Landtag von Baden-Württemberg **Drucksache 14 / 1475**

14. Wahlperiode **29. 06. 2007**

Mitteilung

des Innenministeriums

Vierter Tätigkeitsbericht des Innenministeriums zum Datenschutz im nichtöffentlichen Bereich

Schreiben des Innenministeriums vom 28. Juni 2007 Nr. 2-0552.6/36:

In der Anlage zu diesem Schreiben übersende ich Ihnen den vierten Bericht des Innenministeriums über die Tätigkeit der für den Datenschutz im nichtöffentlichen Bereich zuständigen Aufsichtsbehörde, der dem Landtag nach § 39 des Landesdatenschutzgesetzes zu erstatten ist.

Rech

Innenminister

Eingegangen: 29. 06. 2007 / Ausgegeben: 25. 07. 2007

Datenschutz im nichtöffentlichen Bereich

Vierter Tätigkeitsbericht des Innenministeriums nach § 39 des Landesdatenschutzgesetzes 2007

Baden-Württemberg
INNENMINISTERIUM

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. Der Bericht dient zugleich der Unterrichtung der Öffentlichkeit. Er ist auch dazu bestimmt, nichtöffentliche Stellen und betriebliche Datenschutzbeauftragte über die Auffassung der Aufsichtsbehörde zu bestimmten Fragen zu informieren.

Dies ist der vierte Bericht nach Einführung der gesetzlichen Berichtspflicht. Er baut auf den ersten drei Tätigkeitsberichten (Landtags-Drucksachen 13/40, 13/2200 und 13/4469) auf und beschränkt sich im Wesentlichen auf Neuerungen und Entwicklungen, die im Berichtszeitraum (1. Juli 2005 bis 30. Juni 2007) eingetreten sind.

A Entwicklung der Aufgaben und des Datenschutzrechts seit 2005

1 Allgemeines zur Aufsichtstätigkeit

1.1 Eingaben, Anlasskontrollen

Schwerpunkt der Tätigkeit der Aufsichtsbehörde war 2005 und 2006 wiederum die Bearbeitung von Beschwerden betroffener Bürger. In diesen beiden Jahren machten insgesamt 850 Bürger von ihrem Recht Gebrauch, die Datenschutzaufsicht anzurufen. Zwar ging die Zahl der Beschwerden damit gegenüber den Vorjahren leicht zurück. Die Beschwerden waren aber teilweise erheblich komplexer als früher. Die meisten Eingaben betrafen Auskunfteien, Kreditschutzorganisationen und Inkassounternehmen, gefolgt von Einzel-, Groß- und Versandhandel, dem Adresshandel und der Direktmarketing- und Werbebranche einschließlich der Lotterien, der Kreditwirtschaft und – branchenunabhängig – der Videoüberwachung. Seltener waren Eingaben zum Versicherungs- und zum Gesundheitsbereich, zum Arbeitnehmerdatenschutz, zum Datenschutz in Vereinen sowie zur Markt- und Meinungsforschung.

Die meisten Beschwerden konnten im schriftlichen Verfahren mit den betroffenen Unternehmen geklärt werden. In einigen Fällen waren *Anlasskontrollen* erforderlich, beispielsweise bei Lotterien, Call-Centern, den Betreibern eines Internetportals, einer Auskunftei, einer Rechtsanwaltskanzlei, einem Krankenhaus, einer Arztpraxis, einer Partnervermittlung und zur Überprüfung mehrerer Videoüberwachungsanlagen.

Häufig festgestellte Mängel waren die Nichterfüllung beziehungsweise die nicht rechtzeitige Erfüllung des Auskunftsanspruchs des Bürgers nach § 34 des Bundesdatenschutzgesetzes (BDSG), die zu Unrecht verweigerte Auskunft über die Datenempfänger, die Erhebung und Speicherung nicht erforderlicher Daten, die Nichtbeachtung der Aufklärungs- und Informationspflichten bei der Erhebung von Daten beim Betroffenen (§ 4 Abs. 3 BDSG), die Nichtbeachtung des Grundsatzes der Direkterhebung beim Betroffenen (§ 4 Abs. 2 BDSG), die Erhebung, Verarbeitung und Nutzung personenbezogener Daten auf der Grundlage nicht wirksamer Einwilligungserklärungen (§ 4 a BDSG), die Videobeobachtung und Anfertigung von Videoaufzeichnungen ohne Vorliegen der gesetzlichen Voraussetzungen des § 6 b BDSG, die Nichtdurchführung gebotener Datensperrungen und -löschungen, der in Werbeschreiben fehlende beziehungsweise unzureichend gefasste Hinweis auf die Möglichkeit, gegen die Nutzung oder Übermittlung der Daten zu Werbezwecken Widerspruch einzulegen (§ 28 Abs. 4 BDSG) sowie die Nichtbeachtung des Werbewiderspruchs.

1.2 Anlassunabhängige Kontrollen

Die Aufsichtsbehörde führte im Berichtszeitraum einige anlassunabhängige Kontrollen bei Auskunfteien, Kreditschutzorganisationen und Inkassounternehmen durch. Über deren Ergebnisse wird nur insoweit berichtet, als die Auswertung der umfangreichen Überprüfungen bereits abgeschlossen ist.

1.3 Beratung von Bürgern, Unternehmen und betrieblichen Datenschutzbeauftragten

Zusätzlich zu den förmlichen Beschwerden gab es 420 schriftliche und ca. 4.000 telefonische Anfragen und Beratungswünsche von Bürgern, Unternehmen und betrieblichen Datenschutzbeauftragten. Die Zahl der schriftlichen Anfragen ist damit um circa 80 % gestiegen. Zugenommen hat insbesondere die Zahl der schriftlichen Anfragen externer betrieblicher Datenschutzbeauftragter und von kleinen Unternehmen, in denen es um die Frage ging, ob ein betrieblicher Datenschutzbeauftragter bestellt werden muss.

Unverändert gilt jedoch die Aussage aus dem letzten Tätigkeitsbericht, betriebliche Datenschutzbeauftragte scheuten sich, Kontakt zur Aufsichtsbehörde aufzu-

nehmen. Der damalige Appell, stärker von dieser im Bundesdatenschutzgesetz ausdrücklich vorgesehenen Möglichkeit Gebrauch zu machen und die Aufsichtsbehörde insbesondere vor dem Einsatz neuer Formen der Datenverarbeitung oder bei Fragen zur Auslegung des Bundesdatenschutzgesetzes zu beteiligen, blieb – von den oben genannten Fällen abgesehen – leider weitgehend unbeachtet. Die Aufsichtsbehörde kann deshalb nur noch einmal wiederholen, dass sie der Beratung einen hohen Stellenwert beimisst. Vorbeugender Datenschutz ist der beste Datenschutz.

Im Rahmen ihrer personellen und finanziellen Möglichkeiten nimmt die Aufsichtsbehörde auch an den von der Gesellschaft für Datenschutz und Datensicherung e. V. mehrmals im Jahr in Stuttgart, Karlsruhe, Mannheim/Ludwigshafen und Freiburg veranstalteten Sitzungen der Erfahrungsaustausch-Kreise der betrieblichen Datenschutzbeauftragten teil, in denen aktuelle Datenschutz- und Datensicherheitsfragen erörtert werden.

1.4 Datenschutzregister

In dem von der Aufsichtsbehörde nach § 38 Abs. 2 BDSG zu führenden Datenschutzregister haben sich nur geringfügige Änderungen ergeben. Es sind insgesamt 87 nichtöffentliche Stellen mit 95 automatisierten Verfahren gemeldet. 64 dieser Verfahren dienen dem Zweck der Übermittlung personenbezogener Daten (Auskunfteien und Adresshändler), 31 dem Zweck der anonymisierten Datenübermittlung (Markt- und Meinungsforschungsinstitute).

Es besteht allerdings nach wie vor der Eindruck, dass nicht alle meldepflichtigen Verfahren gemeldet sind. Stattdessen melden Unternehmen immer wieder nicht meldepflichtige Verfahren an.

1.5 Ordnungswidrigkeitenverfahren

Nach dem Bundesdatenschutzgesetz ist eine Reihe von Verstößen gegen dieses Gesetz bußgeldbewehrt. Die Aufsichtsbehörde macht von der Möglichkeit, ein Bußgeld zu verhängen, allerdings sehr zurückhaltend Gebrauch. Der Aufsichtsbehörde ist es wichtiger, für die Zukunft ein datenschutzgerechtes Verhalten eines Unternehmens sicherzustellen, als Verstöße in der Vergangenheit zu ahnden.

Im Berichtszeitraum hat die Aufsichtsbehörde in insgesamt zehn Fällen ein Bußgeldverfahren eingeleitet. Fünf Fälle wurden mit dem Erlass eines Bußgeldbescheid abgeschlossen, der bestandskräftig wurde. Dreimal wurde eine Geldbuße in Höhe von 500 € verhängt, davon zweimal wegen nicht sachgerechter Entsorgung von Patientenunterlagen durch einen Arzt und einmal wegen einer unbefugten Datenerhebung bei der Kraftfahrzeugzulassungsstelle. In einem Fall wurde wegen einer unbefugten SCHUFA-Abfrage, in einem anderen Fall wegen einer zu privaten Zwecken erfolgten Abfrage von Bankdaten einer Kundin durch einen Bankmitarbeiter eine Geldbuße von 300 € festgesetzt. Keinen Bestand hatte ein von der Aufsichtsbehörde gegen den Verantwortlichen eines Unternehmens erlassener Bußgeldbescheid über 500 €. Der Betroffene hatte gegenüber der Aufsichtsbehörde beharrlich die Erteilung von Auskünften verweigert. Nach dem Einspruch des Betroffenen stellte das Amtsgericht das Verfahren ein.

2 Rechtsentwicklung

2.1 Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz wurde durch das Erste Gesetz zum Abbau bürokratischer Hemmnisse insbesondere in der mittelständischen Wirtschaft vom 22. August 2006 (BGBl. I S. 1970) in einigen Punkten geändert. Unternehmen müssen erst ab zehn „ständig“ mit der Verarbeitung personenbezogener Daten beschäftigten Personen einen Beauftragten für den Datenschutz bestellen; bisher bestand die gesetzliche Verpflichtung schon ab fünf Arbeitnehmern. Die Erhöhung der maßgeblichen Personenzahl dient nach der Gesetzesbegründung einem sachgerechten Ausgleich im Spannungsverhältnis zwischen dem Ziel, kleinere Unternehmen zu entlasten und dem Erfordernis, personenbezogene Daten zu schützen. Unterneh-

men, die weniger als zehn Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigten, wickelten in der Regel entweder ein im Hinblick auf den Datenschutz eher weniger belastendes Massengeschäft ab oder bedienten einen überschaubaren Kundenkreis.

Diese Änderung ist aus der Sicht des Datenschutzes keineswegs unproblematisch, da gerade kleine nichtöffentliche Stellen häufig über keine oder nur geringe Datenschutzkenntnisse verfügen. Die Zustimmung zur Gesetzesänderung wurde jedoch dadurch erleichtert, dass gleichzeitig bestimmt wurde, dass in nichtöffentlichen Stellen, die keinen Datenschutzbeauftragten bestellen müssen, der Leiter verpflichtet ist, die Erfüllung der ansonsten betrieblichen Datenschutzbeauftragten übertragenen Aufgaben in anderer Weise sicherzustellen. Daraus ergibt sich, dass sich gegebenenfalls der Leiter der nichtöffentlichen Stelle die notwendigen Datenschutzkenntnisse selbst aneignen und dafür Sorge tragen muss, dass seine Mitarbeiter das Bundesdatenschutzgesetz und andere Vorschriften über den Datenschutz einhalten.

Mitzuzählen sind nur noch Personen, die „in der Regel ständig“ mit der automatisierten Datenverarbeitung beschäftigt sind. Urlaubsvertretungen sind also nicht zu berücksichtigen. Indem das Wort „Arbeitnehmer“ durch das Wort „Personen“ ersetzt wurde, wurde ferner klargestellt, dass aus datenschutzrechtlicher Sicht allein die Anzahl und nicht der Status der mit der automatisierten Verarbeitung personenbezogener Daten beschäftigten Personen maßgeblich ist.

Mit einer weiteren Neuregelung wird einem Anliegen der Aufsichtsbehörde Rechnung getragen, es auch Berufsgeheimnisträgern (zum Beispiel Ärzten oder Rechtsanwälten) zu ermöglichen, eine Person außerhalb der nichtöffentlichen Stelle als Beauftragten für den Datenschutz zu bestellen (siehe hierzu dritter Tätigkeitsbericht B 2.2, S. 20 ff.).

Die vom Deutschen Bundestag im Zusammenhang mit der Verabschiedung des Änderungsgesetzes 2001 ausgesprochene Erwartung, das Bundesdatenschutzgesetz werde bald umfassend reformiert, bleibt damit nach wie vor unerfüllt. Realistischer ist es wohl, von weiteren punktuellen Änderungen des Bundesdatenschutzgesetzes auszugehen. Für vordringlich hält es die Aufsichtsbehörde, klarzustellen, dass auch Rechtsanwälte den Vorschriften des Bundesdatenschutzgesetzes unterliegen und die Arbeit der Auskunfteien präziseren Regeln zu unterwerfen (siehe dazu unten C 2 und 3.2).

2.2 Neues Telemediengesetz und Neunter Rundfunkänderungsstaatsvertrag

Am 1. März 2007 trat das Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz vom 26. Februar 2007 (BGBl. I S. 179) in Kraft. Das Artikelgesetz beinhaltet unter anderem das neue Telemediengesetz (TMG). Gleichzeitig trat der Neunte Rundfunkänderungsstaatsvertrag in Kraft. Damit wurde ein einheitlicher Rechtsrahmen für elektronische Medien geschaffen.

Das neue Recht trat an die Stelle des Teledienstegesetzes, des Teledienstedatenschutzgesetzes und des Mediendienste-Staatsvertrags. Die Begriffe „Teledienste“ und „Mediendienste“ wurden durch den einheitlichen Begriff „Telemedien“ ersetzt. Die Zuständigkeiten der Länder für den Rundfunk und des Bundes für Telemedien bleiben erhalten. Der Datenschutz ist jetzt weitgehend im Telemediengesetz geregelt. Inhaltlich wurden im Wesentlichen die bisherigen datenschutzrechtlichen Regelungen des Teledienstedatenschutzgesetzes und des Mediendienste-Staatsvertrags übernommen.

Neu ist § 6 Abs. 2 TMG. Danach darf bei kommerziellen Mails in der Kopf- und Betreffzeile weder der Absender noch der Inhalt der Nachricht verschleiert oder verheimlicht werden. Damit soll der Einsatz von Filtern zum Blockieren und Aussortieren kommerzieller Mails erleichtert werden. Eine Zuwiderhandlung kann mit einem Bußgeld geahndet werden. Erweitert wurden die Auskunftspflichten für Teledienstеanbieter. Sie erstrecken sich nunmehr auch auf die Bestandsdaten, soweit dies zur Gefahrenabwehr durch die Polizeibehörden der Länder oder zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist.

Für den Rundfunk und die von öffentlichen Stellen der Länder betriebenen Telemedien gelten über eine Verweisung im Rundfunkstaatsvertrag die datenschutz-

rechtlichen Vorschriften im Telemediengesetz. Die Verarbeitung personenbezogener Daten zu journalistisch-redaktionellen Zwecken ist wie bisher im Rundfunkstaatsvertrag geregelt.

Unklar geregelt ist nach wie vor die datenschutzrechtliche Kontrollzuständigkeit für Access-Provider (Internet-Zugangsanbieter) und E-Mail-Diensteanbieter. Sie unterliegen nach bisherigem Rechtsverständnis hinsichtlich derjenigen Rechtsvorschriften, die für diese Anbieter zusätzlich zu den Vorschriften des Telekommunikationsgesetzes gelten (§ 11 Abs. 3 TMG), der Kontrolle der für den nichtöffentlichen Bereich zuständigen Datenschutzaufsichtsbehörden der Länder. Wünschenswert wäre, dass für die datenschutzrechtliche Kontrolle von Internet-Zugangsanbietern und E-Mail-Diensteanbietern allein der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) zuständig ist. Damit läge die Bearbeitung von Eingaben, die beide Bereiche berühren, in einer Hand.

Hierzu findet derzeit ein Meinungsaustausch in den Gremien des Düsseldorfer Kreises [1)] statt.

2.3 Kreditwesengesetz

Das Kreditwesengesetz (KWG) wurde durch das Gesetz zur Umsetzung der neu gefassten Bankenrichtlinie und der neu gefassten Kapitaladäquanzrichtlinie vom 17. November 2006 (BGBl. I S. 2606) geändert. Datenschutzrechtlich bedeutsam ist der neu gefasste § 10 KWG. Danach müssen die Kreditinstitute im Interesse der Erfüllung ihrer Verpflichtungen gegenüber ihren Gläubigern, insbesondere im Interesse der Sicherheit der ihnen anvertrauten Vermögenswerte, künftig angemessene Eigenmittel haben (sogenannte risikoadäquate Eigenkapitalausstattung). Zur Messung des Risikos dürfen Kreditinstitute mit vorheriger Zulassung durch die Bundesanstalt für Finanzdienstleistungsaufsicht interne Risikomessverfahren zur Beurteilung der Angemessenheit ihrer Eigenmittelausstattung einführen. Sie dürfen zu diesem Zweck personenbezogene Daten ihrer Kunden, von Personen, mit denen sie Vertragsverhandlungen über Adressenausfallrisiken begründende Geschäfte aufnehmen, sowie von Personen, die für die Erfüllung eines Adressenausfallrisikos einzustehen haben, erheben und verwenden, soweit diese Daten

- unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Bestimmung und Berücksichtigung von Adressenausfallrisiken erheblich und
- zum Aufbau und Betrieb von internen Ratingsystemen für die Schätzung von Risikoparametern des Adressenausfallrisikos des Instituts erforderlich sind; ausgenommen sind Angaben zur Staatsangehörigkeit und besonders sensitive Daten nach § 3 Abs. 9 BDSG.

Für die Bestimmung und Berücksichtigung von Adressenausfallrisiken können insbesondere Daten erheblich sein, die den folgenden Kategorien angehören oder aus Daten der folgenden Kategorien gewonnen worden sind:

- Einkommens-, Vermögens- und Beschäftigungsverhältnisse sowie die sonstigen wirtschaftlichen Verhältnisse,
- das Zahlungsverhalten und die Vertragstreue des Betroffenen,
- vollstreckbare Forderungen sowie Zwangsvollstreckungsverfahren und Zwangsvollstreckungsmaßnahmen gegen den Betroffenen,
- Insolvenzverfahren über das Vermögen des Betroffenen, sofern diese eröffnet worden sind oder die Eröffnung beantragt worden ist.

Diese Daten dürfen beim Betroffenen, bei Institutionen, die derselben Institutsgruppe angehören, bei Ratingagenturen und Auskunfteien sowie aus allgemein zugänglichen Quellen erhoben werden.

[1)] Im Düsseldorfer Kreis sind die obersten Aufsichtsbehörden der Länder für den Datenschutz im nichtöffentlichen Bereich und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit vertreten.

Im Gesetzgebungsverfahren wurde klargestellt, dass § 10 KWG nicht für das sogenannte Scoring [2)] gilt. § 10 KWG regelt die kreditaufsichtsrechtlichen Anforderungen und die Eigenkapitalausstattung der Kreditinstitute und begründet Pflichten im Verhältnis zwischen den Kreditinstituten und der Kreditaufsicht; er regelt nicht die Bewertung der Kreditwürdigkeit der Kunden im Außenverhältnis zu diesen. Im Unterschied zu der internen Risikobemessung nach § 10 KWG betrifft das Scoring das Verhältnis des Instituts zum Kunden und ist mitentscheidend für den Abschluss eines Kreditvertrags und seine konkrete Ausgestaltung. Gleichwohl hat § 10 KWG nach Auffassung des Düsseldorfer Kreises Auswirkungen auf die Erhebung, Verarbeitung und Nutzung personenbezogener Daten beim Einsatz von Scoringverfahren im Bereich der Kreditwirtschaft.

Ausgangspunkt aller Überlegungen ist, dass für die Berechnung von Scorewerten im Bereich der Kreditwirtschaft nur Daten verwendet werden dürfen, deren Bonitätsrelevanz mittels eines wissenschaftlichen Standards entsprechenden mathematisch-statistischen Verfahrens nachgewiesen wurde. Das allein genügt jedoch nicht. Weitere Voraussetzung ist, dass nur solche Daten in ein Scoringverfahren einbezogen werden dürfen, die ein Kreditinstitut für einen Kreditvertrag erheben darf. Die Nutzung von Daten für ein Scoringverfahren ist zulässig, soweit es zur Wahrung berechtigter Interessen des Kreditinstituts erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Kreditantragstellers am Ausschluss der Verarbeitung oder Nutzung überwiegt. Bei dieser Abwägung können – so der Düsseldorfer Kreis – die gesetzgeberischen Wertungen des § 10 KWG herangezogen werden. Die Merkmale, die in ein Scoringverfahren einfließen dürfen, müssen daher ebenso stringent sein wie der Merkmalskatalog des § 10 KWG. Angaben zur Staatsangehörigkeit und weitere sensitive Angaben nach § 3 Abs. 9 BDSG sind als Scoremerkmale ausgeschlossen.

2.4 Heilberufe-Kammergesetz

Datenschutzrechtlich bedeutsam ist auch die durch Gesetz vom 14. Februar 2006 (GBl. S. 23) erfolgte Änderung des Heilberufe-Kammergesetzes. Danach sind die Kammern verpflichtet, Patientenunterlagen von Kammermitgliedern für die Dauer der Aufbewahrungszeiten in Obhut zu nehmen und den Patienten Einsicht in die Unterlagen zu gewähren, sofern dies nicht auf andere Weise gewährleistet ist. Die Verpflichtung besteht auch auf Ersuchen einer öffentlichen Stelle, die sich nicht in der Lage sieht, Patientenunterlagen aufzubewahren und in diese Einsicht zu gewähren.

Diese – von der Aufsichtsbehörde angeregte – Regelung wurde eingefügt, um die Kammern in Fällen heranzuziehen, in denen die Patientenakten nach Auflösung einer Arztpraxis, dem Tod des Heilberuflers, der Insolvenz des Arztes oder bei Herrenlosigkeit ungesichert sind und die Patienten ihr Recht auf Einsichtnahme in ihre Unterlagen nicht verwirklichen können. Da es um berufliche Pflichten ihrer – ehemaligen – Mitglieder geht, ist die Verpflichtung der Kammern sachnäher als die Inanspruchnahme der Gemeinden als Ortspolizeibehörden, die zuvor aufgrund des Polizeigesetzes hatten tätig werden müssen, sich zur Erfüllung der genannten Pflichten aber zumeist nicht in der Lage gesehen hatten (vergleiche zum Ganzen den dritten Tätigkeitsbericht C 6.2.2, S. 106 ff.). Außerdem ist bei den Kammern auch der notwendige medizinische und therapeutische Sachverstand vorhanden, damit die sensitiven Akten nicht nur sicher verwahrt werden, sondern den betroffenen Patienten auch nach Beendigung des Arzt-, Zahnarzt- oder Psychotherapeutenpatientenverhältnisses zugänglich bleiben, wenn dies durch den Heilberufler oder seinen Rechtsnachfolger nicht gewährleistet ist.

Die Erfahrungen mit der Neuregelung bleiben abzuwarten.

[2)] siehe hierzu die Erläuterung unter C.3.2.

B Allgemeine Fragen des Bundesdatenschutzgesetzes – Überprüfung der Einhaltung der Unterrichtungspflichten bei der Datenerhebung (§ 4 Abs. 3 BDSG)

Nach § 4 Abs. 3 Satz 1 BDSG muss eine nichtöffentliche Stelle, die personenbezogene Daten „beim“ Betroffenen erhebt, diesen über

- ihre Identität,
- die Zweckbestimmungen der Erhebung, Speicherung, Übermittlung und Nutzung der Daten und
- die Kategorien von Datenempfängern unterrichten, soweit der Betroffene nach den Umständen des Einzelfalls nicht mit der Übermittlung an diese rechnen muss.

Außerdem muss der Betroffene, sofern die Daten bei ihm aufgrund einer Rechtsvorschrift, die zur Auskunft verpflichtet, erhoben werden oder die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen ist, hierauf, sonst auf die Freiwilligkeit seiner Angaben hingewiesen werden (§ 4 Abs. 3 Satz 2 BDSG).

Durch diese Hinweis- und Aufklärungspflichten soll der Betroffene in die Lage versetzt werden, darüber zu entscheiden, ob er seine Daten preisgeben will oder nicht.

Die Aufsichtsbehörde hat bereits 2002 mit ihrem – vorwiegend an die betrieblichen Datenschutzbeauftragten, aber auch alle anderen Interessierten gerichteten – Hinweis Nr. 41 [3)] versucht, diese in der Praxis wenig beachtete Vorschrift stärker in das Blickfeld zu rücken. Vor allem die in dem Hinweis dargestellten Folgen einer unterbliebenen Unterrichtung hatten seinerzeit eine lebhafte Diskussion ausgelöst (vergleiche dazu den dritten Tätigkeitsbericht B 1, S. 13 ff.).

Da wir wissen wollten, ob dies auch zu einer stärkeren Beachtung der Vorschrift in der Praxis geführt hat, baten wir eine Reihe von Unternehmen, einen Fragebogen auszufüllen und uns ihre Papier- oder Online-Formulare, mit denen sie Daten beim Betroffenen erheben, zu übersenden. Auch wenn noch nicht die Unterlagen aller beteiligten nichtöffentlichen Stellen ausgewertet werden konnten, lässt sich doch schon jetzt sagen, dass dem § 4 Abs. 3 BDSG in der Praxis teilweise nur unzureichend Rechnung getragen wird. Häufig festgestellte Mängel sind:

- Mitunter ist weder aus dem Formular noch aus dem Zusammenhang ersichtlich, welche nichtöffentliche Stelle die Daten erhebt, also verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes ist, beispielsweise bei Datenerhebungen in Autohäusern oder in Konzernen. Im letzteren Fall ist verantwortliche Stelle nicht der Konzern, sondern das einzelne rechtlich selbstständige Unternehmen. Anzugeben sind der Name und die Anschrift der nichtöffentlichen Stelle, sodass der Betroffene in der Lage ist, seine Datenschutzrechte auf Auskunft, Berichtigung, Sperrung und Löschung seiner Daten wahrzunehmen oder einen Werbewiderspruch anzubringen. Die Angabe einer Internet- oder E-Mail-Adresse oder des Namens des Beauftragten für den Datenschutz genügen nicht.
- Die Zwecke der Erhebung, Speicherung, Übermittlung oder Nutzung von Daten (im Folgenden auch als „Datenverwendung“ bezeichnet) werden nicht genannt. Falls der Datenschutz überhaupt angesprochen wird, geschieht dies in einer Form, die den Betroffenen beruhigen soll („Der Datenschutz wird voll gewahrt“ oder „Wir verfahren nach den Vorschriften des Bundesdatenschutzgesetzes“), aber mit keinen Sachinformationen verbunden ist.
- Die Zwecke der Datenverwendung werden – bewusst oder unbewusst – nicht in der für den Betroffenen gebotenen Klarheit angegeben. Es besteht beispielsweise eine große Zurückhaltung, deutlich zu sagen, dass Daten für Zwecke der Werbung verwendet werden sollen.
- Die Zwecke der Datenverwendung werden unvollständig angegeben. Es müssen sämtliche Zwecke genannt werden, die die verantwortliche Stelle im Zeit-

[3)] veröffentlicht unter www.baden-wuerttemberg.de; Datenschutz; weitere Infos; Infomaterial.

punkt der Erhebung verfolgt. Wird nur die „Vertragsabwicklung“ als Zweck der Datenverwendung genannt, ist Werbung ausgeschlossen.

– Es werden oftmals nicht alle Formen der Datenverwendung angegeben, beispielsweise wird die Speicherung oder Nutzung der Daten (zum Beispiel für eigene Werbezwecke) gerne vergessen.

– Datenübermittlungen werden nicht als solche erkennbar, zum Beispiel wenn es heißt, Daten würden „nicht an Stellen außerhalb des Konzerns“ weitergegeben. Dies lässt jedenfalls vermuten, dass Datenübermittlungen zwischen Konzern und Unternehmen stattfinden. Welche und für welche Zwecke bleibt jedoch offen.

– Die Kategorien der Datenempfänger werden, wenn überhaupt, zumeist nur unzureichend bezeichnet. Angaben wie „andere Unternehmen“, „verbundene Unternehmen“ oder „Partnerunternehmen“, „Unternehmen innerhalb des Konzerns“ (welche?) genügen nicht. Wichtig für die Entscheidung des Betroffenen, ob er seine Daten angibt, ist die Branche, zu der das datenempfangende Unternehmen gehört (zum Beispiel Auskunftei, Versandhandelsunternehmen, Adresshandel). Anzugeben sind auch hier sämtliche Kategorien von Datenempfängern.

  Nicht aufgeführt werden häufig Unternehmen, bei denen Bonitätsauskünfte eingeholt oder Scorewerte abgefragt werden. Diese müssen selbstverständlich erwähnt werden, weil an sie Name, Anschrift und zumeist auch das Geburtsdatum des Betroffenen übermittelt werden. *Die Aufsichtsbehörde empfiehlt dringend, diese Unternehmen mit Namen und Anschriften zu nennen und den genauen Zweck der Abfrage (Bonitätsabfrage und/oder Scorewertberechnung) anzugeben.* Die Aufsichtsbehörde stellt hier immer wieder fest, dass die verantwortlichen Stellen zwischen Bonitätsabfrage und Scorewertberechnung nicht unterscheiden können und nicht wissen, welche Art von Abfrage sie durchführen. Es ist deshalb auch nicht verwunderlich, dass diese Angabe oftmals falsch ist.

  Als Datenempfänger häufig nicht erwähnt werden auch Unternehmen, die Daten im Auftrag verarbeiten, zum Beispiel externe Rechenzentren.

  Als Nachteil erweist sich in diesem Zusammenhang, dass die Datenempfänger nach dem Wortlaut des Gesetzes nur angegeben werden müssen, soweit der Betroffene nach den Umständen des Einzelfalls nicht mit der Übermittlung an diese rechnen muss. Aus Eingaben und Gesprächen mit Bürgern weiß die Aufsichtsbehörde jedoch, dass ihnen die Zusammenhänge bei der Datenverarbeitung zumeist nicht bekannt sind. Die Einschränkung wird daher selten zum Tragen kommen. Für Unternehmen, die die Datenverarbeitung für ihre Kunden transparent machen wollen, sollte es ohnehin eine Selbstverständlichkeit sein, ihre Kunden umfassend zu informieren. Im Interesse der Rechtsklarheit wäre es hilfreich, wenn der Gesetzgeber auf diese Einschränkung der Informationspflicht verzichten würde.

– Häufig werden in Vordrucken Daten abgefragt, die für den angegebenen Zweck nicht benötigt werden. Sofern auf die Erhebung dieser Daten nicht ganz verzichtet wird, muss auf die Freiwilligkeit dieser Angaben hingewiesen werden. Hinweise auf die Freiwilligkeit von Angaben fanden sich im Rahmen der Überprüfung jedoch nur selten. Mit Sorge hat die Aufsichtsbehörde festgestellt, dass viele an der Untersuchung beteiligte Unternehmen ohne jede Notwendigkeit Telefon- und Telefaxnummer sowie die E-Mail-Adresse ihrer Kunden erheben. Selbst wenn eine Telefonnummer im Einzelfall für Rückfragen hilfreich sein mag, ist diese Angabe nicht notwendig, sondern als „freiwillig“ zu kennzeichnen. Auf keinen Fall dürfen derartige Angaben dazu genutzt werden, die Kunden zu Werbezwecken zu kontaktieren. Dafür bedarf es einer ausdrücklichen schriftlichen Einwilligung des Kunden (§ 4 a Abs. 3 Satz 1 BDSG). Darauf hat die Aufsichtsbehörde die betreffenden Unternehmen ausdrücklich hingewiesen.

– Den gesetzlichen Unterrichtungs- und Hinweispflichten wird zum Teil durch entsprechende Ausführungen in den Allgemeinen Geschäftsbedingungen Rechnung getragen. Das allein genügt jedoch nicht. Sofern keine Möglichkeit besteht, die vorgeschriebene Unterrichtung vollumfänglich in die Antragsvordrucke oder Verträge zu integrieren – was zweifellos am Besten ist – muss in

den Formularen selbst ein deutlicher Hinweis auf die Datenschutzinformation in den Allgemeinen Geschäftsbedingungen angebracht sein; die Kennzeichnung freiwilliger Angaben muss auf jeden Fall auf dem Formular selbst erfolgen.

– Manche Unternehmen lassen ihre Kunden über versteckte Klauseln in den Allgemeinen Geschäftsbedingungen darin einwilligen, durch das Unternehmen oder dritte Unternehmen, an die man die Daten übermitteln möchte, telefonisch, per Fax oder per E-Mail für Werbezwecke kontaktiert zu werden. Die Aufsichtsbehörde sieht darin keine rechtswirksame Einwilligung.

Insgesamt hat die Überprüfung schon jetzt ergeben, dass hinsichtlich der Umsetzung der Unterrichtungs- und Hinweispflichten des § 4 Abs. 3 BDSG und der Einholung der Einwilligung in die E-Mail-, Fax- und Telefonwerbung erheblicher Verbesserungsbedarf besteht. Viele Änderungen sind rechtlich geboten, manche nur wünschenswert. Wünschenswert ist beispielsweise, dass den Unterrichtungspflichten nach § 4 Abs. 3 Satz 1 BDSG *an einer Stelle komprimiert* Rechnung getragen wird. Auch das gehört zur Transparenz. Die Aufsichtsbehörde sieht hier vielfältige Betätigungsmöglichkeiten für betriebliche Datenschutzbeauftragte. Es sollte ihnen Ansporn sein, dafür zu sorgen, dass „ihr“ Unternehmen in puncto Transparenz der Datenverwendung für den Kunden mit gutem Beispiel vorangeht.

C Einzelne Tätigkeitsbereiche

1 Inkassounternehmen

1.1 Allgemeines zur Tätigkeit von Inkassounternehmen und zur Zusammenarbeit mit Auskunfteien

Ein Thema, das die Aufsichtsbehörde im Berichtszeitraum in besonderem Maße beschäftigt hat, ist die Tätigkeit von Inkassounternehmen.

Inkassounternehmen betreiben gewerbsmäßigen Forderungseinzug für Gläubiger, die sie hiermit beauftragt haben. Nach dem Rechtsberatungsgesetz ist die Tätigkeit von Inkassounternehmen erlaubnispflichtig.

In der Regel fordert ein Gläubiger, bevor er ein Inkassounternehmen einschaltet, selbst den Schuldner zur Bezahlung der Forderung auf. Falls erforderlich mahnt er mehrfach. Begleicht der Schuldner die Forderung nicht, sei es, dass er überhaupt nicht reagiert oder Einwendungen gegen die Forderung erhebt, entschließen sich vor allem Unternehmen, die eine Vielzahl ausstehender Forderungen besitzen, ein Inkassounternehmen einzuschalten. Dieses versucht sodann, die Forderung für den Gläubiger beizutreiben. In manchen Fällen ist es hierzu erforderlich, dass das Inkassounternehmen zunächst die aktuelle Adresse des Schuldners ermittelt, zum Beispiel über eine Anfrage beim Einwohnermeldeamt. Üblicherweise fordert das Inkassounternehmen den Schuldner zunächst schriftlich zur Zahlung auf, bei Bedarf auch wiederholt. Die Zahlungsaufforderungen des Inkassounternehmens enthalten in der Regel einen Hinweis an den Schuldner, dass das Inkassounternehmen seine Daten an eine Auskunftei übermittelt, wenn er die Forderung nicht begleicht oder begründete Einwendungen erhebt. Die Reaktionen auf die Zahlungsaufforderungen sind vielfältig. Manche Schuldner begleichen die Forderung, andere bringen ihre Einwendungen gegen die geltend gemachte Forderung (erstmals oder wiederholt) gegenüber dem Gläubiger und/oder dem Inkassounternehmen vor. Manche Schuldner melden sich nicht, weil sie ihre Einwendungen bereits gegenüber dem Gläubiger erhoben hatten. Wieder andere erkennen die Schuld zwar an, sehen sich aber nicht in der Lage, die Zahlung zu leisten. Während im erstgenannten Fall das Inkassoverfahren erfolgreich abgeschlossen ist, folgen in den anderen Fällen weitere Maßnahmen, sei es, dass der Fall im Auftrag des Gläubigers an einen Rechtsanwalt übergeben wird (zum Beispiel, um einen Mahnbescheid zu erwirken), sei es, dass das Inkassounternehmen mit dem Schuldner eine Ratenzahlungsvereinbarung trifft, deren Einhaltung es im Folgenden überwacht.

