, dass die Seriennummer im privaten Rechtsverkehr die Qualität einer Personenkennziffer-Surrogats erlangt. Im

vorliegenden Fall wäre der Personalausweis zum automatisierten Abgleich mit anderen Dateien verwendet worden. Das Verfahren war daher unzulässig.

Wir teilten der Firma mit, dass wir mit der Rechtsauffassung der ostdeutschen Aufsichtsbehörde übereinstimmen.

7.3 Melderegisterabgleich beim Energieversorgungsunternehmen (EVU)

Ein EVU wollte von uns wissen, ob es berechtigt oder gar verpflichtet ist, einer Gemeinde regelmäßig die Zu- und Abgänge von Kunden und deren Umzugsadressen mitzuteilen. Die Gemeinde war mit einer entsprechenden Bitte an das EVU herangetreten. Sie versprach sich davon eine Verbesserung der Qualität ihres Melderegisters, insbesondere eine größere Aktualität der Daten, weil sich die Kunden bei EVU´s erfahrungsgemäß zeitnah an- und abmelden.

Wir kamen zu dem Ergebnis, dass eine solche Datenübermittlung unzulässig ist.
Die kommunale Meldebehörde ist weder nach dem Meldegesetz noch ergänzend nach dem Landesdatenschutzgesetz befugt, solche Daten im Einzelfall bei einem Dritten zu erheben oder sich diese systematisch von einem Dritten übermitteln zu lassen. Hat die Meldebehörde im Einzelfall Zweifel an der Richtigkeit des Melderegistereintrags bzw. vermutet sie eine nicht erfolgte Anmeldung, muss sie nach dem Grundsatz der Direkterhebung zuerst versuchen, die Daten beim Betroffenen zu erheben.

Übermitteln dürfte das EVU die Daten
- für eigene Zwecke im Rahmen der Zweckbestimmung des Vertragsverhältnisses mit ihren Kunden. Diese Voraussetzungen liegen offensichtlich nicht vor;
- für andere Zwecke, soweit dies zur Wahrung berechtigter Interessen eines Dritten erforderlich ist und kein Grund zu der Annahme besteht, dass die Betroffenen ein berechtigtes Interesse am Ausschluss der Übermittlung haben. Das berechtigte Interesse der Meldebehörde an der Übermittlung der Daten ist hier schon deshalb zu verneinen, weil ihr das Recht keine entsprechenden Erhebungsbefugnis einräumt. Daran scheitert im Übrigen auch die Übermittlung der Kundendaten an die Meldebehörde zur „Abwehr von Gefahren für die öffentliche Sicherheit“.

7.4 Radio Frequency Identification (RFID)

RFID bezeichnet die kontaktlose Identifikation von Objekten durch Funkübertragung. Ein RFID-Chip ist ein mobiles, miniaturisiertes IT-System, das über eine Antenne

Funksignale empfangen und abgeben kann (Transponderfunktion). Dabei können unterschiedliche Techniken zum Einsatz kommen. Es gibt RFID-Chips, die nur ausgelesen werden können, sogenannte **passive Chips**. Es gibt aber auch RFID-Chips, die wie herkömmliche Chip-Karten eine Verarbeitung von Daten erlauben (derzeitige Speicherkapazität bis ca. 100 MByte). Diese werden auch als **aktive Chips** bezeichnet.

RFID-Chips werden heutzutage beispielsweise in Verfahren zur Produktsteuerung in der Industrie, zur Steuerung des Warenmanagements, als Diebstahlsicherung, zur Tieridentifikation, bei Zutrittkontrollsystemen und elektronischen Wegfahrsperren eingesetzt. Seit neuestem gibt es einige RFID-Pilotinstallationen im Bereich des Einzelhandels, bei denen die verkaufte Ware zur Steuerung des Warenmanagements (z.B. Auffüllen der Regale) erfasst und der Bezahlvorgang durchgeführt wird.

Dabei wächst die Sorge vor einem möglichen Missbrauch der Technik, vor einer Entwicklung hin zum gläsernen Menschen, dessen Interessen und Bewegungen aufgezeichnet und verfolgt werden können. Damit dies nicht geschieht, ist es notwendig, von vornherein den Einsatz der RFID-Technik zu begleiten, um die Persönlichkeitsrechte der Betroffenen zu wahren. Deshalb berät das Innenministerium über einen Verband mittelständische IT-Unternehmen, wie der Datenschutz beim Einsatz der RFID-Technik zu berücksichtigen ist.

Der Datenschutz greift nur ein, wenn entweder der RFID-Chip selbst personenbezogene Daten enthält oder die nicht personenbezogenen Daten auf dem RFID-Chip an Hand der Person erkannt oder mit Hilfe eines Hintergrundsystems personenbeziehbar sind, also einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Für die datenschutzrechtliche Beurteilung der RFID-Technik kommt es so auf ihren konkreten Einsatzbereich an:

- RFID-Etiketten in reinen Automations-, Warenmanagement- oder Logistiksystemen enthalten keine personenbezogenen Daten.

- Bei auf der RFID-Technik basierenden Zutrittssystemen werden hingegen regelmäßig personenbezogene Daten übermittelt.

Damit der Bürger auch künftig „Herr“ seiner Daten bleibt, darf der Einsatz von RFID mit personenbezogenen Daten nicht heimlich erfolgen, sondern muss transparent gemacht werden. Das bedeutet, dass der Betroffene über den Einsatz personenbeziehbarer RFID-Technik informiert werden muss, dass keine Daten unbefugt ausge-

lesen werden dürfen, und dass die Auskunftsrechte der Betroffenen zu beachten sind.

Das BDSG enthält hierzu Regelungen. Danach darf die Verarbeitung personenbezogener Daten nur erfolgen, wenn ein Gesetz dies erlaubt oder der Betroffene hierin einwilligt (§ 4 Abs. 1 BDSG). Werden beim Betroffenen Daten erhoben, so ist er über die Identität der verantwortlichen Stelle, die Zweckbestimmung der Datenverarbeitung und die Kategorien der Empfänger der Daten zu unterrichten. Nicht mehr benötigte Daten sind zu löschen, d.h. die Daten des RFID-Chips, der zu Abrechnungszwecken beispielsweise an der Kasse im Supermarkt eingesetzt wurde, sind nach der erfolgten Abrechnung zu löschen, notfalls durch Zerstören des Chips. Es muss auch verhindert werden, dass RFID-Chips, die im Zusammenhang mit einer Person stehen, unbemerkt ausgelesen werden können.

Bei einem Einsatz aktiver RFID-Chips mit zusätzlichen Speicher- und Verarbeitungsmöglichkeiten ist zusätzlich § 6c BDSG zu beachten. Diese Vorschrift beinhaltet weitergehende Informationspflichten, z.B. welche personenbezogene Daten sich auf dem RFID-Chip befinden und welche Verarbeitungsvorgänge ausgelöst werden.

