Landtag von Baden-Württemberg **Drucksache 13 / 40**

13. Wahlperiode **02. 07. 2001**

Mitteilung

des Innenministeriums

Erster Tätigkeitsbericht des Innenministeriums zum Datenschutz im nichtöffentlichen Bereich

Schreiben des Innenministeriums vom 28. Juni 2001 Nr. 2-0552.6/21:

In der Anlage zu diesem Schreiben übersende ich Ihnen den Ersten Tätigkeitsbericht des Innenministeriums zum Datenschutz im nichtöffentlichen Bereich, der nach § 39 des Landesdatenschutzgesetzes dem Landtag zu erstatten ist.

Dr. Schäuble

Innenminister

Eingegangen: 02. 07. 2001 / Ausgegeben: 18. 07. 2001

Datenschutz im nichtöffentlichen Bereich

Erster Tätigkeitsbericht des Innenministeriums nach § 39 des Landesdatenschutzgesetzes

2001

Erster Bericht des Innenministeriums über die Tätigkeit der Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich

Das Innenministerium hat bereits in der Vergangenheit in größeren Zeitabständen, zuletzt 1995, Tätigkeitsberichte zur Information der Bürger und der Unternehmen der Privatwirtschaft herausgegeben. Die Tätigkeitsberichte beruhten nicht auf gesetzlichen Vorgaben.

Der Landesgesetzgeber hat im Gesetz zur Änderung des Landesdatenschutzgesetzes und anderer Gesetze vom 23. Mai 2000 (GBl. S. 450) in Umsetzung einer entsprechenden Regelung der EG-Datenschutzrichtlinie eine Verpflichtung des Innenministeriums aufgenommen, dem Landtag zum 1. Juli eines jeden zweiten Jahres, beginnend ab 2001, einen zu veröffentlichenden Bericht über die Tätigkeit der für den Datenschutz im nichtöffentlichen Bereich zuständigen Aufsichtsbehörde zu erstatten (§ 39 des Landesdatenschutzgesetzes – LDSG –).

Das Innenministerium erstattet nachfolgend seinen ersten Tätigkeitsbericht nach § 39 LDSG. Dieser Bericht umfasst – wie die künftigen Berichte auch – die Tätigkeit der zuständigen Aufsichtsbehörde über zwei Jahre (hier die Jahre 1999 und 2000). Zu immer wiederkehrenden Problemen und Fragen der Bürger und nichtöffentlichen Stellen wird dabei ausführlich Stellung genommen, um auch im Hinblick auf künftige Berichte eine Grundlage zu schaffen. Die Gliederung nach Themenschwerpunkten erleichtert die Nutzung als Nachschlagewerk. Zum besseren Verständnis der Funktionsweise des Internets, seiner Gefahren für das Persönlichkeitsrecht und der möglichen Gefahrenminimierung gibt der Bericht darüber hinaus im Kapitel: Technik, Organisation und Teledienste eine umfassende allgemeine Darstellung.

Der Bericht verweist punktuell auf die „Hinweise zum Datenschutz für private Unternehmen und Organisationen (HIM)“, die das Innenministerium im Rahmen seiner umfangreichen Beratungstätigkeit jährlich veröffentlicht. Sie sollen ebenfalls dazu beitragen, bereits im Vorfeld datenschutzrechtliche Probleme zu erkennen und zu lösen. Für die Bürger wurde ein Serviceheft mit Musterbriefen zu Fragen des Datenschutzes aufgelegt. Die Hinweise ab Nr. 30, das Serviceheft und weitere Informationen werden – wie auch dieser Bericht – im Internet angeboten (www.im.bwl.de).

Der Bericht betrifft die Jahre 1999 und 2000 und die damaligen Rechtsgrundlagen. Darüber hinaus werden aber bereits punktuell auch die seit dem 23. Mai 2001 geltende Novelle des Bundesdatenschutzgesetzes (BDSG) sowie die geplanten weiteren Änderungen angesprochen. Das novellierte BDSG führt zwar in etlichen Punkten zu Verbesserungen für die Bürger, ändert aber nicht die wesentlichen Grundstrukturen und Regelungsinhalte des Gesetzes.

Inhaltsverzeichnis

		Seite
1.	**Datenschutz und Aufsicht im nichtöffentlichen Bereich**	**7**
1.1	Aufgaben des Innenministeriums auf dem Gebiet des Datenschutzes im nichtöffentlichen Bereich	7
1.2	Aufsicht im nichtöffentlichen Bereich	8
1.3	Aufsicht in Zahlen	10
1.3.1	Datenschutzregister	10
1.3.2	Anfragen, Eingaben und Anlasskontrollen	11
1.3.3	Schwerpunktmäßige Sonderüberprüfungen, Regelüberprüfungen	13
1.4	Ordnungswidrigkeitenverfahren	13
1.5	Rechtsgrundlagen, weitere Entwicklungen	15
1.6	Prüfungs- und Fortentwicklungsbedarf einzelner Regelungen	17
1.7	Aufgaben des Innenministeriums auf dem Gebiet des Datenschutzes im öffentlichen Bereich	18
1.8	Abgrenzung zum öffentlichen Bereich	19
2.	**Technik, Organisation und Teledienste**	**20**
2.1	Internet und Datenschutz	20
2.1.1	Surfen im Web	22
2.1.2	Einsatz von Cookies	23
2.1.3	Hacker nutzen Schlupflöcher im Internet	25
2.1.4	Bestellung per Maustaste	26
2.1.5	Umgang mit elektronischer Post	28
2.1.6	Zukünftige technische Entwicklung	30
2.2	Einzelne Teledienste	31
2.2.1	Internetzugang	31
2.2.2	Internetportal	32
2.2.3	Kostenlose E-Mail-Postfächer	33
2.2.4	Konzernunternehmen als Teledienstanbieter	33
2.3	Technischer und organisatorischer Datenschutz	36
2.3.1	Datenspeicherung im Mobiltelefon	36
2.3.2	Datenübermittlung beim Austausch von Computerfestplatten	37
2.3.3	Übermittlung fremder Kontoauszüge durch einen Kontoausdrucker	38
2.4	Auftragsdatenverarbeitung	39
2.4.1	Öffentlich zugängliche Bankkundendaten	39
2.4.2	Überprüfung von Zustelladressen	40
2.5	Videoüberwachung	41
3.	**Auskunfteien und Kreditschutzorganisationen**	**43**
3.1	Datenerhebung und Datenübermittlung durch Auskunfteien und Kreditschutzorganisationen	43
3.2	Besondere Fälle der Datenspeicherung bei Auskunfteien	45

3.3	Personenverwechslung	45
3.4	SCHUFA-Score-Wert	46
3.5	Kosten für die Selbstauskunft	49
3.6	Prüfungen bei Auskunfteien	50
3.7	Auskunftssystem auf Internetbasis	51
4.	**Kreditwirtschaft**	**53**
4.1	Bankenfusion und der Schutz von Kundendaten	53
4.2	Ausweiskopie bei Kontoeröffnung oder Identifizierung nach dem Geldwäschegesetz	55
4.3	Offenlegung der wirtschaftlichen Verhältnisse gegenüber Kreditinstituten	57
4.4	Kundenbefragungen durch Kreditinstitute	57
4.5	SCHUFA-Abfrage ohne berechtigtes Interesse	59
4.6	Einschaltung von Detekteien zur Schuldnerermittlung	60
4.7	Datenübermittlung an Partnerunternehmen	61
4.8	Telefon-Servicecenter für Banken	61
4.9	Datenübermittlung bei Forderungsabtretung	63
4.10	Depotnummer und Depotinhaber im Adressfeld	64
5.	**Handel und Dienstleistungen**	**65**
5.1	Abwicklung des bargeldlosen Einkaufs	65
5.2	Erfassung von Personalausweisdaten bei elektronischen Lastschriftverfahren	67
5.3	Speicherung von Einkaufsdaten bei Kundenkarteninhabern	67
5.4	Nahverkehrsfahrscheine auf der Chipkarte	68
5.5	Speicherung von Kundendaten in Fitnesscentern	69
5.6	Adressermittlung über die Telefonnummer	70
5.7	Gebäudebilddatenbank	70
6.	**Versicherungswirtschaft**	**72**
6.1	Finanzdienstleistungsklausel bei Fusion oder Verbund von Versicherung und Bank	72
6.2	Informationsaustausch bei Wechsel des Versicherungsunternehmens in der privaten Krankenversicherung	74
6.3	Übermittlung von Versichertendaten in die USA im Rahmen der Entschädigung von Holocaust-Opfern	75
6.4	Hinweis- und Warnsysteme der Versicherungen	76
6.5	Übermittlung von Daten an Ehegatten	77
7.	**Werbewirtschaft**	**79**
7.1	Adresshandel und Direktwerbung	79
7.2	Rechte der Betroffenen	81
7.3	Konsumentenbefragung mittels Fragebogen	83
7.4	Verwendung von Kfz-Daten für Werbezwecke	85

8.	**Arbeitnehmer-Datenschutz**	**86**
8.1	Angaben über Arbeitnehmer im Internet	86
8.2	Bekanntgabe von Abwesenheitszeiten von Arbeitnehmern am schwarzen Brett	87
8.3	Abrechnung von Mobiltelefon-Kosten bei erlaubter Privatnutzung	87
8.4	Bewerbung über eine Personalagentur	88
9.	**Gesundheitswesen**	**90**
9.1	Elektronische Vernetzung der Ärzte	90
9.2	Weitergabe von Patientendaten	91
9.3	Bonitätsprüfung vor ärztlicher Behandlung	92
9.4	Verarbeitung und Archivierung von Patientendaten außerhalb des Krankenhauses	92
9.5	Schutz der Patientendaten in der Apotheke	93
9.6	Einsicht in Patientenunterlagen	93
9.7	Information von Angehörigen durch den Krankenhausarzt	94
9.8	Erhebung und Verarbeitung von Praxisdaten	94
10.	**Verbände, Vereine, Parteien und Gewerkschaften**	**96**
10.1	Wohnungswesen und Mieterdatenschutz	96
10.1.1	Benennung einer Wohnung als Vergleichsobjekt im Mieterhöhungsverfahren	96
10.1.2	Übermittlung von Daten durch den Wohnungsverwalter an die Wohnungseigentümer	98
10.1.3	Übermittlung von Verbrauchsdaten des Mieters durch Energieversorgungsunternehmen an den Vermieter	98
10.2	Datenverarbeitung in Vereinen	98
10.2.1	Bekanntgabe von Mitgliederdaten innerhalb des Vereins	100
10.2.2	Bekanntgabe von Mitgliederdaten für Werbezwecke	102
10.2.3	Veröffentlichung von Daten	103
10.2.4	Wahrung des Datengeheimnisses	106
Anhang – Begriffsbestimmungen		**107**

1. Datenschutz und Datenaufsicht im nichtöffentlichen Bereich

1.1 Aufgaben des Innenministeriums auf dem Gebiet des Datenschutzes im nichtöffentlichen Bereich

Innenministerium als Aufsichtsbehörde

Das Innenministerium ist nach § 38 des Bundesdatenschutzgesetzes (BDSG) in Verbindung mit § 1 der Datenschutzzuständigkeitsverordnung der Landesregierung vom 10. Januar 1978 zuständige *Aufsichtsbehörde* für den Datenschutz *im nichtöffentlichen Bereich*. Es hat in dieser Funktion die Aufgabe, die Ausführung des BDSG und anderer Vorschriften über den Datenschutz durch die nichtöffentlichen Stellen zu überprüfen und zu überwachen. Die Berichtspflicht bezieht sich ausschließlich auf diese Tätigkeit.

Schwerpunkte dieser Tätigkeit waren im Berichtszeitraum insbesondere die Prüfung der Teledienstanbieter (Ziff. 2.2.1 bis 2.2.3), die Sicherstellung des Schutzes der Kundendaten bei Fusionen und einer datenschutzgerechten Einführung von so genannten Finanzdienstleistungsklauseln bei Fusionen oder Verbünden von Versicherungen und Banken (Ziff. 4.1 und 6.1) sowie die datenschutzgerechte Ausgestaltung von Fragebogen für Konsumentenbefragungen (Ziff. 7.3).

Die Aufsichtsbehörde sieht ihre Aufgabe im Datenschutz im nichtöffentlichen Bereich nicht allein auf den Aspekt Datenschutz beschränkt. Vielmehr ist sie sich stets bewusst, dass der Datenschutz als Teilbereich in größere Zusammenhänge eingebettet ist. Allgemein gilt, dass der Datenschutz nicht isoliert für sich betrachtet werden darf. Insbesondere im modernen Wirtschaftsleben zeigt es sich immer wieder, wie wichtig es ist, in einem konstruktiven Dialog mit den Beteiligten praktikable und sachgerechte Lösungen zu entwickeln, die in Übereinstimmung mit den geltenden gesetzlichen Regelungen einerseits den Datenschutz und die Belange des Einzelnen hinreichend wahren und andererseits die Tätigkeit der Wirtschaft allgemein und von Unternehmen im Besonderen unter Nutzung der gesetzlichen Gestaltungsspielräume unterstützen. Ziel der Aufsichtsbehörde ist es deshalb, den Datenschutz und das Verständnis für seine Notwendigkeit durch eine konstruktive Zusammenarbeit mit der Wirtschaft, den Unternehmen, aber auch mit allen anderen Institutionen wie Vereinen und Verbänden zu fördern. In diesem Bemühen um Kooperation lässt sich am ehesten gewährleisten, dass sinnvolle Abgrenzungen zwischen zulässigen Datenverarbeitungen und solchen Datenverarbeitungen, die das Persönlichkeitsrecht der Betroffenen über Gebühr beeinträchtigen, gefunden werden können. Mit diesem Ansatz kann nach Auffassung der Aufsichtsbehörde auch am Besten die Akzeptanz für die Belange des Datenschutzes im allgemeinen Bewusstsein verankert werden.

Innenministerium als oberste Aufsichtsbehörde

Das Innenministerium ist daneben *oberste Aufsichtsbehörde* für den Datenschutz im *nichtöffentlichen Bereich*. In dieser Funktion nahm es Stellung zu zahlreichen datenschutzrechtlichen Regelungen auf EU- und Bundesebene, wie beispielsweise zu

- der Telekommunikations-Datenschutzverordnung,
- dem Gesetz über die rechtlichen Rahmenbedingungen für den elektronischen Geschäftsverkehr,
- dem Namensaktiengesetz,
- der Verwertung von Genomanalysen in der Privatwirtschaft,
- der EG-Verordnung zur Durchführung der in Artikeln 81 und 82 EG-Vertrag niedergelegten Wettbewerbsregelungen zur Änderung bestehender EWG-Verordnungen und
- der Datenschutzkonvention.

Im Vordergrund stand hier die Mitwirkung am Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18. Mai 2001 (BGBl. I S. 904), durch das die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung per-

sonenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie) in Bundesrecht umgesetzt sowie der Datenschutz punktuell weiterentwickelt wurde.

Düsseldorfer Kreis

Um, insbesondere auch im Interesse der Wirtschaft bundesweit eine möglichst einheitliche Rechtsanwendung der datenschutzrechtlichen Vorschriften für den nichtöffentlichen Bereich zu erreichen, haben die Länder ein Gremium der *obersten Aufsichtsbehörden* für den Datenschutz im nichtöffentlichen Bereich, den *„Düsseldorfer Kreis“*, eingerichtet. Mitglieder des Düsseldorfer Kreises sind mehrheitlich Vertreter der obersten Aufsichtsbehörden der Länder, so auch das Innenministerium Baden-Württemberg, teilweise entsprechend beauftragte Vertreter der Landesdatenschutzbeauftragten, soweit sie zuständige Aufsichtsbehörde für den nichtöffentlichen Bereich sind, sowie der Bundesbeauftragte für den Datenschutz, der bundesweit für den Telekommunikationsbereich zuständig ist. Die Beschlüsse des Düsseldorfer Kreises werden von den Arbeitsgruppen „Kreditwirtschaft“, „Auskunfteien“, „Versicherungswirtschaft“, „Tele- und Mediendienste“ und „Internationaler Datenverkehr“ vorbereitet. Das Innenministerium ist in allen diesen Arbeitsgruppen vertreten, in der Arbeitsgruppe „Auskunfteien“ führt es für den Bereich der Kreditschutzorganisation „SCHUFA“ den Vorsitz. Der Düsseldorfer Kreis tagt zweimal jährlich, die Arbeitsgruppen nach Bedarf ein- bis zweimal jährlich.

1.2 Aufsicht im nichtöffentlichen Bereich

Das Kontrollsystem des BDSG ist zweistufig angelegt. Dieses System wird durch die Novelle des BDSG vom 18. Mai 2001 nicht aufgegeben, sondern auf beiden Stufen gestärkt.

Eigenverantwortung und Selbstkontrolle

An erster Stelle stehen die Eigenverantwortung und die Selbstkontrolle durch die Privatwirtschaft. Die Vorschriften des BDSG und anderer datenschutzrechtlicher Vorschriften sind von der Privatwirtschaft in eigener Verantwortung anzuwenden. Behördliche Genehmigungen oder Zulassungen sind dem bisherigen BDSG fremd, das novellierte BDSG führt auch nur einen Genehmigungsvorbehalt beschränkt auf bestimmte Datentransfers in Drittstaaten ein.

Als *Instrument* der Selbstkontrolle hat der Gesetzgeber in §§ 36 und 37 des bisherigen BDSG die Einrichtung der *betrieblichen Datenschutzbeauftragten* geschaffen. Danach hat jede nichtöffentliche Stelle einen Datenschutzbeauftragten zu bestellen, wenn sie personenbezogene Daten verarbeitet und damit

– mindestens fünf Arbeitnehmer bei einer automatisierten Datenverarbeitung oder
– mindestens 20 Arbeitnehmer bei einer Datenverarbeitung auf andere Weise ständig beschäftigt.

Aufgabe des betrieblichen Datenschutzbeauftragten ist es, die Ausführung des BDSG und anderer Vorschriften des Datenschutzes im Unternehmen sicherzustellen.

Nach dem novellierten BDSG ist ein betrieblicher Datenschutzbeauftragter unabhängig von der Zahl der mit der Verarbeitung personenbezogener Daten beschäftigten Arbeitnehmer zusätzlich auch dann zu bestellen, wenn das Unternehmen

– personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung oder der anonymisierten Übermittlung erhebt, verarbeitet oder nutzt oder
– eine automatisierte Verarbeitung personenbezogener Daten, die mit besonderen Risiken für die Rechte und Freiheiten der davon Betroffenen verbunden ist, vorsieht oder durchführt, für die wegen dieser besonderen Risiken eine Vorabkontrolle durchzuführen ist. Zuständig für die Vorabkontrolle ist der betriebliche Datenschutzbeauftragte.

Staatliche Kontrolle

Ergänzt wird die betriebliche Selbstkontrolle durch die *Aufsichtsbehörden* für den Datenschutz im nichtöffentlichen Bereich, in Baden-Württemberg das Innenminis-

terium. Es hat die Ausführung des BDSG und anderer spezialgesetzlicher Vorschriften über den Datenschutz, des Teledienstedatenschutzgesetzes (TDDSG) und des Mediendienste-Staatsvertrags zu überprüfen.

Das bisherige BDSG differenziert für die Überprüfung nichtöffentlicher Stellen in Stellen, die der Vollkontrolle, und Stellen, die der Anlasskontrolle unterliegen.

– Der *Vollkontrolle* oder anlassunabhängigen Aufsicht unterliegen nach § 38 Abs. 2 BDSG nichtöffentliche Stellen, die geschäftsmäßig personenbezogene Daten zum Zwecke der Übermittlung oder der anonymisierten Übermittlung speichern oder im Auftrag als Dienstleistungsunternehmen verarbeiten, wie Auskunfteien, Adressverlage, Markt- und Meinungsforschungsinstitute, Dienstleistungsrechenzentren und Datenerfassungsbüros. Der Vollkontrolle unterliegen auch Tele- und Mediendiensteanbieter.

– Alle anderen Daten verarbeitenden nichtöffentlichen Stellen unterliegen der *Anlassaufsicht* nach § 38 Abs. 1 BDSG. Sie können nur dann überprüft werden, wenn der Aufsichtsbehörde im Einzelfall hinreichende Anhaltspunkte für eine Verletzung des BDSG oder anderer spezialgesetzlicher datenschutzrechtlicher Vorschriften vorliegen.

Rechte der Aufsichtsbehörde

Zur Ausübung der Aufsicht stehen der Aufsichtsbehörde nach § 38 Abs. 3 und 4 BDSG ein *Auskunftsrecht* gegenüber der nichtöffentlichen Stelle sowie ein *Betretungsrecht* des Grundstücks und der Geschäftsräume der nichtöffentlichen Stelle und ein *Einsichtsrecht* in geschäftliche Unterlagen, die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme zu. Ein Verstoß gegen diese Vorschriften ist bußgeldbewehrt (siehe Ziff. 1.4).

Nur bei technischen und organisatorischen Mängeln kann die Aufsichtsbehörde unter den engen Voraussetzungen des § 38 Abs. 5 BDSG ausnahmsweise die Beseitigung der Mängel durch Verwaltungsakt anordnen und gegebenenfalls den Einsatz einzelner Verfahren untersagen. Auf festgestellte Verstöße gegen datenschutzrechtliche Vorschriften kann die Aufsichtsbehörde die nichtöffentlichen Stellen deshalb grundsätzlich nur hinweisen und um Abhilfe bitten. Gravierende Verstöße werden beanstandet. Ob die nichtöffentliche Stelle den Mangel beseitigt oder nicht, bleibt ihr überlassen. Ist sie dazu nicht bereit oder hat der Betroffene durch die Verarbeitung seiner personenbezogenen Daten einen Schaden erlitten, bleibt ihm nur die Beschreitung des Zivilrechtswegs. Hat die nichtöffentliche Stelle den Straftatbestand des bisherigen § 43 BDSG verletzt, kann der Betroffene, nicht jedoch die Aufsichtsbehörde, einen Strafantrag stellen. Bestimmte Verstöße gegen datenschutzrechtliche Vorschriften kann das Innenministerium nach dem bisherigen § 44 BDSG durch Erlass eines Bußgeldbescheides mit bis zu 50 000 DM ahnden.

Das novellierte BDSG stärkt die Aufsichtsbehörde durch

– den Wegfall der Anlasskontrolle mit der Folge, dass alle nichtöffentlichen Stellen der Vollkontrolle unterliegen,

– die Einräumung eines eigenen Strafantragsrechts sowie

– eine wesentliche Erweiterung der Bußgeldtatbestände.

Inwieweit die Änderungen des Kontrollsystems, die Aufwertung der dezentralen Selbstkontrolle einerseits und die Stärkung der Position der Aufsichtsbehörde andererseits, Auswirkungen auf den Kontrollumfang haben wird, bleibt abzuwarten. Angesichts der vorhandenen personellen Ressourcen wird die Überprüfungstätigkeit der Aufsichtsbehörde – im Wesentlichen wie bisher – vorrangig anlassbezogen und nach Schwerpunkten durchzuführen sein. Auch wenn sich die Unternehmen in der weit überwiegenden Mehrzahl der Fälle kooperativ zeigen, so wird die Stärkung der Stellung der Aufsichtsbehörde jedenfalls in den immer wieder auftretenden Problemfällen zu einer wirkungsvolleren Zusammenarbeit beitragen können.

Beratung

Korrespondierend mit der betrieblichen Selbstkontrolle nimmt die Aufsichtsbehörde in großem Umfang *Beratungstätigkeiten* wahr. Ihnen kommt ganz erhebliche Bedeutung zu, da durch sie in vielen Fällen bereits im Vorfeld datenschutz-

rechtliche Probleme gelöst werden können und nicht erst im Nachhinein auf Grund von Überprüfungen und gegebenenfalls Beanstandungen bereinigt werden müssen. Zumindest für das erste Jahr nach In-Kraft-Treten des novellierten BDSG ist von einem zusätzlichen, erheblichen Beratungs- und Informationsbedarf der Privatwirtschaft auszugehen.

Zur Unterstützung der privaten Wirtschaft bei der Lösung datenschutzrechtlicher Fragen gibt das Innenministerium jährlich *Hinweise zum Datenschutz für private Unternehmen und Organisationen* (HIM) heraus, die die während des Jahres aufgetretenen besonderen Problemstellungen behandeln. Die HIM wurden bis Nr. 38 im Staatsanzeiger veröffentlicht; ab Nr. 30 können sie im Internet auf den Seiten „Datenschutz" des Innenministeriums unter der Adresse „www.im.bwl.de" abgerufen werden.

Die Neuregelungen für den Datentransfer ins Ausland werden ein besonderer Schwerpunkt der künftigen Beratungstätigkeit der Aufsichtsbehörde sein. Um die Unternehmen rechtzeitig auf die neue Rechtslage einzustellen und ihnen die Anwendung der neuen Normen zu erleichtern, wurde diese Thematik bereits im Vorfeld zusammen mit international tätigen Unternehmen mit Sitz in Baden-Württemberg aufgegriffen und beraten. Den Vorsitz des dazu gegründeten Arbeitskreises *„Datenweitergabe ins Ausland"* hatte das Innenministerium. Das Ergebnis der Beratung ist in einem Arbeitspapier des Arbeitskreises „Datenweitergabe ins Ausland" vom Mai 2000 unter dem Thema „Datenübermittlung ins Ausland, insbesondere innerhalb internationaler Konzerne" zusammengefasst. Zusätzlich hat die Aufsichtsbehörde in ihren HIM Nr. 39 vom 25. Januar 2001 unter dem Thema „Übermittlung personenbezogener Daten im internationalen Bereich" die auf die jeweiligen Fallkonstellationen anzuwendenden Regelungen systematisch dargestellt. Das Arbeitspapier „Datenübermittlung ins Ausland, insbesondere innerhalb internationaler Konzerne" und die HIM Nr. 39 können ebenfalls im Internet auf den Seiten „Datenschutz" des Innenministeriums unter der Adresse „www.im.bwl.de" abgerufen werden.

Um frühzeitig datenschutzrechtliche Probleme der Wirtschaft zu erkennen und als Ansprechpartner für die Wirtschaft präsent zu sein, nimmt die Aufsichtsbehörde auch an den Sitzungen der von den Industrie- und Handelskammern ins Leben gerufenen *Erfahrungskreise für den Datenschutz* (ERFA-Kreise) teil.

1.3 Aufsicht in Zahlen

1.3.1 Datenschutzregister

Nach § 32 BDSG haben die Stellen, die geschäftsmäßig personenbezogene Daten zum Zwecke der Übermittlung nach § 29 BDSG oder der anonymisierten Übermittlung nach § 30 BDSG speichern oder nach § 11 BDSG im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen, die *Aufnahme und Beendigung ihrer Tätigkeit* innerhalb eines Monats *der Aufsichtsbehörde*, in deren Zuständigkeitsbereich sich der Sitz der Firma befindet, *mitzuteilen.* Die Aufsichtsbehörde führt dazu nach § 38 Abs. 2 Satz 2 BDSG ein Register.

Am 31. Dezember 2000 waren im *Register* der Aufsichtsbehörde 1352 meldepflichtige Unternehmen erfasst.

– Mit 1258 haben den größten Anteil daran die nach § 32 Abs. 1 Nr. 3 BDSG gemeldeten Unternehmen, die im Auftrag Dritter als Dienstleistungsunternehmen weisungsgebunden i. S. d. § 11 BDSG personenbezogene Daten verarbeiten oder nutzen. Darunter fallen Konzern- und Dienstleistungsrechenzentren, Datenerfassungsbüros, Mikrofilm-Serviceunternehmen, Datenträgervernichter sowie Lettershops und ähnliche Unternehmen aus dem Bereich des Direktmarketings. Nach dem Entwurf des novellierten BDSG werden diese Unternehmen künftig nicht mehr meldepflichtig sein.

– Den zweitgrößten Anteil am Melderegisterbestand mit 65 Meldungen haben die nach § 32 Abs. 1 Nr. 1 BDSG meldepflichtigen Unternehmen, die personenbezogene Daten zum Zwecke der Übermittlung speichern. Bei diesen nach § 29 BDSG tätigen Unternehmen handelt es sich um Adressbuchverlage und Auskunfteien sowie Kreditschutzorganisationen.

– Mit 29 Registereintragungen haben die nach § 32 Abs. 1 Nr. 2 BDSG meldepflichtigen Unternehmen der Markt- und Meinungsforschung, die nach § 30

BDSG personenbezogene Daten zum Zwecke der anonymisierten Übermittlung speichern, den geringsten Anteil.

Im Berichtszeitraum gab es rund 1 000 *Änderungsmeldungen* zu Registereintragungen. Die häufigsten Gründe dafür waren Änderungen bei den meldepflichtigen Angaben zur Geschäftsleitung und zum betrieblichen Datenschutzbeauftragten sowie zur Anschrift des UnternehmenS. Aber auch Löschungen aus dem Register waren in nicht geringem Umfange zu verzeichnen.

In regelmäßigen Abständen wurden die zum Register gemeldeten Unternehmen im Hinblick auf die gemeldeten Angaben in schriftlicher Form überprüft. Dabei waren nur in wenigen Fällen Verstöße gegen die Meldepflicht festzustellen.

1.3.2 Anfragen, Eingaben und Anlasskontrollen

Die Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich überprüft nach § 38 Abs. 1 BDSG im Einzelfall die Ausführungen des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die Verarbeitung oder Nutzung personenbezogener Daten in oder aus Dateien regeln, wenn ihr hinreichende Anhaltspunkte dafür vorliegen, dass eine dieser Vorschriften durch eine nichtöffentliche Stelle verletzt ist, insbesondere wenn es Betroffene selbst begründet darlegen.

Telefonische Anfragen

Aber auch die Beratungsfunktion der Aufsichtsbehörde ist in immer stärkerem Maße gefragt. So gingen im Berichtszeitraum bei den Mitarbeiterinnen und Mitarbeitern der Aufsichtsbehörde rund 4000 telefonische Anfragen ein. In der weit überwiegenden Anzahl der Fälle war eine telefonische Information und Beratung über die Rechtslage ausreichend. In den anderen Fällen war eine schriftliche Vorlage unter Anschluss der entsprechenden Unterlagen erforderlich, um den Sachverhalt bei den betroffenen Stellen überprüfen und eine datenschutzrechtliche Bewertung abgeben zu können.

Schriftliche Anfragen und Eingaben

Neben den telefonischen Anfragen sind auch rund 1 000 schriftliche Anfragen – zunehmend auch per E-Mail – eingegangen.

Rund 220 der schriftlichen Eingaben betrafen die Aktion einer Firma aus Niedersachsen, die derzeit eine Gebäudedatenbank von größeren Städten anlegt. Zuständigkeitshalber wurden die Eingaben an die Aufsichtsbehörde in Niedersachsen abgegeben und die Betroffenen mit einer – mit Niedersachsen abgestimmten – kurzen datenschutzrechtlichen Beurteilung darüber unterrichtet.

In rund 540 dieser *schriftlichen Eingaben* wandten sich betroffene Bürger an die Aufsichtsbehörde, weil sie im Umgang mit ihren personenbezogenen Daten einen Datenschutzverstoß annahmen.

Im Einzelnen betrafen diese Eingaben

- in 68 Fällen Auskunfteien,
- in 67 Fällen Einzel-, Groß- und Versandhandel und Energieversorgungsunternehmen (die weit überwiegende Anzahl der Fälle betraf die Nutzung und Weitergabe von Daten für Werbezwecke),
- in 58 Fällen Markt- und Meinungsforschungsinstitute (47 Fälle davon betrafen eine zweimal jährlich durchgeführte bundesweite Verbraucherbefragung),
- in 44 Fällen Kreditinstitute, Banken und Bausparkassen,
- in 43 Fällen Versicherungsgesellschaften (rund die Hälfte der Fälle betrafen die Aktualisierung von Einwilligungserklärungen anlässlich der Fusion von Versicherungsunternehmen – auch mit Kreditunternehmen),
- in 33 Fällen die Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA),
- in 33 Fällen das Gesundheitswesen,
- in 32 Fällen den Datenschutz in Arbeitsverhältnissen,

- in 31 Fällen Unternehmen des Adresshandels sowie der Direktmarketing- und Werbebranche,
- in 17 Fällen Vereine, Parteien und sonstige Interessengemeinschaften,
- in 12 Fällen Adressbuchverlage und Herausgeber öffentlicher Verzeichnisse,
- in 8 Fällen Vermieter, Hausverwaltungen und Mietervereine,
- in 8 Fällen Tele- und Mediendienste,
- in 2 Fällen Berufe mit besonderer Schweigepflicht,
- in 2 Fällen Presse und Printmedien,
- in 78 Fällen sonstige Unternehmensbereiche (z. B. Verkehrsbetriebe, Kreditkarten- und Rabattkartenunternehmen, Videoüberwachung).

Anlasskontrollen

In rund 240 dieser Fälle lagen auf Grund der Sachverhaltsschilderungen und den vorgelegten Unterlagen *Anhaltspunkte für einen Verstoß* gegen datenschutzrechtliche Bestimmungen vor, so dass eine anlassbezogene Überprüfung nach § 38 Abs. 1 BDSG bei den Daten verarbeitenden Stellen erforderlich wurde. Diese Überprüfungen wurden vornehmlich auf schriftlichem Wege durchgeführt. Nur in zwei Fällen bestand Veranlassung für eine Überprüfung vor Ort.

In rd. 70 v. H. dieser Fälle ergab die Überprüfung nach der Sachverhaltsaufklärung keine *datenschutzrechtlichen Verstöße*, in rund 30 v. H. der Fälle allerdings waren die Beschwerden begründet. Die festgestellten unzulässigen Datenverarbeitungen und anderen Verstöße gegen Vorschriften des Datenschutzes sowie des Rechts der Tele- und Mediendienste wurden gegenüber den Daten verarbeitenden Stellen beanstandet. In diesen Fällen wurden die betroffenen Bürger über ihre rechtlichen Möglichkeiten aufgeklärt.

Zu den häufigsten Mängeln zählten die Nichterfüllung des Auskunftsanspruchs über die gespeicherten personenbezogenen Daten in Werbeangelegenheiten. Es kam auch zu Personenverwechslungen auf Grund nicht ausreichender Identifizierung und Prüfung der Angaben, insbesondere im Bereich Auskunfteien und Kreditschutzorganisationen. Auch hinsichtlich der Erforderlichkeit einer schriftlichen Einwilligung zur Datenübermittlung wurde in einigen Fällen von falschen Voraussetzungen ausgegangen. Aber auch unzureichende technische und organisatorische Maßnahmen, die nach § 9 BDSG und der Anlage dazu zu treffen sind, gaben Anlass für einen nicht unerheblichen Anteil der Beanstandungen.

In den übrigen Fällen der schriftlichen Eingaben waren *keine Anhaltspunkte für Verstöße* gegen datenschutzrechtliche Bestimmungen ersichtlich und es konnte den Betroffenen mit einer Beratung geholfen werden. Bei diesen Anfragen handelte es sich vor allem um Angelegenheiten und Fragen von Bürgern, die keine ausreichenden Kenntnisse über die Rechtslage und Zulässigkeit von Datenverarbeitung hatten und darüber von der Aufsichtsbehörde aufgeklärt werden konnten. Oftmals handelte es sich dabei allerdings auch um Eingaben, aus denen ersichtlich war, dass die Betroffenen den Datenschutz als „letzten Ausweg“ ansahen und die dann mit dem Hinweis darauf, dass datenschutzrechtliche Bestimmungen auf ihren Fall nicht anwendbar sind, beschieden werden mussten. In einigen Fällen war der Datenschutz nur ein Begleitproblem für im Grunde andere Sachprobleme. Durch die Hinweise der Aufsichtsbehörde konnten den Betroffenen vielfach andere Wege zur Problemlösung aufgezeigt werden.

Stellungnahmen und Beratung

Neben den dargestellten Eingaben von Betroffenen betrafen rund 240 Fälle schriftliche Anfragen zu konkreten datenschutzrechtlichen Fragen. Im Vordergrund stand in den meisten Fällen die Bitte um *datenschutzrechtliche Stellungnahme* zu laufenden Verarbeitungsvorhaben sowie *Beratungen* im Vorfeld geplanter Vorhaben wie zum Beispiel der Fusion von Versicherungsunternehmen. Dabei nahmen auch Fragen zum internationalen Datenverkehr im Rahmen der Konzerndatenverarbeitung einen nicht unerheblichen Umfang ein. Hinsichtlich der zunehmenden Nutzung der Möglichkeiten des Internets waren auch Beratungen zu Geschäftsideen, die datenschutzrechtlich abgesichert werden sollten, in starkem Maße gefragt. Im Vordergrund standen dabei Fragen zur Zulässigkeit

und Sicherheit der Verarbeitung von Daten der Nutzer von Telediensten sowie zur Ausgestaltung von Hinweis- und Einwilligungstexten in den Firmen-Homepages.

Ein weiterer großer Anteil der Anfragen kam von *betrieblichen Datenschutzbeauftragten* oder *Betriebsräten*, die zur Meldepflicht des Unternehmens und zum Umgang mit Arbeitnehmerdaten um Auskunft baten. Vielfach ging es auch dabei um vorgesehene konzernweite Personaldatenverarbeitungen sowie um geplante betriebsinterne Bekanntgaben personenbezogener Daten von Arbeitnehmern und deren Veröffentlichung im Internet. Aber auch zur Position und Funktion des betrieblichen Datenschutzbeauftragten, bestand insbesondere bei kleinen und mittleren Unternehmen noch erheblicher Aufklärungsbedarf.

Es ist ein Trend festzustellen, dass Unternehmen für datenschutzrechtliche Fragen zunehmend sensibilisiert sind und sich deshalb frühzeitig hinsichtlich der datenschutzrechtlichen Anforderungen – auch im technischen Bereich – an die Aufsichtsbehörde wenden. Die Beratungstätigkeit der Aufsichtsbehörde war auch im Hinblick auf das novellierte BDSG im Vorfeld von geplanten Firmenprojekten sehr gefragt. Sie dürfte nach Verabschiedung des novellierten BDSG erheblich zunehmen.

1.3.3 Schwerpunktmäßige Sonderüberprüfungen, Regelüberprüfungen

Nach § 32 Abs. 1 BDSG meldepflichtige Unternehmen sowie Teledienstean-bieter unterliegen nach § 38 Abs. 2 BDSG bzw. § 8 Abs. 1 TDDSG der so genannten Vollkontrolle. Überprüfungen sind jederzeit, das heißt ohne Vorliegen hinreichender Anhaltspunkte für eine Verletzung datenschutzrechtlicher Vorschriften, zulässig.

Geprüft wurden im Berichtszeitraum *Auskunfteien*, *Telefon-Servicecenter* für Banken und *Teledienstean-bieter*. In der ersten Hälfte des Berichtszeitraums wurden drei Auskunfteien und drei Telefon-Servicecenter überprüft. In der zweiten Hälfte des Berichtszeitraums folgten Prüfungen bei Unternehmen, die Teledienste anbieten.

Überprüft wurden:

Auskunfteien	3 (siehe Ziff. 3.6 und 3.7)
Telefon-Servicecenter für Banken	3 (siehe Ziff. 4.8)
Zugangsanbieter	2 (siehe Ziff. 2.2.1)
Internetportal	1 (siehe Ziff. 2.2.2)
Kostenlose E-Mail-Postfächer	2 (siehe Ziff. 2.2.3).

Bei den Überprüfungen mussten in einzelnen Fällen datenschutzrechtliche Verstöße in den Verfahren sowie bei den technisch-organisatorischen Maßnahmen festgestellt werden. Zwischenzeitlich wurden aber für alle beanstandeten Maßnahmen datenschutzkonforme Lösungen gefunden.

1.4 Ordnungswidrigkeitenverfahren

Liegen der Aufsichtsbehörde Anhaltspunkte für eine Verletzung datenschutzrechtlicher Vorschriften vor, beispielsweise auf Grund einer Beschwerde, wird das betreffende Unternehmen in der Regel schriftlich unter Hinweis auf seine *Auskunftspflicht* nach § 38 Abs. 3 BDSG um Auskunft gebeten. Eine unangemeldete Überprüfung vor Ort nach § 38 Abs. 4 BDSG erfolgt ausnahmsweise dann, wenn wegen besonderer Umstände, insbesondere der Gefahr der spurenlosen Beseitigung des streitigen Datenbestandes, ein schriftliches Auskunftsverlangen nicht Erfolg versprechend erscheint.

Nach § 44 Abs. 1 Nr. 6 BDSG begeht eine bußgeldbewehrte *Ordnungswidrigkeit*, wer den sich aus § 38 Abs. 3 und 4 BDSG ergebenden Pflichten zuwiderhandelt, indem er eine Auskunft nicht, nicht richtig oder nicht rechtzeitig, d. h. unverzüglich erteilt oder den Zutritt zu den Grundstücken oder Geschäftsräumen, die Vornahme von Prüfungen oder Besichtigungen oder die Einsicht in geschäftliche Unterlagen nicht duldet.

Nicht selten werden von der Aufsichtsbehörde angeforderte Auskünfte von den Auskunftspflichtigen nicht fristgerecht oder zunächst unvollständig erteilt. Auf

entsprechende nochmalige Aufforderung und mit dem Hinweis darauf, dass dies eine Ordnungswidrigkeit darstellt, werden in der Regel dann die gewünschten Auskünfte erteilt. Insgesamt ist festzustellen, dass die meisten nichtöffentlichen Stellen sich gegenüber der Aufsichtsbehörde bei Fragen des Datenschutzes in aller Regel zur Mitwirkung bereit zeigen.

In zwei Fällen wurden wegen Verstoßes gegen die Mitwirkungspflichten Bußgelder in Höhe von 2000 DM und 5000 DM verhängt.

Nichtreaktion auf Auskunftsverlangen

Im ersten Fall wurden bei einem Unternehmen, bei dem auch private Adressdaten verarbeitet werden, nach einem Betriebsbesuch verschiedene datenschutzrechtliche Mängel beanstandet. Anschließend wurde mit Fristsetzung insbesondere um die Vorlage eines Datenschutz- und Sicherheitskonzepts gebeten. In diesem Zusammenhang bat die Aufsichtsbehörde auch darzulegen, inwieweit das Betriebsgebäude, in dem sich an vielen Stellen personenbezogene Daten befinden, bei Abwesenheit gesichert und überwacht werden kann. Außerdem wurde bei dem Betriebsbesuch beanstandet, dass die Mitarbeiter nicht nach §5 BDSG auf das Datengeheimnis verpflichtet sind. Es wurde darum gebeten, diese Verpflichtung nachzuholen und der Aufsichtsbehörde bis zu einer angemessenen Frist Auskunft über die erfolgten Verpflichtungen zu erteilen.

Trotz nochmaliger Aufforderung wurden die *Auskünfte nicht erteilt*. Ebenso wenig erfolgte eine Reaktion durch das Unternehmen im Zuge der Anhörung im Bußgeldverfahren. Daraufhin wurde ein Bußgeldbescheid erlassen, der auch bestandskräftig wurde.

Bestreiten der Überprüfungsvoraussetzungen

Im zweiten Fall verweigerte der Geschäftsführer eines so genannten Finanzdienstleistungsunternehmens bei einem *unangemeldeten Prüfbesuch vor Ort* sowohl die Erteilung der erforderlichen Auskünfte als auch die Einsicht in die geschäftlichen Unterlagen und Datenverarbeitungsprogramme. Obwohl er auf die Rechtslage hingewiesen wurde, *bestritt* er *pauschal* die *Berechtigung* der Aufsichtsbehörde zu ihrer Vorgehensweise und verwies ihre Vertreter des Gebäudes. Anlass für die unangemeldete Überprüfung vor Ort war die Beschwerde eines arbeitslosen und im Schuldnerverzeichnis eingetragenen Bürgers, der von dem ihm unbekannten Unternehmen einen direkt adressierten Werbebrief erhalten hatte, mit dem er beim Unternehmen einen „Antrag auf Schuldentilgung“ stellen sollte, dessen unbürokratische Bearbeitung (ohne SCHUFA-Auskunft etc.) in Aussicht gestellt wurde. Da in diesem Fall der Verdacht bestand, dass sich das Unternehmen unzulässigerweise Daten aus dem Schuldnerverzeichnis beschafft hat und bei Bekanntwerden des Beschwerdeführers die Gefahr bestand, dass der Datensatz spurenlos beseitigt wird, wurde von einem schriftlichen Verfahren und einer Ankündigung des Prüfbesuchs abgesehen.

Im Bußgeldverfahren und dem sich nach seinem Einspruch anschließenden gerichtlichen Verfahren bestritt der Geschäftsführer die Verletzung seiner Mitwirkungspflichten mit folgenden Argumenten:

– Ihm habe ein Aussageverweigerungsrecht – auch wegen der unangemeldeten Überprüfung vor Ort – zugestanden, da bei der Art und Weise einer solchen Kontrolle von einer Pflichtverletzung ausgegangen werden müsse.

– Hinreichende Anhaltspunkte für eine Überprüfung habe es nicht gegeben, da schon die Person des Beschwerdeführers zweifelhaft sei und entsprechende Daten rechtmäßig erhoben werden könnten (über den Adresshandel oder das Schuldnerverzeichnis).

– Die Überprüfung vor Ort sei unverhältnismäßig gewesen.

– Durch die Verweigerung der Aufsichtsbehörde, ihm Akteneinsicht in die Beschwerdeakte zu gewähren, sei das rechtliche Gehör verletzt worden.

Die Einwendungen waren insgesamt nicht haltbar.

Nach §38 Abs. 3 S. 2 BDSG besteht zwar ein *Auskunftsverweigerungsrecht* auf solche Fragen, deren Beantwortung den an sich Auskunftspflichtigen oder bestimmte Angehörige der Gefahr strafgerichtlicher Verfolgung oder eines Verfah-

rens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Ein Auskunftsverweigerungsrecht besteht aber nicht pauschal, sondern nur zu einzelnen Fragen, deren Beantwortung eine Verfolgungsgefahr auslösen könnte. Zudem muss es ausdrücklich erklärt werden. Ein Aussageverweigerungsrecht ergibt sich auch nicht aus der Art der Überprüfung. Zudem sieht § 38 Abs. 4 BDSG, der ebenfalls verletzt wurde, kein Auskunftsverweigerungsrecht vor.

Es bestand keinerlei Anlass, an den *Angaben* des *Beschwerdeführers* zu zweifeln. Auch für eine *rechtmäßige Datenerhebung* war nichts ersichtlich. Eine rechtmäßige Auskunft und Nutzung der Daten aus dem Schuldnerverzeichnis schied bereits auf Grund des streng geregelten Verfahrens aus, zumal die Nutzung ohnehin auf Zwecke der Zwangsvollstreckung beschränkt ist. Das für den Adresshandel bestehende Listenprivileg des § 28 Abs. 2 Nr. 1 b und § 29 Abs. 2 Nr. 1 b BDSG gilt für Listen arbeitsloser und/oder verschuldeter Personen deshalb nicht, da solche Listen, wenn sie zwei dieser Merkmale aufweisen, bereits schon aus diesem Grund unzulässig sind, und bei Ausweisung auch nur eines der genannten Merkmale diskriminierenden Charakter haben und deshalb Grund zur Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat.