In vielen Fällen übermitteln Inkassounternehmen personenbezogene Daten aus dem Inkassoverfahren (zum Beispiel, dass gegen eine Person ein Inkassoverfahren eingeleitet wurde oder auch, dass an die Adresse des Schuldners nicht zugestellt werden kann) an Auskunfteien. Dies ist für die Betroffenen mit weitreichenden Folgen verbunden. Auskunfteien erteilen nämlich auf Anfrage in einem automatisierten Verfahren Auskünfte über Personen. Diese beinhalten Aussagen zur Bonität und zum Zahlungsverhalten des Einzelnen. Dadurch werden die von Inkassounternehmen übermittelten Daten in großem Umfang gestreut. Eine negative Auskunft einer Auskunftei kann zum Beispiel dazu führen, dass die betroffene Person einen gewünschten Kredit nicht erhält.

Da Inkassounternehmen somit über Daten zu Schuldnern verfügen, die für Auskunfteien von großem Interesse sind, besteht zwischen diesen Geschäftszweigen oftmals eine enge Verknüpfung. Inkassounternehmen nutzen personenbezogene Daten daher sowohl für Zwecke der Inkassobearbeitung (originär eigene Zwecke) als auch für Meldungen an Auskunfteien. Wegen der Gefahren für das informationelle Selbstbestimmungsrecht des Einzelnen dürfen Inkassounternehmen personenbezogene Daten eines Schuldners nur unter strengen Voraussetzungen an Auskunfteien übermitteln (hierzu unten Nr. 1.6).

Bei der Aufsichtsbehörde sind im Berichtszeitraum zahlreiche Beschwerden über Inkassounternehmen eingegangen, die zu einem Großteil die Übermittlung von Daten aus dem Inkassoverfahren an Auskunfteien beziehungsweise die Ankündigung durch Inkassounternehmen, dass eine solche beabsichtigt sei, betrafen.

Die Aufsichtsbehörde hat – auch vor diesem Hintergrund – bei mehreren Inkassounternehmen Vor-Ort-Prüfungen durchgeführt. Es handelte sich dabei um eine umfassende Prüfung, die bereits mit einem Prüfungsbericht an das betreffende Unternehmen abgeschlossen wurde, um eine kursorische Vor-Ort-Prüfung, bei der die datenschutzrechtlichen Problempunkte gegenüber dem Unternehmen dargestellt wurden und um eine weitere Prüfung, bei der eine abschließende Bewertung allerdings noch nicht erfolgt ist. Das erstgenannte Inkassounternehmen hat aufgrund des Prüfungsberichts wesentliche Punkte bereits aufgegriffen und Änderungen umgesetzt beziehungsweise in die Wege geleitet. Im Rahmen der Prüfungen hat die Aufsichtsbehörde einen umfassenden Einblick in die Arbeitsweise der Inkassounternehmen erhalten. Von grundsätzlicher Bedeutung sind folgende Prüfungsergebnisse:

1.2 Darf ein Gläubiger die Daten eines Schuldners bei bestrittener Forderung an ein Inkassounternehmen übermitteln? Darf das Inkassounternehmen diese Daten zur Beitreibung der Forderung nutzen?

Beauftragt ein Gläubiger ein Inkassounternehmen mit dem Einzug einer Forderung, übermittelt er die erforderlichen Schuldner- und Forderungsdaten an das Inkassounternehmen. Datenschutzrechtlich ist dies völlig unproblematisch, wenn die Forderung unbestritten ist. Inkassounternehmen beschäftigen sich typischerweise mit dem Einzug unbestrittener Forderungen und vereinbaren mit dem Gläubiger zumeist, dass nur „voraussichtlich unbestrittene Forderungen“ zur Einziehung übergeben werden. Der Aufsichtsbehörde sind aber Fälle bekannt, in denen Forderungen, die schon gegenüber dem Gläubiger bestritten wurden, durch Inkassounternehmen beigetrieben wurden. Es fragt sich daher, ob ein Gläubiger die Daten eines Schuldners auch dann an ein Inkassounternehmen übermitteln darf, wenn der Schuldner die Forderung bestritten hat, und ob das Inkassounternehmen diese Daten zur Beitreibung der Forderung nutzen darf.

Die Aufsichtsbehörde hat beide Fragen bejaht. Unerheblich ist dabei, ob der Vertrag zwischen Gläubiger und Inkassounternehmen die oben erwähnte Beschränkung auf voraussichtlich unbestrittene Forderungen enthält. Auf diese Einschränkung kann sich der Schuldner nämlich nicht berufen, da diese nur zwischen den Vertragsparteien wirkt. Auch wenn der Schuldner die Forderung nach deren Übergabe an das Inkassounternehmen bestreitet, ist es datenschutzrechtlich zulässig, wenn dieses die Daten für die weitere Beitreibung der Forderung nutzt. Dem Inkassounternehmen ist es nämlich rechtlich nicht verwehrt, auch strittige Forderungen beizutreiben. Das Rechtsberatungsgesetz schränkt die Erlaubnis für Inkassotätigkeiten nicht in dieser Weise ein. Überdies hat das Bundesverfassungsgericht in einem Kammerbeschluss vom 14. August 2004 (Az.: 1 BvR 725/03) fest-

gestellt, dass zur Tätigkeit von Inkassobüros auch die Äußerung von Rechtsansichten gegenüber dem Schuldner nach Erhebung von Einwendungen gehört.

Daraus ergibt sich, dass ein Inkassounternehmen auch im Fall des Bestreitens der Forderung durch den Schuldner seine Bearbeitung nicht einstellen muss. Für sein weiteres Tätigwerden ist es erforderlich, dass es die bestrittenen Daten auch nutzt.

An der Rechtslage wird sich auch nach Inkrafttreten des Rechtsdienstleistungsgesetzes, das das Rechtsberatungsgesetz ablösen wird, nichts ändern.

1.3 Wie wird sichergestellt, dass der Gläubiger das Inkassounternehmen über Einwendungen des Schuldners gegen die geltend gemachte Forderung unterrichtet?

Immer wieder erreichen die Aufsichtsbehörde Beschwerden über Inkassounternehmen, in denen der Beschwerdeführer (=Schuldner) belegt, dass er die geltend gemachte Forderung bereits gegenüber dem Gläubiger bestritten hat. Nachfragen beim Inkassounternehmen ergeben in solchen Fällen meist, dass der Gläubiger das Inkassounternehmen bei Übergabe der Forderung nicht über die vom Schuldner erhobenen Einwendungen informiert hat. Dies zeigt ein strukturelles Problem auf: Die Übergabe der Forderung erfolgt heutzutage nicht mehr in der Weise, dass der Gläubiger dem Inkassounternehmen eine Papierakte zur Verfügung stellt, in der sich sämtliche Schreiben des Gläubigers und gegebenenfalls auch die Reaktionen des Schuldners hierauf befinden. Vielmehr übermittelt der Gläubiger dem Inkassounternehmen lediglich die Personalien des Schuldners und einige wenige Daten zur Forderung in automatisierter Form. Der Akteninhalt wird dadurch unter Umständen wesentlich verkürzt wiedergegeben. Zwar ist zumeist vertraglich vorgesehen, dass der Gläubiger lediglich voraussichtlich unbestrittene Forderungen an das Inkassounternehmen zum Einzug übergibt. Bei Übergabe der Forderung wird jedoch nicht ausdrücklich danach gefragt, ob die Forderung unbestritten ist. Eine *automatisierte Abklärung* des Eingangsstatus ist nicht vorgesehen. Die Aufsichtsbehörde hält eine solche angesichts der Erfahrungswerte aus der Praxis für *erforderlich.* Die durch die Verfahrensweise bedingte Verkürzung des Akteninhalts darf nicht zu Lasten des Betroffenen gehen.

Selbstverständlich muss der Vertrag zwischen dem Inkassounternehmen und dem Auftraggeber auch vorsehen, dass der Gläubiger das Inkassounternehmen über nachträglich erhobene Einwendungen des Schuldners unterrichtet. Kommt der Gläubiger seiner Verpflichtung zur Unterrichtung wiederholt nicht nach, halten wir das Inkassounternehmen für verpflichtet, weitergehende Maßnahmen zum Schutz des Schuldners zu ergreifen (vergleiche dazu auch unten Nr. 1.6.1). Nur so wird sichergestellt, dass das Inkassounternehmen vollständige und damit richtige Daten über den Schuldner speichert.

1.4 Was muss ein Inkassounternehmen bei der Anschriftenermittlung beachten?

Inkassounternehmen benötigen oft die aktuelle Anschrift eines Schuldners und holen diese bei der Meldebehörde ein. Eine einfache Melderegisterauskunft über Familienname, Vorname, Doktorgrad und aktuelle Anschrift eines Schuldners wird nach dem Meldegesetz ohne nähere Begründung, insbesondere ohne Darlegung eines berechtigten Interesses erteilt. Hierauf ist bei Melderegisteranfragen strikt zu achten, um Schuldner nicht unnötig bloß zu stellen.

1.5 Wann muss ein Inkassounternehmen personenbezogene Daten berichtigen?

Soweit sich im Zuge der Inkassobearbeitung für das Inkassounternehmen aus der Reaktion des Schuldners (zum Beispiel durch ein Bestreiten der Forderung, Angabe eines anderen Geburtsdatums) oder auch aus anderen Quellen (zum Beispiel einer Melderegisterauskunft) ein Anhaltspunkt dafür ergibt, dass die gespeicherten Daten unrichtig oder unvollständig sein könnten, muss es die Richtigkeit der Daten überprüfen. Dies ergibt sich aus § 35 Abs. 1 BDSG, der den Berichtigungsanspruch des Betroffenen regelt. Stellt sich bei der Überprüfung heraus, dass unrichtige Daten gespeichert sind, sind diese zu berichtigen.

Bei der Prüfung ist die notwendige Sorgfalt an den Tag zu legen. Diese vermissten wir beispielsweise, als eine Betroffene, die einen Doppelnamen hat, sowohl der Auftraggeberin als auch dem Inkassounternehmen zu verdeutlichen versuchte, dass die Auftraggeberin und Gläubigerin der Forderung aufgrund ihres Doppelnamens versehentlich zwei Kundennummern für sie angelegt und eingehende Zahlungen nur auf ein Kundenkonto verbucht hatte. Obwohl die Betroffene den Sachverhalt beziehungsweise den sich aufdrängenden Verdacht hinreichend deutlich gegenüber der Gläubigerin darstellte, musste sie zur Durchsetzung ihres Berichtigungsanspruchs die Aufsichtsbehörde einschalten, da ihr eigenes Bemühen fruchtlos blieb.

1.6 Unter welchen Voraussetzungen darf ein Inkassounternehmen personenbezogene Daten eines Schuldners an eine Auskunftei übermitteln?

Immer wieder beschweren sich Betroffene bei der Aufsichtsbehörde darüber, dass ein Inkassounternehmen Daten aus dem Inkassoverfahren (zum Beispiel dass ein Inkassoverfahren eingeleitet wurde) an eine Auskunftei übermittelt oder für den Fall der Nichtzahlung in Aussicht gestellt hat, obwohl sie Einwendungen gegen die Forderung entweder schon gegenüber dem Gläubiger oder auch gegenüber dem Inkassounternehmen selbst geltend gemacht haben. Dabei reicht die uns bekannt gewordene Bandbreite der Einwendungen vom bloßen Vorbringen, man bestreite die Forderung, bis hin zum dezidierten Auseinandersetzen mit den rechtlichen und tatsächlichen Voraussetzungen des der geltend gemachten Forderung zugrunde liegenden Rechtsanspruchs. Die Beschwerdeführer fassten den Hinweis in der Zahlungsaufforderung der Inkassounternehmen, dass die Daten an eine Auskunftei übermittelt würden, wenn die Forderung nicht ausgeglichen oder begründete Einwendungen erhoben würden, oftmals als Nötigung auf.

Bei Daten aus Inkassoverfahren handelt es sich um sogenannte Negativdaten zu Personen, da sie ein nicht vertragsgemäßes Verhalten betreffen. Bei den Negativdaten, die bei Auskunfteien gespeichert werden, wird zwischen „harten“ und „weichen“ Daten unterschieden. Zu den harten Negativmerkmalen gehören Daten, denen eine objektive gerichtliche Entscheidung zugrunde liegt. Teilweise werden darunter zusätzlich auch noch Daten verstanden, die eine solche Bedeutung für die kreditgebende Wirtschaft haben, dass entgegenstehende Interessen des Betroffenen nicht schutzwürdig sind (zum Beispiel Abgabe der eidesstattlichen Versicherung). Als „weich“ werden Negativmerkmale bezeichnet, die auf eine einseitige Rechtsausübung zurückgehen. Diese haben folglich einen eingeschränkteren Aussagewert im Hinblick auf Zahlungsunfähigkeit oder Zahlungsunwilligkeit des Betroffenen. Bei der Frage der Zulässigkeit der Übermittlung solcher Daten an Auskunfteien ist dies zu berücksichtigen.

Bereits im zweiten Tätigkeitsbericht (C 4.1, S. 37 ff.) haben wir dargestellt, dass der Übermittlung von Daten aus Inkassoverfahren an Auskunfteien, der sogenannten „Einmeldung“, Schranken gesetzt sind und diese im Einzelnen aufgezeigt.

Der Düsseldorfer Kreis ist unserer Auffassung in einem Ende 2006 gefassten Beschluss gefolgt. Auch er hält eine generelle Übermittlung von weichen Negativdaten aus dem Inkassobereich an Auskunfteien aufgrund entgegenstehender überwiegender schutzwürdiger Interessen der Betroffenen nicht für zulässig. Kann jedoch nach sorgfältiger Einzelfallabwägung die Zahlungsunfähigkeit oder Zahlungsunwilligkeit zweifelsfrei festgestellt werden, das heißt, besteht kein Grund zu der Annahme, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, wird eine Übermittlung unter den folgenden Voraussetzungen als zulässig angesehen:

- Es muss sich um eine unbestrittene Forderung handeln (dazu unten Nr. 1.6.1).
- Sowohl Gläubiger als auch Inkassounternehmen haben die der Einmeldung zugrunde liegende Forderung gegenüber dem Schuldner nachweisbar jeweils mindestens zweimal vergeblich gemahnt (dazu unten Nr. 1.6.2).
- Der Schuldner wird – zum Beispiel in den Mahnschreiben – darüber informiert, dass eine Einmeldung bei einer Auskunftei erfolgt, soweit die Forderung unbestritten ist und keine Zahlung innerhalb der gesetzten Frist erfolgt (dazu unten Nr. 1.6.3).

– Die Einmeldung erfolgt frühestens dann, wenn vier Arbeitstage seit Ablauf der im letzten Mahnschreiben des Inkassounternehmens genannten Zahlungsbeziehungsweise Rückantwortfrist von zehn Tagen verstrichen sind (dazu unten Nr. 1.6.4).

1.6.1 Vorliegen einer unbestrittenen Forderung

Um überhaupt beurteilen zu können, ob eine Forderung unbestritten ist, muss das Inkassounternehmen von sämtlichen eine Forderung betreffenden Äußerungen des Schuldners Kenntnis erhalten (vergleiche dazu oben Nr. 1.3). Andernfalls läuft das Inkassounternehmen Gefahr, unzulässig Daten an eine Auskunftei zu übermitteln.

Die Praxis, Einwendungen des Schuldners nicht an das beauftragte Inkassounternehmen zu melden, war besonders auffällig bei einem großen, nicht in Baden-Württemberg ansässigen Auftraggeber eines Inkassounternehmens. Nachdem die Aufsichtsbehörde das Inkassounternehmen deutlich auf das Problem hingewiesen hatte, entschied es sich, Daten, die den auffälligen Forderungsbereich dieses Auftraggebers betrafen, generell nicht mehr an Auskunfteien zu übermitteln.

Sodann stellt sich die Frage, in welchen Fällen eine Forderung „unbestritten“ ist beziehungsweise von einem relevanten Bestreiten auszugehen ist.

Mit den oben genannten Voraussetzungen soll sichergestellt werden, dass nur Fälle eingemeldet werden, bei denen aus dem Gesamtverhalten des Schuldners auf dessen Zahlungsunfähigkeit oder Zahlungsunwilligkeit geschlossen werden kann. Ein relevantes Bestreiten liegt dann nicht vor, wenn der Schuldner lediglich pauschal und unsubstantiiert ohne jegliche Begründung eine Forderung bestreitet oder lediglich ein „Bestreiten um des Bestreitens Willen“ vorliegt. Das gleiche gilt, wenn die Einwendungen in rechtlicher Hinsicht offenkundig und nach allen vernünftigen Erwägungen haltlos sind, wobei bei der Prüfung ein strenger Maßstab anzulegen ist. Soweit nicht völlig ausgeschlossen werden kann, dass Einwendungen dem Bestehen oder der Durchsetzbarkeit einer Forderung entgegenstehen, darf eine Einmeldung nicht erfolgen.

In Fällen, in denen Einwendungen in tatsächlicher Hinsicht geltend gemacht werden, ist in der Regel von einem relevanten Bestreiten auszugehen, wenn zur Prüfung der Forderung Beweis erhoben werden müsste. *Nicht ausreichend für die Einmeldung ist, dass das Inkassounternehmen und der Gläubiger nach Prüfung der Sach- und Rechtslage davon überzeugt sind, dass die Forderung besteht und letztlich durchgesetzt werden kann.*

Von der Aufsichtsbehörde durchgeführte Prüfungen wie auch einige Beschwerdefälle haben gezeigt, dass Inkassounternehmen das Bestreiten von Betroffenen teilweise zu Unrecht als irrelevant eingestuft haben.

1.6.2 Vergebliche Mahnungen

Eine Einmeldung ist erst dann zulässig, wenn sowohl der Gläubiger als auch das Inkassounternehmen den Schuldner jeweils zweimal vergeblich schriftlich zur Zahlung aufgefordert haben. Von einer vergeblichen schriftlichen Zahlungsaufforderung ist nicht auszugehen, wenn der Schuldner zur Rückgabe einer Sache bis zu einem bestimmten Datum aufgefordert wird, verbunden mit dem Hinweis, dass, sofern eine Rücksendung bis dahin nicht erfolge, ein bestimmter Geldbetrag in Rechnung gestellt werde, dessen Überweisung für den Fall der Unmöglichkeit der Rücksendung bis zum entsprechenden Datum erbeten wurde. Denn in einem solchen Fall steht im Zeitpunkt der Aufforderung noch gar nicht fest, ob eine Zahlungsverpflichtung ent-/beziehungsweise besteht. Auch Hinweise in Verträgen oder Allgemeinen Geschäftsbedingungen auf Rückgabe- beziehungsweise Zahlungspflichten, die bei Kündigung eines Vertrags entstehen können, ersetzen keine für die Einmeldung erforderliche Zahlungsaufforderung.

1.6.3 Information des Schuldners über die drohende Einmeldung

Der Schuldner muss vor der Einmeldung – zum Beispiel in den Zahlungsaufforderungen des Inkassounternehmens – davon in Kenntnis gesetzt werden, dass eine

Einmeldung bei einer Auskunftei erfolgt, soweit die Forderung unbestritten ist und keine Zahlung innerhalb der gesetzten Frist erfolgt. Durch diese Information soll dem Schuldner die Möglichkeit gegeben werden, vor der Einmeldung zu der Forderung beziehungsweise der beabsichtigten Datenübermittlung Stellung zu nehmen. Bei der Formulierung hat das Inkassounternehmen darauf zu achten, dass der Betroffene den Hinweis nicht als Nötigung auffasst. Einem Inkassounternehmen war dies nach Meinung zahlreicher Beschwerdeführer „nicht gelungen". Die Aufsichtsbehörde hat deshalb dieses Unternehmen dabei unterstützt, einen neuen Benachrichtigungstext zu erarbeiten. Dieser soll dem Empfänger auch verdeutlichen, in welchen Fällen eine Übermittlung an eine Auskunftei erfolgen kann. Es darf keinesfalls der Eindruck entstehen, Daten würden immer dann übermittelt, wenn der Schuldner die Forderung nicht erfüllt.

1.6.4 Einmeldung nach Fristablauf

Die Einmeldung darf frühestens dann erfolgen, wenn vier Arbeitstage seit Ablauf der im letzten Mahnschreiben des Inkassounternehmens genannten Zahlungs- beziehungsweise Rückantwortfrist von zehn Tagen verstrichen sind. Hierdurch soll dem Schuldner eine angemessene Reaktionszeit eingeräumt werden.

1.6.5 Gesamtwürdigung

Wie sich aus dem Beschluss ergibt, kann selbst bei Vorliegen der oben genannten (Mindest-)Voraussetzungen die Übermittlung von Daten aus einem Inkassoverfahren unzulässig sein, wenn sich aus der Gesamtbetrachtung des Einzelfalls ergibt, dass schutzwürdige Belange des Betroffenen einer Übermittlung entgegenstehen. Inkassounternehmen sind daher gehalten, besondere Umstände des Einzelfalls zu überprüfen und zu berücksichtigen.

1.7 Unter welchen Voraussetzungen darf ein Inkassounternehmen das Merkmal „Adressermittlung" an eine Auskunftei übermitteln?

Neben den klassischen Negativmerkmalen übermitteln manche Inkassounternehmen auch sogenannte „sonstige Merkmale" an Auskunfteien. Darunter fällt auch das Datum „Adressermittlung". Es bedeutet, dass der Person unter der angegebenen Adresse keine Schreiben (zum Beispiel Rechnungen) zugestellt werden können.

In einem an uns herangetragenen Einzelfall hatte das Inkassounternehmen zunächst erfolgreich eine Zahlungsaufforderung an die ihm bekannte Adresse des Betroffenen gesandt. Weshalb die zweite Zahlungsaufforderung nicht zugestellt werden konnte, wusste das Inkassounternehmen nicht, da es die Gründe hierfür aus Kostengründen nicht bei der Post ermittelte. In der Folgezeit führte das Unternehmen zu unterschiedlichen Zeitpunkten insgesamt drei Anfragen zum Betroffenen bei der Meldebehörde durch; darin war auch das Geburtsdatum des Betroffenen angegeben. Die Melderegisterauskünfte ergaben, dass eine Person mit dem entsprechenden Namen unter der dem Inkassounternehmen bekannten Anschrift gemeldet war. In zwei Auskünften hatte die Meldebehörde allerdings das angegebene Geburtsdatum als falsch gekennzeichnet. Über ein Jahr nach der letzten Melderegisterabfrage versandte das Inkassounternehmen zwei weitere Zahlungsaufforderungen an den Betroffenen unter der bekannten Anschrift. Diese Schreiben gingen dem Betroffenen offensichtlich zu, es war allerdings kein Zahlungseingang zu verzeichnen. Erst eine weitere Zahlungsaufforderung, die von den mittlerweile beauftragten Rechtsanwälten versandt wurde, kam zurück. Die Gründe hierfür ermittelte das Inkassounternehmen nicht. Stattdessen veranlasste es eine Suche in der Umzugsdatei der Deutschen Post, die jedoch erfolglos blieb. Daraufhin meldete das Inkassounternehmen den Betroffenen mit dem ihr vorliegenden Geburtsdatum und dem Merkmal „Adressermittlung" an eine Auskunftei ein.

Die Aufsichtsbehörde ist der Auffassung, *dass ein Inkassounternehmen auch bei der Einmeldung des Datums „Adressermittlung" bei einer Auskunftei besondere Vorsicht walten lassen muss*, ebenso die Auskunftei bei der Speicherung dieses Datums. Übermittelt nämlich eine Auskunftei dieses Datum an einen Dritten, können sich für den Betroffenen daraus ähnliche Folgen ergeben, wie bei der Übermittlung eines echten Negativmerkmals.

Aus diesem Grund muss an die Einmeldung ein strenger Maßstab angelegt werden. Nur wenn mit sehr hoher Wahrscheinlichkeit davon ausgegangen werden kann, dass der Betroffene nicht an der angegebenen Anschrift wohnt und eine neue Anschrift nicht festgestellt werden kann, darf das Merkmal „Adressermittlung“ an eine Auskunftei übermittelt werden. Das Inkassounternehmen muss dabei *alle ihm zumutbaren Aufklärungsmöglichkeiten nutzen*. Welche dies sind, hängt vom Einzelfall ab. Regelmäßig werden dafür jedoch eine Würdigung der von der Post angegeben Gründe für die Nichtzustellbarkeit, die Nutzung gängiger Adressdatenbestände, insbesondere von Telefonverzeichnissen, und die Einholung von Auskünften bei den Meldebehörden gehören. Gibt es Anhaltspunkte dafür, dass der Betroffene nach wie vor unter der bekannten Anschrift wohnt, darf eine Einmeldung des Merkmals „Adressermittlung“ nicht erfolgen.

In dem dargestellten Einzelfall haben wir die Einmeldung beanstandet, da diese Grundsätze nicht beachtet wurden. Das Inkassounternehmen durfte nicht davon ausgehen, dass der Betroffene mit sehr hoher Wahrscheinlichkeit nicht an der angegebenen Anschrift wohnt. Immerhin konnten dem Betroffenen an die fragliche Anschrift drei Zahlungsaufforderungen zugestellt werden. Zudem hatte die Meldebehörde bestätigt, dass eine Person entsprechenden Namens an der bekannten Anschrift gemeldet war. Dass das vom Inkassounternehmen angegebene Geburtsdatum möglicherweise falsch war, konnte nicht als Hinweis darauf gewertet werden, dass der Gesuchte mit der unter der fraglichen Anschrift gemeldeten Person nicht identisch war. Davon ging offensichtlich auch das Inkassounternehmen aus, da es die folgenden Zahlungsaufforderungen an die bekannte Adresse sandte. Auch die Tatsache, dass keine Zahlungen seitens des Betroffenen erfolgten, besagt für die Frage, wo dieser wohnt, nichts. Hinsichtlich der Rückläufer hätte angesichts der erfolgreich versandten Briefe Anlass für weitere Ermittlungen und Nachforschungen bestanden. Dass das Inkassounternehmen die Gründe, weshalb die Schreiben nicht zugesandt werden konnten, aus Kostengründen nicht ermittelte, durfte nicht zu Lasten des Betroffenen gehen. Hätte der Betroffene beispielsweise die Annahme des Schreibens verweigert, hätte festgestanden, dass er unter der angegebenen Adresse wohnt. Auch die erfolglose Suche in der Umzugsdatei rechtfertigte in Anbetracht mehrerer „erfolgreicher“ Zustellungen die Einmeldung nicht. Zu bemängeln war insbesondere, dass das Inkassounternehmen zu keinem Zeitpunkt das Telefonbuch heranzog, in dem der Betroffene mit seiner vollständigen Anschrift eingetragen war.

Darüber hinaus hätte auch das dem Unternehmen bekannte Geburtsdatum nicht an die Auskunftei übermittelt werden dürfen, da es das Einwohnermeldeamt in zwei Melderegisterauskünften als falsch bezeichnet hatte.

Wir haben das betreffende Inkassounternehmen aufgefordert, eine interne Anweisung zu erarbeiten, die die Vorgehensweise in derartigen Fällen unter Berücksichtigung oben genannter Grundsätze regelt. Dieses hat inzwischen erste Änderungen am Verfahren vorgenommen.

1.8 Darf ein Inkassounternehmen Daten an eine Auskunftei übermitteln und gleichzeitig eine Beauskunftungssperre bei der Auskunftei veranlassen?

Bestreitet ein Schuldner eine Forderung gegenüber dem Inkassounternehmen, nachdem dieses seine Daten an eine Auskunftei übermittelt hat, hat dies auch Auswirkungen auf die Zulässigkeit der Datenspeicherung bei der Auskunftei. Soweit sich aus dem Bestreiten ergibt, dass das Verhalten des Schuldners nunmehr keinen zweifelsfreien Schluss mehr auf Zahlungsunwilligkeit oder Zahlungsunfähigkeit des Schuldners zulässt, hat das einmeldende Inkassounternehmen dies der Auskunftei mitzuteilen. Dann müssen die Daten bei der Auskunftei gesperrt oder gegebenenfalls auch gelöscht werden, sodass diese bei Anfragen Dritter nicht übermittelt werden (Beauskunftungssperre). Die Verfahrensweise kann auch so ausgestaltet sein, dass das Inkassounternehmen selbst in automatisierter Form eine Beauskunftungssperre an die Auskunftei meldet, die eine Übermittlung der von der Sperre betroffenen Daten durch die Auskunftei an Dritte verhindert. Unzulässig ist es aber, Inkassodaten an eine Auskunftei zu übermitteln und gleichzeitig eine Beauskunftungssperre für diese Daten bei der Auskunftei zu veranlassen.

In einem an die Aufsichtsbehörde herangetragenen Fall hatte ein Betroffener die Forderung gegenüber dem Gläubiger bestritten, der sie zur Einziehung an ein In-

kassounternehmen übergeben hatte. Nachdem der Gläubiger das entsprechende Schreiben an das Inkassounternehmen weitergeleitet hatte, übermittelte dieses die den Schuldner betreffenden Inkassodaten an eine Auskunftei und veranlasste gleichzeitig bei dieser in automatisierter Form eine Beauskunftungssperre. Im Anschluss daran nahm das Inkassounternehmen Kontakt mit dem Gläubiger auf, um die Einwände des Schuldners abzuklären. Kurze Zeit später wurden die Daten bei der Auskunftei auf Veranlassung des Inkassounternehmens gelöscht. Das Inkassounternehmen hat seine Verfahrensweise damit begründet, dass dadurch am besten sichergestellt werde, dass die Daten über die Auskunftei nicht an Dritte übermittelt würden. Auch werde dadurch ausgeschlossen, dass ein Mitarbeiter des Inkassounternehmens während der Bearbeitung des Inkassofalls aufgrund eines Versehens die Daten ohne Beauskunftungssperre an die Auskunftei übermittle, obwohl die Einmeldevoraussetzungen nicht vorlägen.

Wenn auch dem Inkassounternehmen kein böser Wille vorgeworfen werden konnte, haben wir diese Verfahrensweise gleichwohl beanstandet. Eine Einmeldung darf erst und nur dann erfolgen, wenn das Verhalten des Betroffenen zweifelsfrei den Schluss auf dessen Zahlungsunfähigkeit oder Zahlungsunwilligkeit zulässt. Im vorliegenden Fall hätte eine Einmeldung schon deshalb nicht erfolgen dürfen, weil die Daten im Zeitpunkt der Einmeldung bestritten waren. Angesichts der Voraussetzungen für eine Einmeldung ist es im Übrigen ein Widerspruch in sich, gleichzeitig Inkassodaten einzumelden und eine Beauskunftungssperre zu veranlassen. Wir haben das Unternehmen aufgefordert, von dieser Handhabung künftig Abstand zu nehmen und empfohlen, in solchen Fällen bereits im Datensystem des Inkassounternehmens eine automatisierte Sperre zu setzen, die eine unzulässige Datenübermittlung an die Auskunftei durch eigene Mitarbeiter verhindert.

1.9 In welchen Fällen muss ein Inkassounternehmen personenbezogene Daten sperren beziehungsweise löschen?

Bei den überprüften Inkassounternehmen wurden die Vorschriften des Bundesdatenschutzgesetzes über das Sperren und Löschen personenbezogener Daten nicht beachtet, obwohl diese – teilweise modifiziert – auch für Inkassounternehmen gelten. So hatte eines der überprüften Unternehmen im Zeitpunkt unseres Kontrollbesuchs rund zehn Millionen Datensätze von Schuldnern gespeichert; Datensperrungen und Datenlöschungen hatten bisher nicht stattgefunden. Ein Unternehmen verfuhr in der Weise, dass ein sogenanntes Einstellungskennzeichen im automatisierten Inkassosystem gesetzt wurde, wenn die Forderung nicht beweisbar oder unbegründet war, wodurch der automatisierte Ablauf des Inkassoverfahrens gestoppt wurde. Die Sachbearbeiter konnten aber weiterhin uneingeschränkt auf die Daten zugreifen. Gespeicherte Daten zu abgeschlossenen Forderungsvorgängen kopierte dieses Unternehmen in regelmäßigen Zeitabständen aus dem Inkassosystem auf Datenträger und lagerte diese separat. Die ausgelagerten Vorgänge verblieben im System nur noch als Kurzdatensätze. Um in Einzelfällen nähere Informationen zu den Vorgängen zu erhalten, mussten die Datenträger mit erheblichem technischen Aufwand wieder in das Inkassosystem eingespielt werden.

Es bestand daher Veranlassung, darauf hinzuweisen, dass

- das Bundesdatenschutzgesetz mehrere Alternativen kennt, bei denen Daten gesperrt werden müssen (dazu unten Nrn. 1.9.1 und 1.9.2);
- unter Sperren das Kennzeichnen gespeicherter personenbezogener Daten zu verstehen ist, um ihre weitere Verarbeitung oder Nutzung einzuschränken (§ 3 Abs. 4 Nr. 4 BDSG; dazu unten Nr. 1.9.3).

1.9.1 Sperrung von Daten wegen Nichtfeststellbarkeit ihrer Richtigkeit oder Unrichtigkeit

Nach § 35 Abs. 4 BDSG sind personenbezogene Daten zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt. Die Voraussetzungen für eine Sperrung nach dieser Vorschrift liegen vor, wenn einerseits der Betroffene die Unrichtigkeit der Daten behauptet, sie aber nicht beweisen kann, andererseits die verantwortliche Stelle an der Richtigkeit der Daten festhält und ihr gleichfalls der Beweis dafür

nicht gelingt. Solange eine abschließende gerichtliche Klärung nicht erfolgt ist, müssten die Daten eigentlich gesperrt werden. Dies hätte zur Folge, dass das Inkassounternehmen die Daten auch nicht mehr für die Inkassobearbeitung nutzen dürfte.

Dem steht allerdings die Rolle des Inkassounternehmens als Interessenvertreter des Gläubigers, wie sie auch das Bundesverfassungsgericht sieht, entgegen. Würde der Gläubiger selbst versuchen, seine Forderungen gegenüber dem Schuldner durchzusetzen, wäre es ihm nicht verwehrt, sein Bemühen trotz Bestreitens des Schuldners fortzusetzen. Für das Inkassounternehmen muss dasselbe gelten, da es nach der Entscheidung des Bundesverfassungsgerichts auch bestrittene Forderungen beitreiben darf. Dies gilt allerdings dann nicht, wenn eine Fortführung des Inkassoverfahrens rechtsmissbräuchlich wäre. Eine Fortsetzung des Verfahrens und damit auch eine weitere Nutzung der Daten für Inkassozwecke ist datenschutzrechtlich aber jedenfalls dann nicht zu beanstanden, wenn das Inkassounternehmen und der Gläubiger der übergebenen Forderung nach Prüfung des Sachverhalts zu dem Ergebnis kommen, dass das Bestreiten unerheblich ist. Ferner müssen bei Einwendungen des Schuldners in tatsächlicher Hinsicht die Forderung belegende Unterlagen zur Verfügung stehen. Bei Einwendungen im rechtlichen Sinn müssen diese hinreichend überprüft worden sein. Bei rechtlichen Einwendungen gilt dies zumindest dann, wenn zu einer Streitfrage unterschiedliche Auffassungen vertreten werden können. Nur wenn die Position des Gläubigers völlig abwegig und nach allen Betrachtungen unhaltbar ist (zum Beispiel wenn der Wortlaut einer gesetzlichen Vorschrift eindeutig entgegensteht), müssen die Daten gesperrt werden.

1.9.2 Sperrung von Daten wegen fehlender Erforderlichkeit

Inkassounternehmen müssen personenbezogene Daten ferner sperren, wenn

- ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist und
- einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen.

So verhält es sich hier. Inkassounternehmen sind sowohl nach der Abgabenordung als auch nach dem Handelsgesetzbuch und aufgrund analoger Anwendung der Bundesrechtsanwaltsordnung verpflichtet, Unterlagen noch für fünf, sechs oder zehn Jahre aufzubewahren. Erst nach Ablauf dieser Aufbewahrungsfristen müssen die Daten folglich gelöscht werden. Solange die Aufbewahrungsfristen laufen, sind die Daten zu sperren.

Wenn Inkassofälle abgeschlossen beziehungsweise dauerhaft eingestellt sind, ist die Kenntnis der Daten für die Erfüllung des Zwecks der Speicherung, nämlich der Bearbeitung des Inkassofalls, nicht mehr erforderlich. Praktische Beispiele sind die vollständige Bezahlung einer Forderung durch den Schuldner beziehungsweise eine erfolgreiche Beitreibung der Forderung beim Schuldner, die auf Wunsch des Gläubigers kulanzweise erfolgte dauerhafte Einstellung des Verfahrens oder die (nachträglich) bekannt gewordene Tatsache, dass die behauptete Forderung nie bestand oder auch nicht hinreichend nachgewiesen werden kann. In diesen Fällen sind die Daten zu sperren.

Dagegen ist bei Inkassovorgängen, die nicht durch Bezahlung oder Beitreibung erledigt sind und zudem nicht auf Wunsch des Gläubigers dauerhaft eingestellt wurden, die weitere Speicherung der Daten erforderlich und damit zulässig. Dies gilt auch dann, wenn das Verfahren ruht, aber jederzeit – zum Beispiel nach Verbesserung der finanziellen Situation des Schuldners – wieder aufgegriffen werden kann. In diesen Fällen muss das Inkassounternehmen die Daten nicht sperren.

