Landtag von Baden-Württemberg **Drucksache 14 / 4963**

14. Wahlperiode **31. 07. 2009**

Mitteilung

des Innenministeriums

Fünfter Tätigkeitsbericht des Innenministeriums zum Datenschutz im nichtöffentlichen Bereich

Schreiben des Innenministeriums vom 30. Juli 2009 Nr. 2-0552.6/37:

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

Rech

Innenminister

Eingegangen: 31. 07. 2009 / Ausgegeben: 28. 08. 2009

Datenschutz im nichtöffentlichen Bereich

Fünfter Tätigkeitsbericht des Innenministeriums nach § 39 des Landesdatenschutzgesetzes 2009

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 fünfte Bericht nach Einführung der gesetzlichen Berichtspflicht. Er baut auf den ersten vier Tätigkeitsberichten (Landtags-Drucksachen 13/40, 13/2200, 13/4469 und 14/1475) auf und beschränkt sich im Wesentlichen auf Neuerungen und Entwicklungen, die im Berichtszeitraum (1. Juli 2007 bis 30. Juni 2009) eingetreten sind.

Die bisherigen Tätigkeitsberichte sind auch im Internet (*www.im.baden-wuerttemberg.de* – darin Auswahl „Datenschutz“ – „Weitere Infos“ – „Infomaterial“) veröffentlicht.

A Entwicklung der Aufgaben und des Datenschutzrechts seit 2007

1 Allgemeines zur Aufsichtstätigkeit

1.1 Beschwerden

Ein Schwerpunkt der Tätigkeit der Aufsichtsbehörde war im Berichtszeitraum die Bearbeitung von Beschwerden betroffener Bürgerinnen und Bürger*. In der Zeit vom 1. Juli 2007 bis 30. Juni 2009 machten insgesamt 1.262 Bürger von ihrem Recht Gebrauch, die Aufsichtsbehörde anzurufen (zum Vergleich: im vorigen Berichtszeitraum waren es 850 Bürger). Allein im Jahre 2008 verzeichnete die Aufsichtsbehörde mit 658 Beschwerden so viele wie nie zuvor. In diesem Jahr gingen bis 30. Juni bereits 376 Beschwerden bei der Aufsichtsbehörde ein, was einen neuen Jahresrekord erwarten lässt.

Der starke Anstieg der Beschwerden ist vor allem auf eine deutliche Zunahme der Eingaben im Werbebereich zurückzuführen, die ihre Ursache in dem im August 2008 bekannt gewordenen massenhaften Missbrauch von Kontodaten und der Ankündigung der Bundesregierung haben dürfte, das sogenannte Listenprivileg einzuschränken und durch eine Einwilligungslösung zu ersetzen (vergleiche dazu unten A 2.1.2). Ein Teil der Beschwerdeführer ging ersichtlich davon aus, dass das Bundesdatenschutzgesetz bereits entsprechend geändert ist.

Mehr Beschwerden gab es auch in den Bereichen Tele- und Mediendienste und Arbeitnehmerdatenschutz (seit Herbst 2008). Möglicherweise hat der Abschluss der datenschutzrechtlichen Prüfung bei einem Discounter, der Mitarbeiter durch den Einsatz von Videotechnik und Detektiven unzulässig überwachen ließ, dazu beigetragen, dass sich mehr Arbeitnehmer wegen einer ihrer Meinung nach unzulässigen Überwachung durch den Arbeitgeber an die Aufsichtsbehörde wenden.

Die meisten Eingaben betrafen jedoch nach wie vor Auskunfteien und Inkassounternehmen, gefolgt vom Adresshandel und der Direktmarketing- und Werbebranche einschließlich der Lotterien, den Tele- und Mediendiensten und der Kreditwirtschaft. Seltener waren Eingaben zum Versicherungs- und zum Gesundheitsbereich und – trotz des Anstiegs in den vergangen Monaten – zum Arbeitnehmerdatenschutz. Eine gleichbleibend hohe Zahl an Beschwerden betraf – branchenunabhängig – die Videoüberwachung, teilweise auch von Mitarbeitern.

1.2 Tätigwerden von Amts wegen

Seit März 2008 ist die Aufsichtsbehörde durch mehrere datenschutzrechtliche Überprüfungsverfahren sehr stark belastet, die sie aufgrund von Medienberichten von Amts wegen eingeleitet hat. Es begann mit einem Verfahren gegen einen Discounter wegen unzulässiger Überwachung seiner Mitarbeiter unter Einsatz von Videotechnik und Detektiven (siehe dazu unten B 1.1). An dieser Überprüfung waren zwölf Datenschutzaufsichtsbehörden beteiligt, deren Koordination der baden-württembergischen Aufsichtsbehörde oblag. Die Überprüfung band für fast ein halbes Jahr erhebliche personelle Ressourcen der Aufsichtsbehörde.

Die Untersuchungsergebnisse haben die Aufsichtsbehörde veranlasst, bei vier Großunternehmen mit Sitz in Baden-Württemberg zu überprüfen, ob und gegebenenfalls in welcher Weise und in welchem Umfang von diesen Videokameras und Sicherheitsunternehmen zur Überwachung von Kunden und Mitarbeitern eingesetzt werden (siehe dazu unten B 1.2).

Ebenfalls aufgrund von Presseberichten hat die Aufsichtsbehörde in diesem Jahr datenschutzrechtliche Überprüfungen bei einem Discounter, einem Automobilhersteller und einer Drogeriemarktkette eingeleitet. Sie sollen von Mitarbeitern im Rahmen von Rückkehrgesprächen nach einer Erkrankung unerlaubt Daten über den Grund der Erkrankung erhoben und gespeichert haben (siehe dazu unten B 1.6).

---

* Im Folgenden wird aus Gründen der besseren Lesbarkeit des Berichts nur noch die männliche Form verwendet.

In einem weiteren Fall wird von Amts wegen geprüft, ob ein Versorgungsunternehmen Telefon- und E-Mail-Daten seiner Mitarbeiter ausgewertet hat um festzustellen, ob jemand und gegebenenfalls wer vertrauliche Informationen aus einer Aufsichtsratssitzung an die Presse übermittelt hat. Die Prüfung erstreckt sich auch auf generelle Verfahrensweisen dieses Unternehmens.

1.3 Durchführung von Kontrollen vor Ort

Die meisten datenschutzrechtlichen Überprüfungen konnten im schriftlichen Verfahren erledigt werden. In Einzelfällen, insbesondere bei den von Amts wegen eingeleiteten Verfahren, war beziehungsweise ist es jedoch erforderlich, sich durch – angemeldete oder unangemeldete – Kontrollen vor Ort und durch Gespräche in den Unternehmen einen unmittelbaren Eindruck zu verschaffen. Solche Kontrollbesuche hat die Aufsichtsbehörde im Berichtszeitraum unter anderem in Filialen und Dienstleistungsunternehmen eines Discounters, bei einer Drogeriemarktkette, einem Automobilhersteller, in einem Lebensmittelgeschäft, einem Reisebüro, in der Personaldatenverarbeitung eines Dienstleisters, bei einem Verkehrsunternehmen, einem Versorgungsunternehmen, in einer Bank, einer Versicherung, beim Betreiber des AGG-Archivs, in einer Bildungseinrichtung, mehreren Detekteien, einem medizinischen Labor und wegen der Videoüberwachung in einigen sonstigen nichtöffentlichen Stellen durchgeführt.

1.4 Hauptsächlich festgestellte Datenschutzmängel

Die Aufsichtsbehörde führt keine Statistik darüber, in wie vielen datenschutzrechtlichen Überprüfungsverfahren ein oder mehrere Datenschutzverstöße festgestellt wurden. Sie schätzt jedoch, dass dies – je nach Branche – in 70 bis 80 % aller Überprüfungsverfahren der Fall war. Häufig festgestellte Mängel waren

- die Nichterfüllung beziehungsweise die nicht rechtzeitige Erfüllung des Auskunftsanspruchs des Bürgers nach § 34 des Bundesdatenschutzgesetzes (BDSG); es fällt allerdings auf, dass manche Bürger sich bereits dann an die Aufsichtsbehörde wenden, wenn ihnen die um Auskunft ersuchte Stelle nicht innerhalb weniger Tage geantwortet hat. Hierzu ist zu sagen: Das Bundesdatenschutzgesetz sieht keine Frist für die Auskunftserteilung vor. Die Aufsichtsbehörde geht davon aus, dass die Auskunft „unverzüglich“ zu erteilen ist, jedoch die im Geschäftsverkehr üblichen Fristen eingehalten werden müssen. Die Aufsichtsbehörde erachtet eine Frist von zwei bis maximal drei Wochen in der Regel als angemessen;
- die Erhebung und Speicherung nicht erforderlicher Daten, vor allem die standardmäßige Erhebung der Telefon- und der Telefaxnummer sowie der E-Mail-Adresse eines Betroffenen. Auch das Geburtsdatum wird häufig ohne Rechtsgrund abgefragt;
- die unzulässige Übermittlung von Daten;
- die Nichtbeachtung der Aufklärungs- und Informationspflichten bei der Erhebung von Daten beim Betroffenen (§ 4 Abs. 3 BDSG, vergleiche dazu vierter Tätigkeitsbericht, B S. 19 ff.);
- die Nichtbeachtung des Grundsatzes der Direkterhebung beim Betroffenen (§ 4 Abs. 2 BDSG);
- die Erhebung, Verarbeitung und Nutzung personenbezogener Daten auf der Grundlage einer nicht wirksamen Einwilligungserklärung, sei es, dass
  - die angebliche Einwilligungserklärung keine solche ist,
  - die Einwilligung nicht freiwillig erfolgt ist (z. B. im Arbeitsverhältnis),
  - die Einwilligung nicht auf der Grundlage ausreichender Informationen über die Zwecke der Erhebung und Verarbeitung der Daten abgegeben wurde,
  - die Einwilligung nicht in der notwendigen Form (grundsätzlich ist Schriftform im Sinne des § 126 BGB vorgeschrieben) abgegeben wurde;
- Telefon- und E-Mail-Werbung ohne die dafür erforderliche Einwilligung (vergleiche dazu unten B 6.1.1);

– in Werbeschreiben das Fehlen eines Hinweises auf die Möglichkeit, gegen die Nutzung oder Übermittlung personenbezogener Daten zu Werbezwecken Widerspruch einzulegen und die Nichtbeachtung des Werbewiderspruchs (§ 28 Abs. 4 Sätze 1 und 2 BDSG, vergleiche dazu unten B 6.1.1);
– die Videoüberwachung von Kunden und/oder Mitarbeitern ohne Vorliegen der gesetzlichen Voraussetzungen;
– ferner die Nichtbestellung eines Beauftragten für den Datenschutz oder die Bestellung eines Beauftragten für den Datenschutz, der wegen einer Interessenkollision nicht über die erforderliche Zuverlässigkeit verfügt.

1.5 Beratung von Bürgern, Unternehmen und Beauftragten für den Datenschutz

Zusätzlich zu den förmlichen Beschwerden gab es in der Zeit vom *1. Juli 2007 bis 30. Juni 2009* 447 schriftliche und – vorsichtig geschätzt – mindestens 4.000 telefonische Anfragen und Beratungswünsche von Bürgern, Unternehmen und Beauftragten für den Datenschutz. Diese Zahlen sind gegenüber den Vorjahren in etwa gleichgeblieben. Nimmt man die Zahl der schriftlichen Beschwerden und Beratungswünsche zusammen, kommt man auf *1.709 Eingaben* gegenüber 1.270 im letzten Berichtszeitraum. Beraten lassen sich vor allem Bürger und in geringerem Maße kleine Unternehmen und – zumeist externe – Beauftragte für den Datenschutz. Letzteren geht es zumeist um die Klärung datenschutzrechtlicher Einzelfragen.

1.6 Datenschutzregister

In dem von der Aufsichtsbehörde nach § 38 Abs. 2 BDSG zu führenden Datenschutzregister haben sich nur geringfügige Änderungen ergeben. Es sind insgesamt 92 nichtöffentliche Stellen mit 97 automatisierten Verfahren gemeldet. 46 dieser Verfahren dienen dem Zweck der Übermittlung personenbezogener Daten (Auskunfteien und Adresshändler), 39 dem Zweck der anonymisierten Datenübermittlung (Markt- und Meinungsforschungsinstitute). Die Aufsichtsbehörde hat festgestellt, dass nicht alle meldepflichtigen Verfahren gemeldet sind. Die Qualität der Meldungen lässt teilweise sehr zu wünschen übrig.

Von der Möglichkeit, in das Datenschutzregister Einsicht zu nehmen, hat eine Person Gebrauch gemacht.

1.7 Durchführung von Bußgeldverfahren

Entgegen einer weit verbreiteten Auffassung ist es nicht primäres Ziel einer datenschutzrechtlichen Überprüfung, im Falle eines Datenschutzverstoßes ein Bußgeld gegen die Verantwortlichen zu verhängen. Vielmehr geht es in erster Linie darum, festzustellen, ob eine verantwortliche Stelle mit einem bestimmten, zumeist von einem Beschwerdeführer gerügten Verhalten gegen datenschutzrechtliche Vorschriften verstoßen hat oder nicht. Liegt ein Datenschutzverstoß vor, wirkt die Aufsichtsbehörde darauf hin, dass sich die verantwortliche Stelle künftig datenschutzkonform verhält. Nur wenn der Datenschutzverstoß eine Ordnungswidrigkeit darstellt, offensichtlich ist und die verantwortliche Stelle in schwerwiegender Weise oder wiederholt gegen datenschutzrechtliche Vorschriften verstoßen oder datenschutzrechtliche Vorschriften bewusst missachtet hat, leitet die Aufsichtsbehörde in einem zweiten Schritt ein Bußgeldverfahren ein. Diese Praxis stimmt mit der anderer Aufsichtsbehörden überein.

Im Berichtszeitraum hat die Aufsichtsbehörde gegen fünf Regionalgesellschaften eines Discounters ein Bußgeld in Höhe von jeweils 10.000 Euro verhängt, weil diese über viele Jahre hinweg keinen betrieblichen Datenschutzbeauftragten bestellt hatten. Die Ahndung war geboten, weil diese Unternehmen in erheblichem Umfang sensible personenbezogene Daten erhoben und gespeichert hatten.

Neun Bußgeldverfahren sind derzeit bei der Aufsichtsbehörde anhängig:

Leitenden Mitarbeitern eines Versicherungsunternehmens wird vorgeworfen, in mehreren hundert Fällen unter Angabe eines unzutreffenden Grundes Bonitätsabfragen bei einer Auskunftei durchgeführt zu haben, obwohl dafür kein Anlass

(mehr) bestand. Ein Mitarbeiter einer anderen Firma soll sich illegal Informationen von der Personalabteilung beschafft haben. Gegen einen Arzt wird ermittelt, weil er möglicherweise Patientenkarteikarten in einer Mülltonne so entsorgt hat, dass Dritte die Daten zur Kenntnis nehmen konnten. Einem selbstständigen Versicherungsvertreter wird vorgeworfen, im Rahmen eines Scheidungsverfahrens Daten aus dem Versicherungsverhältnis einer Versicherungsnehmerin deren Ehemann zugänglich gemacht zu haben. Gegen einen Firmeninhaber musste ein Bußgeldverfahren eingeleitet werden, weil er sich, ohne dass dafür eine Notwendigkeit bestand, von der Bonität eines angeblichen Geschäftspartners durch Abfragen bei Auskunfteien überzeugen wollte. Gegen die Verantwortlichen eines Glücksspielunternehmens wurde ein Verfahren eröffnet, weil diese lange Zeit Auskunftsersuchen der Aufsichtsbehörde nach § 38 Abs. 3 BDSG nicht beantwortet hatten. Ein Callcenter steht im Verdacht, den erforderlichen betrieblichen Datenschutzbeauftragten nicht bestellt zu haben. Bußgeldrechtliche Ermittlungen wurden auch eingeleitet, weil ein Discounter eine Betriebsrätin außerhalb des Betriebs ohne Rechtfertigung mit Hilfe eines Detektivs überwachen ließ. Einem Rechtsanwalt wird vorgeworfen, wiederholt Rechnungen an einen Mandanten geschickt zu haben, deren Inhalt diesem nicht hätte bekannt werden dürfen, weil sie für eine andere Person bestimmt waren.

In zwei Fällen gab die Aufsichtsbehörde das Verfahren an die Staatsanwaltschaft ab. In einem Fall stellte sie einen Strafantrag nach § 44 Abs. 2 BDSG, weil ein Mitarbeiter einer Firma einen Privatdetektiv beauftragt hatte, einen missliebigen Konkurrenten, Staatsanwälte und Beauftragte von Behörden auszuspionieren, wobei unter anderem auch Steuerdaten ausgekundschaftet worden waren (vergleiche dazu unten B 7.1.1). In dem anderen Fall bestand der Verdacht, dass nicht nur Daten unbefugt verarbeitet, sondern auch ohne Wissen des Betroffenen in einer Sitzung Tonbandaufnahmen gefertigt worden sind. Dies ist nach § 201 des Strafgesetzbuchs (StGB) strafbar.

Einige Bußgeldverfahren hat die Aufsichtsbehörde eingestellt, weil das Verschulden der für den Datenschutz Verantwortlichen letztlich doch gering war.

Mehrfach musste die Aufsichtsbehörde Bußgeldverfahren einstellen, weil zwar der begründete Verdacht einer Ordnungswidrigkeit nach dem Bundesdatenschutzgesetz bestand, jedoch die dafür verantwortliche Person nicht ermittelt werden konnte. Vor allem bei größeren Unternehmen ist dies oftmals schwierig. Zwar sieht § 30 des Ordnungswidrigkeitengesetzes die Möglichkeit vor, auch gegen eine juristische Person einen Bußgeldbescheid zu verhängen. Voraussetzung dafür ist jedoch, dass einem vertretungsberechtigten Organ dieses Unternehmens oder einem leitenden Mitarbeiter ein Datenschutzverstoß nachgewiesen werden kann.

2 Rechtsentwicklung

2.1 Änderungen des Bundesdatenschutzgesetzes

Die letzte grundlegende Novellierung des Bundesdatenschutzgesetzes datiert vom 18. Mai 2001. Mit ihr wurde im Wesentlichen die EG-Datenschutzrichtlinie in nationales Recht umgesetzt. Seitdem gab es nur kleinere Änderungen, beispielsweise durch das Erste Gesetz zum Abbau bürokratischer Hemmnisse insbesondere in der mittelständischen Wirtschaft vom 22. August 2006 (BGBl. I S. 1970). 2008 legte die Bundesregierung dann gleich zwei Gesetzentwürfe zur Änderung des Bundesdatenschutzgesetzes vor:

- der erste befasst sich mit der Übermittlung personenbezogener Daten an Auskunfteien und der Verarbeitung und Nutzung personenbezogener Daten durch diese sowie mit der Durchführung von Scoringverfahren (siehe dazu unten Nr. 2.1.1),
- der zweite mit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten für Zwecke der Werbung und durch Adresshändler (siehe dazu unten Nr. 2.1.2).

2.1.1 Gesetz zur Änderung des Bundesdatenschutzgesetzes (Auskunfteien, Scoring)

Der Gesetzentwurf wurde im Juni 2009 von Bundestag und Bundesrat verabschiedet. Das Gesetz soll am 1. April 2010 in Kraft treten.

Nach seiner Begründung verfolgt das Gesetz das Ziel, die Regelungen des Bundesdatenschutzgesetzes für die Tätigkeit insbesondere von Auskunfteien der gestiegenen und weiter steigenden Bedeutung von Auskunfteien und dem vermehrten Einsatz von Scoringverfahren anzupassen (vergleiche Bundesrats-Drucksache 548/08). Zur Stärkung der Rechte der Betroffenen sollen die Transparenz der Verfahren verbessert und mehr Rechtssicherheit sowohl für die Betroffenen als auch für die Unternehmen und damit auch bessere Planungsmöglichkeiten für die Unternehmen geschaffen werden.

Das Gesetz sieht insbesondere folgende Neuerungen vor:

– Die Voraussetzungen für die Übermittlung von Angaben über eine Forderung, die trotz Fälligkeit nicht beglichen wurde, an Auskunfteien (sogenannte Einmeldung von Daten) werden präzise festgelegt. Derzeit gelten dafür die allgemeinen Vorschriften über die Übermittlung personenbezogener Daten für eigene Zwecke (§ 28 BDSG), die der Düsseldorfer Kreis, das oberste Gremium der Datenschutzaufsichtsbehörden von Bund und Ländern, für einen Teilbereich, nämlich die Einmeldung personenbezogener Daten durch Inkassounternehmen, präzisiert hat (vergleiche dazu zweiter Tätigkeitsbericht C 4.1, S. 37 ff.* und vierter Tätigkeitsbericht C 1.6, S. 40 ff.).

– Es wird ein spezieller Erlaubnistatbestand für bestimmte Übermittlungen personenbezogener Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung eines Vertrags im Rahmen eines Bankgeschäfts geschaffen. Diese Datenübermittlungen werden derzeit mangels spezieller Rechtsgrundlage auf eine Einwilligung des Betroffenen nach §§ 4 und 4 a BDSG gestützt (sogenannte Schufa-Klausel). Dies ist insofern problematisch, als in der Praxis eine natürliche Person einen Bankkredit regelmäßig nicht mehr ohne eine von der Bank angeforderte Bonitätsauskunft einer Auskunftei erhält, wobei diese mit einer Einwilligungserklärung des Betroffenen in die Übermittlung bestimmter personenbezogener Daten an diese Auskunftei verbunden wird. Mangels möglichen und zumutbaren Alternativverhaltens kann es daher zweifelhaft sein, ob die vom Betroffenen erteilte Einwilligung noch als freiwillig anzusehen ist.

– Die Erhebung und Verwendung sogenannter Scorewerte wird gesetzlich geregelt. Unter einem Scorewert versteht man einen Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen. Solche Scorewerte sollen als Entscheidungsgrundlage für die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit einem Betroffenen erhoben oder verwendet werden dürfen, wenn die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit erheblich sind und – je nach dem – die allgemeinen gesetzlichen Voraussetzungen für eine Datenübermittlung nach § 29 BDSG oder eine Datennutzung nach § 28 BDSG vorliegen. Sollen Anschriftendaten in die Scorewertberechnung einfließen (zum Beispiel die Tatsache, dass jemand in einer Straße wohnt, in der nach Informationen einer Auskunftei überdurchschnittlich viele Personen eine negative Bonität aufweisen), ist der Betroffene hierüber vorher zu unterrichten.

– Es wird klargestellt, dass Verhaltensweisen des Betroffenen, die der Herstellung von Markttransparenz dienen, zum Beispiel Anfragen zu den Kreditkonditionen verschiedener Banken, nicht in Scorewertberechnungen einfließen dürfen.

– Der Betroffene soll in Zukunft durch die für die Entscheidung oder die Scorewertberechnung verantwortliche Stelle über die während eines bestimmten Zeitraums errechneten Wahrscheinlichkeitswerte, die für die Wahrscheinlich-

* Die bei Querverweisen verwendeten Seitenangaben beziehen sich jeweils auf die gedruckten Ausgaben.

keitsberechnung genutzten Datenarten und das Zustandekommen der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form Auskunft erhalten können.

– Werden personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert, kann der Betroffene künftig einmal im Jahr eine unentgeltliche Auskunft nach § 34 BDSG verlangen.

– Geschätzte Daten müssen als solche kenntlich gemacht werden.

– Die Tatsache einer Datensperrung darf Dritten nicht mitgeteilt werden.

Das Gesetz ist alles in allem zu begrüßen, weil es in einigen Punkten Klarheit schafft und zu einheitlichen Verfahren der Auskunfteien führen wird. Dies gilt namentlich für die Einmeldung von Daten bei Auskunfteien und für die Auskunftserteilung über Scorewerte. An der einen oder anderen Stelle greift das Gesetz jedoch zu kurz beziehungsweise verzichtet darauf, seit langem kontrovers diskutierte Fragen einer Lösung zuzuführen. Kritisiert hatte der Bundesrat in seiner Stellungnahme [vergleiche Bundesrats-Drucksache 548/08 (B)] beispielsweise, dass der Gesetzentwurf

– teilweise hinter Verfahrensweisen zurückbleibt, die zwischen einzelnen Auskunfteien und den für sie zuständigen Aufsichtsbehörden in Bezug auf die Einmeldung von Daten bislang verabredet waren,

– nicht klar regelt, welche Daten(-arten) für die Scorewertberechnung herangezogen werden dürfen. Damit wird der Gesetzentwurf in diesem Punkt seiner Zielsetzung, die Transparenz der Verfahren zu verbessern und gleichzeitig mehr Rechtssicherheit für Unternehmen zu schaffen, nicht gerecht. Der Bundesrat war der Auffassung, dass wenigstens diejenigen Daten(arten) durch Gesetz festgelegt werden sollten, die nicht in die Berechnung von Wahrscheinlichkeitswerten einfließen dürfen. Dazu gehören nach seiner Meinung sensitive Daten im Sinne des § 3 Abs. 9 BDSG, Daten, die an die Anschrift des Betroffenen anknüpfen einschließlich der sogenannten Wohnumfelddaten sowie Schätzdaten;

– nicht klärt, unter welchen Voraussetzungen Auskunfteien nicht allgemein zugängliche Daten über die Kreditwürdigkeit eines Betroffenen (Bonitätsauskünfte) an nichtöffentliche Stellen übermitteln dürfen. Die Aufsichtsbehörden vertreten hierzu die Auffassung, Auskunfteien dürften Daten über die Kreditwürdigkeit nur übermitteln, wenn der Auskunftsuchende zumindest ein finanzielles Ausfallrisiko geltend macht. Demgegenüber vertreten Verbände und Unternehmen zum Teil die Auffassung, für die Auskunftserteilung genüge jedes wirtschaftliche Interesse;

– nicht regelt, ob und gegebenenfalls unter welchen Voraussetzungen eine Auskunftei eine Bonitätsauskunft erteilen darf, wenn der bei ihr gespeicherte Datensatz mit dem Anfragedatensatz nicht völlig übereinstimmt. Solche Fälle sind in der Praxis nicht selten;

– die Auskunftserteilung über die Herkunft und die Empfänger von Daten gegenüber dem bestehenden Rechtszustand nicht erweitert. Auskunfteien sollten die Auskunft nur verweigern dürfen, wenn *im Einzelfall* das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt;

– dem Betroffenen keinen Auskunftsanspruch einräumt, über die für einen Scorewert maßgeblichen Faktoren in absteigender Reihenfolge unterrichtet zu werden. Nur dann ist er in der Lage, seine Datenschutzrechte wahrzunehmen.

Der Deutsche Bundestag hat zwar den Gesetzentwurf bei seinen abschließenden Beratungen noch etwas nachgebessert, die Vorschläge des Bundesrats jedoch weitgehend unberücksichtigt gelassen.

2.1.2 Gesetz zur Änderung datenschutzrechtlicher Vorschriften (Werbung)

Anlass und wesentlicher Inhalt des Gesetzentwurfs

Im August 2008 wurde bekannt, dass Call-Center und andere Unternehmen an einem Datenhandel mit Namen, Anschriften, Telefonnummern und Kontoverbindungsdaten vieler Millionen Bürger beteiligt waren. In der Folge wurden die bestehenden gesetzlichen Regelungen für den Adresshandel und die werbliche Nutzung personenbezogener Daten in Frage gestellt und Vorschläge zur Verbesserung des Persönlichkeitsrechts der Betroffenen erörtert. Auf Antrag Baden-Württembergs beschloss der Bundesrat Anfang September 2008 eine Reihe von Prüfaufträgen an die Bundesregierung.

Nahezu zeitgleich fand beim Bundesminister des Innern ein Gespräch unter anderem mit Datenschutzbeauftragten und Datenschutzaufsichtsbehörden aus Bund und Ländern (sogenannter Datenschutzgipfel) statt. Ein wesentliches Ergebnis war, das bislang bestehende sogenannte „Listenprivileg“ zwar nicht abzuschaffen, aber spürbar einzuschränken. Dieses gestattet es Unternehmen, Vereinen und Verbänden, bestimmte ihnen etwa aus Vertragsabschlüssen bekannt gewordene personenbezogene Daten, zu denen insbesondere die Postanschrift gehört, für Zwecke der Werbung oder der Markt- und Meinungsforschung zu verwenden oder anderen Unternehmen hierfür zu übermitteln, sofern kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Anschluss der Nutzung oder Übermittlung hat und der Betroffene dieser Verarbeitung und Nutzung nicht widersprochen hat.

Ferner sollten

- die Bußgeldtatbestände für Datenschutzverstöße erweitert,
- Möglichkeiten zur Abschöpfung unrechtmäßiger Gewinne aus illegaler Datenverwendung geschaffen und
- ein gesetzliches Koppelungsverbot für marktbeherrschende Unternehmen eingeführt werden, das verhindern soll, dass diese ein Angebot davon abhängig machen, dass die Betroffenen ihre Einwilligung zu einer weitergehenden Verarbeitung und Nutzung ihrer personenbezogenen Daten geben, als dies zur Erbringung des Angebots notwendig ist.

Der vom Bundesministerium des Innern ausgearbeitete Referentenentwurf trug diesem Ergebnis des Datenschutzgipfels Rechnung und sah insbesondere eine Einschränkung des Listenprivilegs vor: Danach sollte die bisher ohne Einwilligung zulässige Übermittlung bestimmter personenbezogener Daten an andere Unternehmen zum Zweck der Fremdwerbung künftig grundsätzlich nur noch mit Einwilligung des Betroffenen zulässig sein.

Weiterer Bestandteil des Gesetzentwurfs war ein Datenschutzaudit-Gesetz, mit dem dem in § 9 a BDSG enthaltenen Gesetzesauftrag Rechnung getragen werden sollte. Es sah Regelungen dafür vor, auf welche Weise Daten verarbeitende Stellen ihr Datenschutzkonzept und Anbieter von Datenverarbeitungsanlagen und -programmen diese von unabhängigen Stellen überprüfen lassen und dafür eine Art Gütesiegel erhalten können.

Auch wenn der Gesetzentwurf noch eine Reihe weiterer Änderungen beinhaltete, konzentrierte sich die daran vorgebrachte Kritik zum einen auf das Listenprivileg und zum anderen auf das Datenschutzaudit.

- Kritik an der geplanten Änderung des Listenprivilegs:

  Betroffene Unternehmen, Vereinigungen und Verbände wandten sich im Rahmen des Anhörungsverfahrens sowie durch unmittelbare Ansprache beteiligter Stellen insbesondere gegen eine Einschränkung des Listenprivilegs. Sie brachten vor, die im Gesetzentwurf vorgesehenen Regelungen beeinträchtigten die Direktwerbung und einzelne besonders darauf angewiesene Branchen massiv und führten zur Vernichtung von Arbeitsplätzen.

– Kritik am Datenschutzaudit:

  Die Reaktionen auf den vorgelegten Gesetzentwurf für ein Datenschutzaudit waren fast durchweg negativ. Auch wenn das Ziel, ein solches Gütesiegel einzuführen, überwiegend geteilt wurde, war man sich in der Kritik einig, dass die im Entwurf enthaltenen Regelungen ungeeignet sind, dieses Ziel zu erreichen.

Stellungnahme des Bundesrats

Der unter Berücksichtigung dieser Kritik fortgeschriebene und vom Bundeskabinett am 10. Dezember 2008 beschlossene Gesetzentwurf (vergleiche Bundesrats-Drucksache 4/09) behielt die vorgesehenen Neuregelungen hinsichtlich des Listenprivilegs und des Datenschutzaudit-Gesetzes jedoch bei. Auch der Bundesrat hatte nur zwei grundsätzliche Einwände [vergleiche Bundesrats-Drucksache 4/09 (B)]. Er forderte,

– die Tätigkeit der Markt- und Meinungsforschungsinstitute besser abzusichern und

– das Datenschutzaudit-Gesetz entweder ganz zu streichen oder grundlegend zu überarbeiten. Der Bundesrat kritisierte

  • die damit verbundene überbordende und überflüssige Bürokratie;

  • das vorgesehene Verfahren der Zulassung und Überwachung der Stellen, die zukünftig die Befugnis erhalten sollen, bei Daten verarbeitenden Stellen im nichtöffentlichen Bereich Datenschutzkonzepte und informationstechnische Einrichtungen zu kontrollieren. Es führe zu einem unverhältnismäßig hohen Verwaltungsaufwand bei den Aufsichtsbehörden der Länder;

  • das unklare Verhältnis der privaten Kontrollstellen zur Selbstkontrolle durch Beauftragte für den Datenschutz und zur Fremdkontrolle durch die Aufsichtsbehörden für den nichtöffentlichen Bereich.

Im Übrigen regte der Bundesrat – teilweise auf Antrag, im Übrigen mit Unterstützung Baden-Württembergs – weitere datenschutzrechtliche Verbesserungen an, insbesondere

– die Vorschriften über die Datenverarbeitung im Auftrag (§ 11 Abs. 2 Satz 2 BDSG) klarer zu fassen. Die Auftraggeber müssten besser als derzeit erkennen können, dass sie Auftragnehmern *schriftlich* konkrete Vorgaben in Bezug auf die Datenerhebung, -verarbeitung und -nutzung machen müssten. Des Weiteren müssten Häufigkeit, Tiefe und Dokumentation der vom Auftragnehmer vorzunehmenden Kontrollen in § 11 Abs. 2 Satz 4 BDSG näher geregelt werden. Anlass für diese Forderung war der in der Kontodaten-Affäre zutage getretene rechtswidrige Umgang von Callcenter-Mitarbeitern mit personenbezogenen Daten;

– in das Bundesdatenschutzgesetz eine Verordnungsermächtigung aufzunehmen, um anschließend die Anforderungen an die Fachkunde der Beauftragten für den Datenschutz durch Rechtsverordnung konkretisieren zu können. In der Praxis ist nämlich festzustellen, dass ein Teil der Beauftragten für den Datenschutz nicht über die zur Erfüllung ihrer Aufgaben erforderlichen Mindestkenntnisse, namentlich des Datenschutzrechts, verfügt. Eine effektive Selbstkontrolle der Einhaltung datenschutzrechtlicher Vorschriften durch die nichtöffentlichen Stellen ist damit oftmals nicht gewährleistet. Eine solche ist jedoch zur Verhinderung von Datenschutzverstößen und zur Unterstützung der nur über begrenzte Ressourcen verfügenden Aufsichtsbehörden unabdingbar;

– die Anordnungsbefugnisse der Aufsichtsbehörden zu erweitern. Sie müssen über § 38 Abs. 5 BDSG hinaus generell Anordnungen und Untersagungsverfügungen in Bezug auf eine materiell rechtswidrige Datenerhebung, -verarbeitung und -nutzung oder wegen sonstiger Verstöße gegen datenschutzrechtliche Vorschriften erlassen können. Aufsichtsbehörden müssen ihre Rechtsauffassung auch dann gegenüber einer nichtöffentlichen Stelle durchsetzen können, wenn diese sie nicht teilt. Durch Erlass eines Bußgeldbescheids kann eine verbindliche Klärung der Rechtslage nicht herbeigeführt werden, ganz abgesehen davon, dass dies auch nicht der richtige Weg ist;

– weitere Bußgeldtatbestände zu schaffen. Mit einem Bußgeld sollte beispielsweise belegt werden können, wer

  • entgegen § 9 BDSG unzureichende technische oder organisatorische Maßnahmen zur Gewährleistung der Datensicherheit trifft und dadurch ermöglicht, dass Unbefugte personenbezogene Daten zur Kenntnis nehmen können (siehe dazu den unter B 3.1 dargestellten Fall),

  • beharrlich gegen die Informations- und Unterrichtungspflichten des § 4 Abs. 3 BDSG verstößt (vergleiche dazu Abschnitt B des vierten Tätigkeitsberichts, S. 19 ff.),

  • als Auftraggeber einen Datenverarbeiter im Auftrag nicht ausreichend kontrolliert (siehe dazu die unter B 3.1 und 9.2 dargestellten Fälle),

  • unbefugt eine Telefon- oder Telefaxnummer oder eine E-Mail-Adresse für Werbezwecke nutzt. Die im Gesetz gegen den unlauteren Wettbewerb (UWG) neu geschaffene Ahndungsmöglichkeit der Bundesnetzagentur in Fällen unbefugter Telefonwerbung reicht nicht aus. Aufsichtsbehörden sollten eine entsprechende Ahndungsmöglichkeit erhalten. Überdies sollte auch unerlaubte Telefax- und E-Mail-Werbung jedenfalls dann bußgeldbewehrt sein, wenn der Verantwortliche beharrlich gegen § 7 UWG verstößt.

Weiteres Verfahren

Ungeachtet der Kritik hat die Bundesregierung den Gesetzentwurf im Wesentlichen unverändert in den Bundestag eingebracht. Er wurde Anfang Juli 2009 von Bundestag und Bundesrat mit erheblichen Änderungen verabschiedet. Auf das Audit-Gesetz wurde verzichtet. Von der ursprünglich vorgesehenen Einwilligungslösung ist bei Lichte besehen nicht allzu viel übrig geblieben; daneben gelten das Listenprivileg und die Widerspruchslösung fort. Neu sind im Werbebereich einige der Transparenz der Datenverwendung dienende Regelungen zur Angabe der verantwortlichen Stelle und zur Herkunft der Daten. Zum Ausgleich für dieses Eingehen auf die Forderungen der Wirtschaft wurden an anderer Stelle einige Vorschläge des Bundesrats aufgegriffen, beispielsweise wurden die Regelungen über die Datenverarbeitung im Auftrag teilweise neu gefasst und die Befugnisse der Aufsichtsbehörden erweitert.

Das Gesetz soll bereits am 1. September 2009 in Kraft treten. Es sieht jedoch eine Übergangsregelung für die Verarbeitung und Nutzung vor diesem Zeitpunkt erhobener und gespeicherter Daten für Zwecke der Markt- und Meinungsforschung und der Werbung vor.

2.2 Gesetz zur Bekämpfung unerlaubter Telefonwerbung

Das zwar verabschiedete, jedoch bei Redaktionsschluss für diesen Tätigkeitsbericht noch nicht verkündete Gesetz zur Bekämpfung unerlaubter Telefonwerbung und zur Verbesserung des Verbraucherschutzes bei besonderen Vertriebsformen stärkt die Rechte der Verbraucher und des Datenschutzes. Es sieht unter anderem vor, dass

– telefonisch geschlossene Verträge zur Erbringung von Wett- und Lotterie-Dienstleistungen vom Verbraucher widerrufen werden können (vergleiche § 312 d Abs. 4 Nr. 4 des Bürgerlichen Gesetzbuchs – BGB),

– telefonische Werbung gegenüber einem Verbraucher grundsätzlich nur nach vorheriger *ausdrücklicher* Einwilligung zulässig ist (vergleiche § 7 Abs. 2 Nr. 2 UWG),

– bei telefonischer Werbung die Rufnummernanzeige des Anrufers nicht unterdrückt werden darf (§ 102 Abs. 2 des Telekommunikationsgesetzes – TKG),

– ein Werbeanruf mit unterdrückter Rufnummer mit einem Bußgeld geahndet werden kann (vergleiche § 149 Abs. 1 Nr. 17 c TKG) sowie dass

– unerlaubte telefonische Werbung von der Bundesnetzagentur mit einer Geldbuße bis zu 50.000 Euro geahndet werden kann (vergleiche § 20 Abs. 1 bis 3 UWG).

2.3 Arbeitnehmerdatenschutzgesetz

Ein Arbeitnehmerdatenschutzgesetz oder jedenfalls gesetzliche Regelungen zum Arbeitnehmerdatenschutz werden schon seit langem gefordert. Der Deutsche Bundestag hat daran in einer einstimmig gefassten Entschließung vom 20. März 2007 zum 20. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz noch einmal erinnert:

„Der Deutsche Bundestag erwartet von der Bundesregierung, dass sie seine mehrfach erhobene Forderung aufgreift, den Arbeitnehmerdatenschutz gesetzlich zu regeln, und unverzüglich einen Gesetzentwurf vorlegt." Auch der Bundesrat hat die Bundesregierung in einer Entschließung vom 7. November 2008 gebeten, „angesichts der Vorfälle von Arbeitnehmerüberwachung in Unternehmen und angesichts der für Arbeitgeber wie Arbeitnehmer unübersichtlichen Gesetzeslage eine gesetzliche Regelung zum Arbeitnehmerdatenschutz vorzulegen".

Nachdem die Medien über weitere Fälle angeblich unzulässiger Erhebung und Verarbeitung von Mitarbeiterdaten durch Großunternehmen berichtet hatten, kündigte der Bundesminister des Innern im Februar 2009 an, in der nächsten Legislaturperiode ein Gesetz zum Schutz der Arbeitnehmerdaten in Betrieben auf den Weg zu bringen. Eine erste Regelung wurde jedoch bereits in das von Bundestag und Bundesrat soeben verabschiedete Gesetz zur Änderung datenschutzrechtlicher Vorschriften (dazu oben Nr. 2.1.2) aufgenommen. Ein neuer § 32 BDSG sieht vor, dass personenbezogene Daten eines Beschäftigten, zu denen auch Bewerber für ein Beschäftigungsverhältnis zählen, unabhängig von der Art ihrer Verarbeitung erhoben, verarbeitet oder genutzt werden dürfen, wenn dies für die Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich ist. Zur Aufdeckung von Straftaten sollen personenbezogene Daten eines Mitarbeiters nur dann verwendet werden dürfen, „wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Datenverwendung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Betroffenen am Ausschluss der Datenverarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind".