In Fällen wie dem vorliegenden ist die *Überprüfung* vor Ort die angemessene, einzig erfolgversprechende Verfahrensweise und damit *verhältnismäßig*.

Über die angebliche *Verletzung des rechtlichen Gehörs* durch die Weigerung, Einsicht in die Beschwerdeakte zu gewähren, entschied das Amtsgericht durch Beschluss mit zwei Sätzen: „Die Akteneinsicht wurde im Hinblick auf Akten verweigert, die lediglich Anlass für ein Bußgeldverfahren mit anderem historischem Lebenssachverhalt und demnach nicht „verfahrensbezogen“ waren. Zu einer ordnungsgemäßen Verteidigung war die Kenntnis des Inhalts der verweigerten Akten nicht erforderlich.“

Zu einer gerichtlichen Entscheidung im Übrigen ist es nicht gekommen, da der Einspruch zurückgenommen wurde, nachdem der Richter in der Verhandlung deutlich zum Ausdruck gebracht hatte, dass er die Rechtsauffassung der Aufsichtsbehörde, auch die zu § 38 Abs. 4 BDSG, teilt und deshalb mit einer Verurteilung zu einem Bußgeld, das auch höher ausfallen könne, zu rechnen sei.

1.5 Rechtsgrundlagen, weitere Entwicklungen

Rechtsgrundlagen

Die wichtigsten Rechtsgrundlagen für den Datenschutz im nichtöffentlichen Bereich im Berichtszeitraum sind:

– Das bis zum 22. Mai 2001 geltende Bundesdatenschutzgesetz (BDSG)

  Das BDSG gilt für nichtöffentliche Stellen, z. B. Unternehmen der Privatwirtschaft (nichtöffentlicher Bereich) sowie für Behörden und sonstige öffentlichen Stellen des Bundes (öffentlicher Bereich). Die Regelungen für den nichtöffentlichen Bereich sind weniger restriktiv als für öffentliche Stellen, da sich im nichtöffentlichen Bereich, anders als im öffentlichen Bereich, die privaten Rechtsträger grundsätzlich gleichberechtigt gegenüberstehen und das grundrechtlich geschützte allgemeine Persönlichkeitsrecht zwischen Privaten keine unmittelbare Wirkung entfaltet. Geschützt ist das Persönlichkeitsrecht im nichtöffentlichen Bereich im BDSG nur, wenn Daten in oder aus Dateien (automatisiert oder manuell), nicht jedoch, wenn sie in Akten verarbeitet werden.

  Das BDSG ist das Hauptregelwerk des Datenschutzes für den nichtöffentlichen Bereich. Es stellt die Datenverarbeitung unter ein grundsätzliches Verbot mit Erlaubnisvorbehalt. Das bedeutet, dass alles verboten ist, was nicht ausdrücklich erlaubt ist. Es gilt jedoch nur soweit, als in anderen Gesetzen keine anderen datenschutzrechtlichen Regelungen getroffen sind;

– das Teledienstegesetz (TDG) und das Teledienstedatenschutzgesetz (TDDSG)

  Personenbezogene Daten, die im Zusammenhang mit der Nutzung von Telediensten im Sinne des TDG (z. B. Internetangebote, Telebanking, Telespiele, Warenangebote, Datendienste) stehen, sind nach den besonderen Vorschriften des TDDSG geschützt. Dieses Gesetz regelt den datenschutzgerechten Umgang mit den so genannten Bestands-, Nutzungs- und Abrechnungsdaten, also

denjenigen personenbezogenen Daten, die auf Grund der Wahl des Mediums anfallen.

Auf andere, über den Teledienst übermittelte personenbezogene Daten, die so genannten Inhaltsdaten, z. B. Daten eines Vertragsabschlusses zum Kauf von Waren, finden die Regelungen des BDSG Anwendung;

– das Telekommunikationsgesetz (TKG) und die Telekommunikations(dienste-unternehmen)-Datenschutzverordnung (TDSV)

Telekommunikation (z. B. Telefon, Internet) bedarf eines Übertragungsweges und damit einer entsprechenden technischen Infrastruktur. Das TKG reguliert die technische Infrastruktur Telekommunikation und die Frequenzordnung, die TDSV den datenschutzgerechten Umgang mit den personenbezogenen Daten der die Telekommunikationsinfrastruktur nutzenden Beteiligten;

– der Mediendienste-Staatsvertrag

Der durch Gesetz umgesetzte Mediendienste-Staatsvertrag regelt das Angebot und die Nutzung von an die Allgemeinheit gerichteten Informations- und Kommunikationsdiensten sowie den datenschutzgerechten Umgang mit dabei anfallenden Bestands-, Nutzungs- und Abrechnungsdaten. Diese Regelungen entsprechen denen des TDDSG;

– das Landeskrankenhausgesetz (LKHG)

Als eines der vielen Gesetze, die dem BDSG vorgehen, ist für den Bericht das LKHG zu nennen. Es enthält spezielle datenschutzrechtliche Regelungen zum Umgang mit Patientendaten, die gleichermaßen von öffentlichen und privaten Krankenhäusern zu beachten sind.

Weitere Entwicklungen

Der Schutz des Persönlichkeitsrechts erfordert eine *stete Überprüfung* der bestehenden Regelungen auf ihre Effizienz und gegebenenfalls ihre Anpassung. Deshalb wurden und werden in der nächsten Zeit wesentliche datenschutzrechtliche Vorschriften geändert.

– Das Bundesdatenschutzgesetz (BDSG)

Zwischen dem Bund und den Ländern besteht Übereinstimmung, dass das Datenschutzrecht wegen seiner rechtlichen Zersplitterung unübersichtlich und auf Grund seiner Systematik und Ausdrucksweise schwer verständlich sowie wegen des raschen Fortschritts der Informations- und Kommunikationstechnik und der damit verbundenen Gefahren überarbeitungsbedürftig ist. Einigkeit besteht jedoch auch mit der Vorgehensweise des Bundes, das BDSG in einer ersten Stufe an die EG-Datenschutzrichtlinie anzupassen und erst in einer zweiten Stufe das BDSG grundlegend zu modernisieren, zu vereinfachen und seine Lesbarkeit zu erhöhen.

• Die erste Stufe:
Hauptziel der EG-Datenschutzrichtlinie, die bis zum 24. Oktober 1998 hätte umgesetzt sein müssen, ist die Schaffung eines einheitlichen Datenschutzniveaus in den Mitgliedstaaten der Europäischen Union und damit die Erleichterung des Datenverkehrs auf wirtschaftlichem Gebiet. Der innergemeinschaftliche Datenverkehr wird deshalb dem inländischen Datenverkehr gleichgesetzt. Die Übermittlung personenbezogener Daten in Drittstaaten ist von der Gewährleistung eines entsprechend angemessenen Datenschutzniveaus in diesen Ländern abhängig. Das novellierte BDSG, das neben der Umsetzung der EG-Datenschutzrichtlinie auch punktuell weiterentwickelt wurde, sieht u. a. auch die Einführung des Grundsatzes der Datenvermeidung und -sparsamkeit, Regelungen zur Videoüberwachung und für Chipkarten sowie ein Datenschutzaudit vor.

Das durch Änderungsgesetz vom 18. Mai 2001 (BGBl. I S. 904) novellierte BDSG berücksichtigt wesentliche Interessen der Länder, die sie im Vorfeld des Gesetzgebungsverfahrens und im Bundesrat, u. a. unter wesentlicher Mitwirkung des Innenministeriums, eingebracht haben. So enthält das Änderungsgesetz insbesondere keine Vorgaben für die Länder, wie die nach der EG-Datenschutzrichtlinie geforderte „völlige Unabhängigkeit“ der Aufsichtsbehörden organisatorisch auszugestalten ist. Es ermöglicht einen Datentrans-

fer in Drittstaaten ohne angemessenes Schutzniveau auf Grund verbindlicher Unternehmensregelungen und verbessert die Rechte der Betroffenen nach Auskunft über die Herkunft ihrer Adressdaten bei Werbemaßnahmen im so genannten Listbrokingverfahren.

Die EG-Datenschutzrichtlinie differenziert zwar nicht zwischen dem öffentlichen und nichtöffentlichen Bereich, die Länder haben sich jedoch auch dafür eingesetzt, dass an der bisherigen Unterscheidung zwischen Vorschriften für den öffentlichen und nichtöffentlichen Bereich festgehalten wird und von den in der EG-Datenschutzrichtlinie eingeräumten Gestaltungsspielräumen zugunsten der Wirtschaft Gebrauch gemacht wird. Die Novelle führt zugleich zu einigen Verbesserungen für die betroffenen Bürger. Die Wirtschaft wird sich möglichst rasch auf die neuen Regelungen einstellen und ihre Datenverarbeitung daran orientieren müssen.

- Die zweite Stufe:
  Mit den Vorarbeiten für die zweite Stufe der Novellierung des BDSG ist bereits begonnen worden. Das Bundesinnenministerium hat einen Gutachtenauftrag an drei Fachleute aus dem Bereich des Datenschutzrechts und der Informatik vergeben. Die umfassende Reform des Datenschutzrechts wird von einer Begleitkommission, die von je einem Bundestagsabgeordneten der SPD-Fraktion und der Fraktion BÜNDNIS 90/DIE GRÜNEN geleitet wird, unterstützt. Das Gutachten soll im Sommer 2001 vorliegen. Nicht nur das Innenministerium geht davon aus, dass angesichts der Komplexität der Materie und der unterschiedlichen Interessenlagen der Beteiligten und Betroffenen die vorgesehene Neukonzeption des BDSG keine leicht zu bewältigende Aufgabe ist, die zudem nicht kurzfristig zu lösen sein dürfte. Es wird die Arbeiten kritisch begleiten und seine Auffassungen im Düsseldorfer Kreis und im Bundesrat vertreten.

– Das Teledienstegesetz (TDG) und das Teledienstedatenschutzgesetz (TDDSG)

  Im Rahmen des Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr werden u. a. das TDG an die sog. e-commerce-Richtlinie 2000/31 angepasst und im TDDSG die Erfahrungen und Entwicklungen mit dem bisherigen TDDSG, die die Bundesregierung in einem Bericht dargelegt hat, umgesetzt. Zugleich wird das TDDSG mit dem novellierten BDSG harmonisiert.

– Der Mediendienste-Staatsvertrag

  Der Mediendienste-Staatsvertrag wird an die Änderungen des TDG und des TDDSG angepasst.

– Die Telekommunikations-Datenschutzverordnung (TDSV)

  Bereits am 18. Dezember 2000 wurde die Telekommunikationsdiensteunternehmen-Datenschutzverordnung novelliert und in Telekommunikations-Datenschutzverordnung umbenannt. Sie steht nunmehr als nachgeordnete und auf dem TKG beruhende Norm mit diesem Gesetz in Einklang.

1.6 Prüfungs- und Fortentwicklungsbedarf einzelner Regelungen

Die Anwendung des BDSG in der Praxis lässt die eine oder andere Schwachstelle des Gesetzes deutlich werden, die entweder zu einer Schwächung des Datenschutzes für die Betroffenen führt, oder aber die wirtschaftliche Betätigung der Unternehmen ohne Notwendigkeit erschwert.

Das novellierte BDSG berücksichtigt *wichtige Anliegen* des Innenministeriums. So sind insbesondere

– Akten nunmehr vom Anwendungsbereich des Gesetzes erfasst, wenn sie gleichartig aufgebaut und nach bestimmten Merkmalen zugänglich sind und ausgewertet werden können,

– Regelungen für die Chipkarte und die Videoüberwachung eingeführt,

– sensitive Daten besonders geschützt,

– die Pflichten der werbetreibenden Unternehmen erweitert und damit die Rechte der Betroffenen gestärkt,

– bei allen vom Gesetz erfassten Datenverarbeitungen anlassunabhängige Kontrollen möglich und

– die Bußgeldvorschriften erheblich erweitert.

Folgende *weitergehende Anliegen*, deren Überprüfung zum Teil vom Bundesinnenministerium in Aussicht gestellt ist, wird das Innenministerium im Rahmen der grundlegenden Novellierung des BDSG – zweite Stufe – aufgreifen:

– Das Schriftformerfordernis für die Einwilligungserklärung stellt ein Hindernis für den elektronischen Geschäftsverkehr dar, da allein die Wahl des Mediums nach Auffassung der Aufsichtsbehörden im Düsseldorfer Kreis ein Abweichen vom Schriftformerfordernis nicht rechtfertigt und nicht davon ausgegangen werden kann, dass die qualifizierte elektronische Signatur, die der Schriftform genügt, rasche und größere Verbreitung findet. Dem Schriftformerfordernis kommt eine Schutz- und Warnfunktion zu. Diese Funktion kann auch durch eine dem TDDSG entsprechende Regelung erfüllt werden, wonach eine Einwilligung elektronisch erteilt werden kann, wenn

  • sie nur durch eine eindeutige und bewusste Handlung des Einwilligenden erfolgen kann und protokolliert wird sowie

  • der Inhalt der Einwilligung jederzeit vom Einwilligenden abgerufen werden kann.

– Die moderne Informations- und Kommunikationstechnik bietet vielfältige Möglichkeiten, einzelne, jeweils rechtmäßig erhobene Daten zu einer Gesamtinformation zu verknüpfen und diese auszuwerten (Data-Warehouse, Data-Mining). Eine Gefährdung des Rechts auf informationelle Selbstbestimmung ergibt sich dann, wenn hierdurch umfassende Persönlichkeitsprofile entstehen. Das BDSG bedarf insoweit einer klaren Regelung zu Zulässigkeit und Grenzen einer Verknüpfung mehrerer personenbezogener Daten unter Wahrung des Rechts auf informationelle Selbstbestimmung.

– Die Erweiterung der Bußgeldtatbestände erfasst keine Verstöße gegen die Auskunftspflicht über die gespeicherten Daten gegenüber dem Betroffenen oder die unbefugte Nutzung von personenbezogenen Daten, z. B. zu Werbezwecken. Eine wirksame Datenschutzkontrolle bedarf einer Sanktionsmöglichkeit auch dieser Verstöße.

– Wird ein Score-Wert nicht gespeichert, besteht keine Pflicht, dem Betroffenen Auskunft über den zu seiner Person errechneten und übermittelten Score-Wert zu erteilen. Aus Gründen der Transparenz ist eine Bekanntgabe des Score-Wertes an den Betroffenen geboten (siehe Ziff. 3.4).

– Die Befugnis der Auskunfteien, für die Auskunftserteilung an den Betroffenen ein Entgelt verlangen zu können, weil die potenzielle Möglichkeit der Nutzung dieser „Selbstauskunft“ zu wirtschaftlichen Zwecken besteht, ist unbefriedigend. Auskünfte an Betroffene sollten jedenfalls dann unentgeltlich erteilt werden, wenn sie vom Betroffenen ausschließlich zur Überprüfung der Richtigkeit der zu seiner Person gespeicherten Daten angefordert werden, was vom Betroffenen nachzuweisen wäre (siehe Ziff. 3.5).

– Unternehmen, die personenbezogene Daten zum Zwecke der Übermittlung speichern (beispielsweise Auskunfteien und Adresshändler), brauchen dem Betroffenen Auskunft über Herkunft und Empfänger der Daten nur bei begründeten Zweifeln an der Richtigkeit der Daten zu erteilen. Es ist fraglich und deshalb zu prüfen, ob diese Regelung, die dem Schutz vor Offenlegung der bestehenden Geschäftsbeziehungen dienen soll, noch zeitgemäß ist (siehe Ziff. 3.1).

1.7 Aufgaben des Innenministeriums auf dem Gebiet des Datenschutzes im öffentlichen Bereich

Das Innenministerium ist auch *oberste Landesbehörde* für den Datenschutz im *öffentlichen Bereich*. In dieser Funktion nahm es zu zahlreichen bereichsspezifischen datenschutzrechtlichen Regelungen auf EU-, Bundes- und Landesebene Stellung, wie beispielsweise zu

– dem Melderechtrahmengesetz,

– der EG-Grundrechtscharta,

– den Informationszugangsgesetzen auf EU- und Landesebene,

– der Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft zum freien Datenverkehr,

– dem G-10-Gesetz,

– dem Polizeigesetz,

– dem Leitfaden zum Sozialhilfebetrug und

– der Verwaltungsvorschrift zur Mitwirkung der Gemeinden in Nachlasssachen.

Im Vordergrund standen hier die Arbeiten zum Gesetz zur Änderung des Landesdatenschutzgesetzes und anderer Gesetze vom 23. Mai 2000 (GBl. S. 450), durch das die EG-Datenschutzrichtlinie in Landesrecht umgesetzt sowie der Datenschutz punktuell weiterentwickelt wurde, und dessen Umsetzung. Das Landesdatenschutzgesetz (LDSG) wurde am 18. September 2000 neu gefasst (GBl. S. 648).

Das Innenministerium ist zudem federführend zuständig für die jährlich zu erstellende Stellungnahme der Landesregierung zum Tätigkeitsbericht des Landesbeauftragten für den Datenschutz.

1.8 Abgrenzung zum öffentlichen Bereich

Ob ein *Unternehmen* mit *Sitz in Baden-Württemberg* den restriktiveren datenschutzrechtlichen Vorschriften für den öffentlichen Bereich oder den freieren Vorschriften für den nichtöffentlichen Bereich unterliegt, ergibt sich in der Regel aus der Rechtsform des Unternehmens. Ist es privatrechtlich organisiert, findet insbesondere das BDSG Anwendung und unterliegt das Unternehmen der Aufsicht des Innenministeriums; ist es öffentlich-rechtlich organisiert und nimmt es nicht am Wettbewerb teil, unterliegt es dem Landesdatenschutzgesetz (LDSG) und der Kontrolle durch den Landesbeauftragten für den Datenschutz.

Mit der Änderung des LDSG vom 23. Mai 2000 hat sich für die juristischen Personen und sonstigen Vereinigungen des Privatrechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und mehrheitlich in der Hand von Behörden, sonstigen öffentlichen Stellen des Landes, der Gemeinden und Gemeindeverbänden oder sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts liegen, die Rechtslage geändert. Nach § 2 Abs. 2 und 4 LDSG gelten sie nun als öffentliche Stellen und unterliegen – wie die Behörden und sonstigen öffentlichen Stellen des Landes und der Kommunen – dem LDSG und der Kontrolle des Landesbeauftragten für den Datenschutz, es sei denn, sie nehmen am *Wettbewerb* teil. Die Gesetzesänderung erfolgte im Hinblick auf die stetig zunehmende Ausgliederung von Organisationseinheiten aus der Verwaltung und deren Umwandlung in Privatrechtsform. Zu nennen sind in diesem Zusammenhang kommunale Versorgungsunternehmen, Wohnungsbauunternehmen, Krankenhäuser, Bildungseinrichtungen, Abfallbeseitigungsgesellschaften, Messegesellschaften und auch Verkehrsbetriebe. Nur wenn solche Unternehmen am Wettbewerb teilnehmen, findet auf sie das BDSG Anwendung, um sie wegen der restriktiveren Regelungen des LDSG keinem Wettbewerbsnachteil auszusetzen.

In der Praxis hat die Neuregelung in bestimmten Einzelfällen bereits zu umfangreicheren Prüfungen der auf das Unternehmen anzuwendenden Vorschriften und auch zu Zuständigkeitsänderungen geführt. So unterlag beispielsweise ein in Privatrechtsform geführter städtischer Verkehrsbetrieb bislang dem BDSG und damit der Aufsicht des Innenministeriums, nach der neuen Rechtslage unterliegt er dem LDSG und der Kontrolle des Landesbeauftragten für den Datenschutz. Eine Zuständigkeitsänderung ist im Übrigen für alle privatrechtlich organisierten Verkehrsbetriebe mit Sitz in Baden-Württemberg erfolgt, an denen die öffentliche Hand mehrheitlich beteiligt ist. Dabei ist auch die Regelung der so genannten Schachtelbeteiligung des § 2 Abs. 2 Satz 2 LDSG zu beachten.

2. Technik, Organisation und Teledienste

2.1 Internet und Datenschutz

Die Bedeutung des Internets nimmt ständig zu. Fast täglich werden neue Nutzungsmöglichkeiten elektronischer Dienste erfunden und auf den Markt gebracht. Die auf der Basis des Internets entwickelten Dienste bieten für die Wirtschaft und die Bürger Chancen, bergen aber auch nicht unerhebliche Risiken für das Recht auf informationelle Selbstbestimmung, das Persönlichkeitsrecht eines jeden, der das neue Medium nutzt. In diesem Kapitel stellt die Aufsichtsbehörde deshalb allgemeine Ausführungen zum besseren Verständnis der Funktionsweise des Internets voran, zu dessen Gefahren für das Persönlichkeitsrecht und den Möglichkeiten der Gefahrenminimierung.

Das Internet, auch als das Netz der Netze bezeichnet, ist ein weltweites Netzwerk, das Computer (u. a. Server, PC) über Grenzen hinweg verbindet und so den Menschen an jedem Ort der Erde die Möglichkeit bietet, miteinander zu kommunizieren, auf Informationsangebote zuzugreifen und diese abzurufen. Das Internet entstand aus dem militärischen Bereich der USA. Die Vorstellung war, dass in einem US-weiten elektronischen Netzwerk (ARP-Anet ca. 1969) das Militär, die Waffenindustrie und die Universitäten miteinander kommunizieren können und das Netz so redundant aufgebaut ist, dass selbst bei einer Teilzerstörung noch über andere Wege kommuniziert werden kann. Schon 1972 erschienen die ersten Programme für die elektronische Post. Ab 1985 wurden sechs große Computerzentren in den USA verbunden. Ende der 80-iger Jahre wurde das Netz (MERIT) den US-Universitäten zur weiteren Pflege und zum Ausbau übertragen. Das war gleichzeitig der Startzeitpunkt für die Öffnung nach außen. Aber erst mit der Einführung der Browser- und der Hyperlink-Technologie (Verlinkung von Informationsinhalten) war der Boom dieses Netzes nicht mehr aufzuhalten. Es entstand das heutige Internet.

Mit der Zahl der Nutzer, der Nutzungsmöglichkeiten und der Informationsangebote erhöhen sich auch die Anforderungen an den Datenschutz und die Datensicherheit. Je mehr Daten über das Internet übertragen werden, umso größer ist die Angriffsfläche für diejenigen, die das Netz und die Daten missbräuchlich nutzen wollen. Deshalb ist es wichtig, dass umfassende Sicherheitskonzepte den Umgang mit dem Internet sicherer gestalten. Alle eingesetzten *Datenschutzmaßnahmen* müssen, damit sie wirksam sind, *Hand in Hand gehen*. Eine hundertprozentige Sicherheit wird es aber nicht geben.

Zum Schutz personenbezogener Daten finden auf die Datenverarbeitung durch im Internet tätige Unternehmen mit Sitz in Deutschland insbesondere die Regelungen des Teledienstedatenschutzgesetzes (TDDSG), des Mediendienstestaatsvertrages, des Telekommunikationsgesetzes (TKG) und der Telekommunikations-Datenschutzverordnung (TDSV) Anwendung. Auch in den anderen Staaten der Europäischen Union oder des Europäischen Wirtschaftsraums gelten adäquate Datenschutzregelungen. Bei Unternehmen mit Sitz im sonstigen Ausland ist dies jedoch eher die Ausnahme. Deshalb wird den Nutzern geraten, möglichst nur solche Internet-Diensteanbieter auszuwählen, die unter den datenschutzrechtlichen Geltungsbereich der Europäischen Union oder des Europäischen Wirtschaftsraums fallen oder die sich in Staaten mit ausgewiesenem angemessenen Schutzniveau befinden.

Die an das Internet angeschlossenen Rechner (Server) bilden die so genannten Netzknoten. Ein Nutzer kann einen eigenen Netzknoten haben und mit einer Festleitungsverbindung (z. B. ein größeres Unternehmen) oder über die Telefonleitung (Wählverbindung; z. B. die Bürger) verbunden sein. Der Datenverkehr über das Internet fließt nicht kontinuierlich zwischen Sender und Empfänger wie beim Telefon, sondern paketorientiert, d. h. die zu übertragenden Daten werden in einzelnen Paketen an den Empfänger gesendet.

Transportbasis des Internets

Die *Transportbasis des Internets* ist das TCP/IP-Protokoll (TCP/IP = Transmission Control Protocoll / Internet Protocoll). Unter einem Protokoll im technischen Sinne wird die eindeutige Definition eines Verfahrens verstanden. Das TCP/IP-Protokoll hat sich seit Beginn des Internets nicht verändert und ist nach dem elektronischen Zeitalter gerechnet ein altes Protokoll. Wesentlicher Inhalt des Verfah-

rens ist, dass jeder einzelne Computer, unabhängig vom Typ und Betriebssystem, durch eine weltweit einmalige TCP/IP-Adressierung (z. B. 194.001.86.02) im Internet identifiziert werden kann und dass die Datenpakete weltweit systemübergreifend übertragen werden können.

Die weltweit gültigen TCP/IP-Adressen werden durch ICANN (Internet Corporation for Assigned Names and Numbers) verwaltet und zugewiesen. Für den europäischen Raum fällt diese Aufgabe der Einrichtung RIPE (Réseaux IP Européens) in Paris zu. Da bei der Einführung des TCP/IP-Protokolls der Umfang der weltweiten Verbreitung und die Vielzahl der Nutzer nicht vorhersehbar waren, reicht die verfügbare Anzahl von TCP/IP-Adressen nicht aus. Wegen der begrenzten Anzahl von statischen TCP/IP-Adressen kann nicht jedem Nutzer eine eigene Adresse fest zugeteilt werden. Jeder Nutzer, der sich über einen Internet-Zugangsanbieter mit dem Internet verbinden lässt, erhält deshalb von diesen statischen TCP/IP-Adressen nur eine für den momentanen Zugang zugeteilt (dynamische Adressvergabe). Die TCP/IP-Adresse wird deshalb hier bei jedem Zugriff neu vergeben. Da die TCP/IP-Adressen für den Nutzer nicht leicht zu merken sind, wurde die Möglichkeit so genannter „sprechender" Adressen geschaffen (z. B. *www.im.bwl.de*), die jedoch im Hintergrund in TCP/IP-Adressen umgewandelt werden.

Datenschutzrechtlich interessant ist, dass sich über die TCP/IP-Adressen mithilfe Dritter, die diese Adressen verwalten, ohne großen Aufwand die dahinterstehenden *Internet-Nutzer identifizieren* lassen (mit Name, Adresse, Geburtsdatum, Telefonnummer). Dritte können zum Beispiel sein:

– *Internet-Zugangsanbieter* (Internet Access Provider), die über eine Logdatei zu jeder zugewiesenen TCP/IP-Adresse die Identität des Nutzers, die Dauer, den genauen Zeitpunkt und das Datum der Nutzung bestimmen können. Kommt der Nutzer statt über eine Leitungsfestverbindung über eine Wählverbindung (u. a. ISDN, Leitungswählverbindung) auf den Internet-Zugangsanbieter zu, können durch die Telefongesellschaft aufgrund der Daten, die für Zwecke der Telefonabrechung gespeichert wurden, die Nutzer anhand der Rufnummer identifiziert werden;

– *Internet-Service-Provider*, die Zugriff (meistens über Portale) auf das Internet und darüber hinaus auch auf das Web-Hosting (Speicherung eigener Web-Seiten auf ihren Servern) bieten. Sie nutzen hierzu Server, die ständig mit dem Internet verbunden sind. Diese Dienste können auch von Firmen oder Einzelpersonen genutzt werden. Die Protokollierung erfolgt in den Servern, wobei die TCP/IP-Adresse z. B. mit der WWW-Anfrage als sog. Logfile generiert werden können;

– *Systemadministratoren*, die die internen Firmennetze (z. B. von Firmen, Behörden) verwalten und diese über einen Gateway mit dem Internet verbinden. Hier werden schon aus Gründen der Sicherheit beide Netzwerke durch die Verwendung anderer IP-Adressbereiche im internen Bereich voneinander getrennt. Jede interne TCP/IP-Adresse und die Kommunikationsbeziehungen lassen sich mittels einer technischen Logdatei identifizieren.

Welche weiteren Gefahren für das Persönlichkeitsrecht können bestehen?

– I*dentifizierung des Nutzers* bei Verwendung von weltweit gültigen, statischen TCP/IP-Adressen. Die Identifizierung eines Nutzers mit statischer TCP/IP-Adresse ist ohne größeren Aufwand möglich;

– *Auslesen von Dateien* mit personenbezogenen Daten auf dem PC mittels spezieller Programme über das Netz;

– *Zwischenspeicherung* in den Zwischenstationen. Das TCP/IP-Protokoll hat die Eigenschaft, aus Netzauslastungsgründen die Nachrichten möglichst optimal durch das Netzwerk zu schicken (sog. Routing). So kann es sein, dass ein Teil einer Nachricht von Stuttgart nach Hamburg z. B. über Paris geführt wird, während der andere Teil über die direkte Verbindung nach Hamburg gelangt. In allen Zwischenstationen werden die Nachrichten oder Teile davon kurz zwischengespeichert und können dort gelesen, gespeichert oder verfälscht werden;

– *DNS (Domaine Name System)*-Server als Datensammler. Die Aufgabe von DNS-Servern ist das Übersetzen der numerischen TCP/IP-Adresse in eine

meist alphabetische Namensbezeichnung (z. B. www.im.bwl.de) bei Aufrufen von WWW-Seiten. Die DNS-Server speichern sämtliche andere DNS-Server im Internet, zu denen ein Internet-Nutzer Kontakt hatte oder herstellen wollte;

– *Horchen* mittels Ping-Befehl, wer im Internet aktiv ist. Der Ping-Befehl erlaubt es festzustellen, ob ein Teilnehmer am Netz angeschlossen und ob sein Computer (Server/Client) eingeschaltet ist oder nicht. Damit ist es möglich herauszufinden, ob jemand zu einem bestimmten Zeitpunkt im Netz war. Der angewählte Computer merkt i.d.R. nicht, dass jemand den Versuch gestartet hat.

Durch welche Maßnahmen kann das Persönlichkeitsrecht besser geschützt werden?

– Verwendung von *dynamischen TCP/IP-Adressen.* Bei Nutzung des Internets als Informationsquelle (z. B. Lesen von Informationsangeboten) können dann keine direkten Rückschlüsse auf den Nutzer gezogen werden und kann damit auch keine Identifizierung auf Grund der verwendeten TCP/IP-Adresse erfolgen. Ausgenommen davon sind – wie ausgeführt – der Diensteanbieter, mit dem der Nutzer einen Vertrag zur Nutzung und Bereitstellung des Teledienstes (Internet) abgeschlossen hat, und der Telekommunikations-Diensteanbieter, der die Leitungsverbindung (insb. bei Wählleitungsverbindungen) zum Einwählen der Verbindung zum Diensteanbieter bereitstellt. Beiden ist trotz Verwendung dynamischer TCP/IP-Adressen eine Identifizierung des Nutzers u. a. über die Bestands- und Abrechnungsdaten möglich.

– *Nutzung von Wählanschlüssen* (u. a. ISDN, Leitungswählverbindungen). Bei Verwendung von Wählanschlüssen erfolgt der Kontakt zum Internet nur, wenn dieser benötigt wird. Diese Anschlussart wird insbesondere von Privat-Nutzern und kleineren Unternehmen genutzt. Hier werden als Schutzmaßnahme die für kleinere Systeme neu auf den Markt gekommenen Firewall-Programme, verbunden mit Virenscanner und Updateservice empfohlen.

– Vorhaltung eines s*eparaten Internet-PC's.* Die empfohlenen Datenschutzmaßnahmen (u. a. Firewall, Virenschutzprogramm) können von einigen Privat-Nutzern bei fehlendem technischen Know-how nicht oder nur unzureichend eingesetzt werden. In solchen Situationen empfiehlt es sich, für sensible Datenbestände einen separaten PC vorzuhalten und diesen nicht mit dem Internet-PC zu verbinden. Um ein Mindestmaß an Sicherheit zu erreichen, sollte auf dem Internet-PC ein aktuelles Virenschutzprogramm mit Updateservice installiert sein. Der Datenaustausch zwischen beiden PC's ist dann mittels Diskette oder CD-ROM möglich.

Datenschutzrechtliche Regelungen

Internet-Zugangsanbieter und Internet-Service-Provider, so genannte Teledienstanbieter, die insbesondere Privatpersonen und kleineren bis mittleren Unternehmen den Zugang zum Internet eröffnen, haben die Vorschriften des TDDSG zu beachten. Es sieht u. a. die Ermöglichung der anonymen und pseudonymen Inanspruchnahme der Teledienste, in besonderen Fällen das Verbot, die Erbringung von Telediensten von der Einwilligung des Nutzers in eine Verarbeitung oder Nutzung seiner Daten für andere Zwecke abhängig zu machen, und eine enge Zweckbindung vor. Die Überprüfung der Einhaltung dieser Vorschriften ist u. a. Aufgabe der Aufsichtsbehörden.

2.1.1 Surfen im Web

Der *Schwerpunkt der Internetnutzung* ist die Nutzung des so genannten *WorldWideWebs (WWW).* Darüber kann sich der Nutzer Informationen zu allen Interessensgebieten anzeigen lassen. Obwohl das Internet aus einer Vielzahl von unterschiedlichen Diensten besteht, ist das WWW zum Synonym für das Internet geworden.

Das WWW erschließt sich dem Nutzer über den auf seinem PC installierten Browser. Der Browser ist ein Programm, das auf dem PC des Nutzers installiert werden muss, um am WWW-Dienst teilnehmen zu können. Ist der Browser installiert, kann auf die WWW-Seiten des Internets zugegriffen werden durch die unmittelbare Eingabe der Internet-Adresse der gewünschten Seite bzw. der über-

geordneten Startseite oder über so genannte Internet-Portale (z. B. Teledienstean-bieter), die eine Vielzahl von Informationen anbieten und von denen wiederum Hyperlinks zu Seiten auf anderen Internet-Servern verweisen. Oft sind Suchmaschinen eingebunden, die das Auffinden von Informationen erleichtern. Die Internet-Portale erfreuen sich zunehmender Beliebtheit bei den Nutzern, da sie ihnen die eigene Informationssuche weitgehend abnehmen.

Welche Gefahren für das Persönlichkeitsrecht können bestehen?

– *Browsermeldungen.* Jeder Browser gibt beim Aufruf einer Internetseite Informationen über sich und den PC bekannt, auf dem er installiert ist, damit der Sender der aufgerufenen Seite diese an den Empfänger-PC anpassen kann (z. B. Browsertyp, Version, Betriebssystem, eingestellte Sprache, bei einigen Browsern noch die auf dem PC eingesetzten Anwendungsprogramme, soweit diese für das Lesen der WWW-Seiten erforderlich sind). Der Sender kann aber auch die zuvor aufgerufenen Seiten abrufen. Damit können personenbezogene Daten preisgegeben werden. Das kann auch geschehen durch Weiterleitung von Browserinformationen bei einer Verlinkung. Hier kann mithilfe der Maustaste von einem zum anderen Teledienst-eanbieter gesprungen werden. Die Problematik der Links ist, dass der Nutzer nicht unbedingt erfährt, wenn er auf einen fremden Rechner weitervermittelt wird. Er weiß daher nicht, an wen die o. a. Browserinformationen gesendet werden;

– *Ausführung der Programme Java und ActiveX*. Einige Anbieter verwenden für die Kommunikation zwischen Server und Browser zur Gestaltung ihrer Internet-Seiten Java-, JavaScript- oder ActiveX-Programme. Diese vom Server mitgesendeten Programme werden automatisch vom Browser des Nutzers ausgeführt. Diese Programme können jedoch oftmals mehr, als der Nutzer weiß. So ist es z. B. möglich, dass die Festplatte ausgelesen und der Inhalt über das Internet an einen Dritten gesendet wird, während sich der Nutzer eine Internetseite anschaut, hinter der sich ein entsprechendes Programm verbirgt;

– Setzen und Auswerten von Cookies. Cookies sind aus datenschutzrechtlicher Sicht ein wichtiges Thema. Aus diesem Grund werden unter Ziff. 2.1.2 Cookies einschließlich der Maßnahmen zum Schutz des Persönlichkeitsrechts und der datenschutzrechtlichen Regelungen ausführlich behandelt.

Durch welche Maßnahmen kann das Persönlichkeitsrecht besser geschützt werden?

– *Browsermeldungen* lassen sich nicht unterdrücken. Die Möglichkeit, Persönlichkeitsprofile zu bilden, nimmt mit dem Zugriff auf jeweils gleiche Internetseiten zu. Durch nicht gleichförmiges Surfen im Web lässt sich dieses Risiko minimieren.

– Bei entsprechender Einstellung des Browsers können *die Programme Java und ActiveX* erkannt und die Ausführung unterbunden werden. Dies ist einerseits sicher, hat andererseits den Nachteil, dass alle Internetseiten, die mit solchen Programmen gestaltet sind, unter Umständen nicht mehr oder auch nicht richtig angezeigt werden können.

Datenschutzrechtliche Regelungen

Für den Schutz personenbezogener Daten bei Telediensten ist das TDDSG einschlägig. Nach § 4 Abs. 3 TDDSG ist dem Nutzer durch den Teledienst-eanbieter die Weitervermittlung zu einem anderen Diensteanbieter anzuzeigen. Diese Anzeigepflicht gilt insbesondere für die Verlinkung von einer Web-Seite zu einer anderen. In der Praxis wird diese Hinweispflicht nicht immer beachtet. Geht aus der Internet-Seite die Anbieterkennzeichnung nach § 6 TDG hervor und lässt sich auf Grund der Aufmachung der Internet-Seite der Teledienst-eanbieter eindeutig zuordnen, so ist der Anzeigepflicht entsprochen.

2.1.2 Einsatz von Cookies

Cookies sind kleine *Textdateien*, die auf dem PC des Nutzers abgelegt werden. Cookies können von jedem Betreiber einer Internet-Seite eingespielt und ausgewertet werden. Der Datenaustausch erfolgt im Hintergrund zwischen PC und Internet-Server. Der Nutzer hat keinen Einfluss auf die Inhalte der Cookie-Datei

und die Speicherdauer. Diese Informationen werden vom Betreiber der Internet-Seite bestimmt. In der Regel sind sie mit einem Verfallsdatum versehen, nach dessen Ablauf sie vom Browser selbstständig gelöscht werden. Der eigentliche Sinn von Cookies ist, das Surfen der Nutzer zu erleichtern. Zwischen dem Browser und dem Server besteht keine permanente Verbindung. Bei jedem Aufruf einer neuen Seite oder z. B. beim Absenden eines Formulars wird der Dialog zwischen Browser (PC) und Server von neuem aufgebaut und nach der Datenübertragung wieder beendet. Genau hier liegt das Problem: Wie soll z. B. das Programm im Server wissen, was bereits im ersten Formular ausgefüllt wurde, wenn ein zweites Formular ausgefüllt wird? Solche Informationen oder auch technische Informationen über Einstellungen, aber auch der Warenkorb im E-Commerce werden mittels Cookies auf dem PC als Merkposten vorgehalten. Im Regelfall verfällt ein Cookie mit dem Ende der Sitzung.

Cookies werden aber auch zur *Nutzerprofilierung* insbesondere für eine zielgerichtete *Werbung* eingesetzt. Hierbei erhält der Nutzer-PC beim ersten Besuch z. B. eines Portals mittels Cookie eine eindeutige Identifizierungsnummer (ID-Cookie) auf der Festplatte abgelegt. Danach wird das Nutzerverhalten, d. h. welche Seiten aufgerufen werden, unter der Identifizierungsnummer auf einem Internetserver des Portals in einer Datenbank gespeichert. Aus den in der Datenbank erfassten Zugriffsdaten kann ein Profil des Nutzers (richtigerweise: des Nutzer-PC's) erstellt werden. Mit diesem Profil kann eine auf den Nutzer speziell ausgerichtete Werbung erstellt und bei jeder Kontaktaufnahme des Nutzer-PC's mit der Internetseite als Werbebanner eingeblendet werden. Wird bekannt, welche Person sich hinter dem Nutzer-PC bzw. dem ID-Cookie verbirgt, z. B. durch eine Bestellung, Anforderung von Informationsmaterial, Teilnahme an einem Preisausschreiben oder bei Verwendung statischer TCP/IP-Adressen, ist ein personenbezogenes Nutzerprofil, d. h. der gläserne Internetnutzer, entstanden.

Eine andere Möglichkeit des Einsatzes von Cookies zu Werbezwecken ist, im Cookie selbst die zuletzt aufgerufene Seite abzuspeichern und beim nächsten Zugriff auf das Internetangebot eine darauf abgestimmte Werbung (z. B. als Bannerwerbung) einzublenden.

Durch welche Maßnahmen kann das Persönlichkeitsrecht besser geschützt werden?

Problematisch sind Cookies aufgrund der geringen Transparenz für den Nutzer. Der Nutzer kann aber Maßnahmen ergreifen, um Cookies zu erkennen und gegebenenfalls auszuschalten. Alle marktgängigen Browser lassen sich so einstellen, *dass Cookies erkannt* und a*ngezeigt* werden. Ist diese Einstellung erfolgt, erhält der Nutzer eine Warnmeldung, wenn ein Cookie auf seinem PC platziert werden soll. Der Nutzer hat auch, je nach Einstellung, die Möglichkeit, die Annahme eines Cookies abzulehnen. Damit behält der Nutzer den Überblick, wer auf seinem PC Cookies hinterlegt und bei zukünftigen Kontakten Informationen aus den Cookies beziehen kann. Cookies werden auf dem PC in einem speziellen Verzeichnis abgelegt. Wer ganz sicher gehen will, dass keine Cookies ausgelesen werden können, sollte den Inhalt dieser Datei nach erfolgter Internet-Sitzung löschen.

Datenschutzrechtliche Regelungen

Entscheidend für die datenschutzrechtliche Bewertung ist, ob durch den Einsatz von Cookies personenbezogene Daten genutzt werden. Cookies, die nur für den aktuellen Zugriff die rein technisch-organisatorischen PC-Einstellungen beinhalten, sind mangels Personenbezugs datenschutzrechtlich nicht relevant.

Werden beim Betrieb eines Teledienstes Nutzerdaten erfasst, so ist das TDDSG maßgeblich. Personenbezogene Daten dürfen nach § 3 Abs. 1 TDDSG nur auf gesetzlicher Grundlage oder mit Einwilligung des Nutzers erhoben, verarbeitet oder genutzt werden.

Nach § 4 Abs. 4 TDDSG ist die Erstellung von *Nutzerprofilen* unter Verwendung von *Pseudonymen* zulässig. Diese Bestimmung wird im novellierten § 6 Abs. 3 TDDSG dahin gehend präzisiert, dass der Diensteanbieter für Zwecke der Werbung Nutzerprofile bei der Verwendung von Pseudonymen erstellen darf, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer nach § 3 Abs. 5 TDDSG (§ 4 Abs. 1 TDDSG in novellierter Fassung) vor der Erhebung der Daten umfassend zu unterrichten und auf sein Widerspruchsrecht hinzuweisen.

Durch die Präzisierung im novellierten § 6 Abs. 3 TDDSG kann davon ausgegangen werden, dass eine Nutzerprofilierung mittels ID-Cookies bei umfassender Information über den Widerspruch (opt-out) zulässig ist. Besteht die Möglichkeit, die ID-Nummer zu personalisieren, so liegen jedoch personenbeziehbare Daten vor, deren Erhebung, Verarbeitung und Nutzung nur mit Einwilligung des Nutzers nach § 3 Abs. 1 TDDSG zulässig ist (opt-in).

Anzumerken ist, dass derzeit noch keine abschließende datenschutzrechtliche Beurteilung von Profilierungen in der Praxis vorliegen. Die Diskussion ist vor allem geprägt durch Vorgänge in den USA, wo wegen eines nicht gleichwertigen Datenschutzniveaus die Nutzerprofilierung Anwendung findet. Bei allen von der Aufsichtsbehörde geprüften Teledienstanbietern wurde auf den Einsatz von Cookies zur Werbesteuerung verzichtet. Lediglich eine Anfrage eines Unternehmens, das in den USA Technologien zur Profilierung anbietet, betraf diesen Bereich. Von dem Vorhaben wurde jedoch noch in der Planungsphase Abstand genommen. Die Aufsichtsbehörden im Düsseldorfer Kreis haben sich wegen Unklarheiten im bisherigen TDDSG noch keine abschließende Meinung gebildet. Die Aufsichtsbehörde geht davon aus, dass nach der Verabschiedung der Änderung des TDDSG die Frage der Nutzerprofilierung erneut diskutiert und anhand der konkreten Ausgestaltung in der Praxis beurteilt werden wird.

Auch wenn auf den Einsatz von Cookies zur Werbesteuerung verzichtet wird, bedeutet dies nicht, beim Surfen im Web von Werbung durch Banner verschont zu bleiben. Bannerwerbung, die unabhängig von einer vorherigen Auswertung von Nutzungsdaten auf den PC des Nutzers eingeblendet wird, wie feste oder nach dem Zufallsprinzip ausgewählte Werbebanner, ist datenschutzrechtlich nicht relevant, d. h. ohne Weiteres zulässig. Das Einblenden von Werbebannern kann aber durch den Einsatz von so genannten Web-Washer-Programmen unterdrückt werden.

2.1.3 Hacker nutzen Schlupflöcher im Internet

Durch die weltweite Verbreitung des Internets nehmen die Angriffe durch Hacker auf Internet-Anschlüsse der Unternehmen zu. Nicht nur die finanziellen Folgen, sondern auch die Verletzungen des Persönlichkeitsrechts können groß sein. Sie sind abhängig vom Erfolg des virtuellen Einbruchs und den dadurch bedingten Ausfällen der Informationstechnik. Zusätzlich ist mit einem Vertrauensverlust oder mit Unsicherheiten bei den Kunden zu rechnen. Erhält der Hacker Zugang zu personenbezogenen Daten wie z. B. zu Patienten-, Personal- oder Privat-Kundendaten, so ist dies auch datenschutzrechtlich relevant. Nach § 9 BDSG hat die nichtöffentliche Stelle, die selbst oder im Auftrag personenbezogene Daten verarbeitet, diejenigen technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG zu gewährleisten, d. h. die personenbezogenen Daten vor Hackern zu schützen.

Durch welche Maßnahmen können sich Unternehmen schützen?

– *Einsatz von Firewall-Systemen*. Eine Firewall ist erforderlich, um zu verhindern, dass Hacker oder schädigende Programme von außen in das DV-System eindringen und dadurch personenbezogene Daten unbefugt gelesen, kopiert, verändert oder entfernt werden können (Ziff. 2 – Datenträgerkontrolle – der Anlage zu § 9 BDSG). Durch das sog. Firewall-System wird das unternehmenseigene Netzwerk vom Internet getrennt und nur zugelassene Dienste und Adressen (z. B. WWW, E-Mail) dürfen die Firewall passieren. Des Weiteren erlauben die Firewalls den Zugang nur zu ausgewählten und für sicher befundenen Internet-Seiten. Firewall-Systeme gibt es auch für kleinere und mittlere Unternehmen, in einfachen Ausführungen auch für den privaten PC.