8 Wohnungswesen

8.1 Zusammenarbeit von Auskunfteien mit der Wohnungswirtschaft

Immer mehr Vermieter gehen dazu über, sich vor Abschluss eines Mietvertrags durch eine Anfrage bei einer Auskunftei Informationen zum Zahlungsverhalten ihres zukünftigen Vertragspartners zu verschaffen. Dies ist unter datenschutzrechtlichen Gesichtspunkten nicht unproblematisch, da ein Mietinteressent auf Grund einer solchen Auskunft unter Umständen erhebliche unberechtigte Schwierigkeiten bekommen kann, eine entsprechende Wohnung zu finden. Die Datenschutzaufsichtsbehörden der Länder haben die damit zusammenhängenden Fragen eingehend mit den Auskunfteien und der Wohnungswirtschaft erörtert.

Fraglich ist bereits, auf welcher Rechtsgrundlage der Vermieter Daten über das bisherige Zahlungsverhalten eines Mietinteressenten erheben kann. In der Praxis wird teilweise (beispielsweise von der SCHUFA) die Einwilligung der Mietinteressenten in eine derartige Abfrage verlangt. Nach § 4a Abs. 1 BDSG ist eine Einwilligung jedoch nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Je nach Lage am Wohnungsmarkt und persönlicher Situation des Mietinteressenten haben die Datenschutzaufsichtsbehörden Zweifel, ob die Einwilligung der Mietinteressenten

auf ihrer freien Entscheidung beruht. Kritisch ist es auch zu sehen, wenn die Einwilligung formularmäßig eingeholt wird und damit die Besonderheiten des Einzelfalls nicht berücksichtigt werden. Die Einholung von Auskünften bei einer Auskunftei sollte deshalb grundsätzlich nicht auf eine Einwilligung gestützt werden.

Daten über den Mietinteressenten können aber in gewissen Grenzen auf der Grundlage des § 29 BDSG erhoben werden, da grundsätzlich ein berechtigtes Interesse von Vermietern besteht, vor der Entscheidung über den Abschluss eines Mietvertrags Informationen über die Zahlungsfähigkeit und -willigkeit des potentiellen Mieters einzuholen. Die Absicht, solche Daten zu erheben, muss aber auf jeden Fall gegenüber dem Mietinteressenten - etwa im Rahmen einer schriftlichen Information - transparent gemacht werden.

Soweit eine Datenübermittlung auf § 29 BDSG gestützt wird, wird vereinzelt die Auffassung vertreten, dass Vermieter nur Auskünfte erhalten dürfen, die sich auf andere Mietverhältnisse des Betroffenen beziehen. Die Mehrheit der Aufsichtsbehörden vermag dem Gesetz eine solche Einschränkung nicht zu entnehmen. Auch sie hält jedoch eine uneingeschränkte Auskunft über bei branchenübergreifenden Auskunfteien gespeicherte Daten an potentielle Vermieter für unzulässig. Bei der Prüfung, in welchem Umfang Daten an potentielle Vermieter übermittelt werden dürfen, sind die schutzwürdigen Belange der Mietinteressenten im Hinblick auf die Bedeutung der Wohnung für die Lebensgestaltung in besonderer Weise zu berücksichtigen. Auskünfte über Eintragungen im Schuldnerverzeichnis sind danach stets zulässig. Im Übrigen stellt sich die Frage, ob schutzwürdige Interessen des Mitinteressenten verletzt werden, wenn Informationen unterhalb dieser Schwelle und insbesondere Bagatellfälle von Auskunfteien an Vermieter übermittelt werden. Eine Übermittlung kommt nur in Betracht, wenn die Daten auf Zahlungsunwilligkeit oder -unfähigkeit des Betroffenen schließen lassen. Nach der ganz überwiegenden Auffassung der Aufsichtsbehörden, die wir teilen, sind Daten für die Wohnungswirtschaft erst ab drei Bagatellfällen oder einem Gesamtbetrag von insgesamt 1500 EURO relevant. Zudem dürfen Daten in diesen Fällen ein Jahr nach Tilgung der Forderung nicht mehr an potentielle Vermieter übermittelt werden. Eine solche differenzierte Bewertung trägt sowohl den berechtigten Interessen von Vermietern als auch den schutzwürdigen Interessen von Mietinteressenten in ausreichendem Maß Rechnung.

Insbesondere die fehlende Information der Mietinteressenten vor Durchführung einer Anfrage bei einer Auskunftei war das Problematische an einem an die Aufsichtsbehörde herangetragenen, auch von den Medien aufgegriffenen Fall. Darüber hinaus stellte sich die Frage, in welchen Fällen der Vertragspartner einer Auskunftei Aus-

künfte für den Vermieter einholen darf. Die Aufsichtsbehörde hat den Vorgang zum Anlass für eine Überprüfung der Verfahrensweise in Baden-Württemberg genommen.

Nach unserer Auffassung kann der Vertragspartner einer Auskunftei von dieser grundsätzlich nur dann eine Auskunft erhalten, wenn er selbst ein berechtigtes Interesse daran glaubhaft machen kann, d. h. wenn er selbst Vermieter oder Verwalter ist und der Abschluss eines Mietvertrags unmittelbar bevorsteht. Eine Ausnahme von diesem Grundsatz kann allenfalls dann akzeptiert werden, wenn die Auskunft von einem Verband bzw. Verein, dessen Zweck gerade die Interessenvertretung von Eigentümern ist, für seine Mitglieder eingeholt wird. Es muss dann aber insbesondere Folgendes sichergestellt werden:

- Der Mietinteressent muss vorab ausreichend und transparent über den gesamten Ablauf der Solvenzprüfung informiert werden.
- Das berechtigte Interesse des Mitglieds muss tatsächlich bestehen und auch nachgewiesen werden, z.B. durch ein vom Vermieter und vom Mietinteressenten gemeinsam unterzeichnetes Formblatt, in dem die Absicht bekundet wird, vorbehaltlich des Ergebnisses der Solvenzprüfung einen Mietvertrag zu schließen.
- Der Mietinteressent ist von dem Verband/Verein auf Anfrage über das Ergebnis der Abfrage zu informieren.
- Das Ergebnis der Abfrage muss von einer fachkundigen Person bewertet, an das Mitglied weitergegeben und diesem gegebenenfalls erläutert werden.
- Das Dokument zum Nachweis des berechtigten Interesses, das Ergebnis der Abfrage und dessen Bewertung sowie die an den Vermieter erteilte Auskunft sind vom Verband/Verein vorübergehend für Auskunftserteilungs- und Prüfzwecke aufzubewahren bzw. zu dokumentieren und anschließend ordnungsgemäß zu vernichten.