Die Befassung mit Fragen des Arbeitnehmerdatenschutzes in der Praxis macht immer wieder deutlich, wie dringlich klare gesetzliche Regelungen sind. Geregelt werden sollte beispielsweise,

- welche Unterlagen einschließlich der in Dateien gespeicherten Informationen zur Personalakte eines Beschäftigten gehören (Personalaktendaten), für welche Zwecke diese Daten verwendet werden dürfen und wer unter welchen Voraussetzungen Zugang zu ihnen erhalten darf. Die Aufsichtsbehörde stellt in der Praxis immer wieder fest, welche Unsicherheit darüber besteht, was zu den Personalakten gehört. Festzustellen ist auch, dass zu den Personalaktendaten zumeist großzügig Zugang gewährt wird. Hinweise auf die hierzu bestehenden gesetzlichen Regelungen für Beamte werden regelmäßig damit abgetan, die Verhältnisse im öffentlichen Dienst und in der Wirtschaft seien zu unterschiedlich, um auf diese Regelungen zurückzugreifen;
- welche Daten von Bewerbern beziehungsweise bei der Einstellung eines Beschäftigten erhoben werden dürfen (Fragerecht des Arbeitgebers), auch inwieweit Eignungstests zulässig sind;
- ob im Falle der Ablehnung eines Bewerbers die von diesem eingereichten Unterlagen zurückzugeben sowie ob und wie lange sie vom Arbeitgeber zu Dokumentationszwecken, auch wegen etwaiger Schadensersatzforderungen abgelehnter Bewerber nach dem Allgemeinen Gleichbehandlungsgesetz, aufbewahrt werden dürfen;
- inwieweit die dienstliche oder private Internet- und E-Mail-Nutzung am Arbeitsplatz vom Arbeitgeber ausgewertet werden darf;
- ob und gegebenenfalls unter welchen Voraussetzungen Telefongespräche von Mitarbeitern zu Kontrollzwecken mitgehört werden dürfen. Ein solches Mithören ist beispielsweise bei Callcentern und Markt- und Meinungsforschungsinstituten weit verbreitet;

– (ob und) inwieweit die offene Videoüberwachung von Arbeitnehmern in nicht öffentlich zugänglichen Bereichen und damit außerhalb des Anwendungsbereichs des § 6 b BDSG, die heimliche Videoüberwachung, deren Voraussetzungen von der arbeitsgerichtlichen Rechtsprechung entwickelt wurden, und die Überwachung von Arbeitnehmern durch Detektive oder unter Einsatz anderer technischer Hilfsmittel (beispielsweise Global Positioning System GPS) zulässig sind;

– in welchen Grenzen Leistungskontrollen von Arbeitnehmern zulässig sind;

– unter welchen Voraussetzungen von einem Arbeitnehmer Gesundheitsdaten erhoben, verarbeitet und genutzt werden dürfen (siehe dazu die Beispiele unter B 1.5 und 1.6) und

– inwieweit im Arbeitsverhältnis angesichts der schwächeren Position des Arbeitnehmers gegenüber dem Arbeitgeber und damit bestehender Zweifel an der Freiwilligkeit die Einwilligung des Betroffenen Rechtsgrundlage für die Datenerhebung, -verarbeitung und -nutzung sein kann.

2.4 Glücksspielstaatsvertrag und Ausführungsgesetz dazu

Der 2007 unterzeichnete Staatsvertrag der Länder zum Glücksspielwesen (Glücksspielstaatsvertrag), der durch Gesetz vom 11. Dezember 2007 (GBl. S. 571) in Landesrecht überführt wurde, enthält auch einige datenschutzrechtlich bedeutsame Regelungen:

– So wird die Werbung für öffentliches Glücksspiel im Internet und über Telekommunikationsanlagen verboten. Dies gilt auch für die Süddeutsche Klassenlotterie (SKL). Aufgrund dieses Verbots erreichen uns inzwischen keine Beschwerden mehr über Unternehmen, die in der Vergangenheit Betroffene ohne deren vorherige Einwilligung angerufen haben, um für die Teilnahme am Glücksspiel zu werben.

– Zum Schutz der Spieler und zur Bekämpfung der Glücksspielsucht sind die Spielbanken und die Toto-Lotto Gesellschaften verpflichtet, ein übergreifendes Sperrsystem zu unterhalten. Die zur Teilnahme am Sperrsystem verpflichteten Veranstalter sperren Personen, die dies selbst beantragen (Selbstsperre) oder von denen sie aufgrund der Wahrnehmungen ihres Personals, aufgrund von Meldungen Dritter oder aufgrund sonstiger tatsächlicher Anhaltspunkte annehmen müssen, dass sie spielsuchtgefährdet oder überschuldet sind, ihren finanziellen Verpflichtungen nicht nachkommen oder Spieleinsätze riskieren, die in keinem Verhältnis zu ihrem Einkommen oder Vermögen stehen (Fremdsperre). Die Sperre beträgt mindestens ein Jahr.

– Die Veranstalter von Glücksspiel haben Name und Anschrift, Geburtsdatum und -ort, Lichtbilder sowie Grund und Dauer einer Spielersperre in eine Sperrdatei einzutragen. Der Staatsvertrag selbst und das Gesetz zur Ausführung des Staatsvertrags zum Glücksspielwesen in Deutschland vom 4. März 2008 (GBl. S. 81) enthalten nähere Regelungen zu den Spielersperren, zur Sperrdatei, zur Mitteilung von Spielersperren an die Sperrdatei sowie zur Verarbeitung und Nutzung der in der Sperrdatei gespeicherten Daten, zur Auskunftserteilung an Betroffene über die in der Sperrdatei gespeicherten Daten und zu erforderlichen technischen und organisatorischen Schutzmaßnahmen.

2.5 Gesetz zur Änderung des Landesjustizkostengesetzes

Der Forderungseinzug für die Justiz wurde bislang vollständig von der Landesoberkasse Baden-Württemberg durchgeführt. Durch das Gesetz zur Änderung des Landesjustizkostengesetzes und anderer Vorschriften vom 14. Oktober 2008 (GBl. S. 333) wurde auf Anregung des Rechnungshofs die Möglichkeit geschaffen, im Rahmen eines auf drei Jahre angelegten Pilotprojekts zu untersuchen, ob durch die Beteiligung privater, auf Forderungseinziehung spezialisierter Unternehmen der Einzug niedergeschlagener Justizkostenforderungen und die Abwicklung von Prozesskostenhilfefällen verbessert werden kann.

Im Vorfeld waren sich alle mit dem Vorhaben befassten Stellen letztlich einig, dass das Landesdatenschutzgesetz für das Pilotprojekt keine ausreichende Rechts-

grundlage darstellt und es dafür einer bereichsspezifischen Datenschutzvorschrift bedarf, da die Gerichtskostenschuldner bisher nicht damit rechnen müssen, dass die Vollstreckungsbehörden so sensible personenbezogene Daten an ein privates Inkassounternehmen übermitteln. Überdies zielt die Zusammenarbeit gerade darauf ab, dass das Inkassounternehmen seinerseits weitere Daten über Schuldner, beispielsweise Bonitätsdaten eines Schuldners bei einer Auskunftei, erhebt und zur Verbesserung des Forderungseinzugs nutzt. Um dem informationellen Selbstbestimmungsrecht des Betroffenen Rechnung zu tragen, setzt der neue § 9 a des Justizkostengesetzes der Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch öffentliche und private Stellen Grenzen:

– Die Vollstreckungsbehörden dürfen nur bestimmte Daten eines Schuldners sowie Informationen über die bisherigen Beitreibungsmaßnahmen an das beauftragte Inkassounternehmen übermitteln und zwar grundsätzlich nur nach rechtzeitiger vorheriger Ankündigung.

– Das Inkassounternehmen darf die Daten nur streng zweckgebunden speichern und nutzen und an Dritte, insbesondere Auskunfteien, nur übermitteln, um von diesen Adress- und Bonitätsdaten zu erheben. Weitere Voraussetzung für die Datenübermittlung an Auskunfteien und Adresshändler ist, dass sich diese verpflichten, die Daten nicht an Dritte zu übermitteln und nur streng zweckgebunden zu verwenden.

– Die Vollstreckungsbehörden dürfen sich im Übrigen nur an sorgfältig ausgewählte schriftlich beauftragte private Stellen wenden, die insbesondere die notwendigen technischen und organisatorischen Maßnahmen gewährleisten. Die Regelung orientiert sich an der Vorschrift über die Auftragsdatenverarbeitung (§ 11 BDSG).

– Die Vollstreckungsbehörden dürfen zur Unterstützung des Forderungseinzugs und zur Bewertung auch selbst Adressdaten beim Adresshandel und Bonitätsdaten bei einer Auskunftei erheben und diesen Stellen die dafür erforderlichen Schuldnerdaten überlassen, wenn eine Weiterübermittlung der Daten ausgeschlossen und die Zweckbindung sichergestellt ist. Die Vollstreckungsbehörden dürfen die auf diese Weise erhobenen personenbezogenen Daten in dem erforderlichen Umfang speichern und nutzen. Soweit es sich dabei um Negativdaten von Betroffenen handelt, müssen diese möglichst frühzeitig zumindest gesperrt werden.

Die Aufsichtsbehörde wird die Einhaltung dieser Vorschriften durch die am Pilotprojekt beteiligten privaten Stellen überwachen.

Falls das Projekt erfolgreich verlaufen und auf andere Forderungen des Landes und der Kommunen übertragen werden sollte, müssten dafür vergleichbare rechtliche Regelungen geschaffen werden.

B Einzelne Tätigkeitsbereiche

1 Arbeitnehmerdatenschutz

1.1 Überwachung von Mitarbeitern eines Discounters unter Einsatz von Videotechnik und Detektiven

Ende März 2008 hatten Medien bundesweit berichtet, Mitarbeiter eines Discounters würden systematisch durch Detekteien oder andere Sicherheitsunternehmen überwacht. Als Belege wurden Auszüge aus Einsatzberichten veröffentlicht, in denen unter anderem Informationen aus dem Privatleben, zum Beispiel über Beziehungsprobleme oder finanzielle Schwierigkeiten, sowie über das Verhalten der Kollegen bei der Arbeit und im Umgang miteinander protokolliert waren.

Auftraggeber der Sicherheitsunternehmen, die diese Einsatzberichte angefertigt hatten, waren rechtlich selbstständige Vertriebsgesellschaften. Daher leiteten die

für die Unternehmenssitze zuständigen zwölf Datenschutzaufsichtsbehörden datenschutzrechtliche Überprüfungsverfahren ein. Da die unternehmensintern mit der bundesweiten Aufklärung der Vorgänge beauftragte zentrale Dienstleistungsgesellschaft des Discounters ihren Sitz in Baden-Württemberg hat, übernahm die baden-württembergische Aufsichtsbehörde dabei die Koordinierung der Datenschutzüberprüfungen.

1.1.1 Mängel der früheren Vorgehensweise

Die Aufsichtsbehörden stellten fest, dass die Vertriebsgesellschaften mit ihrer bis Ende März 2008 praktizierten Verfahrensweise in unterschiedlichem Ausmaß gegen Datenschutzvorschriften verstießen.

(Video-)Beobachtung von Mitarbeitern durch einen Ladendetektiv mit Kamera

Zahlreiche Vertriebsgesellschaften hatten im Untersuchungszeitraum 1. Januar 2006 bis Ende März 2008 vor allem „zur Verringerung inventurrelevanter Verluste“ in mehr als 900 Fällen Sicherheitsunternehmen meist mündlich und ohne exakte Formulierung des Auftrags mit der Durchführung kameragestützter Einsätze in Filialen des Discounters beauftragt (sogenannter „Ladendetektiv mit Kamera“). In der Regel erfolgte der Einsatz so, dass ein Mitarbeiter des Sicherheitsunternehmens (nachfolgend: Detektiv) für die Mitarbeiter erkennbar für eine Woche in die Filiale kam. Der Detektiv nutzte in dieser Zeit selbst installierte Miniaturkameras oder im Verkaufsraum bereits vorhandene Kameras.

Insbesondere drei der seit 2006 für die unterschiedlichsten Aufgaben eingesetzten Sicherheitsunternehmen erstellten im Rahmen ihrer Aufträge umfassende Revisionsberichte. Neben den Kunden beobachteten die Detektive heimlich auch die Mitarbeiter. Ihnen gegenüber begründeten sie ihren Einsatz mit der Aufklärung von inventurrelevanten Verlusten und der Aufdeckung von Kundendiebstählen. Die Detektive hörten Gespräche der Mitarbeiter und deren (private) Telefonate mit, führten mit ihnen Gespräche über sich und Dritte (Vorgesetzte und Kollegen) und legten alles in schriftlichen Einsatzberichten nieder. Die Einsatzberichte enthielten unter anderem folgende mitarbeiterbezogenen Feststellungen und Bewertungen:

– Mitteilungen, die sich auf Inventurdifferenzen bezogen,
– Einschätzungen der Arbeitsleistung, -fähigkeit und -motivation der Mitarbeiter,
– Informationen zum Mitarbeiterverhalten gegenüber Kunden,
– Informationen, die sich auf die Einhaltung organisatorischer oder arbeitsvertraglicher Pflichten bezogen,
– Informationen zum Führungsverhalten und zu den Führungsqualitäten der Vorgesetzten in den Filialen,
– Informationen über das Pausenverhalten einzelner Mitarbeiter,
– Informationen über persönliche Problemlagen,
– Informationen über Zwischenmenschliches und daran anknüpfende Beurteilungen,
– Informationen zum Gesundheitszustand sowie zu (möglichen) Schwangerschaften,
– Informationen über die finanzielle Situation der Mitarbeiter und ihrer Familien,
– Informationen über Ereignisse, die aus Sicht des Detektivs einen wie auch immer gearteten Verdacht gegen einen oder mehrere Mitarbeiter begründeten und
– Informationen über die (vermutete) Stimmungslage und Wesensart der Mitarbeiter.

Die drei Sicherheitsunternehmen führten im Untersuchungszeitraum rund 350 solcher Einsätze für mehr als 20 regionale Vertriebsgesellschaften durch und erstellten darüber Einsatzberichte. Davon standen den Datenschutzaufsichtsbehörden noch etwa 170 zur Auswertung zur Verfügung. Der Rest war bereits vernichtet. In Baden-Württemberg gab es keine Einsatzberichte mehr.

Die Aufsichtsbehörden kamen nach eingehender Überprüfung zu dem Ergebnis, dass die Vertriebsgesellschaften, die immer wieder die drei Sicherheitsunternehmen beauftragten, von denen sie wussten, dass sie Berichte mit solchen unzulässigen Inhalten anfertigen, für das Geschehen datenschutzrechtlich verantwortlich sind. Die mit Erstellung und Verwendung der Einsatzberichte verbundenen Datenschutzverstöße waren vielfach schwerwiegend. Die Datenschutzaufsichtsbehörden der Länder, die solche Verstöße feststellten, belegten deshalb die zwölf dafür verantwortlichen Vertriebsgesellschaften mit einem Bußgeld zwischen 3.000 und 15.000 Euro je Bericht.

Heimliche Beobachtung von Mitarbeiter durch Kameraeinsatz

In rund 80 Fällen hatten Vertriebsgesellschaften in nahezu allen Bundesländern Sicherheitsunternehmen damit beauftragt, im Kassenbereich von Filialen, mitunter aber auch in den Mitarbeitern vorbehaltenen Nebenräumen, beispielsweise im Bereich der Mitarbeiterspinde, von Türen und Fenstern oder im Pausenraum eine verdeckte Observation mit Kameras durchzuführen. Dabei wurden ohne Kenntnis der Filialmitarbeiter meist mehrere Minikameras so in der Filiale angebracht, dass sie von diesen in der Regel nicht entdeckt wurden. Die von den Kameras in Abwesenheit der Detektive erfassten Daten wurden für den Zeitraum des gesamten, in der Regel eine Woche dauernden Einsatzes aufgezeichnet. Anschließend wurden die Videodaten von den Sicherheitsunternehmen nach Auffälligkeiten, zum Beispiel aufgezeichneten Diebstählen oder anderen Straftaten durch Kunden oder Mitarbeiter oder Verstößen gegen betriebliche Vorschriften ausgewertet. Für die auftraggebende Vertriebsgesellschaft wurde sodann ein Bericht gefertigt. 29 derartiger Berichte sowie eine größere Zahl von Videoaufzeichnungen lagen den Datenschutzaufsichtsbehörden vor. In Baden-Württemberg konnten keine Unterlagen mehr aufgefunden werden.

Datenschutzrechtlich ließ sich die heimliche Videoüberwachung der Mitarbeiter nur in einem Teil der Fälle rechtfertigen. In anderen Fällen wurden Daten von Mitarbeitern unbefugt erhoben, verarbeitet oder genutzt. Die Datenschutzaufsichtsbehörden haben dies gerügt und in Einzelfällen auch mit einem Bußgeld geahndet.

Nichtbestellung betrieblicher Datenschutzbeauftragter

Alle Vertriebsgesellschaften hatten bis Anfang Juni 2008 keinen Beauftragten für den Datenschutz bestellt, obwohl sie nach § 4 f des Bundesdatenschutzgesetzes hierzu verpflichtet gewesen wären.

Beauftragte für den Datenschutz haben die Aufgabe, in den Unternehmen auf die Einhaltung des Datenschutzes hinzuwirken. Angesichts des Umfangs und der Art der Erhebung, Verarbeitung und Nutzung personenbezogener Daten wäre es bei den Vertriebsgesellschaften des Discounters besonders dringlich gewesen, über betriebliche Datenschutzbeauftragte zu verfügen. Durch deren Einsatz hätte es möglicherweise vermieden werden können, dass es zu so schwerwiegenden Verstößen kam. Die Datenschutzaufsichtsbehörden haben daher jede der 35 Vertriebsgesellschaften mit einem Bußgeld in Höhe von 10.000 Euro belegt.

Als Fazit konnte am Ende der Untersuchung festgestellt werden, dass zwar insgesamt keine flächendeckende, also alle Filialen betreffende Überwachung vorgenommen wurde, es sich angesichts der Zahl der durchgeführten Einsätze aber auch nicht nur um Einzelfälle handelte. Zumindest einige Vertriebsgesellschaften hatten vielmehr regelmäßig derartige Einsätze in Auftrag gegeben. Dem entsprachen die von den Aufsichtsbehörden gegen die 35 regionalen Vertriebsgesellschaften verhängten Bußgelder in Höhe von annähernd 1,5 Millionen Euro.

Anzuerkennen war, dass die betroffenen Unternehmen nach den Presseberichten sofort reagiert, die Videoüberwachungsgeräte abgebaut, den Einsatz von Detektiven gestoppt und damit begonnen haben, bislang fehlende Datenschutzkonzeptionen zu erarbeiten.

1.1.2 Neukonzeption

Da der Discounter künftig wieder Videoüberwachung und auch Detektive in den Filialen einsetzen will, erarbeitete die zentrale Dienstleistungsgesellschaft hierfür ein

Gesamtkonzept und legte dieses der Aufsichtsbehörde zur Begutachtung vor. Diese machte deutlich, dass für sie insbesondere folgende Punkte von Bedeutung sind:

– Dass in einem Teil der Filialen Diebstähle und auch Überfälle auf Mitarbeiter vorkommen, rechtfertigt nicht die Überwachung aller Filialen unter Einsatz von Videotechnik und Detektiven. Es muss vielmehr filialbezogen festgestellt werden, dass Überwachungsmaßnahmen zur Verhinderung von Straftaten oder zu deren Aufklärung oder aus einem sonstigen rechtfertigenden Grund im Sinne des § 6 b BDSG erforderlich sind. Dies hat im konkreten Fall zur Folge, dass in einem Teil der Filialen keine Überwachung stattfindet.

– Es ist jeweils sehr genau zu prüfen, worauf sogenannte Inventurverluste zurückzuführen sind. Anzunehmen, Ursache seien stets strafbare Handlungen von Kunden oder Mitarbeitern, weshalb eine Videoüberwachung gerechtfertigt sei, ist nicht zwingend. Die Aufsichtsbehörde hat es daher begrüßt, dass das vorgelegte Konzept hierfür ein Prüfschema vorsieht.

– Mitarbeiter dürfen in öffentlich zugänglichen Räumen nur unter Beachtung des § 6 b BDSG offen überwacht werden. Für die offene Videoüberwachung von Mitarbeitern in anderen Räumen, beispielsweise Aufenthaltsräumen, fehlt es derzeit ebenso an einem ausdrücklichen Erlaubnistatbestand wie für die heimliche Videoüberwachung von Arbeitnehmern (siehe dazu oben A 2.3). Die arbeitsgerichtliche Rechtsprechung lässt jedoch beide Maßnahmen unter den von ihr entwickelten Voraussetzungen zu. Bis zur Schaffung entsprechender Regelungen in einem Arbeitnehmerdatenschutzgesetz kann dies hingenommen werden. Notwendig ist jedoch, dass die verantwortliche Stelle das Vorliegen dieser Voraussetzungen in jedem Einzelfall sorgfältig prüft und das Ergebnis schriftlich dokumentiert. Im konkreten Fall will der Discounter auf offene Videoüberwachung in nicht öffentlich zugänglichen Räumen und heimliche Videoüberwachung verzichten. Dies ist zu begrüßen.

– Soweit Überwachungsmaßnahmen in einer Filiale danach grundsätzlich zulässig sind, sind sie – was Intensität und räumliche sowie zeitliche Ausdehnung angeht – auf das Erforderliche zu beschränken. Eine notwendige Eskalation sollte in Stufen erfolgen, die klar definiert sind. Eine Ausweitung der Überwachung kommt dabei erst in Betracht, wenn zuvor die weniger tief in die Persönlichkeitsrechte eingreifende Maßnahme erfolglos eingesetzt wurde.

– In regelmäßigen, nicht zu langen Zeitabständen ist zu prüfen, ob eine Videoüberwachungsmaßnahme noch gerechtfertigt ist.

– Aufträge an Detektive sollten stets schriftlich erteilt werden. Deren Aufgaben sollten ebenfalls schriftlich festgelegt und exakt beschrieben sein. Die Mitarbeiter sollten hierüber unterrichtet werden. Detektiven sollte es untersagt sein, Protokolle über das Verhalten von Mitarbeitern zu erstellen.

– Es müssen die erforderlichen technischen und organisatorischen Maßnahmen getroffen werden. In Betracht kommen unter anderem folgende Maßnahmen:

  • Vier-Augen-Prinzip beim Zugriff auf aufgezeichnete Videodaten,

  • Schutz der Aufzeichnungsgeräte vor unberechtigtem Zugriff,

  • Vorschriften über die (deutlich sichtbare) Anbringung der Kameras,

  • die – auch bei schwenk- und zoombaren Kameras vorgesehene – Ausblendung der (Kassen-)Mitarbeiter sowie der PIN-Pads, über die die Kunden bei EC-Karten-Zahlung ihre PIN-Nummer eingeben.

– Sämtliche Maßnahmen sollten in enger Abstimmung mit dem Beauftragten für den Datenschutz ergehen und jeweils schriftlich dokumentiert werden. Die vorgeschriebene Dokumentation sollte die Verantwortlichen dazu zwingen, das Vorliegen der jeweiligen Voraussetzungen sorgfältig zu prüfen.

Das vorgelegte Konzept entsprach diesen Gesichtspunkten bereits weitgehend.

Die Aufsichtsbehörde setzt sich in Abstimmung mit den übrigen an der Überprüfung des Discounters beteiligten Aufsichtsbehörden dafür ein, dass vergleichbare Unternehmen ebenfalls ein solches Gesamtkonzept für die (Video-)Überwachung in ihren Filialen erstellen.

1.1.3 Verantwortlichkeit der Sicherheitsunternehmen

Die Aufsichtsbehörde hat die Ergebnisse der datenschutzrechtlichen Prüfung in Absprache mit den anderen beteiligten Aufsichtsbehörden zum Anlass genommen, die Verbände, in denen Detekteien und Sicherheitsunternehmen (im Folgenden: „Sicherheitsunternehmen“) organisiert sind, darauf hinzuweisen, dass neben den Auftraggebern auch die Sicherheitsunternehmen für die Rechtmäßigkeit der Datenerhebung, -verarbeitung und -nutzung verantwortlich sind. Die Sicherheitsunternehmen dürfen sich nicht auf den ihnen erteilten Auftrag zurückziehen, sondern müssen in dem nach Sachlage gebotenen und ihnen zumutbaren Umfang die rechtliche Zulässigkeit einer Datenverwendung eigenständig prüfen und bei Zweifeln an der Rechtmäßigkeit an ihren Auftraggeber herantreten. Den maßgeblich in den Fall verwickelten Sicherheitsunternehmen wurden von den für sie zuständigen Aufsichtsbehörden die Grenzen ihres Handelns verdeutlicht.

1.2 (Video-)Überwachung von Mitarbeitern auch bei anderen Discountern?

In der Medienberichterstattung über den unter B 1.1 erwähnten Discounter wurden weitere Discounter genannt, die ihre Mitarbeiter ebenfalls unter Einsatz von Videotechnik und Detektiven überwacht haben sollen. Die an der obigen Untersuchung beteiligten Aufsichtsbehörden waren sich einig, auch bei diesen Unternehmen datenschutzrechtliche Prüfungen durchzuführen. Zuständig dafür war jeweils die für den Hauptsitz des Unternehmens zuständige Aufsichtsbehörde. Keines dieser Unternehmen hat seinen Sitz in Baden-Württemberg.

Dessen ungeachtet untersucht die Aufsichtsbehörde derzeit bei anderen Unternehmen mit Hauptsitz in Baden-Württemberg, in welcher Weise und in welchem Umfang diese Videotechnik und Detektive zur Überwachung von Kunden und Mitarbeitern einsetzen. Es hat diesen Unternehmen einen umfangreichen Fragenkatalog zugesandt, den diese inzwischen beantwortet haben. Die Überprüfung dauert noch an.

1.3 Offene Videoüberwachung von Mitarbeitern in nichtöffentlich zugänglichen Räumen

§ 6 b BDSG regelt die Videoüberwachung von Kunden und Mitarbeitern in öffentlich zugänglichen Räumen. Für die Videoüberwachung von Mitarbeitern in nichtöffentlich zugänglichen Räumen gibt es keinen Erlaubnistatbestand; § 28 BDSG greift in solchen Fällen nicht ein (vergleiche dazu den dritten Tätigkeitsbericht C 10.3, S. 159 f. und den Beschluss des Bundesverfassungsgerichts vom 23. Februar 2007, Az.: 1 BvR 2368/06, zu der Frage, ob die allgemeinen Erlaubnistatbestände eines Landesdatenschutzgesetzes auch für die Videoüberwachung gelten). Dies hätte nach § 4 Abs. 1 BDSG eigentlich zur Folge, dass die Videoüberwachung in diesen Fällen unzulässig ist. Die arbeitsgerichtliche Rechtsprechung zieht diesen Schluss jedoch nicht, ohne allerdings auf die Problematik einzugehen. Sie lässt Videoaufnahmen und -aufzeichnungen nur zu, wenn der Arbeitgeber ein berechtigtes Interesse daran hat, etwa um Diebstählen seitens der Belegschaft vorzubeugen. Seine Interessen sind dabei mit dem berechtigten Interesse der Beschäftigten, nicht in ihrem Persönlichkeitsrecht verletzt zu werden, abzuwägen. Das Persönlichkeitsrecht schützt die Arbeitnehmer vor einer lückenlosen Kontrolle am Arbeitsplatz, die sie einem ständigen Überwachungsdruck aussetzt, dem sie sich nicht entziehen können. Dieses Interesse der Mitarbeiter überwiegt in der Regel, wenn der Arbeitgeber mit den Bildaufnahmen lediglich der abstrakten Gefahr von Diebstählen oder vergleichbaren Verfehlungen seiner Beschäftigten begegnen will. Nur wenn es einen konkreten Diebstahlsverdacht gibt oder wenn Anhaltspunkte dafür vorliegen, dass es zu Unregelmäßigkeiten kommen wird, dürfen Videokameras eingesetzt werden. Ihr Aktionsradius ist auf den Bereich des Geschäfts zu beschränken, in dem sich die Verfehlung zugetragen hat oder zu erwarten ist. Auch muss die Videoüberwachung auf das Umfeld des verdächtigen Mitarbeiters konzentriert sein und darf nur während einer angemessenen Zeit stattfinden, längstenfalls bis zur Ermittlung des Täters. Außerdem muss der durch die Straftat oder durch vergleichbare Rechtsverstöße angerichtete oder zu erwartende Schaden für den Unternehmer nicht unerheblich sein, damit eine derartige Dauerüberwachung nicht unverhältnismäßig erscheint.

Bei einer von der Aufsichtsbehörde auf die Beschwerde zweier früherer Mitarbeiter eines Lebensmittelgeschäfts hin durchgeführten Kontrolle hat sich gezeigt, dass die Inhaber zwar in der Vergangenheit möglicherweise einen Grund hatten, wegen handgreiflicher Auseinandersetzungen des Personals untereinander und wegen Kassenunregelmäßigkeiten Kameras aufzustellen. Da sie aber die Videoüberwachung fortgesetzt hatten, obwohl sich keine Diebstähle damit hatten aufklären lassen und obwohl besagte Mitarbeiter den Betrieb inzwischen verlassen hatten, bestand die Aufsichtsbehörde darauf, dass die Kameras alsbald abgebaut wurden.

1.4 Überwachung eines Arbeitnehmers außerhalb des Betriebs durch einen Detektiv

Eine Mitarbeiterin eines Discounters bat die Aufsichtsbehörde, einen Detektiveinsatz datenschutzrechtlich zu bewerten. Sie war im Auftrag ihres Arbeitgebers außerhalb des Betriebs und ihrer Arbeitszeit von einer Detektei beobachtet worden. Die Mitarbeiterin ist Betriebsrätin in einer Filiale des Discounters. Sie vermutete einen Zusammenhang mit ihrer Betriebsratstätigkeit.

Die Prüfung der Aufsichtsbehörde hat ergeben, dass die Beschwerdeführerin tatsächlich im Auftrag ihres Arbeitgebers beobachtet wurde. Bei der Auftragserteilung wurden der Detektei der Name und die Anschrift der Mitarbeiterin übermittelt. Zu den Gründen, weshalb die Mitarbeiterin beobachtet wurde, hat das Unternehmen keine Angaben gemacht und mitgeteilt, der verantwortliche Geschäftsführer sei mittlerweile von seinen Aufgaben entbunden worden. Dem Unternehmen lägen keine Unterlagen oder Detekteiberichte zu diesem Auftrag mehr vor. Ob und welche Gründe letztlich zur Beauftragung der Detektei geführt haben, konnte daher nicht mehr aufgeklärt werden.

Da das Unternehmen den Detektiveinsatz sowie die zu diesem Zweck erfolgte Datenübermittlung eingeräumt hat, jedoch nicht darlegen konnte, worin sein berechtigtes Interesse hieran bestanden hat, war diese Datenübermittlung als datenschutzrechtlich unzulässig anzusehen. Wir haben diesen Datenschutzverstoß gegenüber dem Unternehmen beanstandet.

Schon eher könnte man ein berechtigtes Interesse im Sinne des § 28 Abs. 1 Satz 1 Nr. 2 BDSG im Falle eines Versicherungsunternehmens annehmen, das personenbezogene Daten einschließlich der Rentenversicherungsnummer eines ausscheidenden Mitarbeiters an einen Privatdetektiv übermittelte. Der gekündigte Mitarbeiter war nämlich vor der Beendigung seines Arbeitsverhältnisses für ein Jahr freigestellt worden und musste seinem Arbeitgeber während dieser Zeit mitteilen, ob er Einkünfte aus „anderweitiger Tätigkeit“ erzielt und gegebenenfalls in welcher Höhe. Der Arbeitgeber vermutete, dass sein Mitarbeiter inzwischen eine andere Tätigkeit aufgenommen hatte, ohne seiner Anzeigepflicht nachzukommen. Seinen Verdacht wollte er durch den Detektiv abklären lassen. Dieser fragte unter anderem unter Angabe der Sozialversicherungsnummer bei der gesetzlichen Rentenversicherung nach, ob die von ihm überwachte Person einer neuen Beschäftigung nachgeht. Die Datenübermittlung und die Beobachtung dieses Arbeitnehmers waren jedoch unzulässig, weil – wie die Ermittlungen der Aufsichtsbehörde ergeben haben – der Arbeitgeber alle Informationen auch von dem freigestellten Mitarbeiter hätte erhalten können. Damit verstieß der Arbeitgeber gegen den Grundsatz der Direkterhebung beim Betroffenen (§ 4 Abs. 2 BDSG). Erschwerend kommt hinzu, dass in der missbräuchlichen Verwendung der Sozialversicherungsnummer auch ein Verstoß gegen das Sozialgeheimnis zu sehen ist.

1.5 Gesundheits- und Fehlzeitenmanagement

Die Aufsichtsbehörde musste sich erstmals mit der datenschutzrechtlichen Bewertung eines betrieblichen Gesundheits- und Fehlzeitenmanagements befassen. Im konkreten Fall sollte es dazu dienen, Fehlzeiten zu reduzieren, Mitarbeiter nach einer Krankheit wieder zu integrieren und gegebenenfalls gemäß ihren Einschränkungen – möglicherweise an einer anderen Stelle als der bisherigen – einzusetzen.

Im Einzelnen sah es Folgendes vor:

Nach jeder Abwesenheit eines Mitarbeiters, unabhängig davon, ob deren Anlass eine Krankheit, Urlaub, eine Fortbildung oder etwas anderes ist, führt der Vorgesetzte ein informelles Gespräch mit diesem, für das es keine inhaltlichen Vorgaben gibt. Es wird nicht dokumentiert.

Soweit ein Mitarbeiter auffällige Fehlzeiten hat, kommt es zu einem „Eskalationsgespräch“, das einen formellen Charakter hat und vom Vorgesetzten teilweise im Beisein weiterer Personen geführt wird. Auf Wunsch des Betroffenen nimmt daran ein Mitglied des Betriebsrats teil. Bei einem solchen Gespräch wird der Mitarbeiter mit seinen auffälligen Fehlzeiten konfrontiert. Er wird gefragt, ob es Probleme gibt. Dabei kann es auch zur Erörterung des Gesundheitszustands kommen, wobei nach Aussage des Unternehmens nicht vorgesehen ist, dass der Mitarbeiter nach einer bestimmten Krankheit gefragt wird. Der Mitarbeiter wird nicht nach § 4 Abs. 3 BDSG belehrt. Zumindest bei Beginn der Überprüfung durch die Aufsichtsbehörde wurde er auch nicht darauf hingewiesen, dass er über seine Krankheit nicht sprechen muss. Dem Mitarbeiter wird auch nicht gesagt, dass seine Angaben möglicherweise an einen „Runden Tisch“ weitergegeben werden. Ist ein Vertreter der Personalabteilung zugegen, fertigt dieser einen Gesprächsvermerk, der zur Personalakte genommen wird. Andernfalls dokumentiert der Vorgesetzte das Gespräch unter Verwendung eines Vordrucks. Die Dokumentation verbleibt bei der Führungskraft; sie wird nicht zur Personalakte genommen. Was mit dem Dokument geschieht, wird dem Mitarbeiter ebenso wenig gesagt wie dass er darin Einsicht nehmen kann.

Auf Abteilungsebene findet in regelmäßigen Zeitabständen ein Runder Tisch statt, an dem außer dem Abteilungsleiter sämtliche Teamleiter und Meister einer Abteilung (bis zu 15 Führungskräfte), Vertreter der Personalabteilung, des werksärztlichen Dienstes und des zuständigen Bereichsbetriebsrats teilnehmen. Die Besprechungen dienen zum einen dem Fehlstandscontrolling, zum anderen werden hier neben allgemeinen Gesundheitsthemen auch Einzelfälle besprochen, die zuvor Gegenstand eines „Eskalationsgespräches“ waren und vom zuständigen Meister unter Verwendung eines Formulars für den Runden Tisch angemeldet wurden. Mindestvoraussetzung für die Behandlung am Runden Tisch sind hohe Fehlzeiten oder sonstige Auffälligkeiten (beispielsweise Suchterkrankungen). Die Personalabteilung stellt die Einzelfälle zusammen und verteilt die Liste, in der unter anderem die „Krankentage“, die „Problemlage“, das „Ziel“ der Erörterung und die Maßnahmen erfasst werden. Unter „Problemlage“ fanden sich unter anderem Einträge wie „Knie-OP missglückt“, „Magen-OP“, „hat starke psychische Probleme, durch seine Scheidung kam er in eine finanzielle Engpasssituation. Seine Mutter ist ebenfalls pflegebedürftig beziehungsweise liegt derzeit im Sterben“. Unter „Ziel“ war unter anderem eingetragen „Versetzung des Mitarbeiters“, „Stabilisierung des Gesundheitszustands“, „Wiedereingliederung in den Arbeitsprozess“. In der Spalte „Maßnahmen“ hieß es beispielsweise „beobachten“, „Termin bei WD“, „Motivationsgespräch“ oder „Kündigung“.

Bei der Besprechung der Einzelfälle waren alle Führungskräfte der Abteilung durchgängig anwesend. Die Mitarbeiter wurden nicht darüber informiert, dass „ihr Fall“ am Runden Tisch erörtert wird. Die Besprechungsergebnisse wurden in der Liste dokumentiert. Zu den Personalakten wurde das Dokument nicht genommen.

Diese Verfahrensweise verstieß in mehrfacher Hinsicht gegen Datenschutzvorschriften:

– Unzulässige Datenerhebung bei den Rückkehrgesprächen wegen auffälliger Fehlzeiten:

  Zwar ist es grundsätzlich zulässig, dass der Arbeitgeber mit dem Mitarbeiter nach einer Erkrankung ein Rückkehrgespräch führt. Dabei muss er jedoch Folgendes beachten:

  • Er darf den Mitarbeiter weder nach ärztlichen Krankheitsdiagnosen und konkreten Befunden noch nach Krankheitsursachen fragen, die im persönlichen Bereich des Mitarbeiters wurzeln und keinen betrieblichen Bezug aufweisen.

- Einige Informationen darf der Arbeitgeber auf der Grundlage des § 28 Abs. 6 Nr. 3 BDSG erheben, beispielsweise, ob die Erkrankung betriebliche Ursachen hat, ob noch Arbeitseinschränkungen bestehen, ob der Arbeitnehmer den Anforderungen seines Arbeitsplatzes noch gewachsen ist und ob in absehbarer Zeit mit weiteren Fehlzeiten zu rechnen ist. Der Arbeitgeber muss den Betroffenen zuvor nach § 4 Abs. 3 BDSG darüber belehren, für welche(n) Zweck(e) er die Daten erhebt, speichert und nutzt.
- Andere Gesundheitsdaten darf der Arbeitgeber nur auf der Grundlage einer Einwilligung des Betroffenen nach § 4 in Verbindung mit § 4 a BDSG erheben, das heißt
  - er muss den Betroffenen auf die Freiwilligkeit seiner Angaben hinweisen (§ 4 Abs. 3 Satz 2 BDSG);
  - die Einwilligung muss auf der freien Entscheidung des Mitarbeiters beruhen (§ 4 a Abs. 1 Satz 1 BDSG). Die Freiwilligkeit ist nur dann gegeben, wenn die Willensbildung des Betroffenen nicht in unangemessener Weise beeinflusst wurde. Über eine Einwilligung dürfen nur solche Daten erhoben werden, die aus objektiver Sicht zur Ausübung der Arbeitgeberfunktion beziehungsweise zur Vornahme sachgerechter (Personal-) Entscheidungen benötigt werden und auch außerhalb des Anwendungsbereichs des Bundesdatenschutzgesetzes erhoben, verarbeitet und genutzt werden dürfen. Eine Einwilligung ist als rechtsmissbräuchlich anzusehen, wenn ihre Einholung gegen zwingende Schutzprinzipien verstößt;
  - der Mitarbeiter muss die Einwilligung auf der Grundlage einer umfassenden Information des Arbeitgebers über die beabsichtigte weitere Verwendung seiner Daten erteilen (sogenannte informierte Einwilligung, § 4 a Abs. 1 Satz 2 BDSG),
  - der Mitarbeiter muss grundsätzlich schriftlich einwilligen (§ 4 a Abs. 1 Satz 3 BDSG).