Eines der überprüften Inkassounternehmen hat die Ansicht vertreten, es bestehe auch bei abgeschlossenen Inkassovorgängen ein Bedürfnis, auf die Forderungsdaten zurückgreifen zu können. Dies sei beispielsweise der Fall, wenn Schuldner bei Zahlungen versehentlich keine oder falsche Angaben zur Identifizierung des betreffenden Forderungsvorgangs gemacht hätten und die Zahlungen dem falschen Vorgang gutgeschrieben worden seien oder wenn der Schuldner bei fruchtbar abgeschlossenen Forderungsvorgängen trotz entsprechender Hinweise

Überzahlungen geleistet habe und eine teilweise Rückerstattung nicht möglich sei, weil die „alte“ Bankverbindung nicht mehr bestehe und/oder der Schuldner zwischenzeitlich mit unbekanntem Aufenthalt verzogen sei.

Solche Beispiele können jedoch nicht dazu führen, dass auf abgeschlossene Vorgänge und damit auf personenbezogene Daten des Schuldners zeitlich unbegrenzt zugegriffen werden darf. Im Hinblick darauf, dass Reklamationen des Schuldners in der Regel in zeitlicher Nähe zum Abschluss des Verfahrens erfolgen, hält es die Aufsichtsbehörde für ausreichend, wenn das Inkassounternehmen fruchtbar abgeschlossene Vorgänge noch für weitere sechs Monate speichert. Im Anschluss daran sind die Daten zu sperren. Für die Festlegung einer kurzen Übergangsfrist spricht im Übrigen, dass in den genannten Beispielsfällen selbst dann noch auf die Daten zugegriffen werden darf, wenn diese gesperrt sind. Es liegen nämlich die gesetzlichen Voraussetzungen für eine „Entsperrung“ vor (vergleiche § 35 Abs. 8 BDSG). Zudem wird der Betroffene in den genannten Fällen ohnehin in der Regel seine Einwilligung zur Nutzung der gesperrten Daten erteilen.

1.9.3 Löschen personenbezogener Daten

Nach Ablauf der oben dargestellten Aufbewahrungsfristen müssen Inkassounternehmen die personenbezogenen Daten löschen. Unabhängig von gesetzlichen Aufbewahrungsfristen sind personenbezogene Daten ferner dann zu löschen, wenn ihre Speicherung unzulässig ist (§ 35 Abs. 2 Satz 2 Nr. 1 BDSG), was zum Beispiel bei Personenverwechslungen der Fall sein kann.

1.9.4 Durchführung der Sperrung und Löschung personenbezogener Daten

Keinem der überprüften Unternehmen konnte bescheinigt werden, dass es Daten ordnungsgemäß sperrt beziehungsweise löscht. Die technische Durchführung – soweit eine solche, wie oben dargestellt, überhaupt stattfand – entsprach nicht dem Bundesdatenschutzgesetz.

Für eine *Sperrung* ist es erforderlich, dass die Kennzeichnung so vorgenommen wird, dass die angeordnete Verarbeitungs- und Nutzungsbeschränkung tatsächlich Wirkung entfaltet und – gegebenenfalls auch durch technisch-organisatorische Maßnahmen – alle unter den Nutzungsbegriff fallenden Funktionen wirksam verhindert werden. Bei automatisierten Verfahren ist es möglich, das Datenfeld, den Datensatz oder andere bestimmte Datenmengen entsprechend zu kennzeichnen, wobei durch Ausgestaltung der Verarbeitungssoftware sicherzustellen ist, dass Zugriffe auf den Inhalt der betreffenden Datensätze nur noch in den gesetzlich vorgesehenen Ausnahmefällen erfolgen können. Eine weitere Möglichkeit besteht darin, die zu sperrenden Daten beziehungsweise Datensätze, die solche enthalten, aus dem Grunddatenbestand herauszunehmen und in einem als gesperrt zu kennzeichnenden und zu behandelnden Sonderdatenbestand anzulegen, auf den im Grunddatenbestand hingewiesen werden kann (Dammann in Kommentar zum Bundesdatenschutzgesetz; Hrsg. Simitis, 6. Auflage, § 3 Rn. 166, 169, 170). Zusätzlich sollte sichergestellt werden, dass nur ein eingeschränkter Personenkreis Zugriff auf die gesperrten Datensätze erhält. Auch darf ein Sachbearbeiter keinesfalls Zugriff auf den vollständigen Datensatz des Schuldners erhalten, wenn dessen Daten gesperrt sind. Dem ist in automatisierter Weise Rechnung zu tragen. Außerdem dürfen die gesperrten Daten nicht mehr genutzt werden, auch nicht für die Bearbeitung weiterer, gegen den Schuldner gerichteter Inkassovorgänge. Insoweit ist auch ein Abgleich im Hinblick darauf, ob vom Schuldner bereits früher Forderungen im Zuge der Inkassobearbeitung eingezogen wurden, unzulässig.

Löschen ist nach der Legaldefinition das Unkenntlichmachen gespeicherter personenbezogener Daten (§ 3 Abs. 4 Nr. 5 BDSG). Ein Unkenntlichmachen liegt dann vor, wenn dadurch eine Information nicht länger aus gespeicherten Daten gewonnen werden kann und damit verschwindet. Nicht ausreichend ist es, wenn lediglich ein gezielter Zugriff auf die Daten ausgeschlossen wird (Dammann in Kommentar zum Bundesdatenschutzgesetz; Hrsg. Simitis, 6. Auflage, § 3 Rn. 174, 182).

Diesen Grundsätzen wurde von keinem der Unternehmen Rechnung getragen.

1.10 Welche Fehler einem Inkassounternehmen bei der Bearbeitung eines Falls unterlaufen können

Ein Paradebeispiel dafür, was bei der Datenverarbeitung eines Inkassounternehmens alles falsch gemacht werden kann, ist folgender Einzelfall:

Das Inkassounternehmen war mit dem Einzug einer Forderung eines Versandhandelsunternehmens beauftragt worden, die sich gegen eine Person A unter einer konkreten Adresse richtete. Nachdem mehrere Mahnungen ergebnislos dorthin versandt wurden, Mahn- und Vollstreckungsbescheid durch beauftragte Rechtsanwälte erwirkt und ein Zwangsvollstreckungsauftrag erteilt worden war, erfolgte die Rückmeldung durch den Gerichtsvollzieher, der Schuldner sei unbekannt verzogen. Die Schuldnerdaten des A waren mit den entsprechenden Negativmerkmalen zuvor an eine Auskunftei übermittelt worden.

Aufgrund der Mitteilung des Gerichtsvollziehers veranlasste das Inkassounternehmen eine Anfrage bei der Meldebehörde. Dieses ließ wissen, die angefragte Person sei an eine benannte Adresse umgezogen. Dort wohnte der unbeteiligte B, der denselben Vor- und Familiennamen wie „Schuldner“ A hat. Das Inkassounternehmen meldete daraufhin an die Auskunftei, dass zu B – unter dessen Adresse – ein Zwangsvollstreckungsauftrag vorliege.

Nachdem B hiervon erfuhr, reklamierte er gegenüber dem Inkassounternehmen. Dieses veranlasste daraufhin – insoweit noch vorbildlich – die Sperrung der Daten bei der Auskunftei. Weiterhin stellte es nochmals eine Anfrage an die Meldebehörde. Noch bevor deren Auskunft vorlag, veranlasste das Inkassounternehmen dann allerdings die Aufhebung der Sperre bei der Auskunftei.

Doch mit diesem Fehler hatte die Angelegenheit noch lange nicht ihr Bewenden. Die neuerliche – erweiterte – Anfrage bei der Meldbehörde ergab, dass B zuvor nicht unter der Adresse des gesuchten Schuldners A gewohnt hatte. Dies hätte dazu führen müssen, dass das Inkassounternehmen die Löschung der bei der Auskunftei zu B gespeicherten Negativdaten veranlasst, da sich diese als falsch herausgestellt hatten. Stattdessen meldete das Unternehmen an die Auskunftei, B sei unbekannt verzogen.

Daraufhin stellte B bei der Polizei Strafanzeige gegen unbekannt. Nunmehr ging auch das Inkassounternehmen davon aus, dass hinsichtlich der dem Forderungsfall zugrunde liegenden Bestellung ein Betrugsfall eines Unbekannten vorlag. Es stellte deshalb das Einzugsverfahren ein.

Allerdings führte auch dies nicht dazu, dass die Daten von B bei der Auskunftei gelöscht wurden. Das Inkassounternehmen veranlasste vielmehr die Speicherung eines „Erledigungsvermerks“ zum Negativmerkmal. Erst als sich B direkt an die Auskunftei wandte und sich diese zur Abklärung des Sachverhalts mit dem Inkassounternehmen in Verbindung setzte, veranlasste dieses die Löschung der Daten bei der Auskunftei.

Das Inkassounternehmen hat sein datenschutzwidriges Verhalten bedauert. Dies hinderte uns jedoch nicht, angesichts der erheblichen Verstöße gegen das Bundesdatenschutzgesetz eine Beanstandung auszusprechen.

2 Wenn eine Rechtsanwaltskanzlei wie ein Inkassounternehmen tätig wird

Inwieweit Rechtsanwälte dem Bundesdatenschutzgesetz unterfallen, ist zwischen den Rechtsanwaltskammern und den Datenschutzaufsichtsbehörden umstritten (siehe hierzu auch dritter Tätigkeitsbericht B 2.3, S. 21 ff.).

Die *Aufsichtsbehörden* sind der Auffassung, dass das Bundesdatenschutzgesetz auch hinsichtlich mandatsbezogener Daten auf Rechtsanwälte anwendbar ist. Die Bundesrechtsanwaltsordnung (BRAO) enthält lediglich punktuelle datenschutzrechtliche Regelungen. Nur insoweit treten die Vorschriften des Bundesdatenschutzgesetzes zurück (§ 1 Abs. 3 BDSG).

Daraus folgt zum einen, dass die Rechtsanwaltskanzleien der Kontrolle der zuständigen Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich unterliegen. Denn durch das anwaltliche Berufsgeheimnis werden die Informationsrechte der Aufsichtsbehörden nach § 38 Abs. 3 BDSG nicht eingeschränkt.

§ 24 Abs. 2 Satz 1 Nr. 2 und Abs. 6 BDSG bestimmt ausdrücklich, dass sich die Kontrolle der Datenschutzaufsichtsbehörden auch auf personenbezogene Daten erstreckt, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen.

Zum anderen folgt daraus, dass Rechtsanwälte verpflichtet sind, einen betrieblichen Datenschutzbeauftragten zu bestellen, wenn die Voraussetzungen des § 4 f Abs. 1 BDSG vorliegen. Dies ist unseres Erachtens nunmehr auch eindeutig geregelt, da im neuen § 4 f Abs. 2 Satz 3 BDSG klargestellt ist, dass sich die Kontrollbefugnisse eines (externen) betrieblichen Datenschutzbeauftragten auch auf personenbezogene Daten erstrecken, die – wie bei Rechtsanwälten – einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Die neueste Fassung des § 203 Abs. 2 a des Strafgesetzbuchs (StGB) sieht vor, dass die Absätze 1 und 2 entsprechend gelten, wenn ein Beauftragter für den Datenschutz unbefugt ein fremdes Geheimnis offenbart, das einem in den Absätzen 1 und 2 Genannten in dessen beruflicher Eigenschaft anvertraut oder sonst bekannt geworden ist und von dem er bei der Erfüllung seiner Aufgaben als Beauftragter für den Datenschutz Kenntnis erlangt hat. Damit gilt § 203 StGB auch für den (externen) betrieblichen Datenschutzbeauftragten einer Rechtsanwaltskanzlei.

Die Aufsichtsbehörden haben ihre Auffassung durch zwei Beschlüsse des Düsseldorfer Kreises bekräftigt.

Die *Bundesrechtsanwaltskammer* wie auch die *Rechtsanwaltskammern in Baden-Württemberg* vertreten dagegen die Ansicht, dass Rechtsanwälte aufgrund des in § 43 a Abs. 2 BRAO und § 203 Abs. 1 Nr. 3 StGB geregelten Mandatsgeheimnisses gegenüber den Aufsichtsbehörden für den Datenschutz zur Verschwiegenheit berechtigt und verpflichtet sind. Die von den Rechtsanwaltskammern durchzuführende Berufsaufsicht (§§ 56, 73 Abs. 2 Nr. 4 BRAO) erstrecke sich auch auf alle Fragen des Datenschutzes und der Datensicherheit bei der Verarbeitung personenbezogener Daten durch den Rechtsanwalt.

Die Rechtsanwaltskammern Baden-Württembergs haben uns dargelegt, dass sich die Verarbeitung mandatsbezogener Daten durch Rechtsanwälte nicht an den Vorschriften des Bundesdatenschutzgesetzes messen lassen müsse und Rechtsanwaltskanzleien auch keinen betrieblichen Datenschutzbeauftragten bestellen müssten. Hieran ändere auch die jüngste Änderung der Vorschriften über den betrieblichen Datenschutzbeauftragten nichts.

Aufgrund dessen verweigern Rechtsanwälte in Beschwerdefällen vielfach Auskünfte gegenüber der Aufsichtsbehörde.

Besondere Brisanz erlangt dieses Verhalten dann, wenn eine Rechtsanwaltskanzlei wie ein Inkassounternehmen tätig wird. So betreibt eine baden-württembergischen Anwaltskanzlei, für ein führendes Telekommunikationsunternehmen im Rahmen des Anwaltsmandats das Forderungsmanagement. Sie bedient sich dabei eines Auftragsdatenverarbeiters.

Die Betroffenen sind letztendlich in der gleichen Situation wie Betroffene, die von einem „normalen“ Inkassounternehmen belangt werden. Werden in einem solchen Fall Auskünfte an die Aufsichtsbehörde verweigert, ist eine datenschutzrechtliche Kontrolle dieser datenschutzrechtlich sensiblen Tätigkeit – anders als bei „normalen“ Inkassounternehmen – nicht möglich.

Anfangs zeigte sich die Rechtsanwaltskanzlei durchaus noch kooperativ und beantwortete Anfragen der Aufsichtsbehörde in Beschwerdefällen. Die Situation änderte sich, nachdem die Aufsichtsbehörde – auch aufgrund einiger Beschwerden gegen die Kanzlei – eine datenschutzrechtliche Kontrolle durchgeführt und nachfolgend Änderungen im Umgang mit den Daten gefordert hatte. Mittlerweile beruft sich die Kanzlei darauf, dass der Anwendungsbereich des Bundesdatenschutzgesetzes auf ihre Tätigkeit allenfalls stark eingeschränkt Anwendung finde. Sie weigert sich daher, einen betrieblichen Datenschutzbeauftragten zu bestellen, der nach unserer Auffassung nicht nur rechtlich erforderlich, sondern dringend vonnöten wäre. Was die Auskunftserteilung uns gegenüber angeht, hat sie uns wissen lassen, sie werde uns ohne Entbindung von der anwaltlichen Schweigepflicht durch ihren Auftraggeber keine Auskünfte mehr erteilen.

Die Situation hat sich inzwischen noch verschärft. In einem Beschwerdefall hatten wir die Anwaltskanzlei aufgefordert, dem Betroffenen, der sich zuvor erfolglos an die Kanzlei gewandt hatte, nach § 34 BDSG Auskunft über die zu seiner

Person gespeicherten Daten zu erteilen. Unter Berufung auf ein zivilgerichtliches Urteil hat uns die Anwaltskanzlei daraufhin mitgeteilt, ein Anspruch auf Auskunft nach § 34 BDSG bestehe aufgrund des Mandantenverhältnisses nicht. Soweit der Rechtsanwalt nicht ausdrücklich durch den Mandanten zur Auskunft beauftragt werde, sei eine solche Auskunft auch nicht zu erteilen. Weitere Beschwerdefälle deuten darauf hin, dass die Rechtsanwaltskanzlei Auskunftsersuchen von Betroffenen nun nicht mehr nachkommt.

Gerade in Fällen, in denen Betroffene nachzuweisen versuchen, dass eine geltend gemachte Forderung nicht besteht, sind sie auf die Kenntnis der zu ihnen gespeicherten Daten sowie gegebenenfalls deren Herkunft und Empfänger – dies sieht § 34 BDSG ebenfalls vor – angewiesen. Wir haben der Rechtsanwaltskanzlei mitgeteilt, dass Betroffene jedenfalls dann einen Auskunftsanspruch nach § 34 BDSG besitzen, wenn, wie im vorliegenden Fall, eine Rechtsanwaltskanzlei Daten der Betroffenen für Inkassozwecke dateimäßig verarbeitet und wie andere Inkassounternehmen auch auftritt. Rechtsanwaltskanzleien, die in dieser Weise tätig werden, haben auch die Vorschriften des Bundesdatenschutzgesetzes über die Sperrung und Löschung personenbezogener Daten zu beachten.

Soweit die Rechtsanwaltskanzlei Betroffenen Auskünfte nach § 34 BDSG verweigert, bleiben diesen, da die Aufsichtsbehörde ihre Auffassung nicht durchsetzen und Verstöße gegen § 34 BDSG auch nicht mit einem Bußgeld ahnden kann, nur zwei Möglichkeiten: Zum einen können sie ihren Auskunftsanspruch gegenüber der Rechtsanwaltskanzlei auf dem Zivilrechtsweg weiter verfolgen. Zum anderen können sie den Auftraggeber der Rechtsanwaltskanzlei, das Telekommunikationsunternehmen, um Auskunft bitten, welche Daten dort über sie gespeichert sind. Dies könnte ein Ansatz sein, weil das Telekommunikationsunternehmen einen Teil seiner Daten mit Erteilung des Inkassoauftrags an die Rechtsanwaltskanzlei übermittelt. Ein gleichwertiger Ersatz für den Auskunftsanspruch gegenüber der Rechtsanwaltskanzlei ist das allerdings nicht, da der Betroffene damit noch nicht weiß, welche Daten die Rechtsanwaltskanzlei über ihn speichert.

Das Telekommunikationsunternehmen hätte darüber hinaus die Möglichkeit, die Rechtsanwaltskanzlei von der Schweigepflicht zu entbinden und vertraglich sicherzustellen, dass diese sämtlichen Verpflichtungen einer „verantwortlichen Stelle“ nach dem Bundesdatenschutzgesetz nachkommt. Da nichts darauf hindeutet, dass das Telekommunikationsunternehmen diesen Weg beschreiten wird, bleibt nur die Hoffnung, dass der Bundesgesetzgeber alsbald eindeutig klarstellt, dass auch Rechtsanwälte den Vorschriften des Bundesdatenschutzgesetzes unterliegen. Auf keinen Fall können Rechtsanwälte, die wie ein Inkassounternehmen tätig werden, Sonderrechte für sich beanspruchen. Dies würde auch zu Wettbewerbsverzerrungen bei Inkassounternehmen führen.

3 Auskunfteien

3.1 Allgemeines

Datenschutzbeschwerden über Auskunfteien sind ein echter „Dauerbrenner“. Auch in diesem Berichtszeitraum wurden hierzu eine Vielzahl von Einzelfällen an die Aufsichtsbehörde herangetragen.

Die Tätigkeit von Auskunfteien besteht darin, dass sie Auskünfte über die wirtschaftlichen Verhältnisse von Privatpersonen oder Unternehmen erteilen, um unternehmerische Risiken zu senken. Aufgrund der weitreichenden Auswirkungen auf das informationelle Selbstbestimmungsrecht enthält das Bundesdatenschutzgesetz in § 29 BDSG Regelungen zur Datenerhebung, -verarbeitung und -nutzung durch Auskunfteien. Daraus ergibt sich aber auch, dass ihre Tätigkeit nicht – wie manche Beschwerdeführer meinen – per se mit dem Datenschutzrecht unvereinbar ist. Hinsichtlich der Daten ist zu unterscheiden zwischen sogenannten Negativdaten, die ein „negatives“ Zahlungsverhalten betreffen und auch ohne Einwilligung des Betroffenen unter bestimmten Voraussetzungen an Dritte weitergegeben werden dürfen, und den Positivdaten, die Auskunft über vertragsgemäßes Verhalten geben. Positivdaten dürfen nur mit Einwilligung des Betroffenen übermittelt werden.

Die bei der Aufsichtsbehörde eingegangenen Beschwerdefälle betrafen im Wesentlichen folgende Fallgruppen:

– Viele der Beschwerdeführer wandten sich an die Aufsichtsbehörde, weil sie unmittelbar zuvor ein sogenanntes Benachrichtigungsschreiben erhalten hatten. Auskunfteien sind grundsätzlich verpflichtet, Personen von der erstmaligen Übermittlung ihrer Daten an Dritte zu benachrichtigen, das heißt in der Regel, wenn sie erstmals eine Bonitätsauskunft zu einer Person erteilen. Die Beschwerdeführer konnten mit dieser Benachrichtigung zumeist wenig anfangen, weil sie das Tätigkeitsfeld von Auskunfteien gar nicht kannten. Sie baten uns um Erläuterung des Schreibens und Überprüfung der Rechtmäßigkeit des Vorgehens.

– Ein weiterer Teil der Beschwerdefälle betraf die Richtigkeit der zu den Betroffenen bei der Auskunftei gespeicherten Daten. Die Beschwerdeführer machten – in vielen Fällen zu Recht – geltend, die zu ihrer Person gespeicherten Daten seien unrichtig beziehungsweise ihnen seien fälschlicherweise Daten einer anderen Person mit gleichem oder ähnlichem Namen zugeordnet worden. Von der Speicherung ihrer Daten bei einer Auskunftei hatten die Betroffenen zumeist dadurch erfahren, dass ihnen ein bestimmter Vertragsabschluss oder auch die Zahlungsweise auf Rechnung wegen schlechter Bonität verwehrt wurde. Andere Beschwerdeführer hatten aufgrund eines Benachrichtigungsschreibens einer Auskunftei bei dieser eine Auskunft über die zu ihrer Person gespeicherten Daten eingeholt und daraufhin die Unrichtigkeit der Daten gerügt.

Die Aufsichtsbehörde hat im Berichtszeitraum mehrere Auskunfteien umfassend geprüft, wobei zwei dieser Prüfungen noch nicht abgeschlossen sind.

3.2 Handlungsbedarf für den Gesetzgeber

Gerade im Bereich der Auskunfteien werden die Datenschutzaufsichtsbehörden aber auch mit grundlegenden Problemen konfrontiert, die sich weder durch die Bearbeitung von Beschwerdefällen noch durch Prüfungen lösen lassen. Das Bundesdatenschutzgesetz, das die Voraussetzungen der Datenerhebung, Datenverarbeitung und Datennutzung durch Auskunfteien regelt, enthält viele unbestimmte Rechtsbegriffe, die die Aufsichtsbehörden einerseits und die Auskunfteien und deren Kunden andererseits oftmals unterschiedlich auslegen. Hinzu kommt, dass die Aufsichtsbehörden nur über sehr begrenzte Handlungsmöglichkeiten verfügen, um ihre Haltung durchzusetzen. Die Aufsichtsbehörden können, sieht man vom technisch-organisatorischen Bereich ab, gegenüber Unternehmen keine Anordnungen erlassen, wonach diese eine bestimmte Datenverwendung künftig zu unterlassen haben. Sie haben zwar die Möglichkeit, bei bestimmten datenschutzrechtlichen Verstößen ein Bußgeld zu verhängen; die Durchführung von Ordnungswidrigkeitenverfahren im Einzelfall ist allerdings nicht dazu geeignet, datenschutzrechtliche Streitfragen einer Klärung zuzuführen.

Angesichts der Vielzahl der Betroffenen sowie von zigmillionen Auskünften, die die Auskunfteien Jahr für Jahr erteilen, der wirtschaftlichen Machtstellung der Auskunfteien und der angespannten Wettbewerbssituation in diesem Bereich wird letztlich der Gesetzgeber für eindeutige gesetzlichen Rahmenbedingungen sorgen müssen.

Aus heutiger Sicht erscheinen insbesondere folgende Punkte regelungs- oder in einem Gesetzgebungsverfahren erörterungsbedürftig:

– die Voraussetzungen für die Übermittlung von Daten durch Inkassounternehmen an Auskunfteien, falls keine einheitliche Praxis herbeigeführt werden kann;

– die Verfahrensweise, wenn Betroffene gegenüber der Auskunftei die Richtigkeit der zu ihrer Person gespeicherten Daten bestreiten. Das Bundesdatenschutzgesetz gibt vor, dass Daten, die unrichtig sind, zu berichtigen beziehungsweise zu löschen sind, wenn nach der Berichtigung kein Anlass zur weiteren Speicherung besteht. In Fällen, in denen die Richtigkeit vom Betroffenen bestritten wird, die Auskunftei aber der Ansicht ist, die Daten seien zutreffend und sich weder die Richtigkeit noch die Unrichtigkeit der Daten feststellen lässt, sind die Daten zu sperren. Das bedeutet eigentlich, dass die Daten für die Auskunftserteilung nicht mehr genutzt werden dürfen. In der Praxis ist zum einen fraglich, welche Qualität das Bestreiten des Betroffenen haben muss, welche Maßnahmen zur Prüfung der Richtigkeit durch die Auskunftei ergriffen

werden müssen und in welchen Fällen davon auszugehen ist, dass die Richtigkeit der Daten erwiesen ist. Zum anderen verfahren manche Auskunfteien in der Weise, dass sie dem Auskunftsempfänger mitteilen, dass bestrittene Daten gerade in der Überprüfung sind. Hier sollte eine Regelung klare Vorgaben machen, die eine einheitliche Praxis sicherstellen;

– die Frage, in welchen Fällen unter Berücksichtigung der schutzwürdigen Interessen des Betroffenen ein „berechtigtes Interesse“ an einer Bonitätsauskunft vorliegt, das heißt, in welchen Fällen eine Bonitätsauskunft eingeholt werden darf. Hierüber sind sich Datenschutzaufsichtsbehörden und Auskunfteien oft uneins. Das Bundesdatenschutzgesetz fordert nach dem Wortlaut als Voraussetzung für die Einholung einer Bonitätsauskunft zwar kein „kreditorisches“, sondern lediglich ein „berechtigtes“ Interesse. Dies kann ein rechtliches, wirtschaftliches oder ideelles Interesse sein. Da aber die schutzwürdigen Belange des Betroffenen berücksichtigt werden müssen, wird von den Aufsichtsbehörden in der Konsequenz gefordert, dass zumindest ein erhebliches finanzielles Ausfallrisiko vorliegen muss, um eine Übermittlung der Daten durch die Auskunftei und damit gleichzeitig eine Erhebung durch die anfragende Stelle zu rechtfertigen. Angesichts des drohenden Ausuferns des Kundenkreises der Auskunfteien sollte eindeutig geregelt werden, wer abfragen darf;

– die Frage, inwieweit Bonitätsauskünfte an Vermieter zulässig sind;

– die Frage, in welchen Fällen einer Person, zu der eine Bonitätsauskunft eingeholt wird, bei einer Auskunftei gespeicherte Merkmale zugeordnet werden dürfen, wenn Name, Adresse und/oder Geburtsdatum der abgefragten Person nicht hundertprozentig mit Name, Adresse und/oder Geburtsdatum einer mit Negativdaten gespeicherten Person übereinstimmen;

– die Löschungsfristen bei Auskunfteien. Hinsichtlich der unterschiedlichen bei Auskunfteien gespeicherten Merkmale sollten klare, differenzierte Löschungsgebote geschaffen werden, die auch dem Bedürfnis des Betroffenen gerecht werden, nach einer finanziellen Notsituation (zum Beispiel einem Insolvenzverfahren) wieder „auf die Beine“ zu kommen;

– grundsätzliche Fragen, die das Scoringverfahren betreffen. Mit einem Scoringverfahren wird anhand mathematisch-statistischer Methoden eine Prognose über das zukünftige (Zahlungs-)Verhalten von Personen(-gruppen) erstellt und in einer Punktzahl (Score) ausgedrückt (siehe hierzu dritter Tätigkeitsbericht C 1.1, S. 27 ff.). Spezifische Regelungen für Scoringverfahren enthält das Bundesdatenschutzgesetz bislang nicht. Solche wären aber sinnvoll, da die Beurteilung derartiger Verfahren nach geltendem Recht schwierig ist. Regelungsbedürftig erscheinen folgende Punkte:

  • Welche Daten beziehungsweise Merkmale dürfen in ein Scoringverfahren einfließen? Für einen Teilbereich enthält § 10 des Kreditwesengesetzes (KWG) nunmehr entsprechende Anhaltspunkte (siehe hierzu oben A 2.3). Außerhalb des Bankenbereichs fehlen solche. Hilfreich wäre zudem eine Klarstellung, inwieweit die Vorschriften des Allgemeinen Gleichbehandlungsgesetzes berücksichtigt werden müssen.

  • Welchen Umfang muss eine Auskunft an den Betroffenen haben? Die im Bundesdatenschutzgesetz enthaltenen Vorschriften sind insoweit nur bedingt zielführend. Dem Betroffenen muss, gerade im Fall einer aufgrund der Scorewertberechnung für ihn negativen Entscheidung, die Möglichkeit eingeräumt werden, diese überprüfen zu lassen. Voraussetzung hierfür ist, dass er eine Auskunft erhält, die Folgendes umfasst:

    – Welche Merkmale sind bei der Scorewertberechnung berücksichtigt worden?

    – Welche konkreten Merkmale waren im Fall des Betroffenen für die Bewertung ausschlaggebend?

    – Welcher Scorewert wurde wem übermittelt?

    – Wie lautet der aktuelle Scorewert?

    Die allgemeine Vorschrift für Auskünfte an den Betroffenen wird diesen Erfordernissen nicht gerecht. Zum einen werden die an Kunden übermittelten

Scorewerte inklusive der konkret eingeflossenen Merkmale oftmals nicht gespeichert und unterfallen damit nicht dem § 34 BDSG, zum anderen machen Unternehmen hinsichtlich der Merkmale, die generell einfließen, häufig das Geschäftsgeheimnis geltend. Hier ist der Gesetzgeber gefordert, eine klare Regelung für den Bereich Scoring zu treffen. In diesem Zusammenhang sollte auch überlegt werden, ob der Auskunftsanspruch hinsichtlich der Auskunftsempfänger (§ 34 Abs. 1 Satz 3 BDSG) nicht ausgeweitet werden kann. Zu oft berufen sich Auskunfteien derzeit auf die Wahrung von Geschäftsgeheimnissen.

§ 6 a Abs. 3 BDSG, der dem Betroffenen im Fall einer automatisierten Einzelentscheidung einen erweiterten Auskunftsanspruch einräumt, hilft im Bereich des Scorings meist nicht weiter, da in der Regel allenfalls eine teilautomatisierte Entscheidung vorliegt.

3.3 Daten aus den Schuldnerverzeichnissen der Amtsgerichte

Auskunfteien können von den Amtsgerichten aufgrund einer Bewilligung Abdrucke aus dem Schuldnerverzeichnis beziehen (§ 915 e der Zivilprozessordnung, § 2 der Schuldnerverzeichnisverordnung) und diese sodann speichern, sowie bei Vorliegen der Voraussetzungen des § 29 BDSG an Dritte übermitteln.

Bei den im Schuldnerverzeichnis gespeicherten Daten (zum Beispiel Abgabe einer eidesstattlichen Versicherung) handelt es sich um sogenannte harte Negativmerkmale, die hinsichtlich der Zahlungsfähigkeit des Schuldners besonders aussagekräftig sind. Übermittelt eine Auskunftei derartige Daten über einen Betroffenen an Dritte, kann das für diesen gravierende Folgen haben. Amtsgerichte und Auskunfteien müssen daher besonders darauf achten, dass die gespeicherten Daten richtig und vollständig sind.

Problematisch ist insoweit auch, dass die Eintragungen im Schuldnerverzeichnis oft nicht eindeutig sind. So muss zum Beispiel das Geburtsdatum des Schuldners nicht zwingend dort eingetragen werden, sondern nur dann, wenn es bekannt ist. Gerade das Geburtsdatum ist aber hilfreich bei der Zuordnung von Daten zu einer bestimmten Person. Bemühungen der Aufsichtsbehörde, bei der anstehenden Novellierung des Zwangsvollstreckungsrechts zu erreichen, dass im Schuldnerverzeichnis immer das Geburtsdatum eines Schuldners angegeben werden muss, blieben ohne Erfolg. Besonders relevant ist das Geburtsdatum in Fällen, in denen ein Elternteil und Sohn oder Tochter den gleichen Namen tragen und unter derselben Adresse wohnen. In diesen Fällen kann es bei der Auskunftserteilung leicht zu folgenschweren Verwechslungen kommen, die durch zwingende Angabe des Geburtsdatums vermieden werden könnten, immer unter der Voraussetzung, dass auch der bei der Auskunftei Anfragende das Geburtsdatum angibt.

In einem Beschwerdefall wandte sich ein Betroffener an uns, der sich über Probleme beim Abschluss eines Vertrags über eine Handy-Telefonkarte beklagte. Die Anbieter hatten vorab eine Auskunft bei der Auskunftei eingeholt und sodann einen Vertragsabschluss abgelehnt. Grund hierfür war, dass die angefragte Auskunftei dem Betroffenen im Rahmen einer fehlerhaften Adresszusammenführung Schuldnerverzeichnisdaten zugeordnet hatte, die eine völlig andere Person betrafen, die mit dem Betroffenen lediglich das Geburtsdatum und den Vornamen gemein hatte. Die Auskunftei hat ihren Fehler eingeräumt und die anfragenden Unternehmen davon benachrichtigt, dass eine Personenverwechslung vorlag und zu dem Betroffenen keine Negativdaten vorlagen. Die unzulässige Speicherung und Übermittlung der (falschen) Daten haben wir förmlich beanstandet.

In einem anderen Fall verlangte der Betroffene von einer Auskunftei die Sperrung der zu seiner Person gespeicherten Daten, die aus dem Schuldnerverzeichnis eines Amtsgerichts stammten, da diese nach seinem Vortrag vom Amtsgericht zu Unrecht eingetragen worden seien. Die Auskunftei hatte sich daraufhin mit dem Amtsgericht zur Klärung der Angelegenheit in Verbindung gesetzt und nachgefragt, ob dieses die Eintragung aufrecht erhält. Da das Amtsgericht die Eintragung mehrfach bestätigte, ging die Auskunftei davon aus, dass die Richtigkeit der Daten nachgewiesen war und teilte dem Betroffenen mit, dass sie eine Sperrung seiner Daten nicht vornehmen werde. Dieser verlangte sodann von der Aufsichtsbehörde Unterstützung.

Wir konnten ihm jedoch nicht helfen. Die Auskunftei hatte mit ihrer Nachfrage beim Amtsgericht ihrer rechtlichen Verpflichtung genügt. Da das Amtsgericht die Richtigkeit der Daten bestätigt hatte, musste die Auskunftei sie nicht sperren. Bei Daten, die nachweislich aus einem amtlichen Verzeichnis stammen, besteht in solchen Fällen eine Vermutung für deren Richtigkeit. Der Betroffene muss sich daher selbst um eine Löschung der Daten im Schuldnerverzeichnis bemühen. Erst wenn der Betroffene dort Erfolg hat und der Eintrag aus dem Schuldnerverzeichnis vorzeitig gelöscht wird, ist auch die Auskunftei verpflichtet, die Daten zu löschen.

3.4 Nachmeldungen an den Versandhandel

Im Rahmen der Kontrolltätigkeit wurde festgestellt, dass Auskunfteien Nachmeldungen an Versandhandelsunternehmen vornehmen. Eine Nachmeldung bedeutet, dass das Versandhandelsunternehmen, das zu einem bestimmten Zeitpunkt eine Bonitätsauskunft zu einer Person eingeholt hat (zum Beispiel wegen einer Lieferung auf Rechnung), automatisch bei Bonitäts- oder Adressänderungen dieser Person benachrichtigt wird. Die Arbeitsgruppe Auskunfteien des Düsseldorfer Kreises hat sich jüngst mit der Frage befasst, ob und inwieweit dies zulässig ist.

Da bei einer Nachmeldung letztlich eine aktuelle Auskunft über eine Person erteilt wird, muss im Zeitpunkt der Datenübermittlung ein berechtigtes Interesse des Versandhandelsunternehmens hieran vorliegen. Ein solches kann bei Dauerschuldverhältnissen bejaht werden. Der Abschluss eines Kaufvertrags im Versandhandel begründet jedoch kein derartiges Dauerschuldverhältnis. Nachmeldungen an Versandhandelsunternehmen sind nur zulässig, soweit den Betroffenen ein Ratenzahlungskredit oder ein Dispo-Kredit eingeräumt wurde. In allen anderen Fällen ist das Rechtsgeschäft nach Abwicklung des einzelnen Kaufgeschäfts für den Versandhandel abgeschlossen. Auch soweit Versandhändler intern zur Erleichterung der Geschäftsabläufe ein „Versandhauskonto“ für die Kunden einrichten, ändert dies nichts an der Bewertung, da hierdurch im Verhältnis zum Kunden keine Dauerrechtsbeziehung begründet wird. Selbst bei Sammelbestellern ist nicht ersichtlich, dass eine echte Dauerrechtsbeziehung begründet wird.