Die Aufsichtsbehörde hat ihre Rechtsauffassung, die sie künftigen Prüfungen zu Grunde legen wird, den betreffenden Auskunfteien, den Landesverbänden Haus und Grund, dem Verband baden-württembergischer Wohnungsunternehmen und dem Mieterverband mitgeteilt und sich zur Beratung im Einzelnen bereiterklärt. Sie wird die Zusammenarbeit von Auskunfteien mit der Wohnungswirtschaft weiter beobachten und die Einhaltung der datenschutzrechtlichen Grundsätze kontrollieren.

8.2 Aufnahme in eine Vergleichsmietenkartei

Ein Mieter wandte sich mit folgender Beschwerde an die Aufsichtsbehörde: Der örtliche Haus- und Grundbesitzerverein hatte im Auftrag seines Vermieters für seine

Wohnung ein Mieterhöhungsverfahren eingeleitet und die geforderte Miethöhe, wie gesetzlich vorgeschrieben, mit der Benennung dreier Vergleichswohnungen begründet. Dabei hatte er auch die Namen der Mieter der betreffenden Vergleichswohnungen angegeben.

Nach der Rechtsprechung des Bundesgerichtshofs muss eine Vergleichswohnung konkret bezeichnet werden, so dass der Mieter, dem gegenüber sie benannt wird, die Vergleichbarkeit überprüfen kann. Der Haus- und Grundbesitzerverein verfügt hierzu, wie andere Vermietervereine auch, über eine eigene Sammlung von Vergleichswohnungen. Da die Vereine für ihre Mitglieder Mietverträge abschließen und Mieterhöhungen durchführen, ist die Speicherung der Daten zulässig. Daten, die eine Wohnung beschreiben, sind personenbezogene Daten des Eigentümers. Sie sind zugleich auch personenbeziehbare Daten des Mieters, selbst wenn der Mietername im Datensatz nicht aufgeführt ist, da dieser über die Beschreibung der Lage der Wohnung identifiziert werden kann. Eine Übermittlung der Wohnungsdaten an Dritte ist nur auf gesetzlicher Grundlage oder mit wirksamer Einwilligung des Betroffenen zulässig.

Eine Übermittlung auf der Grundlage des § 28 Abs. 1 Satz 1 Nr. 2 BDSG scheidet aus, da datenschutzrechtlich schutzwürdige Interessen von Mietern entgegenstehen können. Die zivilrechtliche Regelung, wonach zur Begründung des Mieterhöhungsverlangens drei Vergleichswohnungen herangezogen werden können, reicht als Rechtsgrundlage für die Speicherung personenbezogener Daten in einem Vergleichsmietenkataster und zur Übermittlung an Dritte nicht aus. Daher ist eine datenschutzrechtliche Einwilligung des Mieters erforderlich. Der Mieter wurde zwar im Mietvertrag darüber informiert, dass die Mietvertragsdaten vom Verein gespeichert werden, über den Anlass und die Übermittlung an Dritte wurde er aber nicht unterrichtet. Somit konnte nicht von einer informierten Einwilligung im Sinne des § 4a BDSG ausgegangen werden.

Der Verein sagte zu, dass er bei zukünftigen Mietverträgen, die er für seine Mitglieder abschließt, eine datenschutzrechtlich wirksame Einwilligung der Mieter einholt. Das Innenministerium hat hierzu bereits 1999 eine Datenschutzklausel formuliert und den Landesverbänden der Vermietervereine zur Verfügung gestellt.

9 Arbeitnehmerdatenverarbeitung

9.1 Sicherheitsüberprüfung von Firmenmitarbeitern

Mitarbeiter einer Firma, die Dienstleistungen in Liegenschaften der US-Streitkräfte erbringt, wandten sich an die Aufsichtsbehörde, weil sie sich seit einiger Zeit vor ihrem Arbeitseinsatz einer Sicherheitsüberprüfung durch amerikanische Stellen unterziehen sollen. Jeder Betroffene sollte sich damit einverstanden erklären, dass die US-Dienststelle in seine Akten Einsicht nimmt und alle deutschen Sicherheits- und Polizeibehörden sämtliche über ihn gespeicherte Daten an die amerikanische Dienststelle übermitteln. In dem ergänzenden Informationsblatt der Firma hieß es, dass in alle zurückliegenden Vorgänge - unabhängig von der Schwere des Vergehens - und auch in Akten über waffenrechtliche Erlaubnisverfahren Einsicht genommen wird. Die Mitarbeiter sahen sich auf Grund der ihnen vorliegenden Information außer Stande, in die Sicherheitsüberprüfung einzuwilligen. Sie beklagten insbesondere, dass sie nicht wüssten, welche Stellen - amerikanische oder deutsche - auf welcher Rechtsgrundlage welche Daten erheben, ob diese dabei auch in Akten Einsicht nähmen und von Vorgängen Kenntnis erhielten, die nach datenschutzrechtlichen Vorschriften nicht an andere deutsche Behörden, geschweige denn an amerikanische Stellen übermittelt werden dürften und wie Daten durch die US-amerikanischen Stellen weiterverarbeitet werden. Sie waren auch in Sorge, dass ihr Arbeitgeber auf diesem Weg Informationen erhalten könnte, zu denen er selbst keinen Zugang hat.

Die Aufsichtsbehörde erklärte sich gegenüber Betroffenen bereit, sich im Rahmen ihrer auf den nichtöffentlichen Bereich begrenzten Zuständigkeit darum zu bemühen, dass das Verfahren für sie so transparent wird, dass sie ruhigen Gewissens in die Sicherheitsüberprüfung einwilligen können. Von uns unterstützte Bemühungen auf Bundesebene führten schließlich in Gesprächen mit amerikanischen und britischen Dienststellen zu Verbesserungen des Überprüfungsverfahrens. Es ist nunmehr klargestellt, dass die Sicherheitsüberprüfungen zwar von US-Streitkräften veranlasst, aber unter Federführung des Bundesamtes für Verfassungsschutz von deutschen Behörden auf der Grundlage des § 33 des Sicherheitsüberprüfungsgesetzes des Bundes durchgeführt werden. Die verwendete Einwilligungserklärung und der von dem Betroffenen auszufüllende Fragebogen wurden neu gestaltet. Sicherheitsrelevante Erkenntnisse der deutschen Behörden gehen zwar an die veranlassende US-Dienststelle, bleiben jedoch in Deutschland. Die Verwendung der Daten erfolgt ausschließlich zum Zwecke der Sicherheitsüberprüfung. Die Betroffenen haben Auskunfts- und Berichtigungsansprüche. Im Falle einer Ablehnung besteht die Mög-

lichkeit, den Rechtsweg zu beschreiten; eine Anhörung der Betroffenen ist gewährleistet.