Im konkreten Fall hat das Unternehmen teilweise Daten erhoben, die überhaupt nicht oder nicht ohne Hinweis auf die Freiwilligkeit und die beabsichtigte weitere Verwendung der Daten, insbesondere eine mögliche Weiterleitung an den Runden Tisch, hätten erhoben werden dürfen. Auch hätte die Einwilligung von den Betroffenen schriftlich eingeholt werden müssen.

– Unzulässige Weitergabe an den Runden Tisch

Soweit die Daten unzulässig erhoben wurden, hätten sie auch nicht an den Runden Tisch weitergegeben werden dürfen.

– Unzulässige Teilnahme am Runden Tisch

Bei den Rückkehrgesprächen und bei den Verhandlungen des Runden Tischs werden Gesundheitsdaten erhoben und genutzt, die zugleich Personaldaten sind und in die Personalakte gehören. Bei solchen Daten ist der Kreis der Personen, die Zugang dazu erhalten dürfen, zur Wahrung des Persönlichkeitsschutzes der Betroffenen so eng wie irgend möglich zu ziehen. Das hat zur Folge, dass an der Besprechung eines Einzelfalls am Runden Tisch nur teilnehmen darf, wer diese personenbezogenen Daten nach den für Personalaktendaten geltenden Grundsätzen auch erhalten darf. Dies muss für jeden Teilnehmer am Runden Tisch hinsichtlich jedes Betroffenen und der gesamten über einen Betroffenen auszutauschenden Informationen geprüft werden. Konkret bedeutet das, dass

- ein Vorgesetzter einer Organisationseinheit, der der Betroffene nicht angehört, an der Erörterung des betreffenden Einzelfalls nicht teilnehmen darf, sofern es dafür keinen zwingenden Grund gibt;
- einem Werksarzt personenbezogene Daten nur insoweit bekannt gegeben werden dürfen, als er diese zur Erfüllung seiner Aufgaben als Werksarzt benötigt, beispielsweise um als Mediziner beurteilen zu können, welche Arbeitsplatzbedingungen für einen Betroffenen erforderlich sind. Bei der Erörterung bestimmter Personalmaßnahmen wie zum Beispiel Kündigung wird er hingegen in der Regel nicht anwesend sein müssen und dürfen. Selbstverständlich ist, dass der Werksarzt bei solcher Gelegenheit nicht offenbaren

darf, was ihm über den Betroffenen bei Untersuchungen oder Behandlungen bekannt geworden ist, sofern ihn dieser nicht von der ärztlichen Schweigepflicht entbunden hat;

- Vertreter des Betriebsrats an der Erörterung von Einzelfällen nur auf Wunsch der jeweils Betroffenen teilnehmen dürfen. Dies gilt selbst dann, wenn der Betriebsrat anschließend nach dem Betriebsverfassungsgesetz zu beteiligen ist, weil das Ergebnis der Erörterung am Runden Tisch eine Personalmaßnahme ist.

Diese Grundsätze hat das Unternehmen nicht beachtet.

Die Aufsichtsbehörde hat ferner darauf hingewiesen, dass im Zusammenhang mit dem Gesundheitsmanagement erstellte Dokumente über einzelne Mitarbeiter materiell zu den Personalakten gehören. Die Betroffenen haben daher ein Einsichtsrecht in diese Unterlagen. Die Aufsichtsbehörde hat deshalb im konkreten Fall angeregt, die Betroffenen frühzeitig darüber zu informieren, wo im Rahmen des Gesundheitsmanagements über sie angelegte Unterlagen wie lange aufbewahrt werden, dass sie ein Einsichtsrecht in diese Unterlagen haben und wie sie dieses ausüben können.

Die Aufsichtsbehörde hat die festgestellten Verstöße gegenüber dem Unternehmen beanstandet und es aufgefordert, seine Verfahrensweise so umzustellen, dass sie den Datenschutzvorschriften entspricht. Das Unternehmen hat die Prüfungsergebnisse sofort akzeptiert und die bisherige Verfahrensweise, insbesondere die Runden Tische, ausgesetzt. Es arbeitet derzeit unter Beteiligung des Betriebsrats an einem neuen datenschutzkonformen Gesundheits- und Fehlzeitenmanagement. Angestrebt wird der Abschluss einer Betriebsvereinbarung mit dem Betriebsrat. Das Unternehmen hat zugesagt, der Aufsichtsbehörde ihr neues Konzept vor dessen Umsetzung zur Prüfung zuzuleiten.

1.6 Erhebung von Krankheitsdaten im Rahmen von Rückkehrgesprächen

Anfang April 2009 wurden in einem Mülleimer einer Autowaschanlage in Nordrhein-Westfalen Listen mit Gesundheitsdaten von Mitarbeitern eines Discounters entdeckt. Die Medien berichteten, in Filialen dieses Discounters würden Mitarbeiter nach einer Erkrankung systematisch von ihren Vorgesetzen nach der Art der Erkrankung befragt. Diese Angaben, die im Beispielsfall von „Grippe“ über „Rückenleiden“ bis zu „will schwanger (werden), Befruchtung nicht funktioniert“ reichten, würden in Listen erfasst, in die auch beabsichtigte weitergehende Maßnahmen (zum Beispiel „Kündigung zum 31. Juli 2008“) eingetragen würden. Für die Erfassung werde bundesweit ein einheitlicher Vordruck verwendet.

Die für die Dienstleistungsgesellschaft des Discounters zuständige baden-württembergische Aufsichtsbehörde leitete daraufhin Ermittlungen ein. Diese ergaben, dass „nur“ sieben der bundesweit 35 Regionalgesellschaften Krankheitsdaten ihrer Mitarbeiter erhoben hatten. Keine dieser Regionalgesellschaften hat ihren Sitz in Baden-Württemberg. Für die Erhebung hatten die Regionalgesellschaften von ihnen selbst entworfene Vordrucke eingesetzt. Sie hatten die Datenerfassung zu unterschiedlichen Zeitpunkten im Laufe des Jahres 2008 beendet, die letzten Regionalgesellschaften im Dezember 2008, nachdem die Dienstleistungsgesellschaft hiervon Kenntnis erhalten und die Erfassung wegen datenschutzrechtlicher Bedenken gestoppt hatte. Die Vordrucke wurden spätestens im Januar 2009 vernichtet. Die weitere Aufarbeitung der Vorgänge erfolgt durch die für die sieben Regionalgesellschaften zuständigen Datenschutzaufsichtsbehörden; die Koordinierung obliegt der baden-württembergischen Aufsichtsbehörde. Die zuständigen Aufsichtsbehörden werden demnächst über die abschließende datenschutzrechtliche Bewertung der Vorgänge entscheiden.

Mitte April 2009 wurde der baden-württembergischen Aufsichtsbehörde bekannt, dass ein in einem anderen Bundesland ansässiges Werk des unter C 1.5 erwähnten Unternehmens bis April 2008 Gesundheitsdaten von Mitarbeitern des Werkssicherheitsdienstes erhoben und gespeichert hatte. Betroffen waren rund hundert Personen. Die Datenerhebung erfolgte bei Gesprächen, die die Vorgesetzten mit ihren Mitarbeitern nach Rückkehr aus einer Erkrankung führten. Dabei wurde insbesondere nach dem Grund der Erkrankung, der weiteren Einsatzfähigkeit des

Mitarbeiters, dem Betreuungsbedarf bei der Wiedereingliederung und etwaigen betriebsbedingten Gründen für die Erkrankung gefragt. Auch sollten Krankheitsschwerpunkte innerhalb des Arbeitsfelds „Betriebssicherheit“ identifiziert werden. Die Angaben der Mitarbeiter zu ihrer Erkrankung wurden in Listen erfasst, auf die zwölf Vorgesetzte zugreifen konnten. Infolge eines Speicherfehlers war es jedoch weiteren Mitarbeitern des Werks möglich, in die Liste mit den Krankheitsdaten Einsicht zu nehmen. Diese Daten sind gelöscht worden, nachdem der Beauftragte für den Datenschutz die Unzulässigkeit der Datenspeicherung erkannt hatte.

Die Aufsichtsbehörde hat dem Unternehmen nach Bekanntwerden der Vorgänge einen umfangreichen Fragenkatalog zugesandt und es aufgefordert, eingehend zu untersuchen, ob auch in anderen Bereichen dieses Werks und an anderen Werksstandorten vergleichbare Listen geführt werden oder ein Gesundheitsmanagement im oben beschriebenen Sinn betrieben wird. Bei der Überprüfung in anderen Bereichen des Werks wurden neun weitere derartige Listen in sieben Abteilungen gefunden. Auch diese Daten sind inzwischen gelöscht worden. Das Unternehmen hat die Aufsichtsbehörde hierüber inzwischen eingehend unterrichtet. Eine abschließende Bewertung der Vorgänge in dem Unternehmen soll erst nach Abschluss sämtlicher Überprüfungen an allen Werksstandorten erfolgen.

Ebenfalls Mitte April 2009 hat die Aufsichtsbehörde aus Medienberichten erfahren, dass auch eine Drogeriemarktkette mit ihren Beschäftigen Krankenrückkehrgespräche führt und darüber Aufzeichnungen mit Gesundheitsdaten fertigt. Die Unternehmensleitung hat inzwischen gegenüber der Aufsichtsbehörde dazu Stellung genommen. Die Aufsichtsbehörde hat sich „vor Ort“ eingehend über die Praxis informiert. Eine abschließende datenschutzrechtliche Beurteilung ist noch nicht erfolgt.

1.7 Mitarbeiterbefragungen

Zur Verbesserung der Arbeitsbedingungen, aber auch um Arbeitsabläufe optimieren zu können, führen Unternehmen Mitarbeiterbefragungen durch. Dabei versichert die Betriebsleitung ihrer Belegschaft, die Befragung erfolge in anonymisierter Form, weil sie sich davon eine größere Bereitschaft der Beschäftigten, sich an der Aktion zu beteiligen, und ehrlichere Auskünfte verspricht. Die Anonymität einer Befragung ist allerdings nur gewährleistet, wenn sich die Einzelangaben auf den Erhebungsbögen nicht oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren Person zuordnen lassen. Die Gefahr, dass Rückschlüsse auf einen Mitarbeiter, der an der Befragung teilgenommen hat, möglich sind, besteht insbesondere in den Fällen, in denen dieser einer sehr kleinen Organisationseinheit des Betriebs angehört und über Vorgänge oder Verhältnisse Auskunft gibt, die seine Stellung und Funktion mehr oder weniger deutlich erkennen lassen. Um die erwünschte und zugesicherte Anonymität einer Befragung nicht zu gefährden, sollten solche Fragen nur an Mitarbeiter von Organisationseinheiten gerichtet werden, die mindestens fünf Beschäftigte umfassen.

In einem Fall eines Unternehmens, mit dem sich die Aufsichtsbehörde befassen musste, sollten die Mitarbeiter auf den Fragebögen die ihnen jeweils zugeteilte sogenannte Transaktionsnummer (TAN) eintragen, um sicherzustellen, dass jeder Beschäftigte nur einen Fragebogen erhält. Bei TAN handelt es sich um Kennzahlen, die für einen bestimmten Bearbeitungsvorgang nur einmal vergeben werden, also nicht um ein Identifizierungsmerkmal, das einer Person für sämtliche Nutzungen eines Systems zugeteilt ist. Um auch hier keine Verbindung zwischen dem Befragten und dessen Angaben herstellen zu können, sollte darauf geachtet werden, dass bei der Vergabe der Nummern keine Systematik entsteht, die es später ermöglicht, die Zuordnung einer TAN an einen bestimmten Mitarbeiter nachzuvollziehen. Letzteres kann etwa der Fall sein, wenn das Unternehmen auf einer alphabetisch aufgebauten Mitarbeiterliste die TAN der Reihe nach vergibt. Vielmehr sollte man die TAN nach dem Zufallsprinzip (zum Beispiel durch Auslosung) den einzelnen Mitarbeitern zuteilen. Auch sollten die Organisatoren der Befragung keine „sprechenden“ TAN verwenden, die beispielsweise einen Rückschluss auf eine Organisationseinheit oder eine Mitarbeitergruppe zulassen. Ferner dürfen die Aufzeichnungen, aus denen sich ergibt, wer welche TAN erhalten

hat, nur kurzfristig gespeichert bleiben. Am besten wäre eine Löschung dieser Zuordnungsinformation unmittelbar nachdem dem jeweiligen Beschäftigten mitgeteilt worden ist, welche TAN er benutzen soll. Spätestens wenn der Fragebogen zurückgesendet wird, müssen diese Aufzeichnungen gelöscht werden, um die Anonymität der Befragung zu gewährleisten.

1.8 Bewerberfragebögen

Wer sich um eine Stelle bewirbt, muss für gewöhnlich einen Personalfragebogen ausfüllen. Doch nicht alle dort gestellten Fragen sind datenschutzrechtlich zulässig. Maßgeblich ist, inwieweit die erbetenen Angaben zunächst für eine Vorauswahl und später für die endgültige Entscheidung des künftigen Arbeitgebers geeignet und erforderlich sind. Selbstverständlich muss der Bewerber seinen Namen, seinen Vornamen und seine Adresse offenbaren. Aber bereits hier sind den Informationswünschen des Arbeitgebers Grenzen gesetzt. Es ist nämlich nicht zwingend erforderlich, auch die Telefonnummer, die E-Mail-Adresse oder die Faxnummer des Interessenten zu kennen. Vielmehr genügt es zunächst einmal, wenn sich der Arbeitgeber mit dem Bewerber postalisch in Verbindung setzen kann. Wohl vereinfacht es das Verfahren, wenn dieser für das Beschäftigungsunternehmen „auf kurzem Wege“ erreichbar ist. Deswegen darf man diese Angaben auf dem Bewerbungsbogen zwar erfragen, allerdings mit dem Hinweis, dass die Auskunft freiwillig ist, jedoch die Kontaktaufnahme erleichtert.

In einem Fall, mit dem sich die Aufsichtsbehörde befassen musste, warb ein Unternehmer junge Leute für kurzfristige Tätigkeiten an und erkundigte sich in seinen Bewerbungsbögen auch nach deren Geburtsdatum und Staatsangehörigkeit. Er begründete das damit, dass er nach dem Jugendarbeitsschutzgesetz Jugendliche nur beschäftigen darf, wenn deren Sorgeberechtigte zugestimmt haben. Die Angaben zur Staatsangehörigkeit hielt er für erforderlich, um klären zu können, ob die Interessenten, die nicht deutsche Staatsbürger sind, aufenthalts- und arbeitserlaubnisrechtlich der angebotenen Tätigkeit nachgehen dürfen.

Die generelle Erhebung des Geburtsdatums ist für diesen Zweck ungeeignet, weil die Altersangabe für sich genommen nichts darüber aussagt, ob der Sorgeberechtigte mit dem Vertragsabschluss einverstanden ist. Die Aufsichtsbehörde hat dem Unternehmer deswegen empfohlen, sich künftig nicht mehr nach dem Geburtsdatum zu erkundigen, sondern stattdessen danach zu fragen, ob der Bewerber volljährig ist. Wenn er dies verneint, sollte der Unternehmer den Bewerber darauf aufmerksam machen, dass er nur beschäftigt werden kann, wenn er zum Zeitpunkt der Arbeitsaufnahme das 13. Lebensjahr vollendet und sein Sorgeberechtigter zugestimmt hat.

Was die Frage nach der Staatsangehörigkeit anbetrifft, ist es nicht nur legitim, sondern einem Arbeitgeber im Aufenthaltsrecht sogar vorgeschrieben, sich davon zu überzeugen, ob ein Arbeitnehmer mit fremdländischer Staatsangehörigkeit die Tätigkeit, für die er eingestellt werden soll, überhaupt ausüben darf. Im Falle illegaler Beschäftigung drohen dem Beschäftigungsunternehmen nicht unerhebliche Sanktionen. Die bloße Erkundigung nach der Staatsangehörigkeit ist für diesen Zweck jedoch ungeeignet, weil der Arbeitgeber für seine Entscheidung darüber hinaus noch eine ganze Reihe zusätzlicher Informationen benötigt, etwa die bisherige Aufenthaltsdauer oder die Staatsangehörigkeit des Ehegatten, um angesichts der sehr komplizierten ausländer- und arbeitserlaubnisrechtlichen Regelungen die Zulässigkeit einer Beschäftigung selbst beurteilen zu können. Die Aufsichtsbehörde hat deswegen vorgeschlagen, auf dem Bewerbungsformular folgende Passage zum Ankreuzen vorzusehen: „Ich bin nicht im Besitz der deutschen Staatsangehörigkeit, bin aber aufenthaltsrechtlich befugt, der angestrebten Erwerbstätigkeit nachzugehen“. Diese Versicherung kann der Bewerber, wenn es zu einem Vertragsabschluss kommt, mit seinem Pass belegen.

Besonders sensible Daten darf der Arbeitgeber nur erheben, falls der Bewerber in die engere Wahl kommt. Das betrifft insbesondere die Prüfung der persönlichen Zuverlässigkeit, wenn dem Betroffenen eine entsprechende Funktion übertragen werden soll. Die Frage nach der Schwerbehinderung ist sowohl nach dem Allgemeinen Gleichbehandlungsgesetz als auch nach dem Bundesdatenschutzgesetz grundsätzlich nicht erlaubt. Sie kommt allenfalls im Einzelfall in Betracht, etwa wenn der Bewerber sich für eine Tätigkeit im Außendienst interessiert, die kör-

perliche Belastungen mit sich bringt. Aber auch dann darf sich der Unternehmer nur danach erkundigen, ob der Bewerber an einem bestimmten körperlichen Gebrechen leidet, das der angestrebten Beschäftigung entgegensteht. Im Finanzdienstleistungsgewerbe legt man großen Wert darauf, keine Personen einzustellen, deren Ehegatte oder Lebenspartner für ein Konkurrenzunternehmen tätig ist, um zu verhindern, dass die Betroffenen in Gewissenskonflikte kommen. Die Zulässigkeit dieser Frage hängt nicht zuletzt davon ab, welche Funktion dem Bewerber künftig übertragen werden soll.

1.9 Standortbestimmung von Kundendienstfahrzeugen mittels eines Global Positioning Systems (GPS)

Ein Arbeitnehmer fragte die Aufsichtsbehörde, ob es zulässig ist, dass seine Firma, die bei ihren Kunden Reparaturarbeiten durchführt, die Kundendienstfahrzeuge der Monteure mit einem GPS ausgestattet hat. Durch das eingesetzte Verfahren können während der Geschäftszeiten stets der Standort der Fahrzeuge auf einem Monitor in den Betriebsräumen der Firma angezeigt, die zurückgelegten Fahrstrecken und die Fahrtunterbrechungen nach Ort und Zeit festgehalten und diese Daten gespeichert werden. Die Firma hat dieses Informationssystem nach eigenen Angaben installiert, um ihre Fahrzeuge und Mitarbeiter optimal einsetzen zu können. So ließen sich, während das Fahrzeug unterwegs ist, leichter Aufträge erteilen und ändern. Auch könne man die elektronischen Aufzeichnungen für die Abrechnung der Anfahrts- und Arbeitszeiten mit den Kunden nutzen. Eine Überwachung der Mitarbeiter sei nicht beabsichtigt.

Datenschutzrechtlich kann man es einem Firmeninhaber grundsätzlich nicht verwehren, stets darüber im Bilde zu sein, wo sich seine Kundendienstfahrzeuge gerade befinden, um deren Einsatz dirigieren zu können. Darüber müssten ihn seine Mitarbeiter auch ohne GPS auf dem Laufenden halten. Darüber hinaus hat ein Außendienstmitarbeiter seinen Arbeitgeber über die Anfahrts- und Arbeitszeiten zum und beim Kunden wahrheitsgemäß zu informieren, damit dieser die dafür anfallenden Kosten abrechnen kann, sodass grundsätzlich der Einsatz dieses Ortungssystems auch zu diesem Zweck berechtigt ist.

Schutzwürdige Interessen der Beschäftigten werden im Falle des GPS-Einsatzes jedoch dann verletzt, wenn der Mitarbeiter losgelöst von einem betrieblich gerechtfertigten Informationsbedarf des Arbeitgebers einer umfassenden Kontrolle seines Verhaltens an seinem externen Arbeitsplatz unterworfen ist. So war jedoch der von der Aufsichtsbehörde zu beurteilende Fall nicht gelagert. Insbesondere konnte hier mit Hilfe des GPS nicht festgestellt werden, wie der Mitarbeiter seine Arbeit verrichtet, wie er seine Pausen gestaltet und wie er sich während der Fahrt im Straßenverkehr verhält.

Da jedoch mit einer derartigen Nutzung eines GPS das Risiko eines nicht unerheblichen Eingriffs in das Persönlichkeitsrecht der Mitarbeiter verbunden ist, muss die Firma eine sogenannte Vorabkontrolle nach § 4 d Abs. 5 BDSG durchführen. Ferner muss sie schriftlich festlegen, welche mit Hilfe des GPS erlangten Informationen für welche(n) Zweck(e) und wie lange gespeichert und genutzt werden dürfen. Dabei müssen die Grundsätze der Erforderlichkeit und der Verhältnismäßigkeit beachtet werden. Ferner muss es eine Datenlöschkonzeption geben. Diese muss unter anderem vorsehen, dass die Angaben über den Standort der Kundendienstfahrzeuge alsbald nach Beendigung der Betriebsfahrten gelöscht werden. Dagegen können die Daten, die zu Abrechnungszwecken mit den Kunden erforderlich sind, so lange gespeichert bleiben, wie mit Reklamationen und dergleichen normalerweise zu rechnen ist. Ferner empfahl die Aufsichtsbehörde, die Nutzung der Daten zur persönlichen Kontrolle der Mitarbeiter, etwa zur Überwachung der Geschwindigkeit während der Betriebsfahrten oder der Dauer der Pausen sowie zur Berechnung von Leistungsentgelten ausdrücklich auszuschließen, auch wenn insoweit für die Mitarbeiter kein Grund zur Besorgnis bestand. Außerdem müssen die Mitarbeiter nach § 4 Abs. 3 BDSG über die Zweckbestimmungen der Erhebung, Verarbeitung und Nutzung der Daten unterrichtet werden.

1.10 Bekanntmachung von Tarifverträgen

Die Leitung eines Unternehmens erkundigte sich bei der Aufsichtsbehörde, ob und in welchem Umfang tarifvertragliche Regelungen einschließlich der für die Entlohnung maßgeblichen Aufgabenbeschreibungen im Intranet der Firma veröffentlicht werden dürfen. Der in diesem Unternehmen geltende Tarifvertrag sieht unter anderem vor, dass den Beschäftigten ein Grundentgelt zusteht, dessen Höhe sich an der Qualifizierung der jeweiligen Tätigkeit orientiert. Die Bewertung richtet sich im Einzelnen nach den Arbeitsaufgabenbeschreibungen als Bestandteil des Tarifvertrags (sogenannte Niveaubeispiele), die von den Tarifparteien festgelegt worden sind. Weil es jedoch auch unternehmensspezifische Aufgaben gibt, die die Tarifparteien nicht generell für den gesamten Geltungsbereich des Tarifvertrags bewerten konnten, ist eine „Paritätische Kommission“ vorgesehen, die für diese Art von Tätigkeiten die für die Entlohnung maßgeblichen Kriterien festlegt. Diese muss bei der Bestimmung der jeweiligen Einstufung auch berücksichtigen, in welchem Maße eine bestimmte Tätigkeit Anforderungen an die körperliche Belastbarkeit mit sich bringt und über welche persönlichen Erfahrungen der Arbeitsplatzinhaber verfügen muss. Die Zahl der auf diese Weise für das Unternehmen insgesamt geltenden beziehungsweise erstellten Beispiele soll letztlich ein Mehrfaches der durch Tarifvertrag festgelegten Niveaubeispiele betragen haben. Der Betriebsrat entschloss sich daher nach eigenen Angaben, über die vom Arbeitgeber bereits veröffentlichten Beispiele hinaus weitere Beispiele in das Intranet einzustellen, da der Arbeitgeber seinen Wünschen nach Erläuterung der Zusammenhänge und Differenzierungen nicht nachgekommen sei. Dies habe zu einer großen Zahl von Reklamationen durch Mitarbeiter geführt, die mit der Beschreibung und/oder Bewertung ihrer Arbeitsaufgaben und damit auch ihrem daraus resultierenden Grundentgelt nicht einverstanden gewesen seien. Auch habe sich gezeigt, dass weitere Beispiele erstellt und einzelne Beschreibungen modifiziert werden müssten. Die Veröffentlichung der Beispiele führte im Unternehmen aber auch zu der Befürchtung, Kollegen könnten das Gehalt ihrer Kollegen „errechnen“.

Bei der datenschutzrechtlichen Bewertung dieses Vorgehens ist grundsätzlich zwischen der Veröffentlichung der Niveaubeispiele und den unternehmensspezifischen Ergänzungen zu differenzieren.

Die Veröffentlichung der Niveaubeispiele ist nicht nur zulässig, sondern sogar vorgeschrieben. § 8 des Tarifvertragsgesetzes (TVG) verpflichtet den Arbeitgeber, die für seinen Betrieb maßgebenden Tarifverträge dort auszulegen. Besagte Niveaubeispiele sind Anhang zu dem erwähnten Tarifvertrag, also dessen Bestandteil. Folglich erstreckt sich die Auslegungspflicht auch auf diese und zwar unabhängig davon, ob es sich bei den Beispielen um personenbezogene Daten handelt oder nicht. Die Veröffentlichung des Tarifvertrags samt Niveaubeispielen im Intranet ist eine Form der „Auslegung“, die den heutigen Gegebenheiten in den Betrieben entspricht. Dabei ist es unerheblich, ob dies auf Veranlassung des Betriebsrats oder des Arbeitgebers erfolgt. Dagegen sind die ergänzenden unternehmensspezifischen Tätigkeitsbewertungen nicht Bestandteil des Tarifvertrags. Es besteht daher keine Veröffentlichungspflicht nach § 8 TVG. Somit stellt sich die Frage, ob die unternehmensspezifischen Beispiele veröffentlicht werden dürfen. Sie ist zu bejahen, wenn die unternehmensspezifischen Beispiele keine personenbezogenen Daten enthalten, da dann das Bundesdatenschutzgesetz nicht anwendbar ist. Geht man jedoch von einem Personenbezug aus, ist § 28 Abs. 1 Satz 1 Nr. 2 BDSG zu beachten. Darüber, ob in solchen Fällen ein Personenbezug im Sinne des § 3 Abs. 1 BDSG vorliegt, lässt sich streiten:

– Dass allgemein formulierte Tarifbeispiele für gewöhnlich auf mehrere Personen Anwendung finden, schließt einen Personenbezug nicht aus. Immer wenn die zu einer Personenmehrheit erfassten Daten zugleich etwas über die Verhältnisse der einzelnen Personen aussagen und diese bestimmbar sind, sind es deren Daten. Dieser Aspekt dürfte unproblematisch sein.

– Dass die hinter den veröffentlichten Aufgabenbeschreibungen stehenden Personen nirgends namentlich genannt werden, steht der Annahme eines Personenbezugs ebenfalls nicht entgegen. Bestimmbarkeit ist gegeben, wenn es die Veröffentlichung lesende Unternehmensangehörige mit ihnen normalerweise zur Verfügung stehenden Hilfsmitteln und ohne unverhältnismäßigen Aufwand er-

kennen können, auf welche(n) konkrete(n) Mitarbeiter eine bestimmte Tätigkeitsbeschreibung zutrifft. Dies wäre – bezogen auf den vorliegenden Fall – für die einzelnen Beschreibungen zu prüfen.

– Unstrittig ist ferner, dass auch Daten, die Aussagen über eine Sache enthalten, personenbezogen sein können. Allerdings muss ein unmittelbarer Bezug zur Person des Betroffenen herstellbar sein. Ein mittelbarer Zusammenhang genügt nicht, da der Personenbezug sonst kaum noch eine begrenzende Funktion hätte. Jede sachbezogene Angabe wäre zugleich ein Datum der Person, die mit der Sache in einer auch nur entfernten Verbindung steht. Was theoretisch einfach ist, bereitet in der Praxis Abgrenzungsschwierigkeiten. So sollen zu den Daten eines Arbeitnehmers auch die Angaben gehören, die seinen Arbeitsplatz oder seine Stelle bezeichnen und allgemein charakterisieren, nicht aber die Details der Arbeitsplatz- beziehungsweise Stellenbeschreibung wie Tätigkeitsmerkmale und Anforderungsprofil. Das heißt, dass man für jede Aufgabenbeschreibung das Vorliegen eines solchen unmittelbaren Bezugs zur Person des Betroffenen sehr genau prüfen müsste.

Letztlich braucht die Frage des Personenbezugs solcher Beispiele jedoch nicht entschieden zu werden. Denn auch wenn man sie bejaht, ist deren Veröffentlichung durch § 28 Abs. 1 Satz 1 Nr. 2 BDSG gedeckt.

Der Betriebsrat hatte ein erhebliches berechtigtes Interesse an der Veröffentlichung der Daten, um den von ihm Vertretenen – auch angesichts der vielen Zusatzbeispiele und möglicherweise fehlender Transparenz – die Möglichkeit zu geben, selbst zu prüfen, ob in den Beispielen alle wesentlichen Faktoren für die Einstufung und Entlohnung aufgeführt waren, und um notfalls dagegen vorzugehen. Zu diesem Zweck war die Veröffentlichung im Intranet auch erforderlich. Demgegenüber wurden die schutzwürdigen Interessen der Betroffenen nur wenig tangiert. Sie wurden nicht anders behandelt als die Personen, die die Veröffentlichung ihrer Entlohnungsregelungen hinnehmen müssen, weil für sie die tarifvertraglichen Niveaubeispiele gelten. Vor allem aber ist das individuelle Entgelt aus der Beschreibung nicht ersichtlich, weil die leistungsabhängige Variable nicht unerheblich ist und zudem die Zuschläge auch aus dem Arbeitszeitmodell oder Belastungen nicht bekannt oder erkennbar sind.

1.11 Einsichtnahme in die Arbeitsverträge durch den potenziellen Erwerber eines Unternehmens?

Die Veräußerung ganzer Unternehmen an eine andere Gesellschaft ist in Zeiten der Globalisierung nichts Ungewöhnliches. Verständlich ist, dass sich der Erwerber vor einer Betriebsübernahme ein Bild machen will, welche finanziellen Belastungen dadurch auf ihn zukommen und – insbesondere wenn er nur einen Teil einer anderen Firma aufzukaufen beabsichtigt – eine Auswahl treffen muss, welche Arbeitnehmer mit übernommen werden sollen. So kommt es, dass sich der Kaufinteressent vor seiner Entscheidung bei dem Verkäufer möglichst umfassend informieren will und dabei unter anderem auch Einblick in die Arbeitsverträge der für eine Übernahme infrage kommenden Mitarbeiter sowie Auskünfte zu sonstigen gehaltsrelevanten Daten verlangt.

Die Erhebung von personenbezogenen Daten der Mitarbeiter durch den Kaufinteressenten beziehungsweise Käufer eines Unternehmens und die Übermittlung durch den Verkäufer ohne Einwilligung der Betroffenen sind nach § 28 Abs. 1 Satz 1 Nr. 2 und Abs. 2 BDSG nur zulässig, soweit dafür ein berechtigtes Interesse besteht und der Auskunft keine überwiegenden schutzwürdigen Belange der Beschäftigten entgegenstehen. Um in Erfahrung zu bringen, in welcher Größenordnung Löhne, Gehälter, Betriebsrenten und dergleichen im Falle der Betriebsübernahme zu Buche schlagen, muss der potenzielle Erwerber keinen Einblick in die einzelnen Arbeitsverträge oder Abrechnungsunterlagen nehmen. Es genügt, wenn er sich von dem Management der Firma, die verkauft werden soll, über die zu erwartenden Gesamtverbindlichkeiten – also ohne Personenbezug – unterrichten lässt.

Was die Auswahl der Mitarbeiter anbetrifft, die weiterbeschäftigt werden sollen, kann sich der Kaufinteressent beziehungsweise Käufer zwar von der bisherigen Betriebsleitung beraten lassen. Einblick in Personalunterlagen oder Auskünfte

daraus können ihm jedoch ohne deren Einwilligung nicht gewährt werden. Dabei ist es unerheblich, ob der neue Arbeitgeber diese Mitarbeiter zu den bisherigen Bedingungen übernehmen oder ob er ihnen ein Angebot für einen neuen Arbeitsvertrag unterbreiten will. Einer Übernahme durch einen anderen Arbeitgeber kann der Arbeitnehmer nach § 613 a Abs. 6 BGB widersprechen. Soll ein neuer Arbeitsvertrag geschlossen werden, muss ohnehin mit dem Beschäftigten verhandelt werden. In beiden Fällen ist es also ohne Weiteres möglich, dass der Kaufinteressent seine Informationen unmittelbar bei den Betroffenen selbst einholt, da ihr Wechsel zu dem aufnehmenden Betrieb allemal von ihrer Zustimmung oder von ihrem Widerspruch abhängt. Bei den Verhandlungen können diese selbst entscheiden, ob sie „mit dem neuen Chef ins Geschäft kommen“ und was sie ihm dazu von sich offenbaren wollen, oder ob sie es ablehnen, in die Dienste des Erwerbers zu treten, sodass sie auch dessen Fragen nicht beantworten müssen.

In einem an die Aufsichtsbehörde herangetragenen Fall wollte der potenzielle Erwerber eines Unternehmens bereits bei der Personalvorauswahl die Geburtsdaten der Mitarbeiter der Firma in Erfahrung bringen. Vermutlich wollte er davon abhängig machen, wen er in die engere Wahl zieht. Abgesehen von den bereits erläuterten datenschutzrechtlichen Hindernissen, die einer solchen Datenerhebung entgegenstehen, kam hier noch hinzu, dass das Lebensalter nach dem Allgemeinen Gleichbehandlungsgesetz grundsätzlich kein Kriterium für derartige Personalentscheidungen sein darf.

1.12 Übermittlung von Daten an das Arbeitsgericht

Wer einen Arbeitsgerichtsprozess führt, muss bei Gericht die geltend gemachten Ansprüche begründen und gegebenenfalls beweisen beziehungsweise geeignete Tatsachen vortragen, wenn er sich gegen eine Klage zur Wehr setzen will. Zu diesem Zwecke müssen die Parteien unter Umständen Schriftstücke beim Gericht vorlegen, die auch personenbezogene Daten Dritter enthalten. Für solche Datenübermittlungen kann man sich grundsätzlich auf ein berechtigtes Interesse im Sinne des § 28 Abs. 1 Satz 1 Nr. 2 und Abs. 2 BDSG berufen, soweit sie sich auf solche Angaben beschränken, die für die Führung des Prozesses unabdingbar sind. Ordnet das Gericht die Erteilung bestimmter Auskünfte oder die Vorlage von Urkunden an, muss die jeweilige Partei diesem Ersuchen nach § 142 Abs. 1 der Zivilprozessordnung entsprechen. Können die Informationen, die dem Gericht zugänglich gemacht werden müssen, aus programmtechnischen Gründen nur zusammen mit solchen personenbezogenen Daten aus einem PC ausgedruckt werden, die für den jeweiligen Prozess nicht beweiserheblich sind, kann von der vorlagepflichtigen Partei die Schwärzung dieser „überflüssigen“ Angaben nur erwartet werden, wenn angesichts des § 419 der Zivilprozessordnung der Beweiswert der Urkunde dadurch nicht eingeschränkt wird. Gegebenenfalls muss dieser Umstand durch eine Rückfrage beim Gericht geklärt werden.

Diese Grundsätze gelten prinzipiell auch für die Offenlegung besonders sensibler Daten wie zum Beispiel Personal- oder Gesundheitsdaten gegenüber dem Gericht. Doch muss hier das Übermaßverbot in noch stärkerem Maße beachtet werden. Lassen sich die für die Beweisführung nicht erforderlichen Angaben nicht unkenntlich machen, ohne die Urkunde in nachteiliger Weise zu verändern, sollte man beim Gericht beantragen, diese Schriftstücke nicht oder nur auszugsweise der Gegenseite zu überlassen. In einem an uns herangetragenen Fall musste der Arbeitgeber in einem Kündigungsschutzprozess dem Arbeitsgericht eine Liste mit Angaben über zahlreiche Arbeitnehmer seines Unternehmens zur Beurteilung der sogenannten Sozialauswahl vorlegen. Aus dieser Liste konnte man auch die Steuerklasse und Leistungsbewertungen der dort aufgeführten Mitarbeiter ersehen. Bei beiden Angaben handelt es sich um vertraulich zu behandelnde Personaldaten, die wohl für den konkreten Prozess nicht entscheidungserheblich waren. Sollte es tatsächlich technisch nicht möglich gewesen sein, einen Ausdruck ohne diese Daten zu fertigen, hätte sich der Arbeitgeber vor der Übersendung der Liste zumindest bei Gericht erkundigen müssen, ob er die Angaben auf der Liste schwärzen darf.

1.13 Erhebung von Personalausweisdaten von Arbeitnehmern für Flugbuchungen

In einem Unternehmen wurden einige Mitarbeiter per E-Mail gebeten, ihre Personalausweisnummer mitzuteilen. Die Personalausweisnummer sollte vertraulich und nur für interne Zwecke registriert werden. Wir haben auf Anfrage geprüft, ob diese Vorgehensweise des Arbeitgebers zulässig ist. Die Prüfung hat ergeben, dass das Unternehmen die Daten irrtümlich erhoben und gespeichert hat, weil es davon ausgegangen ist, dass für die Buchung einer Geschäftsreise bei einer Fluggesellschaft die Personalausweisdaten der Mitarbeiter erforderlich sind.

Da diese Daten für die Buchung nicht benötigt wurden, war die Datenerhebung und -speicherung unzulässig. Das Unternehmen hat die Personalausweisdaten umgehend gelöscht.

2 Auskunfteien

Die meisten Beschwerden betrafen im Berichtszeitraum wie schon in den Jahren zuvor Auskunfteien und Inkassounternehmen. Eine umfassende Darstellung der Situation und der Probleme in diesem Bereich findet sich im vierten Tätigkeitsbericht (C 1 und 3, S. 27 bis 65 und S. 72 bis 94). Diesmal soll aus der Fülle der Einzelfälle nur eine grundsätzliche Fragestellung (siehe dazu unten Nr. 2.1) herausgegriffen werden. Die datenschutzrechtlichen Probleme mit einer besonderen Form von Auskunfteien, dem AGG-Archiv, werden unter Nr. 2.2 dargestellt.

2.1 Löschungsfristen bei Insolvenzen

Auskunfteien beziehen regelmäßig öffentlich bekannt gemachte Informationen aus Insolvenzverfahren (zum Beispiel den Eröffnungsbeschluss) und speichern diese nach § 29 Abs. 1 Satz 2 BDSG zum Zweck der Übermittlung. Die Frage ist, wie lange Daten aus Insolvenzverfahren gespeichert werden dürfen.

Eine Auskunftei in Baden-Württemberg meinte fünf Jahre und berief sich dafür auf § 26 Abs. 2 Satz 2 der Insolvenzordnung (InsO). Diese Vorschrift besagt, dass das Insolvenzgericht die Schuldner, bei denen der Antrag auf Eröffnung eines Insolvenzverfahrens mangels Masse abgelehnt wurde, in ein Schuldnerverzeichnis einzutragen hat. Die Löschungsfrist für die dort gespeicherten Daten beträgt fünf Jahre. Nach Meinung der Auskunftei gilt diese Löschungsfrist für sämtliche Insolvenzdaten. Dem widersprach die Aufsichtsbehörde. Der Wortlaut des § 26 Abs. 2 Satz 2 InsO und die Systematik sind eindeutig. Die Vorschrift erfasst nur solche Fälle, in denen die Eröffnung des Insolvenzverfahrens mangels Masse abgelehnt wurde. Eine sich auf andere Insolvenzdaten beziehende Löschungsfrist findet sich in der Insolvenzordnung nicht. Die für die Löschung von Daten im Schuldnerverzeichnis nach der Zivilprozessordnung (ZPO) geltende Dreijahresfrist (vergleiche § 915 a ZPO) ist nicht anwendbar. Ein Analogieschluss zu § 26 Abs. 2 InsO kommt mangels einer Regelungslücke nicht in Betracht. Es gilt daher die allgemeine Löschungsfrist für Daten, die geschäftsmäßig zum Zwecke der Übermittlung verarbeitet werden. Diese sind nach § 35 Abs. 2 Satz 2 Nr. 4 BDSG zu löschen, wenn eine Prüfung am Ende des vierten Kalenderjahres nach ihrer erstmaligen Speicherung ergibt, dass eine längerwährende Speicherung nicht erforderlich ist.

Die Auskunftei hat unsere Rechtsauffassung inzwischen akzeptiert. Sie wird die Löschungsfrist für nicht von § 26 Abs. 2 Satz 2 InsO erfasste Insolvenzdaten von fünf auf vier Jahre umstellen.