Die Aufsichtsbehörde hat die Versandhandelsunternehmen und die Auskunfteien im Lande entsprechend unterrichtet.

3.5 Auskunfteien ohne eigenen Datenbestand („Durchleite-Auskunfteien“)

Mittlerweile gibt es Dienstleistungsunternehmen, die Bonitätsauskünfte anbieten, aber über keine eigenen Daten verfügen. Sie greifen im Falle einer Anfrage eines Kunden bei ihnen auf den Datenbestand einer oder mehrerer klassischer Auskunfteien zurück und geben die dort gegebenenfalls gespeicherten Daten an den Kunden weiter beziehungsweise teilen diesem mit, dass keine Daten gespeichert sind. Die Auskunftsdaten speichern sie lediglich zu Protokollzwecken.

Die Aufsichtsbehörde hat im Berichtszeitraum ein solches Unternehmen, das nicht als Auftragsdatenverarbeiter für seine Kunden tätig wird, überprüft und generelle Anforderungen an derartige „Durchleite-Auskunfteien“ formuliert. Bei den Kunden des überprüften Unternehmens handelt es sich um Vermieter vor allem aus dem privaten Bereich, die im Vorfeld einer Vermietung Bonitätsabfragen zum potenziellen Mieter einholen möchten, wegen einer zu geringen Zahl an Bonitätsauskünften aber keinen Vertrag mit einer großen Auskunftei abschließen können.

Auf „Durchleite-Auskunfteien“ ist der für Auskunfteien geltende § 29 BDSG anwendbar, da ihre Tätigkeit letztlich die gleichen Auswirkungen auf Betroffene hat, wie wenn die Auskunft durch eine klassische Auskunftei erteilt wird, die selbst Daten speichert.

Eine Datenerhebung der „Durchleite-Auskunftei“ bei der klassischen Auskunftei und die für die Geschäftstätigkeit der „Durchleite-Auskunftei“ erforderliche Datenübermittlung durch die klassische Auskunftei sind nur zulässig, wenn die „Durchleite-Auskunftei“ an der Kenntnis der Daten ein berechtigtes Interesse hat, die Kenntnis insoweit erforderlich ist und die schutzwürdigen Interessen der Betroffenen hinreichend gewahrt werden. Das berechtigte Interesse der „Durchleite-

Auskunftei“ ergibt sich zwar nicht unmittelbar aus dem Interesse ihres Kunden an der Bonitätsauskunft, da das Unternehmen mit dem Verkauf von Bonitätsauskünften originär ein eigenes wirtschaftliches Interesse verfolgt. Ein berechtigtes Interesse des Kunden an einer Bonitätsauskunft ist aber im Rahmen der Abwägung des berechtigten Interesses der „Durchleite-Auskunftei“ mit den schutzwürdigen Belangen des Betroffenen zu berücksichtigen. Es führt letztlich dazu, dass die schutzwürdigen Belange des Betroffenen zurücktreten müssen und das Geschäftsmodell „Durchleite-Auskunftei“ überhaupt zulässig ist. Maßstab ihrer datenschutzrechtlichen Bewertung war für die Aufsichtsbehörde, dass die Datenschutzrechte des Betroffenen auch bei diesem Geschäftsmodell voll gewahrt werden.

3.5.1 Wie werden die schutzwürdigen Belange des Betroffenen bei der Datenübermittlung gewahrt?

Eine „Durchleite-Auskunftei“ muss in hinreichender Art und Weise sicherstellen, dass ihr Kunde (beispielsweise der Vermieter), dessen Anfrage weitergeleitet wird, weiß, in welchen Fällen ein berechtigtes Interesse tatsächlich besteht und unter welchen Voraussetzungen er eine Bonitätsauskunft einholen darf. So darf ein Vermieter eine Bonitätsauskunft zu einem Mietinteressenten nur dann einholen, wenn er mit diesem – vorbehaltlich des Ergebnisses der Bonitätsauskunft – tatsächlich einen Mietvertrag abschließen will. Nicht zulässig wäre es hingegen, wenn ein Vermieter bei einer anstehenden Vermietung zunächst einmal alle Mietinteressenten abfragen würde, um dann nur mit denjenigen weitere Gespräche beziehungsweise Vertragsverhandlungen zu führen, die keinen Negativeintrag bei der Auskunftei haben.

Bietet eine „Durchleite-Auskunftei“ Auskünfte für Anfragende an, die mit dem Bundesdatenschutzgesetz nicht vertraut sind und auch nicht – wie größere Firmen oder Unternehmen – über einen betrieblichen Datenschutzbeauftragten verfügen, muss sie zudem dafür Sorge tragen, dass ihr Kunde (beispielsweise der Vermieter) seine datenschutzrechtlichen Pflichten im Vorfeld der Abfrage, insbesondere seine Informationspflichten nach § 4 Abs. 3 BDSG, kennt beziehungsweise erfüllt. Wenn der Vermieter die persönlichen Daten beim Mietinteressenten erhebt, muss er ihn auch über die geplante Nutzung seiner Daten für eine Bonitätsanfrage informieren. Die „Durchleite-Auskunftei“ muss dies ihren Kunden in ihren Allgemeinen Geschäftsbedingungen oder im Teilnahmevertrag verdeutlichen.

Eine weitere Voraussetzung im Hinblick auf die schutzwürdigen Belange der Betroffenen ist, dass das Verfahren und die Datenflüsse sowohl gegenüber dem Kunden (zum Beispiel Vermieter) als auch gegenüber dem Betroffenen (zum Beispiel Mietinteressent) hinreichend transparent gemacht werden.

Nach den Vorgaben des Bundesdatenschutzgesetzes darf die „Durchleite-Auskunftei“ Daten an einen Kunden nur dann übermitteln, wenn dieser ihr gegenüber sein berechtigtes Interesse glaubhaft dargelegt hat. Eine solche Darlegung erfolgt im Rahmen der Anfrage des Kunden.

Im Fall der überprüften „Durchleite-Auskunftei“ haben wir angesichts des mit dem Bundesdatenschutzgesetz zumindest teilweise nicht vertrauten Kundenkreises gefordert, dass der anfragende Vermieter ihr gegenüber auch angeben muss, dass er den Mietinteressenten im Vorfeld über die Bonitätsabfrage informiert hat.

3.5.2 Wie werden die schutzwürdigen Belange des Betroffenen bei der Auskunftserteilung nach § 34 BDSG gewahrt?

Gemäß § 34 BDSG kann eine Person Auskunft über die zu ihrer Person gespeicherten Daten verlangen. Bei der „Durchleite-Auskunftei“ sind keine Bonitätsdaten gespeichert, allenfalls Protokolldaten zu abgefragten Personen.

Da die „Durchleite-Auskunftei“ im Falle einer Kundenanfrage auf den Datenbestand der Auskunftei zurückgreift und über die dort gespeicherten Daten Auskunft gibt, muss sie entsprechend verfahren, wenn der Betroffene bei ihr eine Selbstauskunft beantragt. Sie muss also dem Betroffenen mitteilen, ob und gegebenenfalls welche Daten bei der klassischen Auskunftei über ihn gespeichert sind. Die Auskunftei, von der die Daten stammen, ist dabei namentlich zu benennen. Nur so wird den Besonderheiten des Geschäftsmodells und den schutzwürdigen Belan-

gen des Betroffenen hinreichend Rechnung getragen und der Betroffene in die Lage versetzt, seine Datenschutzrechte wahrzunehmen und gegen Datenspeicherungen und -übermittlungen durch die klassische Auskunftei und die „Durchleite-Auskunftei“ vorzugehen, die nach seiner Ansicht zu Unrecht erfolgt sind.

3.5.3 Auswirkungen auf den Vertrag zwischen den beteiligten Auskunfteien

Der Sondersituation solcher „Durchleite“-Modelle sollte durch eine entsprechende Gestaltung des Vertrags zwischen der datenliefernden Auskunftei und dem durchleitenden Unternehmen Rechnung getragen werden.

3.6 Nachweis der Identität des Antragstellers bei Beantragung einer Selbstauskunft

Bei einem Unternehmen haben wir festgestellt, dass es zur Prüfung der Identität eines Betroffenen, der eine Auskunft nach § 34 BDSG begehrt, die Übersendung einer Kopie des Personalausweises sowie einer Meldebestätigung verlangt.

Verantwortliche Stellen sind verpflichtet, vor Erteilen einer Auskunft die Identität des Betroffenen zu prüfen, um zu vermeiden, dass personenbezogene Daten an einen tatsächlich nicht betroffenen Dritten übermittelt werden, der sich diese unter Umständen erschleichen will. Gerade bei der Beantragung einer Selbstauskunft über das Internet ist ein gewisser Sicherheitsstandard zu wahren. Durch die Vorlage einer Kopie des Personalausweises wird diesem Erfordernis nach Ansicht der Aufsichtsbehörde aber hinreichend Rechnung getragen.

Um zu vermeiden, dass die Auskunftei dabei auch von Daten Kenntnis erhält, die sie für die Identitätsprüfung nicht unbedingt benötigt (zum Beispiel Personalausweisnummer, Größe, Augenfarbe, Geburtsort), muss sie den Betroffenen darauf hinweisen wird, dass er diese Daten schwärzen kann.

Dagegen ist vom Anfordern einer Meldebestätigung abzusehen. Eine Meldebestätigung bringt im Hinblick auf die Identitätsfeststellung nicht so viel mehr, dass der Aufwand des Betroffenen gerechtfertigt wäre, der ihm durch das Einholen einer Meldebestätigung entsteht. Zwar legt grundsätzlich die verantwortliche Stelle das Verfahren und die Form der Identitätsprüfung fest; es dürfen aber keine überzogenen Anforderungen gestellt werden, die geeignet sind, den Betroffenen von der Geltendmachung seiner Rechte abzuhalten. Wir haben das Unternehmen deshalb aufgefordert, künftig entsprechend unseren Vorstellungen zu verfahren.

4 Versicherungen

4.1 Sachstand bei einigen zentralen datenschutzrechtlichen Fragestellungen

In unserem dritten Tätigkeitsbericht (C 4.1, S. 79 ff. und C 4.2, S. 82 .ff) hatten wir einige zentrale datenschutzrechtliche Fragestellungen im Bereich der Versicherungswirtschaft näher beleuchtet. Inzwischen gibt es bei allen Fragestellungen Fortschritte:

4.1.1 Entbindung von der ärztlichen Schweigepflicht

Zur Beurteilung der Leistungspflicht im Einzelfall erheben die privaten Krankenversicherer, bei Ärzten, anderen Angehörigen von Heilberufen und Krankenhäusern Gesundheitsdaten, die der ärztlichen Schweigepflicht unterliegen. Damit Ärzte Patienteninformationen offenbaren dürfen, bedarf es einer wirksamen Einwilligungserklärung des Patienten. Derzeit greifen die Krankenversicherer hierfür auf eine vor 18 Jahren zwischen der Versicherungswirtschaft und dem Düsseldorfer Kreis abgestimmte pauschale Schweigepflichtentbindungserklärung zurück, die die versicherte Person bei dem oftmals viele Jahre zurückliegenden Vertragsschluss abgegeben hat. Dies halten wir ebenso wie andere Datenschutzaufsichtsbehörden im Hinblick auf das 2001 geänderte Bundesdatenschutzgesetz nicht für ausreichend, weil die versicherte Person bei Vertragsabschluss nicht erkennen kann, wann von der Erklärung Gebrauch gemacht werden soll und welche Patien-

tendaten künftig bei wem angefordert werden. Eine wirksame Einwilligungserklärung im Sinne des § 4 a BDSG liegt damit nicht vor.

In dieselbe Richtung weist auch die Entscheidung des Bundesverfassungsgerichts vom 23. Oktober 2006 (Az: 1 BvR 2027/02). In der Sache ging es um Leistungen aus einer Berufsunfähigkeitsversicherung, die eine Versicherungsnehmerin wegen Berufsunfähigkeit bei ihrer Versicherung beantragt, jedoch nicht bekommen hatte, nachdem sie es abgelehnt hatte, eine generelle Schweigepflichtentbindungserklärung zu unterzeichnen. Sie war jedoch bereit, Einzelermächtigungen für jedes Auskunftsersuchen der Versicherung gegenüber einem Arzt zu erteilen. Die Versicherung hatte es daraufhin abgelehnt, auf dieser Grundlage den Leistungsfall festzustellen. Das Bundesverfassungsgericht setzt sich in seiner Entscheidung kritisch mit der Frage der möglichen Verletzung des Rechts auf informationelle Selbstbestimmung durch eine allgemeine Schweigepflichtentbindungsklausel in einem Berufsunfähigkeitsversicherungsvertrag auseinander. Es geht im entschiedenen Fall davon aus, dass bei Abschluss des Versicherungsvertrags ein erhebliches Verhandlungsungleichgewicht bestanden hat und die Beschwerdeführerin ihren informationellen Selbstschutz nicht eigenverantwortlich und selbstständig sicherstellen konnte. Es hebt hervor, dass Vertragsbedingungen der Versicherer praktisch nicht verhandelbar sind. Es liege nicht auf der Hand, dass es für den Versicherer unmöglich oder unzumutbar sei, bestimmte Aufklärungsmaßnahmen im Voraus zu beschreiben und dem Versicherungsnehmer zur Entbindung von der Schweigepflicht vorzulegen. Des Weiteren wird die staatliche Verantwortung betont, die Voraussetzungen eines wirkungsvollen informationellen Selbstschutzes zu gewährleisten.

§ 213 des Entwurfs eines Versicherungsvertragsgesetzes sieht nunmehr vor, dass ein Versicherer personenbezogene Gesundheitsdaten bei Dritten nur erheben darf, soweit die Kenntnis der Daten für die Beurteilung des zu versichernden Risikos oder der Leistungspflicht erforderlich ist, die Daten bei einem nach § 203 StGB der Verschwiegenheit Verpflichteten erhoben werden und der Betroffene *im Einzelfall* eine Einwilligung nach § 4 a BDSG erteilt hat.

Die Aufsichtsbehörden begrüßen die vorgesehene Regelung und hoffen, dass sie Gesetz wird.

4.1.2 Datenverwendungsklauseln in Versicherungsverträgen

Im dritten Tätigkeitsbericht (C 4.2, S. 82 ff.) hatten wir noch darüber berichtet, dass die Datenschutzaufsichtsbehörden Verhandlungen mit der Versicherungswirtschaft über eine Neufassung der 1994 zwischen den obersten Datenschutzaufsichtsbehörden und dem Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV) abgestimmten Datenweitergabeklausel in Versicherungsverträgen führen und unserer Hoffnung Ausdruck verliehen, dass diese in absehbarer Zeit erfolgreich abgeschlossen werden können. Ziel der Verhandlungen sollte es sein, die Einwilligungsklausel und die damit verbundenen Folgen für den Betroffenen transparenter zu gestalten. Eine Einigung war nicht möglich. Inzwischen bestehen aber auch andere Vorstellungen hinsichtlich des weiteren Vorgehens. Dies basiert auf der Erkenntnis, dass die Einwilligungsklausel, die derzeit im Versicherungsbereich verwendet wird, mit § 4 a Abs. 1 Satz 1 BDSG nicht vereinbar ist. Die Einwilligung beruht nämlich nicht auf der freien Entscheidung des Betroffenen. Der Betroffene hat praktisch keine andere Möglichkeit, als in die Erhebung, Verarbeitung und Nutzung seiner Daten einzuwilligen, weil die Versicherung andernfalls keinen Versicherungsvertrag mit ihm abschließen wird. So handelt aber auch jede andere Versicherung, sodass der Druck auf den Betroffenen noch erhöht wird (vergleiche dazu auch die in Nr. 3.1.1 zitierte Entscheidung des Bundesverfassungsgerichts). Die Erhebung, Verarbeitung und Nutzung der Daten sollte daher in diesem Bereich nicht auf die Einwilligung der Betroffenen, sondern nach Möglichkeit auf eine Vorschrift im Bundesdatenschutzgesetz gestützt werden. Soweit es eine solche nicht gibt, die Erhebung, Verarbeitung oder Nutzung der Daten jedoch zwingend erforderlich ist, sollte dafür eine Grundlage im Bundesdatenschutzgesetz oder im neuen Versicherungsvertragsgesetz, das sich im Gesetzgebungsverfahren befindet, geschaffen werden. Die Einwilligung des Betroffenen sollte nur noch dann Grundlage der Erhebung, Verarbeitung oder Nutzung der Daten sein, wenn die Entscheidung dem Betroffenen freigestellt ist.

Ob man sich auf dieser Basis mit der Versicherungswirtschaft verständigen kann, wird derzeit in Gesprächen mit dem GDV geklärt.

4.1.3 Hinweissystem der Versicherungswirtschaft (HIS, vormals „UNIWAGNIS“)

Die Datenschutzaufsichtsbehörden haben damit begonnen, sich erstmals seit langem wieder intensiver mit dem sogenannten Hinweis- und Informationssystems (HIS, früher UNIWAGNIS) zu informieren. Mithilfe dieses Systems wollen sich die Versicherungen zum einen vor Versicherungsbetrügern und -missbrauch schützen, zum anderen dient es der Risikoprüfung bei Vertragsabschluss. Die meisten Versicherungen sind an dieses System angeschlossen. In unserem dritten Tätigkeitsbericht hatten wir die Sparte der Rechtsschutzversicherer näher beleuchtet (C 4.6, S. 90 ff.). Außerdem gibt es die Sparten Kraftfahrzeug, Leben, Unfall, Sachversicherungen, Transport und Haftpflicht. HIS funktioniert folgendermaßen:

Die Versicherungen melden die relevanten Daten an den GDV. Eine Meldung erfolgt, wenn bestimmte, spartenspezifisch festgelegte, auf einen auffälligen Fall hinweisende Kriterien, die zum Teil mit bestimmten Punktewerten gewichtet werden, beziehungsweise eine bestimmte Punktzahl vorliegt. Von einer Meldung können nicht nur Versicherungsnehmer, sondern auch Personen betroffen sein, die einen (letztendlich abgelehnten) Antrag auf Abschluss eines Versicherungsvertrags gestellt haben, ferner Zeugen und Geschädigte eines Schadensfalls. Der GDV erfasst die Daten und verschlüsselt sie mithilfe eines phonetischen Codeverfahrens. Die ihm gelieferten Klardaten vernichtet er, einmal verschlüsselte Daten kann er nicht entschlüsseln. Der GDV leitet den angeschlossenen Versicherungen in regelmäßigen Abständen den verschlüsselten Gesamtdatenbestand zu. Er wird im Rahmen des HIS als Auftragsdatenverarbeiter für die meldenden Versicherungen tätig.

Insbesondere im Fall der Leistungsprüfung, in manchen Sparten aber auch vor Abschluss eines Versicherungsvertrags, durchsuchen Versicherungen spartenspezifisch den Datenbestand des HIS mithilfe einer Software, die sodann die phonetischen Treffer anzeigt. Das bedeutet, bei der Suche nach einer Person mit einem bestimmten Namen werden als Ergebnis alle Personen mit phonetisch gleich klingendem Namen als Treffer dargestellt, wobei zu einem Treffer auch die zugehörige Anschrift der gefundenen Person angezeigt wird. Über die einmeldende Versicherung, die ebenfalls mit Kontaktdaten zu einem Treffer angezeigt wird, kann sodann abgeklärt werden, ob es sich bei dem aufgeführten Treffer zweifelsfrei um die gesuchte Person handelt.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Rahmen des HIS wird auf einen Passus in der Einwilligungserklärung gestützt, die der Betroffene anlässlich der Antragstellung auf Abschluss eines Versicherungsantrags unterschreibt. Entsprechend der Klausel willigt er darin ein, dass der Versicherer im erforderlichen Umfang Daten, die sich aus den Antragsunterlagen oder der Vertragsdurchführung ergeben, zur Beurteilung des Risikos und der Ansprüche an andere Versicherer übermittelt.

Problematisch ist zum einen, dass der Betroffene anhand dieser Formulierung in keiner Weise überblicken kann, welche konkreten Datenübermittlungen in welchen Fällen erfolgen und welche Folgen sich dadurch für ihn ergeben können. Auch von der für eine Einwilligung erforderlichen Freiwilligkeit ist nicht auszugehen (siehe hierzu oben). Dritte haben zudem nicht in die Übermittlung ihrer Daten eingewilligt. HIS kann auch nicht auf eine gesetzliche Grundlage im Bundesdatenschutzgesetz gestützt werden, da die teilnehmenden Versicherungen in bestimmten Abständen alle vorhandenen Daten erhalten, unabhängig davon, ob sie die Daten zu einer betroffenen Person aktuell benötigen. Die übermittelten Daten sind zwar verschlüsselt, nach Ansicht der Aufsichtsbehörden aber eindeutig personenbeziehbar und damit personenbezogen. Der erforderliche Umfang einer zulässigen Datenübermittlung ist somit jedenfalls überschritten.

Die Arbeitsgruppe Versicherungswirtschaft des Düsseldorfer Kreises ist der Auffassung, dass eine datenschutzkonforme Umgestaltung des HIS erforderlich ist. Sie steht insoweit in Gesprächen mit dem GDV.

4.2 Nachträgliche Bonitätsabfragen wegen eines Rechtsstreits

Die Arbeitsgruppen Versicherungswirtschaft und Auskunfteien des Düsseldorfer Kreises haben sich wiederholt mit der Frage der datenschutzrechtlichen Zulässigkeit von Bonitätsabfragen durch Versicherungsunternehmen befasst. Da mit dem Abschluss eines Versicherungsvertrags in der Regel kein erhebliches finanzielles Ausfallrisiko verbunden ist, werden Bonitätsabfragen von Versicherungen bei Vertragsabschluss – mit Ausnahme bestimmter Einzelfälle – grundsätzlich als unzulässig angesehen.

In einem durch mehrere Eingaben Betroffener an uns herangetragenen Fall ging es jedoch vorrangig um etwas anderes: Ein Versicherungsunternehmen hatte in den Jahren 2005 und 2006 für mehrere hundert Personen Bonitätsabfragen durchgeführt. Das Versicherungsunternehmen wollte mit den Abfragen feststellen, ob die zu einem früheren Zeitpunkt – überwiegend 2004 – gestellten Versicherungsanträge wegen zu schlechter Bonität abgelehnt worden waren. Ziel war folglich die Rekonstruktion der bei Antragstellung erhobenen Daten. Die Datenerhebung und -übermittlung, die nach Ablehnung der Versicherungsanträge erfolgte, wurde gegenüber den Betroffenen und der Aufsichtsbehörde mit der Beweisführung in einer zivilrechtlichen Auseinandersetzung begründet.

Eine Auskunftei darf eine Bonitätsauskunft über eine Person nur erteilen, wenn der Anfragende ein bestimmtes berechtigtes Interesse glaubhaft dargelegt hat. Gegenüber der Auskunftei hatte die Versicherung zur Glaubhaftmachung des berechtigten Interesses an der Auskunft angegeben, dass die Anfrage vor beziehungsweise im Zusammenhang mit der Einleitung beziehungsweise Durchführung von Inkassomaßnahmen erfolge. Dies entsprach nicht den Tatsachen.

Die Prüfung hat ergeben, dass das Versicherungsunternehmen nicht berechtigt war, 2005 und 2006 Bonitätsabfragen zu den betroffenen Kunden durchzuführen. Zum einen war die Datenerhebung schon nicht geeignet, den von der Versicherung angegebenen Zweck – die Rekonstruktion von damals erhobenen Daten – zu erreichen, da sich die wirtschaftlichen Verhältnisse und damit auch die bei Auskunfteien gespeicherten Daten zwischen Versicherungsantrag und der im nachhinein vorgenommenen Bonitätsabfrage erheblich geändert haben können. Schon aus diesem Grund war die Datenerhebung zur Wahrung berechtigter Interessen der Versicherung nicht erforderlich.

Hinzu kommt: Nach Ablehnung ihrer Versicherungsverträge wurden die Daten der Betroffenen für eine weitere Nutzung gesperrt, da die Kenntnis der Daten für die Versicherung mangels Zustandekommens eines Versicherungsvertrags nicht mehr erforderlich war und einer Löschung gesetzliche Aufbewahrungsfristen entgegenstanden. Nach dem Bundesdatenschutzgesetz ist es jedoch zulässig, gesperrte Daten zur Behebung einer bestehenden Beweisnot zu verarbeiten. Auch deshalb waren die Bonitätsabfragen für den beabsichtigten Zweck nicht erforderlich und damit unzulässig. Die Datenerhebung war des Weiteren unzulässig, weil die Versicherung die Datenübermittlung durch die Auskunftei durch unrichtige Angaben erwirkt hat. Die Datenabfrage erfolgte nicht im Hinblick auf die Einleitung beziehungsweise Durchführung eines Inkassoverfahrens.

Wir haben die Versicherung auf die Sach- und Rechtslage hingewiesen, die Verletzung datenschutzrechtlicher Vorschriften beanstandet und uns weitere Schritte vorbehalten.

Die Überprüfung des Verhaltens der Auskunftei ist noch nicht abgeschlossen.

4.3 Bonitätsabfrage über einen Versicherungsvermittler

Ein ehemaliger Außendienstmitarbeiter einer Bausparkasse wandte sich an die Aufsichtsbehörde, weil sein Arbeitgeber während seiner Vertretertätigkeit eine Abfrage bei der SCHUFA durchgeführt hatte.

Im Falle von Anfragen bei Auskunfteien ist der Anfragende verpflichtet, ein berechtigtes Interesse an der Kenntnis der Daten darzulegen. Die Bausparkasse hatte gegenüber der SCHUFA als Grund beziehungsweise berechtigtes Interesse der Anfrage das Merkmal „Kreditanfrage“ angegeben. Der Betroffene hatte aber keinen Kredit beantragt. Die Bausparkasse hatte von dem Mitarbeiter bei dessen Ein-

stellung die Einwilligung dazu eingeholt, dass sie zusätzlich zu der von ihm vorgelegten SCHUFA-Selbstauskunft eine SCHUFA-Auskunft über seine Person einholen kann. Sie hat sich uns gegenüber auf diese Einwilligung berufen und mitgeteilt, sie sei aufgrund von „Mindestanforderungen zur Überprüfung der Beratungsqualität und der Sicherstellung der Zuverlässigkeit von Personen, die Bausparverträge vermitteln“, die aus einer Erklärung des Verbandes der Privaten Bausparkassen e. V. und der Bundesgeschäftsstelle Landesbausparkassen gegenüber dem damaligen Bundesaufsichtsamt für das Kreditwesen herrührten, zur sorgfältigen Auswahl von zuverlässigen Vermittlern und zu deren laufender Kontrolle verpflichtet. Da sie auch Provisionskonten führe, die Sollsalden zuließen, habe sie „Kreditanfrage“ als Grund für die SCHUFA-Abfrage angeben dürfen.

Bei SCHUFA-Abfragen mit dem Merkmal „Kreditanfrage“ erfolgt eine Beauskunftung im sogenannten A-Verfahren, bei dem die SCHUFA sowohl Auskünfte über nicht vertragsgemäßes als auch über vertragsgemäßes Verhalten übermittelt. Die SCHUFA selbst sieht aber Anfragen zu bestimmten Fällen von Vermittlungsprovisionsverträgen jedenfalls nur im B-Verfahren mit einer vom Umfang her beschränkten B-Auskunft vor. Letztere enthält ausschließlich Informationen über nicht-vertragsgemäßes Verhalten. Hierfür gibt es ein gesondertes Anfragemerkmal und eine vom Vermittler zu unterschreibende Einwilligungsklausel. Daher war jedenfalls die Nutzung des A-Verfahrens und die damit verbundene Datenerhebung unzulässig.

Es ist auch äußerst fraglich, ob Bausparkassen und Versicherungsunternehmen allein wegen der Möglichkeit, Rückzahlungsansprüche aus Provisionszahlungen nicht realisieren zu können, ein berechtigtes Interesse an Bonitätsauskünften über Vermittler zugebilligt werden kann. Auch die Bundesanstalt für Finanzdienstleistungsaufsicht hat die Einholung derartiger Auskünfte bei Auskunfteien nicht ausdrücklich gefordert.

Wir haben die Bausparkasse zudem darauf hingewiesen, dass wir die Forderung nach Vorlage einer SCHUFA-Eigenauskunft durch den Vermittler bei dessen Einstellung für unzulässig erachten. Hierdurch erlangt die Bausparkasse nämlich von wesentlich mehr Daten Kenntnis als bei der – in diesem Fall ebenfalls unzulässigen – Einholung von A-Auskünften. Wir haben die Bausparkasse gebeten, künftig auf die Vorlage einer Eigenauskunft zu verzichten.

4.4 Erhebung von Gesundheitsdaten für die Berufsunfähigkeitsversicherung

Soweit ein Versicherungsnehmer Leistungen aus seiner Berufsunfähigkeitsversicherung beantragt, prüft die Versicherung, ob sie hierzu verpflichtet ist. In einem an uns herangetragenen Fall war fraglich, ob eine Versicherung im Rahmen der Leistungsprüfung über den zulässigen Umfang hinaus Gesundheitsdaten erhoben hat. Die Betroffene hatte im Zusammenhang mit der Beantragung von Leistungen darin eingewilligt, dass die Versicherung zur Prüfung der Ansprüche alle Ärzte, Krankenhäuser und sonstige Krankenanstalten sowie Pflegeeinrichtungen und Pflegepersonen, bei denen sie in Behandlung war, über Ursache, Beginn, Art, Verlauf und voraussichtliche Dauer der Berufsunfähigkeit sowie über diejenigen Krankheiten, die zur Berufsunfähigkeit geführt haben, befragen kann. Sie hatte diese Stellen insoweit von der Schweigepflicht entbunden.

Die Versicherung wandte sich sodann an den Hausarzt der Betroffenen, den diese im Versicherungsantrag angegeben hatte. In einem Formularschreiben bat sie diesen um einen ärztlichen Bericht über die Betroffene, um Übersendung sämtlicher vorhandener Unterlagen und Berichte über die Betroffene zur Einsichtnahme und um Beantwortung eines Fragebogens, der insbesondere Fragen zu bislang behandelten Krankheiten enthielt. Der Anforderung („sämtliche Unterlagen“) entsprechend übersandte der Arzt der Versicherung unter anderem einen von der Betroffenen ausgefüllten Wartezimmer-Fragebogen, den diese rund zehn Jahre zuvor ausgefüllt hatte. Darin hatte sie umfassend Auskunft zu Gesundheitszustand, zu ihren bisherigen Erkrankungen und zu deren Auswirkungen auf den Tagesablauf, zu Stimmungen, Beschwerden, Allergien, Krankheiten in der Familie, Trink-, Ernährungs- und Schlafgewohnheiten, zur psychischen Verfassung und zur Bewertung ihrer Sexualität und ihrer Beziehungen zu anderen Personen erteilt. Die Versicherung trat aufgrund einiger Angaben, die die Betroffene im Fragebogen, nicht jedoch im Versicherungsantrag gemacht hatte, vom Vertrag

zurück und focht diesen zusätzlich an. Wir teilten der Versicherung mit, dass wir Bedenken hätten, ob hinsichtlich der Einwilligungserklärung und Schweigepflichtentbindungserklärung eine zulässige Datenerhebung der Versicherung vorlag.

Bei der Datenerhebung durch die Versicherung ist zu beachten, dass diese nur solche Daten umfassen darf, hinsichtlich derer die Entbindung des Versicherten von der Schweigepflicht vorliegt. Erhebungs- und Übermittlungsbefugnis (durch den Arzt) korrespondieren insoweit. Diesen Maßstab muss eine Versicherung auch anlegen, wenn sie Daten bei einem Arzt anfordert.

Das von der Versicherung verwendete Anforderungsformular haben wir als zu weit gehend angesehen, da es pauschal alle bei einem Arzt vorliegenden Gesundheitsdaten erfasst, unabhängig davon, ob diese mit der geltend gemachten Berufsunfähigkeit überhaupt in Verbindung stehen können und wann sie entstanden sind. Die Zulässigkeit der Datenerhebung konnte die Versicherung auch nicht auf die von der Betroffenen im Versicherungsantrag erteilten Entbindung von der Schweigepflicht stützen. Diese bezieht sich auf Angaben über die Gesundheitsverhältnisse des Versicherten bei Vertragsabschluss. Das Schreiben der Versicherung an den Arzt enthielt keinerlei zeitliche Konkretisierung hinsichtlich der angeforderten Daten, Unterlagen und Berichte. So stammt der übermittelte Fragebogen, der auch viele Fragen zum „augenblicklichen“ Gesundheitszustand enthielt, aus einer Zeit, die rund fünf Jahre vor Abschluss des Versicherungsvertrags lag.

Wir haben die Versicherung um Überarbeitung des Musteranfrageschreibens gebeten. Dies hat sie zugesagt und erste Vorschläge erarbeitet.

Im konkreten Beschwerdefall konnte der Betroffenen insoweit weitergeholfen werden, als sich die Versicherung bereit erklärte, den Fragebogen zu vernichten und die weitere Regulierung ohne dessen Berücksichtigung vorzunehmen.

4.5 Anforderung von Krankenhausentlassungsberichten

Private Krankenversicherungen sind nach dem Versicherungsvertragsgesetz berechtigt, zur Prüfung ihrer Leistungsverpflichtung die Vorlage von Arztrechnungen und anderen erforderlichen Nachweisen zu fordern. Dabei müssen allerdings die Grundsätze der Datenvermeidung und Datensparsamkeit beachtet werden. Das Versicherungsunternehmen darf daher nur in dem Umfang Daten erheben, wie sie zur Feststellung der Leistungspflicht notwendig sind.

Der Krankenhausentlassungsbericht enthält viele nach dem Bundesdatenschutzgesetz besonders geschützte sensible Gesundheitsdaten, die für die Leistungsentscheidung der Krankenversicherung nicht entscheidungsrelevant sind, zum Beispiel Informationen über den Therapieverlauf und Behandlungshinweise für den Hausarzt. Deshalb sollen Krankenhausentlassungsberichte nur angefordert werden, wenn sie vollumfänglich erforderlich sind. Dies sieht auch ein zwischen Vertretern des Verbands der Privaten Krankenversicherung e. V. (PKV) und den obersten Datenschutzaufsichtsbehörden abgestimmtes Verfahren vor. In den meisten Fällen kann durch eine einzelfallbezogene konkrete Anfrage beim Arzt die Leistungsverpflichtung geklärt werden.

In einem Beschwerdeverfahren hat ein Versicherungsunternehmen zur Feststellung, ob der Leistungsausschlussgrund „Durchführung von Entziehungsmaßnahmen beziehungsweise einer Entziehungskur“ besteht, einen Befund- und Entlassungsbericht angefordert. Unsere Prüfung um die wir nach Anerkennung des Leistungsverpflichtung gebeten wurden, hat ergeben, dass es in diesem Fall ausreichend gewesen wäre, die Versicherte aufzufordern, eine Bescheinigung des Krankenhauses über den Grund der stationären Behandlung vorzulegen.

Wir haben die Versicherung gebeten, durch eine Änderung des Verfahrens sicherzustellen, dass nur die Daten erhoben werden, die zur Prüfung der Leistungspflicht erforderlich sind. Das Unternehmen hat in der Zwischenzeit mitgeteilt, dass künftig bei der Anforderung medizinischer Unterlagen der medizinische Dienst mitwirkt.

5 Kreditwirtschaft

5.1 Swift-Verfahren – Übermittlung personenbezogener Bankdaten in die USA

Der internationale Zahlungsverkehr wird von den Banken und Kreditinstituten in Deutschland unter Einschaltung von Rechenzentren des belgischen Unternehmens SWIFT (Society for Worldwide Interbank Financial Telecommunications) abgewickelt. Bei SWIFT handelt es sich um einen weltweit tätigen Bankendienstleister, welcher den Finanzverkehr von circa 7.800 Geldinstituten in mehr als 200 Ländern abwickelt. Nach den zur Verfügung stehenden Informationen handelt es sich um ein auf dem fraglichen Geschäftsfeld konkurrenzloses Unternehmen. SWIFT speichert für Zwecke der Datensicherung den gesamten Datenbestand der durchgeführten Transaktionen in zwei Rechenzentren. Ein Rechenzentrum befindet sich in den Niederlanden, das andere in den USA. Deshalb sind nicht nur Überweisungen in die USA, sondern auch sämtliche Daten innereuropäischer Überweisungen bei SWIFT im Rechenzentrum in den USA gespeichert.

Mitte 2006 wurde festgestellt, dass US-amerikanische Behörden seit den Terroranschlägen am 11. September 2001 aufgrund einer Anweisung des US-Finanzministeriums das internationale Datennetz SWIFT über das SWIFT-Rechenzentrum in den USA überwachen. Den US-Behörden wird der gesamte Datenbestand ungefiltert zur Verfügung gestellt.