– *Einsatz von Intrusion Detection Systemen*. Intrusion Detection Systeme, kurz IDS genannt, zeigen dem Netzwerk-Administrator unerwünschte Aktivitäten im Unternehmens-Netzwerk auf und wo diese stattfinden. IDS ist als zusätzliche Sicherheit u. a. zu Firewall-Systemen gedacht. Gelingt es beispielsweise einem Hacker, das Firewall-System zu überlisten, und versucht er, ein Programm zu installieren, das wiederum dazu dient, Passwörter auszuspionieren, wird dieser Ausspähvorgang durch IDS entdeckt und der Systemverantwortliche oder Sicherheitsbeauftragte sofort per E-Mail oder Ruffunktion informiert, der dann entsprechende Abhilfe schaffen kann.

– *Trennung von internen und externen TCP/IP-Adressen*. Für die Trennung zwischen dem Internet und Firmen- oder Behördennetzen werden spezielle Router eingesetzt. Sie werden auch als Network-Address-Table (NAT) bezeichnet. Diese sorgen dafür, dass im internen Netz andere TCP/IP-Adressen als im Internet verwendet werden.

– *Installation von Virenschutzsoftware*. Mit dem Einsatz einer zentralen Virenschutzsoftware werden eingehende Dokumente oder Files auf eventuelle Viren untersucht, bevor diese in das interne Netz eindringen und aktiv werden können.

– *Ausschluss nicht zertifizierter Makros*. Makros sind automatisierte Befehlsfolgen, die insbesondere bei der Textverarbeitung zur Vereinfachung von Vorgängen eingesetzt werden können. So können Formatvorlagen mittels Makros so gestaltet werden, dass der Nutzer beim Ausfüllen der Adressfelder automatisch geführt wird. Makros können aber auch Schäden anrichten, wenn sie gewollte falsche Befehlsfolgen enthalten (Makroviren). Daher sollte die Makrofunktion beim Öffnen von externen Dokumenten grundsätzlich ausgeschaltet sein. Für das Erstellen von Dokumenten sollte das Bürokommunikationssystem so eingestellt sein, dass nur Makros ausgeführt werden können, die von einer vertrauenswürdigen Stelle stammen (zertifiziertes Makro).

Nur ein *Zusammenspiel* der o. a. *Sicherheitstechnik* garantiert einen *hohen Grad an Datenschutz durch Datensicherheit*. Die Aufzählung ist nicht abschließend und ist dem technischen Fortschritt unterworfen. Eine hundertprozentige Sicherheit wird es aber nie geben.

2.1.4 Bestellung per Maustaste

Der elektronische Geschäftsverkehr im Internet wird auch als elektronischer Handel oder electronic Commerce (E-Commerce) bezeichnet. Er beinhaltet den Geschäftsverkehr, der den Erwerb von Gütern oder Dienstleistungen zum Inhalt hat. Durch das Internet werden die Unternehmen in die Lage versetzt, ihre Produkte global anzubieten oder Waren zu erwerben. Der elektronische Geschäftsverkehr ermöglicht Unternehmen, flexibler und effizienter zu operieren, mit Lieferanten enger zusammenzuarbeiten und auf die Bedürfnisse und Erwartungen der Kunden einzugehen. Bisher lag der Schwerpunkt des elektronischen Geschäftsverkehrs im sog. Business-to-Business-Geschäft (B-to-B) zwischen Unternehmen, die auf den Online-Marktplätzen ihre Waren rasch und gegebenenfalls kostengünstig einkaufen können. Mit Zunahme der Internet-Anschlüsse in Privathaushalten wird auch dieser Zweig für den elektronischen Geschäftsverkehr interessanter. Man spricht hier auch von Business-to-Consumer-Geschäften (B-to-C).

Mit der weiteren Verbreitung von mobilen Endgeräten (z. B. Mobiltelefone und künftig UMTS-PC-Endgeräte) können auch Geschäfte unabhängig von einem festen Standort abgeschlossen werden. Diese Art der Geschäfte steht erst am Anfang der Entwicklung. Sie wird auch als M-Commerce (Mobil-Commerce) bezeichnet.

Bei allen diesen Geschäften steht die *elektronische Bestellung von Gütern* im Vordergrund. In manchen Fällen kann die Lieferung direkt über das Internet erfolgen (z. B. bei Softwareanbietern). Der Zugang zum Internet-Angebot erfolgt vielfach über die bereits beschriebenen Internet-Portale. In naher Zukunft werden diese Portale dann zusätzlich so genannte „user-agents“ zur Verfügung stellen, die im Internet im Auftrag des Nutzers selbstständig auch über einen längeren Zeitraum hinweg nach Angeboten suchen, die den Vorgaben des Nutzers entsprechen und ihm das Ergebnis mitteilen, gegebenenfalls sogar die Bestellung vorbereiten.

Der Durchbruch im privaten Bereich wird dem elektronischen Handel erst mit einem sicheren elektronischen Zahlungsmittel gelingen. Derzeit weit verbreitet ist die Bezahlung durch die Übermittlung der Kreditkartendaten. Für geringe Beträge ist die elektronische Bezahlung durch das so genannte elektronische Bargeld – auch „Geldkarte“ oder „e-cash“ genannt – in Vorbereitung. Hierbei wird Geld auf eine Chipkarte geladen. Bei den Chipkarten gibt es zum einen personenbezogene Karten, z. B. die EC-Karte mit Chip, zum anderen neutrale Karten, die keine Rückschlüsse auf den Inhaber zulassen. Beide Karten haben in ihrer Anwendung Vor- und Nachteile. Auch gibt es bereits erste Verfahren, bei denen über das Mobiltelefon die Zahlungsautorisierung erfolgen kann.

Welche Gefahren für das Persönlichkeitsrecht können bestehen?

- Derzeit weit verbreitet ist die Bezahlung durch die Übermittlung der Kreditkartendaten. Diese Daten können bei der Übermittlung von unbefugten Dritten im Internet abgefangen und missbraucht werden.
- Eine Gefahr besteht in der offenen Übermittlung von personenbezogenen Daten, die zum Abschluss eines Geschäftes notwendig sind. Bei unverschlüsselter Übertragung besteht die Möglichkeit, dass die Daten in jedem Zwischenserver ausgelesen und missbraucht werden können.
- Es muss damit gerechnet werden, dass der Auftragnehmer Persönlichkeitsprofile für Marketingzwecke erstellt.
- Die personenbezogenen Bestelldaten können an Dritte weitergegeben werden.
- Dritte können bei Bestellungen im Internet den Namen eines anderen Nutzers missbrauchen.

Durch welche Maßnahmen kann das Persönlichkeitsrecht besser geschützt werden?

- Nur auf eindeutig gekennzeichnete Angebote und Inhalte zugreifen und sichere Zahlungsverfahren verwenden.
- Darauf achten, dass sich die Internet-Anbieter im Hoheitsgebiet der Europäischen Union oder des Europäischen Wirtschaftsraumes oder in Staaten mit ausgewiesenem angemessenen Schutzniveau befinden.
- Verschlüsselungs-Techniken verwenden, die den gesetzlichen Bestimmungen entsprechen, um so weit wie möglich die Vertraulichkeit der elektronischen Interaktion zu gewährleisten, und über die digitale Signatur die Datenintegrität der Meldungen garantieren.
- Bei höherwertigen elektronischen Interaktionen ist es angezeigt, digitale Zertifikate zu verwenden und diese auf Chipkarten zu speichern.

Datenschutzrechtliche Regelungen

Das *Anbieten von Waren und Dienstleistungen* in elektronisch abrufbaren Datenbanken mit interaktivem Zugriff und unmittelbarer Bestellmöglichkeit *ist ein Teledienst* nach § 2 Abs. 2 Nr. 5 TDG. Somit gelten die Vorschriften des TDDSG für den Schutz personenbezogener Daten. Danach dürfen die Daten nur unter den engen gesetzlichen Voraussetzungen erhoben, verarbeitet und genutzt werden. Mit der Bestellung endet der Teledienst. Nach Absenden der elektronischen Bestellung unterliegen die Bestelldaten, dazu gehören auch die personenbezogenen Daten (u. a. Name, Adresse, Bankverbindung), als Inhaltsdaten dem BDSG. Aus dem Teledienste-Nutzer wird dann der Kunde. Daher können E-Commerce-Anbieter nur hinsichtlich des Anbietevorgangs nach dem TDG und TDDSG beurteilt werden. Der Anbieter muss seine Kunden vor Vertragsabschluss über die Geschäftsbedingungen informieren, also insbesondere seine Waren oder Dienstleistungen beschreiben, ihren Preis sowie etwaige Versandkosten benennen und auf das Widerrufs- und Rückgaberecht nach dem Fernabsatzgesetz hinweisen. Darüber hinaus hat der Diensteanbieter nach § 6 TDG für geschäftsmäßige Angebote Namen und Anschrift anzugeben.

Bei der Nutzung des Teledienstes angefallene Daten dürfen für Werbezwecke personenbezogen nach § 3 Abs. 2 TDDSG nur mit Einwilligung des Nutzers genutzt oder übermittelt werden.

Die *Inhaltsdaten* unterliegen insbesondere den Vorschriften nach § 28 BDSG. Danach ist die Nutzung der Daten für eigene Werbezwecke zulässig. Nach dem Listenprivileg des § 28 Abs. 2 Nr. 1b BDSG können die Daten auch an Dritte übermittelt werden (z. B. Name, Anschrift und die Tatsache, dass etwas bestellt wurde). Die E-Mail-Adresse, die Telefonnummer und Angaben über die Kontoverbindungen dürfen jedoch nicht ohne Einwilligung des Kunden zu Werbezwecken verwendet werden. Der Kunde hat nach § 28 Abs. 3 BDSG das Recht, der Nutzung seiner Daten zu Werbezwecken zu widersprechen.

2.1.5 Umgang mit elektronischer Post

Die elektronische Post (E-Mail) ist neben dem WWW-Dienst der am häufigsten benutzte Dienst im Internet.

Zum *Versenden und Empfangen einer E-Mail* ist eine weltweit eindeutige E-Mail-Adresse erforderlich. Die hierzu benötigte Internet E-Mail-Adresse beinhaltet zwei Teile, die durch das „@"-Zeichen getrennt sind. Zum Beispiel „poststelle@im.bwl.de". Der linke Teil vor dem „@" beschreibt die Kennung des Nutzers, der rechte Adressteil weist auf die eindeutige Adressierung des Rechners bzw. des Mail-Servers im Internet hin. Für die Kennung des Nutzers gibt es keine Vorschriften, sodass auch Pseudonyme verwendet werden können.

Wer eine E-Mail versenden möchte, benötigt auf seinem PC

– ein E-Mail-Client-Programm und/oder

– einen Internet-Browser,

– eine Verbindung zum Internet und

– einen Zugang zu einem Mail-Server.

Das E-Mail-Client-Programm ist immer einem PC zugeordnet. Es funktioniert nur in Verbindung mit einem Mail-Server oder mit dem Internet-Mail-Dienst eines Internet-Zugangsvermittlers. Bei der Verbindung zum Internet ist zu unterscheiden, ob der PC direkt mit dem Internet verbunden ist (a), wie z. B. im Falle eines betrieblichen Rechnernetzes, welches einen eigenen Mail-Server im Internet hat, oder ob der PC über einen Internet-Zugangsvermittler und einen Internet-Mail-Dienst mit dem Internet verbunden ist (b).

Das Erstellen, Versenden und Empfangen einer E-Mail ist einfach:

– Der Nutzer schreibt eine Nachricht auf seinem PC in sein E-Mail-Client-Programm und füllt das Adressfeld mit der E-Mail-Adresse des Empfängers aus.

– Durch einen Mausklick auf die Versende-Schaltfläche wird die E-Mail vom PC im Fall a) an den mit dem Internet verbundenen Mail-Server des eigenen Rechnernetzes (meistens Unternehmen oder Behörden) und von dort aus im Internet an den Mail-Server des Empfängers oder im Fall b) an eine Mailbox (Postfach) des Empfängers, in der Regel beim Internet-Diensteanbieter, übertragen. Im Fall b) eröffnet der PC des Absenders eine Verbindung zur Mailbox des Internet-Zugangsvermittlers zum Internet und die E-Mail wird über diesen Dienst an das Empfängerpostfach versandt. Die E-Mail kann in beiden Fällen über mehrere so genannte Mail-Relaisstellen (Knoten im Internet) geführt werden, bevor sie den Mail-Server oder die Mailbox des Empfängers erreicht.

– Die Inhalte einer Mail werden solange auf dem Mail-Server oder in der Mailbox gespeichert, bis der Nutzer diese in seinem PC abgerufen und anschließend dort gelöscht hat.

E-Mails können aber auch unter Nutzung des Internet-Browsers geschrieben, gelesen, empfangen und versendet werden. Hierzu werden die E-Mails vom Internet-Diensteanbieter auf Internet-Seiten zur Verfügung gehalten. Diese Technik wird auch als Webmail bezeichnet. Im Gegensatz zum E-Mail-Client-Programm kann Webmail von jedem Internet-Anschluss aus aufgerufen werden. Die Webmail-Technik wird insbesondere von freien E-Mail-Diensten, so genannten Freemailern, eingesetzt und wird u. a. auch für die Rückantwort auf Internetseitenbetreiber verwendet.

Welche Gefahren für das Persönlichkeitsrecht können bestehen?

– *Sammeln von E-Mail-Adressen*. E-Mail-Adressen sind wie Telefonnummern personenbezogene Daten des Inhabers. Über E-Mail kann schnell und billig Massenwerbung (Spam-Mails) verschickt werden. Deshalb kann es für Werbetreibende interessant sein, möglichst viele E-Mail-Adressen zu sammeln. Die einfachste Möglichkeit, an die E-Mail-Adressen zu kommen, ist das Erfragen und die Speicherung von E-Mail-Adressen, z. B. im Zusammenhang mit Bestellvorgängen, Zusendungen von Informationsmaterial und Nutzungen anderer Internet-Dienste oder das Kopieren von Absenderadressen von Chatroom-Teilnehmern. Ferner können E-Mail-Adressen aus öffentlich zugänglichen

E-Mail-Verzeichnissen (E-Mail-Directories) kopiert werden. Auch das Abfangen von E-Mail-Adressen während der Übermittlung ist technisch möglich, allerdings aufwändig.

– *Auswertung und Veränderung der Verkehrs- und Inhaltsdaten.* Die *Verkehrsdaten* werden für eine korrekte Übermittlung zwischen dem Absender und dem Empfänger benötigt. Das sind im Wesentlichen die E-Mail-Adressen von Sender und Empfänger, die TCP/IP-Adresse des Senders, der Weg, den die E-Mail über das Internet zurückgelegt hat, das Datum und der Zeitpunkt des Versands der E-Mail (Zeitstempel), die Größe der E-Mail und die Betreffzeile (hier wird auch über den Inhalt informiert). Die Verkehrsdaten werden in der Regel auf dem Versende- und Empfängersystem gespeichert. Sie können aber auch auf allen durchlaufenen Relaisstellen im Internet zwischengespeichert und damit dort ausgelesen und manipuliert werden.

  Die *Inhaltsdaten* einer E-Mail sind deren Text sowie gegebenenfalls angehängte Dateien (so genannte Attachments). Besonders darauf hinzuweisen ist, dass der Inhalt einer E-Mail den Vertraulichkeitsgrad einer Postkarte hat. Jeder, über dessen Knoten im Internet die E-Mail geleitet wird, und das sind wegen des Routings immer mehrere Knoten (auch im Ausland), hat die Möglichkeit, den Inhalt zu lesen und zu manipulieren.

– *Zusendung von unverlangten E-Mails (Spam-Mails).* Hierunter wird die Zusendung von E-Mails mit meist kommerziellen Inhalten an einen E-Mail-Empfänger verstanden, der vorher keinen Kontakt zum Absender hatte.

Durch welche Maßnahmen kann das Persönlichkeitsrecht besser geschützt werden?

– Einen behutsamen *Umgang* mit der *Eintragung*, *Registrierung* und *Verteilung* der eigenen E-Mail-Adresse.

– Nutzung von *E-Mail-Filtern* bei eingehenden E-Mails, die dafür sorgen, dass nur solche E-Mails empfangen werden können, die vom Nutzer für den Empfang freigegeben wurden. Damit lassen sich u. a. Massensendungen aussortieren.

– Anonymer Versand von E-Mails mittels *„Remail-Systemen“*. Hierbei werden vor dem Weiterversand durch den Remailer die Versandadresse entfernt und von ihm im Falle einer Rückantwort zur Weiterleitung an den Empfänger wieder hinzugesetzt.

– Einsatz von *Verschlüsselungssystemen* zur Wahrung der Vertraulichkeit und der Datenintegrität.

– Einsatz der digitalen Signatur. Sie dient der Erkennung, dass der Absender tatsächlich derjenige ist, der er zu sein angibt (Authentifizierung).

Datenschutzrechtliche Regelungen

Ein *E-Maildienst ist ein Teledienst* im Sinne des TDG. Der Schutz personenbezogener Daten bei Telediensten ist im TDDSG geregelt. Die bei den E-Maildiensten anfallenden Verkehrsdaten sind Nutzungsdaten. Die Auswertung dieser Daten, z. B. über Datenströme, ist zulässig, soweit keine personenbezogenen Daten erfasst werden. Eine Auswertung personenbezogener Daten durch die beteiligten Teledienstleister ist nur im Rahmen der engen Zweckbindung des TDDSG oder mit Einwilligung des Nutzers zulässig. Ein Zugriff auf die Inhaltsdaten durch die Teledienstanbieter ist datenschutzrechtlich und teledienstrechtlich nicht zulässig. Er stellt zudem einen Verstoß gegen das Fernmeldegeheimnis dar.

Für den Datentransport gilt das Telekommunikationsgesetz (TKG), da der E-Maildienst technisch mittels der Telekommunikation durchgeführt wird. Die Inhaltsdaten sind hier ebenfalls durch das Fernmeldegeheimnis geschützt.

Das *Sammeln von E-Mail-Adressen* durch den Teledienstanbieter ist nach § 3 Abs. 2 TDDSG unzulässig, durch die E-Mail-Empfänger im Übrigen datenschutzrechtlich wie das Sammeln von Postadressen zu bewerten. Adressen können nach § 28 BDSG zulässigerweise aus verschiedenen Quellen, wie z. B. nach § 28 Abs. 1 Nr. 1 BDSG aus Vertragsdaten, gesammelt und damit gespeichert werden. Ob das Sammeln von E-Mail-Adressen zulässig ist, kann nicht pauschal, sondern immer nur für den konkreten Einzelfall festgestellt werden. Liegt eine zulässige Erhebung vor, so dürfen die Adressen nach § 28 Abs. 1 Nr. 2 und Abs. 2 Nr. 1 b BDSG

für Werbezwecke genutzt werden. Der Beworbene hat jedoch nach § 28 Abs. 3 BDSG das Recht, einen Werbewiderspruch einzulegen.

Die *Zusendung unverlangter Werbe-E-Mails* ist jedoch auch dann unzulässig, wenn die E-Mail-Adressen für Werbezwecke datenschutzgerecht erhoben wurden. Nach gesicherter zivilrechtlicher Rechtsprechung stellt nämlich die Zusendung unverlangter Werbe-E-Mails, wie auch unverlangter Werbefaxe, eine Eigentumsstörung dar, da die Speicherung im Postfach technische Ressourcen bindet und der Abruf Kosten verursacht. Wird ein Werbewiderspruch nicht beachtet, kann der Betroffene eine zivilrechtliche Unterlassungsklage gegen das werbende Unternehmen erheben. Hat dieses Unternehmen seinen Sitz in Deutschland, kann sich der Betroffene auch an die zuständige Aufsichtsbehörde wenden. Gegen unverlangte Werbe-E-Mails aus dem Ausland haben die Aufsichtsbehörden aber keine Handhabe.

2.1.6 Zukünftige technische Entwicklung

UMTS (Universal Mobil Telecommunications System)-Endgeräte

Das Ziel von UMTS ist es, weltweit einen breitbandigen Mobilfunk-Zugang mit einer Übertragungsgeschwindigkeit von 384 kbit/s und in Gebäuden bis zu 2000 kbit/s zur Verfügung zu stellen. Zum Vergleich: die heutigen Technologien für Mobilfunk (Stand April 2001) lassen eine Übertragungsgeschwindigkeit von maximal 100 kbit/s zu. Mit der UMTS-Technologie können Sprache, Daten und Multimedia-Anwendungen auf mobile Endgeräte in kürzerer Zeit übertragen werden. Damit ist es möglich, mit einem einzigen mobilen Endgerät weltweit zu kommunizieren, sei es zu telefonieren, Faxe zu versenden, E-Mails zu übertragen oder im Internet zu surfen. Noch nicht einig sind sich die Fachleute, ob die Hauptanwendungen im Sprachdienst- (Telekommunikation) oder Datendienstebereich (Tele- und Mediendienste) liegen. Zumindest in der Anfangszeit wird der Sprachdienst für Kundenbindung und Umsätze sorgen. Die Fachleute prognostizieren aber auch dem Datendienst bereits für die nächsten Jahre (spätestens für 2005/2006) höhere Umsätze. Jedenfalls ist für UMTS ein zusätzliches eigenes Mobilfunknetz aufzubauen.

UMTS ist datenschutzrechtlich relevant. Schließlich tangiert es durch die multifunktionalen Möglichkeiten (Telefonieren, E-Mails übertragen, Surfen im Internet) den Datenschutz im Telekommunikations-, im Teledienste- und im Mediendienstebereich.

Eigenprofilierung des Internetnutzers

Jede Profilbildung über Cookies ist datenschutzrechtlich bedenklich, zumal das Ergebnis ungenau ist, da über das Cookie und die dazugehörige Datenbank nur das Nutzungsverhalten des Rechners und nicht das der ihn bedienenden Personen erfasst werden kann. Aus diesem Grund werden die Cookies in der Zukunft für die Erforschung des Nutzers an Bedeutung verlieren und Marketingformen Platz machen, bei denen der einzelne *Nutzer* selbst *auf freiwilliger Basis* seine *Profildaten offenbart* (Permission Marketing). Wenn diese Datenerhebung durch eine datenschutzrechtlich einwandfreie Einwilligung abgesichert wird und gesichert ist, dass die Daten nur entsprechend der Einwilligung genutzt werden, besteht die Möglichkeit, dass das unerlaubte Ausforschen des Internetnutzers abgebaut wird. Der Aufbau dieser Marketingform bedarf der eingehenden Überwachung und Betreuung durch die Aufsichtsbehörde.

Elektronischer Handel und elektronische Bezahlung in Internet

Der elektronische Handel im Internet (E-Commerce) wird erst dann zu einem Massenmarkt, wenn einfache und sichere Methoden zur Bezahlung zur Verfügung stehen. Es gibt auf dem Markt schon eine Vielzahl von sicheren Verfahren, diese kranken jedoch meist daran, dass sie von den Kunden als umständlich empfunden werden, da z. B. Kartenleser anzuschaffen sind oder besondere Software auf dem PC zu installieren ist. Ein neuer, viel versprechender Ansatz geht in Richtung der *Bezahlung unter Einsatz des Mobiltelefons.* Damit wäre dann auch die Brücke zum Handel über das Mobiltelefon (M-Commerce) geschlagen. Wie auch die zukünftigen Techniken und Verfahren aussehen werden, ihre Entwick-

lung und ihr Einsatz bedürfen der Begleitung durch die Aufsichtsbehörde, um sicherzustellen, dass die Persönlichkeitsrechte der Bürger gewahrt bleiben.

2.2 Einzelne Teledienste

Das Innenministerium ist nach § 8 TDDSG und nach § 18 des Mediendienste-Staatsvertrags die datenschutzrechtliche Aufsichtsbehörde über Teledienste und Mediendienste, die ihren Sitz in Baden-Württemberg haben.

Der überwiegende *Schwerpunkt der Aufsichtstätigkeit* bei den elektronischen Diensten lag bei den Telediensten, weil die Nutzung des Internets im Wesentlichen über die Nutzung von Telediensten erfolgt. Das heißt, jedes Angebot im Internet, das über die reine Informationsvermittlung an die Allgemeinheit hinausgeht, stellt im Regelfall einen Teledienst dar. Da das Teledienstерecht noch sehr jung ist und eine Vielzahl von Unternehmen sich im Gründungs- oder Konsolidierungsstadium befanden, lag der Schwerpunkt der Tätigkeit der Aufsichtsbehörde im Teledienstebereich in der Beratung von Unternehmen.

Um einen Überblick über die datenschutzrechtliche Situation bei den Telediensten im Lande zu erhalten, wurden verschiedene Fallgruppen gebildet, aus denen heraus stichprobenartig einzelne Teledienstеanbieter überprüft wurden.

2.2.1 Internetzugang

Die Zugangsmöglichkeit zum Internet für den privaten Nutzer schafft der Teledienstеanbieter, der den Netzzugang zur Verfügung stellt (Zugangsanbieter, Zugangsprovider). Es gibt Zugangsanbieter, bei denen sich der Nutzer anmelden muss und von denen er eine eigene Zugangskennung und ein Passwort erhält (fester Zugang), und Zugangsanbieter, über die der Nutzer ohne vorherige Anmeldung ins Internet gelangen kann (Call-by-Call).

Ergebnis der Überprüfung

Das Innenministerium hat im Berichtszeitraum mehrere *Zugangsanbieter* mit festem Zugang überprüft. Dabei wurden im Wesentlichen folgende Feststellungen getroffen, die hier zusammengefasst in allgemeiner Form wiedergegeben werden:

Der Nutzer schließt mit dem Zugangsanbieter einen *Vertrag über den Zugang* zum Internet gegen Entgelt ab. Neben dem Zugang erhält er einen Speicherplatz für eine eigene Homepage und ein E-Mail-Postfach. Ein neuer Nutzer erhält nach seiner Anmeldung mittels Briefpost seine Benutzerkennung und ein generiertes Passwort, das er beim ersten Netzaufruf ändern muss, zugeschickt.

Eine anonyme oder pseudonyme Nutzung ist bei dieser Zugangsart nicht möglich, da für die Abrechnung des Dienstes Bestands- und Nutzungsdaten des Nutzers benötigt werden. Mit der Anmeldung werden Name, Anschrift, Geburtsdatum, Telefon und Bankverbindung vom Nutzer erhoben. Dieser Datensatz wird um die Zugangsadresse und die E-Mail-Adresse ergänzt (Bestandsdaten). An Nutzungsdaten fallen Datum und Uhrzeit jeder Sitzung sowie die technischen Verbindungsdaten an. Die Summe der monatlichen Nutzungszeit wird dem Nutzer bei der Abrechnung mitgeteilt. Ein Einzelnachweis wird nur auf Anforderung erstellt, wenn Unstimmigkeiten über die Abrechnung bestehen. Die Nutzungsdaten werden nach Ausgleich der Rechnung gelöscht. Eine Weitergabe der Nutzungsdaten an Dritte oder eine Auswertung (Nutzerprofilierung) und Weitergabe der Auswertung erfolgt nicht. Die Inhalte der von dem Nutzer aufgerufenen Seiten (Inhaltsdaten) bzw. die von ihm übermittelten Daten (z. B. Mailinhalt) werden nicht erfasst.

Der *E-Mail-Dienst* ist nur für den Nutzer des Internetzugangs nutzbar. Die auf dem Mailserver gespeicherten E-Mails können von dem Systemverwalter des Servers eingesehen werden. Eingegangene, aber nicht gelesene Mails werden nach einer festgelegten Anzahl von Tagen automatisch gelöscht.

Die neu eingestellten bzw. geänderten *Homepages* werden vom Web-Master stichprobenartig auf unzulässige Inhalte nach § 8 des Mediendienste-Staatsvertrags hin überprüft. Werden dabei oder durch Informationen Dritter unzulässige Inhalte bekannt, so wird die Homepage vom Zugangsanbieter gesperrt.

Bei den Zugangsanbietern waren Datenschutzbeauftragte benannt, die Mitarbeiter mit Kontakt zu personenbezogenen Daten waren auf das Datengeheimnis verpflichtet.

Beanstandungen

Bei einem Zugangsanbieter wurde das *Nutzerpasswort* bei der Anmeldung fest vergeben und war für den Nutzer selbst nicht änderbar. Dies wurde beanstandet, da damit gegen Ziff. 1 (Zugangskontrolle) der Anlage zu § 9 BDSG verstoßen wurde. Das Zugangspasswort darf nur dem Nutzer selbst bekannt sein und muss von ihm jederzeit geändert werden können.

Mehrfach wurde festgestellt, dass der Zugangsanbieter die technische Ausführung an ein *fremdes Rechenzentrum vergeben* hatte. Hier stellte sich die Frage, ob das gegenüber dem Nutzer in Erscheinung tretende Unternehmen überhaupt noch selbst einen Teledienst erbringt oder ob eine so genannte *Funktionsübertragung* an ein anderes Unternehmen erfolgte. Bei einer Funktionsübertragung wird die eigentliche Datenverarbeitung durch eine andere Stelle in einem Umfang ausgeführt, der über die reine „handwerkliche" Datenverarbeitung im Auftrag hinausgeht. Zwischen den beiden Unternehmen findet in diesem Fall eine Übermittlung personenbezogener Daten statt. Da diese Übermittlung nicht nach § 28 BDSG zulässig ist, muss der Nutzer in die Übertragung nach § 4 Abs. 1 BDSG bei Vertragsabschluss einwilligen. Ferner ist die Anbieterkennzeichnung des § 6 TDG zu beachten.

Bei einem Unternehmen war die Übertragung als Funktionsübertragung zu bewerten. Es wurde beanstandet, dass die Kunden vor Vertragsabschluss nicht auf die komplette Ausführung des Teledienstes durch ein anderes Unternehmen und damit auf die Speicherung ihrer Daten dort hingewiesen wurden und dazu ihre Einwilligung erteilt haben.

Da der Systembetreuer des E-Mail-Servers die technische Möglichkeit hat, alle E-Mails zu lesen, muss er nach § 85 TKG auf das *Fernmeldegeheimnis verpflichtet* werden. Die fehlende Verpflichtung wurde in einem Fall beanstandet.

2.2.2 Internetportal

Unter einem *Internetportal* ist ein Internetauftritt zu verstehen, der unter einem Dach verschiedene Internetangebote wie z. B. allgemeine Informationen, Suchmaschinen, kostenlose Zusatzdienste und gewerbliche Angebote bereithält. Die Finanzierung erfolgt in der Regel über Einnahmen aus der Bannerwerbung und gegebenenfalls auch über Vermittlungsprovisionen. Ein Internetportal ist ein Teledienst im Sinne des § 2 Abs. 2 TDG.

Bei der Nutzung eines Internetportals fallen eine Vielzahl von Daten an, da die Rechner des Portalbetreibers über die Informationen verfügen, welcher Nutzer-PC welche Internetseiten aus dem Angebot des Portals aufruft. Kann dann noch festgestellt werden, welche Person (Nutzer) den betreffenden Seitenaufruf ausgeführt hat, so kann ein Interessenprofil des Nutzers (Nutzerprofil) erstellt werden, das z. B. zu Werbezwecken genutzt werden kann. Die Gefahr der Profilierung der Nutzer ist im Internet latent immer vorhanden. Allerdings muss einschränkend eingeräumt werden, dass es schwierig ist, den Aufrufer einer Seite zu identifizieren, da lediglich seine momentane TCP/IP-Adresse bekannt ist.

Die Erstellung eines personalisierten Nutzerprofils ohne die informierte Einwilligung des Betroffenen ist nach § 3 Abs. 1 und 5 TDDSG unzulässig. Bei den Überprüfungen der Internetportale richtete die Aufsichtsbehörde daher ihr Hauptaugenmerk auf das Setzen von Cookies, die Sammlung von Profilen von Aufrufern von Internetseiten und auf die Ermittlung von personenbezogenen Nutzerdaten (siehe Ziff. 2.1.2).

Ergebnis der Überprüfung

Das Ergebnis der Überprüfungen war insgesamt positiv. So wurden keine Nutzerdaten und Nutzungsdaten gespeichert. Wenn in Shops, die an das Portal angeschlossen sind, Bestellungen über das Internet getätigt werden konnten, erfolgte die Verarbeitung der personenbezogenen Daten der Besteller datenschutzgerecht. Der Portalbetreiber setzte bei dem Aufruf des Bestellformulars einen Link zum

eigentlichen Shop-Betreiber, sodass die personenbezogenen Bestell- und Zahlungsdaten direkt beim Shopbetreiber und nicht beim Internetportal anfielen.

Da es sich bei den überprüften Portalen rundweg um neu gegründete Unternehmen handelte, wurde von der Aufsichtsbehörde eine Beratung der zukünftigen Aktivitäten angeboten.

2.2.3 Kostenlose E-Mail-Postfächer

Neben den Zugangsanbietern, die ihren Kunden E-Mail-Postfächer anbieten, bieten andere Unternehmen *kostenlose E-Mail-Postfächer* für jedermann an. Auch hier liegt ein *Teledienst* im Sinne des § 2 Abs. 2 TDG vor. Ein größerer Anbieter von kostenlosen E-Mail-Postfächern wurde vor Ort überprüft.

Beim Betreiber des Dienstes fallen Bestandsdaten, Nutzungsdaten und Inhaltsdaten an. Bestandsdaten sind die Daten der Postfachinhaber, die sich über ihre Postanschrift identifizieren müssen. Eine anonyme Nutzung ist nicht vorgesehen. An Nutzungsdaten fallen der Zeitpunkt des jeweiligen Einbuchens und die TCP/IP-Adresse an. Diese technischen Daten werden mit dem Ende des Zugangs gelöscht. Das Datum des letzten Zugriffs des Nutzers wird bis zu seinem nächsten Zugriff gespeichert und dort angezeigt. Danach wird es gelöscht. Der Umfang der Inhaltsdaten wird durch den vorgegebenen Speicherplatz begrenzt. Ist das Postfach „voll“, so sind keine neuen Nachrichten mehr zustellbar. Der Zugriff auf das Postfach wird durch den Postfachnamen und ein individuelles Passwort geschützt. Eine Vergabe von Identifizierungsmerkmalen wie z. B. Cookies erfolgt nicht. Die Mitarbeiter sind auf das Datengeheimnis verpflichtet und ein betrieblicher Datenschutzbeauftragter ist bestellt. Der Teledienst konnte insgesamt als datenschutzgerecht beurteilt werden.

Beanstandet wurde das Abmeldeverfahren bei Postfächern, die von Dritten unter falschem Namen angelegt wurden. Hier wurden an die Abmeldung durch den Betroffenen, dessen Name und Adresse missbräuchlich genutzt wurde, mit dem Verlangen auf Vorlage einer Personalausweiskopie höhere Anforderungen als an die Anmeldung gestellt, was zur Preisgabe weiterer personenbezogenen Daten führte. Das Unternehmen hat zugesagt, das Abmeldeverfahren zu ändern.

2.2.4 Konzernunternehmen als Telediensteanbieter

Konzerne gehen zunehmend dazu über, Internetdienstleistungen zentral durch ein Konzernunternehmen erbringen zu lassen. Zu klären war insbesondere, in welchem Umfang das dienstleistende Konzernunternehmen (das im Folgenden *Konzern-Serviceprovider* – KSP – genannt wird) aus datenschutzrechtlicher Sicht verantwortlich ist und welche Rechtsvorschriften bei dessen Geschäftstätigkeit zu beachten sind. In diesem Zusammenhang geht es immer wieder auch um die Frage, inwieweit ein Arbeitgeber auf E-Mails der Mitarbeiter zugreifen darf.

Die Aufsichtsbehörde vertrat zu diesem Themenkomplex folgende Auffassung:

Vermittlung des Internetzugangs an Konzernmitarbeiter für betriebliche Zwecke

Der KSP betreibt einen *Teledienst* nach dem TDG und dem TDDSG. Nutzer des Teledienstes sind nicht die Mitarbeiter, sondern ist nach § 3 Nr. 2 TDG das jeweilige Konzernunternehmen, *für* dessen *betriebliche Zwecke* der Internetzugang eröffnet wird.

Nach dem im Entwurf vorliegenden Gesetz über die rechtlichen Rahmenbedingungen für den elektronischen Geschäftsverkehr, durch den u. a. das TDG und das TDDSG geändert werden, wird das TDDSG auf diese Fallkonstellation keine Anwendung mehr finden. Nach § 1 Abs. 1 Nr. 1 und 2 und § 2 Nr. 2 des novellierten TDDSG gilt das Gesetz nicht bei der Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten im Dienst- und Arbeitsverhältnis, soweit die Nutzung der Teledienste zu *ausschließlich beruflichen und dienstlichen Zwecken* erfolgt. Es gilt auch nicht innerhalb oder zwischen Unternehmen oder öffentlichen Stellen, soweit die Nutzung der Teledienste zur ausschließlichen Steuerung von Arbeits- und Geschäftsprozessen erfolgt und es werden juristische Personen von der Definition des Begriffs „Nutzer“ nicht mehr erfasst.

Unabhängig von der zu erwartenden Änderung der Rechtslage sind die Konzernmitarbeiter bei der betrieblichen Nutzung des Internetzugangs dem jeweiligen Unternehmen, bei dem sie beschäftigt sind (Beschäftigungsunternehmen), zuzurechnen. Für den Umgang mit ihren Daten gelten deshalb das TDG und das TDDSG nicht. Die Verarbeitung ihrer bei der Internetnutzung entstehenden Daten richtet sich beim Beschäftigungsunternehmen nach § 28 Abs. 1 Satz 1 Nr. 1 und 2 BDSG. Unbeschadet der Mitbestimmungsrechte des Betriebsrats nach dem Betriebsverfassungsgesetz dürfen die Daten *grundsätzlich auch zur Kontrolle* des Verhaltens und der Leistung verwendet werden. Aus diesem Grund sollte das Beschäftigungsunternehmen klare Regelungen über die zugelassene Internetnutzung, die Speicherung und Verwendung von Arbeitnehmerdaten sowie etwaige Kontrollverfahren treffen und den Mitarbeitern bekannt geben.

Das Beschäftigungsunternehmen kann den KSP auch mit der Verarbeitung von Arbeitnehmerdaten beauftragen. Das gilt insbesondere für die Protokollierung des Nutzungsverhaltens der Mitarbeiter zum Zweck der Verhaltens- und Leistungskontrolle oder für die Einrichtung sonstiger Kontrollsysteme. Für die Rechtmäßigkeit der Erhebung und Verarbeitung von Arbeitnehmerdaten bleibt das Beschäftigungsunternehmen verantwortlich. Dieses hat auch die Auskunfts- und Benachrichtigungspflichten nach dem BDSG gegenüber seinen Beschäftigten zu erfüllen. Der KSP wird in diesem Fall nicht als Teledienstеanbieter für die Mitarbeiter, sondern als Auftragsdatenverarbeiter für das Beschäftigungsunternehmen im Sinne des § 11 BDSG tätig.

Der KSP ist für die Gewährleistung der technischen Systemsicherheit, insbesondere der sicheren Abschottung der Datenverarbeitungsanlagen gegenüber unberechtigten Zugriffen aus dem Internet verantwortlich. Seine Verantwortlichkeit gründet sich auf § 9 BDSG.

Vermittlung des Internetzugangs an Konzernmitarbeiter für private Zwecke

In diesem Fall *sind die Mitarbeiter* von Konzernunternehmen nach alter und neuer Rechtslage *Nutzer im Sinne des TDDSG*, soweit ihnen der KSP eine Einwählmöglichkeit in das Internet *für private Zwecke* zur Verfügung stellt. Der KSP als Teledienstеanbieter hat seine Datenverarbeitungssysteme deshalb so zu gestalten, dass er seine Pflichten nach § 4 des bisherigen TDDSG erfüllen kann. Er hat insbesondere dafür zu sorgen, dass die private Nutzung eindeutig von der betrieblichen Nutzung zu trennen ist (z. B. durch die Bereitstellung differenzierter Nutzerkonten).

Der KSP hat die Daten der Konzernmitarbeiter über die Nutzung des Internetzugangs nach § 6 Abs. 2 des bisherigen TDDG (§ 6 Abs. 4 des novellierten TDDSG) frühestmöglich zu löschen. Rechnet der KSP die Kosten für die Privatnutzung des Internetzugangs (z. B. Fernsprechgebühren und kalkulatorische Kosten) unmittelbar mit den Konzernmitarbeitern ab, hat er dafür zu sorgen, dass *lediglich die für die Abrechnung erforderlichen Daten* gespeichert und verwendet werden. Dies sind regelmäßig nur Zeitpunkt und Dauer der Inanspruchnahme des Internetzugangs. Das Gleiche gilt, wenn der KSP die Kosten über das Beschäftigungsunternehmen abrechnet. Trägt das Beschäftigungsunternehmen die Kosten für die Privatnutzung des Internetzugangs durch seine Mitarbeiter, dürfen diesem nur anonymisierte und aggregierte Daten für Abrechnungszwecke weitergegeben werden.

Ist die private Nutzung des Internetzugangs durch Mitarbeiter vom Beschäftigungsunternehmen nur mit zeitlichem Limit zugelassen, kann der KSP im Auftrag des Beschäftigungsunternehmens die Nutzungsdauer aufzeichnen und diesem zu Kontrollzwecken zugänglich machen; für die Verarbeitung gilt insoweit § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Die für diesen Zweck gespeicherten personenbezogenen Daten sind jedoch in angemessener Zeit zu löschen. Die Zulässigkeit der Privatnutzung sollte mit allen Rahmenbedingungen, insbesondere auch den vorgesehenen Kontrollmöglichkeiten, in den Konzernunternehmen geregelt und den Mitarbeitern bekannt gegeben werden. Da sich die bei der Privatnutzung des Internetzugangs anfallenden Daten auch zur Verhaltens- und Leistungskontrolle eignen, sind die Mitbestimmungsrechte des Betriebsrats nach dem Betriebsverfassungsgesetz zu beachten.

E-Mail-Service für die betriebliche Kommunikation

Der KSP, der den E-Mail-Service für die *anderen Konzernunternehmen* betreibt (z. B. Mail-Server, Router), ist Diensteanbieter im Sinne des TDG. Er ist für die technische Sicherheit der Kommunikationseinrichtungen verantwortlich. Nutzer ist das jeweilige Konzernunternehmen, für dessen Geschäftsbetrieb E-Mails versandt oder empfangen werden. Daten aus dem *geschäftlichen E-Mail-Verkehr* stehen dem jeweiligen Konzernunternehmen zu. Dies gilt sowohl für die Inhalte empfangener und versandter E-Mails als auch für die näheren Umstände der E-Mail-Kommunikation. In Bezug auf die beim Transport von E-Mails anfallenden Telekommunikationsdaten unterliegt der KSP den einschlägigen Vorschriften des TKG. Gegenüber Dritten, die nicht an einem Kommunikationsvorgang beteiligt sind (z. B. die Konzernmutter), hat der KSP nach § 85 TKG auch das Fernmeldegeheimnis zu wahren. Er darf deshalb weder über die näheren Umstände von E-Mail-Kommunikation (Mail-Adressen, Verbindungszeit und -dauer, Umfang übertragener Mails oder Dateien) noch über deren Inhalt Auskunft geben.

E-Mail-Service für die Kommunikation der Konzernmitarbeiter

Datenschutzrechtlich ist hier danach zu unterscheiden, ob die private Nutzung des Mail-Systems erlaubt ist oder sich die Nutzung auf rein betriebliche Zwecke zu beschränken hat.

Ist in einem Unternehmen die *private Nutzung* erlaubt, ist der Arbeitgeber sowohl Anbieter von Telekommunikationsdiensten im Sinne des TKG als auch von Telediensten im Sinne des TDDSG. Besteht in einem Unternehmen die dienstliche Weisung, dass ein Mail-System *nur* für *betriebliche Zwecke* genutzt werden darf, ist der Arbeitgeber kein Anbieter im vorgenannten Sinne.

– Private Nutzung erlaubt

  Ist eine private Nutzung erlaubt, hat das Unternehmen grundsätzlich dafür zu sorgen, dass den Arbeitnehmern eine von der betrieblichen Nutzung getrennte private Nutzung (z. B. über unterschiedliche Adressen) möglich ist. Wenn eine solche Trennung der betrieblichen E-Mails von den privaten E-Mails bei erlaubter privater Nutzung systemtechnisch nicht vorgesehen ist, erstreckt sich die Geheimhaltungspflicht nach § 85 TKG (Fernmeldegeheimnis) nicht nur auf den privaten, sondern auch auf den betrieblichen E-Mail-Verkehr. Dann ist schon aus diesem Grund ein Zugriff des Arbeitgebers auf den Inhalt oder dessen Kenntnisnahme vom Inhalt jeder E-Mail unzulässig.

  Ist systemtechnisch eine Trennung von privater und betrieblicher Nutzung möglich, dann hat der Arbeitgeber dafür Sorge zu tragen, dass Inhaltsdaten der versandten und empfangenen privaten E-Mails unverzüglich nach dem Abruf bzw. dem Versand auf dem Mail-Server zu löschen sind. In jedem Fall können nach § 6 TDDSG Verbindungsdaten gespeichert werden, soweit diese notwendig sind, um die Inanspruchnahme des E-Mail-Dienstes gegenüber dem Arbeitnehmer unmittelbar abrechnen oder zur Abrechnung an Dritte weitergeben zu können.

  Wenn die Privatnutzung des E-Mail-Systems betriebsintern mengenmäßig oder zeitlich limitiert und diese Regelung den Arbeitnehmern bekannt gegeben worden ist, sind Missbrauchskontrollen durch das Unternehmen zulässig. Dazu können die erforderlichen Daten der Arbeitnehmer ausgewertet werden; auch dabei ist eine Kenntnisnahme vom Inhalt der privaten E-Mail-Kommunikation nicht zulässig.

– Private Nutzung ausgeschlossen

  Ist eine private Nutzung des E-Mail-Dienstes ausgeschlossen, dient die Zurverfügungstellung von E-Mail-Diensten am Arbeitsplatz *lediglich als Arbeitsmittel* zur Erfüllung der betrieblichen Aufgaben und ist gleichzusetzen mit der Zurverfügungstellung anderer Arbeitsmittel wie Telefon oder PC. Solche reinen Arbeitsmittel unterliegen grundsätzlich dem Direktionsrecht des Arbeitgebers.

  Für eine Protokollierung und Auswertung der E-Mail-Nutzung ist hier im Übrigen Folgendes zu beachten: In diesem Fall gilt zunächst § 31 BDSG. Werden die Daten im Zusammenhang mit der Nutzung des E-Mail-Dienstes nur für Zwecke der Datensicherung gespeichert, ist die sich aus § 31 BDSG ergebende Zweckbindung zu beachten. Mithin dürfen diese Daten dann nur für den Zweck der Datensicherung, nicht aber für andere Zwecke verwendet werden.

Sollen diese Daten auch zur Verhaltens- und Leistungskontrolle verwendet werden, sind die Mitbestimmungsrechte des Betriebsrates nach dem Betriebsverfassungsgesetz einzuhalten.