Gleichwohl bleiben Wünsche offen. Die betroffene Firma setzte sich deshalb im Namen ihrer Mitarbeiter dafür ein, dass diese verständlicher über das Überprüfungsverfahren informiert werden, im Fragebogen weniger Daten erhoben werden und das Ergebnis der Sicherheitsüberprüfung zuerst an den Betroffenen und erst dann an die amerikanische Dienststelle übermittelt wird. Die Betroffenen sollen so Bedenken gegen etwa vorliegende Erkenntnisse und deren Übermittlung an die US-Dienststelle erheben können. Entsprechende - datenschutzfreundlichere - Verfahrensweisen finden sich bereits in § 12b des Atomgesetzes und § 7 des Luftsicherheitsgesetzes. Die Änderungswünsche wurden an das Bundesministerium des Innern herangetragen.

9.2 Beschränkung der privaten Internetnutzung am Arbeitsplatz

Ein Mitarbeiter eines Unternehmens teilte uns folgenden Sachverhalt mit und bat uns um eine datenschutzrechtliche Bewertung: Seit einigen Jahren wurde den Mitarbeitern das Internet als Arbeitsmittel zur Verfügung gestellt. Zunächst hatte es für dessen Nutzung keine Regelungen gegeben. Erst einige Zeit später hatte die Geschäftsführung in einem Aushang am schwarzen Brett die private Nutzung des Internets verboten. Ein Jahr später wurde dann eine Filtersoftware installiert, mittels derer die Internetnutzung der Mitarbeiter protokolliert und ausgewertet werden konnte. Diese Filtersoftware diente dem Virenschutz, dem Schutz vor missbräuchlicher Nutzung des Internets sowie der Sicherung von Betriebs- und Geschäftsgeheimnissen. Da der Verdacht bestand, dass Mitarbeiter das Internet für private Zwecke nutzten, wurde eine stichprobenartige personenbezogene Auswertung der von den betreffenden Mitarbeitern aufgerufenen Internetseiten vorgenommen. Die Personalabteilung hatte daraufhin einige Mitarbeiter auf Grund von Verstößen gegen das Verbot der Privatnutzung des Internets abgemahnt. Wie sich aus einer Stellungnahme des Betriebsrats des Unternehmens ergab, war dieser vor der Installierung der Filtersoftware nicht beteiligt worden.

Bei der Bewertung der datenschutzrechtlichen Zulässigkeit der Erhebung, Speicherung und Nutzung von Arbeitnehmerdaten im Rahmen der Kontrolle und Überwachung der Nutzung des Internets am Arbeitsplatz sind einerseits die Folgen der Maßnahme für das allgemeine Persönlichkeitsrecht des Arbeitnehmers und andererseits die betrieblichen Interessen des Arbeitgebers zu berücksichtigen.

Der Arbeitgeber hat das Recht, die Nutzung des Internets auf dienstliche Zwecke zu beschränken. Es ist grundsätzlich auch zulässig, dass er Filtersoftware einsetzt, um den Zugriff auf bestimmte Internetseiten auszuschließen. Eine Protokollierung der Verbindungsdaten zu Zwecken der Datensicherung, des Datenschutzes oder zur Sicherung des ordnungsgemäßen Betriebs der Datenverarbeitungsanlage ist in der Regel zulässig. Problematisch ist es jedoch, wenn der Arbeitgeber die gewonnenen Daten zur Verhaltens- und Leistungskontrolle des Arbeitnehmers nutzt, wie es hier der Fall war. Bei einer derart weitgehenden Überwachung und Kontrolle des Arbeitnehmers durch den Arbeitgeber muss wegen des damit verbundenen Eingriffs in das allgemeine Persönlichkeitsrecht ein gewisses Maß an Transparenz hinsichtlich der vorgesehenen Kontrollen hergestellt werden. Der Arbeitnehmer ist über die Regeln für die Nutzung des Internets und die Voraussetzungen und Modalitäten etwaiger Kontrollen zu informieren, ferner darüber, welche personenbezogenen Daten in diesem Zusammenhang erhoben, gespeichert und genutzt werden und zu welchem Zweck dies konkret geschieht. Hinzuweisen ist auch auf die Tatsache, dass Verbindungsdaten protokolliert und wie diese ausgewertet werden. Auch über etwaige Sanktionen ist zu informieren.

Regelungen zur Nutzung des Internets werden zumeist im Rahmen einer Betriebsvereinbarung getroffen. Entscheidet sich der Arbeitgeber - wie in dem geschilderten Fall - dagegen für eine andere Art der Regelung, so ist auch hier das Mitbestimmungsrecht des Betriebsrats zu beachten. Die Einführung technischer Systeme zur Überwachung des Mitarbeiters ist mitbestimmungspflichtig. Es genügt, dass das System zu einer Überwachung objektiv geeignet und eine Auswertung der Arbeitnehmerdaten unmittelbar möglich ist. Gemessen daran war die Einführung der Filtersoftware hier mitbestimmungspflichtig. Die Beachtung der Mitbestimmungsrechte des Betriebsrats ist als Wirksamkeits- und Rechtmäßigkeitsvoraussetzung für die Datenerhebung und -verarbeitung der Arbeitnehmerdaten anzusehen. Nach der Rechtsprechung des Bundesarbeitsgerichts ist eine technische Überwachung des Arbeitnehmers ohne Beachtung des Mitbestimmungsrechts des Betriebsrats geeignet, das Persönlichkeitsrecht des Arbeitnehmers zu gefährden. Da in dem von uns zu beurteilenden Fall aber eine entsprechende Beteiligung des Betriebsrats nicht erfolgte, war sowohl die Erhebung der Daten mittels der Filtersoftware als auch ihre spätere Verwendung datenschutzrechtlich unzulässig.

Wir teilten dem Unternehmen dieses Ergebnis mit. Wir wiesen es auf die Möglichkeit hin, in einer Betriebsvereinbarung eine auch unter datenschutzrechtlichen Aspekten angemessene Regelung für das Unternehmen zu treffen. Wir rieten dem Unterneh-

men, auf den Betriebsrat zuzugehen und zu einer einvernehmlichen Lösung zu kommen.

9.3 Fertigung von Kopien aus Personalakten

Ein Betriebsratsvorsitzender wandte sich an die Aufsichtsbehörde mit der Frage, ob es datenschutzrechtlich zulässig sei, aus Personalakten von Mitarbeitern Kopien bestimmter Unterlagen zu fertigen und diese dann den jeweiligen Personalvorgesetzten zur Verfügung zu stellen.