Die gegenwärtige Spiegelung von Datensätzen im SWIFT-Rechenzentrum in den USA und die anschließende Herausgabe von dort gespeicherten Daten an US-amerikanische Behörden ist sowohl nach deutschem als auch nach EG-Datenschutzrecht wegen fehlender Rechtsgrundlage unzulässig. Insbesondere verfügen die USA über kein angemessenes Datenschutzniveau nach § 4 b BDSG beziehungsweise im Sinne des Art. 25 Abs. 1 und 2 der EG-Datenschutzrichtlinie. Rechtlich verantwortlich für die Übermittlung der Daten in die USA sind sowohl die in Belgien ansässige SWIFT als auch die deutschen Banken, die sich trotz des Zugriffs der US-amerikanischen Behörden auf die im SWIFT-Rechenzentrum in den USA gespeicherten Datensätze auch weiterhin der Dienstleistungen von SWIFT bedienen.

Der Düsseldorfer Kreis hat in seiner Sitzung am 8./9. November 2006 die Banken aufgefordert, unverzüglich Maßnahmen vorzuschlagen, durch die im SWIFT-Verfahren entweder eine Übermittlung von Daten in die USA unterbunden werden kann oder aber zumindest die übermittelten Datensätze hinreichend gesichert werden, damit der bislang mögliche Zugriff der US-amerikanischen Sicherheitsbehörden künftig ausgeschlossen ist. Die Datenschutzgruppe nach Art. 29 der EG-Datenschutzrichtlinie hat ein entsprechendes Papier beschlossen. Nach den der Aufsichtsbehörde derzeit vorliegenden Informationen plant SWIFT zusätzliche Rechenzentren in Europa. Für innereuropäische Transaktionen sollen künftig ausschließlich europäischen Rechenzentren genutzt werden. Entsprechende Zahlungsdaten sollen damit nicht mehr in die USA übermittelt werden.

Unabhängig davon müssen die deutschen Banken ihrer Unterrichtungspflicht nach § 4 Abs. 3 BDSG genügen. Sie müssen ihre Kunden darüber informieren, dass im Falle der Weiterleitung von grenzüberschreitenden Zahlungsaufträgen die Datensätze derzeit auch an ein in den USA ansässiges SWIFT Operating Center übermittelt werden. Die in Baden-Württemberg ansässigen Banken und Kreditinstitute wurden über ihre Verbände entsprechend unterrichtet.

Die Aufsichtsbehörde hat die Umsetzung dieser Vorschrift in der Praxis überprüft. Sie hat dabei festgestellt, dass einige Banken ihre Kunden bei der Erteilung des Überweisungsauftrags unterrichten und damit korrekt verfahren. Andere Banken halten entsprechende Informationen für „interessierte“ Kunden bereit, zum Beispiel im Internet, ohne dass sie hierauf im Zusammenhang mit der Überweisung besonders hinweisen. Diese Art der Unterrichtung reicht nicht aus. Die Aufsichtsbehörde wird deshalb diese Banken, soweit sie ihren Sitz in Baden-Württemberg haben, auffordern, ihre Verfahrensweise zu ändern.

SWIFT ist für deutsche Banken auch im nationalen Zahlungsverkehr bei Eilüberweisungen tätig. Da diese Daten ebenfalls in die USA und gegebenenfalls an US-amerikanische Behörden übermittelt werden, müssen auch diese Kunden zumindest gesetzeskonform unterrichtet werden.

5.2 Verwendung von Kundendaten für Zwecke der Werbung

Banken dürfen Kundendaten dafür verwenden, für bankeigene Produkte zu werben. Bei der Erhebung der Daten, zum Beispiel bei der Eröffnung eines Kontos, muss der Kunde allerdings über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung unterrichtet werden (siehe oben B). Beabsichtigt ein Unternehmen, die personenbezogenen Daten erst nach der Erhebung für Werbezwecke zu verwenden, muss der Kunde nachträglich unterrichtet werden, weil er mit einer solchen Datenverwendung wegen der fehlenden Information bei Beginn der Vertragsbeziehungen nicht rechnen muss. Für telefonische Werbung ist immer die Einwilligung des Kunden erforderlich.

An die Aufsichtsbehörde wurden mehrere Fälle herangetragen, in denen Banken die gespeicherten Kundendaten ohne Kenntnis der Betroffenen ausgewertet und zu Werbezwecken – teilweise auch für andere (Partner-)Unternehmen – verwendet haben. Die Betroffenen wurden dabei weder jemals darüber unterrichtet, dass ihre Daten zu Werbezwecken genutzt oder übermittelt werden sollen, noch wurden sie auf die Möglichkeit des Widerspruchs gegen die Nutzung beziehungsweise Übermittlung der Daten für Werbezwecke hingewiesen.

In einem Fall erhielt eine Kundin einen Werbebrief ihrer Bank mit einem vorbereiteten Antrag für den Abschluss einer Pflegeversicherung bei einer Versicherungsgesellschaft. In dem Antrag waren außer Namen und Anschrift auch das Geburtsdatum, die Bankverbindung und die tarifabhängige Beitragshöhe eingetragen. Die Prüfung hat Folgendes ergeben:

Die Bank hat für diese Werbeaktion eines externen Unternehmens die gespeicherten Kundendaten nach mehreren Kriterien ausgeweitet und zur Datenanreicherung an ein anderes Unternehmen übermittelt. Für den Druck und Versand der dort erstellten Informationsunterlagen wurden die Kundendaten an eine weitere Firma übergeben. Mit der Nutzung der Kundendaten für diese Werbeaktion und der Datenübermittlung erfolgte eine unberechtigte Verarbeitung von Kundendaten, weil sie ohne Rechtsgrundlage und ohne Einwilligung des Kunden erfolgt ist.

Wegen der gravierenden Verletzung datenschutzrechtlicher Bestimmungen und des Bankgeheimnisses wurde die Vorgehensweise beanstandet und die Bank aufgefordert, künftig eine gesetzeskonforme Datenverarbeitung sicherzustellen.

5.3 Adressenbekanntgabe im Lastschrifteinzugverfahren

Der Inhaber eines Girokontos hatte Ware beim Kauf mit EC-Karte bezahlt. Die Lastschrift wurde eingelöst. Einige Monate später bat das Handelsgeschäft die Bank, ihr wegen Ansprüchen gegen den Kunden die Anschrift des Kontoinhabers mitzuteilen. Die Bank entsprach dieser Bitte.

Eine Bank darf die Adresse eines Kontoinhabers nur mit dessen schriftlicher Einwilligung an Dritte übermitteln. Sowohl nach den im Bankenbereich geltenden Bedingungen für das bargeldlose Bezahlen ohne Zahlungsgarantie durch Lastschrift (POZ) als auch nach der im Handel üblichen Einwilligung im Lastschriftverfahren ist zwingende Voraussetzung für eine Adressenbekanntgabe, dass die Lastschrift nicht eingelöst oder Widerspruch gegen die Lastschrift erhoben wurde.

Die Nachprüfung ergab, dass aufgrund eines Bearbeitungsfehlers nicht geprüft wurde, ob die Lastschrift eingelöst wurde. Die Bank hat daraufhin umgehend ihre Arbeitsanweisung geändert, um künftig sicherzustellen, dass eine Datenübermittlung nur noch erfolgt, wenn eine wirksame Entbindung vom Bankgeheimnis vorliegt.

5.4 Unberechtigte Datenübermittlung durch fehlerhafte Adressierung

Die SCHUFA informiert ihre Vertragspartner, zum Beispiel Kreditinstitute, durch eine sogenannte Nachmeldung auch über eine ihr mitgeteilte Änderung der Anschrift eines Betroffenen. Die Empfänger einer Nachmeldung sind verpflichtet, vor der Übernahme zu prüfen, ob die Adressänderung richtig ist. Aufgrund einer unzureichenden Plausibilitätsprüfung hat ein Kreditinstitut Name und Anschrift eines Bankkunden geändert mit der Folge, dass unter anderem Kontoauszüge un-

ter Verletzung von BDSG-Vorschriften sowie des Bankgeheimnisses unberechtigt an Dritte übermittelt wurden.

Die Vorgehensweise wurde beanstandet. Das Kreditinstitut wurde aufgefordert, unverzüglich das Verfahren beziehungsweise die Arbeitsanweisung dahin gehend zu ändern, dass vor der Übernahme der Adressänderung eine sorgfältige Prüfung erfolgt, die sicherstellt, dass keine falsche Adresse übernommen wird. Dies ist inzwischen geschehen.

5.5 Weiterleitung von Bankverbindungsdaten des Überweisenden an den Begünstigten

Zwischen den Aufsichtsbehörden und dem Zentralen Kreditausschuss (ZKA) ist umstritten, ob es zulässig ist, die Bankverbindungsdaten des Überweisenden auf den Kontoauszügen des Zahlungsempfängers mitzuteilen. Es handelt sich hierbei um eine Datenübermittlung, deren Zulässigkeit sich nach § 28 BDSG beurteilt.

Der ZKA vertritt die Ansicht, die Übermittlung von Kontonummer und Bankleitzahl des Überweisenden an den Zahlungsempfänger sei im beleglosen Zahlungsverkehr zulässig. Er beruft sich darauf, dass diese Daten gerade im gewerblichen Geschäftsverkehr eine hohe Bedeutung hätten, da sie von Unternehmen für eine weitgehend automatisierte Kundenbuchhaltung benötigt würden, um Zahlungen eindeutig und korrekt zuordnen und verbuchen zu können. Bei Zahlungen im Rahmen von Dauerschuldverhältnissen bestünden auch keine besonderen Geheimhaltungsbedürfnisse der Zahlenden gegenüber den Empfängern. Gemeinnützige Organisationen hätten außerdem ein erhebliches Interesse an den Daten, da sie verpflichtet seien, zweckgebundene Spenden zurück zu überweisen, wenn der Spendenzweck erfüllt sei. Bei der Abwicklung von Rückzahlungen oder der Auszahlung von Gewinnen liege die Kenntnis der Bankverbindungsdaten im Interesse des Zahlenden.

Nach Auffassung der Aufsichtsbehörden ist diese Übermittlung hingegen grundsätzlich unzulässig. Sie ist weder durch die Zweckbestimmung des Vertrags nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG gedeckt noch nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich. Zur Ausführung des Überweisungsauftrags ist es nicht erforderlich, dem Überweisungsempfänger Kontonummer und Bankleitzahl des Einzahlers zur Kenntnis zu bringen. Auch § 676 a Abs. 1 und § 676 f Satz 2 des Bürgerlichen Gesetzbuchs (BGB) sehen eine Übermittlung der Bankverbindung der überweisenden Person nicht vor.

Die Kenntnis dieser Daten ist grundsätzlich auch nicht zur Wahrung berechtigter Interessen des Empfängers erforderlich (§ 28 Abs. 3 Satz 1 Nr. 1 BDSG). Für den Empfänger ist es ausreichend, wenn Name des Einzahlers, angegebener Verwendungszweck sowie die Höhe des Betrags auf seinem Kontoauszug ausgewiesen sind, um die Zahlung zuordnen zu können. Außerdem besteht im Fall der Übermittlung der Bankverbindungsdaten Grund zu der Annahme, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. Viele Überweisende möchten gerade nicht, dass der Überweisungsempfänger mit Hilfe ihrer Bankverbindungsdaten Kontakt zu Ihnen aufnehmen kann.

Auch nach Ansicht der Aufsichtsbehörden kann allerdings im Einzelfall eine Berechtigung zur Übermittlung vorliegen, nicht aber bei pauschal vorgenommenen Massenübermittlungen.

5.6 Auswertung von Kreditkarten- und Abrechnungsunterlagen zur Ermittlung der Nutzer eines kinderpornographischen Internetportals (Operation „Mikado“)

Die Staatsanwaltschaft Halle hat im Juli und August 2006 in einem Ermittlungsverfahren wegen des Verdachts der Verbreitung sowie des Erwerbs und Besitzes von kinderpornografischen Schriften die mit der Verarbeitung von Kreditkartendaten beauftragten Unternehmen bundesweit darum gebeten, die Konten von Kreditkartenbesitzern nach bestimmten Kriterien zu durchsuchen und ihr im Trefferfall die erbetenen Informationen zu den Karteninhabern zu übermitteln. In dem Schreiben der Staatsanwaltschaft hieß es dazu unter anderem:

„... in dem oben genannten Ermittlungsverfahren benötigt die Staatsanwaltschaft Halle Beweismaterial, das zur Namenhaftmachung der bislang unbekannten Nutzer des oben genanten Internet-Portals führt ...

Zur Vermeidung einer zeugenschaftlichen Vernehmung des zuständigen Mitarbeiters Ihres Hauses gemäß § 161 a StPO bitte ich, folgende Frage zu beantworten ..."

Grundlage für das staatsanwaltschaftliche Ermittlungsverfahren gegen „Unbekannt" war das Angebot von kinderpornographischem Material (Fotos und Videos) im Internet. Den Zugang hierzu konnte sich der Nutzer durch Zahlung eines Geldbetrags in Höhe von 79,99 $ (für 20 Tage) per Kreditkarte erkaufen. Um mögliche Nutzer des Angebots zu ermitteln, wurden die oben genannten Unternehmen unter Angabe des Zahlungszeitraums, des Überweisungsbetrags, der Umsatzbeschreibung, der Merchant-ID (darunter versteht man eine dem Zahlungsempfänger durch die Bank zugewiesene Ziffernfolge) und der Händlerbank gebeten, zu recherchieren, welche Kreditkartenkonten einen entsprechenden Geldtransfer aufweisen. Die Unternehmen werteten die gespeicherten Kundendaten aus – insgesamt soll es sich um die Daten von 22 Millionen Kreditkarteninhabern gehandelt haben – und teilten der Staatsanwaltschaft die erbetenen Informationen zu den Kreditkartenkonten und Karteninhabern mit.

Bei der Aufsichtsbehörde haben sich mehrere Personen darüber beschwert, dass ihre Daten aufgrund des Auskunftsersuchens der Staatsanwaltschaft Halle in die Untersuchung einbezogen worden waren. In keinem Fall waren Daten an die Staatsanwaltschaft Halle übermittelt worden. Der Aufsichtsbehörde für den Datenschutz obliegt die Bewertung, ob die Recherche – datenschutzrechtlich handelt es sich um eine Nutzung gespeicherter Daten – durch die datenschutzrechtlich verantwortlichen Kreditkartenunternehmen, die ihren Sitz in Baden-Württemberg haben, beziehungsweise durch die mit der Datenverarbeitung beauftragten Unternehmen (im Folgenden „Auftragsdatenverarbeiter") datenschutzrechtlich zulässig war.

Die Prüfung, ob das Auskunftsersuchen der Staatsanwaltschaft Halle zulässig war, obliegt der Justiz in Sachsen-Anhalt. Das Amtsgericht Halle – Saalkreis hat auf Antrag eines von dem Auskunftsersuchen Betroffenen die Zulässigkeit der Maßnahme der Staatsanwaltschaft gerichtlich überprüft und mit Beschluss vom 11. März 2007 festgestellt, dass die Datenabfrage der Staatsanwaltschaft bei den bundesdeutschen Kreditkarten- und Abrechnungsunternehmen im Rahmen des Ermittlungsverfahrens zulässig war. Diese Entscheidung ist noch nicht rechtskräftig.

Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt hat die Datenerhebung der Staatsanwaltschaft ebenfalls als zulässig angesehen.

Unsere – noch nicht abgeschlossene – Prüfung hat in tatsächlicher Hinsicht ergeben, dass die Staatsanwaltschaft stets die von den Kreditkartenunternehmen mit der Datenverarbeitung beauftragten Unternehmen um Auskunft ersucht hat. Ein Auftragsdatenverarbeiter hat die Staatsanwaltschaft gebeten, sich mit ihrem Auskunftsersuchen an das Kreditkartenunternehmen (Auftraggeber) zu wenden. Er hat das Auskunftsersuchen der Staatsanwaltschaft erst nach entsprechender Weisung seines Auftraggebers bearbeitet. Ansonsten erfolgte die Auswertung und – im Trefferfall – Übermittlung der gespeicherten Kreditkartendaten jeweils durch den Auftragsdatenverarbeiter, ohne den Auftraggeber zu konsultieren.

Datenschutzrechtlich zulässig war die Nutzung der gespeicherten Daten, soweit sie „zur Verfolgung von Straftaten" erforderlich war und kein Grund zu der Annahme bestand, dass die Betroffenen ein schutzwürdiges Interesse am Ausschluss der Nutzung haben (§ 28 Abs. 3 Satz 1 Nr. 2 BDSG). Das Herunterladen kinderpornographischer Schriften aus dem Internet stellt nach § 184 b Abs. 4 des Strafgesetzbuchs eine strafbare Handlung dar. Mit der Bezahlung des Betrags für den Zugang zu der Internet-Seite an den Anbieter war der Straftatbestand erfüllt. Zweifelhaft könnte jedoch sein, ob bereits unmittelbar vor Beginn der Datennutzung wegen einer „Straftat" eines Inhabers einer deutschen Kreditkarte ermittelt wurde. Schließlich gab es keine konkreten Anhaltspunkte dafür, dass die fragliche Internet-Seite von Inhabern deutscher Kreditkarten aufgesucht und die strafbaren Inhalte von ihnen gegen Bezahlung heruntergeladen worden waren. Damit stellt sich die Frage, ob ein Anfangsverdacht einer Straftat vorlag, der auch im Rahmen

des § 28 Abs. 3 Satz 1 Nr. 2 BDSG genügen dürfte, oder ob „ins Blaue hinein“ ermittelt wurde und die erforderlichen tatsächlichen Anhaltspunkte für eine Straftat erst auf dem Wege der „Durchsuchung“ der Datenbestände geschaffen werden sollte.

Diese Frage ist identisch mit der Frage nach der Zulässigkeit der Maßnahme der Staatsanwaltschaft Halle. Auch dafür ist maßgeblich, ob ein Anfangsverdacht für eine Straftat eines Besitzers einer deutschen Kreditkarte vorlag. Das Amtsgericht Halle – Saalkreis hat diese Frage im Ergebnis bejaht. Die Staatsanwaltschaft Halle habe annehmen dürfen, dass sich unter den Datennutzern mit aller Wahrscheinlichkeit auch Inhaber deutscher Kreditkarten befinden. Sie habe sich insoweit zu Recht auf die kriminalistische Erfahrung, insbesondere auf die Erkenntnisse aus anderen Verfahren, berufen.

Es liegt nahe, diese Beurteilung auch auf die von der Aufsichtsbehörde zu beantwortende Frage zu übertragen, ob die Datennutzung „zur Verfolgung von Straftaten“ erforderlich war. Da gegen die Entscheidung des Amtsgerichts jedoch Rechtmittel eingelegt ist, hat die Aufsichtsbehörde ihre datenschutzrechtliche Beurteilung zurückgestellt, bis über die Zulässigkeit der Maßnahme der Staatsanwaltschaft rechtskräftig entschieden ist. Sollte sie endgültig bejaht werden, dürften auch gegen die Datennutzung durch die Kreditkartenunternehmen keine durchgreifenden datenschutzrechtlichen Bedenken bestehen.

Die Operation „Mikado“ hat uns jedoch noch auf ein weiteres Problem aufmerksam gemacht: Die datenschutzrechtlich verantwortlichen Kreditkartenunternehmen haben die Datenverarbeitung an Auftragsdatenverarbeiter übertragen. Die betrieblichen Datenschutzbeauftragten der Kreditkartenunternehmen hatten hiervon jedoch durchweg keine Kenntnis. Einem Kreditkartenunternehmen lag noch nicht einmal der vom Verband mit dem Auftragsdatenverarbeiter abgeschlossene Vertrag vor. Er konnte daher der Aufsichtsbehörde auch nicht die Frage beantworten, welche Aufgaben auf die Auftragsdatenverarbeiter übertragen und welche konkreten Festlegungen für die Datenverarbeitung getroffen wurden und ob sowie gegebenenfalls von wem die Einhaltung der datenschutzrechtlichen Vorschriften bei den Auftragsdatenverarbeitern kontrolliert wird.

Es verwundert daher nicht, dass die meisten Auftragsdatenverarbeiter ihre Auftraggeber nicht konsultierten, als sie das Auskunftsersuchen der Staatsanwaltschaft auf den Tisch bekamen beziehungsweise bevor sie den Datenbestand ihres Auftraggebers nutzten und daraus in Einzelfällen Daten an die Staatsanwaltschaft übermittelten. Es bestehen erhebliche Zweifel, ob dies noch mit § 11 BDSG in Einklang steht, nach dem der Auftragsdatenverarbeiter die Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten oder nutzen darf. Immerhin wird daraus hergeleitet, dass es dem Auftragsdatenverarbeiter verboten ist, ohne ausdrückliche Autorisierung durch den Auftraggeber Daten zu übermitteln oder für andere Auftraggeber zu nutzen. Dies dürfte selbst dann gelten, wenn eine Staatsanwaltschaft um Auskunft ersucht. Im vorliegenden Fall kommt hinzu, dass sich die Staatsanwaltschaft – entgegen dem Verständnis einiger ersuchter Stellen – nicht auf eine zur Auskunft verpflichtende Vorschrift gestützt hat. Grundlage für ihr Ersuchen war § 161 und nicht § 161 a StPO.

Die Aufsichtsbehörde wird die das Verhältnis zwischen Kreditkartenunternehmen und Auftragdatenverarbeitern berührenden Fragen unabhängig vom Anlassfall weiterverfolgen.

6 Werbung, Adresshandel, Glücksspiele

Die Zahl der Beschwerden im Bereich Werbung, Adresshandel und Lotterien ist im Berichtszeitraum weiter gestiegen. Sie beziehen sich nur noch zu einem geringen Teil auf die herkömmliche Direktwerbung. Daraus den Schluss zu ziehen, die Datenschutzvorschriften würden hier weitgehend beachtet, wäre jedoch falsch. Stichproben zeigen, dass nach wie vor viele Unternehmen Werbung betreiben, ohne den Betroffenen bei der Erhebung der Daten über eine derartige Nutzung unterrichtet zu haben oder auf die Möglichkeit des Werbewiderspruchs hinzuweisen (vergleiche dazu auch oben B).

Nach wie vor erhalten wir auch Beschwerden wegen Haushaltsbefragungen, bei denen die Betroffenen mehrseitige Fragebögen zugesandt bekommen. Daten-

schutzrechtlich ist gegen sie nichts einzuwenden, weil die Betroffenen auf die Freiwilligkeit ihrer Angaben hingewiesen werden und ihre Einwilligung in die Datenverarbeitung eingeholt wird. Die Beschwerden zeigen, dass mancher meint, die Datenschutzvorschriften setzten solche Befragungen engere Grenzen als das tatsächlich der Fall ist. Auch hat die Aufsichtsbehörde keine Möglichkeit, eine andere Gestaltung solcher Fragebögen durchzusetzen, wenn die rechtlichen Grenzen beachtet sind.

Zugenommen haben Beschwerden wegen Telefon- und E-Mail-Werbung, unter anderem in Form regelmäßig versandter Newsletter. Häufig haben die Betroffenen zunächst versucht, die werbenden Unternehmen zur Löschung ihrer Daten zu veranlassen, jedoch darauf keine Antwort erhalten. Offensichtlich werden die Datenschutzaufsichtsbehörden in solchen Fällen als weitere Anlaufstellen neben den Verbraucherzentralen angesehen.

Ein Teil der Beschwerden, vor allem im Jahre 2005, bezog sich auf unerlaubte Anrufe von Lotterien.

6.1 Telefon- und E-Mail-Werbung

Werbende Unternehmen nutzen in immer größerem Umfang die Möglichkeiten der elektronischen Kommunikation. Bei Telefonwerbung erfolgten die Anrufe zumeist durch Call-Center. Erhoben werden Telefonnummer und E-Mail-Adresse häufig im Zusammenhang mit einem Vertragsabschluss, der Anforderung von Unterlagen durch einen Betroffenen oder bei Gewinnspielen. Viele Unternehmen greifen auch auf die Datenbestände von Adresshändlern zurück.

§ 7 Abs. 2 des Gesetzes gegen den unlauteren Wettbewerb (UWG) setzt einer Kontaktaufnahme per Telefon oder E-Mail jedoch Grenzen:

- Der „Verbraucher“ darf ohne seine Einwilligung nicht telefonisch beworben werden.
- Werbung per E-Mail ist ohne Einwilligung des „Adressaten“ ebenfalls unzulässig.

Dies gilt jedoch dann nicht, wenn

- ein Unternehmen im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten hat,
- das Unternehmen die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet,
- der Kunde der Verwendung nicht widersprochen hat und
- der Kunde bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann.

§ 7 Abs. 2 UWG ist keine datenschutzrechtliche Vorschrift. Sie bezweckt allein den Verbraucherschutz. Sie will den Verbraucher vor den Belästigungen schützen, die mit einer Telefon- und E-Mail-Werbung verbunden sind. Das Recht auf informationelle Selbstbestimmung, das dem Einzelnen zugesteht, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten bestimmen zu können, wird durch das Bundesdatenschutzgesetz geschützt. Das Gesetz gegen den unlauteren Wettbewerb und das Bundesdatenschutzgesetz stehen daher nebeneinander. Eine wettbewerbswidrige Nutzung der Telefonnummer und der E-Mail-Adresse ist immer auch datenschutzrechtlich unzulässig, weil sie mangels legitimer Zweckbestimmungen nicht durch § 28 BDSG gedeckt ist. Das Nebeneinander des Gesetzes gegen den unlauteren Wettbewerb und des Bundesdatenschutzgesetzes hat – wie auch der Düsseldorfer Kreis festgestellt hat – zur Folge, dass die *Einwilligung in die Nutzung der Telefonnummer und der E-Mail-Adresse unter Beachtung des § 4 a BDSG erfolgen muss*. Die Einwilligung bedarf daher der Schriftform, sofern nicht „wegen besonderer Umstände eine andere Form angemessen ist“. Eine „andere Form“ ist eine ausdrücklich mündliche, nicht jedoch eine stillschweigende oder konkludente Einwilligung.

Gegen diese Vorschriften wird häufig verstoßen. Immer wieder wird eine Einwilligung bereits dann angenommen, wenn der Betroffene (Kunde/Teilnehmer) seine

Telefonnummer und/oder seine E-Mail-Adresse in ein Formular einträgt und zwar selbst dann, wenn hinter der vorgedruckten „Telefonnummer“ ein Klammerzusatz wie zum Beispiel „für Gewinnbenachrichtigung“ oder „für Rückfragen“ angebracht ist und über die beabsichtigte Nutzung für Werbezwecke nicht weiter informiert wird. Die Vorschriften werden auch dadurch umgangen, dass Unternehmen Betroffene anrufen, um dann während des Telefonats die Einwilligung in die Telefonwerbung einzuholen. Mitunter steht am Beginn eines solchen Telefonats eine – vorgeschobene – Markt- oder Meinungsumfrage.

Erkundigt sich die Aufsichtsbehörde bei Unternehmen nach der Einwilligungserklärung, wird von diesen häufig erklärt, die Daten stammten von einem Adresshändler, der versichert habe, es handle sich um Daten mit einem „Opt-In“. Nachgeprüft habe man dies jedoch nicht. Der Bitte nach Vorlage des Originalbelegs mit der Einwilligung des Betroffenen kann in solchen Fällen zumeist nicht entsprochen werden, sei es, dass der Ursprung der Einwilligung nicht mehr festgestellt werden kann oder ein Beleg nicht existiert. Mitunter besteht der Beleg auch darin, dass Call-Center-Mitarbeiter hinter den Namen angeblich angerufener Personen ein Kreuz setzen.

Angesichts dieses „Wildwuchses“ besteht Veranlassung auf Folgendes hinzuweisen:

– Die Einwilligung in die Telefon- und E-Mail-Werbung muss, auch wenn sie vorformuliert ist, als eigene Erklärung des Betroffenen ausgestaltet sein („ich willige ein, dass ...“), ein bloßer Hinweis darauf, was mit den Daten geschieht oder eine Kenntnisnahme des Betroffenen („mir ist bekannt, dass ...“) genügen nicht. Es muss in *Werbung* per Telefon und/oder per E-Mail eingewilligt werden. Die Einwilligungserklärung muss, wenn sie zusammen mit anderen Erklärungen abgegeben wird, *grafisch besonders hervorgehoben und entsprechend platziert sein*. Sie darf nicht in den Allgemeinen Geschäftsbedingungen oder Fußzeilen versteckt sein. Sie muss *eigenhändig unterschrieben* sein (§ 126 Abs. 2 BGB), was häufig nicht der Fall ist, und sollte aus Beweisgründen ein Datum tragen. *Datenschutzfreundlicher ist es, wenn der Betroffene mehrere Erklärungen auch jeweils gesondert unterschreiben kann.*

– Sollen E-Mail-Adresse und Telefonnummer an Dritte für Zwecke der Werbung übermittelt werden, muss die Einwilligungserklärung dies beinhalten. Der Kreis der Datenempfänger ist möglichst genau anzugeben.

– Die Einwilligung muss ausdrücklich erteilt werden. Das Nichtankreuzen des Satzes „hier ankreuzen, falls die Einwilligung nicht erteilt wird“ (...), ist als Schweigen des Betroffenen zu werten. Ihm kann keine Einwilligung in die Telefon- oder E-Mail-Werbung entnommen werden. Der gegenteiligen Entscheidung des OLG München vom 28. September 2006 (Az.: 29 U 2769/06) kann nicht gefolgt werden. Es bleibt zu hoffen, dass der Bundesgerichtshof diese Entscheidung im Revisionsverfahren korrigiert.

– Die Einwilligung muss vorliegen, bevor der erste Anruf getätigt oder die erste E-Mail versandt wird. Umgehungen des Gesetzes durch vorgeschobene Meinungsumfragen sind unzulässig. Telefonate zu Zwecken der Markt- und Meinungsforschung dürfen nicht mit der Einholung der Einwilligung verbunden werden.

– Ist es aufgrund „besonderer Umstände“ nach § 4 a Abs. 1 BDSG zulässig, die Einwilligung in das Telefonmarketing telefonisch einzuholen, muss über jede Einwilligung ein Beleg erstellt werden, aus dem hervorgeht, wer die Einwilligung wann eingeholt und wer sie erteilt hat. Bestreitet der Betroffene, eine Einwilligung in die Telefonwerbung erteilt zu haben, genügt ein solcher Beleg allerdings nicht als Beweis. Bewiesen werden kann eine im Rahmen eines Telefonats erteilte Einwilligung nur durch eine Aufzeichnung, aus der sich ergibt, wer in die Telefon- und E-Mail-Werbung wann eingewilligt hat. Selbstverständlich muss der Betroffene zuvor in die Aufzeichnung dieses Teils des Telefonats eingewilligt haben.

– Die Einwilligungserklärungen sind in Papierform oder mikroverfilmt aufzubewahren, solange von ihnen Gebrauch gemacht wird. Bezieht ein Unternehmen Opt-In-Daten vom einem Adresshändler, hat das Unternehmen die Aufbewahrung der Unterlagen durch vertragliche Vereinbarungen mit diesem sicherzu-

stellen. Auch hat es sich durch Stichprobenkontrollen davon zu überzeugen, dass dem Gesetz genügende Einwilligungserklärungen vorliegen.

– Von Einwilligungserklärungen darf nur zeitlich begrenzt Gebrauch gemacht werden. Das gilt vor allem, wenn die Daten aus dem Adresshandel stammen. Dies verlangt der Grundsatz von Treu und Glauben.

6.2 Online-Gewinnspiele

Im Berichtszeitraum hatten wir uns auch mit über das Internet angebotenen Gewinnspielen zu befassen. Wir haben hierzu folgende Auffassung vertreten:

Bei einem über das Internet angebotenen kostenlosen Gewinnspiel handelt es sich um einen Teledienst (seit 1. März 2007 „Telemediendienst"). Daher sind für das Anbieten und die Nutzung des Gewinnspiels die bereichsspezifischen Regelungen des Teledienstedatenschutzgesetzes (seit 1. März 2007 des Telemediengesetzes) anzuwenden. Für die eingestellten personenbezogenen Inhalte gelten ergänzend die Vorschriften des Bundesdatenschutzgesetzes.

Um die Inanspruchnahme des Gewinnspiels über das Internet zu ermöglichen, fallen beim Anbieter Nutzungsdaten (hierzu gehören beispielsweise die IP-Adressen) an. Diese dürfen nur für die Dauer des Gewinnspiels vorgehalten und nicht darüber hinaus gespeichert werden. Der Anbieter hat den Teilnehmer zu Beginn des Gewinnspiels über Art, Umfang und Zwecke der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu unterrichten.

Inhaltsdaten dürfen bei einem Gewinnspiel nur auf freiwilliger Basis und unter Beachtung des Grundsatzes der Datenvermeidung und Datensparsamkeit erhoben, verarbeitet und genutzt werden. Dies gilt insbesondere für die Erhebung der Telefonnummer und der E-Mail-Adresse sowie die Abfrage des genauen Geburtsdatums. Soll die Spielteilnahme nur Personen ab 18 Jahren ermöglicht werden, wird zumeist die Versicherung des Teilnehmers genügen, dass er diese Altergrenze erreicht beziehungsweise überschritten hat. Wie sonst auch ist der Betroffene nach § 4 Abs. 3 BDSG bei der Datenerhebung und in räumlichen Zusammenhang mit dieser darüber zu unterrichten, für welche Zwecke die (welche) Daten erhoben, gespeichert, übermittelt und genutzt werden (beispielsweise zur Gewinnbenachrichtigung, für eigene und fremde Werbezecke) und an welche Kategorien von Empfängern die Daten übermittelt werden.

Eine darüber hinausgehende Nutzung der erhobenen Daten für andere Zwecke bedarf der Einwilligung des Spielteilnehmers. Die Einwilligung kann auch elektronisch erfolgen. Die Erklärung setzt eine eindeutige und bewusste Handlung des Nutzers voraus. Die elektronische Einwilligung ist zu protokollieren; der Inhalt der Einwilligung muss vom Nutzer jederzeit abgerufen werden können. Indem das Gesetz eine eindeutige und bewusste Handlung verlangt, knüpft es an die allgemeinen Anforderungen an eine rechtsgeschäftliche Handlung an: zum objektiven Tatbestand der Kundgabe muss ein subjektiver Erklärungstatbestand in Form des Handlungswillens, des Erklärungsbewusstseins und des Geschäftswillens hinzukommen. Der jeweilige Spielteilnehmer muss sich bewusst sein, überhaupt eine rechtsverbindliche Einwilligung in Bezug auf die Nutzung und Verarbeitung seiner personenbezogenen Daten abzugeben. Es muss für ihn erkennbar sein, auf welche Daten sich die beabsichtigte Nutzung bezieht und zu welchen Zwecken diese verwendet werden sollen. Dies kann nur durch ein aktives Tun des Spielteilnehmers in Form des Ausfüllens eines Kästchens erfolgen. Ein vorbelegtes Kästchen oder ein „Opt-Out" erfüllen diese Voraussetzungen nicht. Zweckmäßig ist es, den Spielteilnehmer schon vor Ausfüllen des Kästchens auf sein jederzeitiges Widerspruchsrecht gegen die Werbung hinzuweisen.

Falls sich der Spielteilnehmer mit der Verwendung seiner Daten für Werbezwecke einverstanden erklärt hat, sollte er in einer Bestätigungsmail nochmals darauf hingewiesen werden.

6.3 Lotterien

Bei Vor-Ort-Prüfungen von staatlichen Lotterieeinnehmern wurde festgestellt, dass diese vor allem durch Telefonmarketing Neukunden werben beziehungswei-

se Altkunden „reaktivieren“. Sie tun dies über eigene Call-Center und über sogenannte Kooperationspartner. Letztere sind Handelsvertreter in der Form eines Vermittlungsvertreters. Sie werden vom Lotterieeinnehmer durch eine „Zusammenarbeitsvereinbarung“ damit beauftragt, Mitspieler zu werben. Die Kooperationspartner setzen regelmäßig eigene Kundendaten ein. Sie können einen weiteren Subkooperationspartner beauftragen. Die Kooperationspartner müssen bestimmte (Mindest-)Vertragsklauseln, die von der Süddeutschen Klassenlotterie (SKL) und dem Lotterieeinnehmer vorgegeben werden, einhalten. Die Kooperationspartner sind entweder selbst Call-Center beziehungsweise haben ein solches oder beauftragen ein Sub-Call-Center, das ebenfalls Kundendaten anmieten kann.