2.2 AGG-Archiv

Das am 18. August 2006 in Kraft getretene Allgemeine Gleichbehandlungsgesetz (AGG) verfolgt das Ziel, Benachteiligungen aus Gründen der Rasse oder wegen der ethnischen Herkunft, des Geschlechts, der Religion oder Weltanschauung, einer Behinderung, des Alters oder der sexuellen Identität zu verhindern oder zu beseitigen (§ 1 AGG). Auch wer sich um eine Stelle bewirbt, darf nicht aus diesen Gründen benachteiligt werden. Letzteres kann bereits dann der Fall sein, wenn eine Stellenausschreibung in einer Form erfolgt ist, die gegen dieses Verbot ver-

stößt, etwa weil sie nicht geschlechtsneutral formuliert wurde. Das Allgemeine Gleichbehandlungsgesetz sieht für solche Fälle einen Entschädigungsanspruch vor. Wenn ein abgelehnter Bewerber im Streitfall Indizien nachweist, die eine derartige Benachteiligung vermuten lassen, ist der Arbeitgeber beweispflichtig, dass er nicht gegen diese Schutzbestimmungen verstoßen hat, sonst kann der Schadensersatzanspruch begründet sein.

Diese Regelungen veranlassen sogenannte AGG-Hopper, sich immer wieder zu bewerben, allerdings ohne ernsthafte Absicht, die Stelle auch antreten zu wollen. Sie tun dies vielmehr in der Hoffnung, dass dem potenziellen Arbeitgeber ein Fehler im Sinne des Allgemeinen Gleichbehandlungsgesetzes unterläuft, sodass ihn der „Bewerber“ zur Kasse bitten kann. Die Rechtsprechung sieht solche Klagen als rechtsmissbräuchlich an und weist sie ab. Allerdings muss der Arbeitgeber entsprechende Umstände zumindest darlegen. Eine Anwaltskanzlei hat deswegen eine Datei eingerichtet (sogenanntes AGG-Archiv), in der sie – angebliche – AGG-Hopper speichert. Zweck ist es, Arbeitgebern und deren Anwälten die Verteidigung gegen rechtsmissbräuchliche Diskriminierungsklagen zu erleichtern. Die Nutzung der Datei ist unentgeltlich. Auf ihre Existenz wird im Internet aufmerksam gemacht.

Die Speicherung in und die Auskunftserteilung aus dieser Datei erfolgten bislang folgendermaßen:

Arbeitgeber, die von einem Bewerber wegen einer angeblichen Diskriminierung in Anspruch genommen werden, konnten sich beim AGG-Archiv erkundigen, ob dieser in der Vergangenheit bereits mehrfach solche Forderungen geltend gemacht hat. Dabei wurde seitens des AGG-Archivs lediglich verlangt, dass ein entsprechendes Anspruchsschreiben des Betroffenen oder eine Klage zusammen mit der Anfrage vorgelegt werden. Nicht darlegen musste der anfragende Arbeitgeber, ob und gegebenenfalls welche Anhaltspunkte er dafür hat, dass der Antragsteller beziehungsweise Kläger rechtsmissbräuchlich handelt. Die übersandten Unterlagen wurden ohne nähere Prüfung der Person des Einsenders und ohne Prüfung, ob sich aus ihnen der Vorwurf rechtsmissbräuchlichen Handelns gegenüber dem Antragsteller erheben lässt, im AGG-Archiv abgelegt. Zudem wurde eine Karteikarte angelegt, auf der entsprechende Daten gespeichert sind. In Einzelfällen kam es vor, dass auch Anfragen, denen kein Anspruchsschreiben beziehungsweise keine Klageschrift beigefügt war, in die Datei aufgenommen wurden. Selbst Fälle, in denen ohne Betreiben des AGG-Archivs durch eine nachträgliche Anfrage eines Arbeitgebers bekannt wurde, dass der Betroffene mit seinem Antrag beziehungsweise seiner Klage Erfolg hatte, wurden mit der Begründung gespeichert, es könne nicht ausgeschlossen werden, dass das Obsiegen auf einem Prozessbetrug beruht. Dementsprechend wurden Speicherungen in dem Archiv selbst dann nicht bereinigt oder gelöscht, wenn bekannt wurde, dass der Betroffene in einem gerichtlichen Verfahren gegenüber dem Arbeitgeber erfolgreich war und ihm bestätigt wurde, dass er diskriminiert worden war.

Auskunft erhielt der Anfragende aber nur, wenn im AGG-Archiv über den Betroffenen mindestens zwei weitere Einmeldungen vorlagen. Nicht geprüft wurde, ob ein berechtigtes Interesse an der Auskunftserteilung bestand. Die Betreiber des AGG-Archivs stellen sich auf den Standpunkt, dass drei derartige Speicherungen den Verdacht als sogenannter AGG-Hopper rechtfertigen, wenn sie diesen auch nie ausdrücklich als solchen qualifizieren. Der Anfragende erhält nämlich als Auskunft nur die Mitteilung, dass der Betroffene im AGG-Archiv gespeichert ist und wo über ihn weitere Informationen zu in der Vergangenheit geltend gemachten Ansprüchen eingeholt werden können. Werden dem AGG-Archiv zu einem späteren Zeitpunkt insgesamt drei Einmeldungen zu ein und derselben Person bekannt, werden frühere Auskunftsuchende, die zunächst abschlägig beschieden worden sind, noch nachträglich davon in Kenntnis gesetzt.

Speicherung von Daten im AGG-Archiv

Nach § 29 Abs. 1 Satz 1 Nr. 1 BDSG dürfen Auskunfteien personenbezogene Daten zum Zwecke der Übermittlung speichern, wenn kein Grund zu der Annahme besteht, dass diesem Ansinnen ein schutzwürdiges Interesse des Betroffenen entgegensteht. Zwar ist die Führung einer Datei zur Unterstützung anderer bei der Verteidigung gegen missbräuchliche Schadensersatzforderungen grundsätzlich

ein billigenswerter Zweck. Doch darf nicht übersehen werden, dass das Allgemeine Gleichbehandlungsgesetz bei Diskriminierungen ausdrücklich einen Anspruch auf Schadensersatz vorsieht und selbstverständlich nicht jeder als sogenannter AGG-Hopper angesehen werden darf, der dieses Recht für sich in Anspruch nimmt. Selbst wenn ein Kläger mit seinem Begehren vor Gericht erfolglos bleibt, lässt dies noch lange nicht den Schluss auf rechtsmissbräuchliches Verhalten zu. Erst recht darf niemand, der in der Sache mit seinem Schadensersatzbegehren obsiegt hat, in der AGG-Datei gespeichert werden. Bereits die Speicherung einer personenbezogenen Information, die bis auf Weiteres gar nicht an Dritte übermittelt werden soll, stellt nämlich einen Eingriff in das Persönlichkeitsrecht des Betroffenen dar – auch wenn diese Sichtweise den Betreibern des AGG-Archivs nach wie vor schwer fällt. Deswegen muss bei jeder Einspeicherung sehr gewissenhaft geprüft werden, ob die bisherigen Erkenntnisse für sich genommen gesicherte Anhaltspunkte dafür bieten, dass der Betroffene einen Anspruch nach dem AGG rechtsmissbräuchlich geltend gemacht hat. Dafür kann sprechen, dass der Betroffene die Teilnahme an einem Vorstellungsgespräch ohne vernünftige Begründung abgelehnt hat, dass er wahrheitswidrig behauptet, das Ablehnungsschreiben sei nicht aussagekräftig gewesen oder beruhe offensichtlich auf Diskriminierung, dass er sein Bewerbungsschreiben schlampig abgefasst hatte, die Bewerbungsunterlagen offensichtlich unvollständig waren oder dass seine Bewerbung auf die ausgeschriebene Stelle so gut wie nicht eingeht. Ob die Voraussetzungen für die Speicherung im AGG-Archiv gegeben sind beziehungsweise ob Umstände vorliegen, die einer solchen ausdrücklich entgegenstehen, müssen die Betreiber der Datei jeweils im Einzelfall vor der Speicherung prüfen. Sie dürfen sich dabei weder ohne Weiteres auf die Angaben des Einsenders verlassen, noch davon ausgehen, dass drei Einmeldungen zusammen einen hinreichenden Verdacht rechtfertigen.

Übermittlung von Daten aus dem AGG-Archiv

Dieselbe Pflicht trifft sie, wenn sie eine Anfrage beantworten wollen. Selbst wenn die Anwaltskanzlei bei ihrer Auskunft den Betroffenen nicht als sogenannte AGG-Hopper qualifizieren will und lediglich mitteilt, wer über diese Person weitere Angaben machen kann, lässt die Aussage, dass sie im AGG-Archiv gespeichert ist, den Schluss zu, dass der Betroffene als jemand angesehen wird, der rechtsmissbräuchlich handelt. Die Beantwortung einer Anfrage muss stets unterbleiben, wenn die Betroffenen daran ein schutzwürdiges Interesse haben (§ 29 Abs. 2 Satz 1 Nrn. 1 a und 2 BDSG). Das ist immer der Fall, wenn der Anfragende kein berechtigtes Interesse an der Auskunft dargelegt hat, wenn die Speicherung der Daten, über die Auskunft erteilt werden sollen, schon gar nicht hätte erfolgen dürfen, wenn sie inzwischen wieder hätten gelöscht werden müssen, etwa weil ein Gericht den Anspruch das abgelehnten Bewerbers bestätigt hat und nichts dafür spricht, dass Prozessbetrug im Spiel war, oder wenn die Umstände des Einzelfalls einer Auskunftserteilung entgegenstehen.

Übermittlung von Daten an das AGG-Archiv

Aber auch die beim AGG-Archiv anfragenden nichtöffentlichen und öffentlichen Stellen, die dabei Unterlagen mit personenbezogenen Daten übermitteln, müssen prüfen, ob die Übermittlung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG oder den für öffentliche Stellen geltenden Datenschutzvorschriften zulässig ist. Sie dürfen Daten nur übermitteln, wenn sie aufgrund des Anspruchschreibens beziehungsweise der Klageschrift und des Verhaltens der Bewerber im Verfahren tatsächliche Anhaltspunkte dafür haben, dass es sich um einen sogenannten AGG-Hopper handelt. Die Anfrage beziehungsweise die Datenübermittlung dient also der „Verdachtsverdichtung“.

Da die Anfragen aus ganz Deutschland kommen, unterliegen die anfragenden öffentlichen Stellen sowie die nichtöffentlichen Stellen, die nicht in Baden-Württemberg ansässig sind, der Aufsicht anderer Datenschutzaufsichtsbehörden. Die baden-württembergische Aufsichtsbehörde hat deswegen ihre datenschutzrechtliche Beurteilung mit den anderen für den nichtöffentlichen Bereich zuständigen Datenschutzaufsichtsbehörden abgestimmt.

Aktueller Sachstand

Da die Betreiber des AGG-Archivs die Auskunftei in ihrer bisherigen Form für zulässig hielten, musste die Aufsichtsbehörde mit ihnen eine eingehende Rechtsdiskussion führen, die sich über einen längeren Zeitraum hinzog. In zahlreichen Schreiben und Gesprächen hat die Aufsichtsbehörde versucht, auf einen datenschutzkonformen Betrieb der Datei hinzuwirken. Von Nachteil war, dass das geltende Bundesdatenschutzgesetz (§ 38 Abs. 5) den Aufsichtsbehörden in solchen Fällen nicht die Möglichkeit einräumt, eine verbindliche Anordnung zu erlassen und diese erforderlichenfalls im Wege des Verwaltungszwangs durchzusetzen. Die an sich mögliche Verhängung eines Bußgelds wegen datenschutzrechtlicher Verstöße ist kein geeignetes Mittel, die Rechtslage verbindlich zu klären.

Trotz dieser Schwierigkeiten konnte mit den Betreibern des AGG-Archivs inzwischen eine grundsätzliche Einigung über die künftige Verfahrensweise erzielt werden. Einige Details sind allerdings noch zu klären. Die Aufsichtsbehörde bedauert es sehr, dass die Betreiber des Archivs bei diesem Diskussionsstand trotz mehrfacher Aufforderung durch die Aufsichtsbehörde nicht bereit waren, mit der Bereinigung ihres Datenbestands wenigstens zu beginnen. Dabei steht schon jetzt fest, dass in erheblichem Umfang Datensätze gelöscht werden müssen, weil die Betroffenen ganz offensichtlich keine sogenannten AGG-Hopper sind.

3 Rechtsanwälte

3.1 Entsorgung von Mandantenakten am Straßenrand

Eine Anwaltskanzlei rückte für einige Zeit in das Blickfeld der Aufsichtsbehörde, als Medien darüber berichteten, Teile von Mandantenakten seien mehrfach als Altpapier gebündelt vor dem Geschäftsgebäude dieser Kanzlei gefunden worden. Die Ermittlungen der Aufsichtsbehörde ergaben, dass in den Kanzlei- und den Kellerräumen, in denen Altakten der Kanzlei aufbewahrt wurden, außer den Kanzleiangehörigen weitere, nicht auf das Datengeheimnis verpflichtete Personen Zugang zu den Mandantenakten hatten. Des Weiteren wurde festgestellt, dass Altakten im fraglichen Zeitraum vorübergehend in einem nicht abgeschlossenen Kellerraum zwischengelagert worden waren, weil sie von einem Rechtsanwalt der Kanzlei daraufhin überprüft werden sollten, ob sie endgültig in einem vor dem Gebäude stehenden Container entsorgt werden können. In diesem Kellerraum wurde auch Altpapier, beispielsweise Zeitungen, gelagert, bevor es am Straßenrand gebündelt entsorgt wurde. Auch zu diesem Raum hatten mehrere nicht der Kanzlei angehörende Personen Zutritt. Ob die hier zwischengelagerten oder in anderen Räumen aufbewahrten Akten an den Straßenrand gelangten, wie und wie oft dies geschah und wer dafür verantwortlich war, konnte die Aufsichtsbehörde trotz intensiver Bemühungen nicht klären. Es konnte lediglich noch in Erfahrung gebracht werden, dass die Entsorgungsfirma den Container mit den aussortierten Mandantenakten zu einem auf die Entsorgung von Haus-Wertstoff- und Biomüll sowie von Gewerbe- und Sonderabfällen spezialisierten, der Rechtsanwaltskanzlei nicht namentlich bekannten Unternehmen brachte, das die Akten aufgrund eines Unterauftrags „nach den Bestimmungen des Bundesdatenschutzgesetzes“ vernichten sollte.

Bei dieser Sachlage konnte die Aufsichtsbehörde weder der Anwaltskanzlei noch einer anderen Person nachweisen, dass sie unbefugt sensible Daten übermittelt hatte, indem sie die Mandantenakten an den Straßenrand verbracht hatte, sodass Dritte Einsicht nehmen konnten. Ein Übermitteln im Sinne des § 3 Abs. 4 Nr. 3 BDSG lag nicht vor. Der dafür begriffsnotwendige finale Aspekt fehlt nämlich, wenn Datenträger ohne bewusste Mitwirkung des Besitzers – etwa durch versehentliches Liegenlassen oder durch Versäumnisse in technischer oder organisatorischer Hinsicht – in die Verfügung eines Dritten übergehen.

Die Anwaltskanzlei hat jedoch als datenschutzrechtlich verantwortliche Stelle nicht alles Erforderliche getan, um eine datenschutzgerechte Aufbewahrung und Entsorgung ihrer Mandantenakten sicherzustellen. So hätte die Kanzlei – um § 9 BDSG zu genügen – den Zugang der nicht der Kanzlei angehörenden Personen zu den im verschließbaren Keller aufbewahrten Altakten entweder ausschließen oder genau regeln, insbesondere zeitlich und sachlich einschränken müssen. Ferner

hätte die Kanzlei diese Personen eindeutig und schriftlich darüber belehren müssen, wie sie mit sensiblen Unterlagen der Kanzlei umzugehen haben und wie diese zu entsorgen sind, insbesondere dass diese nicht mit Altpapier vermengt werden dürfen.

Darüber hinaus hat die Anwaltskanzlei auch nicht die für die eigentliche Entsorgung der nicht mehr benötigten Mandantenakten erforderlichen technischen und organisatorischen Maßnahmen ergriffen (vergleiche § 9 BDSG). Zum einen bestanden bereits Zweifel, ob die Anwaltskanzlei tatsächlich eine Entsorgungsfirma ausgesucht hatte, die in der Lage war, auch sensibles Datenmaterial vorschriftsmäßig zu vernichten (§ 11 Abs. 2 Satz 1 BDSG). Zum andern hätte sie mit dieser nach § 11 Abs. 2 Satz 2 BDSG insbesondere *schriftlich* vereinbaren müssen, wie der sichere Transport und die sichere Aufbewahrung der Datenträger bis zur endgültigen Vernichtung gewährleistet werden, wie die Vernichtung der Daten unter Berücksichtigung ihrer Schutzbedürftigkeit zu erfolgen hat, wo die Vernichtung durchgeführt wird, dass die Vernichtung zu protokollieren ist sowie ob und gegebenenfalls welche Unterauftragnehmer eingeschaltet werden dürfen. Auch hätte sich die Anwaltskanzlei nach § 11 Abs. 2 Satz 4 BDSG zumindest durch Stichproben davon überzeugen müssen, dass die eingeschalteten Firmen tatsächlich die vereinbarten technischen und organisatorischen Maßnahmen einhalten.

Die Aufsichtsbehörde hat das Vorgehen der Rechtsanwaltskanzlei beanstandet und sie aufgefordert, Maßnahmen zu treffen, die einen datenschutzgerechten Umgang mit den Mandantenakten in Zukunft sicherstellen. Ein Bußgeld konnte gegen die Rechtsanwaltskanzlei nicht verhängt werden, weil ein „unbefugtes Übermitteln“ personenbezogener Daten im Sinne des § 43 Abs. 2 Nr. 1 BDSG aus den oben genannten Gründen nicht festgestellt werden konnte und die festgestellten Verstöße gegen die §§ 9 und 11 BDSG (bislang) nicht bußgeldbewehrt sind (siehe dazu oben A 2.1.2).

Die Aufsichtsbehörde hat aus Anlass dieses Falls über die Kammern an alle Berufsgeheimnisträger, insbesondere Rechtsanwälte, appelliert, mit den ihnen anvertrauten sensiblen personenbezogenen Daten und Unterlagen sorgsam umzugehen, ihre Mitarbeiter auf das Datengeheimnis zu verpflichten und die im Bundesdatenschutzgesetz enthaltenen Vorschriften über die Datensicherung und die Beauftragung von Unternehmen, die sensible personenbezogene Unterlagen transportieren und vernichten, einzuhalten. Als Auftraggeber seien sie insbesondere verpflichtet, Serviceunternehmen unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen und diese mit den erforderlichen schriftlichen Anweisungen zu versehen.

3.2 Wenn eine Rechtsanwaltskanzlei wie ein Inkassounternehmen tätig wird – Teil 2

Die Aufsichtsbehörde hatte bereits in ihrem vierten Tätigkeitsbericht (C 2, S. 65 ff.) über eine Rechtsanwaltskanzlei berichtet, die für ein führendes Telekommunikationsunternehmen im Rahmen des Anwaltsmandats das gesamte Forderungsmanagement betreibt, also wie ein Inkassounternehmen tätig wird. Die Rechtsanwaltskanzlei bedient sich dazu der Unterstützung eines Auftragsdatenverarbeiters. Die Rechtsanwaltskanzlei, die rund zehn Millionen Kundendatensätze speichert, entzieht sich seit Anfang 2006 der Aufsicht durch die Datenschutzaufsichtsbehörde, indem sie sich wie die Rechtsanwaltskammern darauf beruft, Rechtsanwälte seien aufgrund des in § 43 a Abs. 2 der Bundesrechtsanwaltsordnung (BRAO) und § 203 Abs. 1 Nr. 3 StGB geregelten Mandatsgeheimnisses gegenüber den Datenschutzaufsichtsbehörden zur Verschwiegenheit berechtigt und verpflichtet. Die Betroffenen hätten dadurch keinen Nachteil, weil sich die von den Rechtsanwaltskammern durchzuführende Berufsaufsicht (§ 56 und § 73 Abs. 2 Nr. 4 BRAO) auch auf alle Fragen des Datenschutzes und der Datensicherheit strecke. Es bedürfe daher keiner weiteren Aufsicht durch die Datenschutzaufsichtsbehörde.

Bemerkenswert an dem Fall war, dass sich die Rechtsanwaltskanzlei auf ihr angebliches Auskunftsverweigerungsrecht gegenüber der Datenschutzaufsichtsbehörde erst berief, nachdem diese wegen zahlreicher Bürgerbeschwerden eine datenschutzrechtliche Kontrolle bei ihr durchgeführt und eine Reihe von Verstößen gegen datenschutzrechtliche Vorschriften festgestellt hatte. Die Aufsichtsbehörde hatte deswegen die Rechtsanwaltskanzlei aufgefordert, die erforderlichen Verfah-

rensänderungen vorzunehmen. Dies hatte die Rechtsanwaltskanzlei wiederholt unter Hinweis auf die angebliche Nichtanwendbarkeit des Bundesdatenschutzgesetzes abgelehnt.

Keinen Erfolg bei der Rechtsanwaltskanzlei hatten auch diejenigen Betroffenen, die versuchten, ihre Datenschutzrechte selbst durchzusetzen. Insbesondere verweigerte die Rechtsanwaltskanzlei den Betroffenen die Auskunft darüber, welche personenbezogenen Daten sie über sie speichert. Die Rechtsanwaltskanzlei konnte sich dabei auch auf ein zu ihren Gunsten ergangenes Landgerichtsurteil stützen.

Dieser Zustand war außerordentlich unbefriedigend, weil sich immer wieder Bürger bei der Aufsichtsbehörde darüber beschwerten, dass sich die Rechtsanwaltskanzlei geweigert habe, auf ihr datenschutzrechtliches Anliegen einzugehen oder ihnen auch nur zu antworten. Auch kam es auf diese Weise zu einer Ungleichbehandlung der Inkassounternehmen in Baden-Württemberg. Denn selbstverständlich müssen sich die anderen Inkassounternehmen an das Bundesdatenschutzgesetz halten.

Die Aufsichtsbehörde versuchte deshalb, mit Hilfe der Rechtsanwaltskammern wenigstens in diesem besonders gelagerten Einzelfall zu einer den berechtigten Interessen der Betroffenen Rechnung tragenden Lösung zu kommen. Die Rechtsanwaltskammern waren hierzu jedoch nicht bereit. Durch Erlass eines – gerichtlich überprüfbaren – Verwaltungsakts eine Klärung herbeizuführen, schied ebenfalls aus, da das Bundesdatenschutzgesetz diese Möglichkeit nicht vorsieht. Daher wandte sich die Aufsichtsbehörde an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Gemeinsam wurde das Telekommunikationsunternehmen aufgefordert, die Rechtsanwaltskanzlei in den Inkassofällen generell von der anwaltlichen Schweigepflicht zu entbinden. Außerdem sollte es bei der Rechtsanwaltskanzlei darauf hinwirken, dass diese

- der Aufsichtsbehörde generell Auskunft auf ihre Fragen nach § 38 Abs. 3 BDSG erteilt und sich Kontrollen der Aufsichtsbehörde nach § 38 Abs. 4 BDSG unterwirft,
- einen fachkundigen Beauftragten für den Datenschutz bestellt,
- Betroffenen Auskunft nach § 34 BDSG über die zu ihrer Person gespeicherten Daten erteilt,
- ein Verfahrensverzeichnis führt, in das Jedermann Einsicht nehmen kann,
- ein Sperr- und Löschkonzept für die von ihr betriebene automatisierte Datei erarbeitet und die erforderlichen Datenberichtigungen, -sperrungen und -löschungen vornimmt,
- bei Benachrichtigung der Betroffenen nach § 33 BDSG die Art der gespeicherten Daten angibt und
- technische und organisatorische Maßnahmen prüft, um möglichst zu vermeiden, dass bei Namensähnlichkeit der falsche Schuldner angeschrieben und mit Beitreibungsmaßnahmen überzogen wird.

Das Telekommunikationsunternehmen hat den Forderungen der Aufsichtsbehörde inzwischen im Grundsatz Rechnung getragen; Einzelheiten müssen noch bilateral erörtert werden. Die Aufsichtsbehörde wird sich bei einem Besuch vor Ort und bei der Überprüfung von Einzelfällen von der Umsetzung ihrer Forderungen überzeugen.

Möglicherweise ist der Einzelfall damit befriedigend gelöst. Der grundsätzliche Dissens zwischen den Aufsichtsbehörden und den Rechtsanwaltskammern über die Frage, ob beziehungsweise inwieweit Rechtsanwaltskanzleien dem Bundesdatenschutzgesetz und der Aufsicht durch die Datenschutzaufsichtsbehörden unterliegen, bleibt jedoch bestehen. Er kann nur durch den Bundesgesetzgeber gelöst werden. Dies sieht auch der Deutsche Bundestag so. In einer vor kurzem gefassten Entschließung zum 21. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (Bundestags-Drucksache 16/12271) heißt es dazu:

„Der Deutsche Bundestag teilt die Auffassung der Bundesregierung, dass das Bundesdatenschutzgesetz auch für Rechtsanwälte gilt. Er begrüßt, dass die

Bundesregierung prüft, welche gesetzlichen Regelungen sich im Zusammenhang mit der Verarbeitung mandatsbezogener Daten durch Rechtsanwälte empfehlen, um eine wirksame Datenschutzkontrolle zu gewährleisten, ohne dass das besonders geschützte Vertrauensverhältnis zwischen Rechtsanwalt und Mandant in unzulässiger Weise beeinträchtigt wird."

Es bleibt zu hoffen, dass die Prüfung durch die Bundesregierung bald zu einem Abschluss kommt und erforderliche Gesetzesänderungen sodann auf den Weg gebracht werden.

4 Versicherungen

4.1 Neue Einwilligungs- und Schweigepflichtentbindungserklärung in Versicherungsverträgen, Verhaltensregeln für die Versicherungswirtschaft, Umgestaltung des Hinweis- und Informationssystems der Versicherungswirtschaft (HIS)

In ihrem vierten Tätigkeitsbericht (C 4.1, S. 94 ff.) berichtete die Aufsichtsbehörde darüber, dass und weshalb die Datenschutzaufsichtsbehörden mit dem Gesamtverband der Deutschen Versicherungswirtschaft (GDV) über eine neue Einwilligungs- und Schweigepflichtentbindungserklärung in Versicherungsverträgen und eine Umgestaltung des Hinweis- und Informationssystems der Versicherungswirtschaft (HIS) verhandeln. Inzwischen sind auch Verhaltensregeln im Sinne des § 38 a BDSG, die sich die Versicherungswirtschaft selbst geben will, Gegenstand der Erörterung.

Im Einzelnen stellt sich der Sachstand wie folgt dar:

4.1.1 Neue Einwilligungs- und Schweigepflichtentbindungserklärung

Im Grundsatz besteht zwischen Datenschutzaufsichtsbehörden und der Versicherungswirtschaft Einigkeit darüber, dass sich eine neue Einwilligungs- und Schweigepflichtentbindungserklärung auf diejenigen Datenerhebungen, -verarbeitungen und -nutzungen beschränken soll, die in der Versicherungsbranche erforderlich sind und nicht auf eine gesetzliche Grundlage gestützt werden können. Die Erklärung soll sich dementsprechend nur auf Gesundheitsdaten und Werbung beziehen.

Der inzwischen erarbeitete Entwurf einer Einwilligungs- und Schweigepflichtentbindungserklärung begegnet noch einigen datenschutzrechtlichen Bedenken:

- So sieht er vor, dass alle Versicherungssparten durch eine einheitliche Einwilligungs- und Schweigepflichtentbindungserklärung abgedeckt werden. Besonderheiten der einzelnen Sparten werden dabei nicht berücksichtigt. Personenbezogene Daten dürfen nur erhoben werden, wenn sie für die Durchführung des Vertrags erforderlich sind. Die Erhebung von Gesundheitsdaten bei Antragstellung ist beispielsweise bei Kranken-, Lebens- und Berufsunfähigkeitsversicherungen erforderlich, nicht jedoch bei einer Reisegepäck- oder Kraftfahrzeugversicherung. Müssen zur Schadensabwicklung im Rahmen von Versicherungsverträgen Gesundheitsdaten erhoben und verarbeitet werden, genügt es, wenn die Einwilligungs- und Schweigepflichtentbindungserklärung in diesem Zeitpunkt abgegeben wird. Es ist nicht zulässig, wegen der theoretischen Möglichkeit, dass Gesundheitsdaten benötigt werden, auf Vorrat die Abgabe einer Schweigepflichtentbindungserklärung zu verlangen.
- Der Entwurf berücksichtigt nicht die Möglichkeit, die Betroffenen aufzufordern, Unterlagen, die die Versicherung benötigt, selbst beizubringen. Auf diese Möglichkeit hat das Bundesverfassungsgericht in seiner Entscheidung vom 23. Oktober 2006 – 1 BvR 2027/02 hingewiesen.
- Die aufgelisteten Verwendungszwecke für Gesundheitsdaten sind zu allgemein gehalten und nicht abschließend. Eine auf diese Informationen gestützte Einwilligung wäre daher problematisch.
- Problematisch erscheint auch, über eine Einwilligungs- und Schweigepflichtentbindungserklärung die Grundlage für eine zentralisierte Bearbeitung inner-

halb einer Gruppe von rechtlich selbstständigen Versicherungs- und Finanzdienstleistungsunternehmen zu schaffen und auf diesem Weg zu einem im Bundesdatenschutzgesetz nicht vorgesehen Konzernprivileg zu kommen.

– Der Entwurf einer Einwilligungserklärung für die Werbung ist insofern irreführend, als der Eindruck entstehen könnte, der Betroffene könne über die Verwendung seiner Daten für Zwecke der Werbung und der Markt- und Meinungsforschung durchweg selbst entscheiden. Deutlich werden muss, welche Datenerhebungen, -verarbeitungen und -nutzungen auf welcher Grundlage stattfinden, welchen die Betroffenen widersprechen können und welche nur auf Grundlage einer Einwilligung erfolgen.

Es bleibt zu hoffen, dass sich Aufsichtsbehörden und Versicherungswirtschaft in den weiteren Verhandlungen auf eine diesen Bedenken Rechnung tragende Einwilligungs- und Schweigepflichtentbindungserklärung einigen können.

4.1.2 Verhaltensregeln für die Versicherungswirtschaft

Die Versicherungswirtschaft beabsichtigt, sogenannte Verhaltensregeln für den Umgang mit personenbezogenen Daten aufzustellen. Diese sollen von dem für den GDV zuständigen Berliner Beauftragten für Datenschutz und Informationsfreiheit auf Vereinbarkeit mit dem Datenschutzrecht geprüft und danach für alle beitretenden Versicherungsunternehmen verbindlich sein.

Sinn und Zweck dieser Regeln soll es nach eigenen Angaben sein, für die Versicherungswirtschaft weitestgehend einheitliche Standards zu schaffen, die Einhaltung datenschutzrechtlicher Regeln zu fördern und den Versicherten der beigetretenen Unternehmen die Gewähr dafür zu bieten, dass Datenschutz- und Datensicherheitsbelange bei der Gestaltung und Bearbeitung von Produkten und Dienstleistungen berücksichtigt werden.

Der Entwurf umfasst nach derzeitigem Stand ohne Anlage 16 Seiten. Die baden-württembergische Aufsichtsbehörde steht ihm kritisch gegenüber. Sie hält den Nutzen dieser Verhaltensregeln für gering.

Nach § 38 a BDSG dienen Verhaltensregeln der Durchführung datenschutzrechtlicher Regelungen. Sie sollen die aus dem Datenschutzrecht resultierenden Handlungs- und Unterlassungspflichten auf eine branchen- und praxisnahe Weise konkretisieren und präzisieren, sodass sie von den Anwendern gut umgesetzt werden können. Beispielhaft werden in der Literatur die Auslegung einzelner gesetzlicher Erlaubnistatbestände, die anwendungsbezogene Konkretisierung unbestimmter Rechtsbegriffe und die Präzisierung von Abwägungsklauseln durch Fallgruppen genannt. Auch können in Verhaltensregeln stärkere datenschutzrechtliche Garantien gegenüber dem Betroffenen festgelegt werden.

Diesen Anforderungen wird der vorliegende Entwurf nicht gerecht. Er beschränkt sich in weiten Teilen darauf, die geltende Gesetzeslage wiederzugeben; Präzisierungen, Beispielsfälle und Fallgruppen enthält er nur an wenigen Stellen. Insbesondere löst er kaum eine der seit Jahren zwischen Aufsichtsbehörden und Versicherungswirtschaft streitig erörterten Fragen. Beispielsweise gibt er keine Antwort auf die Frage, in welchen Fällen Versicherungen Bonitätsabfragen bei Auskunfteien durchführen dürfen. Grund hierfür ist, dass Datenschutzaufsichtsbehörden und Versicherungswirtschaft unterschiedliche Auffassungen zur Zulässigkeit solcher Abfragen vertreten. Auch die Regelungen zum Scoring, zum Hinweis- und Informationssystem, zur Werbung, zur Markt- und Meinungsforschung und zum Datenaustausch mit Vorversicherern und Rückversicherern lösen die bestehenden Probleme nicht. Es ist daher bereits jetzt absehbar, dass die Versicherungsunternehmen die Verhaltensregeln in ihrem Sinn auslegen und sich dabei auf eine vermeintlich abgestimmte Regelung mit den Aufsichtsbehörden berufen werden.

Einen weiteren Vorteil dürfte die Versicherungswirtschaft in Regelungen zur gemeinsamen Verarbeitung von Daten innerhalb der Unternehmensgruppe, zu den Pflichten bei der Datenverarbeitung im Auftrag und zur Funktionsübertragung an Dienstleister sehen, in denen gewissermaßen durch die Hintertür ein im Bundesdatenschutzgesetz nicht vorgesehenes Konzernprivileg für die Versicherungswirtschaft eingeführt werden soll.

Dem Entwurf sollte daher in seiner jetzigen Fassung kein „Gütesiegel“ erteilt werden. Einen Mehrwert würden Verhaltensregeln nur darstellen, wenn es in den angesprochenen Streitfragen zu datenschutzkonformen Lösungen käme, die anschließend in präziser und konkreter Form in die Verhaltensregeln aufgenommen werden. Die Verhaltensregeln mit sogenannten Platzhalterregelungen für die noch nicht gelösten Probleme in Kraft zu setzen, die sich auf die Wiedergabe des Gesetzes beschränken, hält die baden-württembergische Aufsichtsbehörde nicht für den richtigen Weg.

4.1.3 Umgestaltung des Hinweis- und Informationssystems der Versicherungswirtschaft (HIS)

Im vierten Tätigkeitsbericht (C 4.1.3, S. 99 ff.) wurde das Hinweis- und Informationssystem der Versicherungswirtschaft (HIS) in seiner derzeitigen Form kurz beschrieben; eine ausführliche Darstellung findet sich im Internet unter *www.datenschutzzentrum.de/wirtschaft/20070703-his/htm*. Die Aufsichtsbehörden halten HIS in seiner jetzigen Form in mehrfacher Hinsicht für rechtswidrig. Insbesondere kann HIS nicht – wie es die Versicherungswirtschaft bisher getan hat – auf Einwilligungserklärungen der Versicherungsnehmer gestützt werden. Die Einwilligungserklärung genügt nämlich bereits aufgrund ihrer Unverständlichkeit nicht den gesetzlichen Anforderungen. Auch verstößt sie gegen grundsätzliche Wertungen des Bundesdatenschutzgesetzes und ist daher als Bestandteil allgemeiner Geschäftsbedingungen unwirksam. Überdies haben nicht alle eingemeldeten Personen, zu denen auch Zeugen und Unfallgeschädigte gehören können, eine Einwilligungserklärung unterschrieben. Unzulässig ist auch, dass die an HIS angeschlossenen Versicherungen derzeit alle paar Wochen den aktuellen Gesamtbestand aller eingemeldeten Daten übermittelt bekommen, unabhängig davon, ob die jeweilige Versicherung tatsächlich ein berechtigtes Interesse an den konkreten Informationen hat oder nicht. Eine Information der Betroffenen über die beabsichtigte Einmeldung in HIS erfolgte bislang nicht

Der GDV ist bereit, HIS völlig umzugestalten und als zentrale Auskunftei nach § 29 BDSG zu betreiben. Er hat dazu ein Konzept vorgelegt, das von den Aufsichtsbehörden grundsätzlich gebilligt wurde. Problematisch ist, dass nach dem vom GDV vorgelegten Zeitplan der Umbau von HIS nicht – wie ursprünglich angenommen – Ende 2008, sondern erst im Juli 2011 abgeschlossen sein soll. Der Verband hat dafür mehrere Gründe angeführt: Zunächst habe die Umstellung mit dem Kartellamt abgestimmt werden müssen; jetzt gehe es darum, die Branche für den Umbau in eine Auskunftei zu vernetzen und den Antragsbereich vollständig umzugestalten. Dafür fielen erhebliche Investitions- und jährliche Betriebskosten an. Diese machten eine zeitaufwendige Abstimmung innerhalb des Verbands erforderlich. Der technische Umgestaltungsaufwand ergebe sich vor allem daraus, dass die Suchfunktion künftig einen eindeutigen Treffer generieren müsse.

Die Aufsichtsbehörden brachten ihren Unmut über diese Verzögerung gegenüber dem GDV deutlich zum Ausdruck. Sie hielten diese nur dann für hinnehmbar, wenn die Rechte der Betroffenen sofort gestärkt werden. Der GDV hat inzwischen mitgeteilt, dass

- er seit 1. April 2009 Betroffenen nach § 34 BDSG Auskunft über die zu ihrer Person gespeicherten Daten erteilt;
- er seine Mitgliedsunternehmen auf die Notwendigkeit hingewiesen hat, Personen, die in HIS eingemeldet werden, zu benachrichtigen;
- die Einmeldekriterien für HIS in der Sparte Rechtsschutz schon jetzt eingeschränkt werden. Künftig sollen Einmeldungen erst ab vier Schadensfällen in den vergangenen zwölf Monaten erfolgen. Bisher wurde schon bei zwei Schadensfällen in zwölf Monaten beziehungsweise drei Schadensfällen in 36 Monaten eingemeldet.

Die Aufsichtsbehörde wird prüfen, ob die in Baden-Württemberg ansässigen Versicherungsunternehmen entsprechend verfahren.

Aufsichtsbehörden und Versicherungswirtschaft haben zudem verabredet, die sogenannten 60-Punkte-Kriterienkataloge, die in den einzelnen Sparten Grundlage

für die Einmeldung im HIS sind, in einer gemeinsamen Arbeitsgruppe einer Überprüfung zu unterziehen. Die Kriterienkataloge gehen nach Angaben der Versicherungswirtschaft auf durch Rechtsprechung gestützte Erfahrungswerte aus anderen Schadensfällen zurück. Die Aufsichtsbehörden haben jedoch Zweifel, ob auf den genauen Umständen des Einzelfalls beruhende Gerichtsentscheidungen sich ohne Weiteres auf andere Fälle übertragen lassen und auch bei ihnen als Kriterien für einen beabsichtigten Versicherungsbetrug angesehen werden können.

4.2 Datenübermittlung an einen Versicherungsvermittler

Eine Beschwerdeführerin hat sich an die Aufsichtsbehörde gewandt, weil sie die Art und Weise, wie eine Versicherung mit ihren Daten umging, nicht akzeptieren wollte. Sie hatte die Versicherung telefonisch unter Angabe von Namen, Anschrift, Telefonnummer, Geburtsdatum und Beruf um ein schriftliches Angebot für eine private Krankenversicherung gebeten. Wenige Tage später hatte sie ein Schreiben von einem ihr nicht bekannten Versicherungsmakler erhalten mit dem Hinweis, dass er Kooperationspartner der Versicherung sei und von dieser gebeten worden sei, zu ihr Kontakt aufzunehmen. Mit den Daten der Krankenversicherung hatte der Versicherungsmakler für die Beschwerdeführerin eine Computeranalyse erstellt.

Die Prüfung hat ergeben, dass die Versicherung die zur Erstellung eines Angebots erhobenen Daten an ein rechtlich selbstständiges Versicherungsvermittlungsunternehmen, das an keine bestimmte Versicherung gebunden ist (Versicherungsmakler), übermittelt hat. Die Beschwerdeführerin wurde nach ihren Angaben bei der Datenerhebung weder um eine Einwilligung in die Übermittlung ihrer Daten an den Versicherungsmakler gebeten noch wurde sie darüber unterrichtet, dass und an wen ihre Daten übermittelt werden sollen.

Diese Vorgehensweise verstieß gegen das Bundesdatenschutzgesetz. Es war nicht erforderlich, dass die Krankenversicherung die personenbezogenen Daten der Betroffenen zur Erstellung eines Angebots an ein rechtlich selbstständiges Unternehmen übermittelt. Die Versicherung hätte den Auftrag selbst erledigen können. Auch überwiegen bei dem gegebenen Sachverhalt die schutzwürdigen Belange der Beschwerdeführerin, da diese über die beabsichtigte Datenübermittlung nicht informiert wurde, wie dies § 4 Abs. 3 BDSG gebietet, und daher nicht damit rechnen musste, dass die Versicherung ihre Daten für die Angebotserstellung an einen Versicherungsmakler übermittelt.