Diese Daten wurden benötigt, um die Eingruppierung der Mitarbeiter in bestimmte Entgeltstufen vornehmen zu können, die aufgrund eines neu abgeschlossenen Tarifvertrags notwendig geworden war. Hierfür mussten die jeweilige Qualifikation und die bereits geleisteten Berufsjahre der Mitarbeiter ermittelt und bewertet werden, weshalb die Einsichtnahme in die Personalakten notwendig war. Um das Verfahren zu vereinfachen, beabsichtigte die Geschäftsführung, aus den Personalakten bestimmte Teile (Zeugnisse, Lebensläufe) zu entnehmen und zu kopieren und sie dem jeweiligen Personalvorgesetzten zur Verfügung zu stellen. Dieser sollte das Ergebnis seiner Bewertung dann mit dem jeweiligen Mitarbeiter besprechen.

Hinsichtlich der von dem Unternehmen verwendeten Personalakten waren die Anwendungsvoraussetzungen des BDSG erfüllt, da es sich hier um nicht automatisierte Dateien handelte, die aufgrund ihrer inneren Struktur und der Gliederung in verschiedene Abteilungen (differenziert nach Arbeitsverträgen, Bewerbungsunterlagen, Fortbildungsnachweisen usw.) eine inhaltliche Auswertung ermöglichten.

Wir konnten dem Betriebsratsvorsitzenden nach Anhörung der Geschäftsführung des Unternehmens Folgendes mitteilen: Nach der Rechtsprechung des Bundesarbeitsgerichts ist der Arbeitgeber auf Grund des verfassungsrechtlich gewährleisteten Persönlichkeitsschutzes verpflichtet, die Personalakten des Arbeitnehmers sorgfältig zu verwahren, bestimmte Informationen vertraulich zu behandeln und für die vertrauliche Behandlung durch die Sachbearbeiter zu sorgen. Auch muss der Arbeitgeber den Kreis der mit Personalakten befassten Mitarbeiter möglichst eng halten. Er hat daher sorgfältig zu prüfen, ob es im konkreten Einzelfall tatsächlich erforderlich ist, Einsicht in die Personalakte eines Arbeitnehmers zu nehmen.

Bezogen auf den konkreten Fall bedeutet dies, dass der Arbeitgeber gewährleisten musste, dass der jeweilige Personalverantwortliche nur die für die Bewertung erforderlichen Kopien aus den Personalakten erhielt. Diese mussten in einem verschlos-

senen Umschlag an den jeweiligen Personalvorgesetzten übergeben werden. Es mussten organisatorische Vorkehrungen getroffen werden, dass nur er Zugriff auf die Kopien nehmen konnte. Die Kopien durften ausschließlich zur Ermittlung und Bewertung der für die Eingruppierung maßgeblichen Zeiten verwendet werden; nach Erreichen dieses Zwecks mussten sie vernichtet werden. Nebenakten durften nicht geführt werden und die jeweiligen Vorgesetzten waren nochmals ausdrücklich auf das Datengeheimnis zu verpflichten. Nur bei Gewährleistung dieser Vorkehrungen konnte das Verfahren des Unternehmens als datenschutzrechtlich zulässig erachtet werden.

Neben dieser Bewertung gaben wir dem Betriebsratsvorsitzenden und der Geschäftsführung des Unternehmens auch noch einige Tipps für die praktische Umsetzung dieser Vorgaben.

9.4 Mitarbeiterdaten im Internet

Vermehrt gehen Arbeitgeber dazu über, Personaldaten im Internet zu veröffentlichen, meistens um den Kunden kompetente Ansprechpartner zu benennen. Dieses Bestreben hat in einem der Aufsichtsbehörde vorgetragenen Fall dazu geführt, dass auch Daten eines innerhalb der Probezeit wieder ausgeschiedenen Mitarbeiters samt Begründung für das Ausscheiden im Internet veröffentlicht wurden. Wir beanstandeten dies.

Ein Unternehmen darf Daten seiner Mitarbeiter ohne gesonderte Einwilligungserklärung nur auf Grund einer ausdrücklichen arbeitsvertraglichen Regelung bzw. im Rahmen der Zweckbestimmung des Arbeitsverhältnisses im Internet veröffentlichen (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Mitarbeiter, vor allem in Funktionen mit Außenwirkung und unmittelbarem Kundenkontakt müssen es danach hinnehmen, wenn die Geschäftsleitung im Rahmen ihres Direktionsrechts entscheidet, ihre Namen, Funktionen, Spezialkenntnisse sowie telefonische und elektronische Erreichbarkeit, bekannt zu geben. Zweckmäßig, wenn auch nicht vorgeschrieben ist es, die Mitarbeiter hiervon zu unterrichten.

Eine darüber hinausgehende Bekanntgabe von Mitarbeiterdaten, wie z.B. Privatanschrift, Anzahl der Kinder, Familienstand oder Geburtsdatum, wäre durch diese Vorschrift hingegen nicht gedeckt, sondern bedürfte einer ausdrücklichen Einwilligung des Betroffenen. Dies gilt auch, wenn ein Unternehmen das Bild eines Mitarbeiters veröffentlichen will.

Aus dem Vorstehenden folgt, dass ein Unternehmen die Daten eines ehemaligen Mitarbeiters nicht ohne dessen Einwilligung im Internet veröffentlichen darf.

9.5 Betriebsrats- und Gewerkschaftstätigkeit in Personalunion

In einem der Aufsichtsbehörde vorgetragenen Fall hat sich ein Betriebsratsmitglied einer Organisation in dieser Funktion an mehrere Mitarbeiter gewandt und diese um Mitteilung gebeten, ob sie Mitglied einer Gewerkschaft sind und wenn ja welcher. Es hatte zuvor in seiner Eigenschaft als Vertrauensperson einer Gewerkschaft von dieser eine Liste aller Gewerkschaftsmitglieder in diesem Unternehmen erhalten, um diese zu aktualisieren.

Bei gewerkschaftlichen Vertrauenspersonen handelt es sich um Gewerkschaftsmitglieder, die von der Gewerkschaft bestellt werden und nach deren Weisungen handeln. Sie fungieren als Bindeglied zwischen dem Unternehmen und den Gewerkschaftsmitgliedern im Unternehmen. Sie sollen deren Interessen im Unternehmen wahrnehmen, Tarifverträge und die Tarifpolitik für die Arbeitnehmer vermitteln sowie die Gewerkschaft über Wünsche der Arbeitnehmerschaft informieren. Nach Ansicht des Bundesarbeitsgerichts ist das Institut der gewerkschaftlichen Vertrauenspersonen verfassungsrechtlich durch Art. 9 Abs. 3 des Grundgesetzes abgesichert. Die gewerkschaftlichen Vertrauenspersonen üben in dieser Position eine gewerkschaftliche Funktion aus und sind daher als Teil der Gewerkschaft anzusehen.