Bei der Prüfung eines Lotterieeinnehmers mussten wir feststellen, dass diesem keine Übersicht über die beauftragten Sub-Call-Center vorlag, obwohl die Kooperationspartner verpflichtet sind, dem Lotterieeinnehmer sämtliche Sub-Call-Center schriftlich unter Angabe bestimmter Daten zu melden. Im konkreten Fall waren die Kooperationspartner vertraglich verpflichtet, nur Personen anzurufen, von denen eine Einwilligung in die telefonische Werbung vorliegt. Ansonsten enthielt die „Zusammenarbeitsvereinbarung“ keine Regelungen darüber, wen welche datenschutzrechtlichen Pflichten (zum Beispiel Auskunfts-, Berichtigungs- und Löschungsanspruch sowie Werbewiderspruch) treffen. Unter der Überschrift „Datenschutz“ fanden sich lediglich Ausführungen zur Aufzeichnung von Telefongesprächen der Call-Center-Mitarbeiter. Unklar geregelt war, ob sich die Mitarbeiter des Kooperationspartners am Telefon unter dessen Namen oder unter dem Namen des Lotterieeinnehmers melden müssen. Insgesamt stellte sich die Lage unübersichtlich dar (vergleiche dazu auch schon die Darstellung im dritten Tätigkeitsbericht unter C 2.2 S. 54 ff.). Die Aufsichtsbehörde sah sich deshalb veranlasst, auf Folgendes hinzuweisen:

– Im Verhältnis zwischen Lotterieeinnehmern, Kooperationspartnern, Call-Centern und Sub-Call-Centern muss vertraglich klar geregelt sein, wer verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG ist und daher die datenschutzrechtlichen Verpflichtungen (zum Beispiel Auskunfts- beziehungsweise Löschungsanspruch) erfüllen muss.

– Sofern ein Vertragspartner Daten im Auftrag eines anderen verarbeitet, ist dies in eindeutiger Weise zum Ausdruck zu bringen. Dazu gehört, dass ein schriftlicher Auftrag erteilt wird, der den Vorschriften des § 11 Abs. 2 Satz 2 BDSG genügt. Der Auftrag muss klare Festlegungen hinsichtlich der Datenerhebung, -verarbeitung oder -nutzung, der erforderlichen technischen und organisatorischen Maßnahmen und etwaiger Unterauftragsverhältnisse enthalten. Pauschale Aussagen genügen nicht. Selbstverständlich ist, dass der Auftraggeber den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen sorgfältig auswählt und sich von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt.

– Im Falle telefonischer Werbung muss der Anrufer nicht nur seinen Namen und die datenschutzrechtlich verantwortliche Stelle, sondern gegebenenfalls auch die Stelle nennen, bei der er beschäftigt ist (zum Beispiel Name des Call-Centers). Diese Angabe, auf die in der Praxis meist verzichtet wird, halten wir, insbesondere wenn ein Lotterieeinnehmer mehrere Call-Center beschäftigt, für erforderlich, um Beschwerdefälle aufklären zu können. Call-Centern sollte aus Gründen der Transparenz eine Rufnummerunterdrückung verwehrt sein. Es gilt der Grundsatz, dass seriöse Call-Center nichts zu verbergen haben. Der Vertrag sollte hierzu klare Regelungen enthalten.

– Die Rahmenbedingungen für die telefonische Werbung (siehe dazu oben Nr. 1) sollten im Vertrag aufgeführt werden; den schlichten Hinweis auf § 7 UWG halten wir nicht für ausreichend, da zumindest ein Teil der Call-Center-Betreiber nicht weiß, was datenschutzrechtlich zu beachten ist.

– Von der Einwilligung in die telefonische Werbung sind die Einwilligung in die Teilnahme am Lotteriespiel und die Erhebung und Verarbeitung der Adress- und Kontodaten zu unterscheiden. Selbstverständlich müssen auch insoweit die Unterrichtungs- und Hinweispflichten nach § 4 Abs. 3 BDSG beachtet werden. Die Einwilligung in die Teilnahme am Lotteriespiel muss eindeutig dokumen-

tiert werden; sie darf sich nicht auf die Angabe beschränken, dass die Einwilligung erteilt wurde. Vereinbarungen müssen hierzu Näheres enthalten.

– In dem Beziehungsgeflecht zwischen Lotterieeinnehmern, Kooperationspartnern, Call-und Sub-Call-Centern muss für die Betroffenen klar erkennbar sein, wohin sie sich mit einem Werbewiderspruch wenden können. Es ist sicherzustellen, dass Werbewidersprüche in eine von der verantwortlichen Stelle eingerichtete Werbesperrdatei eingetragen werden. Vor Werbemaßnahmen muss ein Abgleich mit der Werbesperrdatei erfolgen.

– Verweigert ein Betroffener die Einwilligung in die Telefonwerbung, bedarf es keiner Eintragung in eine Werbesperrdatei.

Die Umsetzung dieser datenschutzrechtlichen Anforderungen und aufsichtsbehördlicher Vorgaben der SKL, mit der wir Kontakt aufgenommen hatten, haben die Zahl der Beschwerden wegen unzulässiger Telefonwerbung in diesem Bereich deutlich zurückgehen lassen.

6.4 Nutzung von Telefonbucheinträgen

Ein Rechtsanwalt erhielt von einer baden-württembergischen Firma einen Werbebrief. Dieser war an seine Kanzleianschrift gerichtet. Seine Nachfrage bei der Firma ergab, dass Name und Adresse aus den Gelben Seiten stammten. Der Rechtsanwalt wandte sich mit der Behauptung an uns, seine Daten seien rechtswidrig genutzt worden, da er keineswegs seine Zustimmung erteilt habe, die Adresse für Werbezwecke zu nutzen. Dass seine Daten in den Gelben Seiten abgedruckt seien, lasse auch nicht auf eine solche Zustimmung schließen, wie sich aus dem den Gelben Seiten vorangestellten „wichtigen datenschutzrechtlichen Hinweis“ ergebe. Keineswegs seien die Gelben Seiten als „öffentliches Verzeichnis“ in dem Sinn zu verstehen, dass damit ein Freibrief für Werbung verbunden sei.

Im Einvernehmen mit dem für Telefonbuchverlage zuständigen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit kamen wir zu dem Ergebnis, dass es sich bei den in den Gelben Seiten veröffentlichten Namen und Adressen um allgemein zugängliche Daten handelt, die auch für Werbezwecke genutzt werden dürfen. Dass in den Gelben Seiten auch Daten von Personen enthalten sind, die der Nutzung ihrer Daten zu Werbezwecken widersprochen haben, indem sie ein Sonderzeichen vor ihrer Adresse haben eintragen lassen, ändert hieran nichts. Allenfalls in diesen Fällen könnte daran gedacht werden, hierin einen Werbewiderspruch nach § 28 Abs. 4 BDSG zu sehen. Auf alle anderen Einträge im Telefonbuch wirkt sich dieses Zeichen jedoch nicht aus. Es ist daher davon auszugehen, dass bei allen Anschriften ohne Sonderzeichen kein Werbewiderspruch vorliegt. Soweit im „wichtigen datenschutzrechtlichen Hinweis“ zu den Gelben Seiten von fehlender Einwilligung die Rede ist, bezieht sich diese auf die Telefonwerbung. Für sie ist nach dem Gesetz gegen unlauteren Wettbewerb und dem Bundesdatenschutzgesetz eine Einwilligung des Betroffenen erforderlich (siehe dazu oben Nr. 6.2).

6.5 Werbung für eine politische Partei

Vor der Landtagswahl 2006 nutzten politische Parteien Daten von Adresshändlern, um Wahlberechtigte gezielt anzuschreiben und für ihre Programme zu werben. Dies ist aus datenschutzrechtlicher Sicht nicht zu beanstanden. Politische Werbung ist nach herrschender Meinung, der sich die Aufsichtsbehörde anschließt, datenschutzrechtlich nicht anders zu behandeln als kommerzielle Werbung. Das heißt aber auch, dass Betroffene gegenüber der verantwortlichen Stelle der Nutzung und Übermittlung ihrer Daten für Zwecke der Wahlwerbung widersprechen können. Auf das Widerspruchsrecht müssen sie hingewiesen, die verantwortliche Stelle muss genau bezeichnet werden (§ 28 Abs. 4 BDSG).

Aufgabe der werbenden Parteien ist es dann, solchen Werbewidersprüchen Rechnung zu tragen und dafür zu sorgen, dass die Daten der Widersprechenden in einer Werbesperrdatei erfasst werden. Bei zukünftigen Werbeaktionen der Parteien müssen dann die vorgesehenen Versandadressen vorab mit dieser Sperrdatei abgeglichen werden, um zu verhindern, dass Widersprechende Wahlwerbung erhalten.

Diese Maßnahmen erübrigen sich nicht dadurch, dass Betroffene die Möglichkeit haben, gegenüber der Meldebehörde der Übermittlung ihrer Daten an politischen Parteien für Zwecke der Wahlwerbung zu widersprechen (§ 34 Abs. 1 des Meldegesetzes). Es geht hier um unterschiedliche Datenbestände.

7 Handel, Gewerbe, Gaststätten, Verkehr

7.1 Einsatz kontaktloser Fahrkarten bei einem Verkehrsunternehmen

Ein Verkehrsverbund in Baden-Württemberg plante, seine Fahrscheinautomaten durch ein sogenanntes „Elektronisches-Ticketing-Verfahren“ mit kontaktlosen Fahrkarten zu ersetzen. Der Fahrgast sollte keine Tarifkenntnisse benötigen. Bei jedem Ein-, Aus- oder Umsteigen des Fahrgastes sollten die Fahrwege in den Terminals der Verkehrsmittel sowie auf der Fahrkarte festgehalten und der günstigste Fahrpreis für den Kunden automatisch berechnet werden. Datenschutzrechtlich wie auch technisch stellte das Vorhaben eine Herausforderung dar, als dass Ein-, Aus- oder Umsteigen kontaktlos mittels der RFID-Technik (vergleiche dazu dritter Tätigkeitsbericht C 7.4, S. 132 ff.) auf der elektronischen Fahrkarte und in den Terminals der Verkehrsmittel gespeichert werden sollte (sogenannte aktive RFID-Fahrkarte). In den Ruhe- und Wartungszeiten der Verkehrsmittel – in der Regel nachts – sollten die über die Terminals der Verkehrsmittel sowie am Bahnsteig erfassten Daten mittels WLAN-Technik verschlüsselt auf das Serversystem übertragen werden. Dieses sollte dann die Fahrpreisberechnung und die Zuordnung zum Kundenkonto durchführen. Von diesem Serversystem sollte die Summe der Fahrten zu einem anderen separaten Serversystem übermittelt werden, das monatlich per Briefpost oder per E-Mail einen Kontoauszug mit den erfolgten Abbuchungen und eine Auflistung der Fahrten an die Kunden versenden sollte. Die RFID-Fahrkarte sollte durch ein externes Unternehmen ausgestellt werden. Die Nutzung des Elektronischen-Ticketing-Verfahrens zur Ermittlung des günstigsten Fahrpreises sollte freiwillig sein. Der Fahrgast sollte auch weiterhin einen herkömmlichen Fahrschein lösen können.

Der Verkehrsverbund ließ sich während der Planungs- und Einführungsphase durch uns beraten. Wir haben dabei darauf geachtet, dass der Kunde bei der Beantragung der Karte möglichst wenig persönliche Angaben machen muss und nach § 4 Abs. 3 BDSG über die Erhebung, Verarbeitung und Nutzung seiner Daten unterrichtet wird. Wichtig war uns darüber hinaus, dass den Erfordernissen des § 6 c BDSG in der Praxis Rechnung getragen wird. Dazu haben wir im Einzelnen gefordert:

- Der Verkehrsverbund muss den Kunden zum frühestmöglichen Zeitpunkt in allgemein verständlicher Form über die Funktionsweise der RFID-Karte, die Art der zu verarbeitenden personenbezogenen Daten und die Verarbeitungswege informieren. Dazu gehört auch die Unterrichtung über die getroffenen Vorkehrungen zur Verarbeitung personenbezogener Daten über das auf dem Medium installierte Verfahren, über EDV-Hintergrundsysteme, auf denen die personenbezogene Verarbeitung und Nutzung durchgeführt werden, sowie über Art und Umfang der Schreib- und der Leseberechtigung. Wir haben dem Verkehrsverbund empfohlen, seinen Kunden ein Informationsblatt auszuhändigen. Es muss auch darüber informieren, wie der Kunde seinen Berichtigungs- und Löschungsanspruch nach dem Bundesdatenschutzgesetz ausüben kann.
- Die personenbezogenen Daten dürfen nur für die Zwecke der Fahrpreisberechnung und -abrechnung verarbeitet und genutzt werden. Eine Änderung des Zwecks bedarf der vorherigen Information des Betroffenen und gegebenenfalls seiner Einwilligung.
- Zur Herstellung der Vertraulichkeit der Datenübertragung von den Terminals in den Verkehrsmitteln oder an den Bahnsteigen über WLAN zum Serversystem ist es erforderlich, dass die Übertragungsstrecke mit einem schwer entschlüsselbaren Schlüssel (mindestens 128 Bit) verschlüsselt wird.
- Es ist zu gewährleisten, dass – außer dem Verkehrsverbund – nur die zur Benutzung der RFID-Fahrkarte Berechtigten auf die Daten zugreifen können. Fahrkartenkontrolleure dürfen nur einen begrenzten Lesezugriff auf die Daten haben. Dritte dürfen die Daten nicht unbemerkt auslesen können. Empfohlen

wurde in diesem Zusammenhang eine verschlüsselte Speicherung der Inhaltsdaten.

– Die personenbezogenen Daten dürfen nur so lange gespeichert bleiben, wie es zur Erreichung des angegebenen Zwecks erforderlich ist. Es sind daher Löschfristen festzulegen. Der Betroffene ist über die Löschfristen zu informieren.

– Die Daten müssen sicher aufbewahrt werden, insbesondere gegen zufällige Zerstörung oder Verlust geschützt sein (beispielsweise mittels Back-up-Systemen).

– Der Kunde muss in angemessenem Umfang die Möglichkeit haben, den Inhalt seiner Fahrkarte auslesen zu können.

– Fehlermeldungen des Zugangs-/Erfassungssystems dürfen die Betroffenen nicht öffentlich diskriminieren.

Das hat unter anderem zu folgender Umsetzung geführt:

Für jeden Ein- und Aussteigevorgang stehen am Bahnsteig oder im Verkehrsmittel Terminals zur Verfügung, die den Ein-, Aus- oder Umsteigevorgang erfassen. Diese Vorgänge werden am Terminal akustisch und optisch kurz angezeigt. Hierfür ist die elektronische Fahrkarte in einem Abstand von etwa 10 cm an dem Terminal vorbeizuführen. Die kontaktlose Übermittlung dieser Vorgänge erfolgt mittels verschlüsselter Funkstrecke. Bei jedem Aus-, Ein- oder Umsteigevorgang wird auf der Karte des Fahrgastes ein Datensatz mit Datum, Uhrzeit, Haltestellennummer, Linie, Kurs, Kunden-ID und Kennung gespeichert. Ein gleicher Datensatz wird im Terminal des Verkehrsmittels oder auf dem Bahnsteig gespeichert. Der Kunde kann über aufgestellte Lese-Terminals jederzeit auf die gespeicherten Daten seiner RFID-Fahrkarte Zugriff nehmen. Er kann sich dabei die letzten zehn Fahrten anzeigen lassen. Der Lesezugriff des Kontrollpersonals ist auf die für Kontrolle erforderlichen Daten, das sind die Daten der angetretenen Fahrt, beschränkt. Die Daten sind nur für den Zweck der Fahrpreisberechnung und Abrechnung zu verwenden. Die in den Terminals der Verkehrsmittel gespeicherten Daten werden nach erfolgreicher Datenübertragung gelöscht. Die Löschung der Streckendaten auf dem Serversystem erfolgt nach Ablauf der Einspruchsfrist, die mit der Zusendung des Kontoauszuges beginnt.

Sollte das kontaktlose Ticketing-Verfahren einmal ausfallen, kann eine normale Fahrkarte nachgelöst werden. Das Nichtfunktionieren der kontaktlosen Fahrkarte wird beim Einsteigevorgang akustisch und optisch am Terminal angezeigt. Der Fahrgast kann dann eine normale Fahrkarte beim Fahrer oder Automaten lösen.

Nach Durchführung der Vorabkontrolle und nach Abwägung des datenschutzrechtlichen Restrisikos konnte das E-Ticketing im Verbundsystem eingeführt werden.

7.2 Einsatz eines biometrischen Verfahrens in einer Kantine

Im Rahmen einer datenschutzrechtlichen Anfrage hatten wir uns mit dem Einsatz eines biometrischen Verfahrens zur Abrechnung von Kantinenessen für Schüler zu beschäftigen. Die Schüler sollten die Möglichkeit haben, ihr Mittagessen in einer privat betriebenen Kantine einzunehmen. Die Abrechnung der konsumierten Speisen sollte entweder per Barzahlung oder per Fingerprintverfahren möglich sein. Bei dem Fingerprintverfahren wird der konsumierte Betrag am Monatsende mittels Lastschriftverfahren eingezogen.

Das Fingerprintverfahren ist ein Verfahren, das mittels biologischer Merkmale – hier der Fingerlinien – eine Identifikation und/oder eine Verifikation einer Person durchführt. Dabei entstehen personenbezogene Daten. Bei der Verifikation wird lediglich die Identität einer Person bestätigt, also geprüft, ob es sich bei einer Person um diejenige handelt, für die sie sich ausgibt. Bei der Identifikation wird geklärt, um welche Person es sich wirklich handelt.

Eine Erhebung, Verarbeitung und Nutzung solcher Daten ist nur aufgrund einer gesetzlichen Regelung oder mit Kenntnis der betreffenden Person und deren Einwilligung zulässig. Die Einwilligung ist aber nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht.

Bei der Auswahl des einzusetzenden Fingerabdruckverfahrens ist der Grundsatz der Datenvermeidung und Datensparsamkeit zu beachten. Es gibt mehrere technische Realisierungsmöglichkeiten:

Eine Lösung setzt die zentrale Speicherung der biometrischen Merkmale voraus. Bei einer solchen zentralen Datensammlung besteht die Gefahr, dass durch Änderung des Zwecks und der Verknüpfung mit anderen Daten des Betroffenen in das Persönlichkeitsrecht des Betroffenen eingegriffen werden kann. Dabei werden keine manuellen physischen Abdrucke des Fingerprints, wie sie beispielsweise die Polizei verwendet, gespeichert. Deshalb ist bei einer zentralen Speicherung darauf zu achten, dass der mathematische Algorithmus (Hash-Wert) zur Umsetzung des physischen Fingerabdrucks in ein mathematisches Zahlenmuster immer nur einmalig für den jeweiligen Zweck und das Unternehmen zur Verfügung steht und eine Reproduzierbarkeit des physischen Fingerabdrucks nicht möglich ist. Das gespeicherte und verschlüsselte Ergebnis dieses umgewandelten Zahlenwertes wird auch Template genannt. Um zu verhindern, dass die umgewandelten Zahlenwerte mit anderen Zahlenwerten verschiedener Anwender verknüpft werden können, ist es erforderlich, dass der mathematische Algorithmus zwischen den Anwendern unterschiedlich ist. Ein Fingerabdruck der gleichen Person wird bei unterschiedlichen Anwendern deshalb auch zu unterschiedlichen Ergebnissen (Templates) führen.

Eine andere Lösungsmöglichkeit besteht darin, die biometrischen Daten nicht im Verfügungsbereich der datenverarbeitenden Stelle zu belassen, sondern diese unter die Kontrolle der jeweiligen Person zu stellen. Hierzu bieten sich Chip-basierte biometrische Verfahren an, bei denen die zu identifizierende Person die gemessenen biometrischen Daten der Fingerabdrücke mit sich führt (zum Beispiel als Chip-Karte) und im Identifikationssystem die Übereinstimmung dieser Daten mit den gemessenen biometrischen Daten der Betroffenen über einen sogenannten Hash-Wert überprüft wird. Beim Einsatz dieses Verfahrens wären die datenschutzrechtlichen Vorschriften für mobile personenbezogene Speicher- und Verarbeitungsmedien zu beachten (§ 6 c BDSG).

Neben den rechtlichen Voraussetzungen sind die technischen und organisatorischen Anforderungen zu beachten und zu beschreiben. Außerdem ist es wichtig, dass auch für Fehlerfälle des Fingerabdruckverfahrens (beispielsweise das Nichterkennen eines Fingerabdrucks) Alternativen aufgezeigt werden.

Unsere Beratung hat im vorliegenden Fall zu folgender Umsetzung geführt:

Für die Abrechnung der Kantinenessen mittels Fingerprints wurde das oben beschriebene zentrale Verfahren gewählt. Um am Fingerprintverfahren teilnehmen zu können, müssen sich die Schüler registrieren lassen. Hierzu werden die zum Lastschrifteinzug erforderlichen Bestandsdaten der Eltern und ein Fingerabdruck von jedem Schüler erhoben und in der Datenbank des Kantinenbetriebes gespeichert. Dabei wird der Fingerabdruck, wie oben beschrieben, nicht als manuelles Bild gespeichert, vielmehr werden bestimmte Positionen der Fingerlinien über einen mathematischen Algorithmus in einen Zahlenwert (sogenannter Hash-Wert) umgewandelt und verschlüsselt gespeichert. Es ist bei diesem Verfahren nicht möglich, den Original-Fingerabdruck als manuelles Bild wieder herzustellen.

Die Teilnahme am Fingerprintverfahren und die damit gekoppelte Bezahlung im Lastschriftverfahren beruhen auf der Einwilligung der Schüler beziehungsweise der Eltern. Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Dies ist im vorliegenden Fall gewährleistet, da als Alternative zum Fingerprintsystem mit Lastschriftverfahren Barzahlung angeboten wird. Barzahlung ist auch als sogenannte Back-up-Lösung bei Ausfall des Fingerprintsystems vorgesehen.

Bei der Erhebung der Daten für die Teilnahme am Fingerprintsystem werden sowohl die Schüler als auch die Eltern mithilfe eines Informationsblatts über die verantwortliche Stelle, die genaue Zweckbestimmung der Erhebung und Verarbeitung und die Empfänger der Daten unterrichtet. Die Löschung der Daten erfolgt nach Begleichung des Rechnungsbetrages.

Bei Schülern, die mangels Einsichtsfähigkeit nicht selbst in die Teilnahme am Fingerprintverfahren einwilligen können, bedarf es der Einwilligung der Eltern.

Die Einwilligung muss vor der Verarbeitung personenbezogener Daten vorliegen.

7.3 Bonitätsabfragen bei einer Auskunftei zur Festlegung der Zahlungsart

Ein Call-Center nimmt im Auftrag einer englischen Firma Bestellungen im deutschsprachigen Raum entgegen. Die englische Firma betreibt Fernsehwerbung mit direkter Bestellmöglichkeit über eine am Bildschirm eingeblendete Telefonnummer. Ruft ein Kunde diese Telefonnummer an, wird er mit besagtem Call-Center verbunden. Dabei gibt der Kunde neben seinem Bestellwunsch seinen Vor- und Nachnamen, die Adresse und die Telefonnummer für Rückfragen an. Während der Bestellaufnahme erfolgten bislang unbemerkt vom Kunden eine Adressverifizierung und eine Bonitätsprüfung. Für die Bonitätsprüfung werden die personenbezogenen Daten an eine Auskunftei übermittelt. Diese teilt dem Call-Center einen Scorewert mit, den sie anhand ihr vorliegender Daten über den Kunden errechnet hat. Dies alles geschieht in Sekundenschnelle und ohne Wissen des Kunden. Anhand des übermittelten Scorewertes bietet das Call-Center dem Kunden dann eine oder mehrere Zahlungsmöglichkeiten an: Kreditkarte, Nachnahme, auf Rechnung oder Vorauskasse.

Gegen die Adressüberprüfung ist nichts einzuwenden. Sie ist zur Erfüllung eigener Geschäftszwecke zulässig, damit die bestellte Ware auch richtig zugestellt werden kann.

Unzulässig ist es hingegen, eine Bonitätsüberprüfung durchzuführen, ohne den Kunden zuvor nach der gewünschten Zahlungsart zu fragen. Entscheidet sich dieser nämlich für die Zahlung gegen Vorauskasse, besteht für das Unternehmen, für das das Call-Center tätig wird, kein kreditorisches beziehungsweise erhebliches finanzielles Ausfallrisiko. Es hat daher auch kein berechtigtes Interesse an Bonitätsdaten. Nur wenn aufgrund der vom Kunden gewünschten Zahlungsart ein solches Risiko besteht, darf das Call-Center eine Bonitätsabfrage durchführen. Der Kunde ist hierüber zu informieren.

Das Call-Center hat seine Verfahrensweise inzwischen geändert.

8 Gesundheit und Soziales

8.1 Elektronische Gesundheitskarte

Das Gesetz zur Modernisierung der gesetzlichen Krankenversicherung sieht vor, dass die bisherige Krankenversichertenkarte zu einer elektronischen Gesundheitskarte (eGK) erweitert wird. Mit ihr soll die Wirtschaftlichkeit, Qualität und Transparenz in der Krankenbehandlung verbessert werden. Das Gesetz kennt Pflichtanwendungen und freiwillige Anwendungen. Der Pflichtteil der eGK wird die administrativen Daten der bisherigen Krankenversichertenkarte einschließlich eines Lichtbilds enthalten und die papierlose Übertragung von Rezepten ermöglichen. In einem freiwilligen medizinischen Teil sollen Notfalldaten, Befunde, Diagnosen, Therapieempfehlungen und Maßnahmen, Behandlungsberichte, Impfungen sowie Röntgenreihenuntersuchungen gespeichert werden. Der Gesetzgeber sieht eine schrittweise Verwirklichung vor.

Damit die eGK am Ende im Echtbetrieb funktioniert, bedarf es eines Testlaufs. Das Bundesministerium für Gesundheit hat Anfang 2006 mehrere Testregionen festgelegt, zu denen der Stadt- und der Landkreis Heilbronn gehören. Sie sollen zunächst mit jeweils maximal 10.000 Versicherten, einigen Ärzten und Apotheken sowie einem Krankenhaus einen Test unter realen Einsatzbedingungen, das heißt unter Verwendung von Echtdaten der Versicherten und Leistungserbringer, durchführen. Die Teilnahme der Versicherten ist freiwillig. Bei erfolgreichem Testverlauf soll sich ein weiterer Test mit bis zu 100.000 Versicherten mit einer entsprechend größeren Zahl von Leistungserbringern anschließen.

Nach der Verordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte in der Fassung vom 5. Oktober 2006 (BGBl. I S. 2200) sollen mit der eGK zunächst ohne Netzzugang

- das Auslesen der Versichertenstammdaten,
- die Übermittlung der ärztlichen Verordnungen für apothekenpflichtige Arzneimittel mit Ausnahme von Betäubungsmitteln und

– die Bereitstellung von Daten zur Unterstützung der Notfallversorgung

getestet werden.

In einem zweiten Schritt soll die eGK unter Online-Bedingungen getestet werden. Zusätzlich soll über die Online-Verbindung die Gültigkeit des Krankenversicherungsnachweises überprüft werden. Die Angaben nach § 291 Abs. 2 des Fünften Buchs Sozialgesetzbuch sollen mit den Daten der Krankenkasse abgeglichen und bei Bedarf auf der elektronischen Gesundheitskarte aktualisiert werden.

Die Festlegung der technischen Infrastruktur geschieht durch die hierfür gegründete gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH).

Die Federführung für die Durchführung der Tests hat die Arbeitsgemeinschaft zur Einführung der elektronischen Gesundheitskarte in Baden-Württemberg. Sie wurde im Februar 2005 von medizinischen Leistungserbringern und Krankenkassen mit dem Ziel gegründet, die eGK und den elektronischen Heilberufsausweis (HBA) gemeinsam zu testen und einzuführen.

Der Testlauf mit 10.000 Versicherten hat im Raum Heilbronn Anfang 2007 begonnen. Bis Ende 2007 soll dieser abgeschlossen werden. Die Aufsichtsbehörde begleitet die Tests, da an ihnen Ärzte und Apotheken mitwirken, die ihrer Aufsicht unterliegen. Bislang ging es vor allem um den Inhalt der Einwilligungserklärungen, die die an dem Test teilnehmenden Versicherten, Ärzte und Apotheker unterschreiben sollen. Sie müssen auch Informationen darüber enthalten, welche Daten für welche Zwecke an welche Stellen übermittelt werden, damit die Teilnehmer in die Datenverarbeitung bewusst einwilligen können.

Die weitere Entwicklung bleibt abzuwarten. Der Deutsche Ärztetag hat sich im Mai 2007 gegen die Einführung der eGK in der derzeit geplanten Form ausgesprochen. Er befürchtet unter anderem, dass das Arzt-Patienten-Verhältnis durch die Speicherung sensibler Patientendaten in zentralen Rechnern „schwer beschädigt oder sogar zerstört wird“, der Zugriff auf die Daten und deren Missbrauch nicht sicher zu verhindern sind, die Karte keinen Nutzen für die Ärzte hat und die Praxisabläufe erheblich behindert werden.

8.2 Aufzeichnung von Anrufen für den Ärztlichen Notfalldienst

In Baden-Württemberg haben die vier Kassenärztlichen Vereinigungen, die Landesärztekammer, die Landesverbände der gesetzlichen Krankenkassen und die beiden Landesverbände des Deutschen Roten Kreuzes als Träger der Rettungsleitstellen/integrierten Leitstellen nach langwierigen Verhandlungen in Zusammenarbeit mit dem Ministerium für Arbeit und Soziales Baden-Württemberg Ende 2003 eine „Rahmenvereinbarung über die Zusammenarbeit der Rettungsleitstellen mit dem vertragsärztlichen Notfalldienst in Baden-Württemberg nach § 6 Abs. 4 des Rettungsdienstgesetzes und § 75 Abs. 1 Satz 2 SGB V“ abgeschlossen. Damit wurde das Ziel erreicht, landeseinheitliche Grundlagen für die Zusammenarbeit der Rettungsleitstellen/integrierten Leitstellen mit dem vertragsärztlichen Notfalldienst zu schaffen. Die Rahmenvereinbarung sieht vor, dass die Anrufabfrage, die Vermittlung des Anrufs an den jeweiligen diensthabenden Arzt im Notfalldienst und die Dokumentation in den Rettungsleitstellen erfolgen.

In diesem Zusammenhang musste sich die Aufsichtsbehörde mit der Frage befassen, ob in der integrierten Rettungsleitstelle Anrufe, die für den vertragsärztlichen Notfalldienst eingehen, aufgezeichnet werden dürfen. Diese Frage ist zum einen unter verfassungs- und datenschutzrechtlichen und zum anderen unter strafrechtlichen Gesichtspunkten zu beurteilen.

Verfassungsrechtlich ist anerkannt, dass das von Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes erfasste allgemeine Persönlichkeitsrecht auch das Recht am gesprochenen Wort schützt. Dieses gewährleistet die Selbstbestimmung über die eigene Darstellung der Person in der Kommunikation mit anderen. Dieses Selbstbestimmungsrecht findet seinen Ausdruck in der Befugnis des Menschen, selbst und allein zu entscheiden, ob sein Wort auf einem Tonträger aufgenommen und damit möglicherweise Dritten zugänglich werden soll. Das Grundgesetz schützt davor, dass Gespräche heimlich aufgenommen und ohne Einwilligung des Anrufers oder gar gegen dessen erklärten Willen verwertet werden. Der Schutz besteht grundsätzlich unabhängig davon, ob die Gespräche priva-

ter oder geschäftlicher Natur sind, ob der Inhalt geheimhaltungsbedürftig, vertraulich oder besonders sensibel ist. Eine Aufzeichnung der Anrufe, die beim vertragsärztlichen Notfalldienst eingehen, ist daher nur zulässig, wenn ein Gesetz dies zulässt oder der Anrufer eingewilligt hat. Die für die Kassenärztliche Vereinigung geltenden *sozialdatenschutzrechtlichen Vorschriften* räumen dieser nicht die Befugnis ein, Telefongespräche aufzuzeichnen. Deshalb ist die Aufzeichnung nur mit Einwilligung des Betroffenen zulässig. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Danach kann gegebenenfalls auch eine mündliche Einwilligung genügen. Weitgehend anerkannt ist jedoch, dass es sich um eine ausdrückliche Einwilligung handeln muss; eine konkludente, stillschweigende oder gar eine mutmaßliche Einwilligung genügt datenschutzrechtlich nicht.

Strafrechtlich wird die unbefugte Aufnahme des nichtöffentlich gesprochenen Wortes eines anderen auf einem Tonträger nach § 201 Abs. 1 Nr. 1 StGB mit Strafe bedroht. „Unbefugt“ ist die Aufnahme, wenn es dafür weder eine gesetzliche Befugnis noch einen Rechtfertigungsgrund gibt. Gerechtfertigt sein kann die Aufnahme aufgrund einer Einwilligung des Anrufers. Strafrechtlich genügt auch eine stillschweigende, konkludente oder mutmaßliche Einwilligung. Eine mutmaßliche Einwilligung des Anrufers in die Aufzeichnung liegt nicht vor. Sie setzt voraus, dass die Einwilligung des Anrufers nicht rechtzeitig eingeholt werden kann, eine Würdigung aller Umstände aber die Annahme rechtfertigt, dass er, wenn er gefragt werden könnte, seine Zustimmung erteilen würde. Dem gleichgestellt ist der Fall, dass ohne weiteres davon ausgegangen werden kann, dass der Anrufer auf eine Befragung keinen Wert legt.

Diese Voraussetzungen hat die Aufsichtsbehörde anders als bei Notrufen unter den Telefonnummern 112 oder 19222 beim vertragsärztlichen Notfalldienst nicht für gegeben erachtet. Der vertragsärztliche Notfalldienst dient der „Sicherstellung der vertragsärztlichen Versorgung“ (§ 75 SGB V) in den sprechstundenfreien Zeiten. Er ist für Erkrankungen gedacht, deren Behandlung nicht bis zum nächsten Werktag warten kann. Seine Hauptaufgabe besteht darin, Anrufer darüber zu informieren, welche Arztpraxen und Notfallpraxen zu bestimmten Zeiten geöffnet haben. Der vertragsärztliche Notfalldienst darf nicht mit dem Notarzt verwechselt werden, der Teil des Rettungsdienstes ist. Der vertragsärztliche Notfalldienst ist örtlich unterschiedlich organisiert. Wird er – wie eingangs dargestellt – von einer Rettungsleitstelle im Auftrag der Kassenärztlichen Vereinigung wahrgenommen, ändert dies am Charakter des Dienstes nichts. Er unterfällt deswegen nicht den Vorschriften des Rettungsdienstgesetzes. Der Anruf beim vertragsärztlichen Notfalldienst ist nicht als „Notruf“ im Sinne des § 108 des Telekommunikationsgesetzes anzusehen, für den die Rufnummern 112 und 19222 (rettungsdienstliche Notrufnummer) vorgesehen sind, sondern ist seinem Charakter nach einem Anruf in einer Arztpraxis gleichzustellen. Hier kann nicht davon ausgegangen werden, dass der Anrufer, wenn er gefragt würde, mit einer Aufzeichnung seines Anrufs einverstanden wäre beziehungsweise auf eine Befragung keinen Wert legt.

Eine konkludente Einwilligung kann angenommen werden, wenn dem Anrufer bekannt ist, dass sein Gespräch aufgezeichnet wird, er aber dennoch anruft. Davon kann im vorliegenden Fall ebenfalls nicht ausgegangen werden. Einem Anrufer beim ärztlichen Notfalldienst dürfte nicht bekannt sein, ob beziehungsweise dass dort Gespräche aufgezeichnet werden. Deshalb kann der Strafbarkeit einer Aufzeichnung nur dadurch begegnet werden, dass der Anrufer vor Beginn der Aufzeichnung auf diese hingewiesen wird. Setzt er den Telefonkontakt dann fort, kann von einem grundsätzlichen Einverständnis in die Aufzeichnung ausgegangen werden.

Die Aufsichtsbehörde hat deshalb die Anfrage dahin gehend beantwortet, dass Anrufe beim vertragsärztlichen Notfalldienst beziehungsweise bei Rettungsleitstellen, die die Aufgabe des ärztlichen Notfalldienstes übernommen haben, nur dann aufgezeichnet werden dürfen, wenn der Anrufer zuvor – beispielsweise durch eine kurz gefasste Bandansage – hierauf hingewiesen wurde. Dem Datenschutz, der an sich die ausdrückliche Einwilligung des Anrufers verlangt, ist damit zwar nicht in vollem Umfang Rechnung getragen, es ist jedoch zumindest sichergestellt, dass der Anrufer in Kenntnis der Aufzeichnung das Gespräch fortsetzt und sich die Mitarbeiter der aufzeichnenden Stelle nicht strafbar machen.

8.3 Erhebung und Speicherung der Personalausweisnummer bei der Blutspende

Darf ein Blutspendedienst von einem Erstspender zu dessen eindeutiger Identifizierung die Personalausweisnummer erheben und speichern? Diese Frage wurde uns von einem Betroffenen gestellt.

Der von uns dazu gehörte Blutspendedienst bejahte die Frage unter Berufung auf das Transfusionsgesetz und die dazu ergangenen Richtlinien zur Gewinnung von Blut- und Blutbestandteilen. Danach sei die Identität des Spenders beispielsweise anhand eines amtlichen Dokuments mit Lichtbild festzustellen. Deshalb lasse sich der Blutspendedienst von jedem Blutspender den Personalausweis vorlegen. Um die Überprüfung zu dokumentieren, werde die Personalausweisnummer des Spenders erhoben und automatisiert gespeichert. Dies ermögliche es dem Blutspendedienst, im Falle einer Rückverfolgung einer Blutspende die Identität des Spenders auch über längere Zeiträume hinweg eindeutig festzustellen. Der Name genüge hierfür nicht, weil es immer wieder Fälle von Namensidentität gegeben habe. Die Anschrift könne wechseln und sei daher zur Feststellung der Identität ebenfalls nicht hinreichend geeignet.