Die Versicherung hat zugesagt, künftig Interessenten über die beabsichtigte Datenverarbeitung zu unterrichten und von ihnen eine Einwilligung in die Datenübermittlung an einen Versicherungsmakler einzuholen.

4.3 Übermittlung personenbezogener Daten nach Auflösung einer Versicherungsmakler-GmbH an ein Nachfolgeunternehmen

Ein Unternehmen hat den Kunden einer von ihm übernommenen Versicherungsmakler-GmbH mitgeteilt, der Geschäftsbetrieb dieses Unternehmens werde eingestellt. Die GmbH hatte bisher sämtliche Versicherungsangelegenheiten ihrer Kunden erledigt. Um auch künftig eine qualitativ hochwertige Betreuung der bisherigen Kunden sicherzustellen, sollten die Kunden- und Vertragsdaten der Versicherungsmakler-GmbH an ein anderes Unternehmen übermittelt werden. Das Versicherungsunternehmen räumte den Kunden der Versicherungsmakler-GmbH ein Widerspruchsrecht gegen die Datenübermittlung ein. Der Widerspruch konnte jedoch nur innerhalb einer sehr kurzen Frist ausgeübt werden. Daher haben sich einige Betroffene an die Aufsichtsbehörde gewandt. Deren Prüfung hat ergeben, dass eine Datenübermittlung nur mit Einwilligung der Betroffenen zulässig ist, da die Voraussetzungen des § 28 Abs. 1 Satz 1 Nr. 2 BDSG nicht vorliegen. Die vom Unternehmen behauptete nachwirkende Betreuungspflicht besteht nicht. Eine solche kann auch nicht Vorschriften des Versicherungsvertragsgesetzes (VVG), insbesondere dessen § 61, entnommen werden. Zweifelhaft ist bereits, ob zur Ansprache der Kunden die Übermittlung von Vertragsdaten und Unterlagen erforderlich ist. Dies bedurfte jedoch keiner abschließenden Klärung, da einer umfänglichen Datenübermittlung auf jeden Fall schutzwürdige Belange der bisherigen Kunden entgegenstehen. Diese Bedenken können nicht durch Gewährung eines Widerspruchrechts ausgeräumt werden.

Beim Vertrag mit einem Versicherungsmakler geht es häufig um ein besonderes Vertrauensverhältnis. Mit Kündigung der Maklerverträge durch den Rechtsnachfolger des bisherigen Vertragspartners ist es den bisherigen Kunden überlassen, ob sie die Hilfe eines anderen Versicherungsmaklers in Anspruch nehmen wollen und wessen sie sich hierfür bedienen. Auf keinen Fall dürfen personenbezogene Daten und Unterlagen der Kunden einfach an einen Dritten übermittelt werden. Der bisherige Maklervertrag sah vor, dass das Unternehmen nach Beendigung des Vertrags sämtliche Unterlagen, die es aus der Tätigkeit erhalten hat, an den Auftraggeber herauszugeben hat. Hiervon ausgenommen waren nur Unterlagen, zu deren Aufbewahrung ein Versicherungsmakler nach anderen Vorschriften verpflichtet ist. Der Vertrag enthielt keine Grundlage für eine Datenübermittlung an einen vom Unternehmen als „Nachfolger“ ausgewählten Versicherungsmakler. Dies wurde dem Unternehmen mitgeteilt.

Dagegen hat die Aufsichtsbehörde eine Übermittlung von Namen, Vornamen und Anschriften der bisherigen Kunden an einen anderen Versicherungsmakler für Zwecke der Werbung nach § 28 Abs. 3 BDSG als zulässig angesehen, sofern den bisherigen Kunden zuvor eine angemessene Frist zur Einlegung des Widerspruchs gegen die Datenübermittlung eingeräumt wird. Außerdem muss sichergestellt sein, dass das Nachfolgeunternehmen keine weitere Kontaktaufnahme versucht, wenn der Kunde des bisherigen Unternehmens auf die Werbeansprache nicht reagiert.

Kurze Zeit später teilte uns das Unternehmen mit, es verzichte auf eine Übermittlung von Vertragsdaten der Kunden an das vorgesehene Nachfolgeunternehmen.

5 Kreditwirtschaft

5.1 Verwendung von Kundendaten für Zwecke der Werbung

5.1.1 Auswertung von Girokontodaten durch Zahlungsstromanalysen

Auch im Berichtszeitraum haben sich wieder mehrere Bankkunden darüber beschwert, dass ihre Girokontodaten gezielt für Werbeaktionen ausgewertet wurden. Beispielsweise hat eine Bank die Girokontenumsätze ihrer Kunden daraufhin durchgesehen, ob diese Versicherungsbeiträge an eine Gebäudeversicherung leisten und gegebenenfalls an welche (Zahlungsstromanalyse). Je nach Ergebnis rief sie dann ihre Kunden an mit dem Ziel, ihnen den Abschluss einer Gebäudeversicherung mit einem Versicherungsunternehmen zu vermitteln, das mit ihr geschäftlich verbunden ist. Der Beauftragte für den Datenschutz wurde vorher nicht beteiligt.

Eine Nutzung der bei einer Bank gespeicherten personenbezogenen Daten ist nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat. Wenn für die gezielte Auswertung des Überweisungsverkehrs keine Einwilligung des Betroffenen vorliegt, beurteilt sich deren Zulässigkeit an Hand einer vom Bundesdatenschutzgesetz geforderten Interessenabwägung. Diese führt zu dem Ergebnis, dass die schutzwürdigen Interessen der Betroffenen an dem Ausschluss der Nutzung ihrer für andere Zwecke gespeicherten Daten gegenüber der Wahrung der berechtigten Interessen der Bank überwiegen. Dabei fällt ins Gewicht, dass diese Kunden von ihrer Bank nicht darüber informiert wurden, dass und in welchem Umfang ihre Kontodaten ausgewertet und für Werbezwecke genutzt werden. Bankkunden erwarten von ihrer Bank jedoch mit Fug und Recht, dass sie die ihr im Rahmen eines Girokontovertrags bekannt werdenden Daten, gleich welchen Inhalts, ausschließlich zum Zweck der Durchführung der Girokontotransaktionen verwendet. Damit ist eine Datennutzung nicht vereinbar, bei welcher der Kunde den Eindruck haben muss, dass er gezielt beobachtet wird.

Unzulässig war auch, dass die Bank die Telefonnummern der Betroffenen ohne deren ausdrückliche Einwilligung zum Zwecke der telefonischen Werbung nutzte. Dies ergibt sich aus § 7 Abs. 2 UWG in Verbindung mit § 4 a BDSG (vergleiche dazu schon den vierten Tätigkeitsbericht C 6.1, S. 133 ff.). Die Aufsichtsbehörde stellt in diesem Zusammenhang immer wieder fest, dass Banken der Auffassung sind, Telefonwerbung sei datenschutzrechtlich der Direktwerbung per Post gleichgestellt und daher immer dann zulässig, wenn der Betroffene der Werbung nicht

widersprochen habe. Teilweise wird von Banken auch die Auffassung vertreten, der telefonische Hinweis auf günstige Anlagemöglichkeiten oder auf das Angebot einer mit der Bank zusammenarbeitenden Versicherung stelle keine unerlaubte Telefonwerbung dar, sondern diene der umfassenden Wahrung der finanziellen Interessen ihres Kunden, zu der die Bank mit Abschluss eines (Girokonto-) Vertrags verpflichtet sei. Dies ist so nicht richtig. Unter den Begriff „Werbung“ fallen alle Anrufe, die darauf abzielen, über die Klärung von Fragen innerhalb eines bereits bestehenden Vertragsverhältnisses hinaus den Kunden zum Abschluss eines neuen Vertrags oder auch nur zur inhaltlichen Änderung, insbesondere zur Verlängerung, Ausweitung oder Ergänzung des bestehenden Vertragsverhältnisses zu bewegen. Die Aufsichtsbehörde nutzt daher jede Gelegenheit, um die Banken auf die Rechtslage hinzuweisen. Dazu gehört nunmehr auch der Hinweis, dass nach der Änderung des Gesetzes gegen den unlauteren Wettbewerb (vergleiche dazu A 2.3) Telefonwerbung ohne Einwilligung der Betroffenen künftig von der Bundesnetzagentur als Ordnungswidrigkeit bußgeldrechtlich geahndet werden kann.

Im Übrigen hat die Aufsichtsbehörde die zahlreichen datenschutzrechtlichen Verstöße von Banken zum Anlass genommen, mit dem Verband ein Gespräch zu führen, damit er seine Mitglieder über die Rechtslage unterrichtet.

5.1.2 Werbeanruf einer Versicherung nach einer Bankveranstaltung

Ein Bankkunde hat sich an die Aufsichtsbehörde gewandt, weil er einen Werbeanruf von einer Versicherung erhalten hatte. Seine eigenen Recherchen haben ergeben, dass „seine“ Bank seine Daten an diese Versicherung übermittelt hatte, nachdem er bei einer Veranstaltung der Bank bei der Bewirtung geholfen hatte.

Die Prüfung hat ergeben, dass die Bank nach einem Mitgliederforum sowohl Namen, Adressen und Geburtsdaten von Helfern bei dieser Veranstaltung, soweit sie Kunden der Bank sind, als auch von in der Anwesenheitsliste gespeicherten Teilnehmern an der Mitgliederversammlung an die ihr verbundene Versicherung (Kooperationspartner) übermittelt hat. Die Datenübermittlung erfolgte ohne Einwilligung des Beschwerdeführers und der betroffenen Kunden, da die bei Kontoeröffnung im Standardformular enthaltene Einwilligungserklärung sich nicht auf die Versicherung erstreckte, an die die Daten übermittelt wurden. Die gesetzlichen Voraussetzungen für die Datenübermittlung lagen nicht vor. Die schutzwürdigen Interessen der Betroffenen an dem Ausschluss der Übermittlung überwogen die Interessen der Bank, da weder die Daten der Bewirtungshelfer noch die Daten der Teilnehmer an der Mitgliederversammlung für „Werbezwecke“ gespeichert wurden. Mit einer derartigen Zweckänderung muss niemand rechnen, zumal die Bank darauf auch nicht hingewiesen hatte. Die unbefugte Verarbeitung von Kundendaten wurde beanstandet.

5.2 Auswertung der Umsätze eines gemeinsamen Girokontos durch die Personalabteilung

Eine Bankangestellte hatte bei ihrem Arbeitgeber zusammen mit ihrem Ehemann ein Girokonto eingerichtet. Im Rahmen einer arbeitsgerichtlichen Auseinandersetzung mit ihrer Mitarbeiterin wertete die Bank die Umsätze des gemeinsamen Girokontos der Eheleute aus, um festzustellen, wie hoch die Einkünfte der Mitarbeiterin aus einer genehmigten Nebentätigkeit waren. Der Ehemann beschwerte sich hierüber bei der Aufsichtsbehörde.

Die Überprüfung hat ergeben, dass Mitarbeiter der Personalabteilung die Umsätze des gemeinsamen Girokontos der Eheleute ausgewertet hatten. Das war nicht zulässig. Bei Gemeinschaftskonten muss die Bank die schutzwürdigen Interessen aller Vertragspartner berücksichtigen. Die Auswertung der Girokontodaten des Gemeinschaftskontos diente nicht der Zweckbestimmung des (Bank-)Vertragsverhältnisses zwischen der Bank und den Eheleuten, vielmehr ging es allein um das Arbeitsverhältnis zwischen der Bank und ihrer Angestellten und die Nutzung der Daten für eine arbeitsgerichtliche Auseinandersetzung. Diese Zweckentfremdung verletzte die schutzwürdigen Interessen der Mitarbeiterin und erst recht des beschwerdeführenden Ehemanns, der durch die Auswertung zwangsläufig mitbetroffen war. Die Bank durfte sich die Daten nicht selbst beschaffen, sondern hätte die Höhe der Nebeneinkünfte ihrer Angestellten im Arbeitsgerichtsprozess feststellen lassen müssen.

Unzulässig war es auch, Mitarbeitern der Personalabteilung den Zugriff auf die Kontodaten zu eröffnen. Girokontoumsätze enthalten viele durch das Bankgeheimnis geschützte Daten. Auf diese Daten sollen nur die Bankmitarbeiter Zugriff haben, die in der Kundenbetreuung tätig sind.

Die Aufsichtsbehörde hat die Vorgehensweise der Bank beanstandet und diese aufgefordert, künftig durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass nur die in der Kundenbetreuung tätigen Mitarbeiter im Rahmen der datenschutzrechtlichen Vorschriften unter Beachtung des Erforderlichkeitsgrundsatzes Zugriff auf die Kontodaten der Kunden haben.

5.3 Identifizierung minderjähriger Vertragspartner

Banken und Kreditinstitute sind nach dem Geldwäschegesetz verpflichtet, ihre Vertragspartner grundsätzlich vor Begründung der Geschäftsbeziehung zu identifizieren. Bisher verlangen die Banken und Institute in Einklang mit den gesetzlichen Regelungen die Vorlage eines gültigen Ausweises. Nach dem Geldwäschegesetz sind sie berechtigt, zu Dokumentationszwecken eine Ausweiskopie anzufertigen (siehe dazu auch zweiter Tätigkeitsbericht B Nr. 7.5 S. 73 ff.).

Die Pflicht zur Identifizierung besteht auch bei Begründung einer Geschäftsbeziehung mit minderjährigen Vertragspartnern. Deshalb ist es datenschutzrechtlich nicht zu beanstanden, wenn die gesetzlichen Vertreter eines Minderjährigen zum Zwecke der Identitätsfeststellung um Vorlage eines Kinderreisepasses gebeten werden und die Bank von diesem eine Kopie anfertigt. Dabei dürfen nur diejenigen Seiten kopiert werden, welche die erforderlichen Identifizierungsdaten enthalten. Abweichend hiervon kann sich eine Bank bei der Kontoeröffnung durch Minderjährige aber auch mit der Vorlage einer Geburtsurkunde begnügen.

Nach den sich aus dem Geldwäschegesetz ergebenden allgemeinen Sorgfaltspflichten sind die Banken und Kreditinstitute zu einer kontinuierlichen Überwachung der Geschäftsbeziehung verpflichtet. Sie haben daher sicherzustellen, dass die jeweiligen Dokumente, Daten oder Informationen in angemessenen zeitlichen Abständen aktualisiert werden.

5.4 Identität Datenschutzbeauftragter/Geldwäschebeauftragter

Die Aufsichtsbehörde hat bei mehreren Kreditinstituten beziehungsweise Banken festgestellt, dass diese dem Beauftragten für den Datenschutz auch die Funktion des Geldwäschebeauftragten beziehungsweise umgekehrt übertragen haben.

Die Aufsichtsbehörde hat die Unternehmen darauf hingewiesen, dass dies unzulässig ist. Der Geldwäschebeauftragte hat zur Wahrnehmung seiner Aufgabe einen umfassenden Zugriff auf personenbezogene Daten und verarbeitet diese unter anderem auch durch den Einsatz automatisierter Verfahren. Da der Beauftragte für den Datenschutz auch den Geldwäschebeauftragten kontrollieren muss, würde dies bedeuten, dass er sich im Falle der Personenidentität selbst kontrollieren muss. Eine Selbstkontrolle ist jedoch grundsätzlich nicht effektiv. Um Interessenkonflikte zu vermeiden und um die unabhängige Stellung des Datenschutzbeauftragten nicht zu gefährden (§ 4 f Abs. 2 Satz 1 BDSG verlangt, dass der Beauftragte zuverlässig ist), ist nach Auffassung aller in der AG Kreditwirtschaft des Düsseldorfer Kreises vertretenen Datenschutzaufsichtsbehörden eine Trennung der beiden Aufgaben unverzichtbar.

Die Aufsichtsbehörde hat die Unternehmen, bei denen die beiden Funktionen von einer Person wahrgenommen werden, gebeten, diese Funktionen voneinander zu trennen. Die Aufsichtsbehörde wird die Umsetzung überwachen.

5.5 Darlehensinformationen auf dem Kontoauszug

Der Darlehensvertrag einer Bank sah vor, dass dem Darlehensnehmer aktuelle Darlehensinformationen beim Einzug der fälligen Zahlungen grundsätzlich auf den Kontoauszügen mitgeteilt werden. Für die Fälle, in denen das Konto, von dem die Forderungen eingezogen werden, nicht bei der darlehensgebenden Bank geführt wird, enthielt der Darlehensvertrag folgende Regelung: „Sofern das Kon-

to, von dem die Bank ihre Forderungen einzieht, bei einem anderen Kreditinstitut als der Bank geführt wird, ist der Darlehensnehmer damit einverstanden, dass auf den Kontoauszügen bei diesem Kreditinstitut der jeweils aktuelle Stand der Kapitalrestschuld sowie Zinsen und Tilgung angegeben werden ...". Diese Erklärung war im Darlehensvertrag optisch nicht besonders hervorgehoben.

Die Aufsichtsbehörde hat bei der Überprüfung dieser Vorgehensweise festgestellt, dass diese Einverständniserklärung nicht den Anforderungen des § 4 a Abs. 1 Satz 3 BDSG entsprach, der vorsieht, dass die Einwilligung besonders hervorzuheben ist, wenn sie zusammen mit anderen Erklärungen schriftlich erteilt werden soll. Die Bank hat die erforderlichen Anpassungen zugesagt.

6 Werbung, Adresshandel, Glücksspiele

6.1 Werbung

Im Werbebereich erreichten uns so viele Beschwerden wie nie zuvor. Gerügt wurde unter anderem:

– Nichtbeachten der gesetzlichen Voraussetzungen des § 28 Abs. 1 bis 3 in Verbindung mit § 4 Abs. 3 BDSG

  Teilweise war die Verarbeitung und Nutzung personenbezogener Daten für Zwecke der Werbung rechtswidrig, weil keiner der in § 28 Abs. 1 bis 3 BDSG genannten Zulässigkeitstatbestände vorlag. Für manche Unternehmen verkürzt sich der Datenschutz bei der Werbung auf die Widerspruchsmöglichkeit des Betroffenen. Sie übersehen dabei völlig, dass zunächst einmal die materiellen Voraussetzungen für die Datenerhebung, -verarbeitung und -nutzung vorliegen müssen. Häufig lag dies daran, dass der Betroffene bei der Datenerhebung nicht, wie es § 4 Abs. 3 Satz 1 BDSG vorschreibt, darüber unterrichtet worden war, dass seine Daten (auch) für Werbezwecke genutzt oder an Dritte für Werbezwecke übermittelt werden. Bei Preisausschreiben und Gewinnspielen, die zumeist der Gewinnung von Adressdaten dienen, stellten wir wiederholt solche Mängel fest. Die im vierten Tätigkeitsbericht (B, S. 19 ff.) dargestellten Ergebnisse einer Untersuchung der Aufsichtsbehörde zur Beachtung des § 4 Abs. 3 BDSG bestätigten sich damit. Dies ist bedauerlich, da § 4 Abs. 3 BDSG eine zentrale Vorschrift für den Persönlichkeitsrechtsschutz der Bürger darstellt. Der Bürger muss, wie es das Bundesverfassungsgericht schon in seinem Volkszählungsurteil (BVerfGE 65, 1 ff. auszugsweise zitiert unter Nr. 11.4) gesagt hat, wissen können, was mit seinen Daten geschieht. Um die Beachtung des § 4 Abs. 3 BDSG zu verbessern, hat der Bundesrat in seiner Stellungnahme zum Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften vorgeschlagen, § 4 Abs. 3 BDSG stringenter zu fassen und Verstöße dagegen als eigenständige Ordnungswidrigkeit auszugestalten.

– Fehlender Hinweis auf die Widerspruchsmöglichkeit (§ 28 Abs. 4 Satz 2 BDSG)

  Weite Teile der Wirtschaft haben die im Entwurf eines Gesetzes zur Regelung eines Datenschutzaudits und zur Änderung des Bundesdatenschutzgesetzes vorgesehene Einschränkung des sogenannten Listenprivilegs und den Übergang von der Widerspruchs- zur Einwilligungslösung (vergleiche dazu oben A 2.1.2) heftig bekämpft. Sie haben dabei auch damit argumentiert, die Widerspruchslösung habe sich in der Praxis bewährt, nennenswerte Verstöße dagegen seien nicht bekannt geworden. Dies kann die Aufsichtsbehörde so nicht bestätigen.

  In der Praxis wird nach wie vor häufig nicht beachtet, dass der Betroffene bei der „Ansprache zum Zwecke der Werbung" über die verantwortliche Stelle und darüber zu unterrichten ist, dass er der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung gegenüber der verantwortlichen Stelle widersprechen kann (§ 28 Abs. 4 Satz 2 BDSG). Mitunter wird verkannt, dass sich dieser Hinweis weder dadurch erübrigt, dass der Betroffene bei der Datenerhebung nach § 4 Abs. 3 BDSG über die beabsichtigte Verwendung seiner Daten

(auch) für Werbezwecke unterrichtet wurde, noch dadurch, dass der Betroffene bei einer früheren „Ansprache zum Zwecke der Werbung“ auf sein Widerspruchsrecht hingewiesen wurde. Der *Hinweis muss* nach Wortlaut sowie nach Sinn und Zweck der Regelung *bei jeder Werbeaktion erfolgen*. Wünschenswert wäre freilich, dass die Unternehmen ihre Kunden – wenn möglich – schon bei der Datenerhebung auf ihr Widerspruchsrecht gegen Werbezusendungen hinweisen und ihnen die Möglichkeit einräumen, es sofort auszuüben, indem sie beispielsweise in Vordrucken ein entsprechendes Kästchen zum Ankreuzen vorsehen. So weit gehen jedoch noch nicht einmal Unternehmen, die lautstark nach der Einführung eines Datenschutzaudits rufen, und damit indirekt zum Ausdruck bringen, dass sie sich selbst in datenschutzrechtlicher Hinsicht als vorbildlich ansehen.

– Nichtbeachtung eines eingelegten Werbewiderspruchs (§ 28 Abs. 4 Satz 1 BDSG)

  Widerspricht der Betroffene bei der verantwortlichen Stelle der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung, ist eine Nutzung oder Übermittlung für diese Zwecke unzulässig (§ 28 Abs. 4 Satz 1 BDSG). Obwohl diese Vorschrift verhältnismäßig klar gefasst ist, kommt es immer wieder zu Verstößen. Zum Teil liegt dies daran, dass Unternehmen die Dauerwirkung eines Widerspruchs nicht beachten. Diese zwingt die Unternehmen dazu, die Widersprechenden in eine Sperrliste einzutragen, mit der vor jeder neuen Werbeaussendung ein Abgleich stattfindet. Die Aufsichtsbehörde stellt jedoch immer wieder fest, dass eine solche Sperrliste nicht geführt wird oder in Einzelfällen ein Eintrag in diese „vergessen“ wurde. Mitunter hat die Aufsichtsbehörde allerdings auch den Eindruck, dass Unternehmen Verstöße gegen diese Vorschrift als „Kavaliersdelikt“ ansehen, für die man sich im Falle einer Beschwerde entschuldigt.

  Hin und wieder beruft sich ein Unternehmen auch darauf, sein Schreiben an Kunden sei kein Verstoß gegen das Nutzungsverbot des § 28 Abs. 4 Satz 1 BDSG gewesen, weil es sich dabei nicht um eine „Ansprache zum Zwecke der Werbung“ gehandelt habe. So war es beispielsweise in einem Fall, in dem ein Unternehmen seine Kundenkarteninhaber – auch solche, die der Zusendung von Werbeschriften widersprochen hatten – auf eine Neuerung im Zusammenhang mit der Kundenkarte, aber eben auch auf einen neu eröffneten Shop aufmerksam machen wollte. Das Schreiben enthielt damit zumindest auch Werbung, weshalb die Kundenkarteninhaber, die einen Werbewiderspruch eingelegt hatten, nicht hätten angeschrieben werden dürfen. Das Unternehmen hat zugesagt, dies künftig zu beachten.

– Nichtbeachtung des Einwilligungserfordernisses bei Telefon- und E-Mail-Werbung

  Telefon- und E-Mail-Werbung sind nach § 7 UWG ohne die dafür erforderliche Einwilligung des Betroffenen in der Regel unzulässig und verstoßen damit auch gegen den Datenschutz (vergleiche dazu im Einzelnen vierter Tätigkeitsbericht, C 6.1, S. 133 ff.). Erstaunlich ist, wie viele Unternehmen dies noch nicht wissen oder zu wissen scheinen. Manche Unternehmen argumentieren damit, die Kontaktaufnahme erfolge nicht zum Zwecke der Werbung, sondern der Beratung. Andere Unternehmen verknüpfen Meinungsumfrage und Werbung in der Weise miteinander, dass sie den Angerufenen zunächst nach seiner Meinung zu einem bestimmten Thema fragen, um anschließend für ein konkretes Produkt zu werben. In der Regel wird es sich dabei um unzulässige Telefonwerbung handeln.

– Auskunft über gespeicherte Daten

  Viele Bürger beantragen, wenn sie von einer Firma adressierte Werbung erhalten, bei dieser Auskunft über die zu ihrer Person gespeicherten Daten, teilweise auch über die Herkunft dieser Daten. Manche Firmen reagieren darauf überhaupt nicht, andere lassen sich damit Zeit und/oder geben nur unvollständig Auskunft. Wieder andere verweisen an dritte Stellen, die Eigner der Adressen sind. Im Falle eines großen Adresshändlers mit Sitz in Baden-Württemberg stellten innerhalb kurzer Zeit Tausende von Bürgern einen Auskunftsantrag

nach § 34 BDSG mit der Folge, dass sich die Auskunftserteilung erheblich verzögerte. In vielen dieser Fälle wenden sich die Bürger an die Aufsichtsbehörde. In der Regel kann ihnen zu einer Auskunft verholfen werden. Allerdings kann auch von der Aufsichtsbehörde nicht immer (zuverlässig) festgestellt werden, woher Adressdaten stammen, weil viele Unternehmen mit mehreren Adresslieferanten zusammenarbeiten und das Wandern der Daten nicht vollständig nachvollzogen werden kann. Deshalb wäre es wichtig, dass in Werbebriefen die Herkunft der Daten angegeben wird. Das von Bundestag und Bundesrat vor kurzem beschlossene Gesetz zur Änderung datenschutzrechtlicher Vorschriften verpflichtet in Werbefällen unter bestimmten Voraussetzungen zur Angabe der Stelle, die die Daten erstmalig erhoben hat beziehungsweise zur Angabe der verantwortlichen Stelle.

6.2 Wahlwerbung

Im Vorfeld der jüngsten Kommunalwahlen in Baden-Württemberg beschwerten sich mehrere Bürger bei der Aufsichtsbehörde darüber, Kandidaten für den Gemeinderat hätten für ihre Wahlwerbung in unzulässiger Weise ihnen zur Verfügung stehende Adressenlisten genutzt oder sie aus anderem Grund unzulässig angeschrieben. Bei Redaktionsschluss für diesen Tätigkeitsbericht waren noch nicht alle Beschwerdefälle abgeschlossen. Generell kann dazu Folgendes gesagt werden:

- Kandidaten für den Gemeinderat sind nichtöffentliche Stellen, die den Vorschriften des Bundesdatenschutzgesetzes unterliegen, soweit sie personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen erheben, verarbeiten oder nutzen oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben. Sie verwenden die Daten nicht ausschließlich für persönliche Angelegenheiten, weil sie als Bewerber um ein öffentliches Amt mit ihrer Wahlwerbung in die Öffentlichkeit treten.
- Ein Kandidat darf nicht einfach auf personenbezogene Daten, die ihm in anderer Eigenschaft, beispielsweise als Gemeinderat oder als Mitglied einer Kammer oder eines Vereins zugänglich oder als Arzt oder Rechtsanwalt anvertraut worden sind, zugreifen und diese für seine eigene Wahlwerbung nutzen. Diese Daten (zum Beispiel die Daten der Vereinsmitglieder) wurden für einen bestimmten Zweck oder für bestimmte Zwecke (beispielsweise des Vereins) erhoben und gespeichert und dürfen grundsätzlich auch nur hierfür genutzt werden. Jedenfalls wenn die Daten nicht für den Zweck erhoben und gespeichert wurden, eine politische Partei oder einen Kandidaten bei einer Wahl zu unterstützen, wird die Verwendung der Daten für einen anderen Zweck, nämlich für Zwecke der Wahlwerbung, in der Regel unzulässig sein, da dadurch schutzwürdige Belange der Betroffenen beeinträchtigt werden. Daten beispielsweise der Vereinsmitglieder dürfen daher von einem Kandidaten in der Regel nicht für seine Wahlwerbung genutzt werden, der Verein darf sie in der Regel nicht für diesen Zweck zur Verfügung stellen.
- Auch wenn ein Kandidat Adressdaten rechtmäßig für Zwecke der Wahlwerbung erhalten hat, muss er bei deren Verarbeitung und Nutzung die dafür geltenden Datenschutzvorschriften beachten. Dabei müssen Wahlbewerber beim Versand adressierter Wahlwerbung nach Rechtsprechung und datenschutzrechtlicher Literatur beachten, dass diese der kommerziellen Werbung gleichsteht:
  - Adressierte Werbung darf daher per Post nur unter Beachtung des § 28 Abs. 4 BDSG verschickt werden. Sie muss also einen Hinweis darauf enthalten, dass und wem gegenüber der Empfänger der weiteren Nutzung (oder Übermittlung) seiner Daten für Zwecke der Wahlwerbung widersprechen kann. Legt der Betroffene Widerspruch ein, muss dieser beachtet werden (§ 28 Abs. 4 Satz 1 BDSG).
  - Der Versand von Wahlwerbung per E-Mail ist ohne Einwilligung des Betroffenen unzulässig. Dies ergibt sich zwar in diesem Fall nicht aus § 7 UWG, wohl aber hat ein Betroffener einen Unterlassungsanspruch aus § 823 in Verbindung mit § 1004 BGB. Die Nutzung von E-Mail-Adressen für Zwecke der Wahlwerbung ohne Einwilligung der Betroffenen ist daher datenschutzrechtlich unzulässig.

6.3 Glücksspiel

Im August 2008 häuften sich Meldungen, wonach Unternehmen insbesondere aus dem Lotteriebereich und von diesen beauftragte Callcenter per Lastschrift Geldbeträge von Konten abgebucht hätten, obwohl deren Inhaber angaben, diesen Unternehmen keine personenbezogenen Daten, insbesondere keine Bankverbindungsdaten, mitgeteilt zu haben (sogenannte Kontodatenaffäre). Einen solchen Sachverhalt trugen auch zwei Bürger vor, die sich über ein Unternehmen beschwerten, das in Baden-Württemberg Lotto-Tippgemeinschaften organisiert (siehe dazu unten Nr. 6.3.1).

Dass im Zusammenhang mit der Kontodatenaffäre immer wieder der Name der Süddeutschen Klassenlotterie (SKL) fiel, war für die Aufsichtsbehörde Anlass, den Datenschutz bei der SKL näher zu untersuchen (siehe dazu unten Nr. 6.3.2).

6.3.1 Missbrauch von Kontodaten?

Zwei Beschwerdeführer trugen vor, ein Lotto-Tippgemeinschaften organisierendes Unternehmen habe von ihren Girokonten Geld abgebucht, obwohl sie dem Unternehmen keine personenbezogenen Daten über sich mitgeteilt hätten. Die Aufklärung des Sachverhalts gestaltete sich außerordentlich schwierig. Fragen der Aufsichtsbehörde an das Unternehmen blieben unbeantwortet. Auch der Rechtsanwalt, der die Vertretung des Unternehmens angezeigt hatte, reagierte lange nicht. Schließlich konnte in Erfahrung gebracht werden, dass das Unternehmen ein Callcenter beauftragt hatte, mit den potenziellen Kunden telefonisch in Kontakt zu treten.* Die Aufsichtsbehörde führte deshalb bei dem Callcenter einen unangekündigten Kontrollbesuch durch. Das Callcenter teilte mit, es habe die beiden Beschwerdeführer angerufen. Die Adressdaten seien von anderen Unternehmen bezogen worden, wobei sich die Herkunft der Daten nur in einem Fall letztlich klären ließ. In beiden Fällen konnte das Unternehmen keine Einwilligungserklärung der Betroffenen in die Telefonwerbung vorlegen. Es behauptete, mit seinen Adresslieferanten stets zu vereinbaren, dass für die gelieferten Daten wirksame Einwilligungen in die Telefonwerbung vorliegen müssen (sogenannte Opt-Ins). Dass solche tatsächlich vorliegen, sei von ihm allerdings zu keinem Zeitpunkt geprüft worden. Allerdings wisse man inzwischen aus anderen Verfahren, dass die Opt-Ins nicht den rechtlichen Anforderungen genügt hätten. In den Telefonaten mit den beiden Beschwerdeführern sei es zu einem Vertragsabschluss gekommen. Dabei hätten die Beschwerdeführer auch ihre Kontonummern genannt. In einem Fall sei der Vertragsabschluss ausdrücklich bestätigt worden. Zum Beweis legte das Callcenter entsprechende Eintragungen der Callcenter-Agenten in die von diesen benutzte automatisierte Datei vor. Da die Beschwerdeführer am Spiel teilgenommen hätten, seien von ihren Konten entsprechende Beträge per Lastschrift abgebucht worden.

Die Aufsichtsbehörde kam zu dem Ergebnis, dass das Unternehmen die Betroffenen ohne die dafür erforderliche Einwilligung in die Telefonwerbung angerufen hatte. Dies wurde beanstandet. Offen blieb, ob es zum Abschluss eines Spielvertrags gekommen war. Insoweit standen die Aussagen der Beschwerdeführer gegen die Aussage des Unternehmens. Das Unternehmen war daher rechtlich zumindest zur Sperrung der Daten verpflichtet. Es erklärte sich zur Löschung der Daten bereit.

6.3.2 Datenschutz bei der SKL

6.3.2.1 Verwicklung der SKL in den sogenannten Kontodatenskandal?

Dem Unabhängigen Datenschutzzentrum Schleswig-Holstein wurde im August 2008 eine CD mit 17.000 Datensätzen zugespielt, die aus einem Callcenter in Lübeck stammten. Darunter sollen sich auch knapp 2.000 Datensätze von Bürgern aus Baden-Württemberg befunden haben. Die Datensätze enthielten Nachnamen, Vornamen, Adressen, Telefonnummern und Bankverbindungen der betroffenen Personen. Der Zusammenhang zwischen diesen Datensätzen und der SKL ergab

* Hinweis: Die Anrufe erfolgten vor Inkrafttreten des Glücksspielstaatsvertrags.

sich daraus, dass die Namen der Dateien, in denen diese Datensätze enthalten waren, unter anderem das Kürzel „skl“ enthielten. Später wurden noch weitere derartige Vorgänge in anderen Bundesländern bekannt. Die Aufsichtsbehörde nahm deshalb sofort Kontakt zu der SKL-Direktion in München und zu den Datenschutzaufsichtsbehörden der mit den datenschutzrechtlichen Ermittlungen befassten Bundesländer auf, um festzustellen, ob ein der hiesigen Datenschutzaufsicht unterliegender staatlicher Lotterieeinnehmer in die Kontodatenaffäre verwickelt ist. Dafür ergaben sich jedoch keine Anhaltspunkte.

6.3.2.2 Ist der Datenschutz bei der SKL gewährleistet?

Die Aufsichtsbehörde ließ es jedoch nicht bei dieser Überprüfung bewenden. Sie ging vielmehr auch der Frage nach, ob der Datenschutz „bei der SKL“ gewährleistet ist. Dabei spielte eine Rolle, dass die Aufsichtsbehörde bei der Überprüfung mehrerer staatlicher Lotterieeinnehmer in den Jahren 2004 und 2005 datenschutzrechtliche Mängel festgestellt hatte.

Um beurteilen zu können, ob der Datenschutz „bei der SKL“ gewährleistet ist, muss man deren Organisation kennen:

Die SKL wird als staatliche Klassenlotterie von den Ländern Baden-Württemberg, Bayern, Hessen, Rheinland-Pfalz und Thüringen veranstaltet. Rechtsgrundlage ist das Gesetz zum Staatsvertrag zwischen den genannten Ländern über eine staatliche Klassenlotterie (SKL-Staatsvertrag vom 15. Dezember 1992, GBl. S. 798). Die SKL ist eine rechtsfähige Anstalt des öffentlichen Rechts mit Sitz in München. Organe der Anstalt sind der Staatslotterieausschuss und die Direktion. Die SKL-Lose werden von staatlichen Lotterieeinnehmern im Auftrag und auf Rechnung der SKL verkauft. Ein Direktvertrieb durch die SKL erfolgt nicht. Deshalb verfügt die SKL auch nicht über eigene Kunden- beziehungsweise Spielerdaten. Die Direktion speichert lediglich die Daten von Großgewinnern, deren Gewinne von ihr ausgezahlt werden sowie von Personen, die Anfragen an das Kunden-Service-Center der Direktion gerichtet haben. Die Spielerdaten hält jeder staatliche Lotterieeinnehmer für sich vor. Einen gemeinsamen Datenpool gibt es nicht. Die rechtlich selbstständigen staatlichen Lotterieeinnehmer entscheiden – bislang jedenfalls – selbst darüber, welche Spielerdaten sie wie erheben, verarbeiten und nutzen, ob sie die Daten automatisiert oder manuell speichern, welche IuK-Technik sie im Falle der automatisierten Datenverarbeitung einsetzen, wie lange sie die Daten speichern, wer auf die Daten Zugriff hat und ob und gegebenenfalls welche Daten sie an Dritte übermitteln. Sie müssen dabei insbesondere die Vorschriften des Bundesdatenschutzgesetzes, den seit 1. Januar 2008 geltenden Staatsvertrag zum Glücksspielwesen in Deutschland, der die Telefonwerbung untersagt, sowie die Geschäftsanweisung, die zu Stillschweigen bezüglich der Spielteilnehmer und deren Teilnahme an den Lotterien verpflichtet, beachten. Soweit die staatlichen Lotterieeinnehmer ihren Sitz in Baden-Württemberg haben, unterliegen sie der Kontrolle der hiesigen Aufsichtsbehörde. Die Datenschutzaufsicht über die Anstalt übt der Bayerische Landesbeauftragte für den Datenschutz aus.

Zusammenfassend lässt sich sagen, dass die staatlichen Lotterieeinnehmer, was den Datenschutz und die Datensicherung angeht, weitgehend eigenverantwortlich handeln, obwohl sie im Auftrag und auf Rechnung der SKL tätig sind und ansonsten Vorgaben der Direktion unterliegen, die in der Geschäftsanweisung enthalten sind. Die Aufsichtsbehörde hat deshalb gegenüber der SKL-Direktion angeregt, zu prüfen, ob im Lichte der jüngsten Ereignisse den staatlichen Lotterieeinnehmern Vorgaben auch in Bezug auf die Erhebung, Verarbeitung und Nutzung von Spielerdaten sowie zu den erforderlichen technischen und organisatorischen Datenschutzmaßnahmen (§ 9 BDSG) gemacht werden können und sollen. Die SKL-Direktion hat hierzu eine Arbeitsgruppe einberufen, an der zeitweise auch die Aufsichtsbehörde teilnahm. Die Arbeitsgruppe kam zu dem Ergebnis, dass die staatlichen Lotterieeinnehmer zwar Beauftragte der SKL sind und die ihnen obliegenden Geschäfte nach den Weisungen der Anstalt zu besorgen haben, datenschutzrechtlich jedoch nicht als Datenverarbeiter im Auftrag (§ 11 BDSG) anzusehen sind. Sie werden vielmehr im Wege der Funktionsübertragung tätig. Die Arbeitsgruppe war sich ferner einig, dass die SKL-Direktion den staatlichen Lotterieeinnehmern – ungeachtet der unterschiedlichen Verhältnisse bei ihnen – Vorgaben in Bezug auf technisch-organisatorische Maßnahmen machen sollte. Die

Aufsichtsbehörde hat darüber hinaus weitere Vorgaben in Bezug auf den Datenschutz gefordert, beispielsweise dass die Betroffenen bei der Datenerhebung nach § 4 Abs. 3 BDSG stets über die Zwecke der Erhebung, Verarbeitung und Nutzung der Daten und die Kategorien von Datenempfängern zu unterrichten sind und dass geregelt wird, ob und inwieweit Spielerdaten für Werbezwecke gespeichert, genutzt und übermittelt werden dürfen, wann die Daten zu löschen sind und was bei der Beauftragung von Serviceunternehmen, beispielsweise Callcentern, zu beachten ist. Besonders wichtig erscheint der Aufsichtsbehörde, dass die staatlichen Lotterieeinnehmer angehalten werden, die Auftragsdatenverarbeiter sorgfältig auszuwählen und diesen konkrete schriftliche Vorgaben in Bezug auf die Nutzung und Verarbeitung personenbezogener Daten, insbesondere auch die Löschung der Daten nach Auftragserledigung, sowie die technischen und organisatorischen Datenschutzmaßnahmen zu machen. Auch muss sichergestellt werden, dass sich staatliche Lotterieeinnehmer in regelmäßigen Zeitabständen von der Einhaltung des Datenschutzes bei den Datenverarbeitern im Auftrag überzeugen. Geregelt werden muss, wie dies zu geschehen hat und zu dokumentieren ist.