Bei der weiteren Prüfung der Frage der Zulässigkeit einer Kontrolle durch den Arbeitgeber ist auch der Inhalt einer eventuell vorhandenen Betriebsvereinbarung zu Grunde zu legen. Ebenso muss von vornherein die Zweckbindung entsprechend erweitert werden. Im Übrigen gilt für solche Kontrollen, dass der Verhältnismäßigkeitsgrundsatz gewahrt bleiben muss, so dass Kontrollen nur stattfinden dürfen, soweit sie im Rahmen der Zweckbestimmung des Arbeitsverhältnisses geeignet, erforderlich und angemessen sind.

Die Aufsichtsbehörde hat die Problematik zum Anlass genommen, in den HIM Nr. 37 vom 18. Januar 1999 (Staatsanzeiger für Baden-Württemberg Nr. 2 vom 18. Januar 1999, Seite 13) die generellen datenschutzrechtlichen Anforderungen zu veröffentlichen.

2.3 Technischer und organisatorischer Datenschutz

Bei allen technischen Überprüfungen wurde der Sicherheit der Datenverarbeitung das Hauptaugenmerk gewidmet. Ein datenschutzrechtlicher Verstoß liegt nicht nur dann vor, wenn eine Stelle beispielsweise unbefugt Daten verarbeitet, sondern auch dann, wenn sie zulässigerweise personenbezogene Daten verarbeitet, die Verarbeitung jedoch wegen technischer oder organisatorischer Mängel unsicher ist, sodass die Gefahr besteht, dass personenbezogene Daten verfälscht, vernichtet oder an unbefugte Dritte übermittelt werden können. Das BDSG hat in § 9 BDSG und der Anlage zu §9 die technischen und organisatorischen Anforderungen zur Gewährleistung der Datensicherheit und damit auch des Datenschutzes geregelt.

2.3.1 Datenspeicherung im Mobiltelefon

Dass die Reparatur von Mobiltelefonen zu Datenschutzproblemen führen kann, ergab sich aus mehreren Beschwerden betroffener Bürger. Ein Mobiltelefon ist nicht nur ein Kommunikationsgerät, sondern zugleich auch ein Datenspeicher, in dem der Nutzer ein Telefonverzeichnis mit Namen und Rufnummern anlegen kann. Die gespeicherten Rufnummern sind personenbezogene Daten, die insbesondere die regelmäßigen Kommunikationsbeziehungen des Geräteinhabers widerspiegeln. Die mit Namen gespeicherten Rufnummern sind auch personenbezogene Daten der Inhaber der betreffenden Anschlüsse. Deshalb kann ein Gerätedefekt zu datenschutzrechtlichen Problemen führen, wenn das *Mobiltelefon* ausgetauscht wird, ohne dass zuvor sein *Rufnummernspeicher* mit dem Telefonverzeichnis gelöscht wurde.

Verantwortung des Nutzers

Zwar ist grundsätzlich der Nutzer für die in seinem Mobiltelefon gespeicherten Daten verantwortlich und hat selbst dafür zu sorgen, dass das Telefonverzeichnis vor einem Geräteaustausch gelöscht wird. Dies wird von den Kunden *oftmals versäumt*, da sie vielfach der Meinung sind, dass das defekte Gerät von der Servicestelle vernichtet wird und der Kunde im Austausch dafür eine neues Gerät erhält. Vermutlich ist der geringe direkte Abgabepreis Ursache dieses Irrtums. Auch kann wegen der Art des Defekts der Rufnummernspeicher im Gerät vom Nutzer oftmals nicht mehr selbst gelöscht werden.

Die Herausgabe von Geräten mit Telefonverzeichnissen früherer Nutzer ist eine Datenübermittlung im Sinne des BDSG. Die Offenbarung der Kommunikationsbeziehungen früherer Nutzer greift in deren schutzwürdige Belange ein und ist nach § 28 BDSG nicht zu rechtfertigen.

Verantwortung des Vertreibers

Die Vertreiber von Mobiltelefonen, in der Regel die Mobilfunkgesellschaften oder ihre Provider, können deshalb nicht davon ausgehen, dass reparierte Geräte an andere als die ursprünglichen Nutzer unbesehen weitergegeben werden dürfen. Es liegt in ihrer Verantwortung, dafür zu sorgen, dass keine Mobiltelefone mit ungelöschten Rufnummernspeichern in Verkehr kommen. Rechtsgrundlage für diese Anforderung ist Ziff. 3 (Speicherkontrolle) der Anlage zu § 9 BDSG.

Zwar haben die Vertreiber von Mobiltelefonen in der Regel die Serviceunternehmen, welche die Gerätereparatur für sie vornehmen, zum Löschen des Speichers verpflichtet. Dass diese Verpflichtung eingehalten wird, muss aber von den Unternehmen durch geeignete Maßnahmen nach Ziff. 10 (Organisationskontrolle) der Anlage zu § 9 BDSG kontrolliert werden.

Die betroffenen Unternehmen wurden auf die *Lösch- und Kontrollpflicht* hingewiesen.

Die Aufsichtsbehörde hat die Fälle zum Anlass genommen, in den HIM Nr. 38 vom 18. Januar 2000 (Staatsanzeiger für Baden-Württemberg Nr. 2 vom 24. Januar 2000, Seite 12) generelle datenschutzrechtliche Anforderungen an den Umgang mit dem Mobiltelefonspeicher bei Gerätereparatur zu veröffentlichen.

2.3.2 Datenübermittlung beim Austausch von Computerfestplatten

Die Festplatte gehört als Datenspeicher zu den wichtigsten Bestandteilen eines Computers. Da die Daten im Regelfall auf ihnen unverschlüsselt abgespeichert werden, kann jeder, der in den Besitz einer *Festplatte* gelangt, von den Daten Kenntnis nehmen.

Eine PC-Eigentümerin wandte sich an die Aufsichtsbehörde, als sie feststellte, dass auf der in ihren PC eingebauten Ersatzfestplatte Texte und Tabellen mit personenbezogenen Daten eines Dritten vorhanden waren. Die ursprüngliche Festplatte war noch während der Garantiezeit ausgefallen, und die Kundin hatte deshalb den PC zum Händler zur Reparatur gebracht. Dieser gab den PC an eine Werkstatt weiter, die die *defekte Festplatte gegen eine andere Festplatte austauschte*. Da es sich bei dem Austausch um eine Garantieleistung handelte, ging die defekte Festplatte der Kundin an einen Reparaturbetrieb des Festplattenherstellers. Dort werden solche während der Garantiezeit ausgefallenen Festplatten soweit möglich repariert. Die reparierten Festplatten werden dann den Werkstätten als Austauschfestplatten für nachfolgende Garantiefälle zur Verfügung gestellt. Da die Daten des Vorgängers auf der reparierten Festplatte nicht gelöscht waren, kam die Kundin in den Besitz von dessen Daten, unter anderem von Bewerbungsschreiben, die sie mit der Textverarbeitung und Tabellenkalkulation lesen konnte. Sie hatte nun die Befürchtung, dass die ungelöschten personenbezogenen Daten auf ihrer alten Festplatte ebenso Dritten zur Kenntnis gelangen.

Bewertung der Aufsichtsbehörde

Gibt ein Kunde seinen PC zur Reparatur ab, obliegt es ihm als speichernder Stelle, *grundsätzlich selbst* für die Sicherung seiner Daten zu sorgen (Anfertigen von Sicherungskopien, Löschen einzelner Dateien oder der gesamten Festplatte). Ist dem Kunden die o. a. Sicherung auf Grund des Defekts nicht möglich, so muss er die Stelle, bei der er den PC zur Reparatur abgibt, und diese die weiter in den Reparaturvorgang einbezogenen Unternehmen darauf hinweisen, dass auf der Festplatte personenbezogene Daten gespeichert sind. In diesem Falle muss die Stelle, die den Austausch vornimmt, selbst oder durch Verpflichtung des Betriebs, der die Reparatur der Festplatte vornimmt, dafür sorgen, dass die Daten auf der alten Festplatte gelöscht werden, bevor sie nach ihrer Reparatur anderweitig weiterverwendet wird.

Sind auf der Festplatte Daten gespeichert, die einer *besonderen Schweigepflicht* im Sinne des § 203 StGB, wie z. B. der ärztlichen Schweigepflicht unterliegen, so darf der Kunde den PC bzw. die Festplatte nur dann zur Reparatur außer Haus geben, wenn die betreffenden Daten zuvor sicher gelöscht sind. Ist eine Löschung nicht möglich, so muss der Eigentümer dafür sorgen, dass die Platte datenschutzgerecht vernichtet und keiner Reparatur zugeführt wird.

Nimmt ein Händler den PC zur Reparatur an, ohne die Reparatur selbst durchzuführen, muss er den Kunden darüber aufklären, dass und an welche Werkstatt er den PC weitergibt und dass die Festplatte möglicherweise in einem anderen PC weiterverwendet wird. Es ist dann Sache des Kunden zu entscheiden, ob er unter diesen Voraussetzungen den Reparaturauftrag erteilt und ob eine Löschung erforderlich ist.

Ergebnis der Überprüfung

Im vorliegenden Fall war die Kundin nicht darüber informiert worden, dass der PC vom Händler zum Austausch der Festplatte an eine Werkstatt gegeben und ihre alte Festplatte von dort einem weiteren Unternehmen zur Reparatur übergeben wurde. Sie konnte daher nicht auf die Notwendigkeit der Löschung hinweisen. Dadurch bestand die Gefahr, dass ihre ursprüngliche Festplatte ungelöscht in einen anderen PC wieder eingebaut wird und somit ihre personenbezogenen Daten an unbekannte Dritte übermittelt werden. Eine nach Ziff. 10 (Organisationskontrolle) der Anlage zu §9 BDSG erforderliche organisatorische Maßnahme des Händlers wäre gewesen, die *Kundin* über den Reparaturweg und die mögliche Weiterverwendung zu *informieren.* Das Unterlassen der Information wurde beanstandet.

Der Unterschied zwischen der generellen Löschpflicht im vorausgegangenen Fall und der Löschpflicht nach Aufforderung durch den Kunden in diesem Fall liegt darin, dass der Speicher eines Telefons in aller Regel personenbezogene Daten des Inhabers und Dritter enthält. Bei einer Festplatte hingegen ist nicht automatisch davon auszugehen, dass auf ihr personenbezogene Daten gespeichert sind.

Die Aufsichtsbehörde hat den Fall zum Anlass genommen, in den HIM Nr. 37 vom 18. Januar 1999 (Staatsanzeiger für Baden-Württemberg Nr. 2 vom 18. Januar 1999, Seite 13) generelle datenschutzrechtliche Anforderungen an den Austausch von Festplatten zu veröffentlichen.

2.3.3 Übermittlung fremder Kontoauszüge durch einen Kontoauszugsdrucker

Ein Bürger beschwerte sich, dass er, als er an einem Kontoauszugsdrucker bei einer Filiale seiner Bank einen aktuellen *Kontoauszug ausdrucken* lassen wollte, den Auszug eines Dritten erhielt. Er hatte nun Sorge, dass sein Kontoauszug eventuell auch einem Dritten ausgedruckt wurde.

Ein Kontoauszug enthält sensible personenbezogene Daten und fällt unter den Regelungsbereich des BDSG. Um festzustellen, ob im Beschwerdefall die Vorschriften über den technischen und organisatorischen Datenschutz eingehalten waren, wurde der Vorgang eingehend überprüft.

Die Funktionsweise des Ausdruckvorgangs

Durch das Einstecken der Karte und die Eingabe der Geheimzahl in den Kontoauszugsdrucker veranlasste der Kunde im Rechenzentrum der Bank die Erstellung einer Druckdatei mit den betreffenden Kontobewegungen, die in einzelnen Datenpaketen vom Rechenzentrum an den Kontoauszugsdrucker geschickt wurde. Nach Beendigung der Übertragung startete der Drucker den Druckvorgang. Nach Abschluss des Drucks las der Drucker nochmals die Daten der EC-Karte aus, übermittelte sie als „Ausgabequittung“ an das Rechenzentrum und gab die EC-Karte und den Kontoauszug aus. Dauerte das Übertragen der Druckdatei vom Rechenzentrum zum Drucker zu lange, so brach der Drucker von sich aus den Vorgang ab, gab die EC-Karte aus und signalisierte dem Kunden und dem Rechenzentrum, dass ein Ausdruck nicht möglich ist.

Soweit die theoretische Funktionsweise. Der *tatsächliche Vorgang* sah wie folgt aus: Der Vorgänger des Beschwerdeführers versuchte am Kontoauszugsdrucker einen Auszug zu erhalten. Wegen einer Überlastung von Rechenzentrum und Netzwerk verzögerte sich die Übertragung der Druckdatei, sodass der Kontoauszugsdrucker den Vorgang abbrach, die Karte ausgab und die Abbruchmitteilung an das Rechenzentrum schickte. Da wegen der Netzüberlastung die Mitteilung des Kontoauszugsdruckers über den Abbruch verzögert beim Rechenzentrum ankam, war zwischenzeitlich dort die Druckdatei fertig gestellt und auf dem Weg zum Kontoauszugsdrucker. Zeitgleich mit der Ankunft des letzten Datenpakets der Druckdatei beim Kontoauszugsdrucker führte der Beschwerdeführer als nächster Kunde seine Karte in den Kontoauszugsdrucker ein, und der Drucker ratterte sofort los und arbeitete die gerade vollständig gewordene Druckdatei des Vorgängers ab. Nach dem Ende des Druckvorgangs las der Drucker nochmals die Kartendaten, gab den Kontoauszug aus und übermittelte die Kartendaten mit dem Merkmal „Auszug ausgegeben“ an das Rechenzentrum.

Beim Rechenzentrum war inzwischen die Abbruchmeldung des vorherigen Auftrags angekommen und wurde dahingehend verarbeitet, dass die noch nicht fertig

gestellte Druckdatei des Beschwerdeführers gelöscht wurde. Danach erhielt das Rechenzentrum die Quittung über die Ausgabe übermittelt. Letztere bezog das Rechenzentrum auf den Druckauftrag des Beschwerdeführers, bei dem in Wirklichkeit soeben die Druckdatei gelöscht worden war. Somit wurde der Druckauftrag des Beschwerdeführers nicht mehr ausgeführt. Sein Konto wurde jedoch mit dem Buchungsposten für den Auszug des Vorgängers belastet.

Ergebnis der Überprüfung

Wie von der Aufsichtsbehörde festgestellt wurde, hatte dieses System trotz mehrfacher Sicherungen *einen gravierenden Fehler:* Eine Ausgabesicherung war zwar vorhanden, diese prüfte aber nur, ob zum Zeitpunkt der Ausgabe überhaupt eine EC-Karte eingeführt war, jedoch nicht, ob dies auch die Karte war, mit der der Druckauftrag veranlasst wurde. Die Programmierung des Ausgabevorgangs hätte so gestaltet sein müssen, dass auch Letzteres geprüft wird. Nur durch diesen Programmfehler war es möglich, dass der Beschwerdeführer den Auszug seines Vorgängers erhalten konnte. Auch fehlte es an internen Plausibilitätskontrollen, weil ein Programmmodul den Auftrag stoppen, ein anderes Programmmodul den gestoppten Auftrag aber als ausgeführt verbuchen konnte.

Durch die Herausgabe des Auszugs wurden sensible personenbezogene Daten an einen nichtberechtigten Dritten übermittelt. Durch die unvollständige Ausgabekontrolle hat die Bank gegen Ziff. 10 (Organisationskontrolle) der Anlage zu § 9 BDSG verstoßen. Dies wurde gegenüber der Bank beanstandet. Das Verfahren wurde zwischenzeitlich durch die Aufnahme der geforderten weiteren Sicherungen geändert.

2.4 Auftragsdatenverarbeitung

Auftragsdatenverarbeiter sind Unternehmen, die personenbezogene Daten eines anderen Unternehmens in dessen Auftrag, nach dessen Vorgaben und unter dessen datenschutzrechtlicher Verantwortung verarbeiten. Es ist der typische Fall des *Subunternehmers*, der für die speichernde Stelle eine bestimmte Dienstleistung ausführt. Bei der Auftragsdatenverarbeitung findet keine Datenübermittlung im rechtlichen Sinn zwischen dem Auftraggeber und dem Auftragnehmer statt. Speichernde Stelle und damit verantwortlich für die Daten bleibt der Auftraggeber, der den Umfang der Verarbeitung der Daten in einem schriftlichen Auftrag festlegen muss. Die Grundlagen der Auftragsdatenverarbeitung sind in § 11 BDSG geregelt. Für den Auftragsdatenverarbeiter gelten neben den vertraglichen Pflichten die Vorschriften des BDSG über die Verpflichtung auf das Datengeheimnis, die Bestimmungen über die technisch-organisatorischen Maßnahmen nach § 9 BDSG und der Anlage zu § 9 BDSG sowie die Straf- und Ordnungswidrigkeitenvorschriften.

Von der Auftragsdatenverarbeitung zu unterscheiden ist die *Funktionsübertragung*, bei der nicht nur eine genau definierte Dienstleistung, sondern die Erfüllung einer bestimmten Aufgabe übertragen wird. Dort finden eine Datenübermittlung und ein Wechsel der Verantwortung statt.

2.4.1 Öffentlich zugängliche Bankkundendaten

Von einem besorgten Bürger wurde der Aufsichtsbehörde mitgeteilt, dass auf einem nicht eingezäunten Werkgelände einer Druckerei eine große Papierrolle mit Werbebriefen einer Bank mit aufgedruckten Kundendaten offen gelagert würden.

Ergebnis der Überprüfung

Adressdaten und Daten, die auf bestimmte Geschäftsbeziehungen hindeuten, z. B. auf die Kundenbeziehung zu einer Bank, sind personenbezogene Daten der Betroffenen. Die Aufsichtsbehörde überprüfte, ob dadurch gegen datenschutzrechtliche Vorschriften verstoßen wurde, dass hier Daten so gelagert waren, dass sich Dritte leicht Zugang zu ihnen verschaffen konnten.

Die Druckerei, die sich auf Werbedrucksachen spezialisiert hat, führte für eine Bank einen Druckauftrag durch, bei dem Werbebriefe mit Anschrift und persönlicher Anrede erstellt wurden. Die Adressdaten der Empfänger wurden von der

Bank zur Verfügung gestellt. Die Druckerei druckte lediglich die Adressdaten und die Anrede in die vorliegenden Werbebriefe ein (Letter-Shop) und brachte die Werbebriefe frankiert zur Post. Bei dem Unternehmen handelt es sich um einen *typischen Auftragsdatenverarbeiter*, der fremde Daten nach Anweisung verarbeitet. Die rechtlichen Voraussetzungen waren klar, ein detaillierter schriftlicher Auftrag lag vor. Das Unternehmen war im Register nach § 32 Abs. 1 BDSG gemeldet.

Bei der Überprüfung des Betriebsablaufs wurde festgestellt, dass es sich bei der offen gelagerten Papierrolle um eine Rolle mit Fehldrucken handelte, die vernichtet werden sollte. Damit Dritte den Inhalt nicht erkennen können, war die Rolle mit neutralem Papier umwickelt worden. Durch eine unzureichende betriebliche Organisation wurde die umwickelte Rolle jedoch im weiteren Fortgang für normalen Druckereiabfall gehalten und hinter das Gebäude zum Altpapiercontainer gelegt, wo sie von dem Bürger entdeckt wurde. Wer die Umhüllung entfernt hatte, konnte nicht mehr festgestellt werden.

Beanstandung

Auch wenn aus den Werbeschreiben nicht hervorging, ob die Adressaten Kunden der Absenderbank waren, lag diese Vermutung nahe. Unabhängig davon stellen aber bereits die aufgedruckten Adressen personenbezogene Daten dar. Durch ihre Lagerung im frei zugänglichen Betriebshof wurde es Dritten ermöglicht, unbefugt von ihnen Kenntnis zu erlangen. Dass es sich hier um ein Privatgelände handelt, ist datenschutzrechtlich unerheblich. Die schriftliche Anweisung durch den Auftraggeber war nicht zu beanstanden. Mit der *nicht ausreichenden Organisation* der Aufbewahrung personenbezogener Daten hatte die Druckerei jedoch gegen Ziff. 2 (Datenträgerkontrolle) der Anlage zu § 9 BDSG verstoßen. Die Rolle mit den Fehldrucken hätte danach bis zum Abtransport so gelagert werden müssen, dass sie nicht mit unkritischen Druckereiabfällen verwechselt werden konnte. Dieser Verstoß wurde beanstandet.

2.4.2 Überprüfung von Zustelladressen

Auf Bitten der Aufsichtsbehörde eines anderen Bundeslands wurde das Rechenzentrum, in dem die *Zustelladressdatenbank* (Referenzanschriftendatei) eines Postdienstunternehmens geführt wird, einer Überprüfung unterzogen. Das Rechenzentrum und die Datenbank wird von einem rechtsfähigen Tochterunternehmen (Unternehmen) dieses Postdienstunternehmens (Post) betrieben.

Ergebnis der Überprüfung

Die Referenzanschriftendatei wurde von dem Unternehmen selbst aufgebaut und wird als eigene Datei des Unternehmens geführt. Sie besteht aus den aktuellen Zustelladressen und wird von der Post für die Überprüfung von Sendungen mit unzureichender Adressierung genutzt. Ferner werden von dem Unternehmen mit der Datei Adressbestände gewerblicher Kunden überprüft. Hierbei werden die zu prüfenden Adressdaten vom gewerblichen Kunden per Datenträger oder per Datenfernübertragung an das Rechenzentrum des Unternehmens übermittelt und dort mit der Referenzanschriftendatei auf die Existenz der Zustelladresse und deren richtige Schreibweise verglichen, soweit erforderlich bereinigt und dann an den gewerblichen Kunden zurück übermittelt. Die Adressdaten des gewerblichen Kunden können auf den Rechnern des Unternehmens auch, je nach Auftrag, mit Telefonnummern, Geokoordinaten und mikrogeographischen Marktforschungsdaten (hauptsächlich) angereichert werden, die dazu von Dritten zur Nutzung angemietet werden.

Datenabgleich mit der Referenzanschriftendatei

Das Unternehmen führt die Referenzanschriftendatei im Auftrag der Post. Deshalb war zunächst zu prüfen, ob es sich auch um eine Verarbeitung personenbezogener Daten im Auftrag der Post oder um eine *geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung* nach § 29 BDSG handelt. Dadurch, dass das Unternehmen die Referenzanschriftendatei selbst aufgebaut hat und selbst aktualisiert, ist es Eigner der Datei. Mit der Anschriftenbereinigung, auch für die Post, verarbeitet es seine „eigenen“ Daten. Eine Auftragsdatenverarbeitung, bei der „fremde“ Daten verarbeitet werden, scheidet daher aus.

§ 5 der Postdienstunternehmen-Datenschutzverordnung (PDSV), nach dem Postdienstunternehmen Dritten Auskunft über die Richtigkeit einer Anschrift geben und Schreibfehler und ähnliche offenbare Unrichtigkeiten berichtigen dürfen, scheidet als Rechtsgrundlage aus, da das Tochterunternehmen selbst kein Postdienstunternehmen ist.

Die Datei war daher nach den Vorschriften des BDSG zu beurteilen. Es handelt sich hierbei um eine Datenspeicherung zum Zwecke der Übermittlung. Die Speicherung der Adressdaten in der Referenzanschriftendatei ist nach § 29 Abs. 1 BDSG zulässig, da die Angaben zum Teil aus öffentlich zugänglichen Quellen und Adresslisten erhoben wurden, zum Teil mit Einwilligung der Betroffenen gespeichert wurden. Nach der Überprüfung werden insoweit Daten übermittelt, als fehlerhafte Adressdaten berichtigt werden. Sowohl die Post als auch die gewerblichen Kunden, die ihren Adressbestand prüfen lassen, haben ein berechtigtes Interesse an einer postalisch richtigen Adresse. Schutzwürdige Interessen des Betroffenen an der Beibehaltung einer falschen Adresse sind nicht ersichtlich. Die *Übermittlung* ist daher nach § 29 Abs. 2 BDSG *zulässig*.

Adressdatenanreicherung

Die *Anreicherung* der *Adressdaten gewerblicher Kunden* durch das Unternehmen ist zulässig, weil es sich dabei um eine Datenverarbeitung im Auftrag handelt. Der gewerbliche Kunde liefert dem Unternehmen seine Adressdatei und bestimmt, welche Daten Dritter, in der Regel wohngebietsbezogene Angaben von gewerblichen Marktforschungsinstituten, in welcher Form den Adressen zugemischt werden. Das Unternehmen mietet dazu im Namen des gewerblichen Kunden diesen Marktforschungsdatenbestand an und verarbeitet damit die Adressdatei des gewerblichen Kunden, also fremde Daten. Nach Abschluss der Verarbeitung erhält der gewerbliche Kunde die Adressdatei in angereicherter Form zurück.

Die Voraussetzungen für die Auftragsdatenverarbeitung des § 11 BDSG waren bei dem überprüften Unternehmen erfüllt.

2.5 Videoüberwachung

Die Überwachung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist vom Anwendungsbereich des bisherigen BDSG nicht erfasst, da die Überwachung eines Objekts mittels Videotechnik und die Aufzeichnung der Aufnahmen nicht den Dateibegriff des Gesetzes erfüllen.

Unabhängig davon wird jedoch das *Recht auf informationelle Selbstbestimmung*, eine Ausprägung des allgemeinen Persönlichkeitsrechts nach Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 2 des Grundgesetzes, durch die Videoüberwachung dadurch eingeschränkt, dass der Einzelne nicht mehr selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen kann. Der Aufenthalt an einem bestimmten Ort zu einer bestimmten Zeit ist ein personenbezogenes Datum des Betroffenen.

Auslegung des Rechts auf informationelle Selbstbestimmung

Die Aufsichtsbehörden im „Düsseldorfer Kreis“ haben daher 1997 einen Beschluss zu den Voraussetzungen einer zulässigen Videoüberwachung gefasst. In Anlehnung an diesen Beschluss hielt die Aufsichtsbehörde Einschränkungen des Rechts auf informationelle Selbstbestimmung durch eine Videoüberwachung unter folgenden Voraussetzungen für zulässig:

- Die Videoüberwachung muss im Rahmen des Hausrechts geboten sein.
- Auf die Videoüberwachung muss vor dem Eintritt in den Aufnahmebereich der Kameras gut erkennbar hingewiesen werden, sofern die Kameras selbst nicht gut erkennbar sind.
- Erfolgt eine Videoüberwachung durch direkte Beobachtung über den Monitor, darf eine Aufzeichnung nur dann erfolgen, wenn sich bei der Überwachung der Verdacht einer Straftat oder sonstigen nicht rechtmäßigen Handlung ergeben hat. Ist eine direkte Überwachung aus objektiven Gründen nicht möglich, darf generell eine Aufzeichnung erfolgen. Die Aufzeichnung darf aber nur dann eingesehen werden, wenn zumindest der Verdacht besteht, dass im Aufzeich-

nungszeitraum eine Straftat oder nicht rechtmäßige Handlung begangen wurde. Besteht ein solcher Verdacht nicht, ist die Aufzeichnung unverzüglich zu löschen. Werden Aufnahmen als Beweismittel benötigt, darf nur die betreffende Sequenz oder Folge von Einzelbildern als Beweismittel gespeichert bzw. genutzt, insbesondere an die Strafverfolgungsbehörden weitergegeben werden.

Nach diesen Kriterien beriet die Aufsichtsbehörde die Unternehmen, darunter auch einen Verkehrsbetrieb, der seine Fahrzeuge mit Videokameras ausstatten wollte. Der Verkehrsbetrieb hat die Einhaltung der Vorgaben der Aufsichtsbehörde zugesagt.

Einem Amtsgericht, das zur Klärung der Frage der Verwertbarkeit einer Videoaufzeichnung im Rahmen eines Strafverfahrens wegen eines Kaufhausdiebstahls die Aufsichtsbehörde um eine datenschutzrechtliche Beurteilung der Zulässigkeit von Videoüberwachungen ersuchte, wurde ebenfalls diese Rechtsauffassung mitgeteilt. Das Amtsgericht lehnte dann die Zulassung der Videoaufzeichnung als Beweismittel ab, da die Videoüberwachung im konkreten Fall verdeckt erfolgte, und sprach die Angeklagte frei. Das Urteil ist nicht rechtskräftig.

Neue gesetzliche Regelung

Das novellierte BDSG bezieht die Videoüberwachung in den Geltungsbereich des Gesetzes ein und regelt in § 6b die Zulässigkeitsvoraussetzungen für die *Beobachtung öffentlich zugänglicher Räume* mit optisch-elektronischen Einrichtungen. Danach ist die Videoüberwachung durch nichtöffentliche Stellen zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Der Umstand der Überwachung und die verantwortliche Stelle müssen durch geeignete Maßnahmen erkennbar gemacht werden. Darüber hinaus bestehen eine enge Zweckbindung für die Verarbeitung und Nutzung der dabei erhobenen Daten, eine Pflicht, den Betroffenen zu benachrichtigen, wenn die erhobenen Daten seiner Person zugeordnet werden, und eine unverzügliche Pflicht zur Löschung der Daten, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen des Betroffenen einer weiteren Speicherung entgegenstehen.

3. Auskunfteien und Kreditschutzorganisationen

3.1 Datenerhebung und Datenübermittlung durch Auskunfteien und Kreditschutzorganisationen

Bei der Aufsichtsbehörde gehen in jedem Jahr eine größere Zahl von Beschwerden ein, die sich auf die Fragen beziehen, ob Datenerhebungen und Datenübermittlungen durch Auskunfteien und Kreditschutzorganisationen (SCHUFA) datenschutzrechtlich zulässig sind und welche Rechte den Betroffenen dabei zustehen. In diesen Fällen erhalten die Betroffenen von der Aufsichtsbehörde jeweils eine umfassende Aufklärung über die bestehende Rechtslage.

Datenerhebung

Auskunfteien beschäftigen sich im Wesentlichen damit, Informationen zur Beurteilung der Kreditwürdigkeit, d. h. Zahlungsfähigkeit und Zahlungswilligkeit (sog. Negativdaten) von Privatpersonen und Firmen auch ohne deren vorherige Einwilligung zu erheben, zu speichern und bei Anfragen von Dritten an diese zu übermitteln. Die grundsätzliche Zulässigkeit des geschäftsmäßigen Speicherns personenbezogener Daten durch Auskunfteien zum Zwecke der Übermittlung ergibt sich aus § 29 Abs. 1 BDSG. In diesem Zusammenhang darf die erhebliche Bedeutung solcher Auskunfteien und Kreditschutzorganisationen im Wirtschaftsleben bei der Gewährung von Geld- oder Warenkrediten für die Kreditgeber nicht verkannt werden. Dabei geht es nicht nur um den Schutz der Kreditgeber vor Kreditausfällen, sondern zugleich auch um den Schutz der Kreditnehmer vor einer übermäßigen Verschuldung.

Die Informationen beziehen die Auskunfteien zunächst aus allgemein zugänglichen Quellen, wie z. B. Vereinsregister, Handelsregister oder auch über die Schuldnerverzeichnisse der Amtsgerichte. Diese Informationserhebung und deren Speicherung aus allgemein zugänglichen Quellen ist nach § 29 Abs. 1 Satz 1 Nr. 2 BDSG zulässig. Informationen erhalten die Auskunfteien zudem durch Selbstauskünfte der Betroffenen.

Darüber hinaus sind auch Mitteilungen von Inkassobüros oder Vertragspartnern der Auskunfteien (die Auskünfte erhalten, wenn sie im Gegenzug Daten, die für die Beurteilung der Bonität relevant sind, der Auskunftei mitteilen) nach § 28 Abs. 2 Satz 1 Nr. 1 a BDSG und entsprechend deren Speicherung bei der Auskunftei nach § 29 Abs. 1 Satz 1 Nr. 1 BDSG zulässig. Die Zulässigkeit setzt dabei eine Abwägung der schutzwürdigen Interessen des Betroffenen mit den berechtigten Interessen eines Dritten voraus. Nach der Rechtsprechung ist damit die Übermittlung bestimmter Kreditdaten an Auskunfteien im Sinne eines Kreditinformationssystems gestattet, das eine Kreditvergabe an Kreditunwürdige verhindern und damit den Interessen der Kreditgeber, aber auch der Allgemeinheit und der Kreditnehmer selbst dienen soll. Eine Übermittlung von Daten über nichtvertragsgemäßes Verhalten von Inkassobüros oder Vertragspartnern über Betroffene an eine Auskunftei ist daher nur zulässig, wenn ein Sachverhalt vorliegt, der eindeutige Rückschlüsse auf eine Zahlungsunfähigkeit oder -unwilligkeit des Betroffenen erlaubt. Dies ist z. B. gegeben, wenn ein Vollstreckungsbescheid oder eine Zwangsvollstreckung vorliegen.

Bei der *SCHUFA* besteht die Besonderheit, dass auch sog. Positivdaten, also Daten von Betroffenen, bei denen kein vertragswidriges Verhalten vorliegt, gespeichert und zu Auskunftszwecken übermittelt werden. Darunter fallen z. B. Angaben über das Bestehen eines Girokontos oder den Abschluss eines Kreditvertrages. Die Meldung solcher Daten eines Betroffenen insbesondere von Kreditinstituten an die SCHUFA und die Erteilung von Auskünften dazu durch die SCHUFA ist nur dann zulässig, wenn vorher eine entsprechende Einwilligung des Betroffenen erfolgte. § 28 Abs. 1 Satz 1 Nr. 2 sowie Abs. 2 Satz 1 Nr. 1 a BDSG sind hier nämlich nicht auf das meldende Kreditinstitut anwendbar, da kein berechtigtes Interesse von Kreditinstituten oder sonstiger Dritter dafür ersichtlich ist, dass diese Daten über ein vertragsgemäßes Verhalten eines Betroffenen an eine Kreditschutzorganisation übermittelt werden. Im Übrigen gelten auch für die SCHUFA die obigen Ausführungen.

Datenübermittlung

Nach § 29 Abs. 2 Satz 1 BDSG ist die Übermittlung personenbezogener Daten durch Auskunfteien oder die SCHUFA an Dritte zulässig, wenn diese als Empfänger ein berechtigtes Interesse an der Kenntnis glaubhaft dargelegt haben und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Von den Auskunfteien werden diese Daten auf Anfrage z. B. an Banken, Einzelhandels-, Versandhandels- und sonstige Unternehmen (z. B. Handy-Anbieter), die wegen wirtschaftlicher Vorleistungen finanzielle Kreditrisiken eingehen, übermittelt. Grundsätzlich trifft die Auskunftei die Verantwortung für die Zulässigkeit der Übermittlung der Daten der Betroffenen an die anfragenden Dritten. Sofern jedoch ein automatisiertes Abrufverfahren eingerichtet wurde, was häufig der Fall ist, geht die Verantwortung für die Zulässigkeit des einzelnen Abrufs nach § 10 Abs. 4 Satz 1 BDSG auf den Empfänger, also die anfragende Stelle über. Die Auskunftei als speichernde Stelle hat dann nach § 10 Abs. 4 Satz 2 BDSG nur noch die Zulässigkeit der Abrufe zu prüfen, wenn dazu Anlass besteht. Allerdings haben die Auskunfteien wegen § 10 Abs. 4 Satz 3 BDSG zu gewährleisten, dass die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann.

Speicherung, Auskunftserteilung, Sperrung und Löschung von Daten

Über die *Speicherung* der Daten muss eine Auskunftei oder die SCHUFA die Betroffenen wegen § 33 Abs. 1 Satz 2 BDSG zunächst nicht benachrichtigen. Erst dann, wenn sie erstmals Daten an Dritte übermittelt, muss sie den Betroffenen davon unterrichten und ihm dabei nach § 33 Abs. 1 Satz 2 BDSG die Art der weitergegebenen Daten mitteilen. Aus der Tatsache, dass ein Betroffener von einer Auskunftei oder der SCHUFA erstmals über die Datenspeicherung unterrichtet wird, ist jeweils zu folgern, dass die Auskunftei oder die SCHUFA unmittelbar zuvor eine Anfrage zu dem Betroffenen beantwortet hat.

Die Betroffenen können bei der Auskunftei oder der SCHUFA jederzeit nach § 34 Abs. 1 BDSG *Auskunft* über die zu ihrer Person gespeicherten Daten und den Zweck der Speicherung verlangen. Jedoch haben die Betroffenen nach der gesetzlichen Regelung grundsätzlich keinen Anspruch auf Auskunft darüber, von wem die Auskunftei oder die SCHUFA die Daten erhalten hat (Herkunft der Daten) und an wen die Daten übermittelt worden sind (Empfänger der Daten). Nur wenn die Betroffenen begründete Zweifel an der Richtigkeit der Daten geltend machen können, muss ihnen die Auskunftei oder die SCHUFA nach § 34 Abs. 1 Satz 3 BDSG Herkunft und Empfänger der Daten nennen. Diese Regelung wird von den Betroffenen insbesondere dann als unzureichend empfunden, wenn sie keinerlei Vorstellung darüber haben, an wen die sie betreffenden Daten übermittelt wurden.

Dieses Thema wurde auch im Düsseldorfer Kreis mit dem Verband der Handelsauskunfteien (VdH) erörtert. Dabei konnte erreicht werden, dass unbeschadet der gesetzlichen Regelung die Auskunfteien folgende Verfahrensweise akzeptieren: Die Aufsichtsbehörde wendet sich an die Auskunftei und diese holt dann ihrerseits beim Empfänger die Einwilligung in die Weitergabe seines Namens an den Betroffenen ein. Die Auskunftei teilt dem Betroffenen anschließend den Empfänger mit. Voraussetzung für dieses Verfahren bleibt aber eine Begründung, weshalb der Betroffene Kenntnis vom Empfänger erhalten will; bloße Neugier des Betroffenen über den Empfänger der Daten reicht nicht aus.

Wenn die Betroffenen die Richtigkeit einzelner Daten bestreiten und die Auskunftei oder die SCHUFA nicht in der Lage ist, die Richtigkeit der gespeicherten Daten nachzuweisen, dann muss diese nach § 35 Abs. 4 BDSG die Daten *sperren*. Über gesperrte Daten darf nur noch in den in § 35 Abs. 7 BDSG genannten engen Ausnahmefällen Auskunft erteilt werden.

Stellt sich bei der Überprüfung heraus, dass die Daten unrichtig sind, sind sie nach § 35 Abs. 1 BDSG zu berichtigen, was ggf. auch bedeuten kann, dass die Daten zu löschen sind. Im Übrigen besteht nach § 35 Abs. 2 BDSG insbesondere ein Anspruch auf Löschung von Daten, wenn die Speicherung unzulässig ist, z. B. wenn die Daten nicht auf rechtmäßige Weise beschafft worden sind, oder wenn eine Prüfung am Ende des fünften Kalenderjahres nach ihrer erstmaligen Speicherung ergibt, dass eine längere Speicherung nicht erforderlich ist. Eintragungen aus dem Schuldnerverzeichnis der Amtsgerichte über eidesstattliche Versicherungen

und Haftbefehle zur Erzwingung der Abgabe der eidesstattlichen Versicherung werden nach Ablauf des dritten auf die Abgabe der eidesstattlichen Versicherung oder die Anordnung der Haft folgenden Kalenderjahres gelöscht. Wird gegenüber dem Amtsgericht nachgewiesen, dass die zu Grunde liegende Forderung beglichen ist, löscht das Amtsgericht die Eintragung im Schuldnerverzeichnis und teilt dies turnusgemäß der Auskunftei oder der SCHUFA mit, die ebenfalls eine Löschung vornimmt. Wird eine umgehende Löschung im Datenbestand der Auskunftei oder der SCHUFA gewünscht, ist eine Löschungsbescheinigung des Amtsgerichts bei der Auskunftei oder der SCHUFA einzureichen.

In einigen Beschwerdefällen konnte durch die Einschaltung der Aufsichtsbehörde erreicht werden, dass unrichtig gespeicherte Daten berichtigt oder gelöscht worden sind. Zudem konnten Löschungen erreicht werden in Fällen, in denen die Nichterfüllung einer Forderung von einer Auskunftei gespeichert war, obwohl die Forderung vom Betroffenen dem Grunde und/oder der Höhe nach bestritten war und damit kein Rückschluss auf eine mangelnde Bonität des Betroffenen gezogen werden konnte.

3.2 Besondere Fälle der Datenspeicherung bei Auskunfteien

Ausgehend von den unter Ziff. 3.1 dargestellten allgemeinen Grundsätzen waren auch die beiden folgenden Fälle von der Aufsichtsbehörde zu bewerten:

Mahnbescheid

Im ersten Fall wandte sich eine Betroffene dagegen, dass eine Auskunftei die bei ihr gespeicherte Tatsache, dass ein *Mahnbescheid* wegen einer Geldforderung ergangen war, nicht sperren wollte, obwohl gegen den Mahnbescheid Widerspruch eingelegt wurde. Dem unstreitig ergangenen Mahnbescheid vorausgegangen war eine Zahlungsaufforderung durch die Gläubigerin, auf die die Betroffene nicht reagiert hatte.

Bei einer solchen Fallkonstellation bestehen nach Ansicht der Aufsichtsbehörde keine Bedenken gegen eine Speicherung der Tatsache, dass ein Mahnbescheid gegen die Betroffene erlassen wurde. Schließlich ist ein Mahnbescheid für sich genommen ein ausreichendes Merkmal, das auf eine mangelnde Bonität schließen lässt. Auch ein später gegen den Mahnbescheid eingelegter Widerspruch ändert hieran nichts mehr. Allerdings ist die Tatsache des Widerspruchs gegen den Mahnbescheid hinzuzuspeichern, um ein zutreffendes Bild zu vermitteln.

Vollstreckungsbescheid

Im zweiten Fall wurden nach Zahlungsaufforderungen durch ein Inkassounternehmen ein Mahnbescheid und im Anschluss daran ein *Vollstreckungsbescheid* erlassen. Erst nach der Zustellung des Vollsteckungsbescheides erfolgte die Zahlung durch den Betroffenen. Der Betroffene wollte, dass die dazu gespeicherten Daten bei der Auskunftei gelöscht werden. Auch hier gilt, dass ein Mahnbescheid und erst recht ein Vollstreckungsbescheid ausreichen, um auf eine mangelnde Bonität schließen zu können. Der nach Erlass des Vollstreckungsbescheides erfolgte Zahlungsausgleich ändert nichts daran, dass erst ein Mahn- und ein Vollstreckungsbescheid erwirkt werden mussten, um eine Zahlung auf eine berechtigte Forderung zu erreichen.

Diese Daten zu den Mahn- und Vollstreckungsbescheiden sind auch trotz Zahlung nach § 35 Abs. 2 Nr. 4 BDSG erst am Ende des fünften Kalenderjahres nach ihrer erstmaligen Speicherung zu löschen, wenn eine Prüfung ergibt, dass eine länger währende Speicherung nicht erforderlich ist. Nachdem die Forderung beglichen wurde, kommt eine längere Speicherung allerdings nicht in Betracht.

3.3 Personenverwechslung

Hin und wieder stellt sich im Zusammenhang mit Beschwerden heraus, dass es bei der Erteilung von Auskünften durch Auskunfteien an anfragende Dritte zu *Personenverwechslungen* kommt. Dies hat zur Folge, dass an den anfragenden Dritten, der die Bonität eines Kunden prüfen will, Daten übermittelt werden, die mit dem Kunden nichts zu tun haben, jedoch für diesen negative Merkmale ent-

halten. Auf Grund solcher negativen Auskünfte werden die Kunden dann z. B. von Versandhandelsunternehmen nicht gegen Rechnung beliefert oder erhalten von Telekommunikationsunternehmen kein Handy.

Grundsätzlich gilt in solchen Fällen, dass datenschutzrechtlich eine solche Personenverwechslung nicht vorkommen sollte und im Ergebnis eine Verletzung von Datenschutzrechten vorliegt.

Auf Grund der Vielzahl der bei Auskunfteien anfallenden Vorgänge sind jedoch Personenverwechslungen nie ganz auszuschließen. So kann auch bei einem Vergleich zwischen den Personalien derjenigen Personen, zu denen eine Anfrage eingeht, mit den Personalien der gespeicherten Personen nicht immer und in jedem Fall eine vollständige Übereinstimmung verlangt werden. Geringfügige Abweichungen können z. B. auf Hör- und Erfassungsfehlern beruhen, etwa wenn eine Anfrage auf Grund eines handschriftlich ausgefüllten Antrags vorgenommen wird und beim Ablesen des Antrags und der Übernahme von Daten für Zwecke der Anfrage Fehler gemacht werden. Auch ist festzustellen, dass die Betroffenen bei ihren Angaben gelegentlich selbst Variationen vornehmen und beispielsweise anstelle eines Doppelnamens nur den ersten Namen eintragen oder ihren Vornamen mit einem Buchstaben abkürzen, wenn sie etwas bestellen.

In solchen Fällen kommt es naturgemäß zu einer gewissen Fehlerquote bei der Prüfung der Personenidentität. Allerdings hält sich die Zahl von Personenverwechslungen nach dem bisherigen Eindruck der Aufsichtsbehörde insgesamt in Grenzen und ist auf nie ganz ausschließbare Einzelfälle beschränkt. Zudem ist in diesen Fällen zu berücksichtigen, dass sich die Auskunfteien bei Personenverwechslungen stets bereit gezeigt haben, entsprechende Korrekturen oder spezielle Hinweise in ihren Datenbeständen aufzunehmen, um künftige Verwechslungen zu vermeiden.

In diesem Zusammenhang wird von der Aufsichtsbehörde die Praxis einer Auskunftei, Auskünfte auch dann zu erteilen, wenn zwischen den Daten der angefragten Person und den Daten der gespeicherten Person *geringfügige Abweichungen* bestehen, kritisch betrachtet. Ob hier eine Korrektur erforderlich wird, ist auch anhand der Praxis zu entscheiden. Da die Zahl der Verwechslungsfälle bisher gering geblieben ist, sah die Aufsichtsbehörde bislang noch keine Veranlassung, grundsätzliche Veränderungen von der Auskunftei zu verlangen. Dabei ist auch zu berücksichtigen, dass im Versandhandel jährlich hohe Verluste durch uneinbringliche Forderungen dadurch entstehen, dass zahlungsunfähige oder -unwillige Personen häufig wissen, dass Versandhandelsunternehmen Bonitätsprüfungen über Auskunfteien durchführen und daher versuchen, diese Prüfungen zu unterlaufen, indem sie eine leicht veränderte Schreibweise von Vor- oder Nachnamen, Anschriften und/oder falsche Geburtsdaten angeben.

3.4 SCHUFA-Score-Wert

Im Jahr 1996 wurde von der SCHUFA das Score-Verfahren ASS eingeführt, mit dem die SCHUFA eine zusätzliche Auskunftsdienstleistung neben den sonstigen bisherigen Auskünften über das Bestehen und die Abwicklung von Kreditverhältnissen für ihre Vertragspartner anbietet. Den Vertragspartnern der SCHUFA, die diese Dienstleistung in Anspruch nehmen, wird dabei ein so genannter *Score-Wert, der eine Prognose des Kreditausfallrisikos* darstellt, mitgeteilt. Zu beachten ist, dass von der SCHUFA der Score-Wert nicht isoliert, sondern nur im Zusammenhang mit einer Auskunft, die auch die sonstigen zum Betroffenen vorhandenen Daten der SCHUFA enthält, an die Vertragspartner übermittelt wird.