Nach dem Transfusionsgesetz darf ein Blutspendedienst personenbezogene Daten eines Blutspenders erheben und verarbeiten, insbesondere speichern, soweit dies für die im Gesetz genannten Zwecke erforderlich ist. Darüber hinaus bestimmt das Gesetz lediglich, dass die anlässlich der Spendeentnahme vorzunehmende Feststellung der Identität der spendenden Person nach dem allgemein anerkannten Stand der medizinischen Wissenschaft und Technik zu erfolgen hat. Diesen legt die Bundesärztekammer in Richtlinien fest. Die Richtlinien zur Gewinnung von Blut und Blutbestandteilen und zur Anwendung von Blutprodukten (Hämotherapie) gemäß §§ 12 und 18 des Transfusionsgesetzes wiederholen noch einmal, dass anlässlich jeder Spende die Identität des Spenders festzustellen ist. Dies könne beispielsweise anhand eines gültigen amtlichen Personaldokuments mit Lichtbild erfolgen. An Spenderdaten seien Name, Vorname, Geburtsdatum, Adresse und – falls vorliegend – Blutgruppe des Spenders zu erfassen. Die Personalausweisnummer wird nicht genannt. Obwohl die Richtlinien keine Rechtsvorschriften sind, können sie doch als Maßstab dafür angesehen werden, was nach dem allgemein anerkannten Stand der medizinischen Wissenschaft zur Feststellung der Identität „erforderlich“, aber auch ausreichend ist. Damit wird auch die Grenze für die Erforderlichkeit im Sinne des Transfusionsgesetzes gezogen. Daten des Personalausweises dürfen demnach zwar durch Einsichtnahme in das Dokument erhoben (gelesen), nicht aber gespeichert werden. Die Rückverfolgung einer Blutspende ist also nach Meinung der Richtliniengeber auch ohne diese Angabe gewährleistet.

Wir baten deshalb den Blutspendedienst, künftig von einer Speicherung der Personalausweisnummer abzusehen und das Verfahren entsprechend zu ändern.

8.4 Zugriff von Betriebsärzten eines überbetrieblichen Dienstes auf Gesundheitsdaten von Arbeitnehmern

Das Arbeitssicherheitsgesetz (ASiG) verpflichtet Arbeitgeber dazu, Betriebsärzte zu bestellen, soweit dies im Hinblick auf die Betriebsart und die damit für die Arbeitnehmer verbundenen Unfall- und Gesundheitsgefahren, die Zahl der beschäftigten Arbeitnehmer und die Zusammensetzung der Arbeitnehmerschaft sowie die Betriebsorganisation erforderlich ist (§ 2 ASiG). Die Betriebsärzte sollen den Arbeitgeber beim Arbeitsschutz und bei der Unfallverhütung unterstützen. Ihre Bestellung hat schriftlich zu erfolgen. Ihnen sind die im Gesetz genannten Aufgaben – soweit erforderlich – zu übertragen (§ 3 ASiG). Zu ihren Aufgaben gehört unter anderem, die Arbeitnehmer zu untersuchen, arbeitsmedizinisch zu beurteilen und zu beraten sowie die Untersuchungsergebnisse zu erfassen und auszuwerten. Die Betriebsärzte verarbeiten besonders sensible Gesundheitsdaten im Sinne des § 3 Abs. 9 BDSG. Es ist daher sehr wichtig, dass Betriebsärzte die ihnen obliegende Schweigepflicht, die auch gegenüber dem Arbeitgeber gilt, strikt einhalten.

Der Arbeitgeber kann seine Pflicht, Betriebsärzte zu bestellen, auch dadurch erfüllen, dass er einen überbetrieblichen Dienst von Betriebsärzten zur Wahrnehmung der Aufgaben verpflichtet (§ 19 ASiG). Ein großes Dienstleistungsunternehmen im Bereich des Arbeitsschutzes – ein „überbetrieblicher Dienst“ im Sinne

des ASiG, das bundesweit über zahlreiche Niederlassungen verfügt – wandte sich im Zusammenhang mit dem geplanten Einsatz einer arbeitsmedizinischen Software mit der Frage an uns, ob jeweils alle Betriebsärzte einer Niederlassung die Daten aller Arbeitnehmer sämtlicher Kunden auf ihrem Laptop haben dürfen und zwar auch dann, wenn ein Betriebsarzt nur einen Teil der Kunden des Unternehmens betreut. Hierfür spreche zum einen, dass immer wieder Vertretungssituationen einträten und zum anderen die Tatsache, dass manche Kunden aufgrund ihrer Größe von mehreren Betriebsärzten betreut würden.

Wir haben die Frage im Ergebnis verneint. Der überbetriebliche Dienst übernimmt im Falle seiner Verpflichtung die dem Arbeitgeber in § 2 ASiG zugewiesenen Aufgaben, einen (oder mehrere) geeignete(n) Betriebsarzt (Betriebsärzte) für den Auftraggeber auszuwählen und diesem (diesen) die Wahrnehmung der im Arbeitssicherheitsgesetz genannten Aufgaben zu übertragen. Das sieht auch das von der Verwaltungs-Berufsgenossenschaft (VBG) – gesetzliche Unfallversicherung – herausgegebene Muster eines Vertrags mit einem überbetrieblichen Dienst so vor. Es enthält zusätzlich die Bestimmung, dass der ausgewählte Betriebsarzt in dem erforderlichen Umfang zum Auftraggeber abgeordnet wird. Damit werden allein dem abgeordneten Betriebsarzt und nicht dem überbetrieblichen Dienst als solchem die vorhandenen ärztlichen Unterlagen beziehungsweise Daten über die beim Auftraggeber beschäftigten Arbeitnehmer anvertraut. Der abgeordnete Betriebsarzt hat die ärztliche Schweigepflicht zu wahren (§ 8 Abs. 1 Satz 3 ASiG). Diese ist im Verhältnis zum Auftraggeber, aber auch im Verhältnis zu anderen, beim überbetrieblichen Dienst beschäftigten Ärzten zu beachten. Das heißt, dass die anderen Betriebsärzte nicht auf diese Daten zugreifen dürfen. Dies ist durch organisatorische und technische Maßnahmen nach § 9 BDSG und der Anlage hierzu sicherzustellen. Hat der überbetriebliche Dienst mehrere Betriebsärzte zu einem Auftraggeber entsandt, kommt es für die Frage der Zugriffsbefugnis darauf an, ob jeder allein zuständig ist oder die Aufgaben aufgeteilt sind. Ist ein entsandter Betriebsarzt verhindert, kann der überbetriebliche Dienst nach der vorliegenden Mustervereinbarung ab diesem Zeitpunkt für die Dauer der Vertretung auf die medizinischen Daten der Arbeitnehmer dieses Auftraggebers zugreifen. Auch dies ist durch entsprechende technische und organisatorische Maßnahmen sicherzustellen.

Wir haben dem anfragenden Unternehmen dringend empfohlen, entsprechende Regelungen in seine Verträge aufzunehmen und im Übrigen auch die Entsendung von Betriebsärzten zu regeln, was bisher – abweichend von der uns vorliegenden Mustervereinbarung – nicht geschehen war.

Für klärungsbedürftig halten wir einige weitere datenschutzrechtliche Fragen, insbesondere die der datenschutzrechtlichen Verantwortlichkeit im Verhältnis zwischen überbetrieblichem Dienst und dem jeweiligen Auftraggeber sowie die Unterrichtung der Arbeitnehmer über den für sie zuständigen Betriebsarzt und den Eintritt eines Vertretungsfalls. Darüber stehen wir mit dem Unternehmen noch im Gespräch.

8.5 Nutzung von Patientendaten für Werbezwecke

Eine Bürgerin wandte sich empört an uns, weil sie ein Werbeschreiben einer ihr unbekannten Rehaklinik erhalten hatte. Darin informierte die Rehaklinik darüber, dass Ärzte und Therapeuten einer anderen Klinik, in der die Beschwerdeführerin einige Zeit zuvor stationär behandelt worden war, inzwischen teilweise bei ihr arbeiteten. Die Beschwerdeführerin wollte wissen, woher die Rehaklinik ihre Adresse hat. Die Prüfung ergab Folgendes:

Die Rehaklinik hat für die Werbeaktion Patientendaten genutzt, die ein Mitarbeiter der Rehaklinik von seinem früheren Arbeitgeber – der Klinik, in der die Betroffene behandelt wurde – bei seinem Arbeitsplatzwechsel unberechtigt mitgenommen hatte. Die Daten der Betroffenen waren dort ausschließlich für Behandlungs- und Abrechnungszwecke erhoben und gespeichert worden.

Für das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten – hierzu gehören unter anderem Angaben zur Gesundheit, beispielsweise auch die Behandlung in einem Krankenhaus – gelten besondere datenschutzrechtliche Anforderungen. Diese wurden von der Rehaklinik nicht beachtet. Sie

hat die Daten ohne rechtliche Grundlage für Zwecke der Werbung verarbeitet. Eine Einwilligung der Betroffenen in die Datenverarbeitung konnte nicht nachgewiesen werden. Fehlerhaft war schließlich, dass die Betroffene auch nicht entsprechend den gesetzlichen Vorgaben auf die Möglichkeit des Werbewiderspruchs hingewiesen worden war. Wir beanstandeten deshalb die Verfahrensweise der Rehaklinik.

Ein gegen den Mitarbeiter, der bei seinem früheren Arbeitgeber unberechtigt Patientendaten mitgenommen hatte, eingeleitetes staatsanwaltschaftliches Ermittlungsverfahren wegen Verstoßes gegen das Bundesdatenschutzgesetz wurde mit Zustimmung des Amtsgerichts gegen Zahlung eines Geldbetrags eingestellt.

8.6 Übermittlung von Patientendaten an Krankenkassen

Eine Krankenkasse beschwerte sich bei der Aufsichtsbehörde darüber, dass ihr ein Arzt, der sich über ihr Verhalten bei der Kostenübernahme von Gutachten beschwert hatte, nicht nur Patientendaten der bei ihr Versicherten, sondern auch Namen, Geburtsdaten und Hausarztdaten von Versicherten einer anderen Krankenkasse mitgeteilt hatte.

Die Krankenkasse hatte recht. Schon der Name eines Patienten und die Tatsache, dass er in ärztlicher Behandlung beziehungsweise in Behandlung eines bestimmten Arztes ist, unterliegen der ärztlichen Schweigepflicht. Es handelt sich außerdem um datenschutzrechtlich besonders geschützte sensible Gesundheitsdaten. Der Arzt hat durch den Versand der Patientenliste an eine nicht beteiligte Krankenkasse unberechtigt Daten an Dritte übermittelt, weil es hierfür keine gesetzliche Grundlage gab und die Betroffenen auch nicht eingewilligt hatten.

Wir haben den Arzt unter Hinweis auf die Rechtslage aufgefordert, künftig den Schutz der Patientendaten zu beachten.

8.7 Aufbewahrung von Patientenakten in einer öffentlichen Tiefgarage

Nicht alltäglich war ein bei der Aufsichtsbehörde eingegangener Hinweis, in einer Tiefgarage seien Patientenakten gefunden worden. Was war geschehen?

Eine Arztpraxis hatte im als privat gekennzeichneten Teil einer öffentlichen Tiefgarage, die sich inmitten einer Großen Kreisstadt befindet, einen Abstellraum gemietet und zur Aufbewahrung von Patientenakten genutzt. Der Abstellraum wurde bauseits durch die Montage von Hohlmetallprofilen mit einem Abstand von circa 5 cm auf einer Metallkonstruktion errichtet und durch eine mit einem Schloss gesicherte Tür abgeschlossen. In dem Raum waren etwa fünfzig Kartons mit Röntgenunterlagen und zwei Blechschränke mit Patientenblättern gelagert. Eine unbekannte Person hatte die Metallprofile so beschädigt, dass es möglich war, in den Abstellraum hineinzugreifen und einige Patientenunterlagen daraus zu entfernen.

Datenschutzrechtlich ist dies wie folgt zu bewerten:

Patientendaten sind nach dem Bundesdatenschutzgesetz besonders geschützt, darüber hinaus unterliegen sie der ärztlichen Schweigepflicht. Ärzte sind – ebenso wie die anderen nichtöffentlichen Stellen – verpflichtet, die erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen, um personenbezogene Daten vor unbefugter Kenntnisnahme zu schützen. Da es sich um besonders schutzbedürftige Daten handelt, müssen bei Patientenakten auch die Sicherungsmaßnahmen entsprechend hoch sein. Es muss auch ein angemessener Schutz gegen Kenntniserlangung mittels strafbarer Handlungen bestehen.

Bei einer Abstellkammer mit nicht geschlossenen Außenwänden in einer öffentlichen Tiefgarage sind diese Voraussetzungen auch wegen des hohen Risikos der Beschädigung und der Vernichtung der Patientenakten nicht erfüllt.

Nachdem die Presse ausführlich über den Vorgang berichtet hatte, war es vollends unmöglich geworden, die Unterlagen in der Tiefgarage zu belassen. Auch zusätzliche Sicherungsmaßnahmen halfen hier nicht weiter. Die Aufsichtsbehörde hat deshalb die Arztpraxis aufgefordert, die Patientenunterlagen an einen sicheren Ort zu bringen. Dies geschah auch.

8.8 Datenschutz beim Sammeln von Spenden

Aufgrund einer Bürgerbeschwerde haben wir uns mit datenschutzrechtlichen Fragen bei Haussammlungen befasst. Ein Spender wollte nicht, dass andere um eine Spende gebetene Personen durch Einsichtnahme in die Sammellisten des Sammlers feststellen können, dass und wie viel er gespendet hat. Er beklagte sich darüber, dass Spendensammler solche Listen dazu benutzten, andere potenzielle Spender zu möglichst hohen Spenden zu animieren.

Die Verwaltungsvorschrift des Ministeriums für Arbeit und Soziales zur Durchführung des Sammlungsgesetzes vom 30. November 2005 (GABl. 2006 S. 158) enthält hierzu folgende Regelung:

> „Die (Sammel-)Listen müssen auf der ersten Seite den Namen des Veranstalters und des Sammlers sowie Sammlungsort, -zeit und -zweck enthalten. ... Die folgenden Seiten müssen Spalten für Namen und Wohnung des Spenders, den Spendenbetrag und die Unterschrift des Spenders enthalten. Die Sammler sind darüber zu belehren, dass eine Unterschrift des Spenders nicht gefordert werden darf und dass der Sammler den Namen des Spenders auch nicht ohne dessen ausdrückliche Einwilligung eintragen darf. Der gespendete Betrag muss jedoch in jedem Fall mit Tintenstift oder Kugelschreiber in die Liste eingetragen werden. ...“.

Diese Regelung lässt das Bemühen des Sozialministeriums erkennen, dem Datenschutz bei der Durchführung von Haussammlungen angemessen Rechnung zu tragen, ohne die korrekte Erfassung der Spenden aufzugeben. Wir haben jedoch angeregt, die Verwaltungsvorschrift in zwei Punkten zu ändern:

- Die Anonymität eines Spenders ist nicht bereits dann gewährleistet, wenn auf die Angabe seines Namens und seiner Unterschrift verzichtet wird. Unter Umständen lässt sich auch aus der Angabe der Wohnung auf seinen Namen schließen. Dem Spender sollte daher die Angabe der Wohnung freigestellt werden.
- Die Sammler sollten dazu verpflichtet werden, die (potenziellen) Spender über den Zweck der Erhebung, Verarbeitung und Nutzung ihrer Daten zu unterrichten und sie insbesondere darauf hinzuweisen, dass ihre Daten in Sammellisten erfasst werden, in die jeder Einsicht nehmen kann (§ 4 Abs. 3 BDSG). Sie sollten ferner von sich aus den Spender darüber informieren, dass die Angabe von Name und Wohnung und die Unterschrift freiwillig sind.

8.9 Nutzung eines Notruf-Ortungssystems durch Rettungsleitstellen

Eine private Notfallhilfe bietet den Rettungsleitstellen, die Notrufe über die Notrufnummer 112 entgegennehmen, ein Notruf-Ortungssystem für Mobilfunkgeräte an, das die Ermittlung des Standorts von Mobilfunkteilnehmern ermöglicht. Dabei spielt es keine Rolle, ob das Mobilfunkgerät mit der Location Based Service (LBS) Technik oder der Global Position System (GPS) Technik ausgerüstet ist. Mobilfunkgeräte mit satellitengestütztem GPS ermöglichen eine sehr genaue Ortung des Standortes. Bei Geräten mit LBS-Technik, heute noch in der Mehrzahl, ist die Genauigkeit der Standortbestimmung abhängig von den Mobilfunkzellen des Mobilfunkdienstanbieters.

Damit die Rettungsleitstellen diesen Dienst nutzen können, müssen sie einen Rahmenvertrag mit der privaten Nothilfe abschließen. Der Rahmenvertrag beinhaltet auch datenschutzrechtliche Regelungen, die von den Rettungsleitstellen bei der Ortung zu beachten sind.

Nach dem Telekommunikationsgesetz dürfen nur Mobilfunkteilnehmer geortet werden, die vorab ihre Einwilligung in die Verarbeitung von Standortdaten gegeben haben. Für Mobilfunkteilnehmer, die sich bei der privaten Nothilfe haben registrieren lassen, liegen diese Einwilligungen vor. Sie werden den Leitstellen bei Ortungsabfragen angezeigt. Liegt keine Einwilligung vor, ist der Disponent der Leitstelle vor Durchführung der Ortung verpflichtet, den Anrufer zu fragen, ob er zur Durchführung der Notfallrettung mit einer Standortbestimmung einverstanden ist. Ist der Anrufer nicht in der Lage, diese Einwilligung zu erteilen, kann der Disponent der Leitstelle bei vermuteter Gefahr für Leib und Leben die Ortung des

Anrufers dennoch durchführen. Für diesen Fall ist es erforderlich, dass der Disponent wegen der fehlenden Einwilligung die durchgeführte Ortung in einem Logbuch dokumentiert. Der Rahmenvertrag geht noch einen Schritt weiter, indem er für jede Ortungsabfrage einen Eintrag in das Logbuch vorschreibt. Auch muss der Datenschutzbeauftragte der Rettungsleitstelle durch Stichproben nachprüfen, ob die Ortungsabfrage ordnungsgemäß genutzt wird.

Die Abfragen der Rettungsleitstellen zur Bestimmung des Standorts des Mobilfunkteilnehmers sind nach § 32 Abs. 1 Nr. 1 des Rettungsdienstgesetzes zulässig, da sie zur Durchführung der Notfallrettung einschließlich der Versorgung des Patienten erforderlich sind.

Sofern Rettungsleitstellen die von ihnen vertraglich übernommenen Verpflichtungen einhalten, insbesondere Abfragen ohne Einwilligung des Betroffenen im Logbuch dokumentieren, und dies auch kontrollieren (lassen), ist gegen eine Nutzung der Ortungsplattform der privaten Nothilfe nichts einzuwenden.

9 Arbeitnehmerdatenschutz

9.1 Übermittlung von Sozialdaten an den Betriebsrat im Rahmen einer betriebsbedingten Kündigung

Ein Unternehmen hatte gegenüber einer Arbeitnehmerin eine betriebsbedingte Kündigung ausgesprochen. In diesem Zusammenhang wurde die Frage an uns herangetragen, ob das Unternehmen zu Recht personenbezogene Daten Dritter an die gekündigte Arbeitnehmerin übermittelt hatte.

Nach § 1 Abs. 3 des hier anwendbaren Kündigungsschutzgesetzes muss der Arbeitgeber im Falle betriebsbedingter Kündigungen bei der Auswahl des Arbeitnehmers soziale Gesichtspunkte ausreichend berücksichtigen; er muss also eine Sozialauswahl vornehmen. Auf Verlangen des Arbeitnehmers muss der Arbeitgeber ihm die Gründe für die getroffene Sozialauswahl nennen. Der Arbeitgeber muss angeben, welche Arbeitnehmer weshalb zum auswahlrelevanten Personenkreis gehören. Auswahlkriterien sind in erster Linie Lebensalter, Dauer der Betriebszugehörigkeit und Unterhaltsverpflichtungen. Damit will das Gesetz dem Arbeitnehmer, der Mängel bei der sozialen Auswahl beweisen muss, die Nachprüfung erleichtern, ob er eine betriebsbedingte Kündigung mit Aussicht auf Erfolg angreifen kann. Im datenschutzrechtlichen Sinn handelt es sich dabei um eine Übermittlung personenbezogener Daten der in die Auswahl einbezogenen Mitarbeiter.

Im vorliegenden Fall wurden der gekündigten Arbeitnehmerin bereits im Kündigungsschreiben die Sozialdaten des Personenkreises mitgeteilt, der offensichtlich auswahlrelevant war. Im Anschluss daran wurde ausgeführt, dass „... unter Berücksichtigung der aufgelisteten Sozialdaten aller beschäftigten Mitarbeiter ... eine Kündigung unter dem Aspekt der Sozialverträglichkeit und Schutzbedürftigkeit möglich ...“ sei. Als Anlage erhielt die gekündigte Arbeitnehmerin die Stellungnahme des Betriebsrats, der der Kündigung widersprochen hatte. In dieser war aufgeführt, dass der Betriebsrat die Durchführung einer ordnungsgemäßen Sozialauswahl mit Nichtwissen bestreite.

Das Unternehmen hat uns gegenüber dargetan, dass eine Sozialauswahl stattgefunden habe und diese auch gegenüber dem Betriebsrat dargelegt worden sei. Das entsprechende Schreiben wurde uns vorgelegt.

Die Verfahrensweise des Unternehmens war im konkreten Fall nicht zu beanstanden. Zwar waren die Voraussetzungen des § 1 Abs. 3 des Kündigungsschutzgesetzes nicht gegeben, da die Sozialdaten der in die Sozialauswahl einbezogenen Arbeitnehmer bereits im Kündigungsschreiben offen gelegt wurden, ohne dass die gekündigte Arbeitnehmerin dies verlangt hatte. Das Kündigungsschutzgesetz normiert aber lediglich die *Verpflichtung* des Arbeitgebers, die Gründe anzugeben, die zu der getroffenen Sozialauswahl geführt haben und die entsprechenden Daten zu übermitteln.

Eine Übermittlungsbefugnis kann sich darüber hinaus aus den Bestimmungen des Bundesdatenschutzgesetzes ergeben. Nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist das Übermitteln personenbezogener Daten als Mittel für die Erfüllung eigener Ge-

schäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Nutzung überwiegt.

Die Übermittlung der Daten diente dazu, gegenüber der gekündigten Arbeitnehmerin nachzuweisen, dass eine Sozialauswahl durchgeführt worden war. Dazu bestand Anlass, nachdem der Betriebsrat hieran Zweifel geäußert und das Unternehmen der gekündigten Arbeitnehmerin diese Stellungnahme – wie in § 102 Abs. 4 des Betriebsverfassungsgesetzes vorgeschrieben – zugesandt hatte. Die Übermittlung der Daten der in die Sozialauswahl einbezogenen anderen Arbeitnehmerinnen war daher bereits zu diesem Zeitpunkt erforderlich, um weitere rechtliche Auseinandersetzungen darüber, ob eine Sozialauswahl durchgeführt worden war, zu vermeiden. Überwiegende schutzwürdige Belange der betroffenen Mitarbeiterin standen nicht entgegen, da das Unternehmen auf Anforderung der gekündigten Arbeitnehmerin diese Daten ohnehin hätte übermitteln müssen.

Es ist aber festzuhalten, dass es sich hierbei um einen besonders gelagerten Fall handelt. Im Regelfall ist eine Übermittlung der Sozialdaten nur auf Verlangen des gekündigten Arbeitnehmers zulässig.

9.2 Telefondatenerfassung durch den Arbeitgeber

Ein Unternehmen wandte sich mit folgender Frage an die Aufsichtsbehörde: Ein Mitarbeiter des Unternehmens hatte einen Einzelverbindungsnachweis für seinen Telefonanschluss angefordert, um sowohl gegenüber seinem Arbeitgeber als auch gegenüber einem Kunden nachweisen zu können, dass er an einem bestimmten Tag mit einem Mitarbeiter des Kunden telefoniert hatte, was dieser bestritt. Das anfragende Unternehmen wollte wissen, ob es berechtigt ist, dem Mitarbeiter die gewünschten Daten zu Verfügung zu stellen beziehungsweise inwieweit der Angerufene durch das Fernmeldegeheimnis geschützt wird.

Da keine weiteren Einzelheiten mitgeteilt wurden, haben wir die Anfrage abstrakt beantwortet. Es ist danach zu differenzieren, ob der Teilnehmer sein Telefon nur betrieblich oder auch privat nutzen darf. Letzteres kann vom Arbeitgeber ausdrücklich oder konkludent gestattet worden sein oder auf einer betrieblichen Übung beruhen.

Soweit nur die betriebliche Nutzung gestattet ist, darf der Arbeitgeber grundsätzlich die von jeder Nebenstelle dienstlich verursachten Kosten aufgeschlüsselt nach Zeitpunkt und Dauer festhalten. Ob die komplette Zielnummer gespeichert werden darf, wird unterschiedlich beantwortet. *Maßstab ist allein das Bundesdatenschutzgesetz.* Erfolgte im konkreten Fall eine Speicherung der vollständigen Zielnummern, darf der Arbeitgeber mit Einwilligung des betroffenen Mitarbeiters Einzelverbindungsnachweise zu dem betreffenden Tag darauf auswerten, ob darin die entsprechende Zielnummer enthalten ist.

Ist auch *die private Nutzung* gestattet, unterliegt der Arbeitgeber dem *Telekommunikationsgesetz* (TKG). Er muss nach § 85 Abs. 1 TKG das *Fernmeldegeheimnis* aller beteiligten Personen wahren. Lassen sich die Daten der betrieblichen und der privaten Nutzung auch technisch voneinander trennen, was beispielsweise durch Vorwahl eines bestimmten Codes erfolgen kann, gilt das Telekommunikationsgesetz nur für die private Nutzung. Ist eine solche Trennung nicht möglich, findet das Telekommunikationsgesetz auf den gesamten Datenverkehr Anwendung.

Das Fernmeldegeheimnis schützt nicht nur den Inhalt der Telekommunikation, sondern auch ihre näheren Umstände, insbesondere auch die Tatsache, dass jemand an einem Telekommunikationsvorgang beteiligt war. Bezogen auf Telefongespräche bedeutet dies, dass lediglich die Daten festgehalten und verwertet werden dürfen, die für die Abrechnung erforderlich sind. Das Festhalten der unverkürzten Rufnummer ist daher auf jeden Fall unzulässig, nach einer weitergehenden, wohl herrschenden Ansicht, darf die Zielnummer bei privaten Gesprächen insgesamt nicht festgehalten werden. Da das Fernmeldegeheimnis beide Gesprächsteilnehmer schützt und – sollte die ungekürzte Zielrufnummer gespeichert worden sein – dies in unzulässiger Weise erfolgte, ist eine weitere Nutzung der Daten in diesem Fall problematisch.

Eine Überprüfung der Verbindungsdaten in Bezug auf die ungekürzte Rufnummer wäre in diesem Fall allenfalls dann möglich, wenn sowohl der betroffene Mitarbeiter als auch der Mitarbeiter des Kunden, der die Tatsache eines Telefongespräches in Abrede stellt, als auch alle weiteren Telefongesprächspartner von diesem Tag hierin einwilligen. Dann könnte der Arbeitgeber die Verbindungsdaten für den Tag X nach der relevanten Rufnummer durchsuchen lassen.

9.3 Gesprächsaufzeichnung in Call-Centern

Im Rahmen unserer Besuche bei Call-Centern haben wir festgestellt, dass während der Einarbeitungsphase oder auch bei Nachschulungen die Telefonate der in Call-Centern Beschäftigten zu Schulungszwecken und Qualitätssicherungsmaßnahmen mitgehört und beziehungsweise oder aufgezeichnet werden. Dabei spielt es keine Rolle, ob die Gesprächsführung vom Call-Center weg (outbound) oder zum Call-Center hin (inbound) erfolgt.

Die Schulungs- und Qualitätssicherungsmaßnahmen werden entweder so durchgeführt, dass

- das vom Beschäftigten und vom Kunden gesprochene Wort durch eine Kontrollperson am Arbeitsplatz unter Nutzung eines Kopfhörers offen mitgehört wird oder
- das vom Beschäftigten gesprochene Wort ohne direkte Anwesenheit einer Kontrollperson am Arbeitsplatz durch Aufschalten mitgehört wird, wobei der Beschäftigte und die Kunden hierbei unmittelbar über das Mithören informiert werden.

Bei einigen Call-Centern werden die Beschäftigten mittels eines Formblatts, das zusammen mit dem Arbeitsvertrag ausgehändigt wird, über die Möglichkeiten des Mithörens generell informiert. Darin steht in der Regel, dass sich der Call-Center-Betreiber vorbehält, dienstliche Telefongespräche zu Schulungszwecken mitzuhören und aufzuzeichnen. Die Beschäftigten sollen das Formblatt zur Kenntnis nehmen und ihre unbefristete Zustimmung in das Mithören und Aufzeichnen von dienstlichen Telefongesprächen erteilen.

Aus datenschutzrechtlicher Sicht haben wir dies wie folgt beurteilt:

Der Persönlichkeitsschutz des Arbeitnehmers setzt auch dem *offenen Mithören von geschäftlichen Telefongesprächen* durch den Arbeitgeber Grenzen. Zu den Schutzgütern zählt das Recht am eigenen Wort. Dieses umfasst die Befugnis, darüber zu bestimmen, ob das gesprochene Wort nur dem Gesprächspartner zugänglich sein soll oder auch von Dritten mitgehört werden kann. Eingriffe des Arbeitgebers in das Recht des Arbeitnehmers am gesprochenen Wort sind nur zulässig, soweit im Einzelfall dem Interesse des Arbeitgebers Vorrang vor demjenigen des Arbeitnehmers gebührt. Aufgrund dieser Interessenabwägung kann der Eingriff nur gerechtfertigt sein, wenn er nach Inhalt, Form und Begleitumständen nicht nur erforderlich ist, sondern auch das schonendste Mittel zur Erreichung eines rechtlich gebilligten Zwecks des Arbeitgebers darstellt. Diese Voraussetzungen hat das Bundesarbeitsgericht jedenfalls dann bejaht, wenn das Mithören dem Anlernen des Beschäftigten dient und während der Anlernzeit (Probezeit) erfolgt.

Darüber hinaus halten wir das offene Mithören für zulässig, wenn es durch überwiegende Firmeninteressen gerechtfertigt ist. Es muss sich jedoch auf Einzelfälle, auf gelegentliche Stichproben, beschränken oder anlassbezogen erfolgen.

Die Betroffenen müssen in einem Informationsblatt über die generelle Verfahrensweise des Arbeitgebers informiert werden.

Unter diesen Voraussetzungen ist das offene Mithören eines von einem Arbeitnehmer geführten Telefonats durch § 28 Abs. 1 Satz 1 Nr. 2 BDSG gedeckt. Einer Einwilligung bedarf es nicht. Sie wäre aus Sicht der Aufsichtsbehörde auch nicht wirksam, weil sie dem Betroffenen vor Abschluss eines Arbeitsvertrags abverlangt wird. Er hätte hinsichtlich der Abgabe der Erklärung nur die Wahl hat, entweder zuzustimmen oder auf die Eingehung des Arbeitsvertrags zu verzichten. Die Einwilligung würde daher nicht – wie es § 4 a Abs. 1 Satz 1 BDSG verlangt – auf der freien Entscheidung des Betroffenen beruhen.

Selbstverständlich ist, dass der *Kunde*, also der Gesprächspartner des überwachten Arbeitnehmers, stets über die Tatsache des Mithörens *vor Beginn* des Ge-

sprächs *informiert* wird. Lässt er sich in Kenntnis dessen auf das weitere Gespräch ein, ist von seiner konkludenten Einwilligung auszugehen.

Das *heimliche Mithören von Telefongesprächen des Arbeitnehmers* ist nach dem Grundsatz der Erforderlichkeit und der Verhältnismäßigkeit und in Fortführung der obigen Anführungen nur zulässig, wenn gerade für diese Form ein legitimierender Grund beziehungsweise Anlass besteht, beispielsweise offensichtliche Qualitätsmängel, wiederholte Kundenbeschwerden. Es ist von einer Stufenfolge im Verhältnis zwischen offenem und heimlichem Mithören auszugehen. Das heimliche Mithören ist nur während eines engen Zeitfensters zulässig; der betroffene Arbeitnehmer ist vorher über die Maßnahme zu informieren, ohne dass man ihm sagt, welche konkreten Gespräche mitgehört werden. Je nachdem, ob sich aus der Maßnahme Beanstandungen des Verhaltens des Arbeitnehmers ergeben oder nicht, ist das Ergebnis bei künftigen Maßnahmen in die Abwägung mit einzubeziehen. Im Informationsblatt sollte die Verfahrensweise in genereller Form beschrieben sein. Hinsichtlich der Einwilligung gilt das zuvor Gesagte.

Der *Kunde* muss auch über das heimliche Mithören eines Gesprächs in jedem Fall vorher informiert werden.

Die *Aufzeichnung von Telefongesprächen* ist nur unter den für das heimliche Mithören geltenden Voraussetzungen zulässig. Die Aufzeichnungen sind unverzüglich zu löschen, wenn sich kein Grund für eine Beanstandung ergeben hat. Ansonsten dürfen sie nur im Rahmen des Erforderlichen aufbewahrt werden.

Sogenannte *Mystery-Calls* [4)] dürfen nicht aufgezeichnet, sondern allenfalls auf einem Gesprächsbogen dokumentiert und ausgewertet werden.

Diese Grundsätze wurden im Düsseldorfer Kreis abgestimmt.

9.4 Zusendung einer Arbeitgeberzeitschrift an die Privatadressen der Mitarbeiter

Seit vielen Jahren müssen sich die Aufsichtsbehörden in Deutschland immer wieder mit der Frage befassen, ob es zulässig ist, eine Arbeitgeberzeitschrift an die Privatadressen von Mitarbeitern zu senden.

Zielrichtung der von einem Verlag herausgegebenen, 14-tägig erscheinenden Zeitung ist es, Arbeitnehmer über Entwicklungen in den eigenen Unternehmen sowie diversen Wirtschaftsbranchen und -unternehmen zu informieren. Auch sollen ihnen Auffassungen von Arbeitgebern und ihren Verbänden zu grundsätzlichen, das Arbeitsleben und die Wirtschafts- und Gesellschaftspolitik betreffenden Fragen vermittelt werden. Der Verlag versendet die Zeitschrift auf Veranlassung der Arbeitgeber, die die Zeitschrift abonniert haben, an die Privatanschriften der Arbeitnehmer. Diese erhält er von den Arbeitgebern. Es ist vertraglich vereinbart, dass der Verlag die Adressdaten „im Auftrag“ der Arbeitgeber verarbeitet. Ein geringer Teil der Auflage wird in den Unternehmen ausgelegt.

Erneut an uns herangetragen wurde die Zulässigkeitsfrage von dem Betriebsrat eines Unternehmens, das plante, die Zeitschrift nicht mehr im Betrieb auszulegen, sondern sie allen Beschäftigten nach Hause zusenden zu lassen. Der Betriebsrat hatte Bedenken gegen die Verwendung der Arbeitnehmeradressen. Er sah diese auch nicht dadurch ausgeräumt, dass das Unternehmen den Mitarbeitern Gelegenheit geben wollte, der Zusendung zu widersprechen.

Wir vertreten hierzu folgende Ansicht:

Die Versendung der Zeitschrift an die Privatadressen der Arbeitnehmer stellt eine Datennutzung dar. § 28 Abs. 1 Satz 1 Nr. 1 BDSG gestattet eine solche nur dann, wenn es der Zweckbestimmung des konkreten Arbeitsverhältnisses dient. Diese Voraussetzungen liegen nicht vor. Die Übersendung der Zeitschrift steht in keinem hinreichenden Zusammenhang mit dem konkreten Arbeitsvertrag. Der Inhalt der Zeitschrift hat in der Regel noch nicht einmal einen Bezug zu einzelnen Unternehmen. Insbesondere stellt die Zusendung der Zeitschrift keine arbeitsvertragliche Nebenpflicht des Arbeitgebers dar.

[4)] Darunter versteht man Testanrufe von Scheinkunden, die dem Zweck dienen, das Verhalten der Mitarbeiter beziehungsweise die Qualität ihres Services zu überprüfen.