Außerdem sollte erwogen werden, bei Gelegenheit im Staatsvertrag klarzustellen, dass die staatlichen Lotterieeinnehmer zwar datenschutzrechtlich verantwortliche Stellen im Sinne des § 3 Abs. 7 BDSG sind, ihnen aber gleichwohl in Bezug auf Datenschutz und Datensicherheit Vorgaben gemacht werden können. Klargestellt werden sollte auch, dass die staatlichen Lotterieeinnehmer der Aufsicht der für sie jeweils örtlich zuständigen Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich und die Anstalt der Aufsicht des Bayerischen Landesbeauftragten für den Datenschutz unterliegen.

6.3.3 Altersverifikation von Teilnehmern an Glücksspielen

Nach § 4 Abs. 3 des Glücksspielstaatsvertrags darf das Veranstalten und das Vermitteln von öffentlichen Glücksspielen den Erfordernissen des Jugendschutzes nicht zuwiderlaufen. Die Teilnahme Minderjähriger ist unzulässig. Die SKL als Glücksspielveranstalter sowie die staatlichen Lotterieeinnehmer haben daher sicherzustellen, dass Minderjährige von der Teilnahme ausgeschlossen sind. Die Glücksspielaufsicht hat ihre im Jahr 2008 erteilte Lotteriegenehmigung für die SKL mit der Auflage verbunden, sich bei jedem Spielteilnehmer zu vergewissern, dass dieser mindestens 18 Jahre alt ist. Dies kann in der Weise geschehen, dass man sich vom Spielteilnehmer einen Personalausweis vorlegen lässt. Denkbar sind aber auch andere geeignete Verifikationsverfahren, zu denen ein bestimmtes Verfahren einer Auskunftei, das sogenannte Post-Ident-Verfahren, oder auch die Einholung einer Melderegisterauskunft gehören. Im Hinblick auf langjährige SKL-Kunden wurde dabei folgende Ausnahmeregelung getroffen: „Für Spielteilnehmer, die seit mehr als vier Jahren Inhaber von Losen bzw. Losanteilen der SKL sind, braucht beim Versand der Lose ein Volljährigkeitsnachweis nicht erbracht werden.“

Erfolgt die Altersverifikation in diesem Rahmen, ist nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG auch die damit verbundene Datenerhebung, -verarbeitung und -nutzung zulässig. Es ist nicht notwendig, vom Spielteilnehmer eine Einwilligung einzuholen.

Die Betroffenen sind allerdings bei der Datenerhebung nach § 4 Abs. 3 BDSG über die vorgesehene Datenerhebung, -verarbeitung und -nutzung zu informieren. Sie müssen daher auch über die vorgesehene Nutzung der erhobenen Daten zu einer Altersverifikation und darüber informiert werden, an wen gegebenenfalls welche Daten für welchen Zweck übermittelt werden. Dass dem Betroffenen solche Informationen zu geben sind, bevor sie den mit ihren Daten versehenen Teilnahmeantrag an einen Lotterieeinnehmer übersenden, musste die Aufsichtsbehörde einem Lotterieeinnehmer mitteilen, der diese Information dem Mitspieler erst nach Übersenden des Teilnahmeantrags gab. Der hierin liegende Verstoß gegen die Hinweispflicht führte jedoch nicht zur Unzulässigkeit der Altersverifikation.

Auch wenn die Durchführung einer Altersverifikation in bestimmten Fällen verbindlich vorgeschrieben ist, verbleiben einem Lotterieeinnehmer für die konkrete Durchführung dieses Verfahrens Spielräume. Diese sollten für eine möglichst datenschutzfreundliche Vorgehensweise genutzt werden:

Ein Verfahren zur Altersverifikation darf datenschutzrechtlich grundsätzlich nur dazu verwendet werden, um zu überprüfen, ob die vom Teilnehmer mitgeteilten Angaben zutreffend sind. Sofern die Angaben nicht mit gleichlautenden Angaben bei der die Verifikation durchführenden Stelle übereinstimmen, müsste diese daher zurückmelden, dass es keine Übereinstimmung gibt und somit die mitgeteilten Daten des Teilnehmers nicht bestätigt werden können. Das hat grundsätzlich zur Folge, dass der Betroffene nicht an dem Spiel teilnehmen kann. Sofern die mit der Altersverifikation beauftragte Stelle zum Teil abweichende Daten über die angefragte Person gespeichert hat, dürfen diese nicht ohne Weiteres durch den Lotterieeinnehmer erhoben oder diesem übermittelt werden. Der staatliche Lotterieeinnehmer ist allerdings nicht gehindert, die Altersverifikation anschließend auf anderem Weg durchzuführen. Will er dies, muss er wegen des Grundsatzes der Direkterhebung beim Betroffenen (§ 4 Abs. 2 Satz 1 BDSG) auf diesen zugehen und es diesem ermöglichen, den Nachweis selbst zu erbringen und hilfsweise das Altersverifikationsverfahren angeben, das nunmehr durchgeführt werden soll (§ 4 Abs. 3 BDSG). Allerdings darf der Unternehmer dieses Verfahren nur durchführen, wenn der Betroffene zu erkennen gibt, dass er noch immer am Glücksspiel teilnehmen möchte. Keinesfalls darf der staatliche Lotterieeinnehmer – wie geschehen – ein anderes Altersverifikationsverfahren durchführen, nachdem er dem Betroffenen zuvor mitgeteilt hatte, er werde am Spiel nicht teilnehmen können, wenn er nichts von sich hören lasse und der Betroffene darauf nicht reagiert hat.

Aufgrund einer Beschwerde hat die Aufsichtsbehörde geprüft, ob ein Lotterieeinnehmer, der eine Volljährigkeitsprüfung für eine Person vornahm, die in früheren Jahren vereinzelt SKL-Lose erworben hatte, damit gegen datenschutzrechtliche Vorschriften verstoßen hat. Da sich jedoch die erwähnte Ausnahmeregelung ihrem Wortlaut nach nur auf Spielteilnehmer bezieht, die bei Erhalt eines neuen Teilnahmeantrags seit mehr als vier Jahren SKL-Kunden sind, begegnete die Durchführung einer solchen Altersverifikation keinen Bedenken. Gleichwohl sprach sich die Aufsichtsbehörde gegenüber dem Lotterieeinnehmer dafür aus, zur Vermeidung nicht erforderlicher Verarbeitungsvorgänge personenbezogener Daten auch solche Kunden von einer Altersverifikation auszunehmen, die vereinzelt bereits vor mehr als vier Jahren Lose oder Losanteile der SKL gekauft haben, sofern bekannt ist, dass sie damals bereits die Altersgrenze überschritten hatten.

7 Gewerbe, Verkehr

7.1 Detekteien

Die Aufsichtsbehörde musste sich im Berichtszeitraum gleich mehrfach mit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch Detektive befassen. So waren Detektive beziehungsweise Mitarbeiter von Sicherheitsunternehmen an der (Video-)Überwachung von Mitarbeitern eines Discounters und bei der Anfertigung von Protokollen über jene (siehe dazu oben B 1.1) maßgeblich beteiligt. Zum Einsatz kamen Detektive auch bei der Überwachung von Arbeitnehmern außerhalb des Betriebs (siehe dazu oben B 1.4). In einem weiteren Fall ließ der Inhaber eines Unternehmens unliebsame Konkurrenten und sogar Staatsanwälte durch eine Detektei beobachten (siehe dazu unten Nr. 7.1.1).

Die Aufsichtsbehörde hat im Berichtszeitraum bei zwei Sicherheitsunternehmen einen Kontroll- und bei einem einen Informationsbesuch durchgeführt.

7.1.1 Beobachtung unliebsamer Konkurrenten und von Staatsanwälten durch eine Detektei

Ein Unternehmer beauftragte eine Detektei damit, Konkurrenten, zwei Staatsanwälte, die gegen ihn in einer Wirtschaftsstrafsache ein Ermittlungsverfahren führten, und einen von einer Behörde eingesetzten Sachverständigen „abzuklären“. Anlass dafür war die ständige Furcht des Unternehmers, Konkurrenten in seiner Branche würden ihn benachteiligen, ja sogar auf Ermittlungs- und Aufsichtsbehörden zu seinem Nachteil Einfluss nehmen. Zur Erfüllung dieses Auftrags beschaffte sich der Detektiv unter anderem unter nicht geklärten Umständen Kopien der Steuererklärungen der Betroffenen und ihrer Familienangehörigen und spionierte deren Eigentumsverhältnisse aus. Darüber erstattete er seinem Auftragge-

ber jeweils Bericht. Die Einkünfte des Sachverständigen, der früher in den Abrechnungsunterlagen des Unternehmers Mängel festgestellt hatte, will sich der Detektiv über einen Internetanbieter „außerhalb der EU“ beschafft haben. Er beobachtete den Sachverständigen und seine Ehefrau mehrere Tage in der Öffentlichkeit, fragte Nachbarn über die Familie aus und überwachte deren Hauseingang zunächst mittels eines Video-Wagens, später mit Hilfe eines dort postierten Detektivs. Auch erhob der Detektiv die Fahrzeugbewegungen des Sachverständigen über mehrere Tage hinweg durch den Einsatz eines satellitengestützten Navigationssystems. Darüber hinaus erschlich sich der Detektiv zumindest einmal eine Auskunft von einer Mitarbeiterin einer öffentlichen Einrichtung, wobei er sie durch Vorspiegeln eines Vorwands dazu bewegt hatte. Die Aufsichtsbehörde hat vorsorglich Strafantrag nach § 44 Abs. 2 BDSG gestellt.

Die Gewerbeordnung regelt lediglich die gewerbliche Betätigung von Detekteien, nicht aber die Befugnisse von Detektiven und die Mittel, die diese bei ihrer Arbeit einsetzen dürfen. Maßgeblich sind somit grundsätzlich die Vorschriften des Bundesdatenschutzgesetzes, vorausgesetzt, in der Detektei erfolgt die Datenverarbeitung mit Hilfe automatisierter Datenverarbeitungsanlagen oder nicht automatisierter Dateien. Ist dies nicht der Fall, findet das Datenschutzrecht keine Anwendung, sodass auch keine Kontrollkompetenz der Datenschutzaufsichtsbehörde besteht. Letzteres dürfte angesichts der Arbeitsweise vieler Detekteien teilweise der Fall sein.

Bei der Übernahme und der Durchführung eines Auftrags trifft den Detektiv die volle Verantwortung für die Rechtmäßigkeit seines Tuns, wenn er selbst bestimmt, wie er den ihm erteilten Auftrag durchführt und welche Mittel er dabei einsetzt. Er wird dann nicht lediglich als Datenverarbeiter im Auftrag nach § 11 BDSG tätig. Vielmehr ist er selbst als Daten verarbeitende Stelle im Sinne des Bundesdatenschutzgesetzes anzusehen. Dabei kann er sich nur dann auf ein berechtigtes Interesse im Sinne des § 28 Abs. 1 Satz 1 Nr. 2 BDSG berufen, wenn der Auftrag, den er übernimmt, gemessen an der Rechtsordnung billigenswert ist. Ein Detektiv ist daher verpflichtet, seinen Auftraggeber nach den Gründen für den ihm erteilten Auftrag zu fragen.

Im vorliegenden Fall verstieß das Vorgehen der Detektei gleich in mehrfacher Hinsicht gegen das geltende Datenschutzrecht. So kann sich der Detektiv schon deswegen nicht auf ein berechtigtes Interesse nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG berufen, weil keine der ausgespähten Personen, schon gar nicht deren Familienangehörige, seinem Auftraggeber einen nachvollziehbaren Anlass für die Ausforschung gegeben hatten. Im Gegenteil, wer sich Informationen über einen gegen ihn ermittelnden Staatsanwalt oder sonstige von einer Behörde Beauftragte beschafft, macht dies sicher nicht, um sich auf legalem Weg in dem jeweiligen Verfahren zu verteidigen. Die Voraussetzungen für den Einsatz technischer Mittel bei der Beobachtung waren ebenfalls nicht gegeben. Auch das Täuschen von Behördenangehörigen zur Erlangung einer Information, die dem Detektiv oder seinem Auftraggeber tatsächlich nicht zusteht, war unzulässig. Das gilt natürlich erst recht, wenn ein Detektiv Unterlagen beschafft, die dem Steuergeheimnis unterliegen.

7.1.2 Genügen die gewerberechtlichen Vorschriften?

Die Gewerbeordnung (GewO) trifft in § 34 a Regelungen für das „Bewachungsgewerbe“ und in § 38 unter anderem für „Detekteien“. Unter das Bewachungsgewerbe fallen alle Tätigkeiten, die dem Schutz von Personen und Sachen dienen, ohne dass der dabei eingesetzte Wachmann Ermittlungen vornimmt („Warenhausdetektiv“). Dagegen gehört es zum Berufsbild des Detektivs, Recherchen über Dritte durchzuführen und darüber seinem Auftraggeber zu berichten. Nach den Erfahrungen der Aufsichtsbehörde, die sie beispielsweise im Zusammenhang mit der Überwachung von Mitarbeitern eines Discounters machte, sind die Grenzen zwischen dem reinen Bewachungsgewerbe und der Detekteitätigkeit in der Praxis jedoch fließend. Gleichwohl sind die gesetzlichen Grundlagen für diese beiden Bereiche unterschiedlich ausgestaltet.

Nach § 34 a GewO bedarf die Ausübung eines Bewachungsgewerbes einer behördlichen Erlaubnis. Diese darf nur erteilt werden, wenn durch eine Bescheinigung der Industrie- und Handelskammer nachgewiesen wird, dass der Gewerbe-

treibende über die maßgeblichen Rechtsvorschriften unterrichtet ist. Bestandteil des Unterrichtungsverfahrens ist auch das Datenschutzrecht. Auch müssen Bewachungsunternehmen über jeden Auftrag Aufzeichnungen anfertigen und für eine bestimmte Zeit aufbewahren. Darüber hinaus gelten nach § 8 der Bewachungsverordnung eine ganze Reihe von Vorschriften des Bundesdatenschutzgesetzes für das Bewachungsgewerbe selbst dann, wenn die Datenverarbeitung weder unter Einsatz von automatisierten Datenverarbeitungsanlagen noch mit Hilfe nicht automatisierter Dateien erfolgt.

Ganz anders sind dagegen die Rechtsgrundlagen für das Detekteigewerbe. Hier hat die zuständige Behörde lediglich die Zuverlässigkeit des Gewerbetreibenden nach § 38 Abs. 1 GewO zu prüfen, wenn dieser eine Detektei gewerblich anmeldet. Eine Unterrichtung der Gewerbetreibenden im Datenschutzrecht ist nicht vorgesehen. Eine Aufzeichnungspflicht für die übernommenen Ermittlungsaufträge könnte zwar durch Rechtsverordnung eingeführt werden, fehlt bislang jedoch. Eine § 8 der Bewachungsverordnung vergleichbare Regelung gibt es ebenfalls nicht.

Die Aufsichtsbehörde will sich kein Urteil darüber anmaßen, ob die im Gewerberecht bestehende Differenzierung zwischen Bewachungsgewerbe und Detekteien heutzutage noch sachgerecht ist. Wünschenswert wäre jedoch, dass

- das Gewerberecht vorsieht, dass sowohl die Leitung und die Mitarbeiter von Bewachungsunternehmen als auch von Detekteien über Kenntnisse des Datenschutzrechts verfügen;
- auch Detekteien rechtlich verpflichtet sind, Aufzeichnungen über die Durchführung ihrer Aufträge zu fertigen;
- für Detekteien eine § 8 der Bewachungsverordnung vergleichbare Regelung geschaffen wird. Detekteien müssen, da ihre Tätigkeit unter Umständen in erheblichem Maße in die Persönlichkeitsrechte der Betroffenen eingreift, auch dann Datenschutzvorschriften einhalten und der Datenschutzkontrolle unterliegen, wenn das Bundesdatenschutzgesetz nicht unmittelbar anwendbar ist.

7.2 Speicherung in der Schwarzfahrerdatei trotz Fahrscheins?

Unerwartete Folgen hatte eine Fahrt mit der Straßenbahn für einen Beschwerdeführer. Nach einer Radtour hatte er sein Fahrrad mit in die Straßenbahn genommen. Bei einer Fahrscheinkontrolle führte dies zu Problemen, obwohl er einen gültigen Fahrschein vorweisen konnte. Zwar dürfen nach den Beförderungsbedingungen dieses Verkehrsunternehmens Fahrräder grundsätzlich (kostenlos) mitgenommen werden. Doch gilt dies nicht während der Hauptverkehrszeiten am Vor- und am Nachmittag (Sperrzeit). Dies war dem Beschwerdeführer nicht bekannt. Er hatte sein Fahrrad während der Sperrzeit mitgenommen. Der Kontrolleur stellte deshalb die Personalien des Betroffenen fest und forderte ihn auf, die Straßenbahn an der nächsten Haltestelle zu verlassen. Das Verkehrsunternehmen sah in der unerlaubten Mitnahme des Fahrrads ein „Fahren ohne gültigen Fahrausweis“ und erhob von dem Betroffenen ein erhöhtes Beförderungsentgelt von 40 Euro. Außerdem wurden die Personalien des Reisenden in der Schwarzfahrerdatei erfasst. Hiergegen wehrte er sich.

Er hatte Recht: Die Fahrradmitnahme während der Sperrzeiten kann nur als Verstoß gegen die Beförderungsbedingungen, nicht aber als Fahren ohne gültigen Fahrausweis gewertet werden, da bei dem Verkehrsunternehmen die Mitnahme von Fahrrädern (unentgeltlich) möglich ist – nur eben nicht zu bestimmten Zeiten. Auch das Lösen eines Fahrscheins für das Fahrrad hätte ihm hier nicht geholfen. Der Beschwerdeführer war daher nicht „schwarz“ gefahren. Von ihm durfte weder ein „erhöhtes Beförderungsentgelt“ verlangt noch durfte er in der Schwarzfahrerdatei gespeichert werden. Das Verkehrsunternehmen sah dies nach einer eingehenden Erörterung der Rechtslage ein und löschte die Daten des Beschwerdeführers in der Schwarzfahrerdatei. Darüber hinaus hat das Verkehrsunternehmen seine Bestimmungen wie folgt geändert:

- Die Fahrausweiskontrolleure werden eine Person, die während der Sperrzeit ein Fahrrad in einer Straßenbahn befördert, künftig als „Vertragsverletzer“ und nicht als Schwarzfahrer erfassen.

– Von einem „Vertragsverletzer“ wird kein „erhöhtes Beförderungsentgelt“, sondern beim ersten Verstoß eine Vertragsstrafe in Höhe von 10 Euro erhoben. Die Daten des Vertragsverletzers werden für sechs Monate in einer gesonderten Datei gespeichert und dann gelöscht.
– Nur wenn während der Speicherfrist ein zweiter Verstoß erfolgt, beträgt die Vertragsstrafe 40 Euro. Die Daten werden dann ein Jahr gespeichert.

8 Vermieter, Mieter, Wohnungseigentümer

8.1 Datenerhebung und -übermittlung zur Erstellung eines Energieausweises

Nach der geltenden Energieeinsparverordnung sind Hausbesitzer oder Wohnungseigentümer bei der Vermietung von Wohnungen verpflichtet, den Mietinteressenten einen Energieausweis vorzulegen. Dieser kann entweder aufgrund des tatsächlichen Energieverbrauchs des Gebäudes oder aber aufgrund einer Bedarfsberechnung erstellt werden.

Weder das Energieeinspargesetz noch die Energieeinsparverordnung enthalten besondere Vorschriften, die die Erhebung und Übermittlung personenbezogener Verbrauchsdaten zur Erstellung eines Energieausweises auf der Basis des tatsächlichen Energieverbrauchs des Gebäudes regeln. Maßgeblich sind daher die Vorschriften des Bundesdatenschutzgesetzes. Die Datenschutzaufsichtsbehörden beurteilen die Rechtslage übereinstimmend wie folgt:

– Der Wohnungseigentümer ist grundsätzlich berechtigt, die Verbrauchsdaten zur Erstellung eines Energieausweises beim Mieter zu erheben.
– Mit – in der Regel schriftlicher – Einwilligung der betroffenen Mieter darf der Eigentümer die Verbrauchsdaten auch beim Energieversorgungsunternehmen (EVU) des Mieters erheben, dieses darf die Angaben an den Eigentümer übermitteln. Nach § 4 a Abs. 1 BDSG müssen die Mieter zuvor umfassend darüber informiert werden, welche Daten für welchen Zweck erhoben und wie verarbeitet werden.
– Ohne Einwilligung der betroffenen Mieter darf das EVU bei Mehrfamilienhäusern mit mindestens drei Wohnungen zusammengefasste Daten, nämlich den Gesamtenergieverbrauch der Mieter des Gebäudes, an den Eigentümer übermitteln. In diesem Fall kann nicht mehr von einem Personenbezug der übermittelten Daten im Sinne des Bundesdatenschutzgesetzes ausgegangen werden.

Das Bundesministerium für Verkehr, Bau- und Stadtentwicklung hat darauf hingewiesen, dass Eigentümer und Vermieter für den Fall, dass ein Energieausweis auf Verbrauchsgrundlage im Einzelfall nicht in Betracht kommt, über eine kostengünstige Alternative verfügen. Nach den Regelungen der neuen Energieeinsparverordnung kann ein Bedarfsausweis in einem stark vereinfachten Verfahren ausgestellt werden. Nähere Hinweise hierzu finden sich im Internetangebot des Bundesamts für Bauwesen und Raumordnung *(www.bbr.bund.de)*.

8.2 Bekanntgabe von Mieterdaten an eventuelle Nachmieter

Bei der Aufsichtsbehörde gehen immer wieder Beschwerden darüber ein, dass ein Vermieter nach Kündigung des Mietvertrags Name und Telefonnummer(n) des bisherigen Mieters an Mietinteressenten übermittelt hat. Letztere haben die Daten dann dazu genutzt, mit dem Wohnungsinhaber telefonisch einen Besichtigungstermin zu vereinbaren.

Wir haben in diesen Fällen die Vermieter darauf hingewiesen, dass eine solche Datenübermittlung nur mit Einwilligung der Betroffenen, also der bisherigen Mieter, zulässig ist.

9 Gesundheit

9.1 Telematik im Gesundheitswesen

Im Gesundheitsbereich sollen die bislang durch den Umgang mit Papierunterlagen geprägten Abläufe Zug um Zug durch elektronische Vorgänge abgelöst werden. Dabei soll die elektronische Gesundheitskarte eine ganz entscheidende Rolle spielen (siehe dazu nachfolgend Nr. 9.1.1). Während deren flächendeckende Ausgabe und Nutzung jedoch nach wie vor auf sich warten lässt, bieten Unternehmen im Internet bereits elektronische Gesundheitsakten an, die ohne solche Karten nutzbar sind (siehe dazu unten Nr. 9.1.2).

9.1.1 Elektronische Gesundheitskarte

Mit dem am 1. Januar 2004 in Kraft getretenen Gesetz zur Modernisierung der gesetzlichen Krankenversicherung hat der Bundesgesetzgeber beschlossen, dass die Krankenversichertenkarte „bis spätestens zum 1. Januar 2006“ zu einer elektronischen Gesundheitskarte erweitert wird. Obwohl dieser Stichtag inzwischen dreieinhalb Jahre zurückliegt, hat die flächendeckende Einführung der elektronischen Gesundheitskarte in Baden-Württemberg noch nicht einmal begonnen. Derzeit ist nicht absehbar, bis wann alle baden-württembergischen Versicherten der gesetzlichen Krankenversicherung ihre erste elektronische Gesundheitskarte erhalten haben werden.

In einem ersten Schritt soll die elektronische Gesundheitskarte folgende Funktionen bieten:

- Die elektronische Gesundheitskarte soll es, wie bislang schon die Krankenversichertenkarte, den Arztpraxen ermöglichen, die Versichertenstammdaten wie Name und Anschrift des Versicherten elektronisch in ihre Praxis-EDV übernehmen zu können.
- Des Weiteren soll die elektronische Gesundheitskarte zur Speicherung *elektronischer Rezepte* genutzt werden. Um ein Rezept einzulösen, legt der Patient seine elektronische Gesundheitskarte mit den darauf gespeicherten Rezepten in einer Apotheke vor.
- Darüber hinaus soll die elektronische Gesundheitskarte dazu genutzt werden, medizinische Daten, die für eine Notfallbehandlung von Bedeutung sein können, darauf zu speichern, wenn und soweit die Patienten dies wünschen.

Auch wenn bislang nicht einmal die Tests für diese ersten Funktionen abgeschlossen sind, gibt es bereits Pläne für eine Reihe weiterer freiwilliger Anwendungen, deren gesetzliche Grundlage sich ebenfalls in § 291 a Abs. 3 des Fünften Buches Sozialgesetzbuch (SGB V) findet. Dabei sollen mit Hilfe der Karten im Rahmen eines *Arzneimittelmanagements* unerwünschte Wechselwirkungen von Medikamenten erkannt, ein elektronischer *Arztbrief* sowie eine in ärztlicher Verantwortung geführte *elektronische Patientenakte* ermöglicht und letztlich auch dem Versicherten selbst zahlreiche ihn betreffende medizinische Daten in einer elektronischen Ablage bereitgestellt werden *(„Patientenfachdatenmanagement“)*.

Sofern einmal alle diese weit reichenden Anwendungen realisiert werden, kommt der elektronischen Gesundheitskarte die Rolle eines Schlüssels zu, der den Zugriff auf zahlreiche, besonders sensible Gesundheitsdaten der Versicherten ermöglichen soll. Dabei werden die Daten nicht zwangsläufig alle auf den elektronischen Gesundheitskarten selbst gespeichert sein, sondern zum Teil auch auf anderen Computersystemen. Angesichts des Umfangs dieses Vorhabens, der dabei zu errichtenden vernetzten Datenverarbeitungs-Infrastruktur (sogenannte Telematik-Infrastruktur), den daran mitwirkenden zahlreichen Beteiligten sowie der Sensibilität der gespeicherten, verarbeiteten und genutzten personenbezogenen Daten ist es unverzichtbar, eine umfassende projektbezogene Datenschutz- und Sicherheitskonzeption zu erstellen und umzusetzen. Die vom Bundesgesundheitsministerium hiermit beauftragte Gematik mbH hat hierzu bereits eine Reihe von Konzeptionen erarbeitet. Nur beispielhaft sei dafür das übergreifende Datenschutzkonzept der Gesundheitstelematik erwähnt. Dieses beruht unter anderem auf folgenden Eckpunkten:

– Vorrang des Datenschutzes

  Die Infrastruktur in der Telematik muss sich vorrangig am Nutzen für den Patienten ausrichten und an erster Stelle den Erfordernissen des Datenschutzes und der Datensicherheit entsprechen. Eine nicht rechtskonforme Nutzung der Infrastruktur der Telematik muss technisch unterbunden werden.

– Datenschutzfördernde Techniken

  Versicherte müssen durch datenschutzfördernde Technik in die Lage versetzt werden, ihre Betroffenenrechte und den Selbstdatenschutz wahrzunehmen und innerhalb des gesetzlichen Rahmens selbst aktiv über die Verarbeitung ihrer Daten und jeglicher Weitergabe zu bestimmen.

Weitere wesentliche Anliegen sind, die Freiwilligkeit der Nutzung sowie die Datenhoheit des Versicherten zu sichern und Transparenz für die Versicherten zu schaffen. Um die Herausbildung von „Personenkennzeichen“ zu vermeiden, ist zudem vorgesehen, dass die Identifikationsmerkmale nicht außerhalb des Gesundheitswesens zum Einsatz kommen dürfen. Dabei ist anzuerkennen, dass diese Konzeptionen dem Datenschutz und der Datensicherheit eine erkennbar hohe Bedeutung beimessen.

Aktuell finden in sieben Bundesländern, darunter auch in Baden-Württemberg, sog. 10.000er-Tests statt. Bei dem baden-württembergischen Test in der Region Heilbronn haben mehr als 8.300 Versicherte auf freiwilliger Basis eine elektronische Gesundheitskarte erhalten und setzen diese ein, wenn sie eine der mehr als zehn teilnehmenden Arztpraxen aufsuchen oder dort verschriebene Medikamente in einer der teilnehmenden Apotheken abholen.

Im Rahmen dieser Tests sollen unter anderem auch die im Zusammenhang mit der Nutzung der elektronischen Gesundheitskarte vorgesehenen Datenschutz- und Sicherheitsmaßnahmen praktisch erprobt werden. Dem Abschlussbericht* der von der Hochschule Heilbronn zu diesem Vorhaben durchgeführten Begleitforschung ist unter anderem zu entnehmen, dass die dazu befragten Ärzte, Apotheker und andere Leistungserbringer erhebliche Zweifel daran haben, dass sich auch nach Ausgabe der elektronischen Gesundheitskarten Datenschutz und Datensicherheit der sensiblen Gesundheitsdaten wahren lassen. Beispielsweise befürchten

– 79 % der Befragten, dass die Gesetzeslage irgendwann geändert werden könnte und die gespeicherten Gesundheitsdaten dann für andere Dritte (beispielsweise Arbeitgeber, Lebensversicherung, Staat) zugänglich werden,
– 77 %, dass die Patienten es nicht alleine schaffen, ihre Gesundheitsdaten an einem Patientenkiosk zu lesen, zu löschen oder zu bearbeiten,
– 75 %, dass die Gesundheitsdaten auf den Servern nicht sicher sein werden,
– 74 %, dass die Gesundheitsdaten auf der elektronischen Gesundheitskarte nicht sicher sind,
– 74 %, dass die Patienten gläsern werden.

Von den am Testbetrieb teilnehmenden Ärzten wurde unter anderem auch Kritik an der an einigen Stellen für den Zugriff auf Gesundheitsdaten notwendigen Eingabe einer PIN-Nummer oder anderen zur Wahrung der Persönlichkeitsrechte vorgesehenen Arbeitsschritten und Nutzungsbedingungen geübt, da diese im täglichen Arbeitsablauf der Arztpraxis hinderlich sind. Für die Aufrechterhaltung des in den Datenschutzkonzepten beschriebenen Datenschutzniveaus wird es im weiteren Verlauf des Projekts entscheidend darauf ankommen, ob dem darin festgelegten Grundsatz des Vorrangs des Datenschutzes auch dann Rechnung getragen wird, wenn von Beteiligten dessen Einschränkung mit dem Hinweis auf Praktikabilitätsüberlegungen gefordert wird.

Auch wenn nach wie vor insbesondere von Seiten der Ärzteschaft immer wieder grundlegende Kritik an dem Vorhaben geäußert wurde, wurde in der sogenannten „Startregion“ Nordrhein inzwischen mit der durch finanzielle Anreize geförderten

* Hochschule Heilbronn, Abschlussbericht – Evaluation der Einführung der elektronischen Gesundheitskarten in der Testregion Heilbronn, Dezember 2008.

flächendeckenden Ausstattung von Arztpraxen mit Kartenlesegeräten begonnen. Dort hat sich mittlerweile etwa jede zehnte Arztpraxis ein Kartenlesegerät für die elektronische Gesundheitskarte angeschafft. Demnächst sollen auch die Versicherten in dieser Region von ihrer Krankenversicherung eine elektronische Gesundheitskarte erhalten.

9.1.2 Elektronische Gesundheitsakten

Während derzeit noch nicht absehbar ist, wann elektronische Patientenakten sowie das Patientenfachdatenmanagement mit Hilfe der elektronischen Gesundheitskarte nutzbar sein werden, bieten verschiedene Unternehmen inzwischen im Internet Dienstleistungen an, die bereits heute ähnliche Funktionen bieten sollen.

Die Anbieter stellen mit Diensten, die sich in der Regel unmittelbar an Versicherte richten, elektronische Ablagen zur Verfügung, in denen die Versicherten gesundheitsbezogene Informationen aufbewahren können, wie sie dies früher mit Papierunterlagen in einem klassischen DIN-A4-Ordner getan haben. Da die Versicherten auch Ärzten oder anderen Leistungserbringern einen Zugriff auf diese Ablagen gestatten können, können darin letztlich sowohl Informationen von Ärzten oder anderen Leistungserbringern als auch von den Versicherten selbst eingegebene personenbezogene Gesundheitsdaten enthalten sein. Zudem bieten diese Angebote Funktionen wie beispielsweise eine Unverträglichkeitsüberprüfung für die in der Ablage genannten Medikamente oder eine Erinnerungsfunktion für Impfungen oder Vorsorgeuntersuchungen. Auch wenn diese Angebote nur auf freiwilliger Basis in Anspruch genommen werden können, sind zahlreiche Maßnahmen zu ergreifen, um den Datenschutz beim Umgang mit diesen Diensten zu gewährleisten.

Ein baden-württembergisches Unternehmen, das sein Produkt unter anderem auch Versicherten einer baden-württembergischen gesetzlichen Krankenversicherung anbietet, ließ sich von der Aufsichtsbehörde beraten, welche datenschutzrechtlichen Aspekte es berücksichtigen muss. Die Aufsichtsbehörde nannte folgende Leitlinien:

– Einsatzkonzept präzisieren

  Während die Einführung der elektronischen Gesundheitskarte durch umfangreiche gesetzliche Regelungen flankiert wird, gibt es solche gesetzlichen „Leitplanken“ für die Angebote bislang nicht. § 68 SGB V regelt lediglich, dass die gesetzlichen Krankenkassen ihren Versicherten „zur Verbesserung der Qualität und der Wirtschaftlichkeit der Versorgung“ eine finanzielle Unterstützung für die Nutzung einer „persönlichen elektronischen Gesundheitsakte“ gewähren dürfen. Weitgehend unbeantwortet bleibt jedoch die Frage, welchen Zwecken diese Angebote im Einzelnen dienen sollen. Ohne klare Nutzungskonzeption laufen derartige Angebote jedoch Gefahr, zu einer unstrukturierten und unsystematischen Datensammlung zu werden. Um sicherzustellen, dass in einem solchen Angebot jeweils nur diejenigen personenbezogenen Daten gespeichert werden, die für deren geplante Nutzung notwendig sind, muss zunächst präzisiert werden, für welche Zwecke die Angebote genutzt werden sollen.

– Sicherheitskonzeption erstellen

  Auch wenn es aufgrund der Unbestimmtheit des Nutzungskonzepts schwer fallen mag, muss für die persönliche elektronische Gesundheitsakte ein umfassendes Sicherheitskonzept erstellt und umgesetzt werden. Bei Angeboten, die sich unmittelbar an Versicherte wenden, müssen diese vor Beginn der Nutzung umfassend und verständlich darüber informiert werden, welche Daten in dem System verarbeitet werden und auf welche Weise der Anbieter dabei den notwendigen Schutz der personenbezogenen Daten gewährleistet.

  Was die datenschutzrechtliche Ausgestaltung einzelner Funktionen der elektronischen Gesundheitsakte angeht, die denen der elektronischen Gesundheitskarte, insbesondere dem Arzneimittelmanagement oder dem Patientenfachdatenmanagement entsprechen, empfiehlt es sich, die Schutzmaßnahmen an den gesetzlichen Anforderungen für die jeweilige Anwendung der elektronischen Gesundheitskarte zu orientieren (Äquivalenzprinzip).

– Klare Vertragsverhältnisse zwischen Versicherten und Anbietern, Krankenkassen und weiteren Beteiligten schaffen

  Für die Nutzung freiwilliger Angebote, mit denen sich Internetdiensteanbieter an Versicherte wenden, bedarf es einer Vereinbarung über Art und Umfang des Angebots sowie die dabei vom Anbieter durchzuführenden Datenverarbeitungsvorgänge. Damit die Versicherten die datenschutzrechtlichen Risiken eines solchen Angebots abschätzen können, müssen sie zuvor eingehend, umfassend und allgemein verständlich über alle dafür wesentlichen Aspekte des Angebots aufgeklärt werden. Ihre Einwilligung in die Verarbeitung und Nutzung ihrer Daten müssen sie in Kenntnis dieser Informationen erteilen. Zusätzliche Anforderungen an die Aufklärung der Betroffenen sowie an die Inhalte der für das Vorhaben vorgesehenen Einwilligungserklärungen ergeben sich dabei stets, wenn weitere Beteiligte wie Krankenversicherungen oder Forschungseinrichtungen an dem Angebot oder dessen Umsetzung beteiligt sind.

  • Finanzielle Beteiligung einer Krankenversicherung an den Kosten des Angebots

    Die Mitwirkung einer Krankenversicherung an einem solchen Angebot kann sich insbesondere dadurch ergeben, dass diese – so wie es § 68 SGB V zulässt – ihren Versicherten einen finanziellen Zuschuss gewährt, wenn diese sich von einem entsprechenden Anbieter eine elektronische Gesundheitsakte einrichten lassen. Sofern dabei zwischen dem Anbieter der elektronischen Gesundheitsakte und der den Zuschuss gewährenden Krankenkasse ein Datenaustausch vorgesehen ist, ist bei der Unterrichtung der Betroffenen sowie der Abfassung der Einwilligungsklauseln ergänzend darauf zu achten, dass die Versicherten deutlich über diesen Datenaustausch informiert werden und auch hierzu ihre ausdrückliche Einwilligung eingeholt wird. Zudem ist ein hierfür vorgesehener Datenaustausch so zu gestalten, dass dabei nur im notwendigen Umfang personenbezogene Daten ausgetauscht werden.

  • Datenschutzrechtliche Verantwortlichkeit klarstellen

    Eine Krankenversicherung, die die Nutzung eines solchen Angebots finanziell fördert, wird ihre Versicherten in der Regel auch über dieses Angebot unterrichten. Insbesondere, wenn dies im Internetangebot der Krankenversicherung geschieht, können die daran interessierten Versicherten aus dem Internetangebot der Krankenversicherung nahtlos auf die Internetseite des Anbieters übergeleitet werden. Datenschutzrechtlich ist dabei darauf zu achten, dass die Nutzer klar erkennen, wie lange sie sich (noch) auf den Internetseiten der Krankenversicherung befinden und wann sie das Internetangebot des Anbieters der elektronischen Gesundheitsakte nutzen. Dies ist schon deshalb erforderlich, damit ein Nutzer jeweils beispielsweise zuordnen kann, gegenüber welcher Stelle er personenbezogene Daten offenbart, wenn er die im Internetangebot enthaltenen Formulare ausfüllt. Eine klare Trennung dieser Angebote ist auch deshalb geboten, damit den Nutzern klar wird, dass es sich bei der angebotenen Dienstleistung nicht um ein Angebot der Krankenversicherung handelt und diese auch nicht für die Einhaltung des Datenschutzes bei der Nutzung dieses Angebots verantwortlich ist.

  • Rolle weiterer Beteiligter wie beispielsweise der Forschungsinstitute klarstellen

    Aufgrund der Neuartigkeit der Angebote sind Anbieter wie auch die zur Finanzierung beitragenden Krankenversicherungen mitunter daran interessiert, die Art und Weise der tatsächlichen Nutzung eines solches Angebots im Rahmen eines Forschungsprojekts untersuchen zu lassen. Dabei kann es beispielsweise durch Befragung der Nutzer oder auch durch Auswertung der in den Datenverarbeitungsanlagen anfallenden Nutzungsdaten darum gehen, hierzu geeignete Informationen zu erlangen und auszuwerten. Sofern daran gedacht ist, ein Angebot für eine elektronische Gesundheitsakte mit einem Forschungsvorhaben zu verbinden und dazu ergänzend personenbezogene Daten zu verarbeiten, sind die Betroffenen auch hierüber zu unterrichten. Eine entsprechende Datenverarbeitung darf dabei nur erfolgen, wenn der Nutzer der elektronischen Gesundheitsakte auch hierzu seine Einwilligung erteilt hat.

- Über fehlenden Beschlagnahmeschutz aufklären

  Medizinische Unterlagen in einer Arztpraxis oder einem Krankenhaus sind – so sieht es die Strafprozessordnung vor – vor einer Beschlagnahme geschützt. Im Zuge der Einführung der elektronischen Gesundheitskarte wurde dabei ausdrücklich klargestellt, dass sich dieser Schutz auch auf die elektronischen Gesundheitskarten erstreckt. Demgegenüber unterliegen auch besonders schutzbedürftige Gesundheitsdaten, wenn sie auf dem von einem Internetdiensteanbieter betriebenen Computersystem gespeichert sind, keinem vergleichbaren Beschlagnahmeschutz. Die Anbieter der elektronischen Gesundheitsakte müssen die Interessenten vor Einholung der Einwilligung zur Verarbeitung ihrer personenbezogenen Daten hierüber unterrichten.