Diese von der SCHUFA an ihre Vertragspartner mitgeteilten Score-Werte haben das Innenministerium sowohl im Düsseldorfer Kreis als auch als Aufsichtsbehörde bei Beschwerden intensiv beschäftigt. Von den Betroffenen wird insbesondere die fehlende Transparenz bemängelt.

Die Auskunft der SCHUFA einschließlich des Score-Wertes dient als *zusätzliche Entscheidungshilfe* der Unterstützung des Kreditgebers bei seiner Entscheidung über die Kreditvergabe, indem Informationen über die Kreditwürdigkeit des Betroffenen zur Verfügung gestellt werden. Hier ist jedoch von den Kreditgebern zu beachten, dass Kreditentscheidungen zu Lasten des Betroffenen, also regelmäßig die Ablehnung eines Kredits, nicht ausschließlich auf eine automatisierte Verar-

beitung des Score-Werts gestützt werden dürfen. Dies folgt zum einen aus den Maßgaben, die von der SCHUFA den Vertragspartnern vertraglich vorgegeben werden, zum anderen daraus, dass negative Entscheidungen, die ausschließlich auf automatisierter Verarbeitung beruhen, nach Art. 15 der EG-Datenschutzrichtlinie grundsätzlich unzulässig sind. In § 6 a des novellierten BDSG wird Art. 15 der Richtlinie umgesetzt.

Ermittlung des Score-Wertes

Ein Score-Wert wird nur für Personen errechnet und übermittelt, über die keine Einträge über nicht vertragsgemäßes Verhalten gespeichert sind. Für Personen mit negativen Einträgen erübrigt sich eine *Score-Wertermittlung*, da sich bei ihnen in der Vergangenheit ein Kreditrisiko bereits realisiert hat. Der übermittelte Score-Wert wird von der SCHUFA nicht gespeichert.

Die Score-Werte werden in einem Score-Verfahren ermittelt, in dem mit statistisch-mathematischen Methoden Prognosen über das zukünftige Verhalten von Personengruppen ermittelt und in einer Punktzahl (Score) ausgedrückt werden. Solche Methoden werden z. B. auch bei der Berechnung von Kfz-Haftpflichtprämien verwendet.

Von Seiten der Aufsichtsbehörden im Düsseldorfer Kreis werden die wissenschaftlichen Grundlagen des Score-Verfahrens nicht in Zweifel gezogen, nachdem das Score-Verfahren in seinen Grundzügen vorgestellt wurde. Dabei wurden jedoch Details des Verfahrens und insbesondere die Gewichtung, mit der die einzelnen Faktoren in die Score-Wertermittlung einfließen, den Aufsichtsbehörden nicht bekannt gegeben, da es sich dabei um sensible Geschäftsgeheimnisse der SCHUFA handelt.

Für die Score-Wertermittlung werden durch anonymisierte Auswertung aller im SCHUFA-Datenbestand gespeicherten Daten Gruppenprofile erstellt, aus denen sich ableiten lässt, bei welcher Personengruppe mit zunächst positivem Datenbestand sich in der Vergangenheit welches Kreditausfallrisiko realisiert hat. Diese personengruppenbezogenen Vergangenheitswerte werden als Prognose auf die Zukunft übertragen, wobei davon ausgegangen wird, dass sich dieselbe Personengruppe auch in Zukunft gleich verhalten wird. Es handelt sich mithin um eine Prognose, also eine Aussage über die Wahrscheinlichkeit des Eintretens eines Kreditausfalls bei einer bestimmten Personengruppe. Deshalb gilt die so gewonnene Wahrscheinlichkeitsaussage nicht für eine konkrete Person, sondern für Gruppen von Personen mit gleichem Datenprofil.

Der Score-Wert beschreibt als *Wahrscheinlichkeitswert* immer nur ein allgemeines Risiko für Kredite mit vergleichbaren Merkmalen und kann als Punktzahl (Score) zwischen 1 und 1000 betragen. Dabei gilt: Je niedriger die Punktzahl ist, desto größer ist das Kreditausfallrisiko. Aus Gründen der Übersichtlichkeit des Score-Verfahrens wurden neun Risikoklassen mit nichtlinearer Punkteverteilung gebildet, die jeweils eine bestimmte Risikoquote aufweisen. So wird z. B. bei der risikoreichsten Gruppe in Risikoklasse A mit Score-Werten von 1 bis 40 eine Risikoquote von 27,16 v. H. angenommen. Dies bedeutet, dass auch bei der risikoreichsten Gruppe mit den schlechtesten Score-Werten bei ca. 73 von 100 Personen nicht mit Störungen bei der Vertragsabwicklung zu rechnen ist.

Anzahl der Selbstauskünfte

Als scorerelevante Daten fließen in die Score-Wertermittlung derzeit Daten aus dem SCHUFA-Datenbestand, die auch in einer Selbstauskunft mitgeteilt werden, sowie die Anzahl der Selbstauskünfte ein. Dabei geht die SCHUFA davon aus, dass gerade auch die *Anzahl der Selbstauskünfte*, die häufig als „wirtschaftliches Führungszeugnis“ verwendet werden, scorerelevant ist, da in diesen Fällen auf die Bonität beeinflussende Lebensumstände geschlossen werden könne. Eine Differenzierung danach, ob eine konkrete Selbstauskunft zu Kontrollzwecken (dem eigentlichen Zweck des Auskunftsanspruchs) oder zur Verwendung als „wirtschaftliches Führungszeugnis“ eingeholt wird, ist mangels entsprechender Erkenntnisse nicht möglich. Die Aufsichtsbehörden im Düsseldorfer Kreis halten mit dem Innenministerium diese Verfahrensweise deshalb mehrheitlich für bedenklich, teilweise auch für unzulässig, da dem Betroffenen aus der Wahrnehmung seines datenschutzrechtlichen Auskunftsanspruchs nach § 34 BDSG keine Nachteile entstehen dürfen. Sie haben der BUNDES-SCHUFA, die die regionalen SCHUFA-

Gesellschaften unterstützt und koordiniert, ihre Rechtsauffassung unter maßgeblicher Mitwirkung des Innenministeriums Baden-Württemberg nachdrücklich dargelegt. Die SCHUFA wird die Anzahl der Selbstauskünfte der Betroffenen nach einer aus technischen Gründen erforderlichen Übergangszeit nicht mehr in die Score-Wertermittlung einfließen lassen. Falls die SCHUFA weitere Daten in die Score-Wertermittlung einfließen lassen will, wird hierzu eine vorherige Einbeziehung der Aufsichtsbehörden durch die SCHUFA erfolgen. Mit diesem Ergebnis konnte erreicht werden, dass das Score-Verfahren transparenter wird.

Zulässigkeit der Ermittlung und Übermittlung des Score-Wertes

Erfolgt eine Anfrage eines Vertragspartners der SCHUFA zur Bonität einer bestimmten Person, wird diese Person einer bestimmten Personengruppe mit gleichartigem Profil zugeordnet. Damit wird dann der konkreten Person, zu der eine Anfrage vorliegt, der Score-Wert der Personengruppe, der diese konkrete Person angehört, zugeordnet. Wenn damit auch sichergestellt ist, dass der auf diese Weise ermittelte Score-Wert nicht für eine konkrete Person, sondern immer nur allgemein für eine Personengruppe mit gleichartigem Datenprofil gilt und daher keine Aussage über die konkrete Bonität einer konkreten Person im Einzelfall getroffen wird, so wird über die Zuordnung des personengruppenbezogen ermittelten Score-Wertes zu einer konkreten Person daraus gleichwohl ein *personenbezogenes Datum.*

Die Zulässigkeit der Nutzung der bei der SCHUFA vorhandenen Daten zur angefragten Person und des übrigen Datenbestandes zur Ermittlung eines Score-Wertes folgt aus § 28 Abs. 1 Satz 1 Nr. 2 BDSG, da dies zur Wahrung berechtigter Interessen der SCHUFA erforderlich ist und auf Grund der anonymisiert vorgenommenen Auswertung auch keine überwiegenden schutzwürdigen Interessen der Betroffenen entgegenstehen. Die Übermittlung des Score-Wertes zu einer Person nach einer Anfrage eines Vertragspartners ist, ebenso wie die Übermittlung der sonst üblichen SCHUFA-Auskünfte, bei Vorliegen der Voraussetzungen nach § 29 Abs. 2 Satz 1 Nr. 1 a und 2 BDSG *zulässig*. Diese Ansicht wird auch von den Aufsichtsbehörden im Düsseldorfer Kreis, die mehrheitlich das Score-Verfahren datenschutzrechtlich für zulässig erachten, vertreten.

Transparenz der Score-Verfahren

Immer wieder wird von *Betroffenen* gegenüber der Aufsichtsbehörde bemängelt, dass die SCHUFA zwar über die in ihrem Datenbestand gespeicherten Daten in einer Selbstauskunft Auskunft erteilt, dabei jedoch *keinen Score-Wert mitteilt*. Insbesondere deshalb, aber auch weil das Verfahren zur Ermittlung des Score-Wertes für die außen stehenden Betroffenen oft nur schwer durchschaubar ist und auch nicht im Detail von der SCHUFA offen gelegt wird, wird das Score-Verfahren vielfach heftig kritisiert und als eine Art „Geheimverfahren“ betrachtet.

Zur Kritik hat auch wesentlich beigetragen, dass die SCHUFA gegenüber dem Betroffenen keine Auskunft über den übermittelten Score-Wert erteilt. Dies beruht darauf, dass der zu einer Anfrage übermittelte Score-Wert bei der SCHUFA nicht gespeichert wird. Da sich der Score-Wert laufend ändern kann, wird er nicht gespeichert, sondern für jede Anfrage immer wieder neu ermittelt. Konsequenterweise kann die SCHUFA dann mangels Speicherung des Score-Wertes auch keine Auskunft darüber geben, welcher Score-Wert zu einer konkreten Anfrage eines Vertragspartners übermittelt wurde.

Auch wenn für die SCHUFA keine Pflicht zur Speicherung des Score-Werts besteht, wird es von den Aufsichtsbehörden im Düsseldorfer Kreis einschließlich des Innenministeriums Baden-Württemberg aus grundsätzlichen Überlegungen als unbefriedigend angesehen, dass die SCHUFA keine Auskunft über den übermittelten Score-Wert erteilt. Immerhin konnte in einer gemeinsamen Sitzung der Aufsichtsbehörden unter dem Vorsitz des Innenministeriums Baden-Württemberg mit Vertretern der SCHUFA und des Zentralen Kreditausschusses (ZKA) erreicht werden, dass – in dem für die Praxis besonders wichtigen Fall – die Kreditwirtschaft dem Betroffenen Auskunft über den ihr übermittelten Score-Wert erteilt, sofern der Score-Wert bei den Banken gespeichert wird oder sonst vorliegt. Auf Grund der völlig unterschiedlichen Verfahrensweisen bei der Vergabe von Krediten liegt jedoch häufig auch dort der Score-Wert nicht vor, so z. B., wenn der online übermittelte SCHUFA-Score-Wert direkt in andere computergestützte Bewertungsverfahren der Banken einfließt und deshalb nicht isoliert bei den Banken be-

kannt wird. Das novellierte BDSG ändert nichts an dieser unbefriedigenden Rechtslage.

Als eine *Verbesserung der Transparenz* bewertet das Innenministerium, dass im Zuge einer allgemeinen Überarbeitung der SCHUFA-Klausel, die z. B. bei Neueröffnung eines Girokontos oder bei Kreditanträgen zu unterschreiben ist, ausdrücklich auf das Score-Verfahren hingewiesen wird. Dazu wurde folgender Satz in die SCHUFA-Klausel aufgenommen: „Bei der Erteilung von Auskünften kann die SCHUFA ihren Vertragspartnern ergänzend einen aus ihrem Datenbestand errechneten Wahrscheinlichkeitswert zur Beurteilung des Kreditrisikos mitteilen (Score-Verfahren)."

Der ZKA gibt ein inhaltlich mit den Aufsichtsbehörden im Düsseldorfer Kreis abgestimmtes „SCHUFA-Merkblatt" heraus, in dem auch das SCHUFA-Score-Verfahren erläutert wird. Ebenso wurde von der SCHUFA ein Merkblatt „Informationen für Verbraucher zum Score System ASS der SCHUFA" erarbeitet und weitgehend mit den Aufsichtsbehörden im Düsseldorfer Kreis abgestimmt.

3.5 Kosten für die Selbstauskunft

Immer wieder wird in Beschwerden auch der Umstand kritisiert, dass von Auskunfteien bzw. Kreditschutzorganisationen *für die Erteilung von Selbstauskünften ein Entgelt von dem Betroffenen* verlangt wird. Bei den Betroffenen stößt es häufig auf Unverständnis, dass sie für eine Auskunft über die eigenen Daten, die bei einer Auskunftei gespeichert sind, vor deren Erteilung bezahlen sollen. Erst recht besteht dieses Unverständnis, wenn die Betroffenen diese Selbstauskunft verlangen im Zusammenhang mit dem Bestreiten der Richtigkeit von gespeicherten Daten oder im Zusammenhang mit sonstigen Unregelmäßigkeiten der Datenspeicherung oder -verarbeitung durch die Auskunftei. Regelmäßig wird von den Betroffenen vorgetragen, dass sie nicht bereit seien, durch ein solches Entgelt auch noch die Tätigkeit einer Auskunftei mitzufinanzieren.

Nach § 34 Abs. 1 Satz 1 BDSG kann der Betroffene grundsätzlich u. a. Auskunft verlangen über die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft und Empfänger beziehen. Ebenso kann Auskunft verlangt werden über Personen und Stellen, an die seine Daten regelmäßig übermittelt werden, wenn seine Daten automatisiert verarbeitet werden.

Werden jedoch die personenbezogenen Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, was gerade bei Auskunfteien der Fall ist, kann der Betroffene nach § 34 Abs. 1 Satz 3 BDSG über Herkunft und Empfänger Auskunft nur verlangen, wenn er begründete Zweifel an der Richtigkeit der Daten geltend macht.

Ausnahme der Unentgeltlichkeit

Die Auskunft hat nach § 34 Abs. 5 Satz 1 BDSG unentgeltlich zu erfolgen. Werden jedoch – wie *bei Auskunfteien und Kreditschutzorganisationen* – die personenbezogenen Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, greift die Ausnahmeregelung von § 34 Abs. 5 Satz 2 BDSG. Danach kann in diesem Fall ein Entgelt verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. Dass insbesondere Auskünfte von Auskunfteien und Kreditschutzorganisationen, bei denen es um die Beurteilung der Kreditwürdigkeit des Betroffenen geht, immer zu wirtschaftlichen Zwecken eingesetzt werden können, liegt auf der Hand. Dabei genügt die bloße Möglichkeit einer Verwendung der Selbstauskunft zu wirtschaftlichen Zwecken. Es ist nicht erforderlich, dass die Selbstauskunft im konkreten Fall tatsächlich zu wirtschaftlichen Zwecken eingesetzt werden soll.

Wird für die Auskunft ein Entgelt verlangt, informiert die Aufsichtsbehörde die Betroffenen regelmäßig darüber, dass nach § 34 Abs. 6 BDSG auch die Möglichkeit besteht, sich im Rahmen des Auskunftsanspruchs kostenlos persönlich Kenntnis über die ihn betreffenden Daten und Angaben zu verschaffen. Damit hat also der Betroffene die Gelegenheit, sich vor Ort bei der Auskunftei direkt zu informieren, ohne dass die Auskunftei dafür ein Entgelt erheben darf.

Ausnahmsweise darf ein Entgelt in den Fällen nicht verlangt werden, in denen besondere Umstände die Annahme rechtfertigen, dass Dateien unrichtig oder un-

zulässig gespeichert werden, oder in denen die Auskunft ergibt, dass die Daten zu berichtigen oder unter bestimmten Voraussetzungen zu löschen sind (§ 34 Abs. 5 Satz 4 BDSG).

Höhe des Entgelts

In den Beschwerden, die bei der Aufsichtsbehörde eingehen, wird vielfach auch *die Höhe des verlangten Entgelts* als zu hoch kritisiert. Bei diesem Aspekt ist die Regelung in § 34 Abs. 5 Satz 3 BDSG zu beachten, wonach das Entgelt nicht über die durch die Auskunftserteilung entstandenen direkt zurechenbaren Kosten hinausgehen darf.

Hintergrund der Beschwerden ist hier, dass derzeit bei der SCHUFA ein Entgelt in Höhe von 15,– DM für eine Selbstauskunft erhoben wird. Dabei wird häufig auch auf ein Urteil des Landgerichts Berlin vom 14. Januar 1999 verwiesen, in dem die Höhe des Entgelts von 15,– DM als zu hoch angesehen wurde. Danach könne lediglich ein Betrag von 3,– DM erhoben werden.

Dieses Thema wurde nach Bekanntwerden des Urteils des Landgerichts auch von den Aufsichtsbehörden der Länder in der Arbeitsgruppe Auskunfteien des Düsseldorfer Kreises eingehend erörtert.

Von Seiten der SCHUFA wurde hierzu mitgeteilt, dass es zu diesem Urteil nur gekommen sei, weil eine besondere prozessuale Situation in diesem Verfahren vorgelegen habe. Davor seien diverse Verfahren zu dieser Frage sämtlich von der SCHUFA gewonnen worden. Die SCHUFA habe auch ein Gutachten von einem Wirtschaftsprüfer anfertigen lassen, in dem die bei der SCHUFA mit der Erteilung einer Selbstauskunft anfallenden Kosten ermittelt wurden. Dieses Gutachten habe bestätigt, dass die Höhe des von der SCHUFA erhobenen Entgelts für eine Selbstauskunft mehr als gerechtfertigt sei. Auch aus Sicht der Aufsichtsbehörde ist die Höhe des Entgelts nicht zu beanstanden.

3.6 Prüfungen bei Auskunfteien

Im Zuge von anlassunabhängigen Prüfungen nach § 38 Abs. 2 BDSG wurde bei zwei Auskunfteien die Verfahrensweise bei der *Speicherung und Übermittlung von Ehegattendaten* überprüft.

Getrennte Betrachtung von Ehegattendaten

Hintergrund für die Prüfung im Zusammenhang mit der Speicherung und Übermittlung von Ehegattendaten war eine Diskussion in der AG Handelsauskunfteien im Düsseldorfer Kreis zu diesem Thema, bei der eine gemeinsame Position der Aufsichtsbehörden mit dem Verband der Handelsauskunfteien abgestimmt wurde.

Dabei verständigte man sich darauf, dass grundsätzlich bei der Beantwortung einer Anfrage zu einer einzelnen natürlichen Person *keine Auskünfte über deren Ehepartner* erteilt werden. Dieser Grundsatz gilt vor dem Hintergrund, dass auch in einer Ehe die Ehepartner datenschutzrechtlich als Betroffene jeweils für sich zu betrachten sind. Etwas anderes kann nur gelten, wenn eine so genannte *Strohmanneigenschaft* nachweisbar ist. Dabei bedarf es aber jeweils einer Prüfung im Einzelfall, ob konkrete Anhaltspunkte vorliegen, die es in solchen Fällen rechtfertigen, auch Daten zum Ehepartner an einen Anfragenden zu übermitteln.

Ergebnis der Überprüfung

Bei einer der überprüften Auskunfteien werden diese Grundsätze schon datenverarbeitungstechnisch dadurch gewährleistet, dass in der Datenbank für jede Person ein eigener Datensatz vorgesehen ist. Somit wird auch bei Ehepaaren für jeden Ehepartner ein gesonderter Datensatz angelegt. Aus den Datensätzen zu den einzelnen Ehepartnern ergibt sich lediglich, dass sie verheiratet sind. Es stellte sich heraus, dass die Verknüpfung beider Datensätze nur über eine spezielle Funktion möglich ist. Nur bei Aktivierung dieser Funktion werden in eine Auskunft beide Ehepartner einbezogen. Der Verknüpfungsmodus ist jedoch grundsätzlich inaktiv, sodass bei Anfragen nur eine Auskunft über die jeweils angefragte Person erfolgt. Die Erteilung einer Auskunft über den Ehepartner erfolgt nur, wenn eine Strohmanneigenschaft nachweisbar ist. Hier werden die o. g. Grundsätze eingehalten.

Bei einer anderen Auskunftei zeigte sich, dass dort die vorherige Praxis, bei einer Anfrage über eine verheiratete Person auch zu deren Ehepartner gespeicherte Daten (Identifizierungsdaten, Daten über Bonität) zu übermitteln, umgestellt worden war. Dazu war die erforderliche Software zuvor erarbeitet worden. Mithilfe dieser Software wurden die Datensätze, die neben den Daten zur angefragten Person auch Daten zu den Ehepartnern enthalten haben, aufgefunden und dahingehend verändert, dass in dem Datensatz die Informationen zum Ehegatten gelöscht und in einen eigenen Datensatz übernommen wurden.

Wie anhand von Stichproben festgestellt werden konnte, sind nunmehr in den Datensätzen zu angefragten Personen mit Ausnahme des Hinweises, ob verheiratet oder nicht verheiratet, keine Informationen zum Ehepartner mehr enthalten. Sofern für die Auskunftei erkennbar ist, dass die angefragte Person lediglich im Sinne eines Strohmannverhältnisses vorgeschoben wurde, nimmt sie in einem zum Auskunftsdatensatz gehörenden Datenfeld „Anmerkungen“ einen entsprechenden Hinweis auf.

Erfolgt eine Anfrage zu einem Ehepaar, werden von der Auskunftei in den Fällen, in denen nach den o. g. Grundsätzen nur zu einem Ehepartner Auskunft erteilt wird, die Hinweise gegeben, dass Auskünfte über Ehepartner aus rechtlichen Gründen nicht erteilt werden können bzw. dass in die Auskunft Daten über den Ehepartner grundsätzlich nicht einfließen.

Die Prüfungen haben somit ergeben, dass die Auskunfteien inzwischen die mit dem Verband der Handelsauskunfteien abgestimmten Grundsätze umgesetzt haben und einhalten.

Bonitätsprüfungen durch Ärzte und Zahnärzte

Die beiden Auskunfteien wurden auch darauf überprüft, ob dort Bonitätsprüfungen von Patienten durch Ärzte und Zahnärzte vorgenommen werden. Dabei war festzustellen, dass Ärzte und Zahnärzte bislang nicht zu den Kunden der geprüften Auskunfteien gehören. Damit finden Bonitätsprüfungen bei Patienten durch Ärzte und Zahnärzte durch Einschaltung dieser Auskunfteien bislang nicht statt.

3.7 Auskunftssystem auf Internetbasis

Im Zuständigkeitsbereich des Innenministeriums als Aufsichtsbehörde gibt es eine Wirtschaftsorganisation, die ihren Mitgliedern Auskunftsdienstleistungen anbietet. Sie stellt ihren Mitgliedern Bonitätsdaten von Kunden zur Verfügung und unterhält dazu eine eigene Datenbank mit Bonitätsdaten von Branchenkunden. Bisher wurden die Auskünfte nur auf telefonischem oder schriftlichem Wege erteilt. Diese Organisation hatte angekündigt, künftig *die Bonitätsanfragen* ihrer Mitglieder *über das Internet* abzuwickeln. Die Aufsichtsbehörde hat daraufhin das vorgesehene Verfahren überprüft, das sich im Wesentlichen als datenschutzgerecht herausgestellt hat. Im technischen Bereich hat die Aufsichtsbehörde jedoch einige Verfahrensweisen für problematisch gehalten und teilweise auch beanstandet.

Ergebnis der Überprüfung

Als problematisch angesehen wurde, dass die Anforderungen des § 18 der Schuldnerverzeichnisverordnung (SchuVVO) nicht in vollem Umfang erfüllt wurden.

Beispielsweise war für das Passwort eine Verfallsfrist von 180 Tagen an Stelle von 120 Tagen, wie im § 18 Abs. 2 SchuVVO gefordert, vorgesehen. Das Bundesamt für Sicherheit in der Informationstechnik sieht in seinem Grundschutzhandbuch hierfür sogar nur eine Frist von 90 Tagen vor. In Anbetracht der bisher nur geringen Nutzung des Verfahrens und der vollen Kontrolle der Protokolldateien durch den Systemverwalter hat die Aufsichtsbehörde die bestehende Verfallsfrist für vertretbar gehalten, solange die Abfrageintervalle der einzelnen Nutzer 90 Tage nicht unterschreiten.

Darüber hinaus sind nach § 18 Abs. 6 SchuVVO die Protokolldateien nach drei Jahren zu löschen, eine Löschung war aber bisher nicht vorgesehen. Die Aufsichtsbehörde hat deshalb die Einrichtung einer entsprechenden Löschautomatik für die Protokolldateien gefordert.

Beanstandungen

Zu beanstanden war, dass die Benutzerpassworte nach der Neu- bzw. Erstvergabe nicht beim ersten Anmelden von den Anwendern geändert werden mussten und dass sie im Klartext im System vorgehalten sowie in den Protokolldateien angezeigt wurden. Dies verstößt gegen Ziff. 1 (Zugangskontrolle), 4 (Benutzerkontrolle) und 5 (Zugriffskontrolle) der Anlage zu § 9 BDSG. Da ein Passwort nur dem Eigentümer oder einer von ihm berechtigten Person bekannt sein darf, um einen möglichen Missbrauch zu verhindern, darf es auf dem Server nur in einer nicht entschlüsselbaren Form gespeichert bzw. protokolliert werden. Die Aufsichtsbehörde forderte, das System so einzurichten, dass der Benutzer beim ersten Anmelden zu einer Passwortänderung gezwungen wird.

Die geforderten Änderungen und die Behebung der Mängel wurden der Aufsichtsbehörde zugesichert.

4. Kreditwirtschaft

4.1 Bankenfusion und der Schutz von Kundendaten

In den letzten Jahren kam es zu einer größeren Zahl von *Fusionen zwischen Banken*. Hintergrund dafür waren insbesondere Zusammenschlüsse von kleineren Volksbanken zu größeren Unternehmen.

Dabei kam es auch zu Beschwerden von Bankkunden, insbesondere Darlehensnehmern, die nicht damit einverstanden waren, dass ihre vielfältigen und sensiblen Daten über Vermögens- und sonstige persönliche Verhältnisse, die im Zusammenhang mit dem Kredit bei einer der an der Fusion beteiligten Banken gespeichert waren, nach einer Fusion der neuen Bank bekannt werden. Sie halten dafür ihre Einwilligung für erforderlich.

Bei der datenschutzrechtlichen Beurteilung war zunächst zu prüfen, ob hier eine Übermittlung personenbezogener Daten i. S. v. § 3 Abs. 5 Satz 2 Nr. 3 BDSG von der alten auf die neue Bank vorliegt. Danach ist Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten (Empfänger). Nach § 3 Abs. 9 Satz 1 BDSG ist Dritter jede Person oder Stelle außerhalb der speichernden Stelle.

Wirkungen des Umwandlungsgesetzes

Zur Beurteilung der Frage, ob ein solcher Dritter bei einer Bankenfusion beteiligt ist, ist das Umwandlungsgesetz (UmwG) heranzuziehen. Nach § 20 des auch auf Bankenfusionen anzuwendenden Umwandlungsgesetzes kommt es bei Verschmelzungen von Unternehmen i. S. v. § 2 UmwG bzw. mit der Registereintragung zu einer Gesamtrechtsnachfolge. Damit hat die Eintragung der Verschmelzung in das Register vor allem zur Folge, dass das Vermögen der übertragenden Rechtsträger einschließlich der Verbindlichkeiten auf den übernehmenden Rechtsträger übergeht und dass die übertragenden Rechtsträger erlöschen.

Diese *Gesamtrechtsnachfolge* bewirkt in jedem Fall – sei es eine Verschmelzung durch Neugründung oder eine Verschmelzung durch Aufnahme – , dass sich die rechtliche Identität des fusionierenden Unternehmens, bei dem die Bankkundendaten gespeichert sind, ändert. Aus dieser bloßen Änderung der rechtlichen Identität leitet sich allerdings keine Weitergabe dieser Daten an einen Dritten i. S. v. § 3 Abs. 9 BDSG ab. Vielmehr gehen die Datenbestände der fusionierenden Unternehmen wie alle anderen Rechte und Pflichten auch im Wege der Gesamtrechtsnachfolge auf das neue Unternehmen über, ohne dass eine Übermittlung von Daten im Sinne des Datenschutzrechts erfolgt. Diese Auffassung wird von allen Aufsichtsbehörden im Düsseldorfer Kreis vertreten.

Hierbei ist auch zu beachten, dass die Frage, unter welchen Voraussetzungen Änderungen der rechtlichen Identität von Unternehmen nach dem Umwandlungsgesetz zulässig sind, losgelöst vom BDSG zu beantworten ist. Das BDSG hat hier nur die Aufgabe sicherzustellen, dass die Verarbeitung und Nutzung der bei den fusionierenden Banken gespeicherten personenbezogenen Kundendaten vor und nach der Fusion nach dessen Bestimmungen erfolgen.

Nach Auffassung der Aufsichtsbehörde bleibt mithin angesichts der besonderen Vorschriften des Umwandlungsgesetzes in Bezug auf Fusionen kein Raum für die Anwendung datenschutzrechtlicher Vorschriften: Es wäre widersprüchlich, wenn der Bundesgesetzgeber einerseits im Umwandlungsgesetz eine Fusion durch Verschmelzungsvertrag für zulässig erklären, andererseits aber eine Fusion nach dem Bundesdatenschutzgesetz von Voraussetzungen abhängig machen würde, wie beispielsweise die Einwilligung jedes einzelnen Bankkunden, die eine Fusion praktisch verhindern.

Es ist also einerseits nach dem Umwandlungsgesetz zu beurteilen, ob Änderungen der rechtlichen Identität von Unternehmen im Zuge von Fusionen und eine damit verbundene Gesamtrechtsnachfolge zulässig sind. Unabhängig davon bezieht sich das BDSG andererseits nur auf die von der Zulässigkeit der Fusion getrennt zu sehende Beurteilung der Rechtmäßigkeit der Datenverarbeitung durch die fusionierenden Unternehmen vor und nach der Fusion.

Schutz der Kundendaten

Wie der *Schutz der Kundendaten* im Falle von Fusionen von Banken generell zu gewährleisten ist, wurde von der Aufsichtsbehörde auch in den HIM Nr. 38 vom 18. Januar 2000 (Staatsanzeiger für Baden-Württemberg Nr. 2 vom 24. Januar 2000, Seite 12) erörtert. Danach ist zu differenzieren zwischen der Zeit vor der Fusionsentscheidung und der Zeit danach. Im Einzelnen gilt Folgendes:

Offenlegung von Kundendaten vor der Fusionsentscheidung

Für die Fusion von Kreditinstituten sind neben der Kundenstruktur sowie der Struktur und Höhe der Einlagen insbesondere die Höhe der vergebenen Kredite sowie die Qualität der Kreditsicherheiten und die Bonität der Kreditschuldner bewertungs- und entscheidungserhebliche Kriterien. Das an der Übernahme eines anderen Kreditinstituts interessierte Kreditinstitut oder die an einer Verschmelzung zu einem neuen Unternehmen interessierten Kreditinstitute haben deshalb grundsätzlich ein berechtigtes Interesse daran, vor der Fusionsentscheidung Kundendaten umfassend prüfen zu können. Andererseits haben die betroffenen Bankkunden sowohl aus der Sicht des Datenschutzrechts als auch aus der Sicht ihres bankvertraglich geschützten Bankgeheimnisses ein schutzwürdiges Interesse daran, dass ihre Daten nicht ohne Einwilligung auf ihre Person bezogen offen gelegt und damit übermittelt werden, bevor die Fusionsentscheidung unwiderruflich von den Beschlussgremien der Anteilseigner der beteiligten Kreditinstitute bestätigt worden ist. Erst dann haben die Kunden Gewähr dafür, dass ihre Daten nur dem künftigen Vertragspartner bekannt werden. Vor diesem Zeitpunkt steht der Übermittlung § 28 Abs. 1 Satz 1 Nr. 2 BDSG entgegen, da regelmäßig davon ausgegangen werden muss, dass die schutzwürdigen Interessen der betroffenen Kunden die berechtigten Interessen der beteiligten Kreditinstitute überwiegen.

In dieser *Vorphase der Fusion* ist es deshalb den beteiligten Kreditinstituten datenschutzrechtlich *verwehrt*, die sich aus Kundenbeziehungen und Kreditengagements des jeweils anderen Instituts ergebenden Daten personenbezogen mit eigenen Mitarbeitern zu prüfen. Dies gilt auch dann, wenn die personenbezogenen Kundendaten in einem Gemeinschaftsrechenzentrum verarbeitet werden; weder darf das Rechenzentrum dem übernahmeinteressierten Kreditinstitut von sich aus noch mit Wissen des an der Übertragung des Geschäfts interessierten Kreditinstituts den lesenden Zugriff auf den Gesamtbestand der Daten einräumen. Auch ist die vorübergehende Integration von Mitarbeitern des übernahmeinteressierten Kreditinstituts in den Mitarbeiterstamm des die Übernahme anstrebenden Kreditinstituts zum Zweck der Gewinnung personenbezogener Informationen über die Bankkunden regelmäßig unzulässig, weil die Mitarbeiter vor der Fusionsentscheidung wieder in das entsendende Kreditinstitut aufgenommen werden und dort den Weisungen des Vorstands unterliegen.

Datenbasis für Fusionsverhandlungen

Als *Datenbasis für die Fusionsverhandlungen* kommen regelmäßig nur zusammengefasste *strukturelle Daten* sowie *anonymisierte Einzeldaten* infrage. Das berechtigte Interesse des übernahmeinteressierten Kreditinstituts an der Korrektheit der aggregierten und anonymisierten kundenrelevanten Daten und der betriebswirtschaftlich zutreffenden Bewertung dieser Daten kann durch die Einschaltung unabhängiger Wirtschaftsprüfer oder verbandseigener Prüfer sichergestellt werden. Auf vorliegende Prüfberichte des an der Übertragung des Geschäfts interessierten Kreditinstituts kann nicht zurückgegriffen werden, weil diese regelmäßig personenbezogene Kundendaten enthalten, die sich nur schwer anonymisieren lassen; so sind insbesondere bei problematischen Kreditengagements auch die Personalien der Kreditnehmer ersichtlich. Wird eine Sonderprüfung des zu übernehmenden Kreditinstituts veranlasst, ist darauf zu achten, dass Kundendaten in dem für die Fusionsverhandlungen verwendeten Prüfbericht ausreichend anonymisiert sind. Erforderlichenfalls ist ein Treuhänder einzuschalten, der die Korrektheit der anonymisierten Unterlagen gewährleistet, die Grundlage der Fusionsverhandlungen sind.

Wenn allerdings wegen besonderer Umstände eine zuverlässige Anonymisierung von Kundendaten nicht möglich ist, wie beispielsweise bei einem einzelnen großen Kreditengagement, über das bereits die Presse berichtet hat, überwiegt das berechtigte Interesse der übernahmeinteressierten Bank an der Kenntnis der per-

sonenbezogenen Daten das schutzwürdige Interesse des betroffenen Kunden an der Geheimhaltung seiner Daten. Es sollte aber so weit wie möglich vermieden werden, dass Kundendaten für die wirtschaftliche Bewertung des an der Übertragung des Geschäfts interessierten Kreditinstituts offen gelegt werden, wenn die Fusionsentscheidung noch weitgehend offen ist. Es ist den betroffenen Kunden nicht zumutbar, dass ihre Daten über das ihnen vertraglich verbundene Kreditinstitut hinaus bekannt sind, wenn nach der Prüfung der Kreditengagements die Fusionsverhandlungen abgebrochen werden.

Offenlegung von Kundendaten nach der Fusionsentscheidung

Zwischen der Fusionsentscheidung durch die Beschlussorgane der Anteilseigner der betroffenen Kreditinstitute und der Aufnahme des Geschäftsbetriebs und damit dem Übergang der Vertragsbeziehungen der Kunden auf das Fusionsunternehmen liegt regelmäßig eine Zeitspanne, die der *Vorbereitung und Konsolidierung der Geschäftsprozesse* der beteiligten Kreditinstitute dient. So kann es beispielsweise erforderlich sein, die Kontenführung zu vereinheitlichen oder den Kunden neue Kontonummern zuzuordnen. Auch Serviceleistungen im Interesse der Kunden, wie beispielsweise die Information regelmäßiger Teilnehmer am Lastschrifteinzugsverfahren über neue Kontobeziehungen der Bankkunden, müssen in dieser Phase vorbereitet werden. Für solche Zwecke ist die *Offenlegung* der dafür notwendigen Kundendaten durch die übertragende Bank als Übermittlung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG ohne Einwilligung der betroffenen Kunden *zulässig*. Das Kreditinstitut als Vertragspartner des Kunden hat ein berechtigtes Interesse an der Vorbereitung des ordnungsgemäßen Geschäftsbetriebs des künftigen fusionierten Unternehmens. Dagegen stehende schutzwürdige Belange des Bankkunden sind nicht erkennbar; sein Interesse ist regelmäßig auf die problemlose Fortsetzung seiner Vertragsbeziehungen mit dem Fusionsunternehmen gerichtet.

Übertragung von Kundendaten nach der Fusion

Datenschutzrechtlich unproblematisch ist der Umgang mit den Kundendaten der beteiligten Unternehmen nach dem Wirksamwerden des Verschmelzungsvertrags. Das neu entstandene oder das ein anderes Kreditinstitut übernehmende Kreditinstitut tritt als Gesamtrechtsnachfolger für das Vorgängerinstitut in die Verträge zu den Bankkunden ein; es ist damit nicht Dritter im Sinne des BDSG, eine Datenübermittlung findet nicht statt. Die Zulässigkeit der Datenverarbeitung durch das übernehmende Kreditinstitut gründet sich auf vertragliche Beziehung und damit auf § 28 Abs. 1 Satz 1 Nr. 1 BDSG.

4.2 Ausweiskopie bei Kontoeröffnung oder Identifizierung nach dem Geldwäschegesetz

Nach wie vor kommt es zu Anfragen an die Aufsichtsbehörde, ob es den Banken erlaubt sei, bei einer Kontoeröffnung den Personalausweis einzusehen und dann auch noch zu kopieren. Mit der Vorlage und Einsichtnahme in den *Personalausweis* waren die Meisten einverstanden, nicht jedoch mit der Fertigung einer Kopie. Die Banken haben sich den Kunden gegenüber in der Regel – vielleicht der Einfachheit halber – auf die Identifizierungspflichten nach dem Geldwäschegesetz (GwG) berufen.

Eine Überprüfung der einzelnen Fälle war der Aufsichtsbehörde zum einen dadurch verwehrt, dass die Betroffenen die beteiligte Bank nicht benennen wollten, zum anderen stellt die Fertigung einer Ausweiskopie keine Datenverarbeitung in oder aus Dateien dar; die Kopie wird vielmehr in aller Regel zu den Kundenakten genommen. Datenschutzrechtliche Relevanz erhält die Angelegenheit dann, wenn Daten aus dem Ausweisdokument aufgezeichnet und zu den bereits vorhandenen Kundendaten dazugespeichert werden, denn dann handelt es sich um eine Datenerhebung, die nach § 28 Abs. 1 Satz 2 BDSG nach Treu und Glauben und auf rechtmäßige Weise erfolgen muss.

Die Aufsichtsbehörde konnte den Betroffenen lediglich die Rechtslage darstellen und darauf hinweisen, dass den Banken und Kreditinstituten strikte Identifizierungspflichten sowohl nach § 154 der Abgabenordnung (AO) als auch nach dem GwG obliegen.

Regelungen der Abgabenordnung und des Geldwäschegesetzes

Nach § 154 Abs. 2 AO sind die Banken und Kreditinstitute verpflichtet, sich Gewissheit über die Person und Anschrift des Verfügungsberechtigten zu verschaffen und die entsprechenden *Angaben* in geeigneter Form *festzuhalten*. Das Bundesaufsichtsamt für das Kreditwesen fordert seit 1998 von den Kreditinstituten, dass bei der Neueröffnung von Konten durch natürliche Personen die nach § 154 AO erforderlichen Legitimationsprüfungen der Kontoinhaber und der Verfügungsberechtigten ausschließlich in der in § 1 Abs. 5 GwG formulierten Art und Weise vorgenommen werden.

Nach § 1 Abs. 5 GwG bedeutet Identifizieren im Sinne des Gesetzes „das Feststellen des Namens auf Grund eines Personalausweises oder Reisepasses sowie des Geburtsdatums und der Anschrift soweit sie enthalten sind, und das Feststellen von Art, Nummer und ausstellender Behörde des amtlichen Ausweises." Die getroffenen Feststellungen zur Identifikation sind nach § 9 GwG aufzuzeichnen. Diese Aufzeichnung soll, soweit möglich, durch *Kopie* der zur Feststellung der Identität vorgelegten Dokumente erfolgen.

Diese Identifizierungspflicht nach dem GwG geht über die Anforderungen der AO hinaus. Nach § 2 Abs. 1 GwG hat ein Kreditinstitut aber bei Annahme oder Abgabe von Bargeld, Wertpapieren oder Edelmetallen im Wert von 30 000 DM oder mehr zuvor denjenigen zu identifizieren, der ihm gegenüber auftritt. Dabei ist unerheblich, ob die auftretende Person bereits ein Konto oder ein Wertpapierdepot bei dem Kreditinstitut unterhält oder nicht. Für den Eintritt der Identifizierungspflicht ist also Voraussetzung, dass Geldbewegungen in der erwähnten Höhe vorgenommen werden. Die bloße Eröffnung eines Girokontos löst nach dem GwG noch keine Identifizierungspflicht aus.

Ursprünglich hatte das Bundesaufsichtsamt für das Kreditwesen den Kreditinstituten anlässlich der Legitimationsprüfung nahe gelegt, Fotokopien der Ausweisdokumente zu erstellen. Die Empfehlung zur grundsätzlichen Fertigung einer Ausweiskopie wurde zwischenzeitlich auch auf Drängen der Aufsichtsbehörden im Düsseldorfer Kreis zurückgenommen. Es reicht nunmehr aus, wenn die Ausweisdaten von sogenannten „Dauerkunden" bei der erstmaligen Identifizierung datenverarbeitungstechnisch oder auch handschriftlich aufgezeichnet werden. Bei Einzelabwicklungen kann ausnahmsweise weiterhin eine Kopie des Legitimationspapiers erfolgen, insbesondere wenn nur durch eine Kopie eine Eindeutigkeit mit der handelnden Person hergestellt werden kann, wie z. B. bei ausländischen Ausweispapieren mit fremden Schriftzeichen.

Praxis der Banken

In der Praxis sind die Banken vielfach dazu übergegangen, die *strengere Identifizierungsprozedur* nach dem GwG mit dem Kopieren des Ausweisdokuments gleich zu Beginn der Geschäftsbeziehung – etwa bei der Eröffnung eines Girokontos – oder zu einem sonstigen geeigneten Zeitpunkt durchzuführen. Falls der Betroffene künftig irgendwann einmal Geldbewegungen der im GwG genannten Art tätigt, ist dann schon alles erledigt, was an Identifizierungsmaßnahmen gegenüber dem Kunden zu veranlassen ist. Wesentlich dabei ist allerdings, dass sich die Bank für eine solche „vorbeugende" Vorgehensweise nicht auf das GwG berufen kann. Sie braucht dazu vielmehr das ausdrückliche Einverständnis des Betroffenen. Dieses Einverständnis ist aber nur wirksam, wenn der Betroffene über den Zweck der Identifizierung informiert wird und ihm keine Rechtspflichten vorgetäuscht werden, wo es auf seine freiwillige Mitwirkung ankommt.

Fazit ist, dass der Kunde für die Legitimation zur Kontoeröffnung zwar ein Ausweisdokument vorlegen muss. Er muss es jedoch nicht dulden, dass dieses Dokument kopiert wird. Ist der Kunde mit dem Anfertigen einer Kopie nicht einverstanden, muss sich die Bank damit begnügen, die notwendigen Angaben auf andere Weise aufzuzeichnen, zumal zum Nachweis der Legitimationsprüfung unstreitig andere technische Möglichkeiten bestehen. Dass die Bank eine andere Aufzeichnungsform wählen muss, wenn der Kunde die Fertigung einer Kopie seines Ausweisdokuments ablehnt, darf sich nicht zum Nachteil des Kunden auswirken.

4.3 Offenlegung der wirtschaftlichen Verhältnisse gegenüber Kreditinstituten

Im Berichtszeitraum beschwerten sich mehrere Bürger bei der Aufsichtsbehörde darüber, dass Kreditinstitute von ihnen als *Nachweis über ihre wirtschaftlichen Verhältnisse* auch bei bereits länger bestehenden Kreditengagements *Einkommensteuerbescheide oder Einkommensteuererklärungen* verlangten. Die Betroffenen fühlten sich durch das Verlangen, die wirtschaftlichen Verhältnisse durch Vorlage der geforderten Nachweise zu belegen, in ihrem Persönlichkeitsrecht verletzt. Die Kreditinstitute bezogen sich mit ihrer Forderung auf § 18 des Kreditwesengesetzes (KWG).

Die Vorgehensweise der Kreditinstitute war datenschutzrechtlich in keinem Fall zu beanstanden. Nach § 27 Abs. 1 BDSG finden die für nichtöffentliche Stellen geltenden gesetzlichen Bestimmungen des BDSG Anwendung, soweit personenbezogene Daten in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeitet oder genutzt werden. Die Kreditinstitute haben die Kopien der geforderten Nachweise aber zu den Akten der Betroffenen genommen, und nach § 3 Abs. 2 Satz 2 BDSG gehören Akten und Aktensammlungen nicht zu Dateien im Sinne des BDSG, es sei denn, dass sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können. Dies ist jedoch bei einer einzelnen Kopie nicht der Fall mit der Folge, dass die gesetzlichen Regelungen des BDSG keine Anwendung finden.

Regelung des Kreditwesengeschäftes

Nach § 18 KWG haben sich Kreditinstitute die *wirtschaftlichen Verhältnisse* der Kreditnehmer *offen legen* zu lassen, denen Kredite von insgesamt mehr als 500 000,– DM gewährt werden oder gewährt worden sind. Nach dem Rundschreiben 9/98 des Bundesaufsichtsamtes für das Kreditwesen haben die Kreditinstitute die erforderlichen Unterlagen beim Kreditnehmer anzufordern, diese zu dokumentieren und auszuwerten. Bei nicht bilanzierenden Kreditnehmern gehören zu den vorzulegenden Unterlagen auch eine aktuelle Aufstellung der Vermögenswerte und Verbindlichkeiten sowie Unterlagen, die eine Beurteilung der Einkommenssituation ermöglichen. Dies gilt nicht nur für die Zeit vor der Kreditgewährung, sondern während der gesamten Dauer des Kreditengagements. In dieser Zeit ist die wirtschaftliche Entwicklung des Kreditnehmers kontinuierlich zu beobachten und zu analysieren. Falls die Offenlegung der wirtschaftlichen Verhältnisse seitens des Kreditnehmers nicht erfolgt, müssen die Kreditinstitute notfalls den Kredit kündigen. Die dafür erforderlichen vertragsrechtlichen Voraussetzungen haben sie mit dem Kreditvertrag zu schaffen.