Die Datennutzung ist auch nicht durch § 28 Abs. 1 Satz 1 Nr. 2 BDSG gedeckt. Danach ist das Übermitteln personenbezogener Daten zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen an dem Ausschluss der Übermittlung überwiegen. Dieser Zulässigkeitstatbestand kann bei Bestehen eines Arbeitsverhältnisses neben § 28 Abs. 1 Satz 1 Nr. 1 BDSG zur Anwendung kommen, ist dann aber eng auszulegen. Der Arbeitgeber hat im vorliegenden Fall sicher ein berechtigtes Interesse daran, aus seiner Sicht bedeutsame Themen an seine Mitarbeiter heranzutragen. Dazu ist es jedoch nicht erforderlich, die Zeitschrift an die Privatadressen der Mitarbeiter zu senden.

Das betroffene Unternehmen hat sich auf die Argumente eines Rechtsgutachtens gestützt, das die Frage der Zulässigkeit des Versands der Zeitung bejaht hat. In diesem wird die Erforderlichkeit der Nutzung der Privatadressen damit begründet, dass der Direktversand der effizienteste Weg der Informationsverschaffung ist. Dadurch werde gewährleistet, dass sich der Mitarbeiter näher mit der Zeitschrift befasse. Lege man diese im Unternehmen aus, ließe sich der eine oder andere Arbeitnehmer unter Umständen davon abhalten, ein Exemplar an sich zu nehmen. Er müsse fürchten, dabei von Kollegen beobachtet zu werden und sich unter Umständen in eine Konfliktsituation zu Betriebsräten beziehungsweise Gewerkschaftern zu begeben. Außerdem könne das Auslegen der Zeitschrift die Mitarbeiter zur unerwünschten Lektüre während der Arbeitszeit verleiten. Presseerzeugnisse könnten auch intensiver konsumiert werden, wenn für die Durchsicht ausreichend Zeit zur Verfügung stünde, was erfahrungsgemäß im häuslichen Bereich eher der Fall sei als im Betrieb.

Dieser Argumentation kann nicht gefolgt werden. Es liegt eine Alternative zum Direktversand vor. Der Arbeitgeber kann die Zeitschrift im Betrieb auslegen, sodass auf die Adressennutzung verzichtet werden kann. Diese Alternative ist dem Arbeitgeber auch zumutbar. Der Arbeitnehmer kann die Zeitschrift in diesem Fall bei Interesse problemlos mit nach Hause nehmen und sie dort eingehend lesen. Dass ein Arbeitnehmer die Zeitschrift nicht am Arbeitsplatz während der Arbeitszeit lesen darf, kann der Arbeitgeber bei Bedarf klarstellen und bei Verstoß unterbinden. Dies kann einem Arbeitgeber auch abverlangt werden.

Die Nutzung der Anschriften ist daher nicht als erforderlich anzusehen.

Zudem überwiegen auch die schutzwürdigen Interessen der Betroffenen am Ausschluss der Nutzung. Der Arbeitnehmer soll sich darauf verlassen können, dass seine Daten nur für den Zweck verwendet werden, zu dem er sie dem Arbeitgeber als seinem Vertragspartner gegeben hat. Die von dem betroffenen Unternehmen in Erwägung gezogene Widerspruchsmöglichkeit ist abzulehnen. Aufgrund des Abhängigkeitsverhältnisses besteht die Gefahr, dass sich der Arbeitnehmer bei einem Direktversand und der damit verbundenen Nutzung seiner Daten durch den Arbeitgeber scheut, der Nutzung seiner Daten zu widersprechen. Auch dass der Arbeitnehmer die Zeitschrift ungelesen entsorgen kann, wenn er sie in seinem Briefkasten vorfindet, schließt eine Beeinträchtigung seiner schutzwürdigen Interessen nicht aus. Die Datennutzung ist nämlich in diesem Zeitpunkt bereits erfolgt.

Die Bedenken werden auch nicht dadurch ausgeräumt, dass man dem Arbeitnehmer ein Widerspruchsrecht gegenüber dem Verlag einräumt, ohne dass der Arbeitgeber hiervon erfahren soll. Es erscheint bereits zweifelhaft, ob eine derartige Vereinbarung noch mit der gesetzlichen Regelung über die Auftragsdatenverarbeitung in Einklang stünde. Im Übrigen würde die Einräumung einer Widerspruchsmöglichkeit nichts daran ändern, dass es bereits an der Erforderlichkeit der Datennutzung fehlt.

Eine Nutzung der Arbeitnehmerdaten ist daher nur mit Einwilligung des Betroffenen zulässig, wobei die Freiwilligkeit der Erteilung der Einwilligung sichergestellt werden muss (vergleiche dazu § 4 a Abs. 1 BDSG), was im Rahmen eines Arbeitsverhältnisses allerdings nicht einfach zu realisieren ist.

9.5 Veröffentlichung von Mitarbeiterdaten einer Privatschule

In einem Einzelfall ging es um die Frage, inwieweit es zulässig ist, dass eine (Privat-)Schule als Arbeitgeber Daten der Mitarbeiter in einem Jahrbuch veröffentlicht, das ins Internet eingestellt wird. Ein solches Jahrbuch soll Schüler – auch

ehemalige – und deren Eltern sowie an der Schule Interessierte informieren und auch für die Schule werben.

Hierzu ist Folgendes zu sagen:

Bei der Veröffentlichung von Mitarbeiterdaten im Internet ist besondere Vorsicht geboten (siehe dazu schon unseren dritten Tätigkeitsbericht C 9.4, S. 151 ff.). Eine Privatschule darf den Namen eines Lehrers beziehungsweise eines Mitarbeiters in einem anderen Bereich nur dann im Internet veröffentlichen, wenn dieser in einer herausgehobenen Funktion oder als Ansprechpartner für Eltern oder Interessenten an der Schule tätig ist oder er aufgrund seiner besonderen Kenntnisse und/oder Fähigkeiten in seiner bisherigen Berufstätigkeit ein „Aushängeschild" für die Schule ist, sodass sie ein legitimes Interesse daran hat, mit ihm zu werben. Ansonsten überwiegen die schutzwürdigen Belange des Betroffenen mit der Folge, dass sein Name nur mit seiner Einwilligung veröffentlicht werden darf.

Für die Veröffentlichung von Schülerdaten im Internet ist auf jeden Fall die Einwilligung der Betroffenen beziehungsweise – sofern diese nicht über die erforderliche Einsichtsfähigkeit verfügen – der Erziehungsberechtigten erforderlich.

Bei der Veröffentlichung von Bildern (im Internet) gelten die Bestimmungen des Kunsturhebergesetzes. Eine Veröffentlichung ist nur mit Einwilligung der Betroffenen zulässig, es sei denn, es handelt sich um Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft erscheinen oder um Bilder von Versammlungen, an denen die dargestellten Personen teilgenommen haben.

10 Vermieter, Mieter, Wohnungseigentümer

10.1 Vermieterfragebögen

Einige Mietinteressenten beschwerten sich darüber, dass der ihnen vom Vermieter zum Ausfüllen vorgelegte Fragebogen zu weitgehende Fragen enthalte.

Die Aufsichtsbehörde steht hier oftmals vor der Schwierigkeit, aufsichtsrechtlich tätig werden zu können. Der Anwendungsbereich des Bundesdatenschutzgesetzes ist nämlich nur eröffnet, soweit nichtöffentliche Stellen Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben (§ 1 Abs. 2 Nr. 3 BDSG). Diese Voraussetzungen liegen zumeist nicht vor. Wir müssen uns daher in diesen Fällen darauf beschränken, Herausgeber solcher Fragebögen auf Fragen hinzuweisen, die nach unserer Auffassung unzulässig sind und eine Überarbeitung der Fragebögen anzuregen.

Grundsätzlich darf der Vermieter vom Mietinteressenten im Rahmen der Anbahnung eines Mietverhältnisses nur insoweit personenbezogene Daten erheben, als diese für den Abschluss eines Mietvertrags tatsächlich erforderlich sind. Er muss in der Lage sein zu beurteilen, ob der Mieter seinen Vertragsverpflichtungen aus dem Mietvertrag nachkommen kann.

Gemessen daran haben wir unter anderem folgende Fragen als problematisch eingestuft:

- Fragen zu Religion und Staatsangehörigkeit;
- Fragen nach der Beschäftigung und dem Einkommen der Ehefrau, wenn diese nicht auch Mietvertragspartei werden soll;
- Forderung, das Einkommen nach Nettoarbeitseinkommen, sonstigem Einkommen und Kindergeld aufzuschlüsseln; nach Auffassung der Aufsichtsbehörde dürfen nur Angaben zum durchschnittlichen Gesamteinkommen des potenziellen Mieters beziehungsweise der potenziellen Mieter verlangt werden;
- Fragen nach Namen und Anschrift des jetzigen Vermieters für etwaige Rückfragen; dies ist problematisch, da dadurch ein weiterer Informationsaustausch über den erforderlichen Umfang hinaus ermöglicht werden soll;
- Fragen nach der Dauer und einer etwaigen Kündigung des derzeitigen Mietverhältnisses sowie nach dem Grund der Wohnungssuche;

– genaue Aufschlüsselung von Darlehen und sonstigen Verpflichtungen; nach Auffassung der Aufsichtsbehörde darf nur nach den laufenden monatlichen Gesamtbelastungen gefragt werden;

– Fragen nach Anschrift und Telefonnummer des Arbeitgebers, da diese Angaben einen Informationsaustausch über den erforderlichen Umfang hinaus ermöglichen sollen; überdies werden personenbezogene Daten eines Dritten übermittelt, der möglicherweise nicht in einer privaten Angelegenheit eines Mitarbeiters telefonisch kontaktiert werden will;

– Bankverbindung; die Kenntnis ist zu dem Zeitpunkt, zu dem der Fragebogen ausgefüllt werden soll, noch nicht erforderlich;

– Frage nach der Anhängigkeit eines Räumungsrechtsstreits; ihr kann nach Auffassung der Aufsichtsbehörde nicht die gleiche Relevanz zugemessen werden wie der Frage nach einem ergangenen Räumungstitel oder einer einstweiligen Verfügung bezogen auf die derzeitige Wohnung.

Vorsicht ist auch geboten, wenn man Datenerhebungen und -verarbeitungen im Rahmen der Anbahnung eines Mietverhältnisses auf eine Einwilligung nach § 4 a BDSG stützen will. Eine solche ist nämlich nur dann wirksam, wenn sie freiwillig erteilt wird. Daran können jedoch Zweifel bestehen, wenn sich der Wohnungssuchende in einer Zwangssituation befindet.

Problematisch ist auch die Forderung, der Interessent möge eine SCHUFA-Selbstauskunft vorlegen. Diese enthält wesentlich mehr Angaben über die finanziellen Verhältnisse eines Mietinteressenten als der Vermieter bekommen würde, wenn er eine Auskunft über einen Mietinteressenten bei einer Auskunftei oder Kreditschutzorganisation (beispielsweise der SCHUFA) einholen würde.

Nach Inkrafttreten des Allgemeinen Gleichbehandlungsgesetzes sind auch dessen Auswirkungen zu beachten. Auch für Vermieter, die insgesamt nicht mehr als 50 Wohnungen vermieten, gilt das absolute Benachteiligungsverbot hinsichtlich der Merkmale „Rasse“ und „ethnische Herkunft“. Fragen hiernach in Vermieterfragebögen sind demnach grundsätzlich unzulässig. Zulässig dürfte es hingegen sein, dass Vermieter von Mietinteressenten ausgefüllte Fragebögen für einen begrenzten Zeitraum aufbewahren, um sich gegen Schadensersatzansprüche abgelehnter Mietinteressenten wegen Verletzung des Allgemeinen Gleichbehandlungsgesetzes zur Wehr setzen zu können.

10.2 Bekanntgabe von Daten eines Wohnungseigentümers an andere Wohnungseigentümer

Immer wieder wenden sich Wohnungseigentümer mit der Frage an die Aufsichtsbehörde, ob es einem nach dem Wohnungseigentümergesetz (WEG) bestellten Verwalter gestattet ist, einem Wohnungseigentümer Einsicht in die Abrechnungsunterlagen eines anderen Wohnungseigentümers zu gewähren. Manchen Beschwerdeführer stört es, dass ein Dritter auf diese Weise kontrollieren kann, wie hoch sein Heizungs- oder Wasserverbrauch ist und ob er seiner Verpflichtung zur Leistung der vom Verwalter festgesetzten monatlichen Vorauszahlung regelmäßig nachgekommen ist.

Die Antwort der Aufsichtsbehörde dürfte für die meisten Beschwerdeführer enttäuschend sein. Der Verwalter ist nicht nur berechtigt, sondern sogar verpflichtet, anderen Wohnungseigentümern Einsicht in derartige Unterlagen zu gewähren.

Nach § 28 Abs. 3 WEG hat der Verwalter nach Ablauf eines Kalenderjahrs eine Jahresabrechnung aufzustellen. Die Jahresabrechnung muss eine vollständige, übersichtliche und nachprüfbare Auskunft über die wirklichen Einnahmen und Ausgaben der Gemeinschaft geben. Über die Abrechnung beschließen die Wohnungseigentümer per Beschluss. Nach der Rechtsprechung (KG Berlin, Beschluss vom 31. Januar 2000, Az.: 24 W 601/99) steht jedem Wohnungseigentümer ein Recht auf Einsichtnahme in sämtliche Buchungs- und Abrechungsunterlagen des Verwalters zu. Dies beinhaltet auch die Einzelabrechnungen zu jedem Wohnungseigentümer, ohne dass der betroffene Wohnungseigentümer hierzu seine Einwilligung erteilen muss. Das Recht auf Einsichtnahme ist danach jedem Wohnungseigentümer individuell zugeordnet. Es ist zum einen im Zusammenhang mit der Prüfung der Jahresabrechnung zu sehen, deren Kontrolle es ermöglichen soll. Es

ergibt sich aber auch daraus, dass alle Verwaltungsunterlagen Bestandteil des gemeinschaftlichen Verwaltungsvermögens sind. Das Einsichtsrecht erstreckt sich damit auch auf Einzelabrechnungen, anhand derer etwa die Zahlungen der anderen Wohnungseigentümer zu kontrollieren sind. Die Einsichtnahme dient zudem der Zweckbestimmung des Gemeinschaftsverhältnisses, nämlich unter anderem der Kontrolle des Verwalters.

Dies führt dazu, dass die mit der Einsichtnahme verbundene Datenübermittlung an einen Wohnungseigentümer nach dem Bundesdatenschutzgesetz zulässig ist.

Auch wenn das Ergebnis letztlich aus den Vorschriften des Wohnungseigentümergesetzes und des Bürgerlichen Gesetzbuchs zur Gemeinschaft hergeleitet werden kann, würde es die Aufsichtsbehörde begrüßen, wenn für die hier angesprochene und einige weitere datenschutzrechtliche Fragen im Wohnungseigentümergesetz eindeutige datenschutzrechtliche Regelungen geschaffen würden. Schließlich müssen sich mit dem Wohnungseigentümergesetz viele Personen befassen, die mit dem Recht nicht so vertraut sind.

11 Videoüberwachung

Im Berichtszeitraum gingen viele Beschwerden und Anfragen zur Zulässigkeit von Videoüberwachungsmaßnahmen ein. Dies ist ein deutlicher Hinweis, dass die Videoüberwachung in der Zwischenzeit auch im Privatbereich erheblich zugenommen hat und sich viele Mitbürger durch Überwachungskameras in ihren Persönlichkeitsrechten beeinträchtigt fühlen.

In den an uns herangetragenen Fällen ging es um die Zulässigkeit der Videoüberwachung an folgenden Orten:

- in Treppenhäusern, Kellerräumen oder Tiefgaragen von Wohn- oder Bürogebäuden,
- in Gebäuden mit Eigentumswohnungen, wobei in einigen Fällen die Videoüberwachung von der Eigentümerversammlung beschlossen worden war,
- auf umfriedetem Betriebsgelände,
- an der Außenwand von Geschäftsgebäuden, wobei teilweise öffentlicher Verkehrsraum in die Überwachung miteinbezogen werden soll beziehungsweise miteinbezogen ist;
- in einer kleinen Bäckerei beziehungsweise Metzgerei,
- in Gaststätten und Cafes,
- in einem Festzelt bei einem Vereinsfest,
- in einem Kinocenter,
- in Bussen und Straßenbahnen,
- auf dem Schulgelände einer Privatschule,
- in Umkleidekabinen eines Bekleidungsgeschäfts.

In den meisten Fällen ging es nicht nur um Videobeobachtung, sondern auch um Videoaufzeichnungen, die unterschiedliche lange aufbewahrt werden sollten.

Als Gründe für die Videoüberwachung wurden die Wahrnehmung des Hausrechts, die Beobachtung des Publikumsverkehrs in entfernt liegenden Geschäftsräumen, die Verhinderung von Straftaten, insbesondere von Sachbeschädigungen, durch Abschreckung möglicher Straftäter und die Sicherung von Beweismaterial im Falle einer Straftat genannt. Teilweise wurden konkrete Anhaltspunkte für drohende Straftaten beziehungsweise konkrete Beispiele für bereits begangene Straftaten vorgetragen.

Bei der Frage nach der Zulässigkeit der Videoüberwachung kommt es zunächst darauf an, ob das Bundesdatenschutzgesetz (§ 6 b BDSG) überhaupt anwendbar ist. Es greift nur ein, wenn es sich um *öffentlich zugängliche Räume* handelt (vergleiche dazu dritter Tätigkeitsbericht C 10.3, S. 159). Liegt diese Voraussetzung nicht vor, bedeutet das nicht, dass damit die Überwachung zulässig ist. So sind etwa bei der Videoüberwachung von Arbeitnehmern die von der arbeitsgericht-

lichen Rechtsprechung entwickelten Grundsätze zu beachten (siehe dazu dritter Tätigkeitsbericht, a. a. O.), bei der Videoüberwachung innerhalb von Privatgebäuden kann der Betroffene einen Unterlassungsanspruch nach §§ 823, 1004 BGB haben, den er notfalls auf dem Zivilrechtsweg durchsetzen muss.

Im Falle der Anwendbarkeit des Bundesdatenschutzgesetzes ist stets zu prüfen, ob die Videoüberwachung zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke *erforderlich* ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Dies wird von manchen Betreibern einer Videoüberwachungsanlage übersehen, die meinen, allein das Hausrecht rechtfertige die Maßnahme. Die Zulässigkeit der Videoüberwachung hängt unter Umständen auch von der Kameraeinstellung ab. Die Einbeziehung öffentlichen Verkehrsraums bedarf einer besonderen Rechtfertigung. *Entgegenstehende Belange Betroffener* kommen vor allem bei der Videoüberwachung an sensiblen Orten (zum Beispiel Umkleidekabinen) zum Tragen. Eine besonders sorgfältige Interessenabwägung muss stattfinden, wenn es um „Orte der Kommunikation“ geht, bei denen der Bürger zu Recht erwartet, dass er nicht beobachtet wird (zum Beispiel Kinos, Gaststätten, Festzelt).

Die Erforderlichkeit einer *Videoaufzeichnung* muss gesondert geprüft werden. Sehr viel stärker als bisher wird auch darauf geachtet werden müssen, ob eine grundsätzlich zulässige Videoüberwachung (und -aufzeichnung) an allen Tagen rund um die Uhr erfolgen muss oder ob angesichts der Erkenntnislage – zum Beispiel wenn eine Gefahr nur in den Abend- oder Nachtstunden beziehungsweise am Wochenende droht – eine zeitlich eingeschränkte Beobachtung und Aufzeichnung genügt. *Bei Videoaufzeichnungen muss sich auch die Speicherdauer strikt am Erforderlichkeitsgrundsatz orientieren.* In der Praxis wird häufig übersehen, dass nach dem Gesetz die Daten unverzüglich zu löschen sind, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind.

12 Internet

12.1 Identifizierung möglicher Urheberrechteverletzer in Internet-Tauschbörsen

Ein Unternehmen bietet an, mithilfe einer speziellen Software Daten möglicher Urheberrechteverletzer in Internet-Tauschbörsen zu erheben, damit diese zivilrechtlich verfolgt werden können. Die Erhebung erfolgt im Auftrag von Rechteinhabern urheberrechtlich geschützter Werke (insbesondere Filme, Musik und Spiele). Die urheberrechtlich geschützten Werke werden als Dateien über Tauschbörsen im Internet angeboten. Dabei gibt sich diese Software als Teilnehmer (Client) in der jeweiligen Tauschbörse aus und geht dann gezielt auf die Suche nach urheberrechtlich geschützten Werken, die sie mittels des Hash-Werts, des sogenannten Fingerprints, identifiziert. Den Hash-Wert, nach dem gesucht werden muss, erhält die Privatfirma von dem Urheberrechtsinhaber. Jedes urheberrechtlich geschützte Werk, das in elektronischer Form angeboten wird, hat seinen eigenen Fingerprint, anhand dessen es eindeutig erkannt werden kann. Wenn die Software das gesuchte Werk in der Tauschbörse findet, beginnt sie das betreffende Werk herunterzuladen. Dabei werden neben dem Fingerprint des geschützten Werks noch Datum und Uhrzeit des Herunterladevorgangs (sogenanntes Download), die zu diesem Zeitpunkt zugeteilte dynamische IP-Adresse des Anbieters, die Größe der Datei und die Netzwerkadresse des Software-Clients (GUID) erhoben und gespeichert.

Diese Daten werden im Rahmen der Staatsanwaltschaft mit dem Ziel übermittelt, beim Internet-Zugangsanbieter über die dynamische IP-Adresse in Verbindung mit der Uhrzeit und dem Datum, an dem diese zugeteilt wurde, an Namen und Adresse des möglichen Urheberrechtsverletzers (des Anbieters der Datei) zu ermitteln. Ist dieser festgestellt nimmt eine Anwaltskanzlei Einsicht in die Akten der Staatsanwaltschaft, um anschließend gegenüber dem Urheberrechtsverletzer zivilrechtliche Ansprüche geltend zu machen.

Unsere datenschutzrechtliche Bewertung ergab Folgendes:

Die von der Firma erhobenen dynamischen IP-Adressen sind – nach inzwischen herrschender und von allen Datenschutzaufsichtsbehörden in Deutschland gerade auch in Bezug auf dieses Projekt vertretener Auffassung – personbezogen. Es handelt sich nämlich um Einzelangaben einer bestimmbaren natürlichen Person

im Sinne der Legaldefinition des § 3 Abs. 1 BDSG. Für die Bestimmbarkeit kommt es auf die Kenntnisse, Mittel und Möglichkeiten der speichernden Stelle an. Sie muss den Bezug mit den ihr normalerweise zur Verfügung stehenden Hilfsmitteln und ohne unverhältnismäßigen Aufwand durchführen können. Die Bestimmbarkeit liegt auch vor, wenn die Identität eines Betroffenen mithilfe eines Dritten festgestellt werden kann. Dies gilt jedenfalls dann, wenn der Dritte rechtlich dazu verpflichtet ist, diese Hilfe zu gewähren und der Aufwand für die Inanspruchnahme der Hilfe nicht unverhältnismäßig ist. So verhält es sich hier. Die Firma kann die Identität des Betroffenen unter Inanspruchnahme hoheitlicher Hilfe feststellen lassen, da die Staatsanwaltschaft aufgrund des Legalitätsprinzips rechtlich verpflichtet ist, im Falle einer Strafanzeige tätig zu werden, sofern es zureichende tatsächliche Anhaltspunkte für das Vorliegen einer Straftat gibt. Das Tätigwerden umfasst die Ermittlung des Täters. Dass sich der Aufwand für die beauftragte Firma für die Inanspruchnahme staatlicher Hilfe im vorliegenden Fall in Grenzen hält, wird schon daraus ersichtlich, dass sie diese Hilfe in zigtausenden von Fällen in Anspruch nimmt, ja das ganze System hierauf ausgerichtet ist. Dass die Feststellung der hinter der IP-Adresse stehenden Person erst zu einem späteren Zeitpunkt und durch eine staatliche Behörde erfolgt, ändert nichts daran, dass bereits die IP-Adresse in Verbindung mit den weiteren genannten Daten personenbeziehbar und damit personenbezogen ist.

Nach § 4 Abs. 2 Satz 1 BDSG sind personenbezogene Daten grundsätzlich „beim“ Betroffenen zu erheben. Dies bedeutet nicht nur, dass die Daten *direkt beim Betroffenen* zu erheben sind, sondern – wie ein Vergleich mit § 4 Abs. 2 Satz 2 BDSG zeigt – auch, dass der Betroffene daran mitwirkt, um vom Erhebungsvorgang Kenntnis zu erlangen (Sokol in Kommentar zum Bundesdatenschutzgesetz; Hrsg. Simitis, 6. Auflage, § 4 Rn. 20). *§ 4 Abs. 2 Satz 1 BDSG ist also so zu lesen, dass die Datenerhebung beim Betroffenen mit dessen Kenntnis zu erfolgen hat.*

An dieser Kenntnis des Betroffenen fehlt es im vorliegenden Fall. Die IP-Adresse und die weiteren Daten werden *heimlich erhoben*. Dies wäre nur aufgrund einer die heimliche Datenerhebung zulassenden Rechtsvorschrift erlaubt. Eine solche ist nicht ersichtlich, insbesondere liegen die Voraussetzungen des § 4 Abs. 2 Satz 2 BDSG nicht vor.

Keine Rechtsvorschrift setzt die hier praktizierte Vorgehensweise bei der Datenerhebung „zwingend“ voraus oder sieht diese vor. Auch geht es im vorliegenden Fall nicht um eine offene Datenerhebung bei Dritten („anderen Personen oder Stellen“), sondern um eine heimliche Datenerhebung beim Betroffenen. Angesicht der Unterschiede zwischen offener und heimlicher Datenerhebung kann diese Vorschrift auf die heimliche Datenerhebung beim Betroffenen auch nicht entsprechend angewandt werden. Agiert eine nichtöffentliche Stelle – wie hier – gleichsam als Internetpolizei, ist es auch sachgerecht, dafür eine ausdrückliche gesetzliche Legitimation zu fordern.

Ein Verstoß gegen § 4 Abs. 2 BDSG führt jedoch nicht automatisch zur Unzulässigkeit einer Datenerhebung. § 4 Abs. 2 BDSG stellt nämlich keine eigenständige Erlaubnisvorschrift im Sinne des § 4 Abs. 1 BDSG. Vielmehr muss sich die Zulässigkeit einer Datenerhebung an § 28 oder § 29 BDSG messen lassen, wobei der Verstoß gegen § 4 Abs. 2 BDSG bei den schutzwürdigen Belangen des Betroffenen und im Rahmen der Abwägung zwischen den berechtigten Interessen des Softwareunternehmens beziehungsweise des Urheberrechtsinhabers und den berechtigten Belangen des Betroffenen zu berücksichtigen ist.

Würde man hier stets zu dem Ergebnis kommen, dass eine Person, die möglicherweise eine – mit Strafe bedrohte – Urheberrechtsverletzung begangen hat, nicht schützenswert ist beziehungsweise die berechtigten Interessen des vom Urheberrechtsinhaber beauftragten Unternehmens stets die schutzwürdigen Belange des Betroffenen überwiegen, sodass die Datenerhebung zulässig wäre, würde der permanente Verstoß des Unternehmens gegen § 4 Abs. 2 BDSG letztlich ohne Folgen bleiben.

Würde man wegen des Verstoßes gegen § 4 Abs. 2 BDSG hingegen zu dem Ergebnis kommen, dass stets die schutzwürdigen Belange des Betroffenen überwiegen, wäre die zivil- und strafrechtliche Ahndung von Urheberrechtsverstößen zumindest erheblich erschwert.

Beide Ergebnisse sind gleichermaßen unbefriedigend. Lösen kann das Problem letztlich nur der Gesetzgeber. Das braucht Zeit. Die rechtliche Prüfung ist jedoch

bereits eingeleitet: Der Bundesrat in seiner Stellungnahme zum Entwurf eines Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums (BR-Drs. 64/07) die Bundesregierung gebeten, im weiteren Gesetzgebungsverfahren zu prüfen, ob und gegebenenfalls wie es Urheberrechtinhabern ermöglicht werden kann, in datenschutzrechtlich unbedenklicher Weise an die Verkehrsdaten (IP-Adressen) potenzieller Urheberrechtverletzer zu gelangen, damit sie ihren Auskunftsanspruch gegenüber Internet-Zugangsanbietern geltend machen können. Eine Lösung könnte darin bestehen, eine eindeutige Rechtsgrundlage für die Art der Erhebung samt Rahmenbedingungen im Bundesdatenschutzgesetz oder in einer anderen Rechtsvorschrift (zum Beispiel im Urheberrechtsgesetz) zu schaffen.

Bis dahin werden wir die jetzige Verfahrensweise des Softwareunternehmens hinnehmen.

12.2 Auswertung des Leseverhaltens von Newsletter-Empfängern

Eine Buchhandlung bietet über ihre Internetseite neben Informationen über Bücher auch einen eigenen Newsletter-Dienst an. Interessierte können sich auf diesem Weg über Neuerscheinungen und Aktuelles auf dem Büchermarkt unterrichten lassen. Sie müssen dazu lediglich ihre E-Mail-Adresse angeben. Dieser Dienst wird über eine Fremdfirma im Wege der Auftragsdatenverarbeitung erbracht.

Ein Beschwerdeführer hat diesen Newsletter-Dienst genutzt und dabei festgestellt, dass in dem Newsletter, für den Nutzer nicht sichtbar, ein sogenannter Webbug versteckt ist, der das Leseverhalten des Newsletter-Empfängers – einmalige oder wiederholte Öffnung des Newsletters – registriert. Der Beschwerdeführer vermutete deshalb, sein Leseverhalten werde personenbezogen festgehalten.

Dies bestätigte sich jedoch nicht. Zwar präsentiert die Buchhandlung auf ihrer Webseite eine monatliche Auswertestatistik, aus der sich ergibt, wie oft ein Newsletter von Kunden einmal oder wiederholt geöffnet wurde. Grundlage der Statistik ist eine Information des Kunden-PCs an den Server des Auftragsdatenverarbeiters, die jeweils gesendet wird, wenn ein Kunde den Newsletter öffnet. Dies wird über den Webbug, der sich im Newsletter befindet, gesteuert. Die Auswertung des Leseverhaltens des Newsletter-Empfängers erfolgt jedoch in anonymisierter Form.

Gleichwohl entsprach die Verfahrensweise der Buchhandlung nicht den Vorschriften des Teledienstedatenschutzgesetzes (jetzt: des Telemediengesetzes). Danach ist der Nutzer über diese Art der Nutzung vor Beginn des Nutzungsvorgangs zu unterrichten. In den Datenschutzhinweisen fand sich jedoch keine entsprechende Information.

Auf unsere Aufforderung hin hat der Auftragsdatenverarbeiter die Datenschutzerklärung entsprechend den gesetzlichen Vorgaben geändert. Daraus geht jetzt unter anderem hervor, dass keine personenbezogene Auswertung des Leseverhaltens des Nutzers stattfindet, sondern das Öffnen des Newsletters in anonymisierter Form zum Zwecke der Verbesserung und Optimierung des Angebots registriert wird. Auf die Möglichkeit, den Newsletter jederzeit abzubestellen, wird der Nutzer nunmehr ebenfalls hingewiesen.

13 Vereine, Verbände

13.1 Veröffentlichung von Sportgerichtsurteilen

Durch mehrere Beschwerden wurden wir auf folgende generelle Problematik aufmerksam:

Es gibt Sportverbände, die Urteile ihrer Sportgerichtsbarkeit in vollem Umfang in ihrer *Verbandszeitschrift* veröffentlichen. Nachzulesen sind dort Vor- und Familiename des betroffenen Sportlers beziehungsweise Funktionärs einschließlich seiner Vereinszugehörigkeit, der von diesem begangene Verstoß, die verhängte Strafe, Angaben zur Kostentragungspflicht und zur Höhe der Verfahrenskosten sowie eine kurze Urteilsbegründung samt Sachverhalt.

Datenschutzrechtlich ist dies, sofern der Anwendungsbereich des Bundesdatenschutzgesetzes nach dessen § 1 Abs. 2 Nr. 3 eröffnet ist, wie folgt zu bewerten:

Die Veröffentlichung in der Verbandszeitschrift stellt eine Datenübermittlung an jedermann dar. Dafür gibt es keine Rechtsgrundlage. In der Regel fehlt es bereits an einem berechtigten Interesse des Sportverbands an einer derartigen Veröffentlichung. Es genügt, die Entscheidung den Verfahrensbeteiligten und etwaigen weiteren Personen, die diese zwingend in vollem Umfang kennen müssen, unmittelbar bekannt zu geben. Falls Dritte (zum Beispiel Mannschaften derselben Spielklasse, Schiedsrichter) über eine gegen einen Sportler verhängte Sperre Bescheid wissen müssen, reicht es aus, ihnen eine hierauf beschränkte Information zukommen zu lassen. Über eine gegen einen Sportler verhängte Geldbuße, die Art des Verstoßes, die Pflicht zur Kostentragung und die Höhe der Verfahrenskosten sowie die Urteilsbegründung müssen Dritte in der Regel nicht unterrichtet werden.

Sofern ein Verband seine Mitglieder über die Auslegung bestimmter, von ihm erlassener Regeln durch das Sportgericht informieren will oder die Veröffentlichung eines Sportgerichtsurteils der Warnung anderer Sportler dienen soll, genügt hierfür eine Veröffentlichung in anonymisierter Form. Die Veröffentlichung von Sportgerichtsurteilen in vollem Wortlaut stellt die Betroffenen unnötig an den Pranger und beeinträchtigt damit deren schutzwürdige Belange.

Sofern das Bundesdatenschutzgesetz nicht anwendbar ist, kann sich ein von der Veröffentlichung eines Sportgerichtsurteils betroffener Sportler oder Funktionär gegen den darin liegenden Eingriff in sein Persönlichkeitsrecht über §§ 823, 1004 BGB zur Wehr setzen.

13.2 Übermittlung von Mitgliederdaten an die Gemeindeverwaltung

Ein Verein fragte bei uns an, ob eine Gemeindeverwaltung von ihm die Vorlage einer Liste mit Namen, Anschriften und Geburtsdaten aller minderjährigen Mitglieder verlangen könne. Die Gemeindeverwaltung begründete ihre Anforderung damit, dass die Höhe der von ihr freiwillig gewährten Vereinsförderung von der Zahl der minderjährigen Vereinsmitglieder abhängig sei. Ob die vom Verein gemeldete Zahl richtig sei, lasse sich nur anhand dieser Liste nachprüfen. Zwar habe die Gemeinde keinen Verdacht, dass die vom Verein gemeldete Zahl unrichtig sei, doch hätten sich bei anderen Vereinen Zweifel ergeben. Die Gemeinde habe sich deshalb dazu entschlossen, von allen Vereinen eine Liste ihrer minderjährigen Mitglieder zu verlangen. Um eine sorgfältige Prüfung durchführen zu können, sei die Übermittlung der Liste erforderlich. Der Verein wollte von uns wissen, ob die Übermittlung einer solche Liste im Einklang mit den Vorschriften des Bundesdatenschutzgesetzes steht.

Nach Auffassung der obersten Kommunalaufsichtsbehörde ist eine Gemeinde, die an Vereine eine freiwillige Leistung auf der Grundlage der Zahl der minderjährigen Vereinsmitglieder gewährt, befugt, einen Nachweis zu verlangen und zwar unabhängig davon, ob Zweifel an den Angaben des Vereins bestehen. Als Nachweis geeignet ist eine Liste mit Vor- und Nachnamen, den Anschriften sowie den Geburtsdaten der minderjährigen Vereinsmitgliedern. Eine derartige Datenerhebung ist zur rechtmäßigen Aufgabenerfüllung der Gemeinde erforderlich (§ 13 Abs. 1 des Landesdatenschutzgesetzes).

Der Verein ist auch berechtigt, derartige Daten zu übermitteln, weil es sowohl zur Wahrung berechtigter eigener Interessen – nämlich um in den Genuss der Vereinsförderung durch die Gemeinde zu kommen – als auch zur Wahrung berechtigter Interessen eines Dritten – der Gemeinde – erforderlich ist und berechtigte Belange der minderjährigen Vereinsmitglieder einer Datenübermittlung nicht entgegenstehen (§ 28 Abs. 3 Satz 1 Nr. 1 BDSG). Anders mag es sich verhalten, wenn die Zugehörigkeit zu einem Verein ein sensibles Datum im Sinne des § 3 Abs. 9 BDSG darstellt. Die Gemeinde darf die ihr übermittelten Daten nur dazu verwenden, nachzuprüfen, ob die ihr vom Verein mitgeteilte Zahl der minderjährigen Vereinsmitglieder richtig ist (§ 28 Abs. 5 Satz 1 BDSG).

Neue minderjährige Vereinmitglieder beziehungsweise deren Eltern sind bei ihrer Aufnahme in den Verein auf die Datenübermittlung an die Gemeinde und deren Zweck hinzuweisen, andere minderjährige Vereinsmitglieder beziehungsweise

deren Eltern in anderer geeigneter Weise. Verlangt die Gemeinde die Vorlage der Liste regelmäßig, empfiehlt es sich, eine Bestimmung in die Vereinssatzung aufzunehmen.