9.2 Externe Digitalisierung, Verfilmung und Vernichtung von Patientenakten

Ende 2008 berichteten Medien darüber, aus einem baden-württembergischen Klinikum stammende Patientenakten seien in einer ehemaligen Messehalle der Alten Messe Leipzig gefunden und zum Teil fotografiert worden. Einzelne dieser Aufnahmen sollen auch im Internet veröffentlicht worden sein. Die von der Aufsichtsbehörde daraufhin bei dem Klinikum durchgeführte Überprüfung ergab Folgendes:

Das Konzept des Klinikums sah vor, dass die in Papierform geführten Patientenakten mikroverfilmt, digitalisiert und anschließend vernichtet werden. Hierzu beauftragte das Klinikum mehrere Unternehmen unter anderem mit der Abholung, der (Zwischen-)Lagerung, der Digitalisierung, der Mikroverfilmung und der anschließenden Vernichtung von Patientenakten. Weitere Aufträge erstreckten sich auf die Indexierung und die elektronische Übertragung der digitalisierten Patientenakten sowie die externe Archivierung der Mikrofilme.

Seit Beginn der externen Digitalisierung im Jahr 2006 wurden regelmäßig Patientenakten vom Klinikum zu dem damit beauftragten Unternehmen transportiert, obwohl dort bei der Verarbeitung der Unterlagen Mängel aufgetreten waren, die dazu führten, dass die Leistungen des Auftragnehmers vom Klinikum nicht abgenommen wurden. So lange sind auch die davon betroffenen Patientenakten nicht vernichtet worden. Während der Nachbearbeitung der unzulänglich bearbeiteten Patientenakten wurden vom Klinikum regelmäßig weitere Akten angeliefert, sodass beim Auftragnehmer ein „Rückstau“ von ca. 100.000 Patientenakten entstand. Das Unternehmen war schließlich nicht mehr in der Lage, die Patientenakten ausschließlich in eigenen Räumen aufzubewahren. Es mietete daher für die Zwischenlagerung der Patientenakten Räume in der erwähnten Messehalle an. Dort war der Lagerbereich nur durch einen Zaun mit Sichtschutz von den übrigen, für andere Zwecke genutzten Räumlichkeiten der Messehalle abgetrennt. Es gelang Unbefugten, in den Lagerbereich einzudringen und Einblick in die Patientenakten zu nehmen.

Da das für die Lagerung verantwortliche Unternehmen nicht der Aufsicht durch die baden-württembergische Aufsichtsbehörde unterliegt, konzentrierte sich die von der Aufsichtsbehörde durchgeführte Überprüfung im Folgenden darauf, ob das Klinikum bei den von ihm erteilten Aufträgen alle datenschutzrelevanten Anforderungen berücksichtigt hat.

Nach § 11 Abs. 2 BDSG muss der Auftraggeber den Auftragnehmer unter anderem schriftlich beauftragen, wobei die Datenerhebung, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse schriftlich festzulegen sind. Gemessen an diesen Anforderungen wiesen die vor dem Zwischenfall erteilten Aufträge des Klinikums erhebliche datenschutzrechtliche Mängel auf:

– Unvollständig war beispielsweise die Kette der Auftrags- und Unterauftragsverhältnisse. So hatte das Klinikum einen Auftrag an ein zu einer Unternehmensgruppe gehörendes Unternehmen erteilt, die Ausführung dieses Auftrags erfolgte jedoch zumindest teilweise auch durch ein anderes Unternehmen dieser Unternehmensgruppe, mit dem hierüber keine schriftlichen Vereinbarungen getroffen wurden. Da beide Unternehmen rechtlich selbstständig waren, hätte das Klinikum entweder mit beiden einen Vertrag schließen müssen oder das

eine Unternehmen hätte mit dem anderen einen Unterauftrag abschließen müssen.

– Auch soweit Aufträge zur Verarbeitung personenbezogener Daten vorgelegt wurden, wurden diese den Anforderungen des § 11 Abs. 2 BDSG nicht gerecht. Teilweise fehlten Regelungen gänzlich, beispielsweise zur (Zwischen-)Lagerung der Patientenakten, teilweise waren sie unzulänglich. Dies galt beispielsweise für die Vereinbarungen zur Abholung, zum Transport und zur Vernichtung von Patientenakten sowie zur Verarbeitung der Indexdaten und zur Aufbewahrung der Mikrofilme:

  • Hinsichtlich des Aktentransports waren die Modalitäten der Übergabe der Patientenakten und deren Dokumentation, die Art der zu verwendenden Transportbehälter und die beim Transport einzuhaltenden Zugriffsschutzmaßnahmen unzureichend geregelt. Zu ungenau waren auch die Vereinbarungen über den Aufbewahrungsort und die Maßnahmen, die dort zum Schutz vor unberechtigtem Zugriff auf die Akten zu treffen waren.

  • Hinsichtlich der automatisierten Verarbeitung von Indexdaten, die auch Patientendaten (zum Beispiel Namen) umfassen, war nicht festgelegt, auf welchen Computern diese Indexdaten verarbeitet werden dürfen und wer diese betreibt, wie dabei die Zugriffsberechtigungen zu gestalten sind, wodurch ein unberechtigter Zugriff etwa aus dem Internet auf die digitalisierten Patientenakten verhindert wird oder welche Anforderungen für den Umgang mit mobilen Datenträgern gelten.

  • Auch gab es keine Vereinbarungen zur Gewährleistung von Datenschutz und Datensicherheit bei der elektronischen Übertragung der digitalisierten Daten.

  • Schließlich fehlten auch Regelungen über die Art und Weise der Aktenvernichtung.

Trotz dieser Mängel war für den Vorfall in Leipzig in erster Linie der Auftragnehmer verantwortlich, der die Patientenakten dorthin verbracht und nicht für einen ausreichenden Zugriffsschutz gesorgt hat. Allerdings haben zwei dem Klinikum anzulastende Mängel mit dazu beigetragen, dass die Unterlagen letztlich in die Messehalle ausgelagert wurden:

– zum einen das Fehlen hinreichend konkreter Festlegungen, wo die Patientenakten bis zu ihrer Vernichtung aufzubewahren sind und

– zum anderen die nicht ausreichende Kontrolle des für das Digitalisieren verantwortlichen Auftragnehmers durch den Auftraggeber. Wäre der Auftraggeber seiner Verpflichtung zur regelmäßigen Kontrolle des Auftragnehmers auf Einhaltung des Datenschutzes (§ 11 Abs. 2 Satz 4 BDSG) nachgekommen, hätte er festgestellt, dass die Übergabe weiterer Patientenakten so lange ausgesetzt werden muss, bis die zuvor angelieferten Patientenakten korrekt digitalisiert sind. Auf diese Weise wäre der Rückstau der Patientenakten, der letztlich zu deren Auslagerung führte, vermieden worden.

Alles in allem hat das Klinikum in erheblichem Maße gegen § 11 in Verbindung mit § 9 BDSG verstoßen. Die Aufsichtsbehörde hat daher eine Beanstandung gegenüber dem Klinikum ausgesprochen. Dieses hat die Mängel eingeräumt. Es hat sich nach dem Vorfall unter anderem durch einen Kontrollbesuch vor Ort über die vom Auftragnehmer veranlassten Änderungen informiert und einen neuen Vertrag mit einem Auftragnehmer abgeschlossen, der nach seiner Mitteilung „jeden einzelnen Prozessschritt von der Abholung über die Digitalisierung bis zur Archivierung/Vernichtung dokumentiert und die Handhabung aus datenschutzrechtlicher Hinsicht detailliert beschreibt“. Die Überprüfung des der Aufsichtsbehörde übersandten Vertragswerks ist bislang noch nicht abgeschlossen.

9.3 Datenweitergabe beim Wechsel des Pflegepersonals im Krankenhaus

Eine Arbeitsanweisung eines Krankenhauses sah vor, dass die Pflegekräfte bei „Übergabe“ der Patienten an die nachfolgende Schicht Angelegenheiten, die nicht

im Patientenzimmer angesprochen werden können, beispielsweise Diagnosen oder Prognosen, die den Patienten noch nicht bekannt sind, auf dem Flur zu besprechen sind. Selbst wenn Pflegekräfte bei der Durchführung solcher Gespräche im Allgemeinen darauf achten, dass keine Unberechtigten mithören können, besteht ein Risiko, dass dies im Einzelfall doch möglich ist. Damit hat das Krankenhaus keine ausreichenden organisatorischen Datenschutzmaßnahmen (§ 9 BDSG) getroffen.

Nachdem wir das Krankenhaus darauf aufmerksam gemacht hatten, hat es das Verfahren der „Patientenübergabe“ so geändert, dass die Übergabegespräche entweder im Patientenzimmer oder im Stationszimmer erfolgen.

9.4 Löschung von Patientendaten nach unzulässiger Übermittlung an externe Abrechnungsstellen

Die Übermittlung von Behandlungsdaten der Patienten an eine externe Abrechnungsstelle ist nur mit Einwilligung der Betroffenen zulässig (siehe dazu dritter Tätigkeitsbericht C 6.6, S. 66 ff.).

Auch im Berichtszeitraum erreichten uns wieder Beschwerden von Patienten, die eine Rechnung für die Arztbehandlung von einer externen Abrechnungsstelle erhalten haben, obwohl sie in die Datenübermittlung an eine solche Abrechnungsstelle nicht eingewilligt hatten. Eine Arztpraxis sorgte, nachdem auch sie versehentlich rechtswidrig Daten eines Patienten übermittelt hatte, für eine Änderung der von ihr genutzten Arztpraxissoftware. Jetzt werden nur noch Daten derjenigen Patienten an die Abrechnungsstelle übertragen, die eine ausdrückliche „Freigabe“ für die Datenübermittlung erteilt haben. Umgekehrt ist es bei der üblicherweise verwendeten Arztpraxissoftware: Darin müssen die Daten derjenigen Patienten markiert werden, die mit einer Übermittlung nicht einverstanden sind. Die neue Lösung hat den Vorteil, dass eine versehentlich vergessene Markierung nicht zu einer unzulässigen Datenübermittlung führt. Wir halten dieses Vorgehen für beispielhaft, weil die Arztpraxis sich nicht damit begnügt hatte, Anweisungen an die Mitarbeiter zu erlassen, um in Zukunft unbefugte Datenübermittlungen zu verhindern.

10 Internet

10.1 „Mitmach-Web“

Seitdem das Internet nicht mehr nur von Hochschulen und Unternehmen, sondern auch von Privatpersonen genutzt wird, nehmen neuartige Dienstleistungen und Kommunikationsformen im Netz zu. Man spricht bei diesen Diensten vom Web 2.0 oder auch vom „Mitmach-Web“. Typisch dafür sind etwa „Soziale Netzwerke“, an denen Personen teilnehmen, die sich mehr oder weniger umfassend selbst darstellen und mit anderen Teilnehmern in Kontakt treten. Zum Teil richten sich diese an bestimmte Zielgruppen, wie Studierende oder Schüler, zum Teil sind diese für „Jedermann“ offen. Weitere Angebote dieser Art sind Bewertungsportale sowie Dienste, über die beispielsweise Videos oder Fotos veröffentlicht werden können.

Ein wesentliches Merkmal dieser Dienste ist, dass daran teilnehmende Privatpersonen nicht mehr nur wie bei anderen Massenmedien von anderen bereitgestellte Inhalte konsumieren, sondern zugleich selbst zu Anbietern vielfältiger, nicht selten auch personenbezogener Inhalte werden. Damit sind die Angebote auch datenschutzrelevant. Im Folgenden sollen beispielhaft hierfür die sozialen Netzwerke (siehe dazu unten Nr. 10.1.1) und die Bewertungsportale (siehe dazu unten Nr. 10.1.2) angesprochen werden.

10.1.1 Soziale Netzwerke

Die vielfach jugendlichen oder studentischen Nutzer verwenden diese Angebote für die Alltagskommunikation. Die darin ausgetauschten Mitteilungen sind für die Kommunikationspartner und Absender vielfach nur für kurze Zeit relevant. Dabei wird leicht übersehen, dass diese Informationen in ganz anderer Weise genutzt

werden können, wenn sie über einen längeren Zeitraum hinweg dokumentiert werden und unter Umständen noch viele Jahre später systematisch auswertbar sind.

Die Aufsichtsbehörden haben deshalb in einem im April 2008 gefassten Beschluss die datenschutzkonforme Ausgestaltung sozialer Netzwerke angemahnt. Folgendes ist zu beachten:

- Anbieter sozialer Netzwerke müssen ihre Nutzer umfassend über die Verarbeitung ihrer personenbezogenen Daten und ihre Wahl- und Gestaltungsmöglichkeiten unterrichten. Das betrifft auch Risiken für die Privatsphäre, die mit der Veröffentlichung von Daten in Nutzerprofilen verbunden sind. Darüber hinaus haben die Anbieter ihre Nutzer aufzuklären, wie diese mit personenbezogenen Daten Dritter zu verfahren haben.
- Nach den Bestimmungen des Telemediengesetzes ist eine Verwendung personenbezogener Nutzungsdaten für Werbezwecke nur zulässig, soweit die Betroffenen wirksam darin eingewilligt haben. Bei Werbemaßnahmen aufgrund von Profildaten müssen die Betroffenen nach den Bestimmungen des Bundesdatenschutzgesetzes mindestens eine Widerspruchsmöglichkeit haben. Die Aufsichtsbehörden empfehlen, dass die Anbieter die Nutzer selbst darüber entscheiden lassen, ob und wenn ja welche Profil- oder Nutzungsdaten zur zielgerichteten Werbung durch den Anbieter genutzt werden.
- Eine Speicherung personenbezogener Nutzungsdaten ist ohne Einwilligung der Nutzer über das Ende der Verbindung hinaus nur gestattet, soweit die Daten zu Abrechnungszwecken gegenüber dem Nutzer erforderlich sind.
- Es ist unzulässig, Daten über die Nutzung sozialer Netzwerke (wie auch anderer Internet-Dienste), die nicht mehr anderweitig benötigt werden, allein aus dem Grund weiter zu speichern, damit diese für eine etwaige zukünftige Strafverfolgung zur Verfügung stehen.
- Das Telemediengesetz verpflichtet die Anbieter dazu, das Handeln in sozialen Netzwerken anonym oder unter Pseudonym zu ermöglichen. Dies gilt unabhängig davon, ob ein Nutzer sich gegenüber dem Anbieter des sozialen Netzwerks mit seinen Echtdaten identifizieren muss.
- Die Anbieter müssen die erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit treffen. Sie müssen insbesondere einen systematischen oder massenhaften Export oder Download von Profildaten aus dem sozialen Netzwerk verhindern.
- Bei der datenschutzfreundlichen Gestaltung von sozialen Netzwerken kommt den Standardeinstellungen, beispielsweise was die Verfügbarkeit von Profildaten für Dritte anbelangt, eine zentrale Bedeutung zu. Die Aufsichtsbehörden fordern die Anbieter sozialer Netzwerke auf, datenschutzfreundliche Standardeinstellungen für ihre Dienste zu wählen, durch die die Privatsphäre der Nutzer möglichst umfassend geschützt wird. Diese Standardeinstellungen müssen besonders restriktiv gefasst werden, wenn sich das Angebot an Kinder richtet. Der Zugriff durch Suchmaschinen auf im sozialen Netzwerk gespeicherte personenbezogene Daten darf jedenfalls nur vorgesehen werden, soweit der Nutzer ausdrücklich eingewilligt hat.
- Der Nutzer muss die Möglichkeit erhalten, sein Profil auf einfache Weise selbst zu löschen. Auch sollten die Anbieter sozialer Netzwerke die Einführung von Verfallsdaten oder zumindest automatische Sperrungen erwägen, die von den Nutzern selbst festgelegt werden können.

10.1.2 Bewertungsportale

Einen starken Nutzerzuwachs verzeichnen auch Bewertungsportale im Internet, bei denen etwa Lehrer von ihren Schülern (wie im Beispiel *www.spickmich.de*) oder Professoren von den Studierenden (wie im Beispiel *www.mein-prof.de*) bewertet werden.

Diese Angebote bezwecken, Bewertungen über einzelne, namentlich genannte Personen zu erfassen und im Internet zu veröffentlichen. Charakteristisch für sie

ist, dass die Betroffenen vor der Veröffentlichung nicht um Einwilligung gefragt und vielfach noch nicht einmal nachträglich über die Veröffentlichung unterrichtet werden. Viele der auf diese Weise Bewerteten fühlen sich dabei an den Pranger gestellt und in ihren Persönlichkeitsrechten verletzt, weil

- die Objektivität der Bewertung in Frage steht,
- die Bewertung als inhaltlich unzutreffend angesehen wird,
- eine Diskussion zwischen Bewertetem und Bewertenden nicht möglich ist, da weder die Bewertenden noch die Hintergründe und Anlässe der Bewertung aus der Veröffentlichung hervorgehen,
- nicht überprüft wird, ob die Personen, die eine Bewertung abgegeben haben, tatsächlich Lehrveranstaltungen des Bewerteten besucht haben.

Mehrere Landgerichte und das Oberlandesgericht Köln, die von Betroffenen angerufen wurden, um die Rechtmäßigkeit der Veröffentlichung zu überprüfen, stellten das durch Artikel 5 Abs. 1 des Grundgesetzes geschützte Recht der Bewertenden auf freie Meinungsäußerung über das durch Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes geschützte informationelle Selbstbestimmungsrecht der Betroffenen. Für die Gerichte war ausschlaggebend, dass in den Portalen keine reine Schmähkritik oder Beleidigungen veröffentlicht werden, sondern bewertet wird, wie die Betroffenen ihre berufliche Tätigkeit ausüben.

Die Aufsichtsbehörden haben in einem Beschluss vom April 2008 Zweifel geäußert, ob die bisher ergangenen Gerichtsentscheidungen hinreichend berücksichtigen, dass es sich bei dem in Internetportalen veröffentlichten Beurteilungen von Angehörigen bestimmter Berufsgruppen um sensible Informationen und subjektive Werturteile handelt, die eingestellt werden, ohne dass die Urheber und das Zustandekommen der Beurteilung erkennbar sind. Vor allem aber berücksichtigen sie nicht hinreichend, dass diese Informationen von jedem registrierten Nutzer abgerufen werden können. Eine Veröffentlichung im Internet unterscheidet sich grundlegend von schul- oder hochschulinternen Veröffentlichungen von Beurteilungsergebnissen.

Der Bundesgerichtshof teilt diese Bedenken nicht. Er hat die Revision einer Lehrerin zurückgewiesen, die sich unter anderem gegen ihre in *www.spickmich.de* veröffentlichten Bewertungen gewehrt hatte. Die Bewertungen stellten Meinungsäußerungen dar, die die berufliche Tätigkeit der Klägerin beträfen, bei der der Einzelne grundsätzlich nicht den gleichen Schutz wie in der Privatsphäre genieße. Die Gründe der erst vor wenigen Wochen ergangenen Entscheidung sind noch nicht bekannt.

Die Klägerin hat inzwischen angekündigt, die Entscheidung durch das Bundesverfassungsgericht überprüfen zu lassen.

10.2 Veröffentlichung von Gebäude- und Grundstücksansichten

In den letzten Monaten hat ein internationaler Suchmaschinen- und Internetdiensteanbieter in zahlreichen deutschen Städten, darunter auch in Stuttgart, Mannheim, Karlsruhe, Reutlingen und Tübingen, systematisch Fotoaufnahmen von Straßenzügen und Gebäuden gemacht. Dabei wurden teilweise auch Personen und Kraftfahrzeuge mit erfasst. Die Aufnahmen sollen zu einem späteren Zeitpunkt so im Internet veröffentlicht werden, dass man sich nach Eingabe einer Anschrift dort befindliche Gebäude ansehen und den Blick vom jeweiligen Standort um 360 Grad schwenken kann, sodass eine Rundumsicht auf alle um diesen Ort herum befindlichen Gebäude besteht. Man kann dabei, ganzen Straßenzügen folgend, die nahtlos aneinander gefügten Aufnahmen der Gebäude wie in einem Film an sich vorbeiziehen lassen. Viele Bürger, vor allem aus den Gemeinden, in denen die wegen ihrer auf dem Dach montierten Kameraanlage auffälligen Fahrzeuge auftauchten, sind mit diesen Aufnahmen und deren Veröffentlichung nicht einverstanden und wandten sich an die Aufsichtsbehörde.

Da sich die mit diesem Vorhaben zusammenhängenden datenschutzrechtlichen Fragen in allen Bundesländern gleichermaßen stellen, hat sich der Düsseldorfer

Kreis damit befasst. Er beurteilt die Zulässigkeit der Veröffentlichung von digitalen Straßenansichten in seinem Beschluss vom November 2008 wie folgt:

> *„Bei digital erfassten Fotos von Gebäude- und Grundstücksansichten, die über Geokoordinaten eindeutig lokalisiert und damit einer Gebäudeadresse und dem Gebäudeeigentümer sowie den Bewohnern zugeordnet werden können, handelt es sich in der Regel um personenbezogene Daten, deren Erhebung und Verarbeitung nach dem Bundesdatenschutzgesetz zu beurteilen ist. Die Erhebung, Speicherung und Bereitstellung zum Abruf ist nur zulässig, wenn nicht schutzwürdige Interessen der Betroffenen überwiegen. Bei der Beurteilung schutzwürdiger Interessen ist von Bedeutung, für welche Zwecke die Bilddaten verwendet werden können und an wen diese übermittelt bzw. wie diese veröffentlicht werden. Die obersten Aufsichtsbehörden sind sich einig, dass die Veröffentlichung von georeferenziert und systematisch bereit gestellten Bilddaten unzulässig ist, wenn hierauf Gesichter, Kraftfahrzeugkennzeichen oder Hausnummern erkennbar sind. Den betroffenen Bewohnern und Grundstückseigentümern ist zudem die Möglichkeit einzuräumen, der Veröffentlichung der sie betreffenden Bilder zu widersprechen und dadurch die Bereitstellung der Klarbilder zu unterbinden. Keine schutzwürdigen Interessen bestehen, wenn die Darstellung der Gebäude und Grundstücke so verschleiert bzw. abstrakt erfolgt, dass keine individuellen Eigenschaften mehr erkennbar sind. Um die Möglichkeit zum Widerspruch schon vor der Erhebung zu eröffnen, sollte die geplante Datenerhebung mit einem Hinweis auf die Widerspruchsmöglichkeit rechtzeitig vorher bekannt gegeben werden. Die Widerspruchsmöglichkeit muss selbstverständlich auch noch nach der Veröffentlichung bestehen.“*

Mittlerweile hat sich das Unternehmen bereit erklärt, diesen Anforderungen zur Wahrung der Persönlichkeitsrechte der Betroffenen unter anderem durch folgende Maßnahmen nachzukommen:

– Gesichter fotografierter Personen und Kraftfahrzeugkennzeichen werden automatisch unkenntlich gemacht („verpixelt“). Hierzu ist kein Widerspruch der Betroffenen erforderlich.

– Wer nicht damit einverstanden ist, dass Fotos seines Hauses oder seiner Wohnung im Internet veröffentlicht werden, kann gegenüber dem Unternehmen dagegen Widerspruch einlegen; das Unternehmen sicherte zu, rechtzeitig eingehende Widersprüche noch vor der Veröffentlichung zu berücksichtigen. Darüber hinaus ist auch noch nach der Veröffentlichung ein Widerspruch möglich.

– Das Unternehmen informiert die Öffentlichkeit darüber, in welchen Städten und Gemeinden in nächster Zeit Straßenaufnahmen erfolgen.

Diese Zusicherungen sind aus der Sicht des Datenschutzes zu begrüßen. Es sind jedoch weitere Maßnahmen erforderlich, um das informationelle Selbstbestimmungsrecht der Betroffenen zu sichern. So müssen die Gesichter und die Kraftfahrzeugkennzeichen auch in den sogenannten Rohdaten unkenntlich gemacht werden. Widersprüche der Betroffenen müssen auch bei diesem Datenbestand berücksichtigt werden. Ferner muss die Qualität der Verpixelung weiter verbessert werden.

Gänzlich unbefriedigend verläuft bislang die Ankündigung von Aufnahmen in den Städten und Gemeinden. Die vom Diensteanbieter im Internet veröffentlichte Gemeindeliste ist, wie die Aufsichtsbehörde aus Rückmeldungen von Gemeindeverwaltungen, Bürgern und Presse weiß, höchst unvollständig: Kleinere Gemeinden werden darin offenbar von vornherein nicht aufgeführt, mitunter werden aber auch größere Städte, beispielsweise Tübingen, „vergessen“.

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit wurde vom Düsseldorfer Kreis gebeten, mit dem Unternehmen weitere Gespräche zu führen. Inzwischen hat sich das Unternehmen bereit erklärt, sämtliche Forderungen der Aufsichtsbehörden zu erfüllen. Dazu gehört auch, die Rohdaten der Aufnahmen, gegen die Widersprüche erhoben wurden, zu löschen. Ob den Ankündigungen entsprechende Taten folgen werden, insbesondere ob alle Widersprüche der Betroffenen in der Praxis berücksichtigt werden, bleibt abzuwarten.

Die Aufsichtsbehörde weist darauf hin, dass sich der Beschluss des Düsseldorfer Kreises vom November 2008 nicht allein auf das Vorhaben eines bestimmten Un-

ternehmens bezieht, sondern selbstverständlich für alle vergleichbaren Sachverhalte gilt.

10.3 Online-Shops

Mittlerweile bieten zahlreiche Unternehmen auf ihren Internetseiten auch die Möglichkeit, Dienstleistungen in Auftrag zu geben, Waren zu kaufen oder andere Verträge abzuschließen. Nach § 9 BDSG und § 13 Abs. 4 Nr. 3 des Telemediengesetzes sind die Betreiber solcher Internet-Shops verpflichtet, die erforderlichen Maßnahmen zu ergreifen, um die für den Vertragsabschluss übertragenen personenbezogenen Daten, zu denen vielfach auch besonders sensible Bankverbindungsdaten gehören, vor Kenntnisnahme oder Änderung durch Unberechtigte zu schützen. Beispielsweise sind folgende Maßnahmen erforderlich:

10.3.1 Schutz der für ein Kunden-Login benötigten Passwörter

In Online-Shops haben Kunden häufig die Möglichkeit, sich mit Benutzerkennung und Passwort an dem elektronischen Bestellsystem des Unternehmens anzumelden und sich dort beispielsweise über den Lieferstatus bestellter Waren zu informieren oder neue Bestellungen aufzugeben, ohne dafür jedes Mal von neuem alle personenbezogenen Stammdaten wie Lieferanschrift oder die für die Abrechnung notwendigen Daten eingeben zu müssen.

Bei solchen Angeboten muss die verantwortliche Stelle dafür sorgen, dass beim Umgang mit den zur Anmeldung benutzten Passwörtern die datenschutzrechtlichen Anforderungen eingehalten werden. Dazu ist unter anderem sicherzustellen, dass außer den Kunden niemand deren Passwörter im Klartext zur Kenntnis nehmen kann. Außerdem ist dafür zu sorgen, dass ein Nutzer, wenn er der Meinung ist, sein Passwort könne einem Unberechtigten bekannt geworden sein, seine Benutzerkennung sperren lassen oder sein Passwort jederzeit ändern kann. Gleich mehrere Beschwerdeführer wiesen die Aufsichtsbehörde darauf hin, dass es ein Versandhändler an den notwendigen Schutzmaßnahmen fehlen lasse. So gebe dieser das vom Kunden gewählte Passwort im Klartext in seinen Lieferscheinen und Rechnungen an. Hinzu komme, dass diese mitunter per unverschlüsselter E-Mail an die Kunden gesandt würden. Auch bei den den Warensendungen beigefügten Lieferscheinen und Rechnungen sei eine unberechtigte Kenntnisnahme nicht ausgeschlossen, da die Waren in einem unverschlossenen Karton versandt würden.

Auf Nachfrage bestätigte das Unternehmen, dass Warensendungen aus Kostengründen generell in dieser Form versandt werden. Es kündigte an, Kundenpasswörter zukünftig nicht mehr auf seinen Lieferscheinen und Rechnungen anzugeben.

10.3.2 Schutz der Login-Daten vor Missbrauch durch eine Sperre nach mehreren Anmeldefehlversuchen

Ein Kunde des Versandhändlers, der aufgrund der oben beschriebenen Versandart befürchtete, dass die zur Online-Anmeldung an dem Firmenportal vorgesehene Benutzerkennung und sein Passwort Unberechtigten zur Kenntnis gekommen sein könnte, wollte diese Benutzerkennung möglichst rasch sperren lassen. Ausgehend von Hinweisen zum Umgang mit Passwörtern, die von Datenschutzbeauftragten wie auch dem Bundesamt für die Sicherheit in der Informationstechnik herausgegeben werden, ging der Beschwerdeführer davon aus, dass seine Benutzerkennung nach wenigen Anmeldefehlversuchen automatisch gesperrt würde. Als er einen entsprechenden Test durchführte, musste er jedoch feststellen, dass dies nicht der Fall war. Die Aufsichtsbehörde forderte das Unternehmen daraufhin auf, auch beim Umgang mit Benutzerkennungen und Passwörtern für die Online-Anmeldung die üblichen datenschutzrechtlichen Anforderungen einzuhalten und eine Benutzerkennung nach mehreren Anmelde-Fehlversuchen zu sperren. Das Unternehmen hat bislang lediglich mitgeteilt, es werde eine solche Sperre realisieren, sofern der dafür erforderliche Aufwand vertretbar sei. Die Aufsichtsbehörde wird auf eine rasche Umsetzung hinwirken.

10.3.3 Schutzmaßnahmen bei Online-Rechnungen

Da der Schutz der Bankverbindungsdaten bei der vom Unternehmen bislang praktizierten unverschlüsselten Übertragung über das Internet nicht gewährleistet ist, hatte die Aufsichtsbehörde darauf hingewiesen, dass sich der notwendige Schutz durch eine Verschlüsselung realisieren ließe. Dies könnte beispielsweise dadurch erreicht werden, dass das Unternehmen die Rechnungen auf seinem Web-Server ablegt und dem Kunden per unverschlüsselter Mail zunächst lediglich einen auf eine durch SSL-Verschlüsselung gesicherte Internetseite führenden Link zusendet. Nach Anklicken dieses Links würde der Kunde zunächst aufgefordert, seine Benutzerkennung und sein Passwort einzugeben und könnte dann Zugriff auf diese Rechnung erhalten. Das Unternehmen lehnte jedoch in seiner ersten Stellungnahme hierzu die Verschlüsselung der Online-Rechnungen ab. Es teilte hierzu lediglich mit, die verschlüsselte Übertragung der Online-Rechnung sei „weder wirtschaftlich noch technisch opportun“ und komme daher für das Unternehmen „nicht in Frage“.

Dass die Forderung der Aufsichtsbehörde nicht unverhältnismäßig ist, zeigt sich schon daran, dass Banken, Kreditkarten- und Telekommunikationsdiensteanbieter Online-Rechnungen nicht per E-Mail versenden, sondern über eine SSL-gesicherte Verbindung zum Abruf bereitstellen. Zum anderen ist zu bedenken, dass das Unternehmen seinen Kunden schon bislang die Möglichkeit der individuellen Anmeldung mit Benutzerkennung und Passwort bietet und zudem eine SSL-Verschlüsselung in seinem Online-Shop einsetzt, sodass eine Kombination beider Funktionen ohne allzu großen Aufwand zu realisieren sein dürfte. Die Aufsichtsbehörde wird weiter darauf hinwirken, dass das Unternehmen die notwendigen Schutzmaßnahmen ergreift.

10.3.4 Verschlüsselte Übertragung der Vertragsdaten

Um die zum Vertragsabschluss notwendigen Daten bei ihrer Übertragung über das Internet vor unberechtigter Kenntnisnahme oder gezielter Veränderung zu schützen, sind diese Daten grundsätzlich zu verschlüsseln.

Durch eine Beschwerde wurde die Aufsichtsbehörde darauf aufmerksam, dass der Betreiber eines Online-Shops seinen Kunden zwar verspricht, deren Bestellung werde über einen „sicheren SSL-Server“ abgewickelt, der die „größtmögliche Verschlüsselungsvariante von 128 Bit“ nutze, tatsächlich wurde jedoch bei der Bestellabwicklung, zu der bei Bezahlung per Kreditkarte auch die dazu notwendigen Kreditkartendaten gehören, keine solche Verschlüsselung vorgenommen.

Nachdem die für den Betrieb des Online-Shops verantwortliche Stelle auf die mehrfache Aufforderung der Aufsichtsbehörde, ihren Internet-Shop so zu gestalten, dass die darin übertragenen personenbezogenen Daten verschlüsselt übertragen werden, nicht reagierte, kündigte die Aufsichtsbehörde an, die Realisierung der Verschlüsselung nach § 38 Abs. 5 BDSG förmlich anzuordnen.

10.4 Webcams

Immer wieder richteten sich Beschwerden gegen die Veröffentlichung von Webcam-Aufnahmen im Internet.

- Ein Beschwerdeführer teilte beispielsweise mit, dass in einem Einzelhandelsgeschäft jeder Kunde, der sich im Verkaufsraum aufhält, Verkaufsgespräche an einem Tresen führt, Waren begutachtet oder eine Warenbezahlung vornimmt, durch eine Webcam aufgenommen wird, deren Aufnahmen auf der Internetseite des Geschäfts für jedermann abruf- und beobachtbar waren.
- In einem anderen Fall wurde die Aufsichtsbehörde darauf aufmerksam gemacht, dass ein Schwimmbad auch Webcam-Aufnahmen aus dem laufenden Betrieb im Internet zum Abruf bereithielt.

Sofern es die aufgenommenen Bilder etwa aufgrund der Kamerapositionierung, fehlender Zoom-Möglichkeit oder niedriger Auflösung nicht zulassen, darauf Personen oder Informationen zu erkennen, die mit beim Betrachter vorhandenem Zu-

satzwissen einzelnen Personen zugeordnet werden können, bestehen gegen die Einstellung von Webcam-Aufnahmen ins Internet keine datenschutzrechtlichen Bedenken.

Sofern jedoch abgebildete Personen identifiziert werden können, ist die Verbreitung solcher Aufnahmen per Webcam nur unter Beachtung der datenschutzrechtlichen Vorschriften zulässig. Dabei ist zu berücksichtigen, dass eine Webcam nicht nur eine Videobeobachtung mit optisch-elektronischen Einrichtungen ermöglicht, sondern dass damit stets auch eine Veröffentlichung der Aufnahmen im Internet und somit eine Übermittlung an eine unbestimmte Vielzahl von Internetnutzern verbunden ist.

Soweit Personen erkannt werden können, ist der Betrieb einer Webcam daher nur zulässig, wenn sowohl die Voraussetzungen für die Videobeobachtung als auch die für die Verbreitung der Aufnahmen vorliegen. Die Verbreitung von Fotos oder anderen „Bildnissen“ ist nach § 22 des Kunsturheberrechtsgesetzes in der Regel nur mit Einwilligung der Betroffenen zulässig.

Nachdem die Aufsichtsbehörde die Betreiber der eingangs genannten Webcams hierüber unterrichtet hatte, stellte das Einzelhandelsgeschäft die Veröffentlichung der Bilder im Internet sofort ein. Der Betreiber des Schwimmbads änderte die Einstellungen der Kameras so, dass keine schutzwürdigen Interessen mehr verletzt werden können.

10.5 Online-Bewerbung

Etliche Unternehmen bieten über ihr Internetangebot die Möglichkeit, sich online um eine Stelle in diesem Unternehmen zu bewerben. Da eine Bewerbung stets zahlreiche personenbezogene Daten des Bewerbers enthält, muss sie, wenn sie online erfolgt, vor unberechtigten Zugriffen geschützt werden. Neben der Verschlüsselung der übertragenen Bewerberdaten ist dabei stets auch auf einen datenschutzgerechten Umgang mit den zur Überprüfung der Zugangsberechtigung verwendeten Passwörter zu achten.

Durch eine Beschwerde wurde die Aufsichtsbehörde auf Unzulänglichkeiten eines solchen Angebots aufmerksam:

In einem Unternehmen können Personen, die sich online um eine Stelle beworben haben, auch später noch auf ihre Bewerbungsdaten zugreifen und diese bei Bedarf ergänzen oder ändern, wenn sie hierfür ein individuelles Passwort festgelegt haben. Den Bewerbern wurde von dem Unternehmen hierzu mitgeteilt: „Nur Sie selbst kennen Ihr Passwort. Für den Fall, dass Sie es vergessen, haben Sie keinen Zugriff mehr auf die gespeicherten Daten.“

Die Beschwerde richtete sich dagegen, dass der Bewerber nach einer Online-Bewerbung noch am gleichen Tag per unverschlüsselter E-Mail eine Eingangsbestätigung erhielt, in der neben der zum Zugriff auf die Bewerberdaten notwendigen Benutzerkennung auch das vom Bewerber bestimmte Passwort im Klartext angegeben war. Damit werden die erfassten Daten nicht ausreichend vor unberechtigten Zugriffen geschützt. Ein wesentlicher Grundsatz beim Umgang mit Passwörtern ist, dass diese außer dem berechtigten Nutzer (hier dem Bewerber) keiner anderen Person bekannt werden dürfen. Da der Passwort-Versand per unverschlüsselter Mail keinen zuverlässigen Schutz vor unberechtigten Zugriffen auf die in einer solchen Mail enthaltenen Daten bieten kann, verstieß das Unternehmen damit gegen die gesetzliche Verpflichtung, bei der Gestaltung der elektronischen Datenverarbeitung die notwendigen technischen und organisatorischen Schutzmaßnahmen zu ergreifen (§ 9 BDSG).

Nachdem wir das Unternehmen aufgefordert hatten, diesen Mangel zu beseitigen, änderte es seine Vorgehensweise so, dass keine Passwörter mehr im Klartext an die Bewerber gesandt werden.

Für den Fall, dass ein Bewerber sein Passwort vergisst, wird ihm folgender Rücksetzungs-Prozess angeboten:

– Auf der durch SSL-Verschlüsselung gesicherten Internetseite, über die sich ein registrierter Benutzer anmelden kann, kann dieser Bewerber einen Link „Passwort ändern/Passwort vergessen?“ anklicken.

- Dort gibt er seine Benutzerkennung ein.
- Daraufhin wird ihm eine Frage vorgelegt, für die er bereits während seiner erstmaligen Registrierung eine individuelle Antwort angegeben hatte.
- Sofern er diese persönliche Frage korrekt beantwortet, wird für den Bewerber ein neues, einmal gültiges Passwort generiert und am Bildschirm angezeigt.
- Dem Bewerber wird zudem eine E-Mail an die bei seiner erstmaligen Registrierung angegebene E-Mail-Adresse gesandt, die einen einmalig gültigen Link erhält.
- Durch Anklicken dieses Links gelangt er auf eine Anmeldeseite, auf der er sich innerhalb eines Zeitraums von 24 Stunden nach Erhalt des Links mit dem zuvor für ihn neu generierten Passwort anmelden kann.
- Wenn er sich damit erfolgreich anmeldet, muss er ein neues, selbstgewähltes Passwort eingeben, welches das generierte (Einmal-)Passwort ersetzt.
- Um zu verhindern, dass Unternehmensangehörige die geheim zu haltenden Passwörter der Bewerber lesen und unberechtigt nutzen können, hat das Unternehmen eine sogenannte Einweg-Verschlüsselung für die Passwörter realisiert. Dadurch können selbst die Systemverwalter des Unternehmens keine Entschlüsselung dieser Passwörter vornehmen.

Damit hat das Unternehmen eine Lösung umgesetzt, bei der das betriebliche Interesse daran, eine Neuvergabe von Passwörtern zu ermöglichen, sofern die Bewerber ihr Passwort einmal vergessen haben und das Gebot des Datenschutzes, keine unberechtigte Zugriffsmöglichkeiten zuzulassen, miteinander in Einklang gebracht werden.

10.6 Hilfe, meine Daten stehen im Internet!

Oft sind Bürger überrascht, welche Informationen sie im Internet über sich finden, wenn sie ihren Namen in eine allgemeine Suchmaschine oder eine spezifische Personen-Suchmaschine eingeben. Personen-Suchmaschinen werben damit, personenbezogene Daten nicht nur aus Internetangeboten aufzuspüren, sondern auch aus vielfältigen anderen Quellen (zum Beispiel elektronischen Telefonbüchern oder sozialen Netzwerken) nachzuweisen.

Viele Betroffenen, die gegen solche Veröffentlichungen vorgehen wollen, weil sie keine Einwilligung dafür erteilt haben oder keine Rechtsgrundlage dafür sehen, tun sich oft schwer damit, den richtigen Adressaten zu finden. Es ist nämlich in der Regel nicht erfolgversprechend, vom Betreiber der Suchmaschine die Entfernung der Daten aus dem Internet zu verlangen. Dieser ist zumeist nicht die Stelle, die die Daten (erstmals) ins Internet gestellt hat. Die Suchmaschine weist den Nutzer lediglich darauf hin, an welchen anderen Stellen im Internet die gesuchten Daten veröffentlicht werden.