Die Funktion der Vertrauensperson einer Gewerkschaft in einem Unternehmen oder einer Organisation wird in der Regel von einem Betriebsratsmitglied wahrgenommen. Beide Funktionen dürfen bezüglich der Erhebung und Verarbeitung personenbezogener Daten nicht miteinander verknüpft werden.

Angaben über die Gewerkschaftszugehörigkeit sind nach § 3 Abs. 9 BDSG besondere Arten personenbezogener Daten. Nach § 28 Abs.9 BDSG dürfen Organisationen, die u.a. gewerkschaftlich ausgerichtet sind und keinen Erwerbszweck verfolgen, besondere Arten personenbezogener Daten erheben, verarbeiten oder nutzen, soweit dies für ihre Tätigkeit erforderlich ist. Dies gilt jedoch nur für personenbezogene Daten ihrer Mitglieder. Die gewerkschaftliche Vertrauensperson als Teil der Gewerkschaft darf also in dieser Funktion Daten der Mitglieder dieser Gewerkschaft in dem Unternehmen erheben und an die Gewerkschaft weitergeben. Daten von Mitgliedern anderer Gewerkschaften darf sie hingegen nicht erheben, da dies weder für „ihre“ Gewerkschaft noch für ihre Arbeit als Vertrauensperson dieser Gewerkschaft erforderlich ist.

Die gewerkschaftliche Vertrauensperson wurde aufgefordert, die unzulässigerweise erhobenen Daten von Mitgliedern anderer Gewerkschaften zu löschen.

10 Videoüberwachung

Zur Videoüberwachung ging eine Vielzahl von Anfragen ein, von Betroffenen, von Firmen, die Videoüberwachungsanlagen projektieren, und von Privatpersonen und Unternehmen, die bei sich eine Videoüberwachungsanlage einrichten wollen. Bei den meist telefonisch durchgeführten Beratungen wurde im Wesentlichen auf den im zweiten Tätigkeitsbericht (S. 23) dargestellten Inhalt der als Nummer 40 unter www.baden-wuerttemberg.de Rubrik: Datenschutz/weitere Infos/Infomaterial veröffentlichten Hinweise des Innenministeriums zum Datenschutz verwiesen. Nachfolgend werden daher nur drei typische Fälle herausgegriffen:

10.1 Rechtswidrige Videoüberwachung durch den Nachbarn

Ein Bewohner eines Einfamilienhauses beschwerte sich bei der Aufsichtsbehörde, dass sein gegenüberliegender Nachbar eine Überwachungskamera direkt auf sein Grundstück gerichtet habe. Zufälligerweise berichtete ein Nachrichtenmagazin über die Videoüberwachung dieses Nachbarn und zeigte dabei auch ein Bild der Überwachungskamera. Daraus konnte entnommen werden, dass die Überwachung des eigenen Grundstücks nur etwa ein Drittel des aufgenommenen Bilds ausmachte und die restlichen zwei Drittel den schmalen Fahrweg zwischen den Grundstücken sowie das Nachbargrundstück des Beschwerdeführers betrafen.

Grundsätzlich darf der Besitzer eines Einfamilienhauses sein Grundstück und den Zugang dazu mit einer Videoüberwachungsanlage selbst überwachen. Die Überwachung muss sich jedoch auf das eigene Grundstück beschränken. Der Anwendungsbereich des BDSG ist bei ausschließlich persönlichen oder familiären Tätigkeiten nicht eröffnet (§ 1 Abs. 3 Nr. 2 BDSG). Um solche handelt es sich jedoch nicht, wie der Düsseldorfer Kreis in einem einstimmig gefassten Beschluss feststellte, wenn der jedermann zugängliche Eingangsbereich einer privaten Haus- oder Wohnungstür videoüberwacht wird, selbst wenn mit der Zugangskontrolle der private Zweck verfolgt wird, sich der Identität eines Besuchers zu versichern.

Da im vorliegenden Fall die Kamera so eingestellt war, dass erhebliche Flächen außerhalb des eigenen Grundstücks mit überwacht wurden, handelte es sich nicht mehr um eine persönliche Tätigkeit. § 6b BDSG, der die Zulässigkeit der Videoüberwa-

chung regelt, war daher anwendbar. Die konkrete Videoüberwachung war nicht - wie es diese Vorschrift verlangt - „erforderlich“ und daher unzulässig. Auch der Hinweis des Überwachers, dass keine andere Kameraausrichtung möglich sei, wenn er sein Grundstück vollständig überwachen wolle, führte zu keiner anderen Beurteilung. Wenn wegen der beengten räumlichen Lage eine bei normalen Verhältnissen zulässige Videoüberwachung schutzwürdige Rechte Dritter tangiert, so muss notfalls der Überwacher eine Einschränkung seiner Möglichkeiten akzeptieren und nicht der Überwachte eine Einschränkung seiner Rechte dulden.

Da die Aufsichtsbehörde selbst keinen Abbau einer unzulässigen Überwachungsanlage verwaltungsrechtlich anordnen und durchsetzen kann, wurde der Beschwerdeführer darauf hingewiesen, dass er vom Überwacher im Klageweg Unterlassung verlangen und dazu die datenschutzrechtliche Beurteilung der Aufsichtsbehörde vorlegen kann.

10.2 Videoüberwachung in Banken

Anlässlich einer Datenschutzüberprüfung einer Bank wurde auch die Videoüberwachung überprüft. Dabei wurde festgestellt, dass im Schalterraum Überfallkameras angebracht sind. Ferner wurden das Foyer der Bankfiliale, der Geldausgabeautomat selbst und der abhebende Kunde aus dem Geldausgabeautomaten heraus überwacht.
Bei den Überfallkameras im Schalterraum handelt es sich um keine Videoüberwachung im Sinne des § 6b BDSG, da die Aufnahmen eine manuelle Betätigung voraussetzen.

Die Foyerräume sind auch außerhalb der Banköffnungszeiten zugänglich. Ihre Überwachung ist zur Verhinderung von Vandalismusschäden und zum Schutz der Kunden erforderlich und damit zulässig. Es genügt jedoch eine kurze Speicherdauer der Überwachungsaufnahme.