Diese *gesetzlichen Pflichten* der Kreditinstitute zur Analyse der wirtschaftlichen Verhältnisse der Kreditnehmer bestehen seit einigen Jahren. Die Bankenaufsicht richtet in neuerer Zeit ihr Augenmerk verstärkt auch darauf, ob die Kreditinstitute ihre Verpflichtungen nach dem KWG erfüllen.

Sofern die Betroffenen zu dem Kreis der Kreditnehmer gehören, deren wirtschaftliche Verhältnisse die Bank laufend zu analysieren hat, hat die Kredit gebende Bank ein rechtliches Interesse an der Offenlegung der wirtschaftlichen Verhältnisse. Ein schutzwürdiges Interesse der Kreditnehmer, diese Informationen geheim zu halten, besteht nicht.

Die Betroffenen, die nicht zu diesem Kreis der Kreditnehmer gehörten, wurden von der Aufsichtsbehörde dahin gehend beraten, dass das konkrete Geschäftsgebaren mit den allgemein üblichen Gepflogenheiten eines ordnungsgemäßen Geschäftsverhaltens eines Kreditinstituts bzw. mit den Regelungen des KWG vereinbar sein muss. Für diese Frage ist jedoch nicht die Aufsichtsbehörde für den Datenschutz, sondern das Bundesaufsichtsamt für das Kreditwesen zuständig.

4.4 Kundenbefragungen durch Kreditinstitute

Auch Kreditinstitute haben ein Interesse daran, die Qualität ihrer Dienstleistungen zu überprüfen. Wenn sie für diese Zwecke ein Markt- und Meinungsforschungsinstitut mit einer *Kundenbefragung* beauftragen und dazu personenbezogene Daten zur Verfügung stellen, ist die Frage der datenschutzrechtlichen Zulässigkeit zu prüfen.

In einem Fall hat ein Kreditinstitut für eine Befragung Kundendaten an ein Meinungsforschungsinstitut gegeben, ohne die Kunden vorher über die Durchführung

einer solchen Befragungsaktion zu informieren und damit auch ohne deren Einwilligung in die Übermittlung ihrer Daten an das Meinungsforschungsinstitut. Das Kreditinstitut ging von einer Auftragsdatenverarbeitung nach § 11 BDSG aus und sah sich deswegen nicht veranlasst, die Kunden vorab zu informieren und deren Einwilligung einzuholen. Auf Grund der gegebenen Sachlage konnte die Aufsichtsbehörde dieser Auffassung nicht folgen und musste das Vorgehen beanstanden.

Auftragsdatenverarbeitung oder Funktionsübertragung?

Für die datenschutzrechtliche Bewertung solcher Befragungsaktionen kommt es zunächst darauf an, wie das Verhältnis zwischen dem Kreditinstitut und dem Fremdunternehmen, das die Kundenbefragung durchführen soll, ausgestaltet ist, insbesondere ob das eingeschaltete Fremdunternehmen im Wege der Auftragsdatenverarbeitung oder der Funktionsübertragung tätig wird.

Bei einer *Auftragsdatenverarbeitung* im Sinne von § 11 BDSG muss die „Datenverarbeitung“ Gegenstand der Auftragserteilung sein, das heißt, das Fremdunternehmen erbringt für das Kreditinstitut ausschließlich Hilfstätigkeiten in Form der technischen Aufbereitung des Datenmaterials zur Erfüllung der Geschäftszwecke des Kreditinstituts. Von einer Datenverarbeitung im Auftrag kann dann ausgegangen werden, wenn sich die Tätigkeit des Fremdunternehmens in der Befragung der Kunden auf der Grundlage der zur Verfügung gestellten und dafür erforderlichen personenbezogenen Daten der Kunden sowie der von dem Kreditinstitut vorgegebenen Fragen erschöpft und konkrete Vorgaben für eine möglichst frühzeitige Anonymisierung gemacht werden. Eine Datenübermittlung im Sinne des BDSG findet dann nicht statt.

Ergebnis der Überprüfung, Beanstandungen

Im vorliegenden Fall wurde die Befragungsaktion durch die Fremdfirma auf Grund eigener wissenschaftlicher Kompetenz sowohl hinsichtlich der Struktur und inhaltlicher Gestaltung des Fragebogens und des Ablaufs der Untersuchung als auch der Auswertung der Befragungsergebnisse durchgeführt. Diese Tätigkeiten sind typisch für die Markt- und Meinungsforschung und stellen eine eigenständige Leistung dar, die weit über die bloße Verarbeitung von Kundendaten hinausgeht. Die Nutzung von Kundendaten ist hier nur Teil einer zur selbstständigen Erledigung übertragenen Aufgabe. Datenschutzrechtlich ist daher von einer *Funktionsübertragung* auszugehen, bei der die Zurverfügungstellung personenbezogener Daten durch das Kreditinstitut als Datenübermittlung zu qualifizieren ist. Die fehlende Information und Einwilligung zur Datenübermittlung wurden beanstandet.

Wäre die Erstellung des Fragebogens und die anschließende Befragung im Rahmen zweier nacheinander liegender Verträge erfolgt, dann hätte der Annahme einer Auftragsdatenverarbeitung für den Komplex „Befragung“ nichts im Wege gestanden.

Zulässigkeit der Nutzung oder Übermittlung von Kundendaten

Die Zulässigkeit sowohl der Nutzung der Daten bei einer Auftragsdatenverarbeitung als auch der Übermittlung der Daten bei einer Funktionsübertragung ist an § 28 BDSG zu messen. Weder die Nutzung noch die Übermittlung von *Kundendaten für Kundenbefragungen* liegt im Rahmen der Zweckbestimmung eines Vertragsverhältnisses mit dem betroffenen Kunden, denn die Kundenbefragung ist weder erforderlich, um die vertraglichen Bankdienstleistungen zu erbringen, noch dient die Kundenbefragung allein Zwecken, die im jeweiligen Vertragsverhältnis begründet liegen. Als Rechtsgrundlage für eine zulässige Datennutzung und -übermittlung kommt deshalb allenfalls die Bestimmung des § 28 Abs. 1 Satz 1 Nr. 2 BDSG infrage. Ein berechtigtes Interesse zur Durchführung von Kundenbefragungen aufseiten des Kreditinstituts kann ebenso bejaht werden wie die Frage, ob zur Wahrung dieses berechtigten Interesses eine Datenübermittlung bzw. -nutzung erforderlich ist. Zu prüfen ist jedoch, ob nicht ein Grund zu der Annahme eines überwiegenden schutzwürdigen Interesses des Betroffenen am Ausschluss der Übermittlung oder der Nutzung besteht.

Bei der Nutzung der Kundendaten im Rahmen der *Auftragsdatenverarbeitung* für eine Kundenbefragung ist kein Grund zur Annahme ersichtlich, dass seitens des

betroffenen Kunden ein überwiegendes schutzwürdiges Interesse gegen diese Nutzung besteht. Um dies aber auf alle Fälle auszuschließen, ist eine Information der Kunden über die beabsichtigte Befragung sinnvoll. Eine *Information* der Kunden erscheint auch deshalb geboten, weil der Kunde von einer unbefugten Übermittlung ausgehen wird, wenn er von einem Markt- und Meinungsforschungsinstitut unvermittelt auf seine Kundenbeziehung zu seinem Kreditinstitut angesprochen wird.

Bei der Datenübermittlung im Rahmen der *Funktionsübertragung* wird die Kundenbeziehung zu einem Kreditinstitut gegenüber einem Dritten offenbart. Dies sind Daten, die den Bereich der Vermögensverhältnisse betreffen und daher im Allgemeinen als besonders schutzwürdig angesehen werden. Hier besteht also schon von vornherein ein Grund zu der Annahme eines überwiegenden schutzwürdigen Interesses des Kunden am Ausschluss der Übermittlung. Als datenschutzrechtlich unbedenklicher Weg bleibt deshalb nur die Einholung einer *schriftlichen Einwilligung* des Kunden zur Übermittlung seiner Daten an die Fremdfirma nach § 4 Abs. 2 BDSG. Um eine wirksame Einwilligung zu erhalten, ist auch dabei eine Information der Kunden über die beabsichtigte Befragung sicherzustellen.

Kundeninformation und Bankgeheimnis

Bei der *Information der Kunden* ist in beiden Fällen konkret anzugeben, welche personenbezogenen Daten zu diesem Zweck an welche Stelle weitergegeben werden sollen. Insbesondere ist offen zu legen, ob die Angaben des Kunden dem auftraggebenden Kreditinstitut zur Beschwerdebearbeitung unter Nennung des Kunden zurückgemeldet werden. Im Falle der Funktionsübertragung sollte dem Kunden zudem Gelegenheit gegeben werden, der Weitergabe seiner Daten zu widersprechen. Zweckmäßig wird dabei auch darüber informiert, innerhalb welcher Frist bei welcher Stelle der Widerspruch einzulegen ist.

Neben den Vorschriften des BDSG ist vom Kreditinstitut bei einer Kundenbefragung sowohl bei einer Auftragsdatenverarbeitung als auch bei einer Funktionsübertragung zudem das *Bankgeheimnis* zu beachten, denn bereits das Bestehen der Kundenbeziehung wird als vom Bankgeheimnis erfasst angesehen. Es sollte daher sichergestellt werden, dass der betroffene Kunde eine Befreiung vom Bankgeheimnis erteilt hat. Diese Befreiung ist nicht an das Schriftformerfordernis des § 4 Abs. 2 BDSG gebunden.

Hinzuweisen ist ergänzend auf § 35 Abs. 5 des novellierten BDSG, der ein Widerspruchsrecht gegen eine rechtmäßige Datenverarbeitung vorsieht. Danach dürfen personenbezogene Daten nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser Verarbeitung bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Datenverarbeitung überwiegt. Das bedeutet, dass den betroffenen Kunden bei Vorliegen einer besonderen persönlichen Situation eine Widerspruchsmöglichkeit zusteht und dass sie darüber auch seitens des Kreditinstituts informiert werden sollten.

Zu der Problematik „Kundenbefragungen durch Kreditinstitute“ hat sich die Aufsichtsbehörde auch in den HIM Nr. 37 vom 11. Januar 1999 (Staatsanzeiger für Baden-Württemberg Nr. 2 vom 18. Januar 1999, Seite 13) geäußert.

4.5 SCHUFA-Abfrage ohne berechtigtes Interesse

Mit der vertraglich festgelegten Möglichkeit, bei der SCHUFA gespeicherte Daten abzurufen, machen es sich manche Kreditinstitute, aber auch einzelne Mitarbeiter von ihnen manchmal zu leicht.

In einem Fall hat ein Kreditinstitut die bei der SCHUFA gespeicherten Daten zu einem ihrer Kunden im Wege des mit der SCHUFA nach §10 BDSG vereinbarten *automatisierten Abrufverfahrens* abgefragt. Der Kunde führte bei der Bank lediglich ein Sparkonto, das er nach Angaben des Kreditinstituts allerdings wie ein Girokonto benutzte, was von der Bank für eine gewisse Zeit toleriert wurde. Auf Grund eines für dieses Konto vorgelegten Pfändungsbeschlusses eines Amtsge-

richts sah sich das Kreditinstitut veranlasst, die Bonität des Kunden zu prüfen, und machte eine SCHUFA-Abfrage. Nach Ansicht der Bank ist der Abruf zur Wahrung ihrer berechtigten Interessen zulässigerweise erfolgt, um sich vor eventuellen Verlustgeschäften zu schützen und entsprechende Gegenmaßnahmen einleiten zu können.

Diese Auffassung konnte die Aufsichtsbehörde unter datenschutzrechtlichen Aspekten nicht teilen und hat die Vorgehensweise des Kreditinstituts beanstandet. Der Datenabruf bei der SCHUFA durch die Bank, für deren Zulässigkeit die Bank nach § 10 Abs. 4 BDSG verantwortlich ist, ist nur unter den in § 29 BDSG genannten Voraussetzungen oder mit Einwilligung des Betroffenen zulässig. Im vorliegenden Fall kam als mögliche Rechtsgrundlage nur § 29 Abs. 2 Satz 1 Nr. 1 a BDSG in Betracht. Danach ist für einen rechtmäßigen Abruf der Daten unter anderem Voraussetzung, dass das Kreditinstitut ein berechtigtes Interesse an der Kenntnis der Daten hat und dies glaubhaft darlegt. Ein solches Interesse wäre gegeben, wenn das Kreditinstitut ein Geschäft mit dem Kunden hätte abschließen wollen, das mit einem kreditorischen Risiko verbunden ist. Da der Kunde bei der Bank jedoch lediglich ein Sparkonto unterhielt und dieses, wie üblich, nur auf Guthabenbasis geführt wurde, hätten dem Kreditinstitut – auch bei der Nutzung dieses Sparkontos in Form eines Girokontos – keine finanziellen Nachteile erwachsen können. Somit lag kein berechtigtes Interesse des Kreditinstituts am Datenabruf vor. Da zudem auch keine Einwilligung des Kunden vorlag, war der Datenabruf unzulässig.

Die Aufsichtsbehörde hat den Betroffenen über seine Rechte informiert. Das Kreditinstitut hat das Fehlverhalten eingeräumt und zugesichert, durch interne Maßnahmen einen datenschutzgerechten Abruf sicherzustellen.

4.6 Einschaltung von Detekteien zur Schuldnerermittlung

Immer wieder kommt es vor, dass Kreditnehmer ihren Zahlungsverpflichtungen nicht mehr nachkommen und durch Unterlassen der Bekanntgabe eines Wohnsitz- oder Arbeitgeberwechsels gewollt oder ungewollt die Durchsetzung der Forderungen erschweren oder unmöglich machen. Manche Kreditinstitute setzen bei einer solchen Verletzung des Bankvertrags zur Ermittlung dieser Angaben *Detekteien* ein. Im Interesse aller Bankkunden wird es von den Kreditinstituten als legitim erachtet, säumige Schuldner, die ihre Pflichten verletzt haben, ausfindig zu machen.

Dazu wurde der Aufsichtsbehörde ein Fall vorgetragen, in dem eine Bank von einem Schuldner zur Kreditsicherung eine Lohnabtretung seiner Ehefrau, die selbst keine Bankkundin war, erhalten hat. Wegen Arbeitslosigkeit des Kreditschuldners wurden die vereinbarten Raten nicht mehr beglichen, sodass sich die Bank im Vorfeld gerichtlicher Durchsetzungsversuche veranlasst sah, die Ehefrau aus der Lohnabtretung in Anspruch zu nehmen. Die Ehefrau hatte zwischenzeitlich den Arbeitgeber gewechselt, der Bank allerdings den neuen Arbeitgeber nicht mitgeteilt, obwohl sie nach den Allgemeinen Geschäftsbedingungen und den Sicherungsverträgen hierzu verpflichtet war. Zur Ermittlung des aktuellen Arbeitgebers der Ehefrau wurde von der Bank eine Detektei eingeschaltet. Der Detektei wurden für diesen Zweck Namen und Anschrift der Ehefrau mitgeteilt. Bei der Detektei kam es zu einer *Personenverwechslung*, sodass dem Kreditinstitut der Arbeitgeber der Tochter mitgeteilt wurde und die Lohnabtretungserklärung dort vorgelegt wurde. Die Ehefrau machte gegenüber der Aufsichtsbehörde geltend, dass die Einschaltung einer Detektei und die Datenübermittlung durch die Bank an die Detektei rechtswidrig erfolgt sei. Der rechtmäßige Weg, um an die Angaben zu kommen, sei die Einleitung eines Vollstreckungsverfahrens, das die Bank schlussendlich auch betrieben hat.

Ergebnis der Überprüfung

Die *Datenübermittlung* an die Detektei war nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG *zulässig*. Ein Kreditinstitut hat ein berechtigtes Interesse daran, die Angaben zu erhalten, die eine Durchsetzung der Forderung erleichtern. Bestimmte Verfahren sind dafür nicht vorgeschrieben, jedoch müssen die gewählten Verfahren der bestehenden Rechtsordnung entsprechen. Zur Wahrung der berechtigten Interessen des Kreditinstituts war die Übermittlung der personenbezogenen Daten aus der vorhandenen Lohnabtretung erforderlich. Nach Auffassung der Aufsichtsbehörde

hätte die Gläubigerbank nicht zuvor versuchen müssen, den aktuellen Arbeitgeber bei der Ehefrau direkt zu erfragen. Dies ist bei auch sonst fehlender Mitwirkung in der Regel zeitraubend und häufig auch nicht Erfolg versprechend und kann sogar den beabsichtigten Erfolg vereiteln.

Überwiegende schutzwürdige Belange der betroffenen Ehefrau, die einer Datenübermittlung zum Zwecke der Ermittlung des aktuellen Arbeitgebers für den Gläubiger der Lohnabtretung entgegenstehen würden, waren auch nicht zu erkennen. Das Interesse, die Bank über den Arbeitgeber im Ungewissen zu lassen, ist nicht von vornherein als schutzwürdig anzusehen.

Bezüglich der Datenverarbeitung durch die Detektei mit damaligem Sitz in Hamburg insbesondere im Hinblick auf die *Personenverwechslung* hat die Aufsichtsbehörde den Hamburgischen Datenschutzbeauftragten eingeschaltet. Dort wurden schon mehrfach Prüfungen durchgeführt und der Detektei Auflagen nach dem BDSG erteilt. Wegen der strengen datenschutzrechtlichen Bestimmungen des BDSG hat die Detektei ihren Firmensitz zwischenzeitlich in das benachbarte Ausland verlegt. Zuvor bestätigte die Detektei noch die Löschung sämtlicher Daten zu der Ehefrau. Nachgeprüft werden konnte dies nicht mehr. Die Aufsichtsbehörde hat daher einzelne Bankenverbände gebeten, vor einer weiteren Zusammenarbeit mit dieser Detektei, die nach wie vor in Deutschland ihre Dienste anbietet, deren Zuverlässigkeit hinsichtlich der Datenerhebung und -verarbeitung, genau zu überprüfen.

4.7 Datenübermittlung an Partnerunternehmen

Der Aufsichtsbehörde wurde ein Fall vorgetragen, in dem der Betroffene von einer Außendienstmitarbeiterin eines Partnerunternehmens einer Bank telefonisch zu Beratungsterminen in der Bank eingeladen wurde. Bei dem Beratungsgespräch mit der Vertreterin des Partnerunternehmens war kein Mitarbeiter der Bank zugegen. Die Vertreterin hatte verschiedene Unterlagen des Betroffenen, darunter auch Kontenübersichten vorliegen. Erst nach dem Beratungsgespräch wurde dem Betroffenen klar, dass es sich nicht um eine Mitarbeiterin der Bank, sondern um eine Vertreterin des Partnerunternehmens gehandelt hat. Der Betroffene hat sich an die Aufsichtsbehörde gewandt, weil er in die *Weitergabe seiner Daten an das Partnerunternehmen* nicht eingewilligt hat.

Ergebnis der Überprüfung, Beanstandung

Die Aufsichtsbehörde musste das Vorgehen der Bank beanstanden. Datenschutzrechtlich gesehen handelt es sich bei den Partnerunternehmen um Dritte im Sinne des BDSG. Bei der Weitergabe von personenbezogenen Kundendaten handelt es sich daher um eine Datenübermittlung, die nur unter den in §28 BDSG genannten Voraussetzungen zulässig ist. Diese Voraussetzungen waren hier allesamt nicht erfüllt: Weder diente die Datenübermittlung der Zweckbestimmung des Vertragsverhältnisses zwischen dem Kunden und der Bank noch konnte die Bank geltend machen, dass die Datenübermittlung zur Wahrung der berechtigten Interessen der Bank erforderlich war. Zudem sind Daten, die eine Kundenbeziehung zu einem Kreditinstitut gegenüber einem Dritten offenbaren und die den Bereich der Vermögensverhältnisse betreffen, im Allgemeinen als besonders schutzwürdig anzusehen. Hier bestand also schon von vornherein ein Grund zu der Annahme eines überwiegenden schutzwürdigen Interesses des Kunden am Ausschluss der Übermittlung. Für eine zulässige Datenübermittlung an das Partnerunternehmen hätte daher eine schriftliche Einwilligung des Kunden nach § 4 Abs. 2 BDSG eingeholt werden müssen.

Die Bank hat versichert, durch organisatorische Anweisungen und interne Vorgaben im Grunde sichergestellt zu haben, dass eine Weitergabe von Kundendaten nur mit schriftlicher Einwilligung des Betroffenen erfolgt. Dass dies im vorliegenden Fall nicht beachtet wurde, sei ein menschliches Versehen. Die Mitarbeiterinnen und Mitarbeiter seien nochmals ausdrücklich auf die Einhaltung der Vorgaben verpflichtet worden.

4.8 Telefon-Servicecenter für Banken

Im Berichtszeitraum wurden von der Aufsichtsbehörde im Rahmen von schwerpunktmäßigen Sonderüberprüfungen drei Telefon-Servicecenter für Banken ge-

prüft. Alle drei Telefon-Servicecenter waren für die *Abwicklung von Telefonbankingverfahren* im Auftrag mehrer Banken tätig. Bei diesem Verfahren wickelt der Bankkunde den größten Teil seiner Bankgeschäfte über das Telefon ab. Das Telefon-Servicecenter erhält dabei Zugriff auf die Kundendaten. Jede Kontaktaufnahme des Kunden mit dem Telefon-Servicecenter wird aufgezeichnet, dabei werden die angegebene Kontonummer und die persönliche Identifikationsnummer (PIN) festgehalten. Zur Aufzeichnung der Telefongespräche geben die Kunden eine Einwilligungserklärung ab. Gegenstand der Prüfungen war vor allem, inwieweit bei der persönlichen Identifikation der Kunden gegenüber dem Telefon-Servicecenter die datenschutzrechtlichen Bestimmungen eingehalten werden.

Ergebnis der Überprüfung

Von der Aufsichtsbehörde wurden im Verlauf der Prüfungen *verschiedene Mängel* beanstandet, wie beispielsweise die Vertragsgestaltung für die Auftragsdatenverarbeitung nach § 11 BDSG, das Fehlen schriftlicher Aufträge, einzelne Formulierungen in der Vereinbarung der Bank mit den Kunden über die Teilnahme am Telefonbankingverfahren und in der Einwilligungserklärung in Telefonmarketingmaßnahmen, die für eine wirksame Einwilligungserklärung unzureichende Information, die mangels Vorgaben für die datenverarbeitungstechnischen Einrichtungen ungenügende Beauftragung weiterer Subunternehmer, das Fehlen eines Datensicherheitskonzepts, der mangelhafte Passwortschutz, die Vergabe einer Kennung für mehrere Benutzer und die mangelhafte räumliche Sicherung von gefertigten Überweisungsdokumentationen. Diese Mängel konnten in allen Fällen unmittelbar im Anschluss an die Überprüfung behoben werden.

Besonders erwähnenswert sind an dieser Stelle aber *folgende festgestellten Verstöße* gegen das Datenschutzrecht:

Bei einem Telefon-Servicecenter wurden für die Bearbeitung von Reklamationen die Aufzeichnungen über die Kundenaufträge vollständig wiedergegeben. Hatte der Kunde die Eingabe per Tastatur vorgenommen, erfolgte die Wiedergabe auf dem Bildschirm, hatte er telefonisch den Kontakt aufgenommen, erfolgte eine Wiedergabe der Sprachaufzeichnung. Dabei wurde auf dem Bildschirm und über Lautsprecher bzw. Kopfhörer neben der Kontonummer auch die PIN wiedergegeben. Die Aufsichtsbehörde sah die von dem Telefon-Servicecenter getroffenen Maßnahmen zum Schutz vor einer unberechtigten Kenntnisnahme der PIN als nicht ausreichend an.

Die Aufzeichnung und die Notwendigkeit für die Wiedergabe der PIN ist nur für die Ausnahmefälle erforderlich, in denen der Kunde bestreitet, überhaupt einen Auftrag erteilt zu haben. In den meisten Fällen, in denen überprüft werden muss, ob der Kundenauftrag weisungsgemäß ausgeführt wurde, besteht diese Notwendigkeit jedoch nicht. Da dem Kunden das Risiko der missbräuchlichen Nutzung der PIN aufgebürdet wird, muss die Bank das Verfahren so gestalten, dass in ihrer Einflusssphäre weitgehend ausgeschlossen wird, dass ein Mitarbeiter oder eine sonstige Person außer dem Kunden selbst Kenntnis von der PIN erlangt.

Die Aufsichtsbehörde forderte von dem Telefon-Servicecenter eine Umgestaltung der Software dahingehend, dass die PIN nur dann kenntlich gemacht werden kann, wenn dies tatsächlich erforderlich ist. Das Telefon-Servicecenter machte geltend, dass bisher kein Hersteller in der Lage sei, bei der Wiedergabe der Sprachaufzeichnungen zwischen der PIN und den weiteren Angaben zu unterscheiden. Die Aufsichtsbehörde hat anlässlich der Überprüfungen bei den anderen Telefon-Servicecentern aber datenschutzgerechte Verfahren festgestellt und dies dem betroffenen Telefon-Servicecenter mitgeteilt. Das Problem wurde letztendlich dadurch gelöst, dass sich das betroffene Telefon-Servicecenter mit einem anderen zusammengeschlossen hat, dessen Verfahren datenschutzgerecht ausgestaltet ist.

Beanstandungen

Bei einem anderen Telefon-Servicecenter mussten sowohl die systemseitige Sicherung als auch die räumliche Sicherung der Kundendaten nach der Anlage zu § 9 BDSG beanstandet werden. Auf dem Server des Telefon-Servicecenters befanden sich durch die Verknüpfung von Namen und Konto personenbezogene Daten der Kunden. Diese Daten waren weder besonders gesichert noch verschlüsselt. Die Arbeitsplätze befanden sich in einem Bürogebäude, dessen Zugangstüren un-

geschützt und nur mit normalen Sicherheitsschlössern mit Anschluss an die Schließanlage des Hauses versehen waren. Es gab keine Alarmanlage. In Anbetracht dieser geringen räumlichen Sicherheit forderte die Aufsichtsbehörde, die Sicherheit der Daten auf dem Server zunächst durch den Einsatz von Verschlüsselungssoftware zu erhöhen und umgehend ein Sicherheitskonzept, das auch die technisch-organisatorischen Maßnahmen des § 9 BDSG umfasst, zu erstellen. Das geprüfte Telefon-Servicecenter hat der Aufsichtsbehörde zwischenzeitlich anhand eines Sicherheitskonzeptes nachgewiesen, dass sowohl die räumliche als auch die systemseitige Sicherung der personenbezogenen Kundendaten gewährleistet ist.

4.9 Datenübermittlung bei Forderungsabtretung

In einem besonders gelagerten Fall, der der Aufsichtsbehörde mit einer Beschwerde zur Kenntnis gebracht wurde, wurde deutlich, dass gerade auch bei der *Abtretung von Forderungen* auf datenschutzrechtliche Erfordernisse zu achten ist.

In der Beschwerde wurde vorgetragen, dass eine Bank aus verschiedenen Forderungen, die sie gegen den Beschwerdeführer selbst bzw. gegen Kapital- und Personengesellschaften, bei denen der Beschwerdeführer Gesellschafter war, aus Darlehen und Bürgschaften hatte, an eine dritte Privatperson abgetreten hatte. Im Zusammenhang mit dieser Abtretung hatte der Rechtsanwalt der Bank an den Rechtsanwalt des Zessionars eine Kopie übergeben, die eine von der Bank erstellte Liste enthielt, in der die Saldenstände von Konten des Beschwerdeführers, der Gesellschaften, an denen dieser beteiligt war sowie von weiteren dritten natürlichen Personen aufgeführt waren. Gegen diese *Weitergabe der Saldenstände* richtete sich die Beschwerde.

Ergebnis der Überprüfung

Zuerst zu klären war, inwieweit es sich bei den Saldenständen der Konten überhaupt um personenbezogene Daten i. S. v. § 3 Abs. 1 BDSG handelt. Danach sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Nach Auffassung der Aufsichtsbehörde fallen hierunter neben den Salden der Konten, die einzelnen natürlichen Personen zuzuordnen sind, auch die Salden der Konten, die solchen Firmen zuzuordnen sind, bei denen eine enge finanzielle, personelle oder wirtschaftliche Verflechtung mit der Person des Beschwerdeführers als (z. T. persönlich haftender) Gesellschafter bzw. Geschäftsführer besteht.

Zulässigkeit der Datenübermittlung, Beanstandung

Im Anschluss daran war zu prüfen, ob sich eine Berechtigung zur Übermittlung der Saldenstände von der Bank an den Zessionar im Hinblick auf den zwischen diesen bestehenden Abtretungsvertrag aus § 1 Abs. 4 BDSG i. V. m. § 402 des Bürgerlichen Gesetzbuches (BGB) ableiten ließ. Danach ist die Bank als bisherige Gläubigerin bei wirksamer Abtretung verpflichtet, dem Zessionar als neuem Gläubiger die zur Geltendmachung der Forderungen nötige Auskunft zu erteilen. Dabei geht entsprechend § 1 Abs. 4 BDSG die Regelung in § 402 BGB den Bestimmungen des Bundesdatenschutzgesetzes vor.

Die Prüfung der Wirksamkeit der Abtretung im konkreten Fall ergab, dass zum einen die Abtretung nach §§ 399 und 400 BGB nicht ausgeschlossen war und zum anderen auch das Bankgeheimnis der Abtretung nicht entgegenstand. Gegenüber dem Bankgeheimnis hat der Auskunftsanspruch des Zessionars nach § 402 BGB in aller Regel Vorrang, sofern eine Forderung wirksam abgetreten wurde.

Allerdings war die Abtretung hier deshalb unwirksam, weil die Forderungen, die abgetreten werden sollten, nicht bestimmt oder bestimmbar waren. Nach dem der Aufsichtsbehörde vorgelegten Abtretungsvertrag wurde ein Teilbetrag, der sich auf eine Mehrheit von Forderungen bezog, abgetreten. Nach ständiger Rechtsprechung ist die Abtretung mehrerer Forderungen in Höhe eines Teilbetrages unwirksam, wenn nicht erkennbar ist, auf welche Forderungen oder Teilforderungen sie sich bezieht. Genau dies war bei dem vorgelegten Abtretungsvertrag der Fall, so dass § 402 BGB als die Übermittlung der Saldenstände gestattende lex specialis nicht in Betracht kam. Ein anderweitiges berechtigtes Interesse der Bank oder von dessen Anwalt an der Übermittlung der Saldenstände an den vermeintlichen

Zessionar i. S. v. § 28 Abs. 1 Satz 1 Nr. 2 BDSG war nicht ersichtlich, da die Übermittlung ausschließlich im Zusammenhang mit der Abtretung erfolgte.

Anzumerken bleibt, dass selbst bei wirksamer, weil hinreichend bestimmbarer Abtretung die Zulässigkeit der Übermittlung der Saldenstände wohl zu verneinen gewesen wäre. Schließlich ist zu fragen, ob eine Mitteilung von Saldenständen in Bezug auf eine größere Zahl von Personen und Firmen in diesem Umfang überhaupt von § 402 BGB gedeckt gewesen wäre. § 402 BGB erlaubt nämlich nur die Erteilung von Auskünften, die der neue Gläubiger zur Geltendmachung der Forderung benötigt. Damit ist aber regelmäßig gerade keine umfassende Mitteilung über die wirtschaftlichen Verhältnisse des Schuldners oder Dritter gemeint. Nach allem hatte die Aufsichtsbehörde die Übermittlung der Saldenstände zu beanstanden.

An diesem Fall lassen sich zwei Aspekte exemplarisch ablesen: Zum einen, dass im Zusammenhang mit Abtretungen und der dabei erfolgenden Weitergabe von Daten über den Schuldner vom bisherigen Gläubiger an den neuen Gläubiger besondere Sorgfalt erforderlich ist. Zum anderen, dass die Tätigkeit der Aufsichtsbehörde immer wieder von komplexen Sachverhalten und rechtlich schwierigen Fragestellungen geprägt wird, die weit über eine ausschließlich auf spezifische Datenschutzregelungen beschränkte Sichtweise hinausgehen.

4.10 Depotnummer und Depotinhaber im Adressfeld

Eine Depotinhaberin hat mit der Post eine Mitteilung über ihren Depotbestand erhalten.
Diese Mitteilung wurde in einem Fensterumschlag versandt. *Im Sichtfeld des Umschlags* waren neben der Adresse der Depotinhaberin auch Angaben zum Depotbestand, zur Depotnummer und Depotinhaberin erkennbar.

Die Aufsichtsbehörde hat dies der Bank gegenüber beanstandet, denn beim Transport von Datenträgern ist nach Ziff. 9 (Transportkontrolle) der Anlage zu § 9 BDSG auch zu verhindern, dass personenbezogene Daten unbefugt gelesen werden können. Es ist daher besondere Vorsorge zu treffen, dass personenbezogene Daten auf dem Transportweg nicht in die Hände Unbefugter gelangen.

Die Bank wurde aufgefordert, entsprechende Maßnahmen zu ergreifen, um solche Vorfälle künftig zu vermeiden, und der Aufsichtsbehörde die innerbetriebliche Anweisung dazu vorzulegen. Die Bank hat bestätigt, dass durch das Einfügen von mehreren Leerzeilen künftig vermieden wird, dass diese Daten im Sichtfeld eines Fensterumschlags erscheinen können, selbst wenn die innenliegende Sendung an den äußersten Rand verschoben wird.

5. Handel und Dienstleistungen

Anknüpfungspunkte zwischen dem Handels- und Dienstleistungsbereich und dem Datenschutz bestehen von der Kundenwerbung über die Auswertung von Kauf-, Nutzungs- und Kundenkartendaten bis zur Abwicklung bargeldloser Zahlungen.

Die meisten Anfragen und Beschwerden der Kunden hatten, von Ziff. 5.5 abgesehen, die elektronische Lastschrift und die damit verbundene Verarbeitung personenbezogener Daten zum Gegenstand. Bargeldlose Zahlungen werden im Handels- und Dienstleistungsbereich häufig durch Vorlage der EC-Karte abgewickelt. Bei den elektronischen Bezahlungsverfahren mit der EC-Karte gibt es zwei Verfahren aus dem Bankenbereich (POS und POZ) und das vom Handel vielfach eingesetzte *elektronische Lastschriftverfahren (ELV)*, bei dem der Kunde eine Abbuchungsermächtigung über den Rechnungsbetrag erteilt. Obwohl das letztere Verfahren regelmäßig genutzt wird, ist sein Ablauf den Kunden jedoch meistens unbekannt. Die EC-Karte *dient lediglich als Nachweis*, dass der Inhaber ein Girokonto hat, und zum Auslesen der Bankverbindung. Die EC-Funktionalität der Karte wird nicht genutzt.

5.1 Abwicklung des bargeldlosen Einkaufs

Am Beispiel des nachfolgenden Beschwerdefalls soll das ELV im Einzelhandel, so wie es von dem betroffenen Unternehmen eingesetzt wurde, aufgezeigt werden.

Ein Bürger beschwerte sich, dass ihm, nachdem er in einem Einzelhandelsgeschäft eingekauft und mittels ELV bezahlt hatte, der Rechnungsbetrag nach einigen Monaten ein zweites Mal von seinem Konto abgebucht wurde. Er vermutete eine missbräuchliche Nutzung seiner Kontendaten.

Überprüfung durch die Aufsichtsbehörde

Der Händler ist bei einem Abrechnungszentrum (ARZ) angeschlossen. Dieses ARZ hat mit dem Händler, neben einer Vielzahl anderer Händler, einen Vertrag über die Abwicklung der bargeldlosen Kundenzahlungen abgeschlossen, stellt ihm ein Zahlungsterminal für die Erfassung der elektronischen Lastschriften zur Verfügung und nimmt das Inkasso für ihn vor.

Legt ein Kunde an einem der Terminals des ARZ seine EC-Karte zur Bezahlung vor, werden die Kontonummer und die Bankleitzahl (Bankverbindung) aus der EC-Karte ausgelesen. Im Terminal wird die Bankverbindung mit einer von dem ARZ geführten Datei aller beim ARZ gesperrten Bankverbindungen (Sperrdatei) und mit einer weiteren Datei, die die Bankverbindungen enthält, die den Höchstbetrag an offenen Forderungen überschritten haben (Zahlungslimit), abgeglichen. Sind die Daten der entsprechenden Kunden nicht in den Dateien enthalten, wird der Zahlungsvorgang mit „OK“ bestätigt und zusammen mit den Daten über den Kauf im Terminal in einem so genannten *Transaktionsdatensatz* gespeichert. Mit dem „OK“ wird eine Lastschrifteinzugsermächtigung, mit Einwilligung in die Bekanntgabe der Anschrift des Kontoinhabers durch die Bank an das ARZ im Falle einer Rücklastschrift, ausgedruckt. Der Kunde muss den Beleg unterschreiben, der beim Händler verbleibt.

Das ARZ liest die Daten der Transaktionsdatensätze i.d.R. einmal pro Nacht über das Telefonnetz aus und lädt das Terminal mit den aktuellen Daten der Sperrdatei und der „Limitüberschreiter“. Das ARZ sammelt die Transaktionsdatensätze aller bei ihr angeschlossenen Händler, sortiert sie nach Banken, reicht sie auf elektronischem Wege im Auftrag der Händler bei den Banken zur Lastschrift ein und überweist die eingegangenen Gutschriften an die Händler. Dem ARZ sind Namen und Anschrift der einzelnen Kunden nicht bekannt, die Kundendaten sind durch die Bankverbindung „synonymisiert“.

Wird eine Lastschrift nicht eingelöst (Rücklastschrift), so wird, soweit die Forderung unbestritten ist, eine im Händlervertrag vereinbarte Forderungsabtretung wirksam. Das ARZ fordert den Beleg mit der unterschriebenen Einzugsermächtigung vom Händler an. Es legt ihn bei der Bank des betreffenden Kunden vor und kann auf Grund der Einwilligungserklärung des Kunden auf dem Beleg von der Bank Namen und Anschrift des Kontoinhabers übermittelt erhalten. Übermittelt die Bank die Daten, kann das ARZ die Forderung als eigene Forderung geltend

machen. Erst in diesem Verfahrensstadium arbeitet das ARZ mit personenbezogenen Daten des Kunden.

Das ARZ speichert die Transaktionsdatensätze, die Sperrdatei und die Datei mit den Limitüberschreitungen synonym. Die Dateien werden systemweit geführt. Die Löschung aus den beiden Dateien erfolgt nach Zahlungseingang bzw. im Falle einer berechtigten Rücklastschrift durch Ausbuchung.

Ergebnis der Überprüfung

Als Ursache für die doppelte Abbuchung stellte sich im Beschwerdefall heraus, dass auf Grund eines gleichzeitig aufgetretenen Hard- und Softwaredefekts an dem Terminal des Händlers die alten, bereits abgearbeiteten Datensätze nicht automatisch gelöscht, sondern vom Terminal erneut an das ARZ zur Durchführung des Abbuchungsvorgangs übermittelt wurden. Die technischen Defekte wurden behoben.

Das elektronische Lastschriftverfahren ist trotz einer solchen einzelnen technischen Panne vom Grundsatz her als *datenschutzgerecht* zu bezeichnen. Die Übermittlung der Transaktionsdaten vom Händler an das ARZ ist zulässig, auch wenn dem Kunden der Datenfluss nicht bekannt ist. Solange sich der Lastschriftbeleg beim Händler befindet, kann das ARZ den Vorgang keiner Person zuordnen, im Falle der Einlösung der Lastschrift werden folglich dort keine personenbezogenen Daten verarbeitet.

Beanstandungen

Erst im Falle der Nichteinlösung werden die Transaktionsdaten auf Grund der Übermittlung des Lastschriftbelegs und der Auskunft der Bank über Namen und Adresse des Kunden für das ARZ zu personenbezogenen Daten. In solchen Fällen war zu beanstanden, dass der Kunde beim Unterschreiben des Lastschriftbelegs *nicht* darüber *informiert* wurde, wie nach § 4 Abs. 2 BDSG erforderlich, dass die Forderung im Falle einer Rücklastschrift an das ARZ *übergeht* und dort seine personenbezogenen Daten bekannt werden. Nur bei rechtzeitiger, d. h. vorheriger Information kann er aber entscheiden, ob er in den Vorgang durch Teilnahme am Lastschriftverfahren einwilligt oder per Bargeld oder Euroscheck bezahlt.

Die Anzeige der Limitüberschreitung beim Händler ist die Übermittlung eines personenbezogenen Kundendatums dem Händler gegenüber. Sie sagt aus, dass der Kunde in den letzten Tagen bei den am Einzugssystem des ARZ angeschlossenen Händlern für über 3000 DM eingekauft hat. Die Übermittlung ist nach § 4 Abs. 1 BDSG nur mit der Einwilligung des Kunden zulässig, da sie nicht von § 28 BDSG gedeckt ist. Der Kunde hätte auf dem Lastschriftbeleg auch über das *Verfahren der Anzeige der Limitüberschreitung* informiert werden müssen, um entscheiden zu können, ob er in die Übermittlung an den Händler einwilligt. Die fehlende Einwilligung nach § 4 Abs. 1 BDSG wurde in solchen Fällen ebenfalls beanstandet.

Das Führen einer Sperrdatei über Kunden, die bei dem betreffenden Händler offene Forderungen haben, ist datenschutzrechtlich nach § 28 Abs.1 Satz 1 Nr. 2 BDSG zulässig. Werden diese Daten jedoch in einer gemeinsamen Sperrdatei aller am Abrechnungssystem angeschlossenen Händler zusammengeführt, so handelt es sich um eine Speicherung personenbezogener Daten zum Zwecke der Übermittlung. Die Daten sind für den Händler, dem angezeigt wird, dass der vor ihm stehende Kunde „gesperrt“ ist, personenbezogen. Die Speicherung und Übermittlung ist nach § 29 Abs. 1 und 2 BDSG zulässig. Jedoch besteht nach § 33 Abs. 1 BDSG eine Benachrichtigungspflicht des Betroffenen (d. h. des Kunden) bei der erstmaligen Übermittlung personenbezogener Daten, sofern er nicht in anderer Weise Kenntnis erlangt hat. Kenntnis in anderer Weise kann er durch einen Hinweis auf der Lastschrifteinzugsermächtigung erlangen. Das Fehlen dieser Information wurde ebenfalls beanstandet.

Das ARZ hat den Beanstandungen entsprochen und hat die *fehlenden Informationen* auf dem Beleg der Lastschrifteinzugsermächtigung entsprechend dem Formulierungsvorschlag der Aufsichtsbehörde *aufgenommen*. Die vorgeschlagenen Passagen lauteten:

„Überschreiten Ihre Einkäufe, die noch nicht abgebucht wurden, das Limit von 3000 DM, so wird dies auf dem Kassenterminal angezeigt, wenn Sie darüber hinaus bargeldlos bezahlen möchten.“

„Wird die Lastschrift von der Bank nicht eingelöst, so ist eine weitere Teilnahme am Lastschriftverfahren bis zur Bezahlung der offenen Forderung nicht möglich. Kontonummer und Bankleitzahl werden in eine Sperrdatei aufgenommen und allen angeschlossenen Händlern zum Abgleich zur Verfügung gestellt."

5.2 Erfassung von Personalausweisdaten bei elektronischen Lastschriftverfahren

Ein weiterer, häufiger Beschwerdegrund war, dass Händler, die das ELV anwenden, zunehmend die *Personalausweisdaten* der Kunden notieren oder den Personalausweis fotokopieren.

Bewertung der Aufsichtsbehörde

Ein Handelsunternehmen, das dem Kunden das Bezahlen mittels ELV anbietet, gewährt ihm einen *Warenkredit ohne Sicherheiten* bis zur Einlösung der Lastschrift. Der Einkauf ist nämlich erst „bezahlt", wenn die Lastschrift auf dem Konto des Händlers gutgeschrieben ist.

Auf dem Lastschriftbeleg lässt sich der Händler zwar vom Kunden für den Fall, dass die Lastschrift nicht eingelöst wird, die Einwilligung zur Bekanntgabe seines Namens und seiner Adresse durch die Bank geben, die Bank wird dadurch jedoch nicht zur Herausgabe der Daten verpflichtet. Teilweise lehnen zwischenzeitlich Banken diese Auskunft ab, sodass die Forderung im Falle der Rücklastschrift uneinbringlich wird. Auch nützt dem Händler die Auskunftsberechtigung der Bank nichts, wenn ihm eine gestohlene EC-Karte vorgelegt wird. Aus diesen Gründen gehen Händler dazu über, einerseits von Kunden, von deren Banken bekannt ist, dass sie die Auskunft verweigern, andererseits von sonstigen Kunden stichprobenweise zur Abschreckung Personalausweisdaten zu speichern.

Dies ist datenschutzrechtlich unerwünscht, aber nicht unzulässig. Der Händler hat ein Interesse, die Identität des Kunden, dem er einen Warenkredit gewährt, festzustellen, da er sich nur so vor Forderungsausfällen schützen kann. Die Erhebung und Speicherung ist nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG im Rahmen der Zweckbestimmung des Kauf- und Warenkreditvertrags zulässig. Der Kunde kann die Preisgabe seiner Identität z. B. durch Barzahlung vermeiden. Da zivilrechtlich die Barzahlung der gesetzlich vorgesehene Weg zur Begleichung einer Geldforderung ist und alle anderen Zahlungsarten nur Leistungen erfüllungshalber darstellen (§ 364 Abs. 2 BGB), wird der Kunde dadurch auch nicht unangemessen unter Druck gesetzt.

Mit der *Fotokopie* des Personalausweises geht der Händler jedoch *über* die datenschutzrechtlich zulässige Datenspeicherung nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG *hinaus*, da sich auf dem Ausweis mehr Daten befinden, als zur Schuldnerermittlung benötigt werden. Für die Kopie ist nach § 4 Abs. 1 BDSG grundsätzlich die schriftliche Einwilligung des Kunden erforderlich. Da die Sammlung der Kopien jedoch im Regelfall nicht den Dateibegriff des BDSG erfüllt, ist das BDSG auf die Personalausweiskopien in der Regel nicht anwendbar.

5.3 Speicherung von Einkaufsdaten bei Kundenkarteninhabern

Eine Kundin beschwerte sich bei der Aufsichtsbehörde, als sie feststellte, dass ein Kaufhaus von Ihrem Girokonto 40 DM abgebucht hatte, ohne dass der Abbuchung ein Einkauf zu Grunde lag. Da die Bankverbindung einer Person ein personenbezogenes Datum ist, das hier möglicherweise missbräuchlich genutzt wurde, wurde die Beschwerde von der Aufsichtsbehörde aufgegriffen.

Wie die Kundin weiter berichtete, hatte ihr Partner den Kauf, der der Abbuchung zu Grunde lag, getätigt und bar bezahlt. Beide besaßen persönliche „Vorteilskarten" (Kundenkarten) des Kaufhauses, eine Art Rabattkarte, mit deren Hilfe die Einkaufsumsätze im Kaufhaus in einem gemeinsamen Kartenkonto beider Karten gespeichert werden. Vom Gesamtumsatz wird nach einer bestimmten Zeit ein Rabattbetrag errechnet.