Der Betroffene sollte daher wie folgt vorgehen, um die Entfernung rechtswidrig im Internet veröffentlichter Daten zu erreichen:

- Ermittlung der verantwortlichen Stelle

  Er sollte ermitteln, welche Stelle für die von der Suchmaschine nachgewiesene Veröffentlichung im Internet verantwortlich ist. In der Regel gelingt dies, indem man den von der Suchmaschine angegebenen Link anklickt, die von der Suchmaschine nachgewiesene Fundstelle damit aufruft und anschließend die Angaben über die verantwortliche Stelle dem Impressum des daraufhin besuchten Angebots entnimmt.

- Kontaktaufnahme mit der verantwortlichen Stelle

  Im nächsten Schritt kann sich der Betroffene unmittelbar an die im Impressum genannte verantwortliche Stelle wenden und diese dazu auffordern, die entsprechenden Daten aus ihrem Internetangebot zu entfernen. Wenn eine nichtöffentliche Stelle dem nicht nachkommt und auch nicht nachvollziehbar begründen kann, weshalb die Veröffentlichung rechtmäßig ist, kann sich der Betroffene hierüber bei der zuständigen Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich beschweren.

– Beschwerdemöglichkeit bei der Aufsichtsbehörde

  Um Verzögerungen zu vermeiden, die sich aus der Weiterleitung eine Beschwerde an die zuständige Aufsichtsbehörde ergeben, sollte sich der Betroffene unmittelbar an diejenige Aufsichtsbehörde wenden, in deren örtlichem Zuständigkeitsbereich (Bundesland) die im Impressum genannte, für das Internetangebot verantwortliche nichtöffentliche Stelle ihren Sitz hat.

– Entfernung personenbezogener Daten aus dem Suchmaschinen-Cache

  Auch wenn auf diese Weise personenbezogene Daten von der Internetseite, auf der sie zuvor veröffentlicht worden waren, entfernt worden sind, kann es sein, dass die entfernten Daten noch in einem Zwischenspeicher (sogenannter Cache) gespeichert sind, der von einigen Suchmaschinen angeboten wird. Über den Cache-Inhalt können Nutzer der Suchmaschine Inhalte der von ihnen gesuchten Internetseite auch dann noch ansehen, wenn die Seite selbst, etwa aufgrund eines technischen Defekts, nicht aufgerufen werden kann. Der Zugriff hierauf ist in der Regel dadurch möglich, dass der Nutzer der Suchmaschine auf den bei dem Suchergebnis genannten Link „Cache“ klickt. Stellt ein Betroffener fest, dass personenbezogene Daten, die von der Internetseite bereits entfernt wurden, noch in dem von der Suchmaschine gespeicherten Cache-Abbild enthalten sind, kann er sich an den Betreiber der Suchmaschine wenden und diesen zur Bereinigung des Cache auffordern. Dabei sollte er darauf hinweisen, dass die fraglichen Daten auf der „Original“-Internetseite bereits entfernt wurden.

11 Videoüberwachung*

Die Zahl der Beschwerden von Bürgern, die sich durch eine Videoüberwachung in ihren Persönlichkeitsrechten beeinträchtigt sehen, ist nach wie vor hoch. Insoweit kann auf die Darstellung im vierten Tätigkeitsbericht (C 11, S. 214 ff.) verwiesen werden. Angesichts des Umfangs unzulässiger Videoüberwachung im privaten Bereich muss man von einem Kampf der Aufsichtsbehörden gegen Windmühlen sprechen.

Die Beschwerden richten sich nicht nur gegen Videoüberwachungsanlagen, die von Gewerbetreibenden, etwa im Einzelhandel, eingesetzt werden, sondern zunehmend auch gegen Videoüberwachungsanlagen, die von Privatpersonen betrieben werden. Dabei handelt es sich meist um Videokameras, die an Wohnhäusern angebracht und zumindest teilweise auf öffentliche Verkehrswege oder Nachbargründstücke gerichtet sind. Ein Grund für die Zunahme derartiger Beschwerden dürfte darin liegen, dass die Videoüberwachung inzwischen zu einer „Jedermann-Technik“ geworden ist, die sich kostengünstig installieren und einfach betreiben lässt. Für die Aufsichtsbehörde bedeutet dies, dass durch die immer leichtere Verfügbarkeit dieser Technik die Zahl der Stellen, die das Bundesdatenschutzgesetz beachten müssen und deshalb der Datenschutzaufsicht unterliegen, spürbar zunimmt. Ein Teil dieser Fälle zeichnet sich dadurch aus, dass es zwischen den am Beschwerdeverfahren Beteiligten bereits zuvor zu Nachbarschaftsstreitigkeiten kam. Hier erweist es sich als schwierig, eine von allen Beteiligten akzeptierte Lösung herbeizuführen, wenn – wie bei der Datenschutzaufsichtsbehörde – Gegenstand der Untersuchung ausschließlich die datenschutzrechtliche Zulässigkeit einer Videoüberwachung ist. Gefragt wäre hier eher ein Streitschlichter.

In Bezug auf den gewerblichen Einsatz der Videoüberwachung ist festzustellen, dass immer mehr „intelligente“ Systeme in Betrieb genommen werden, die nicht nur Daten aufzeichnen, sondern diese auch elektronisch auswerten. Auf diese Weise können die zurückgelegten Wege erfasst und das Verhalten der Betroffenen systematisch ausgewertet werden.

Sorge bereitet, dass die Videoüberwachung immer mehr in sensible Aufenthaltsbereiche wie beispielsweise die Gasträume von Restaurants oder Cafés und öffentliche Bäder vordringt und sogar vor absoluten Tabuzonen wie Pissoirräumen nicht Halt macht.

* Ausführungen zur Videoüberwachung von Arbeitnehmern finden sich unter B 1.1, 1.2 und 1.3.

11.1 Videoüberwachung von Geldautomaten

Der sogenannte Hundekotfall machte tagelang bundesweit Schlagzeilen. Worum ging es?

Im Eingangsbereich einer Bank war es während deren Öffnungszeiten vor einem Geldautomaten zu Verunreinigungen durch ein kleines Kind gekommen. Die Bank bemerkte dies erst etwas später. Sie beauftragte daraufhin eine Firma mit der Reinigung, die ihr dafür rund 53 Euro in Rechnung stellte. Um die Identität des Verursachers festzustellen, ließ die Bank zunächst für den in Frage kommenden Zeitraum die Bilder der Raumkamera auswerten. Dabei stellte sie eine Kundin mit Kleinkind fest. Anschließend wertete sie die von der Porträtkamera am Bankautomaten aufgezeichneten Videobilder aus. Da die Kundin Geld abgehoben hatte, konnte auf diesem Weg deren Kontonummer und über diese auch deren Name und Anschrift ermittelt werden. Sechs Wochen nach dem Ereignis forderte die Bank die Kundin zur Begleichung der ihr entstandenen Unkosten auf.

Im datenschutzrechtlichen Überprüfungsverfahren gab die Beschwerdeführerin an, ihr Kind habe im Bereich des Geldautomaten mehrere Fußabdrücke hinterlassen, weil seine Schuhe durch Hundekot verschmutzt gewesen seien. Die Bank hingegen ging von einer Verunreinigung durch das Kind aus.

Datenschutzrechtlich stellte sich die Frage, ob die Videoaufzeichnungen und Kontodaten der Betroffenen für den Zweck genutzt werden durften, den Verursacher einer Verunreinigung zu ermitteln.

Banken und Kreditinstitute dürfen eine Videoüberwachung im Bereich von Geldautomaten vornehmen, um mögliche Straftäter abzuschrecken und Beweismaterial im Falle einer versuchten oder vollendeten Straftat zu sichern. Soweit erforderlich, dürfen Videoaufzeichnungen im Falle einer Straftat auch durch die Bank und/oder die Polizei ausgewertet werden. Als Zweck einer Videoüberwachung kann – jedenfalls in gewissen Grenzen – auch die Geltendmachung von Schadensersatzansprüchen in Betracht kommen. Allerdings muss die Bank einen solchen Zweck – wie die anderen Zwecke auch – vor Inbetriebnahme einer Videoüberwachungsanlage ausdrücklich festlegen. Dies war nicht geschehen. Selbst wenn dies jedoch der Fall gewesen wäre, hätte die Bank sorgfältig prüfen müssen, ob die in der Auswertung der Videobilder und dem Zugriff auf die Kontodaten liegende Datennutzung unter Berücksichtigung aller Umstände des Einzelfalls erforderlich und insbesondere verhältnismäßig war.

Das hat die Aufsichtsbehörde verneint. Der Einzelfall war insofern besonders gelagert, als es sich um das Verhalten eines kleinen Kindes handelte, dem ein Missgeschick passiert war. Das Kind erfüllte weder den objektiven Straftatbestand der Sachbeschädigung noch war es strafmündig. Ob zivilrechtlich ein Schadensersatzanspruch gegen die Kundin bestand, brauchte nicht abschließend geklärt zu werden, da die Nutzung personenbezogener Daten zur Geltendmachung von Schadensersatzansprüchen nicht als zulässiger Nutzungszweck festgelegt war. Jedoch bestanden auch insoweit erhebliche Zweifel. In jedem Fall aber war die Nutzung der Video- und Kontodaten der Kundin angesichts der Gesamtumstände nicht erforderlich im Sinne des § 6 b Abs. 3 und des § 28 BDSG. Für die datenschutzrechtliche Beurteilung ohne Belang war das Verhalten der Kundin nach dem Missgeschick ihres Kindes.

Eine bußgeldrechtliche Ahndung des Verhaltens der Bankmitarbeiter kam nicht in Betracht, da eine unzulässige Datennutzung nicht bußgeldbewehrt ist.

Nachdem die Aufsichtsbehörde der Bank ihre rechtliche Beurteilung mitgeteilt und mit ihr die Voraussetzungen für die Videoüberwachung und die Verarbeitung und Nutzung von Videoaufzeichnungen sowie die Nutzung von Kontodaten eingehend erörtert hatte, sagte diese zu, künftig in Videoüberwachungsfällen den Anforderungen des Bundesdatenschutzgesetzes Rechnung zu tragen. Sie sagte auch zu, vor einer Anordnung von Videoüberwachungsmaßnahmen und einer Auswertung von Videoaufzeichnungen den Beauftragten für den Datenschutz zu beteiligen.

11.2 Videoüberwachung in Gaststätten

Bei der nach § 6 b BDSG für jede Videoüberwachung notwendigerweise durchzuführende Interessenabwägung sind, wenn es um Gaststätten geht, folgende Aspekte zu berücksichtigen:

Gaststättenbesucher verbringen vielfach geraume Zeit in den Gasträumen. Sie halten sich dort gemeinsam mit anderen Menschen in entspannter Atmosphäre auf. Dieses dem Freizeitbereich der Personen zuzurechnende Verhalten geht mit einem besonders hohen Schutzbedarf der Persönlichkeitsrechte der Betroffenen einher (siehe dazu schon den vierten Tätigkeitsbericht C 11, S. 217, der von „Orten der Kommunikation“ spricht). Erfolgte in diesem Bereich eine Videoüberwachung, würden die Persönlichkeitsrechte der Betroffenen erheblich beeinträchtigt. Da in Gasträumen grundsätzlich nicht von einer überdurchschnittlich hohen Gefährdung des Eigentums des Gaststättenbetreibers auszugehen ist, sind die Interessen der Betreiber von Videoüberwachungsanlagen in Gasträumen nicht als ebenso gewichtig anzusehen, wie dies bei einer Videoüberwachung in Verkaufsräumen der Fall ist. Damit wird eine Videobeobachtung von Gasträumen datenschutzrechtlich in der Regel als unzulässig anzusehen sein. Von entsprechenden Erwägungen ließ sich auch das Amtsgericht Hamburg bei seinem Urteil vom 22. April 2008 leiten. Darin entschied es, dass Kunden einer Kaffeehaus-Kette einen Anspruch nach §§ 823 Abs. 2 Satz 2, 1004 Abs. 1 BGB darauf haben, dass der Kaffeehaus-Betreiber eine Videoüberwachung im Kundenbereich, in dem sich die Kunden zum Verzehr gekaufter Waren aufhalten können, unterlässt (Az. 4 C 134/08).

11.3 Videoüberwachung eines Brauchtumsfests

Vor Beginn eines alljährlich stattfindenden Brauchtumsfests wurde im letzten Jahr die Frage an die Aufsichtsbehörde herangetragen, ob die vom örtlichen Brauchtumsverein an mehreren Stellen des Festgeländes geplante Videoüberwachung datenschutzrechtlich zulässig ist. Zum Hintergrund teilte der Brauchtumsverein mit, die Stadt habe ihm für die Dauer des Festes das Hausrecht über das gesamte, frei zugängliche Festgelände, über das auch öffentliche Wege verlaufen, übertragen. Die geplante Videoüberwachung solle dem Zweck dienen, Straftaten, die im Bereich des Festgeländes geschehen können, zu dokumentieren und entsprechende Aufzeichnungen bei Bedarf an die Polizei herauszugeben.

Die Aufsichtsbehörde konnte in der Kürze der ihr zur Verfügung stehenden Zeit das Vorhaben nur vorläufig bewerten. Sie machte gegenüber dem Veranstalter deutlich, dass sie erhebliche Zweifel an der Rechtmäßigkeit des Vorhabens hat. Zwar dürfe auch eine nichtöffentliche Stelle im Rahmen des Hausrechts Videoüberwachung einsetzen, um Straftaten zu verhindern oder Beweismaterial zur Aufklärung einer Straftat zu sichern. Die Aufsichtsbehörde habe jedoch aus den ihr vorliegenden Unterlagen den Eindruck gewonnen, dass dem Brauchtumsverein für die Dauer des Fests die Gewährleistung der öffentlichen Sicherheit und Ordnung umfassend übertragen werden sollte. So hieß es beispielsweise in einer Unterlage:

> *„Zur Gewährleistung der öffentlichen Sicherheit auf dem ... (Brauchtumsfest) fordert die Stadt ... vom Veranstalter die Installierung von Video-Kameras an einzelnen, von ihr näher bezeichneten Stellen auf dem Festgelände. Die Installation und der Betrieb der Video-Kameras sollen in ersten Linie die Begehung von Straftaten präventiv verhindern, indem ihr Vorhandensein auf mögliche Straftäter abschreckend wirkt. Daneben sollen die Aufzeichnungen, die mit Hilfe der Kameras angefertigt werden, zur Aufklärung von Straftaten beitragen, die von Festbesuchern bei der Polizei zur Anzeige gebracht wurden.“*

An anderer Stelle wurde ausgeführt:

> *„Da die Stadt ... die Videoüberwachung nicht selbst durchführen will, sondern ... (den Brauchtumsverein) mit dieser Aufgabe betrauen möchte, beabsichtigt sie diesem für die Dauer des Festes die tatsächliche Verfügungsgewalt über die Flächen zu übertragen, auf denen eine Videoüberwachung stattfinden soll.“*

In der für die (beabsichtigte) Videoüberwachung erlassenen Verfahrensanordnung hieß es, dass die gewonnenen Aufnahmen „nach Anordnung und Weisung der hierfür gesetzlich zuständigen staatlichen Behörden“ im Rahmen ihrer Zuständigkeit ausgewertet und gespeichert werden, um die Verfolgung rechtswidriger Taten und die hieraus entstandenen Schäden zu ermöglichen.

Die Gewährleistung der öffentlichen Sicherheit und Ordnung kann, so machte die Aufsichtsbehörde gegenüber dem Brauchtumsverein deutlich, nicht auf einen privaten Verein übertragen werden, sondern ist Aufgabe der Polizei. Darüber hinaus äußerte die Aufsichtsbehörde erhebliche Zweifel, ob, selbst wenn § 6 b BDSG anwendbar wäre, dessen Voraussetzungen vorlägen:

– § 6 b BDSG verlangt, dass die Videoüberwachung eine „geeignete“ Maßnahme ist. Die Unterlagen ließen nicht erkennen, dass beziehungsweise wie durch die vorgesehenen drei Videokameras an den konkreten Einsatzorten der Zweck der Videoüberwachung, Straftaten zu verhindern oder aufzuklären, erreicht werden kann. Sie belegten lediglich, welche Straftaten und Ordnungsstörungen sich während eines vorangegangenen Fests im Stadtgebiet, also auch außerhalb des Festgeländes, ereignet hatten. Dass die vorgesehenen Kamerastandorte Schwerpunkte der Kriminalität waren beziehungsweise dass gerade dort Straftaten vorgekommen waren, ging daraus nicht hervor.
– § 6 b BDSG verlangt auch, dass geprüft wird, ob weniger einschneidende Maßnahmen, beispielsweise häufigere Kontrollen durch Sicherheitspersonal, ausreichen. Auch dazu fand sich in den Unterlagen nichts.
– Ferner muss in die durch § 6 b BDSG vorgeschriebene Interessenabwägung eingestellt werden, dass an einem solchen Fest viele Personen teilnehmen, die keine Straftaten verüben („Unbeteiligte“) und dort – noch mehr als in Gaststätten (siehe dazu oben Nr. 11.2) – einen Teil ihrer Freizeit mit anderen kommunizierend und unbeobachtet verbringen wollen.
– Nur der Vollständigkeit halber wies die Aufsichtsbehörde darauf hin, dass die Veranstalter auch nicht geprüft hatten, ob eine zeitliche Beschränkung der Videoüberwachung auf die Nachtstunden möglich war.

Die Veranstalter haben aufgrund dieses Schreibens auf die Videoüberwachung des Fests im Jahr 2008 verzichtet.

Nach einer Ortsbesichtigung während der letzten Brauchtumsveranstaltung und zwei Gesprächen mit den Veranstaltern und der Stadtverwaltung hat die Aufsichtsbehörde den Veranstaltern mitgeteilt, dass ihre vorläufige Bewertung auch die endgültige ist. Sie bleibt dabei, dass die Videoüberwachung schwerpunktmäßig der öffentlichen Sicherheit und Ordnung dienen sollte und soll. § 6 b BDSG bietet Privaten dafür keine Rechtsgrundlage.

Ob eine Videoüberwachung durch den Polizeivollzugsdienst auf der Grundlage des § 21 Abs. 1 des Polizeigesetzes (PolG) möglich ist, bedarf – so das Innenministerium – eingehender Prüfung. Entscheidend dafür ist, ob aufgrund der Art und Größe der Veranstaltung erfahrungsgemäß erhebliche Gefahren für die öffentliche Sicherheit entstehen können (§ 21 Abs. 1 Satz 2 Nr. 2 PolG). Dabei sind nur Straftaten in den zur Videoüberwachung vorgesehenen Bereichen und dessen unmittelbarer Umgebung von Interesse, nicht dagegen solche im sonstigen Stadtgebiet, insbesondere außerhalb des Festgeländes. Zudem ist – wie stets bei polizeilichen Maßnahmen – der Grundsatz der Verhältnismäßigkeit zu beachten. Alle Beteiligten waren sich darüber einig, dass diese Voraussetzungen beim Brauchtumsfest 2008 nicht vorlagen.

11.4 Videoattrappen und unzutreffende Hinweise auf Videoüberwachung

Gelegentlich stellt die Aufsichtsbehörde bei einer datenschutzrechtlichen Überprüfung fest, dass anstelle funktionsfähiger Kameras lediglich funktionsunfähige Attrappen installiert sind. Oder es sind Hinweise auf eine Videoüberwachung angebracht, obwohl eine solche nicht stattfindet. In diesen Fällen ist das Bundesdatenschutzgesetz nicht anwendbar, da die Daten weder, wie es § 1 Abs. 2 Nr. 3 BDSG verlangt, unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben, noch in oder aus nichtautomatisierten Dateien verarbeitet, ge-

nutzt oder dafür erhoben werden. Dementsprechend hat auch die Aufsichtsbehörde keine Kontrollbefugnis nach § 38 BDSG. Dies hat zur Folge, dass die Aufsichtsbehörde keine Möglichkeit hat, etwa die Entfernung von Kameraattrappen oder von unzutreffenden Hinweisschildern zu verlangen.

Unbestritten ist aber auch, dass das Anbringen von Kameraattrappen oder Hinweisschildern auf eine angeblich stattfindende Videoüberwachung bei Personen, die dies zur Kenntnis nehmen, regelmäßig den Eindruck vermittelt und auch vermitteln soll, dass diese tatsächlich videoüberwacht werden. Schon allein das Anbringen der Attrappen oder Hinweisschilder kann somit bei den Betroffenen einen Überwachungsdruck auslösen. Hinzu kommt, dass eine Stelle den Betroffenen letztlich falsche Informationen darüber gibt, welche Daten sie über sie erhebt, verarbeitet oder nutzt. Das Bundesverfassungsgericht hat bereits in seinem Volkszählungsurteil vom 15. Dezember 1983 (BVerfGE 65, 1 ff.) deutlich gemacht, dass Bürger Klarheit darüber benötigen, welche Stelle was über sie weiß. Hierzu führte es unter anderem aus:

> *„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“*

Diese Ausführungen haben nicht nur für den öffentlichen, sondern auch für den privaten Bereich Bedeutung. Die Zivilgerichte haben mehrfach entschieden, dass sich ein Betroffener jedenfalls, dann gegen eine Kameraattrappe zur Wehr setzen kann, wenn diese den Eindruck erweckt, sie sei funktionstüchtig und es könnten damit Aufzeichnungen gemacht werden (zum Beispiel LG Bonn, Urteil vom 16. November 2004, Az. 8 S139/04). Er kann dafür allerdings nicht die Hilfe der Aufsichtsbehörden in Anspruch nehmen, sondern muss selbst versuchen, seinen Unterlassungsanspruch nach § 823 in Verbindung mit § 1004 BGB gegen die verantwortliche Stelle durchzusetzen, notfalls im Klageweg.

12 Vereine, Verbände

12.1 Übermittlung der Mitgliederliste eines Vereins an den Verband

Die Leitung eines Motorsportvereins, der zugleich Ortsverband eines bundesweiten Automobilclubs ist, wurde vom Landesverband des Automobilclubs aufgefordert, ihm eine vollständige Mitgliederliste zu übersenden. Dagegen wandte sich der Motorsportverein. Er wies darauf hin, dass seine Mitglieder nach der Satzung nicht automatisch auch Mitglieder des (bundesweiten) Automobilclubs sein müssten. Der dazu angehörte Automobilclub begründete seine Forderung zum einen damit, dass er feststellen müsse, wie viele Delegierte der jeweilige Ortsclub in die Hauptversammlung des Automobilclubs entsenden dürfe. Die Angaben müssten auch personenbezogen sein, um die Daten der Ortsclubs mit denen des Automobilclubs abgleichen zu können. Dies sei notwendig, weil eine Person zwar Mitglied in mehreren Ortsclubs sein könne, jedoch nur bei einem Ortsclub bei der Bestimmung der Zahl der Delegierten berücksichtigt werden dürfe. Zum anderen stelle der Automobilclub für sämtliche Mitglieder der Ortsclubs, also auch für

solche, die nicht zugleich Mitglied des Automobilclubs sind, einen Versicherungsschutz mit Unfallversicherung und Haftpflichtversicherung für alle Tätigkeiten im Zusammenhang mit Clubveranstaltungen bereit. Hierzu benötige der Automobilclub die Daten der zu versichernden Personen.

Die Aufsichtsbehörde hielt es für zulässig, die Daten derjenigen Ortsclubmitglieder an den Automobilclub zu übermitteln, die zugleich Mitglieder des Automobilclubs sind. Die Notwendigkeit, die Zahl der von jedem Ortsclub zu entsendenden Delegierten festzustellen, ist dafür ein hinreichender Grund. Unzulässig ist hingegen die Übermittlung der Daten der „reinen" Ortsclubmitglieder an den Automobilclub, um diesen Versicherungsschutz zu gewähren. Es handelt sich insoweit um eine freiwillige Leistung des Automobilclubs gegenüber den „reinen" Ortsclubmitgliedern. Es muss daher diesen überlassen bleiben, ob sie von diesem Angebot Gebrauch machen wollen. Die Aufsichtsbehörde hat daher vorgeschlagen, dass der Automobilclub in Zukunft die Mitglieder des Ortsclubs über sein Angebot für eine (kostenlose) Versicherung informiert. Soweit die „reinen" Ortsclubmitglieder eine Versicherung abschließen wollen, können sie dies dem Automobilclub mitteilen, der dann Kontakt zu den Interessenten aufnimmt.

12.2 Datenschutz bei der Aufnahme von Gewerkschaftsmitgliedern

Eine Gewerkschaft wandte sich mit der Bitte an die Aufsichtsbehörde, sie bei der datenschutzrechtlichen Ausgestaltung eines Aufnahmeantrags und einer Einwilligungserklärung zu beraten. Beratungswünsche von Vereinen und Verbänden sind erfreulicherweise häufig. Wir kommen ihnen selbstverständlich gerne nach. Auf die meisten Fragen gibt das von der Aufsichtsbehörde herausgegebene Merkblatt zum „Datenschutz im Verein" eine Antwort. Es ist unter (*www.im.baden-wuerttemberg.de* – darin Auswahl „Datenschutz" – „Weitere Infos" – „Infomaterial") im Internet abrufbar. Im Übrigen ist Folgendes zu beachten:

– Erhebung personenbezogener Daten im Aufnahmeantrag

  Häufig verlangen Vereine und Verbände (im Folgenden: Vereine) von Beitrittswilligen, im Aufnahmeantrag generell in die Erhebung, Verarbeitung und Nutzung ihrer Daten einzuwilligen. Sie meinen, damit dem informationellen Selbstbestimmungsrecht der Betroffenen am besten Rechnung zu tragen. Sie können sich dafür auf den Wortlaut des § 4 BDSG berufen, der das Bundesdatendatenschutzgesetz oder eine andere Rechtsvorschrift einerseits und die Einwilligung des Betroffenen andererseits als Erlaubnistatbestände für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten auf eine Stufe stellt. Dies wird häufig so verstanden, als könne die verantwortliche Stelle die Einwilligung der Betroffenen selbst dann einholen, wenn ihr gesetzliche Verarbeitungsbefugnisse zustehen. Diese Auffassung ist jedoch abzulehnen, weil durch die Einholung einer Einwilligung beim Betroffenen immer der Eindruck erweckt wird, er habe eine Wahlfreiheit und damit die Möglichkeit, die vorgesehene Verwendung seiner Daten für den vorgesehen Zweck abzulehnen. Hat die verantwortliche Stelle jedoch von vornherein die Absicht, im Falle der Verweigerung des Einverständnisses auf die gesetzlichen Verarbeitungsbefugnisse zurückzugreifen, wird der Betroffene getäuscht. Wir empfehlen deshalb, bei einem Aufnahmeantrag beispielsweise die Verarbeitung der Daten für Zwecke der Mitgliederverwaltung und der Einziehung des Mitgliedsbeitrags auf den gesetzlichen Erlaubnistatbestand des § 28 Abs. 1 Satz 1 Nr. 1 BDSG zu stützen, weil ein Verein die Daten seiner Mitglieder für diese Zwecke in der Regel erheben, speichern und nutzen muss, ohne dass es dazu eine Alternative gibt. Von der Einwilligung soll ein Verein daher – wie jede andere nichtöffentliche Stelle auch – nur dann Gebrauch machen, wenn er tatsächlich und rechtlich über mehrere Verarbeitungsalternativen verfügt und bereit ist, die Verweigerung der Einwilligung durch den Betroffenen zu respektieren.

  Zudem dürfen nur erforderliche Daten erhoben und verarbeitet werden. Die Frage nach einer früheren Mitgliedschaft des Beitrittswilligen in einer konkurrierenden Organisation sieht die Aufsichtsbehörde nicht als erforderlich und damit als unzulässig an.

  Zu beachten ist ferner, dass der Beitrittswillige im Aufnahmeantrag darüber informiert wird, für welche Zwecke seine Daten erhoben, gespeichert und ge-

nutzt und ob und gegebenenfalls an wen sie für welche Zwecke übermittelt werden (§ 4 Abs. 3 Satz 1 BDSG). Bestimmte Daten wie beispielsweise Telefonnummern und E-Mail-Adressen sollten als freiwillige Angabe gekennzeichnet werden. Im Übrigen wird empfohlen, die Datenerhebung, -verarbeitung und -nutzung in der Vereinssatzung zu regeln.

– Einwilligungserklärung

In den Fällen, in denen die Datenerhebung, -verarbeitung und -nutzung auf eine Einwilligung des Betroffenen gestützt werden soll und nach dem zuvor Gesagten auch gestützt werden kann, ist Folgendes zu beachten:

- Damit die Betroffenen wissen, wozu sie ihre Einwilligung erklären sollen und damit die Erklärung auch wirksam werden kann, sind die Betroffenen vorab über den Zweck beziehungsweise die Zwecke der beabsichtigten Erhebung, Verarbeitung und Nutzung ihrer Daten zu unterrichten (§ 4 a Abs. 1 Satz 2 BDSG). Legt ein Verein einem Beitrittswilligen sowohl einen Aufnahmeantrag als auch eine Einwilligungserklärung vor, muss er darauf achten, dass beide Erklärungen aufeinander abgestimmte Datenschutzhinweise enthalten, damit der Beitrittswillige nicht irritiert wird.
- Soll, wie im Falle der Gewerkschaft, die Einwilligung zu Datenübermittlungen an verschiedene Empfänger für unterschiedliche Zwecke eingeholt werden, sollte der Vordruck so ausgestaltet sein, dass der Beitrittswillige bei der Einwilligung differenzieren kann (Ankreuzlösung).

– Einwilligung in die Datenübermittlung an Versicherungen

Die Gewerkschaft bot für alle Mitglieder einen Versicherungsschutz an, zu dem unter anderem auch eine Unfallversicherung gehörte. Die Besonderheit war, dass der Beitrittswillige bereits im Zeitpunkt der Aufnahme darin einwilligen sollte, dass seine Daten bei Eintritt des Versicherungsfalls an die Versicherung übermittelt werden. Die Aufsichtsbehörde wies darauf hin, dass sich ein solcher Versicherungsfall möglicherweise erst sehr viele Jahre oder sogar Jahrzehnte nach dem Beitritt des Mitglieds ereignen kann. Es sei äußerst zweifelhaft, ob man sich nach so langer Zeit noch auf eine früher erteilte Einwilligung berufen könne. Die Aufsichtsbehörde legte daher der Gewerkschaft nahe, es dem Betroffenen selbst zu überlassen, ob er nach Eintritt des Versicherungsfalls die Versicherung in Anspruch nehmen und dieser personenbezogene Daten übermitteln will.

12.3 Übermittlung von Spielerdaten durch einen Sportverband oder -verein

Ein Sportverband wollte von der Aufsichtsbehörde wissen, ob er oder ein Sportverein (im Folgenden: Verein) Spielberichte oder andere personenbezogene Angaben zu Spielern an Dritte herausgeben darf oder sogar muss. Es komme immer wieder vor, dass Arbeitgeber aus der Zeitung davon erfahren, dass ein krankgeschriebener Mitarbeiter an einem Spiel teilgenommen hat. Der Arbeitgeber benötige dann Informationen, um mögliche arbeitsrechtliche Maßnahmen gegenüber dem Mitarbeiter ergreifen zu können. In anderen Fällen erbäten Krankenversicherungen Auskünfte, um einen Spieler, der einen anderen verletzt hat, in Regress nehmen zu können. Auch wende sich die Polizei immer wieder mit Fragen an die Vereine, wenn es während eines Spieles oder danach zu gewalttätigen Auseinandersetzungen zwischen den Spielern gekommen sei.

Da Spielberichte nicht für den Zweck erstellt wurden, für den sie nunmehr begehrt werden, richtet sich die Zulässigkeit der Datenübermittlung an den Dritten nach § 28 Abs. 3 Satz 1 Nrn. 1 und 2 BDSG. Danach ist die Übermittlung zulässig, soweit diese zur Wahrung berechtigter Interessen eines Dritten oder zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. Besonderheiten können sich ergeben, soweit es um die Übermittlung von Gesundheitsdaten geht (§ 28 Abs. 8 BDSG) oder wenn der auskunftsuchenden Stelle, beispielsweise der Polizei, die Auskunft erteilt werden muss.

Die Aufsichtsbehörde machte in ihrer Antwort deutlich, dass die Auskunftserteilung an die *Polizei* in der Regel unproblematisch sein dürfte, weil je nach Sachla-

ge die Übermittlung von Teilen oder des ganzen Spielberichts zur Verfolgung von Straftaten erforderlich ist. Im Übrigen vertrat die Aufsichtsbehörde folgende Auffassung:

– Der *Arbeitgeber* sollte sich wegen des Grundsatzes der Direkterhebung beim Betroffenen (§ 4 Abs. 2 Satz 1 BDSG) zunächst unmittelbar an seinen Mitarbeiter wenden, ihn mit dem Zeitungsbericht konfrontieren und zur Stellungnahme auffordern. Nur wenn dies nicht weiterhelfen sollte, könnte er den Verein um Auskunft bitten, ob sein Mitarbeiter an einem Spiel teilgenommen hat. Weitergehende Informationen benötigt der Arbeitgeber nicht. Um schutzwürdige Belange des Betroffenen angemessen berücksichtigen zu können, sollte dieser vor einer Datenübermittlung angehört werden.

– *Krankenversicherungen* sind grundsätzlich berechtigt zu erfahren, gegen wen und in welchem Umfang ihnen ein Regressanspruch wegen der Verletzung einer Person, an die sie deswegen Leistungen erbracht haben, zusteht. Für die gesetzlichen Krankenversicherungen ergibt sich dies aus § 67 a SGB X, für die privaten Krankenversicherungen aus § 28 Abs. 1 Satz 1 Nr. 1 BDSG. Soweit die Übermittlungsvoraussetzungen vorliegen, wird es allerdings genügen, der Versicherung in einem Schritt lediglich die Kontaktdaten des betreffenden Spielers und keinen (Auszug aus dem) Spielbericht zu übermitteln. Nur wenn dies nicht weiterhelfen sollte, könnte in einem zweiten Schritt dann die Übermittlung weiterer personenbezogener Angaben über den Spielverlauf erwogen werden. Um auch hier schutzwürdige Belange des Betroffenen angemessen zu berücksichtigen, sollte er vor einer Datenübermittlung angehört werden.

12.4 Veröffentlichung von Spielsperren im Internet

Ein Betroffener beschwerte sich bei der Aufsichtsbehörde darüber, dass ein Sportverband seinen Vor- und Nachnamen, die ihm vorgeworfene Tat, deren Datum, die verhängte Verbandsstrafe (Spielsperre) sowie weitere Angaben in der Rubrik „Spielsperren“ in seinem Internetangebot für jedermann einsehbar veröffentlicht hatte. Dies war in dieser Form nicht zulässig.

Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG kann ein Verband personenbezogene Daten über einen Spieler, mit dem ein vertragsähnliches Vertrauensverhältnis besteht, im Rahmen des Grundsatzes der Verhältnismäßigkeit übermitteln, soweit dies der Zweckbestimmung dieses vertragsähnlichen Verhältnisses dient und die Verbandsstatuten dies vorsehen (§ 28 Abs. 1 Satz 2 BDSG). Nicht gerechtfertigt ist jedoch, diese Informationen so in das Internet einzustellen, dass weltweit jedermann davon Kenntnis nehmen kann. Damit würden Spieler, die mit einer Verbandsstrafe belegt wurden, regelrecht an den Pranger gestellt. Ein legitimes Interesse daran, sich über die Dauer von Spielsperren informieren und deren Beachtung kontrollieren zu können, hat nur ein begrenzter Personenkreis, beispielsweise Mannschaften derselben Spielklasse oder Schiedsrichter. Aber auch dieser muss nicht wissen, welche Gründe zu der Sperrung geführt haben. Erst recht muss er keine Kenntnis von anderen Verbandsstrafen, etwa Geldbußen, haben. Die Verbandsmitglieder oder die Sportler allgemein über Verbandsstrafen zu informieren, um dadurch einen Abschreckungseffekt zu erzielen, würde eine personenbezogene Veröffentlichung im Internet nicht rechtfertigen. Das Mitteilungssystem des Verbands ist daher so auszugestalten, dass nur der jeweils berechtigte Personenkreis auf die einzelnen Daten zugreifen kann. Dies lässt sich durch eine Intranetlösung erreichen, bei der den berechtigten Nutzern durch Verwendung von Benutzerkennungen und Passwörtern individuelle Zugriffsberechtigungen eingeräumt werden. Diese sind so zu vergeben, dass jeder Nutzer nur auf diejenigen personenbezogenen Daten zugreifen kann, die er zur Wahrnehmung seiner (Vereins-)Aufgaben benötigt.

Erfreulicherweise hat der Verband, nachdem ihn die Aufsichtsbehörde über die Beschwerde informiert hatte, sofort reagiert und die Spielsperren noch vor Abschluss der datenschutzrechtlichen Bewertung vom Netz genommen. Die Wiederinbetriebnahme erfolgte nach Umsetzung der von der Aufsichtsbehörde skizzierten Intranetlösung.

C Allgemeine Fragen des Bundesdatenschutzgesetzes – der Beauftragte für den Datenschutz

Sowohl Beratungsanfragen als auch Beschwerden boten der Aufsichtsbehörde im Berichtszeitraum Anlass, sich mit Fragen zur Bestellung, zur Tätigkeit und zur Erreichbarkeit von Beauftragten für den Datenschutz zu befassen.

1 Bestellung einer Firma oder einer Person?

Ein Unternehmen beabsichtigte, eine Dienstleistungs-GmbH zum externen betrieblichen Datenschutzbeauftragten zu bestellen. Nach Einschätzung der Aufsichtsbehörde lassen die gesetzlichen Vorschriften jedoch nur die Bestellung einer natürlichen Person zum betrieblichen Datenschutzbeauftragten zu. Die Bestellung eines Unternehmens oder einer anderen „juristischen Person“ zum betrieblichen Datenschutzbeauftragten kommt unter anderem aufgrund folgender Erwägungen nicht in Betracht:

- Betroffene müssen die Möglichkeit haben, sich vertraulich und unmittelbar an den betrieblichen Datenschutzbeauftragten zu wenden. Nur eine natürliche Person kann die nach dem BDSG zu beachtende Verschwiegenheitspflicht gewährleisten. Bei der Bestellung eines Unternehmens kann eine gesetzeskonforme Umsetzung kaum sichergestellt werden.
- Nur bei einer natürlichen Person kann festgestellt werden, ob sie die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt.
- Da sich die Kontrolle des Datenschutzbeauftragten auch auf nach dem BDSG besonders sensible Daten sowie auf Daten erstreckt, die einem Berufsgeheimnis, z. B. der ärztlichen Schweigepflicht, unterliegen, ist der Schutz der Persönlichkeitsrechte nur durch die Bestellung einer natürlichen Person sicherzustellen, an die sich der Betroffene unmittelbar wenden kann.

2 Ermöglichung einer unmittelbaren Kontaktaufnahme

Ein Unternehmen, das von einem Betroffenen um die Bekanntgabe der Kontaktdaten des betrieblichen Datenschutzbeauftragten gebeten wird, muss es diesem ermöglichen, sich unmittelbar an den Beauftragten für den Datenschutz zu wenden. Deshalb sind dem Betroffenen die hierfür erforderlichen Kontaktadressen mitzuteilen.

Hierauf wies die Aufsichtsbehörde ein Unternehmen hin, das sich zuvor geweigert hatte, einem Betroffenen gegenüber die Kontaktdaten seines (externen) betrieblichen Datenschutzbeauftragten zu nennen.

Das Bundesdatenschutzgesetz sieht vor, dass sich jedermann an den betrieblichen Datenschutzbeauftragten einer nichtöffentlichen Stelle wenden kann. Den Betroffenen, die hiervon Gebrauch machen wollen, wäre allerdings die Möglichkeit zur Wahrnehmung dieses ihnen Kraft Gesetzes zustehenden Rechts genommen, wenn ihnen das Unternehmen nicht die dafür erforderlichen Kontaktdaten mitteilen würde.

Die Geheimhaltung der Kontaktdaten lässt sich auch nicht damit rechtfertigen, dass das Unternehmen vermeiden wollte, dass der betriebliche Datenschutzbeauftragte, der dieser Tätigkeit von einem an seiner Privatanschrift geführten Büro aus nachgeht, unter den mitgeteilten Erreichbarkeitsdaten quasi „rund um die Uhr“ in Anspruch genommen werden könne. Dem kann jedoch Rechnung getragen werden, wenn der Beauftragte für den Datenschutz für diese Aufgabe nicht seine private Telefonnummer verwendet, sodass sich die für den Beauftragten für den Datenschutz bestimmten Anrufe von den privaten unterscheiden lassen. Entsprechendes kann auch für andere Kommunikationswege wie Briefpost, Fax oder E-Mail realisiert werden.

Das Unternehmen hat daraufhin die Kontaktdaten für eine schriftliche wie auch eine elektronische Kontaktaufnahme zu dem Beauftragten für den Datenschutz in seinem Internetangebot veröffentlicht.