Bei der Überwachung des Geldausgabeautomaten im Foyer liegt der Überwachungsgrund in der Verhinderung von Manipulationen am Automaten selbst, durch die beispielsweise die Karte unbemerkt ausgelesen und die PIN erfasst werden kann. Da zwischen der Manipulation und dem missbräuchlichen Abhebungsvorgang einige Tage vergehen, da mit Hilfe der beschafften Daten erst Kartendubletten hergestellt werden müssen, ist hier eine längere Speicherfrist als bei der Foyeraufnahme erforderlich und zulässig. Bei Überwachungsaufnahmen aus dem Geldausgabeautomaten heraus wird nur der Auszahlungsvorgang dokumentiert, d.h. ob und von wem das

Geld aus dem Ausgabefach entnommen wird. Die Datenschutzaufsichtsbehörden der Länder haben den Banken hierfür eine mehrmonatige Speicherfrist zugestanden.

Die konkreten Speicherfristen sind mit uns abgestimmt.

10.3 Videoüberwachung von Arbeitnehmern

Die Aufsichtsbehörde musste sich auch mit Beschwerden über die Videoüberwachung von Arbeitnehmern befassen. In einem Fall diente die permanente Videoüberwachung zumindest auch dem Zweck, dem Firmeninhaber die Beobachtung zu ermöglichen, wie sich seine Mitarbeiter gegenüber Kunden verhalten. Ein besonderer Grund für diese Überwachungsmaßnahme bestand nicht. Der Fall gibt Veranlassung, auf Folgendes hinzuweisen:

- § 6b BDSG gilt für die Überwachung von Arbeitnehmern nur, wenn diese in „öffentlich zugänglichen Räumen“ stattfindet. Öffentlich zugänglich sind nur solche Räume, die ihrem Zweck nach dazu bestimmt sind, von einer unbestimmten Zahl oder nach nur allgemeinen Merkmalen bestimmten Personen betreten und genutzt zu werden. Dazu zählen beispielsweise Ausstellungsräume eines Museums, Verkaufsräume oder Schalterhallen. Nicht öffentlich zugänglich sind hingegen gegenüber Räume, die nur von einem bestimmten Personenkreis betreten werden dürfen.

- Eine analoge Anwendung des § 6b BDSG auf nicht öffentlich zugängliche Räume scheidet nach dem Verlauf des Gesetzgebungsverfahrens aus. § 28 BDSG ist auf solche Fälle ebenfalls nicht anwendbar, weil der Gesetzgeber mit § 6b BDSG erkennbar eine eigenständige, anderen Vorschriften des BDSG vorgehende Regelung für die Videoüberwachung schaffen wollte und zwar unabhängig davon, ob es sich um öffentlich zugängliche Räume handelt oder nicht.

- Unabhängig davon, ob der Anwendungsbereich des BDSG eröffnet ist oder nicht, sind bei der Videoüberwachung von Arbeitnehmern die vom Bundesarbeitsgericht hierzu entwickelten Grundsätze (vgl. Beschluss vom 29.06.2004 - 1 ABR 21/03, RDV 2005, 21 mit weiteren Nachweisen) zu beachten. Die Videoüberwachung muss geeignet, erforderlich und unter Berücksichtigung der gewährleisteten Freiheitsrechte angemessen sein, um den erstrebten Zweck zu erreichen. Der Zweck der Videoüberwachung und die Art und Weise der Durchführung, insbesondere auch die Dauer der Überwachung spielen dabei eine Rolle. Insgesamt aber sind der Videoüberwachung von Arbeitnehmern, die im Übrigen der Mitbestimmung des

Betriebsrats unterliegt, wegen des damit verbundenen Überwachungsdrucks enge Grenzen gesetzt.

11 Internationaler Datenverkehr

Die Aufsichtsbehörde hat sich in ihrem zweiten Tätigkeitsbericht (S. 30 ff.) ausführlich mit Fragen des internationalen Datenverkehrs befasst, insbesondere mit der Zulässigkeit von Datenübermittlungen auf Grund verbindlicher Unternehmensregelungen und von Standardvertragsklauseln sowie mit deren Genehmigungsbedürftigkeit nach § 4c Abs. 2 BDSG. Diese Themen haben uns auch in den vergangenen beiden Jahren beschäftigt. Vermehrt ist festzustellen, dass die Praxis Datenübermittlungen ins Ausland ausschließlich an § 4b und § 4c BDSG misst. Sie übersieht dabei, dass Datenübermittlungen zuallererst den im Inland geltenden Vorschriften genügen müssen (1. Stufe der Prüfung). Erst auf der 2. Stufe ist zu prüfen, ob eine Datenübermittlung ins Ausland, insbesondere in einen Drittstaat nach § 4b oder § 4c BDSG zulässig ist.

12 Vereine

12.1 Datenschutz im Verein

12.1.1 Übermittlung von Mitgliederdaten zur Wahlwerbung

Ein Gemeinderatskandidat, zugleich Mitglied in einem Sportverein, ließ sich von einem Vereinskollegen eine Liste der Vereinsmitglieder übermitteln, um diese anzuschreiben und für seine Wahl zu werben. Auf die Beschwerde eines Betroffenen hin haben wir dies mangels Rechtsgrundlage und Einwilligung der Betroffenen für unzulässig erklärt.

Die Übermittlung war zur Wahrung berechtigter Interessen des Kandidaten nicht - wie es § 28 Abs. 3 Satz 1 Nr. 1 BDSG verlangt - „erforderlich“. Auch konnte er sich nicht auf das sogenannte Listenprivileg des § 28 Abs. 3 Satz 1 Nr. 3 BDSG berufen, wonach bestimmte listenmäßig zusammengefasste Daten über Angehörige einer Personengruppe (hier Namen, Anschrift und die Tatsache der Vereinszugehörigkeit) an Dritte übermittelt werden dürfen, wenn kein Grund zu der Annahme besteht, dass die Betroffenen ein schutzwürdiges Interesse am Ausschluss der Übermittlung haben. Ein solcher Ausschlussgrund lag hier nämlich vor. Bei der Mitgliedschaft in einem Verein handelt es sich um ein personenrechtliches Rechtsverhältnis, aus dem sich besondere Rücksichtnahmepflichten in Bezug auf die schutzwürdigen Belange der Vereinsmitglieder ergeben. Daraus folgt, dass personenbezogene Daten der

Vereinsmitglieder von vornherein nur unter ganz engen Voraussetzungen ohne Einwilligung für vereinsfremde Zwecke weitergegeben werden dürfen. Im vorliegenden Fall kam hinzu, dass die Daten für Zwecke der politischen Wahlwerbung verwendet werden sollten und auch verwendet wurden. Hier ist regelmäßig davon auszugehen, dass zumindest ein Teil der Vereinsmitglieder die Weitergabe der Daten nicht wünscht.

12.1.2 Veröffentlichung von Spielerdaten im Internet

Ein Sportverein fragte uns, ob auf Vereins- oder Verbandsebene Ranglisten, Bestenlisten, Mannschaftsaufstellungen und Spielerergebnisse im Internet veröffentlicht werden dürfen. Wir bejahten dies.