Ergebnis der Überprüfung

Bei einem gemeinsamen Einkauf hatte die Kundin die Kassenrechnung des Partners im ELV über ihre Bankverbindung beglichen, und der Partner hatte seine

„Vorteilskarte“ vorgelegt. Dabei wurde im Rechnersystem des Kaufhauses neben den Einkaufsdaten des Partners auch die Bankverbindung der Kundin gespeichert. Beim nachfolgenden Einkauf des Partners mit der Vorteilskarte wurde wegen einer Fehlbedienung der Kassiererin der Vorgang als elektronische Lastschrift gespeichert, obwohl der Partner bar bezahlte. Da die Bankverbindung fehlte, wurde bei der manuellen Nachbearbeitung der „fehlerhaften“ Lastschriftzahlung von der Buchhaltung des Kaufhauses auf die gespeicherten Lastschriftdaten des letzten Einkaufs auf dem Vorteilskartenkonto zurückgegriffen und die Bankverbindung der Kundin von dort übernommen. Dass kein unterschriebener Lastschrifteinzugsbeleg vorhanden war und bar bezahlt wurde, wurde bei der Nachbearbeitung nicht bemerkt.

Beanstandung

Bei der Bankverbindung handelt es sich um personenbezogene Daten der Kundin. Durch die Zuordnung zum kaufhausinternen Konto der „Vorteilskarte“ und der daraus resultierenden Lastschrift wurden die Daten widerrechtlich genutzt. § 28 Abs. 1 Satz 1 Nr. 1 und 2 BDSG können nicht als Rechtsgrundlage für die Zulässigkeit der Speicherung und Nutzung herangezogen werden. Die pauschale Einwilligungserklärung auf dem Antrag zur Ausstellung der „Vorteilskarte“ zur Speicherung der „Einkaufsdaten“ berechtigt zur Speicherung der Daten der Einkäufe nur entsprechend dem Zweck der „Vorteilskarte“, aber nicht zur zusätzlichen Speicherung der aus einem Lastschriftverfahren bekannten Bankverbindungsdaten. Die Lastschriftdaten werden nur im Rahmen des Lastschriftverfahrens rechtmäßig zu den offenen Forderungen gespeichert.

Diese *unzulässige Nutzung* der Daten der Bankverbindung wurde beanstandet. Da das Kaufhaus weiterhin auf die Speicherung der Bankverbindung des letzten Einkaufs auf dem Vorteilskartenkonto Wert legt, hat es seine Informationen auf dem Kartenantrag entsprechend geändert und klärt die Kunden darüber auf, welche Daten gespeichert werden, sodass sie wirksam darin einwilligen können.

5.4 Nahverkehrsfahrscheine auf der Chipkarte

Die Aufsichtsbehörde wurde darauf aufmerksam, dass ein großes Nahverkehrsunternehmen für seine Kunden einen Fahrschein auf einer Chipkarte entwickelt hatte.

Bei elektronischen Chipkarten besteht die Gefahr, dass eine Vielzahl von Daten über den Kunden auf einfachem Wege gespeichert und personenbezogen ausgewertet werden können. Die Gefahr von Datenschutzverletzungen kann insbesondere dann bestehen, wenn die Daten nicht nur auf der Chipkarte selbst, sondern zusätzlich auch noch in einem Rechnersystem im Hintergrund verarbeitet werden. So wäre es z. B. denkbar, dass beim Einsatz *elektronischer Fahrkarten* die Fahrten der Kunden personenbezogen gespeichert, ausgewertet und ein *Bewegungsprofil* angelegt wird. Dies ist ohne Einwilligung des Betroffenen unzulässig, da eine solche Verarbeitung personenbezogener Daten nicht von § 28 BDSG gedeckt wird. Um sicherzustellen, dass das Unternehmen datenschutzkonform vorgeht, wurde es von der Aufsichtsbehörde überprüft.

Ergebnis der Überprüfung

Das Unternehmen stellt seinen Kunden kostenlose Chipkarten zur Verfügung. Die Chipkarten werden unpersönlich ausgegeben, das heißt, das Unternehmen hat keine personenbezogen Daten über den Inhaber (Kunde). Der Kunde kann die Chipkarte an verschiedenen Fahrscheinterminals oder bei den Kassen der Fahrer mit einem Geldbetrag aufladen. Mit diesem Guthaben kann er dann Fahrscheine lösen, die elektronisch auf seiner Chipkarte vermerkt und beim Ein- oder Umsteigen elektronisch ausgelesen werden. Alle Aufladungsvorgänge und Fahrscheinkäufe werden von den jeweiligen Kassen an das *Hintergrundsystem im Rechenzentrum* des Verkehrsunternehmens übermittelt. Die Kenntnis der Aufladungen (Einzahlungen) und Abbuchungen für Fahrscheine ist für die Buchhaltung des Unternehmens erforderlich. Die Kenntnis der Fahrstrecken und Nutzungszeiten wird für die Einsatzplanung, die Abrechnung der Nahverkehrsfördermittel und der Schülerbeförderungskosten benötigt. Zum Zwecke der Missbrauchskontrolle werden alle Fahrten und Aufladungen innerhalb eines bestimmten Zeitraums kartenbezogen gespeichert und danach abgeglichen, ob den abgebuchten Fahrten

auch entsprechende Aufladungen der jeweiligen Karte gegenüberstehen. Werden dabei *Manipulationen am Guthaben* der Karte festgestellt, was dann der Fall ist, wenn keine entsprechende Einnahmebuchung im Hintergrundsystem vorliegt, wird die Karte gesperrt.

Dieses System ist *datenschutzgerecht*, solange dem Unternehmen die Identität des Chipkarteninhabers nicht bekannt ist. Das Unternehmen ist in der Zukunft daraufhin zu überwachen, dass es weiterhin die Chipkarten unpersönlich ausgibt und auch nicht durch andere Maßnahmen nachträglich Kenntnis über die Identität des Inhabers erlangt.

5.5 Speicherung von Kundendaten in Fitnesscentern

In der letzten Zeit wurden mehrfach Beschwerden von Kunden gewerblicher Fitnesscenter über die Speicherung ihrer Daten vorgebracht. Grund für die Beschwerden war die Ausgabe maschinenlesbarer „Clubkarten“, mit deren Hilfe der Zugang kontrolliert werden soll.

Ergebnis der Überprüfung

Verarbeitung von Kundendaten

Bei Beginn der Mitgliedschaft werden in einem Nutzungsvertrag in der Regel Name, Anschrift, Geburtsdatum, besondere Hinweise wie z. B. relevante gesundheitliche Beeinträchtigungen und die Bankverbindung vom Kunden erhoben und im DV-System verarbeitet. Je nach Abrechnungsform werden auch die Nutzungszeiten gespeichert. Die genannten Daten sind personenbezogene Daten. Damit ist das BDSG anzuwenden.

Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG dürfen personenbezogene Daten im Rahmen der Zweckbestimmung eines *Vertragsverhältnisses* gespeichert und genutzt werden. Darunter sind alle Daten zu verstehen, die erforderlich sind, um den Vertrag zwischen dem Fitnesscenter und dem Kunden erfüllen zu können. Die Einwilligung des Kunden in diese auf gesetzlicher Grundlage zulässige Datenverarbeitung ist nicht erforderlich.

Elektronische Speicherung von Kundenportraits

Datenschutzrechtlich problematisch ist es, wenn das Fitnesscenter ein digitalisiertes Bild des Kunden in seinem Rechner speichert. Hierzu gehen immer mehr Unternehmen über, um dadurch zu verhindern, dass die persönliche Einlasskarte an Dritte weitergegeben wird. Mit dem Einlesen der Karte am Eingang wird dem Kontrollpersonal das Bild der betreffenden Person auf dem Monitor angezeigt, so dass die Identität kontrolliert werden kann.

Die Aufsichtsbehörde hält eine solche Speicherung und Nutzung des Kundenportraits *nicht* nach § 28 Abs. 1 Satz 1 Nr. 1 und 2 BDSG für *zulässig*, da die Kontrolle auch anhand von Dokumenten mit Foto, wie z. B. Personalausweis, Führerschein, Schülerausweis oder einer Einlasskarte mit Foto durchgeführt werden kann. Die Speicherung des Portraits im Rechnersystem ist daher nach § 4 Abs. 1 BDSG nur mit der *schriftlichen Einwilligung* der betreffenden Person zulässig.

Speicherung von Fitnessdaten

Neben den Daten für die Verwaltung des Kunden werden manchmal auch Daten über die körperliche Fitness des Kunden gespeichert, um Veränderungen bei den Körperwerten festzustellen und das Training entsprechend ausrichten zu können. Bei diesen Körperdaten handelt es sich um sehr *sensible personenbezogene Daten*, da sie sich auf gesundheitliche Verhältnisse des Kunden beziehen. Auch wenn die Daten nur unter Mitwirkung des Kunden erhoben werden können, dürfen sie nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG nur für den Zweck genutzt werden, für den sie erhoben wurden. Die Zweckbestimmung des Vertragsverhältnisses ist sehr eng auszulegen. Daher sind die Daten auch für die Mitarbeiter, die sie nicht kennen müssen, zu sperren. Jede andere Nutzung, insbesondere auch die Einsichtnahme Dritter oder die Weitergabe, wäre ohne eine Einwilligung des Kunden unzulässig.

Die betroffenen Fitnesscenter wurden im Rahmen der Behandlung der Beschwerden auf die Rechtslage hingewiesen.

5.6 Adressermittlung über die Telefonnummer

Am Markt tauchen immer wieder Telefonauskunft-CD's auf, auf denen der Anschlussinhaber über seine Rufnummer ermittelt werden kann (Inverssuche). Diese *Inverssuche* wird von den Aufsichtsbehörden im Düsseldorfer Kreis aus den folgenden Gründen für rechtswidrig erachtet:

Die Daten der Telefonauskunft-CD stammen aus den Teilnehmerverzeichnissen der Telefongesellschaften (Telekommunikationsdienstleister). Diese unterfallen der Telekommunikations-Datenschutzverordnung vom 18. Dezember 2000 (TDSV), die die Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV) ablöste. Nach § 13 Abs. 2 TDSV muss der Kunde der Eintragung in das Teilnehmerverzeichnis zustimmen, wobei er unter anderem bestimmen kann, dass die Eintragung in gedruckten oder elektronischen Verzeichnissen erfolgt. Mit der Zustimmung ermöglicht der Kunde nach § 14 Abs. 1 TDSV ausschließlich die *Auskunftserteilung* über seine *Rufnummer* (Telefonauskunft), was bei dem Anfragenden bestimmte Vorinformationen, vor allen Dingen die Kenntnis des Namens des Eingetragenen voraussetzt. Die Auskunftserteilung über Namen und andere Daten von Kunden, von denen nur die Rufnummer bekannt ist, ist nach § 14 Abs. 4 TDSV unzulässig. Dies bedeutet, dass Kunden, die der Veröffentlichung ihrer Daten im Teilnehmerverzeichnis zugestimmt haben, damit nur der Suche ihrer Rufnummer, nicht aber der Auswertung ihrer Daten im Wege der Inverssuche zugestimmt haben.

Bewertung der Inverssuche

Ein Unternehmen, das eine Telefonauskunft-CD herausgibt, ist *kein Telekommunikationsdienstleister*. Auf dieses Unternehmen finden deshalb nicht die Regelungen der TDSV, sondern die des BDSG Anwendung. Für eine Nutzung der personenbezogenen Daten durch deren Übertragung aus öffentlichen Verzeichnissen und ihre Übermittlung an die Erwerber der CD kann sich das Unternehmen, soweit die Suchfunktion auf die Rufnummer beschränkt ist, auf die Zustimmung der Telefonkunden zur Veröffentlichung ihrer Daten berufen. Die Zustimmung kann insoweit als Einwilligung im Sinne von § 4 Abs. 1 BDSG qualifiziert werden. Für die Inverssuche fehlt es jedoch rechtmäßig an einer entsprechenden Zustimmung bzw. Einwilligung. Auch wenn die Daten öffentlichen Verzeichnissen entnommen sind, kann deren Nutzung und Übermittlung auch nicht auf § 28 Abs. 1 Satz 1 Nr. 3 BDSG gestützt werden, da das Interesse der betroffenen Telefonkunden, nicht über die Rufnummer identifiziert werden zu können, das Interesse des Unternehmens am Vertrieb einer CD-Rom mit Inverssuche offensichtlich überwiegt. In seiner Entscheidung vom 10. November 2000 bewertete das Oberlandesgericht Köln die Rechtslage entsprechend. Die *Inverssuche* auf einer Telefonauskunft-CD ist deshalb *unzulässig*.

Ergebnis der Überprüfung

Mit einem Unternehmen, das eine Telefonauskunft-CD mit Inverssuche herausgab, hat die Aufsichtsbehörde in der Vergangenheit langwierige Verhandlungen geführt. Es hat die Inverssuche beanstandet und die Unterlassung der weiteren Herausgabe verlangt. Das Unternehmen hat schließlich die Inverssuchefunktion auf der Telefonauskunft-CD entfernt, insbesondere nachdem es in einem Rechtsstreit mit einer Telefongesellschaft unterlegen ist. Danach muss es die für die CD benötigten Daten der Anschlussinhaber aus dem Teilnehmerverzeichnis der Telefongesellschaft anmieten. Die Gesellschaft hat in dem Überlassungsvertrag eine Nutzung der Daten für Zwecke der Inverssuche untersagt. Die Aufsichtsbehörde hat die Einhaltung der Unterlassung bei den nachfolgenden Auflagen der Telefonauskunfts-CD überprüft.

5.7 Gebäudebilddatenbank

Eine Vielzahl von Anfragen und Bürgerbeschwerden erreichte die Aufsichtsbehörde, nachdem bekannt wurde, dass ein Verlag aus Niedersachsen mit einem Kamerafahrzeug die Straßen aller Gemeinden mit mehr als 20 000 Einwohnern abfuhr, um *Aufnahmen* von den *Häuserfronten* zu machen. Die Bilder, wie im Film abspielbar, sollen mit den Geokoordinaten versehen in einer Gebäudebilddatenbank eingestellt und gewerblich genutzt werden.

Die für den Verlag datenschutzrechtlich zuständige Aufsichtsbehörde ist der Landesdatenschutzbeauftragte des Landes Niedersachsen, da der Verlag dort seinen Sitz hat. Der Landesdatenschutzbeauftragte hat das Projekt der Gebäudebilddatenbank eingehend überprüft und ist dabei zu dem Ergebnis gekommen, dass die Aktivitäten des Verlags nach der geltenden Rechtslage datenschutzrechtlich *nicht zu beanstanden* sind. Dieser Bewertung haben die Aufsichtsbehörden im Düsseldorfer Kreis nicht widersprochen: Ein Film, auch wenn er mit den Geokoordinaten der jeweiligen Position des Aufnahmewagens versehen ist, ist keine Datei im Sinne des § 3 Abs. 2 BDSG; das Verfahren fällt daher nicht unter den Geltungsbereich des BDSG bei nichtöffentlichen Stellen nach § 1 Abs. 2 Nr. 3 BDSG. Diese Beurteilung wird von der Aufsichtsbehörde *mitgetragen*.

Das OLG Karlsruhe hat zwischenzeitlich die zivilrechtliche Zulässigkeit der Aufnahmen festgestellt mit der Begründung, dass die Außenansicht eines Gebäudes keine Rückschlüsse auf die Privatsphäre der Besitzer zulässt. Mit dem novellierten BDSG ändert sich der Anwendungsbereich des BDSG bei nichtöffentlichen Stellen, was eine Neubewertung der Gebäudebilddatenbank erforderlich macht.

6. Versicherungswirtschaft

6.1 Finanzdienstleistungsklausel bei Fusion oder Verbund von Versicherung und Bank

Die Tätigkeit der Aufsichtsbehörde war nachhaltig geprägt von der Beurteilung datenschutzrechtlicher Fragen im Zusammenhang mit Fusionen bzw. Zusammenschlüssen von Versicherungsunternehmen untereinander oder mit Banken bzw. Bausparkassen. Dabei ging es sowohl um die Beratung der Unternehmen im Vorfeld als auch um die Bearbeitung verschiedener Beschwerden von Versicherungsnehmern.

So hat die Aufsichtsbehörde eine Versicherungsgruppe sowie eine Versicherung und eine Bausparkasse im Zuge ihrer jeweiligen *Unternehmensfusion* bei der Gestaltung einer *einheitlichen Konzerneinwilligungsklausel* beraten. Diese umfasst die gemeinsame Datenverarbeitung auf Konzernebene und die *Finanzdienstleistungsklausel*, also die Klausel, wonach der Vermittler die allgemeinen Antrags-, Vertrags- und Leistungsdaten auch für die Beratung und Betreuung in sonstigen Finanzdienstleistungen nutzen darf. Diese Beratung erstreckte sich auch auf die Einführung der neuen, einheitlichen Klausel in den Versicherungs- bzw. Vertragsbestand. Die neue Klausel ersetzte und erweiterte die in den einzelnen fusionierten Unternehmen bisher gebräuchlichen Einwilligungsklauseln, welche – von wenigen Ausnahmefällen abgesehen – bereits Inhalt der vertraglichen Beziehungen mit den Versicherungsnehmern sind.

Form der Einwilligungserklärung

Nach § 4 Abs. 2 Satz 2 BDSG sind Einwilligungen beim Betroffenen regelmäßig schriftlich einzuholen, wenn nicht wegen besonderer Umstände eine andere Form angemessen ist. Diesen Ausnahmefall sah die Aufsichtsbehörde in solchen Fällen der Unternehmensfusion als gegeben. Zunächst ist das Interesse der fusionierenden Unternehmen, die Datenverarbeitung konzernweit auf eine einheitliche Basis zu stellen, durchaus berechtigt. Innerhalb des neu entstehenden Konzerns müssten sonst eine ganze Reihe unterschiedlicher Einwilligungserklärungen bei der Datenverarbeitung berücksichtigt werden, was die Vertragsführung erheblich erschweren würde. Schließlich dürften alle Versicherungsnehmer, die nach 1983 Versicherungsverträge abgeschlossen haben, bereits zusammen mit dem Versicherungsantrag datenschutzrechtliche Einwilligungserklärungen abgegeben haben. Seitdem existieren in der Versicherungswirtschaft mit der Datenschutzaufsicht im Grundgesetz abgestimmte Standard-Einwilligungsklauseln.

Auch in den von der Aufsichtsbehörde beratenen Fusionsfällen sprachen gute Gründe für die Einführung einer *vereinheitlichten Einwilligungserklärung* in den Versicherungsbestand im Wege der Information der Versicherungsnehmer *mit jederzeitiger Widerspruchsmöglichkeit*. Angesichts der Vielzahl der betroffenen Verträge war diese Lösung eine anstelle der Schriftform angemessene gangbare Alternative. Im Hinblick auf die zu erwartende geringe Rücklaufquote unterschriftlich abzugebender Einwilligungen wäre das auch aus datenschutzrechtlicher Sicht berechtigte Unternehmensziel, die konzerninterne Datenverarbeitung für die Vertragsführung auf einheitliche Grundlagen zu stellen, nicht erreichbar gewesen.

Nach Auffassung der Aufsichtsbehörde beeinträchtigte die gewählte Widerspruchslösung die Betroffenen auch nicht in unangemessener Weise. Den Versicherungsnehmern, die in der überwiegenden Mehrzahl bereits mit dem Vertragsabschluss eine Einwilligungserklärung abgegeben haben bzw. die über die beabsichtigte Verwendung ihrer Daten mitsamt Widerspruchsmöglichkeit informiert wurden, wurde die Einwilligungserklärung mit ihren möglichen Auswirkungen nochmals vor Augen geführt und erläutert. Dabei war für die Aufsichtsbehörde wichtig, dass die Betroffenen auf die so genannte Finanzdienstleistungsklausel besonders hingewiesen wurden. Die Unternehmen haben sich zudem verpflichtet, Widersprüche in jeder Form, insbesondere auch telefonisch entgegenzunehmen und in der Sperrdatei zu vermerken. Die Aufsichtsbehörde hat auch dafür Sorge getragen, dass alle Versicherungsnehmer, die Widerspruch eingelegt haben, eine Bestätigung erhielten.

Historische Entwicklung

Auch in der Vergangenheit wurde dieses Informationsverfahren von der Aufsichtsbehörde nicht beanstandet, weil dieses auch im Einklang mit den Absprachen der Aufsichtsbehörden im Düsseldorfer Kreis mit der Versicherungswirtschaft steht. Dem ist folgende *historische Entwicklung* vorausgegangen:

Vor einigen Jahren ist die Versicherungswirtschaft in Deutschland allgemein dazu übergegangen, die Kunden im Zusammenhang mit Versicherungsanträgen standardisierte Einwilligungserklärungen unterschreiben zu lassen, mit denen die verschiedenen Formen der Verarbeitung von Kundendaten, insbesondere die Weitergabe zu bestimmten Zwecken auf eine datenschutzrechtlich tragfähige Grundlage gestellt werden. Diese Einwilligungsklausel, die auch heute noch bei nahezu allen Vertragsabschlüssen verwendet wird, ist sehr allgemein gehalten und so komplex, dass sie ohne weitere Erläuterung nicht überschaubar ist. Die notwendige Erläuterung enthält ein *„Merkblatt zur Datenverarbeitung“*, in dem beispielhaft die Verarbeitung und Nutzung der Versichertendaten beschrieben ist.

Einwilligungsklausel und Merkblatt sind zwar im Grundsatz zwischen der Versicherungswirtschaft und den Aufsichtsbehörden abgestimmt. Trotzdem gingen bis zum Frühjahr 1995 die Auffassungen sowohl über den Inhalt der Klausel als auch über das Verfahren der Kundeninformation auseinander. Nach Auffassung der Versicherungswirtschaft deckte die Einwilligungsklausel auch die Weitergabe von Daten zur Vermittlung anderer Finanzprodukte ab; die Versicherungswirtschaft war auch der Meinung, dass es für die Rechtswirksamkeit der Einwilligung ausreichend sei, dass der Kunde sich auf Wunsch näher über deren Inhalt und Tragweite seiner Einwilligung informieren kann, nämlich durch Anforderung des Merkblatts. Das Innenministerium hat wie die anderen Aufsichtsbehörden hingegen immer die Auffassung vertreten, dass der Kunde unter „Betreuung durch den Versicherungsvermittler“ keinesfalls eine Geldanlageberatung auf breiter Basis verstehen kann und, dass er auch vor der Unterschrift unter die im Versicherungsantrag abgedruckte datenschutzrechtliche Einwilligungserklärung darüber informiert sein muss, was mit seinen Daten über die Vertragsverwaltung und -erfüllung hinaus geschehen soll. Diese Diskussion wurde schließlich im Jahr 1995 dadurch beendet, dass sich der Gesamtverband der Deutschen Versicherungswirtschaft mit *einer erweiterten Fassung der Einwilligungserklärung* einverstanden erklärte, die die Nutzung der Vertragsdaten zu *Finanzdienstleistungszwecken* ausschließlich durch den Versicherungsvermittler vorsieht, der für die Betreuung der jeweiligen Versicherungskunden zuständig ist. Außerdem wurde die Auffassung der Aufsichtsbehörden anerkannt, dass die Einwilligungserklärung insgesamt nur dann rechtswirksam ist, wenn die betroffenen Kunden durch Aushändigung des „Merkblatts zur Datenverarbeitung“ darüber informiert worden sind, welche Verarbeitungsformen auf Grund ihrer Einwilligung vorgesehen sind.

Nach dem Vorschlag des Gesamtverbands der Deutschen Versicherungswirtschaft sollten die Versicherer die erweiterte Einwilligungsklausel beim Neuabschluss von Verträgen insbesondere bei kapitalbildenden Versicherungen verwenden. Außerdem wollte die Versicherungswirtschaft ihre seit Jahren übliche Praxis beibehalten und auch die bisherigen Kunden im Zusammenhang mit der Fälligkeit von Versicherungsleistungen auf die Wiederanlage der Kapitalbeträge ansprechen. Die Aufsichtsbehörden sind schließlich der Versicherungswirtschaft dadurch entgegengekommen, dass sie akzeptiert haben, dass diejenigen Versicherungsunternehmen, die weiterhin Daten aus Versicherungsverträgen für Finanzdienstleistungszwecke an ihre Versicherungsvertreter übermitteln wollen, ihre „Altkunden“ über die Erweiterung der Standard-Einwilligungserklärung informieren und diesen Gelegenheit zum Widerspruch bieten. Maßgeblich für diese Entscheidung war, dass sich die Versicherungsunternehmen verwaltungstechnisch nicht in der Lage sahen, von Millionen Bestandskunden förmliche Einwilligungserklärungen einzuholen. Die Aufsichtsbehörde hat jedoch darauf bestanden, dass bei dieser Gelegenheit alle Versicherungskunden das „Merkblatt zur Datenverarbeitung“ erhalten, damit die insgesamt vorhandenen Informationsdefizite beseitigt werden.

Im Hinblick auf die oben dargestellten komplizierten datenschutzrechtlichen Fragen im Zusammenhang mit Fusionen, an denen Versicherungen beteiligt sind, ist es als Erfolg der vorab erfolgten Beratungstätigkeit der Aufsichtsbehörde zu werten, dass angesichts der großen Zahl betroffener Versicherungsnehmer dennoch die Zahl der Beschwerden vergleichsweise gering blieb.

Ebenso ist festzuhalten, dass in anderen Bundesländern bei Fusionen von Versicherungen in gleicher Weise verfahren wurde. Auch bei künftigen Fusionen wird dies der einzig gangbare Weg sein, um die Datenverarbeitung im neu entstehenden Fusionsunternehmen konzernweit auf eine einheitliche Grundlage zu stellen.

6.2 Informationsaustausch bei Wechsel des Versicherungsunternehmens in der privaten Krankenversicherung

Die Aufsichtsbehörde hatte sich auch mit der Frage zu befassen, wie der Informationsaustausch beim Wechsel des Versicherten von einer privaten Krankenversicherung zu einer anderen datenschutzrechtlich zu beurteilen ist.

Hintergrund waren verschiedene Beschwerden auch aus anderen Bundesländern, die dazu führten, dass dieses Thema zudem in der AG Versicherungswirtschaft des Düsseldorfer Kreises erörtert wurde. Dabei wurde die vom Innenministerium Baden-Württemberg vertretene Auffassung, die auch in den HIM Nr. 38 vom 18. Januar 2000 (Staatsanzeiger für Baden-Württemberg Nr. 2 vom 24. Januar 2000, Seite 12) ihren Niederschlag fand, von der AG Versicherungswirtschaft übernommen. Der Verband der privaten Krankenversicherer hat mit einem Rundschreiben an seine Mitgliedsunternehmen die HIM Nr. 38 übersandt und damit über die Auffassung der Aufsichtsbehörden informiert.

Bei den Beschwerden wurde im Kern vorgetragen, dass die notwendigen Beschränkungen beim *Informationsaustausch im Zuge eines Wechsels des Versicherungsunternehmens in der privaten Krankenversicherung* weder von den anfragenden noch von den auskunftserteilenden Privatkrankenversicherungsunternehmen hinreichend beachtet worden sind.

So lag der Aufsichtsbehörde ein Fall vor, in dem ein Krankenversicherer erst nach Vertragsabschluss aus Anlass eines Kostenerstattungsantrags des Versicherten bei dessen früherem Versicherer umfassende Auskünfte über die an ihn gewährten Leistungen angefordert und erhalten hat, aus denen über einen Zeitraum von zehn Jahren die Diagnosen sämtlicher Krankheiten und Beschwerden ersichtlich waren, für die der Versicherte medizinische Hilfe in Anspruch genommen hatte. Aus den Auskünften war keine Vorerkrankung des Versicherten ersichtlich, die mit dem Kostenerstattungsantrag in Zusammenhang hätte gebracht werden können. Allerdings fanden sich in der Krankenhistorie des Versicherten weitere, nicht im Vertragsantrag angegebene Vorerkrankungen, die zu einer Änderungskündigung des Versicherungsvertrages in eine höhere Risikoklasse mit höherem Beitrag führte.

Bewertung der Aufsichtsbehörde

Beim Wechsel der privaten Krankenversicherung gilt nach Auffassung der Aufsichtsbehörde datenschutzrechtlich grundsätzlich Folgendes:

Will ein Versicherter seine private *Krankenversicherung wechseln*, muss er dem künftigen Versicherer seine bisherigen *Krankheiten* und *Beschwerden* im Versicherungsantrag *offen legen*. Diese Angaben braucht der neue Versicherer, um das Vertragsrisiko richtig einzuschätzen und für die Versicherung eine risikogerechte Prämie festzulegen. Zur Klärung des Risikos benötigt der Versicherer ergänzend gelegentlich Auskünfte von Ärzten und Krankenhäusern, die den Versicherten behandelt haben, ebenso können Auskünfte des bisherigen Krankenversicherers notwendig sein.

Damit Mitarbeiter von Krankenversicherungen sowie Ärzte und andere Behandler einem Auskunftsersuchen des Privatkrankenversicherers entsprechen können, muss sie der Versicherte jeweils von ihrer beruflichen Schweigepflicht entbinden. Dies geschieht bei Versicherungen regelmäßig mit einer in den Versicherungsantrag aufgenommenen *Schweigepflichtentbindungserklärung*, die üblicherweise einem zwischen der Versicherungswirtschaft und den obersten Aufsichtsbehörden für den Datenschutz abgesprochenen Standard entspricht. Damit wird der Krankenversicherer ermächtigt, an einen anderen Personenversicherer (Kranken-, Lebens-, Unfallversicherer) Auskünfte über den Gesundheitszustand einer bei ihm versicherten Person zur Beurteilung des Risikos eines beantragten Versicherungsvertrags zu erteilen. Die Auskunft ist nur zulässig, soweit dazu ein Anlass besteht, und darf nur Vorgänge der letzten zehn Jahre umfassen. Diese Ermächtigung zur

Auskunftserteilung endet fünf Jahre nach der Antragstellung. Die Entbindung von der Schweigepflicht ist demnach nach Anlass und Zeitpunkt (beantragter Vertrag), Zweck (Risikoprüfung), Umfang (Gesundheitszustand der letzten zehn Jahre) und Geltungsdauer (fünf Jahre) eindeutig beschränkt.

Davon ausgehend, beurteilt die Aufsichtsbehörde die Zulässigkeit des Informationsaustauschs zwischen Unternehmen der privaten Krankenversicherung wie folgt:

– Die *Erhebung von Daten* durch ein Versicherungsunternehmen der privaten Krankenversicherung bei einem anderen Privatkrankenversicherer über einen Versicherten ist am Grundsatz von *Treu und Glauben* zu messen (§ 28 Abs. 1 Satz 2 BDSG). Das Unternehmen, das die Erhebung durchführt, kann dabei davon ausgehen, dass der Versicherte seinen bisherigen Vertragspartner im beschriebenen Umfang von der Schweigepflicht entbunden hat. Zweck und Umfang der Datenerhebung müssen mit der Schweigepflichtentbindung im Einklang stehen, wenn die Erhebung nicht treuwidrig sein soll.

– Ein umfassender *Datenaustausch* zur Risikoprüfung ist *grundsätzlich nur vor dem Vertragsabschluss* von der Schweigepflichtentbindungserklärung gedeckt. Die Pflicht des künftigen Krankenversicherers zur Vertragsgestaltung entsprechend dem Individualrisiko berechtigt ihn, sich über den Gesundheitszustand des künftigen Versicherten umfassend zu informieren. Ein dazu erforderlicher Informationsaustausch mit dem bisherigen Krankenversicherer greift in das informationelle Selbstbestimmungsrecht des Betroffenen nicht unangemessen ein, insbesondere verletzt dieser keine schutzwürdigen Interessen.

– Der *Datenaustausch* zur Risikoprüfung ist auch *nach Vertragsabschluss* nicht grundsätzlich ausgeschlossen; die Befristung der Schweigepflichtentbindungserklärung auf fünf Jahre nach der Antragstellung würde sonst keinen Sinn ergeben. Während des Vertragslaufs ist die Erhebung von Daten beim früheren Privatkrankenversicherer und die Übermittlung durch diesen jedoch durch den Grundsatz der Verhältnismäßigkeit des Eingriffs in die Persönlichkeitsrechte des Betroffenen auf das beschränkt, was für eine Risikoprüfung auf Grund eines konkreten Anlasses erforderlich ist. Dem trägt auch der Wortlaut der Schweigepflichtentbindungserklärung Rechnung. Gesundheitsdaten können dann zulässigerweise nur erhoben werden, wenn und vor allem soweit dazu eine konkrete Veranlassung besteht. Dies wird regelmäßig dann der Fall sein, wenn sich beim Versicherten vor dem Vertragsabschluss nicht bekannte Krankheiten oder Beschwerden zeigen, die nach medizinischer Erfahrung nicht kurzfristig auftreten, sondern auf eine längere Vorgeschichte schließen lassen. Nach Vertragsabschluss ist die Erhebung von Gesundheitsdaten beim Vorversicherer auf Daten zu beschränken, welche die aufgetretenen Krankheits- oder Beschwerdebilder betreffen.

– Unternehmen der Privatkrankenversicherung dürfen Daten über Versicherte oder ehemalige Versicherte nur unter den Voraussetzungen des § 28 Abs. 2 Satz 1 Nr. 1 a BDSG übermitteln, soweit dies zur *Wahrung berechtigter Interessen* des künftigen Krankenversicherers erforderlich ist, darüber hinaus nur mit der *Einwilligung* des Versicherten. Die gebräuchliche datenschutzrechtliche Einwilligungsklausel beschränkt die Zulässigkeit der Übermittlung ebenso wie die Schweigepflichtentbindungsklausel auf den für die Risiko- und Leistungsprüfung erforderlichen Umfang. Datenschutzrechtlich und ggf. auch strafrechtlich verantwortlich für die Zulässigkeit der Übermittlung ist das übermittelnde Unternehmen. Die Privatkrankenversicherer haben vor einer Übermittlung insbesondere von Diagnosedaten die Berechtigung des Auskunftsersuchens zumindest nach Plausibilitätsgesichtspunkten zu prüfen.

Im Zusammenhang mit dem hier zu Grunde liegenden Beschwerdefall hat sich die Aufsichtsbehörde auch mit dem Verband der Privatkrankenversicherer in Verbindung gesetzt, um sicherzustellen, dass die privaten Krankenversicherer künftig entsprechend der dargestellten Rechtslage verfahren.

6.3 Übermittlung von Versichertendaten in die USA im Rahmen der Entschädigung für Holocaust-Opfer

Das in letzter Zeit viel diskutierte Thema einer *Entschädigung für Holocaust-Opfer* hat auch die Aufsichtsbehörde beschäftigt.

Dabei ging es um die von verschiedenen Versicherungsunternehmen aufgeworfene Frage, wie mit Forderungen aus den USA nach Übermittlung sämtlicher *Versichertendaten aller Policen aus den Jahren 1920 – 1945* dorthin datenschutzrechtlich umzugehen ist.

Hintergrund dieser Forderungen sind die sog. Holocaust-Versicherungsgesetze zahlreicher US-Bundesstaaten. Die in die USA übermittelten Versichertendaten sollen anschließend im Internet veröffentlicht werden, um auf diesem Wege den Holocaust-Opfern oder deren Erben die Möglichkeit einzuräumen, die Geltendmachung von Ansprüchen gegen deutsche Versicherungsunternehmen zu klären. Den in den jeweiligen US-Bundesstaaten tätigen Versicherungsunternehmen droht bei Nichtbeachtung dieser Gesetze der Entzug ihrer dortigen Lizenz.

Wegen der grundsätzlichen Bedeutung wurden die damit verbundenen Fragen in der AG Versicherungswirtschaft des Düsseldorfer Kreises erörtert. Dabei wurde auch eine gemeinsame Erklärung erarbeitet, die gegenüber dem Gesamtverband der Deutschen Versicherungswirtschaft abgegeben wurde.

Danach sind die Aufsichtsbehörden – mit Ausnahme des Landesbeauftragten für den Datenschutz Berlin – der Auffassung, dass eine *Übermittlung aller* von den US-amerikanischen Gesetzen *geforderten Daten* – soweit sie sich in automatisierten oder nicht-automatisierten Dateien befinden – weder von § 28 Abs. 1 noch von § 28 Abs. 2 Satz 1 Nr. 1 a oder von § 28 Abs. 2 Satz 1 Nr. 1 b BDSG gedeckt und damit unzulässig ist, weil schutzwürdige Interessen der betroffenen, nicht zum Kreis der Holocaust-Opfer gehörenden Versicherungsnehmer entgegenstehen. Datenschutzrechtlich ist im Rahmen des § 28 Abs. 2 Satz 1 Nr. 1 b BDSG nur die Übermittlung oder Nutzung der personenbezogenen Daten ausschließlich von Holocaust-Opfern unbedenklich.

Von den Aufsichtsbehörden wurde auf *verschiedene Wege* hingewiesen, wie unter Beachtung der datenschutzrechtlichen Vorschriften die Frage, ob noch unbeglichene Ansprüche von Holocaust-Opfern gegen deutsche Versicherungsunternehmen bestehen, geklärt werden kann.

So wäre es datenschutzrechtlich vertretbar, die versicherungseigenen Archive für Nachforschungen durch Dritte zu öffnen, wobei die Rechercheure auf das Datengeheimnis verpflichtet sein müssten. Überwiegende schutzwürdige Interessen von Versicherungsnehmern oder Begünstigten gegen die Einsichtnahme würden nicht bestehen, soweit sich eine anschließende Veröffentlichung auf einzelne Angaben der Holocaust-Opfer, deren Begünstigte oder Erben beschränkt. In diesem Fall könnte von einem berechtigten Interesse der überlebenden Opfer, Begünstigten oder deren Erben an der Veröffentlichung ausgegangen werden, vorbehaltlich zu beachtender Widersprüche in Einzelfällen. Datenschutzrechtlich hätte dieses Verfahren den Vorteil, dass Daten über die Vielzahl von Versicherungsnehmern, die nicht Holocaust-Opfer sind, bei den Versicherern verbleiben.

Ein anderer Lösungsweg wäre, eine Recherche im Wege der Auftragsdatenverarbeitung in Deutschland zu ermöglichen. In diesem Fall würde eine Auswertung nicht durch Dritte im Rechtssinne erfolgen. Dazu müssten die Versicherer einen Dritten damit beauftragen, eine solche Recherche durchzuführen.

6.4 Hinweis- und Warnsysteme der Versicherungen

Häufig wird die Aufsichtsbehörde mit Fragen und Kritik konfrontiert, die sich darauf beziehen, dass Versicherungsunternehmen eine Versicherung kündigen und die Kündigung an ein *zentrales Hinweis- und Warnsystem* weitermelden. Exemplarisch ist ein Fall, in dem ein Arzt sich darüber beschwerte, dass ein Versicherungsunternehmen, bei dem für seine Arztpraxis eine *Rechtsschutzversicherung* bestand, wegen zu vieler Schadensfälle den Versicherungsvertrag kündigen wolle und zudem diese Kündigung an ein zentrales Hinweis- und Warnsystem weitermelden werde.

Zu der datenschutzrechtlich relevanten Frage der Weitermeldung der Kündigung durch den Versicherer an ein zentrales Hinweis- und Warnsystem wies die Aufsichtsbehörde zunächst darauf hin, dass es in Deutschland für einige Versicherungssparten, so auch für Rechtsschutzversicherungen, zentrale Hinweis- und Warnsysteme gibt, an die die Versicherer verschiedene Umstände im Zusammenhang mit dem Vertragsabschluss, der Leistungsgewährung und der Vertragsbeendigung melden.

Diese zentralen Hinweis- und Warnsysteme werden vom Gesamtverband der Deutschen Versicherungswirtschaft (GDV) geführt. Diese Systeme sind dort so gestaltet, dass sämtliche Informationen nur in codierter Form vorliegen. Die Informationen werden dem jeweiligen Versicherungsunternehmen, das die Systeme nutzt, für den Geschäftsbetrieb zur Verfügung gestellt. Durch die Codierung können vorhandene Daten nur dann gelesen werden, wenn im Einzelfall die Daten des Versicherungsnehmers bzw. Antragstellers vorliegen. Der GDV ist als Systembetreiber wegen der Codierung der Datenbestände nicht in der Lage, Auskunft über die zu einzelnen Personen gespeicherten Daten zu geben. Der GDV betreibt die Systeme im Auftrag der angeschlossenen Versicherungsunternehmen, die aus datenschutzrechtlicher Sicht weiterhin für die Meldung und Speicherung der Daten verantwortlich sind.

Bewertung der Aufsichtsbehörde

Die für die datenschutzrechtliche *Zulässigkeit der Übermittlung und Speicherung von Daten in den Hinweis- und Warnsystemen* nach § 28 Abs. 1 Satz 1 Nr. 2 bzw. Abs. 2 Satz 1 Nr. 1a BDSG erforderlichen berechtigten Interessen der Versicherungsunternehmen bestehen darin, dass solche Systeme als präventive Schutzmaßnahmen insbesondere zur Risikobewertung, zur Aufklärung vorvertraglicher Anzeigeverpflichtungen und zur Abwehr von Betrugsmaßnahmen unverzichtbare Hilfsinstrumente für die Versicherer darstellen.

Des Weiteren setzt eine zulässige Verarbeitung von Daten in einem solchen System nach den vorgenannten Bestimmungen voraus, dass schutzwürdige Interessen der betroffenen Versicherungsnehmer nicht entgegenstehen. Sie stehen dann nicht entgegen, wenn die an das zentrale Warn- und Hinweissystem gemeldeten Daten für den Vertragsabschluss oder die Vertragsführung rechtserheblich sind; sie müssen daher entweder *besondere Risiken* aus der bisherigen Vertragsführung oder der Person des Versicherungsnehmers oder *missbrauchsverdächtige Umstände* bei der Inanspruchnahme der Versicherung dokumentieren. In diesen Fällen kann aus datenschutzrechtlicher Sicht davon ausgegangen werden, dass keine schutzwürdigen Interessen des betroffenen Versicherungsnehmers durch die Meldung solcher Umstände verletzt werden können.

In der Rechtsschutzversicherung z. B. sind als solche risikorelevante Umstände die Fälle der Kündigung durch den Versicherer nach mindestens zwei Versicherungsfällen innerhalb von 12 Monaten oder der Kündigung durch den Versicherer nach mindestens drei Versicherungsfällen innerhalb von 36 Monaten anerkannt.

Unabhängig davon ist die Versicherungswirtschaft seit geraumer Zeit dazu übergegangen, aus Gründen der Rechtssicherheit und der Transparenz die Einwilligung der Versicherungsnehmer in die Übermittlung von Daten an solche zentralen Hinweis- und Warnsysteme schon im Zusammenhang mit dem Vertragsabschluss einzuholen. Im Falle einer solchen *Einwilligung* kommt es dann nicht mehr auf das Vorliegen berechtigter Interessen der Versicherungswirtschaft und die Beurteilung der schutzwürdigen Interessen des Betroffenen an.

In jedem Fall steht dem betroffenen Versicherungsnehmer zu, nach § 34 BDSG vom Versicherer *Auskunft* darüber zu verlangen, ob und welche Daten an das zentrale Hinweis- und Warnsystem übermittelt worden sind. Daneben besteht der Anspruch auf Berichtigung unrichtiger Daten und auf Löschung unzulässig gespeicherter Daten nach § 35 BDSG.

Sofern sich die Versicherer an die auch von der Aufsichtsbehörde bewirkte Gestaltung der Hinweissysteme und der beschränkten Auswahl der Meldegründe halten und beachten, dass Daten nicht allgemein, sondern nur im entscheidungserheblichen konkreten Einzelfall abgerufen werden dürfen, besteht für die Aufsichtsbehörde keine Veranlassung, dies zu beanstanden.

6.5 Übermittlung von Daten an Ehegatten

Nicht selten übermitteln Versicherungsunternehmen personenbezogene Daten statt an den eigentlichen Versicherungsnehmer an den Ehegatten, zu dem keine vertraglichen Beziehungen bestehen. Dies führt besonders dann zu Beschwerden, wenn es sich um Lebensversicherungen handelt und die Ehegatten getrennt leben bzw. ein Scheidungsverfahren läuft.

In diesen Fällen muss die Aufsichtsbehörde regelmäßig darauf hinweisen, dass eine solche Datenübermittlung an den nicht in den Vertrag einbezogenen Ehegatten datenschutzrechtlich *nicht zulässig* ist. Auch bei Bestehen einer Ehe kann nicht von der generellen Zulässigkeit der *Datenübermittlung an den jeweiligen Ehegatten* ausgegangen werden. Dies wird schon daran deutlich, dass für einen Dritten häufig nicht erkennbar ist, ob die Ehegatten z. B. getrennt leben bzw. sich in Scheidung befinden. Darüber hinaus gilt grundsätzlich, dass die Ehegatten jeweils zu wirtschaftlich selbstständigem Handeln berechtigt sind, ganz abgesehen davon, dass in einer Ehe auch Gütertrennung vereinbart sein kann.

Die Offenlegung von Daten gegenüber Ehegatten unterliegt daher denselben gesetzlichen Anforderungen wie die Datenübermittlung an Dritte. Deshalb ist für die Zulässigkeit einer Datenübermittlung an einen Ehegatten nach § 28 Abs. 2 BDSG maßgeblich, ob die Übermittlung zur Wahrung von dessen berechtigten Interessen erforderlich ist und ob kein Grund zu der Annahme besteht, dass der Ehegatte, der Vertragspartner des Versicherers ist, ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat.

Da solche schutzwürdigen Interessen des Ehegatten-Versicherungsnehmers ohne eine detaillierte Kenntnis der persönlichen Lebensverhältnisse nicht ausgeschlossen werden können, sollte grundsätzlich keine Übermittlung von Daten an den anderen Ehegatten erfolgen. Nur so kann sichergestellt werden, dass es nicht zu Beschwerden und zu Beanstandungen durch die Aufsichtsbehörde kommt.

7. Werbewirtschaft

7.1 Adresshandel und Direktwerbung

Zahlreiche an die Aufsichtsbehörde gerichtete Anfragen und Beschwerden zeigen, dass die Methoden des Adresshandels und der Direktwerbung für viele Bürger nicht nachvollziehbar sind. Mittels moderner Computertechnik ist es heute leicht möglich, jeden Bürger direkt anzuschreiben und ihm das Gefühl zu vermitteln, er stehe in diesem Anschreiben im Mittelpunkt. Nicht wenige fragen sich aber, woher das werbende Unternehmen Namen und Anschrift kennt und über welche Informationen es möglicherweise zusätzlich verfügt. Auf Kritik stößt die Werbung insbesondere dann, wenn der Angeschriebene bislang in keinem Geschäftsverhältnis mit dem werbenden Unternehmen stand und in der Werbung konkrete persönliche Verhältnisse und Interessen, wie beispielsweise Hausbesitzer oder Gartenfreund, angesprochen werden.

Mit der nachfolgenden Darstellung wurde den Betroffenen das Geschäft mit dem *Adresshandel* und der *Direktwerbung* verdeutlicht und aus datenschutzrechtlicher Sicht bewertet.