§ 28 Abs. 1 Satz 1 Nr. 3 BDSG lässt die Übermittlung personenbezogener Daten zu, wenn sie allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass schutzwürdige Interessen der Betroffenen am Ausschluss der Übermittlung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegen.
Die von einem Verband ausgerichteten Sportveranstaltungen sind öffentlich. Die Namen und die Ergebnisse der Spieler werden dort öffentlich bekannt gegeben. Es handelt sich damit um allgemein zugängliche Daten. Die Daten der Rang- und Bestenlisten sind zwar nicht allgemein zugänglich, stammen jedoch aus allgemein zugänglichen Quellen und stellen nur eine Zusammenfassung und Auswertung dieser Daten dar.

Auch sind keine Anhaltspunkte ersichtlich, dass hier das schutzwürdige Interesse der Spieler an einem Ausschluss der Veröffentlichung das berechtigte Interesse des Verbands offensichtlich überwiegt. Zwar erschließt die Veröffentlichung im Internet die Daten einem unbegrenzten Teilnahmerkreis, auch stellen diese anders als bei der Tagespresse für einen längeren Zeitraum zur Verfügung. Es ist aber nicht anzunehmen, dass durch die Veröffentlichung des **Namens, der Vereinszugehörigkeit** und in Ausnahmefällen des Geburtsjahrgangs eines Spielers im Internet dessen Persönlichkeitsrecht stärker beeinträchtigt wird als durch die Veröffentlichung in einer Tageszeitung, in deren Verbreitungsgebiet er wohnt und bekannt ist. Dabei berücksichtigt die Aufsichtsbehörde, dass gerade die Vereine und die Spieler selbst diese Informationsmöglichkeit nutzen wollen.

Nur mit ausdrücklicher Einwilligung des Betroffenen dürften hingegen dessen **Geburtsdatum** und **private Anschrift** in das Internet eingestellt werden.

12.1.3 Übermittlung von Vereinsmitgliederdaten an Versicherungen für den Abschluss von Gruppenversicherungsverträgen

Nach wie vor ist es üblich, dass Vereine mit Versicherungsunternehmen sogenannte Gruppenversicherungsverträge abschließen, denen die Mitglieder durch den Abschluss von Einzelverträgen beitreten können. Bereits vor mehreren Jahren wurden zwischen den Aufsichtsbehörden für den Datenschutz und den Verbänden der Versicherungswirtschaft Absprachen getroffen, wonach ein Verein im Rahmen eines Gruppenversicherungsvertrags dem Versicherungsunternehmen bzw. dem Versicherungsvertreter die Daten seiner Mitglieder nur unter folgenden Voraussetzungen übermitteln darf:

- Bei Neumitgliedern, die nach Abschluss des Gruppenversicherungsvertrags dem Verein beitreten, muss die Einwilligung eingeholt werden. Dies sollte zweckmäßigerweise in der Beitrittserklärung oder im Aufnahmeantrag vorgesehen werden, wobei das Mitglied darüber aufzuklären ist, welche Daten an welches Unternehmen weitergegeben werden sollen.
- Bei Altmitgliedern, die beim Abschluss des Gruppenversicherungsvertrags bereits Vereinsmitglieder waren, genügt es, wenn der Verein sie vor der Übermittlung ihres Namens und ihrer Anschrift an die Versicherung in einem Avis-Schreiben informiert und ihnen den Besuch eines Versicherungsvertreters ankündigt. In dem Avisschreiben muss auf die Möglichkeit des Widerspruchs gegen die Datenübermittlung und den Vertreterbesuch hingewiesen und dem Vereinsmitglied ausreichend Zeit (vier Wochen) eingeräumt werden, von dieser Widerspruchsmöglichkeit Gebrauch zu machen.

Diese Grundsätze sind in dem von der Aufsichtsbehörde veröffentlichten Merkblatt „Datenschutz im Verein“ enthalten. Es kommt jedoch immer wieder vor, dass Vereine in bester Absicht die Daten ihrer Mitglieder an die Versicherungsunternehmen übermitteln und ihre Mitglieder nicht darüber informieren. Wenn die Vereinsmitglieder dann von einem Versicherungsunternehmen bzw. Versicherungsvertreter angesprochen werden, wenden sie sich an die Aufsichtsbehörde. In solchen Fällen ist regelmäßig festzustellen, dass die Verantwortlichen von den Versicherungsunternehmen nicht über die mit den Aufsichtsbehörden abgesprochenen Modalitäten aufgeklärt wurden.

Da in jüngster Zeit eine Versicherung versuchte, die verabredeten Grundsätze in Frage zu stellen, hat sich der Düsseldorfer Kreis erneut mit dem Thema befasst und

nochmals bekräftigt, dass es nicht genügt, wenn der Verein durch Hinweise am Schwarzen Brett in der Vereinsgeschäftsstelle, im Vereinslokal oder in der Vereinszeitschrift auf die beabsichtigte Übermittlung der Daten an die Versicherung hinweist. Vereinssatzungen können in der Regel nur dann eine Rechtsgrundlage für die Datenübermittlung an eine Versicherung darstellen, wenn mit der Mitgliedschaft automatisch der Abschluss einer mit dem Vereinszweck zusammenhängenden Versicherung verbunden ist oder die Einbeziehung in eine solche Versicherung erfolgt (z. B. Unfallversicherung bei einem Sportverein).

12.2 Übermittlung von Daten einer Selbsthilfegruppe an Kooperationspartner

Ein Mitglied einer Selbsthilfegruppe im medizinischen und sozialen Bereich beschwerte sich darüber, dass der zuständige Verband seine Daten an eine andere Organisation für Werbezwecke übermittelt hatte. Die Überprüfung ergab, dass diese Organisation in Kooperation mit dem Verband eine Veranstaltung zum Themenbereich der Selbsthilfegruppe durchgeführt und die Daten für die Einladung benutzt hatte. Der Verband erklärte, es habe sich um eine vom Verbandszweck getragene Informationsveranstaltung gehandelt. Er selbst sei nicht in der Lage gewesen, sämtliche Mitglieder einzuladen. Zudem habe die Organisation auch die Kosten dafür übernommen. Gleichwohl hätten in diesem Fall die Daten der Mitglieder der Selbsthilfegruppe nicht übermittelt werden dürfen, weil es sich hier um besonders geschützte Daten nach § 3 Abs. 9 BDSG handelte. Es hätte für die Übermittlung der ausdrücklichen Einwilligung der Betroffenen bedurft.

Die Datenempfängerin versicherte, die Daten nur für die Einladung benutzt und anschließend vernichtet zu haben.