Um Informationen über eigene Kunden gezielt für eigene und fremde Werbemaßnahmen nutzen zu können, müssen die Informationen gespeichert und aufbereitet werden. Für die Nutzung eigener Kundendatenbestände zu eigenen Werbezwecken sind die Zulässigkeitsvoraussetzungen des § 28 Abs. 1 Satz 1 Nr. 2 BDSG maßgebend. Bei einer wettbewerbsrechtlich zulässigen Werbemaßnahme stehen der Nutzung der Daten für diese Zwecke in der Regel keine schutzwürdigen Interessen entgegen.

Um aber neue Kunden zu gewinnen, werden für die Durchführung von Werbeaktionen Adressen von solchen Personen benötigt, die den anzusprechenden Zielgruppen am nächsten kommen. Aus Kostengründen sollen schließlich nur solchen Personen Waren oder Dienstleistungen angeboten werden, die nach ihren persönlichen oder finanziellen Verhältnissen sowie nach ihren Vorlieben oder Interessen primär dafür infrage kommen.

Möglichkeiten der Datenerhebung:

- Häufig werden durch *Verlosungen*, *Preisausschreiben* oder anlässlich von Messen und *Informationsveranstaltungen* Daten erhoben, die für die eigentliche Geschäftsabwicklung nicht notwendig sind, wie etwa Beruf, Familienstand, Interessen und Hobbys. Da für eine zulässige Speicherung und Nutzung dieser Daten die Datenerhebung nach § 28 Abs. 1 Satz 2 BDSG nach Treu und Glauben und auf rechtmäßige Weise erfolgen muss, ist bei solchen Befragungen auf den Zweck der Datenerhebung und die Freiwilligkeit der Beantwortung hinzuweisen. Auf die Ausführungen unter Ziff. 7.3 wird Bezug genommen.

- Meist werden jedoch von *Adresshandelsunternehmen* angebotene und bereits auf die Zielgruppe zugeschnittene Adressbestände für die Durchführung von Werbeaktionen angemietet oder gekauft. Adresshandelsunternehmen haben sich, wenn sie Adressen geschäftsmäßig zum Zwecke der Übermittlung erheben, speichern und auch übermitteln, nach den Bestimmungen des § 29 BDSG zu richten. Das Speichern und Verändern personenbezogener Daten durch Adresshandelsunternehmen ist im Rahmen des § 29 Abs. 1 BDSG zulässig, wenn die Datenerhebung nach Treu und Glauben und auf rechtmäßige Weise erfolgt ist. Zur Datenerhebung werden von den Adresshandelsunternehmen systematisch alle *öffentlich zugänglichen Quellen* ausgewertet. Dies sind in der Regel Telefon- und Adressbücher, Branchen- und Behördenverzeichnisse, Handels- und Vereinsregister, Anzeigenteile von Zeitungen und Zeitschriften, Vereinspublikationen, amtliche Mitteilungsblätter und ähnliche Quellen. Allein diese Quellen genügen aber vielfach nicht, um die für die Werbewirtschaft interessanten Bewertungen wie Interessen, Alter, voraussichtliche Kaufkraft, Hausbesitz u.ä. zu erhalten. Es werden daher *Haushaltsbefragungen* mit umfangreichen Fragebögen zu dem Zweck durchgeführt, komplette Werbeprofile anzulegen. Auf die Ausführungen unter Ziff. 7.3 wird Bezug genommen. Die Adresshandelsunternehmen verschaffen sich aber auch weitergehende Informationen beispielsweise durch *Wohngebietsbegehungen* und haben dazu Gebäudedatenbanken mit Angaben über die Wohngebietsstruktur und sogar über

Art und Alter jedes einzelnen Hauses erstellt, denn es wird davon ausgegangen, dass Personen mit vergleichbaren Wohnverhältnissen sich auch in Lebensstil und Kaufverhalten ähneln. Es handelt sich dabei vielfach um *Einschätzungen*. Bei Bedarf werden die Daten aus den verschiedenen Datenbanken verknüpft, um eine möglichst genaue Zielgruppe für eine Werbemaßnahme herauszufiltern. Diskriminierend und nicht zulässig ist eine Zuordnung zu einer bestimmten sozialen Schicht auf Grund der Adresse, wenn damit eine negative Bewertung verbunden ist.

– Auch *Unternehmen* und *sonstige Organisationen* verkaufen oder vermieten für einmalige Zwecke ihre Kunden- oder Mitgliederadressen an nicht konkurrierende Unternehmen für Direktwerbezwecke. Interessant sind die *Daten des Versandhandels:* Dort entsteht vor allem bei einer bereits seit längerem bestehenden Geschäftsbeziehung ein relativ genaues Bild über die Kunden und das Kaufverhalten. Neben einer Vielzahl von Einzeldaten wie z. B. Anschrift, Telefonnummer, Geschlecht, Geburtsdatum, Umsatz oder Zahlungsverhalten fallen auch Daten über die Kaufhäufigkeit, die Art der bezogenen Waren, Reklamationen und Reaktionen auf Werbeaktionen an und lassen verwertbare Aussagen über Verhalten, Einstellungen und Vorlieben zu.

Listenprivileg

Für die *Adressweitergabe zu Werbezwecken* hat der Gesetzgeber im BDSG eine spezielle Vorschrift, das so genannte *Listenprivileg*, geschaffen. Nach § 28 Abs. 2 Satz 1 Nr. 1 b und § 29 Abs. 2 Satz 1 Nr. 1 b BDSG dürfen listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe übermittelt werden, soweit sich die Daten auf eine Angabe über die Zugehörigkeit zu dieser Personengruppe, auf den Namen, Titel, akademische Grade, die Anschrift, die Berufs-, Branchen- oder Geschäftsbezeichnung und das Geburtsjahr beschränken und keine schutzwürdigen Interessen der Betroffenen am Ausschluss der Übermittlung bestehen. Solche schutzwürdigen Interessen werden in der Regel nur bei besonders sensiblen Daten vermutet. Beispielhaft werden im BDSG Daten genannt, die sich auf gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten, religiöse oder politische Anschauungen oder bei Übermittlungen durch den Arbeitgeber auf arbeitsrechtliche Rechtsverhältnisse beziehen. Angaben u. a. über die Kreditwürdigkeit, die ethnische Herkunft oder das Sexualleben sind ebenso schutzwürdig. Für eine zulässige Datenübermittlung darf die in einer solchen Adressliste enthaltene Personengruppe nur durch ein einziges Merkmal beschrieben sein. Es darf also beispielsweise nicht mehr ausgesagt werden, als dass es sich um Kunden eines bestimmten Unternehmens oder Mitglieder einer bestimmten Organisation handelt.

Listbroking-Verfahren

Dies nützt dem werbenden Unternehmen ohne eine weitergehende Bewertung oft nicht viel. Um mehr Daten weitergeben zu können, was für Adresseigner und werbendes Unternehmen wesentlich Gewinn bringender ist, wird die Einschränkung des Listenprivilegs häufig dadurch umgangen, dass die Kundendaten von den Adresseignern nicht direkt dem werbenden Unternehmen zur Nutzung übermittelt, sondern *Adressmaklern* – auch *Listbroker* genannt – für eine Vermietung zu Werbezwecken angeboten und zur Verfügung gestellt werden. Adressmakler werden häufig mit der Beschaffung der zielgruppengerechten Adressbestände für eine Werbecampagne beauftragt. Sie haben einen Überblick über die auf dem Markt befindlichen Adressbestände und vermitteln den Kontakt, zumal für größere Werbeaktionen meist *mehrere* unterschiedliche *Adressbestände* zusammengeführt werden. Die Adressmakler speichern diese Daten aber nicht bei sich, sondern geben sie für einen in der Regel einmaligen Gebrauch weiter an ein mit der Durchführung der Werbemaßnahme beauftragtes Unternehmen – auch Lettershop genannt. Der Lettershop führt das Werbematerial und die Adressen zusammen, eine Speicherung der Daten findet nur für den Zeitraum der Herstellung des Werbemittels statt. Datenschutzrechtlich gesehen handelt es sich um eine Auftragsdatenverarbeitung nach § 11 BDSG. Eine Datenübermittlung vom Adresseigner zum werbenden Unternehmen findet nicht statt, denn das werbende Unternehmen erhält unmittelbar keine Anschriften übermittelt. Vielmehr erfährt es die Daten der Beworbenen nur und erst, wenn diese auf die Werbung reagieren und dabei ihre Daten selbst bekannt geben, wie beispielsweise bei einer Bestellung.

In den meisten vorgebrachten Fällen konnte die Aufsichtsbehörde die Betroffenen über die Rechtslage aufklären. Gravierende Verstöße gegen datenschutzrechtliche Bestimmungen waren im Berichtszeitraum nicht festzustellen.

Werbung mit bereits gewonnenen Abonnenten

Erwähnenswert ist allerdings in diesem Zusammenhang ein Fall, in dem ein freier Handelsvertreter in einer Gemeinde an der Haustüre für eine Firma Zeitschriftenabonnenten geworben hat. Bei der Durchführung der Werbetour waren auch Mitglieder des ortsansässigen Fußballvereins engagiert, denn dieser sollte eine Trikotspende erhalten, wenn genügend Abonnenten für die Zeitschriften gefunden würden. Besonders unter Druck gesetzt wurden die beworbenen Bürger zum einen durch den Hinweis auf die zu erwartende Trikotspende für den Fußballverein, zum anderen vor allem aber dadurch, dass die Abonnementwerber jeweils Listen vorlegten, in denen belegt wurde, dass namentlich benannte andere Gemeindeeinwohner bereits eine Zeitschrift abonniert hatten. Zudem wurden die Listen auch dem von der Spende bedachten Fußballverein vorgelegt.

Ergebnis der Überprüfung, Beanstandung

Diese Handlungen haben nach Auffassung der Aufsichtsbehörde gegen das Datenschutzrecht verstoßen und wurden beanstandet. Die Bekanntgabe der Daten eines geworbenen Abonnenten gegenüber den Nachbarn oder die Meldung an den Fußballverein war nach der Auffassung der Aufsichtsbehörde von keiner der Zulässigkeitsvoraussetzungen des § 28 BDSG gedeckt. Sie entspricht weder der Zweckbestimmung des Vertragsverhältnisses nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG noch war sie zur Wahrung der berechtigten Interessen des werbenden Unternehmens nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG erforderlich. Zudem war davon auszugehen, dass überwiegende schutzwürdige Interessen der Betroffenen vorliegen. Die Offenlegung dieser Daten wäre demnach nur auf der Grundlage einer schriftlichen Einwilligung der Betroffenen zulässig gewesen, über die die Zeitschriftenwerber aber nicht verfügten. Der freie Handelsvertreter wurde von der auftraggebenden Firma zur Änderung seiner Werbemethoden aufgefordert.

7.2 Rechte der Betroffenen

Werbewiderspruch

Der einzelne Betroffene kann sich gegen die Nutzung und Übermittlung seiner Daten für Werbezwecke und für Zwecke der Markt- und Meinungsforschung wehren, indem er bei der speichernden Stelle – und dies ist in der Regel der Adresseigner – dagegen *Widerspruch* nach § 28 Abs. 3 BDSG erhebt. Der Widerspruch kann jederzeit erhoben werden und führt dazu, dass die Daten für diese Zwecke nicht mehr verwendet werden dürfen. Sie dürfen also weder selbst genutzt noch anderen zur Verfügung gestellt werden. Die Anschrift der Betroffenen muss in eine Sperrdatei aufgenommen oder mit einem Werbesperrvermerk versehen werden. Bei neuen Werbeaktionen muss ein Abgleich mit den eingesetzten Adressbeständen erfolgen, um zu verhindern, dass die Betroffenen erneut angeschrieben werden. Hält sich ein Unternehmen nicht daran, kann es sich nach § 43 BDSG strafbar machen.

Häufig richten sich die Eingaben dagegen, dass auf die Bitte, nicht mehr beworben zu werden, keine Bestätigung erfolgt oder dass der Widerspruch vermeintlich nicht beachtet wird. Zu einer schriftlichen Bestätigung über das Setzen einer Werbesperre sind die Unternehmen nicht verpflichtet. Es ist eine Frage des Geschäftsstils, der im Unternehmen gepflegt wird. Die Aufsichtsbehörde kann lediglich auf eine entsprechende Bestätigung hinwirken.

Zu der Annahme einer *Nichtbeachtung* des Widerspruchs führte meist die Tatsache, dass die Betroffenen kurze Zeit nach der Erhebung des Widerspruchs noch Werbesendungen erhielten. Die betroffenen Unternehmen erklärten, dass entweder der Widerspruch zum Zeitpunkt des Abgleichs mit den für die Werbemaßnahme eingesetzten Adressdateien noch nicht vorgelegen hat bzw. eingegeben war oder aber die Aufbereitung der Werbemittel bereits in Auftrag gegeben war und das Heraussuchen des Werbemittels einen wirtschaftlich unverhältnismäßigen Aufwand dargestellt hätte. Die Aufsichtsbehörde war der Auffassung, dass diese

zeitliche Verzögerung von den Betroffenen im Einzelfall hingenommen werden musste, zumal es in keinem Fall eine zeitliche Überschreitung von drei Monaten gegeben hat.

In einem Fall war der Betroffene mit verschiedenen Schreibweisen seines Namens in der Datei gespeichert. Der Sperrvermerk wurde nur zu dem Namen eingegeben, unter dem der Betroffene Widerspruch eingelegt hatte. Mit Hilfe der Aufsichtsbehörde konnte erreicht werden, dass sämtliche seine Person betreffende Datensätze mit einem Sperrvermerk versehen wurden.

Auskunftsanspruch

Um den Widerspruch beim Adresseigner einlegen zu können, muss der Betroffene die Möglichkeit haben, die *Herkunft seiner Adresse* auf dem Werbematerial – also möglichst den Adresseigner – zu erfahren. Ein solcher Auskunftsanspruch ist in § 34 BDSG geregelt. Danach hat jeder Betroffene einen Anspruch darauf zu erfahren, woher seine Anschrift stammt. Dieses Recht besteht aber nur, wenn die Herkunft der Daten auch gespeichert ist. Aus dem *Auskunftsanspruch* des Betroffenen kann keine Verpflichtung der speichernden Stelle zur Speicherung der Adressherkunft abgeleitet werden. Dennoch wirkt die Aufsichtsbehörde bei den Unternehmen darauf hin, die Adressherkunft zu speichern, damit der Auskunftsanspruch und damit die Möglichkeit, Werbewiderspruch einzulegen und auch die sonstigen Rechte nach dem BDSG wahrzunehmen, nicht ins Leere läuft.

Die Adressherkunft lässt sich in der Regel ermitteln, wenn die *Codenummer* auf der Werbesendung bekannt ist. Werden Werbesendungen weggeworfen oder mit entsprechenden Vermerken an die werbende Stelle gesandt, ist im Nachhinein eine Aufklärung über die Adressherkunft meist nicht mehr möglich. Aber auch sonst ist die Ermittlung der speichernden Stelle, von der die Adresse stammt, sehr aufwändig und erfordert häufig die Einschaltung mehrerer Aufsichtsbehörden, weil mehrere Unternehmen aus verschiedenen Bundesländern an der Durchführung der Werbeaktion beteiligt waren. Wenn für Werbemaßnahmen mehrere Adressbestände von verschiedenen Unternehmen angemietet und zu einer Liste zusammengeführt wurden, konnte manchmal nicht mehr festgestellt werden, in welchem Adressbestand die Anschrift des Betroffenen enthalten war. Die Aufsichtsbehörde war der Auffassung, dass das werbende Unternehmen, auch wenn es die Daten der Betroffenen nicht selbst speichert, sondern unterschiedliche Adressbestände über Adressmakler anmietet, dafür sorgen muss, dass die Betroffenen ihren Auskunftsanspruch in angemessener Zeit verwirklichen können. Entweder muss es sich dazu vom Adressmakler eine Liste der verwendeten Codenummern mit den dazugehörigen Herkunftsangaben beschaffen oder den Makler vertraglich verpflichten, Auskunftsansprüche der Betroffenen zu erfüllen. Die Unternehmen wurden aufgefordert, künftig die Herkunft der werblichen Adressdaten nachvollziehbar zu dokumentieren.

Eine wesentlich *größere Transparenz* könnte erreicht werden, wenn die Werbesendungen einen konkreten Hinweis auf die Herkunft der Adresse enthielten. Die Werbewirtschaft kommt diesen Forderungen der Aufsichtsbehörden aber bisher nicht nach. Zum einen wollen die Unternehmen, die die Daten ihrer Kunden oder Interessenten anderen für Werbezwecke überlassen, oftmals nicht, dass die Betroffenen davon erfahren, und zum anderen schreibt das BDSG eine solche Kennzeichnung bisher nicht vor. Künftig dürfte diesem Missstand aber abgeholfen sein, denn das *novellierte BDSG* sieht in § 28 Abs. 4 BDSG eine Regelung vor, wonach der Betroffene bei der Ansprache zum Zwecke der Werbung über die verantwortliche Stelle zu unterrichten ist und wonach der Werbetreibende, soweit ihm die speichernde Stelle nicht selbst bekannt ist, verpflichtet ist sicherzustellen, dass die speichernde Stelle zur Kenntnis genommen werden kann.

Robinson-Liste

Der Weg über den Widerspruch bei jeder speichernden Stelle kann sehr umständlich und Zeit raubend sein. Der Deutsche Direktmarketing-Verband (DDV) hat daher *die Robinson-Liste* eingeführt. Unabhängig von der Möglichkeit, bei jeder speichernden Stelle der Verwendung seiner Daten für Werbezwecke zu widersprechen, kann sich jeder in diese Robinson-Liste eintragen lassen. Die Liste wurde eingerichtet, um den Wunsch von Verbraucherinnen und Verbrauchern, weniger adressierte Werbung zu bekommen, soweit wie möglich zu erfüllen. Bei der

Robinson-Liste handelt es sich um eine freiwillige Einrichtung auf Verbandsebene. Da nur ein Teil der mit Adressen handelnden Unternehmen dem DDV angeschlossen sind, lassen sich mit der Aufnahme in diese Liste Werbesendungen zwar nicht ganz abstellen, aber deren Anzahl verringern. Obwohl die Robinson-Liste nicht nur Verbandsmitgliedern sondern auch Nichtmitgliedern zum Abgleich angeboten wird, scheuen viele Unternehmen den Aufwand und die Kosten für den Abgleich.

Für die Aufnahme in die Robinson-Liste ist ein ausgefüllter Antrag erforderlich. Die Liste wird viermal im Jahr aktualisiert, die Daten bleiben für fünf Jahre gespeichert. Das Formular kann angefordert werden beim:

Deutscher Direktmarketing-Verband e.V.
Robinson-Liste
Postfach 14 01
71243 Ditzingen
Tel.: 0 71 56 / 95 10 10.

Löschung der Daten

Oftmals verlangen die Betroffenen die Löschung ihrer Daten, weil sie mit den Unternehmen keine Geschäftsbeziehungen mehr haben oder haben wollen. Zunächst steht es einer speichernden Stelle grundsätzlich frei, Daten selbst zu löschen. Im Übrigen sind die Voraussetzungen für eine *Löschung* von Daten in § 35 Abs. 2 BDSG geregelt. Die Betroffenen können insbesondere dann nach § 35 Abs. 2 Nr. 3 BDSG einen Löschungsanspruch geltend machen, wenn die Daten für eigene Geschäftszwecke der speichernden Stelle nicht mehr benötigt werden. Anliegen der Betroffenen ist aber in vielen Fällen nicht nur die Löschung ihrer dort gespeicherten Daten, sondern die Unterbindung weiterer persönlich adressierter Werbung von diesen Unternehmen. Dieses Ziel kann mit der Löschung nicht immer ohne Weiteres erreicht werden. Denn sind die Daten bei dem werbenden Unternehmen gelöscht, ist es bei einer Anmietung von Adressen für Werbemaßnahmen nicht auszuschließen, dass der Betroffene erneut beworben wird, da ein Abgleich mit der Werbesperrdatei ins Leere läuft. Die Betroffenen wurden deshalb von der Aufsichtsbehörde dahingehend beraten, keine Löschung zu verlangen, sondern Widerspruch gegen die Nutzung der Daten für Werbezwecke zu erheben.

Eine Löschung ist u. a. nach § 35 Abs. 3 Nr. 1 und 2 BDSG dann unzulässig, wenn die speichernde Stelle zur Aufbewahrung verpflichtet ist oder wenn das schutzwürdige Interesse des Betroffenen die Aufbewahrung gebietet. Anstelle der Löschung tritt dann eine *Sperrung* der Daten.

In einem Fall hat ein Betroffener bei einem Unternehmen die Sperrung seiner Daten bis zur Auskunftserteilung über deren Herkunft verlangt. Das Unternehmen hat seine Daten daraufhin aber gelöscht. Der Betroffene hat dagegen geltend gemacht, dass durch die Löschung nun seinem Auskunftsanspruch auf die Herkunft seiner Adresse nicht mehr nachgekommen werden kann. Da uns das Unternehmen versicherte, weder Adressen für Werbemaßnahmen anzumieten, sondern ausschließlich Daten aus der eigenen Kunden- und Interessentendatei zu verwenden, noch die eigenen Adressen anderen zur Verfügung zu stellen, war gegen die Löschung der Daten nichts einzuwenden. Wir mussten den Betroffenen darüber aufklären, dass die speichernden Stellen nicht zur Speicherung der Daten ausschließlich für Zwecke der Datenschutzkontrolle verpflichtet sind. Liegen für die Unternehmen keine konkreten Anhaltspunkte dafür vor, dass schutzwürdige Belange einzelner Betroffener durch die Löschung der Daten beeinträchtigt sein könnten, können sie jederzeit die Daten löschen. Das schutzwürdige Interesse des Einzelnen erstreckt sich nicht auf die Erfüllung des Auskunftsanspruchs.

7.3 Konsumentenbefragung mittels Fragebogen

Die Nachfrage nach qualifizierten Adressen, mit denen potenzielle Verbraucher möglichst zielgenau beworben werden können, nimmt ständig zu. Konsumentenbefragungen dienen oft der Beschaffung solcher qualifizierter Adressen entweder zu eigenen Werbezwecken oder zum Zwecke der Übermittlung. Je nach den ver-

folgten Werbezwecken werden die unterschiedlichsten Daten aus allen möglichen Lebensbereichen in unterschiedlicher Tiefe erfragt, beispielsweise aus den Lebensbereichen Urlaub, Fahrzeug, Hobbys, Zeitungen und Medien, Haus und Heim, Einkaufen oder Interessengebiete. Erfragt werden aber auch sensible Daten, beispielsweise zu finanziellen, familiären oder gesundheitlichen Verhältnissen. Eine immer wiederkehrende Fallkonstellation war die Konsumentenbefragung für Marketing- und Werbezwecke durch ein Unternehmen, das die Daten zum Zwecke der Übermittlung erhebt, speichert und nutzt. Eine weitere Befragung wurde durch einen Verlag für ausschließlich eigene Marketing- und Werbezwecke durchgeführt. Die entsprechenden Fragebögen waren direkt adressiert, enthielten Fragen nach sensiblen Daten und waren zu unterschreiben. Insbesondere bei den Befragungsaktionen des Unternehmens hatte die Aufsichtsbehörde eine nicht unwesentliche Anzahl von Bürgeranfragen und -eingaben zu bearbeiten. Viele Bürger fragten sich, weshalb gerade sie angeschrieben wurden oder äußerten Zweifel an der datenschutzrechtlichen Zulässigkeit der Fragen. Bei der Befragung durch den Verlag wurde auch bemängelt, dass der ausgefüllte Fragebogen in einem unverschlossenen Umschlag zurückgesandt werden sollte.

Bewertung der Aufsichtsbehörde

Da die Daten nach § 28 Abs. 1 Satz 2 und § 29 Abs. 1 Satz 2 BDSG nach Treu und Glauben und auf rechtmäßige Weise erhoben werden müssen, sind die Befragten klar und verständlich darüber zu *informieren*,

- welches Unternehmen die Befragung durchführt (mit Namen und Anschrift),
- für welche Zwecke die Angaben verwendet werden sollen, beispielsweise, dass die Angaben nicht nur zur anonymen Marktforschung nach statistischen Grundsätzen eingeholt werden, sondern auch zu direkt adressierter Werbung verwendet werden sollen sowie
- im Fall der Erhebung zum Zwecke der Übermittlung, welchen Unternehmen und sonstigen Dritten und zu welchem Zweck die Daten übermittelt werden sollen.

Es darf auch nicht der Eindruck einer amtlichen Befragung erweckt werden. Vielmehr muss klargestellt sein, dass es sich um eine Befragung durch private Firmen handelt und die Teilnahme freiwillig ist.

Sind die Daten nach Treu und Glauben und auf rechtmäßige Weise erhoben, ist im Rahmen der §§ 28 und 29 BDSG grundsätzlich auch deren Speicherung, Verarbeitung, Nutzung und Übermittlung zulässig. Dies gilt jedoch nicht für sensible Daten, da deren personenbezogene Speicherung, Verarbeitung, Nutzung oder Übermittlung grundsätzlich geeignet ist, schutzwürdige Belange der Befragten zu beeinträchtigen. Dies gilt auch, wenn sich aus der Gesamtheit der erhobenen Daten ein Persönlichkeitsprofil erstellen lässt. In diesem Fall ist die *schriftliche Einwilligung* der Befragten nach § 4 Abs. 2 BDSG einzuholen. Die Einwilligungserklärung ist im äußeren Erscheinungsbild des Fragebogens herauszuheben und so abzufassen, dass die Befragten erkennen können, worin sie einwilligen (so genannte *informierte Einwilligung*). Werden vom Befragten sensible Daten Dritter abgefragt, so ist auch deren Einwilligung erforderlich.

Ergebnis der Überprüfung

Mit dem *Unternehmen*, das *wiederkehrende Befragungen* durchführt, konnte nach intensiven Verhandlungen eine Einigung über die *datenschutzgerechte Ausgestaltung der Fragebögen* erzielt werden:

Aus dem Fragebogen geht nun deutlich das befragende Unternehmen hervor. Das Anschreiben enthält konkrete Hinweise darauf, dass die Angaben nicht nur anonymisiert für Marktanalysen, sondern darüber hinaus auch personenbezogen für die Zusendung direkt adressierter Werbung verwendet werden sollen. Im Anschreiben wird darauf hingewiesen, dass die personenbezogenen Verbraucherdaten Herstellern und dem Handel für die Produktentwicklung und zu Marketing- und Werbezwecken zur Verfügung gestellt werden, dass der Befragte für seinen Bedarf Informationen und Angebote, die ihn auch interessieren, erhalten wird, sowie aus den Ausführungen unter der Nachschrift, in der die Zusendung von Warenmuster und Gutscheinen zum kostenlosen Test in Aussicht gestellt wird. Im Anschreiben ist auch klargestellt, dass es sich um die Befragung einer privaten Firma für wirtschaftliche Zwecke handelt und keine Pflicht zur Beantwortung besteht. In der ent-

sprechend hervorgehobenen Einwilligungserklärung, die wegen der Erhebung sensibler Daten erforderlich ist, wird nochmals darauf hingewiesen, dass die Befragungsergebnisse ausschließlich für Marketing- und Werbezwecke personenbezogen erhoben, gespeichert, genutzt und übermittelt werden. Die Einwilligungserklärung ist auch zur Unterschrift für Ehegatten/Partner oder Kinder vorgesehen. Soweit deren Unterschriften fehlen, werden die Daten nur anonymisiert verarbeitet.

Ob der Befragte in Kenntnis des Erhebungszwecks und der weiteren beabsichtigten Verwendung der Daten an einer solchen Befragung teilnehmen und bewusst persönliche Angaben für Werbezwecke offenbaren und bedingt durch die Teilnahme die Zunahme direkt adressierter Werbesendungen in Kauf nehmen will, hat er selbst in der Hand. Auch das für die Teilnahme in Aussicht gestellte Geschenkpaket mit Warenproben ändert an der Freiwilligkeit der Angaben nichts und ist nach Auffassung der Aufsichtsbehörde nicht wettbewerbswidrig, solange der Wert der Geschenke einen in der Werbung üblichen Rahmen nicht übersteigt. Die Adressen der Befragten stammen aus dem Adresshandel, was datenschutzrechtlich zulässig ist. Die Beschwerdeführer wurden auf die Rechtslage hingewiesen.

Beanstandung

Die *Kundenbefragung des Verlags* entsprach nicht in allen Punkten den datenschutzrechtlichen Anforderungen. Im Anschreiben wurden die Kunden zwar allgemein auf den Zweck der Befragung und die Freiwilligkeit der Teilnahme hingewiesen, aus dem Fragebogen und der Einwilligungserklärung, die wegen der Erhebung sensibler Daten erforderlich war, war jedoch nicht eindeutig zu erkennen, dass die Daten personenbezogen gespeichert und für direkt adressierte Werbung verwendet werden sollten. Dies konnte allenfalls aus der persönlich adressierten Zusendung des Fragebogens und aus einer Formulierung im Fragebogen „... Denn nur wenn wir wissen, was für Sie wichtig und interessant ist, können wir das Richtige anbieten...“ geschlossen werden. Dies war aus Sicht der Aufsichtsbehörde für eine informierte Einwilligung nicht ausreichend und wurde beanstandet. Zusätzlich hat die Aufsichtsbehörde angeregt, die Rücksendung ausgefüllter Fragebögen nicht in einem unverschlossenen Umschlag vorzusehen. Das BDSG ist hierfür allerdings nicht anwendbar. Der Verlag wird die Auffassung der Aufsichtsbehörde bei künftigen Kundenbefragungen beachten.

7.4 Verwendung von Kfz-Daten für Werbezwecke

Die Aufsichtsbehörde wurde darüber unterrichtet, dass einem Unternehmen von einer *Direktmarketingfirma* Angebote von *Firmenadressen mit Fuhrparkinformationen* unterbreitet wurden. Die benötigten Kfz-Daten wurden vom Kraftfahrtbundesamt (KBA) anonymisiert geliefert. Hierzu hat das Direktmarketingunternehmen einen Vertrag mit dem KBA geschlossen. Die Frage war, ob KBA-Daten entgegen der vertraglichen Vereinbarung mit dem KBA so mit Adressdaten verknüpft werden können, dass eine Fahrzeug-Halteridentifizierung (Reanonymisierung) möglich ist.

Ergebnis der Überprüfung

Die datenschutzrechtliche Prüfung ergab, dass dem Angebot der Direktmarketingfirma nur zum Teil Echtdaten zu Grunde lagen. Diese stammten aus firmeninternen Businesserhebungen, insbesondere telefonischen Befragungen bei den Firmen. Der größte Teil der Daten wurde jedoch auf Grund von Prognoseverfahren nach Brancheninformationen den Firmenadressen zugeordnet. Die vom KBA gelieferten Daten wurden in diese mathematisch-statistischen Prognoseverfahren mit einbezogen. Die Aufsichtsbehörde sah deshalb keine Anhaltspunkte, die für eine Reanonymisierungsmöglichkeit der Fahrzeughalter sprachen. Aus datenschutzrechtlicher Sicht ist die Verwendung der vom KBA an die Direktmarketingfirma gelieferten anonymisierten Halterdaten zur prognostischen Anreicherung von Firmenadressen nicht zu beanstanden, wenn auf den Wahrscheinlichkeitscharakter der Informationen hingewiesen wird. Da dies bisher aus dem Adressangebot nicht erkennbar war und somit zu Missverständnissen führen konnte, wurde auf Anregung der Aufsichtsbehörde von der Direktmarketingfirma veranlasst, dass das Angebot von Firmenadressen mit Fuhrparkinformationen künftig dahingehend modifiziert wird, dass auf den *prognostischen Charakter* der Daten hingewiesen wird.

8. Arbeitnehmer-Datenschutz

Die Arbeit der Aufsichtsbehörde im Bereich des Arbeitnehmer-Datenschutzes war geprägt von der Bearbeitung einzelfallbezogener Beschwerden und Anfragen.

Dabei zeigten sich folgende Schwerpunkte: Angaben über Arbeitnehmer im Internet, Bekanntgabe von Abwesenheitszeiten von Arbeitnehmern am schwarzen Brett, Abrechnung von Mobiltelefon-Kosten bei erlaubter privater Nutzung und Behandlung von Bewerbungen über eine Personalagentur.

8.1 Angaben über Arbeitnehmer im Internet

Es ist inzwischen weit verbreitet, dass Unternehmen der Privatwirtschaft bei ihren Internet-Auftritten auch Angaben über Arbeitnehmer einstellen und damit veröffentlichen. Dabei wird von den Unternehmen insbesondere der Zweck verfolgt, den potenziellen Kunden, die sich über das Internet über ein Unternehmen informieren oder Kontakte zu diesem herstellen wollen, kompetente Ansprechpartner zu benennen.

Bewertung der Aufsichtsbehörde

Um diesen Zweck zu erreichen, muss das jeweilige Unternehmen die Personaldaten der Arbeitnehmer nutzen. Die Zulässigkeit der Nutzung von Personaldaten durch das Unternehmen bestimmt sich dabei zum einen nach arbeitsrechtlichen Gesichtspunkten, zum anderen nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG.

Arbeitsrechtliche Voraussetzung für die Zulässigkeit der *Veröffentlichung von Personaldaten im Internet* – wobei für Veröffentlichungen in anderen konventionellen Medien wie z. B. Faltblätter oder Broschüren dasselbe gilt – ist in jedem Fall, dass die Nutzung der Personaldaten im Zusammenhang mit dem Arbeitsverhältnis erfolgt. Eine Bekanntgabe von Personaldaten an Dritte kann aber auch schon im Arbeitsvertrag direkt geregelt sein. Insoweit liegt dann im Einzelfall bereits eine entsprechende Einwilligung des Arbeitnehmers vor.

Im Übrigen richtet sich die Zulässigkeit der Bekanntgabe von Personaldaten im Internet nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG, wonach die Nutzung von Daten zur Erfüllung eigener Geschäftszwecke im Rahmen der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen zulässig ist. Danach kann die Geschäftsleitung eines Unternehmens im Rahmen ihres aus dem Arbeitsvertrag abzuleitenden Direktionsrechts Daten über Arbeitnehmer wie z. B. Name, Funktion, Spezialkenntnisse, telefonische und elektronische Erreichbarkeit, die spezifisch im Zusammenhang mit dem Arbeitsverhältnis stehen, im Internet bekannt geben. Dies gilt insbesondere für Arbeitnehmer in Funktionen mit Außenwirkung und unmittelbarem Kundenkontakt.

Eine darüber hinausgehende Bekanntgabe von Daten wie z. B. Privatanschrift, Anzahl der Kinder, Familienstand, Geburtsdatum ist von § 28 Abs. 1 Satz 1 Nr. 1 BDSG nicht gedeckt, da diese Daten nicht mehr in Zusammenhang mit der Funktion des jeweiligen Arbeitnehmers stehen. Sie sind deshalb auch nicht zur Kundeninformation erforderlich. Daher besteht auch kein berechtigtes Interesse i. S. v. § 28 Abs. 1 Satz 1 Nr. 2 BDSG des Arbeitgebers, zu dessen Wahrung eine Bekanntgabe dieser Arbeitnehmerdaten im Internet erforderlich wäre. Vielmehr überwiegen die schutzwürdigen Interessen des Arbeitnehmers, nämlich der Schutz seiner Privatsphäre. Eine Bekanntgabe solcher Daten durch den Arbeitgeber ist nur mit ausdrücklicher Einwilligung des Betroffenen zulässig. Dies gilt nach Auffassung der Aufsichtsbehörde auch für die Veröffentlichung eines Bildes des jeweils Betroffenen.

Aus Sicht der Aufsichtsbehörde ist es wünschenswert, wenn die Unternehmen die betroffenen Arbeitnehmer darüber unterrichten, dass eine Veröffentlichung von Personaldaten im Internet erfolgt. Dies ist jedoch rechtlich nicht vorgeschrieben.

Dieses Thema wurde auch in den HIM Nr. 39 vom 25. Januar 2001 behandelt, die im Internet unter „www.im.bwl.de“, veröffentlicht sind.

8.2 Bekanntgabe von Abwesenheitszeiten von Arbeitnehmern am schwarzen Brett

Ein Betriebsrat eines Unternehmens beschwerte sich darüber, dass in diesem Unternehmen an so genannten Infotafeln *betriebsintern die An- und Abwesenheit der Arbeitnehmer veröffentlicht* wird. Dabei wurde bei den Abwesenheitsgründen unterschieden nach Urlaub, Krankheit und Fehlzeiten.

Bewertung der Aufsichtsbehörde

Die Vorschriften des BDSG gelten auch in solchen Fällen, soweit derartige personenbezogene Daten über Arbeitnehmer in oder aus Dateien verarbeitet oder genutzt werden. Als Rechtsgrundlage für diese Nutzung und Verarbeitung personenbezogener Daten aus dem Arbeitsverhältnis kommt § 28 Abs. 1 Satz 1 Nr. 1 BDSG deshalb nicht in Betracht, weil eine betriebsinterne Veröffentlichung personenbezogener Daten wie Krankheits- oder Urlaubsdaten am Schwarzen Brett über die Zweckbestimmung des einzelnen Arbeitsverhältnisses hinausgeht. Nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist eine Nutzung personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Ergebnis der Überprüfung

Die Prüfung ergab, dass vorliegend der Arbeitgeber ein berechtigtes Interesse daran hatte, aus *organisatorischen Gründen* betriebsintern darüber zu informieren, welche Arbeitnehmer an welchen Tagen nicht anwesend sind. Anders liegt es jedoch hinsichtlich der Angabe der *Abwesenheitsgründe* wie Urlaub oder Krankheit. Für die bloße Information über die Abwesenheit als solche ist der Grund der Abwesenheit irrelevant. Soweit der Arbeitgeber ein darüber hinausgehendes Interesse verfolgt, wie z. B. durch eine solche Veröffentlichung die Arbeitsbereitschaft der Beschäftigten zu erhöhen, stehen dem die schutzwürdigen Interessen der Arbeitnehmer auf Wahrung ihrer Privatsphäre entgegen.

So sind im Arbeitsverhältnis personenbezogene Daten auch nach arbeitsrechtlichen Grundsätzen vertraulich zu behandeln. Dies bedeutet, dass Arbeitnehmerdaten, die nicht aus organisatorischen Gründen betriebsintern allgemein bekannt sein müssen, auch nicht ohne Weiteres betriebsintern veröffentlicht werden dürfen. So verhält es sich aber gerade bei Angaben über die Gründe einer Abwesenheit von einzelnen Beschäftigten wie Urlaub oder Krankheit.

Somit darf ein Arbeitgeber, wenn er seinen Arbeitnehmern den *Krankenstand* vor Augen halten will, dazu allenfalls *zusammengefasste Angaben* machen, die sich nicht auf einzelne Arbeitnehmer beziehen lassen. Wenn ein Arbeitgeber auf die Beschäftigten einwirken will, muss dies im Rahmen des jeweiligen Arbeitsverhältnisses direkt gegenüber dem einzelnen Arbeitnehmer geschehen (etwa in Personalgesprächen). Eine Anprangerung durch Aushang am schwarzen Brett oder durch Verteilen von Listen an die Arbeitnehmer stellt eine unverhältnismäßige, das Persönlichkeitsrecht der Arbeitnehmer verletzende Maßnahme dar.

Etwas Anderes kann nur gelten, wenn eine ausdrückliche Einwilligung der Betroffenen hierzu vorliegt. Dabei ist jedoch die Problematik der Freiwilligkeit einer solchen Einwilligung im Arbeitsverhältnis kritisch zu prüfen.

Im konkreten Fall wurde, nachdem die Aufsichtsbehörde ihre Rechtsauffassung schriftlich mitgeteilt hatte, im unmittelbaren Anschluss an das Schreiben in allen Werken des betroffenen Unternehmens dafür Sorge getragen, dass künftig den oben genannten datenschutzrechtlichen Erfordernissen entsprochen wird.

8.3 Abrechnung von Mobiltelefon-Kosten bei erlaubter Privatnutzung

In einer Beschwerde wurde es vom Betroffenen als datenschutzrechtlich unzulässig angesehen, dass sein Arbeitgeber, der ihm die Nutzung eines geschäftlichen Zwecken dienenden Mobiltelefons auch für private Zwecke einräumte, seinen Namen und seine Anschrift zu Abrechnungszwecken ohne seine vorherige Einwilligung an das Mobilfunkunternehmen weitergeleitet hat.

Ergebnis der Überprüfung

Nach Prüfung durch die Aufsichtsbehörde ergab sich jedoch im Hinblick auf § 28 Abs. 1 BDSG eine andere Einschätzung. Zwar scheidet der Fall von § 28 Abs. 1 Satz 1 Nr. 1 BDSG aus, wonach eine Datenübermittlung zur Erfüllung eigener Geschäftszwecke im Rahmen der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen zulässig ist. Denn dass der Arbeitgeber dem Arbeitnehmer die Möglichkeit einräumt, von einem durch den Arbeitgeber zur Verfügung gestellten Mobiltelefon privat zu telefonieren, ist zur Erbringung der Arbeitsleistung durch den Arbeitnehmer gerade nicht erforderlich. Es handelt sich dabei vielmehr um allgemeine organisatorische Regelungen der Arbeitsbedingungen.

Zulässig war jedoch die *Übermittlung von Namen und Anschrift des Arbeitnehmers* durch den Arbeitgeber *an den Mobilfunkbetreiber* nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Danach ist eine Datenübermittlung zulässig, soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Übermittlung überwiegt. Grundsätzlich besteht ein berechtigtes Interesse des Arbeitgebers daran, dass er *für Abrechnungszwecke* über die geschäftlich geführten Gespräche Kenntnis erlangt. Im vorgelegten Fall weisen die Rechnungen jedoch sämtliche angerufenen Nummern aus, und nur der Arbeitnehmer kann angeben, welche Gespräche geschäftlicher und welche privater Natur waren. Wenn also der Arbeitgeber im Interesse des Arbeitnehmers die private Nutzung des Mobiltelefons zulässt, bleibt dem Arbeitgeber nichts Anderes übrig, als Namen und Anschrift des Arbeitnehmers für die Übersendung der Rechnung der Abrechnungsstelle des Mobilfunkbetreibers an den Arbeitnehmer zu übermitteln. Nur so kann der Arbeitgeber sicherstellen, dass er nicht ohne berechtigtes Interesse hinsichtlich der privat geführten Gespräche in die Rechte des Arbeitnehmers eingreift. Der Arbeitnehmer kann dann die privat geführten Gespräche streichen und erhält die Kosten für die anderen, geschäftlich geführten Gespräche vom Arbeitgeber erstattet. Bei dieser Vorgehensweise waren für die Aufsichtsbehörde keine überwiegenden schutzwürdigen Interessen des Arbeitnehmers erkennbar, denn die Offenlegung von Namen und Anschrift des Betroffenen gegenüber dem Mobilfunkbetreiber ist als weitaus weniger belastend einzustufen als die Offenlegung der Kommunikationsbeziehungen der Arbeitnehmer gegenüber dem Arbeitgeber. Im Übrigen wurde der Betroffene rechtzeitig über das vorgesehene Verfahren informiert, sodass es ihm unbenommen geblieben wäre, auf die zu seinen Gunsten eingeräumte private Nutzung des Mobiltelefons zu verzichten.

8.4 Bewerbung über eine Personalagentur

Häufig werden von Unternehmen, die neue Mitarbeiter suchen, Personalagenturen mit der Suche, der Stellenausschreibung und der Abwicklung der Bewerbungen beauftragt. Im Zuge der Bewerbungen werden von den Bewerbern die erforderlichen Unterlagen eingereicht, die naturgemäß eine Vielzahl von teilweise sehr sensiblen personenbezogenen Daten enthalten.

Verschiedentlich wurde in solchen Fällen von Bewerbern gegenüber der Aufsichtsbehörde vorgetragen, dass die *bei der Personalagentur eingereichten Bewerbungsunterlagen* ohne vorherige Zustimmung des Bewerbers an das einen neuen Mitarbeiter suchende Unternehmen vollständig weitergegeben worden sind. Problematisch kann dies für die Bewerber schon deshalb sein, weil diese in der Regel nicht wissen, um welches dritte Unternehmen es sich dabei handelt.

Bewertung der Aufsichtsbehörde

Unabhängig davon, ob hier auch arbeitsrechtliche Regelungen berührt sind, ist datenschutzrechtlich danach zu differenzieren, ob lediglich die eingereichten Unterlagen weitergegeben wurden oder ob zuvor die Daten der Bewerber von der Personalagentur in einer Datei gespeichert oder verarbeitet wurden.

Da die Bestimmungen des BDSG bei nichtöffentlichen Stellen nur Anwendung finden, soweit diese die Daten in oder aus Dateien verarbeiten oder nutzen, fällt der Fall der bloßen Weitergabe eingereichter Unterlagen an das dritte Unternehmen nicht in dessen Anwendungsbereich.

Anwendung findet das BDSG dann, wenn die Personalagentur die Bewerberdaten in einer Datei speichert und daraus die Daten an den Auftraggeber übermittelt. Die Speicherung der Daten bei der Personalagentur ist dabei nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG zur Erfüllung eigener Geschäftszwecke im Rahmen eines vertragsähnlichen Vertrauensverhältnisses auch ohne vorherige Einwilligung zulässig.

Die Übermittlung der Daten durch die Personalagentur an den Auftraggeber ist ebenfalls ohne vorherige Einwilligung des Bewerbers nach § 28 Abs. 1 Satz 1 Nr. 2 bzw. § 28 Abs. 2 Satz 1 Nr. 1 a BDSG zulässig. Das danach erforderliche berechtigte Interesse der Personalagentur liegt in der Erfüllung ihres Auftrags gegenüber dem Auftraggeber. Das berechtigte Interesse des Auftraggebers besteht darin, auf diese Weise die Stellenbewerber kennen lernen und eventuell eine Vorauswahl treffen zu können. Bei der Personalagentur besteht auch kein Grund zur Annahme, dass ein Bewerber ein schutzwürdiges Interesse am Ausschluss der Übermittlung seiner Daten an den Auftraggeber hat. Schließlich bezieht sich die Bewerbung gerade auf eine Stelle beim Auftraggeber.

Erst wenn die Daten beim Auftraggeber gespeichert werden würden, wäre dieser nach § 33 BDSG verpflichtet, den Bewerber über diese Speicherung zu unterrichten. Dass der Auftraggeber solange dem Bewerber gegenüber anonym bleibt, ist datenschutzrechtlich nicht zu beanstanden, da es sich dabei um Geschäftsgeheimnisse handelt, zu deren Wahrung die Personalagentur berechtigt ist.

Diese Einschätzung gilt entsprechend für den Fall, dass die Personalagentur ohne einen konkreten Auftrag zunächst einmal Bewerber sucht, um diese dann später bei entsprechender Nachfrage an ein drittes Unternehmen zu vermitteln.

9. Gesundheitswesen

Aus Krankenhäusern ist die elektronische Datenverarbeitung nicht mehr wegzudenken. In Arztpraxen werden die Patientenunterlagen vielfach noch in Papierform als Karteikarten geführt und unterliegen in aller Regel damit ebenfalls als nicht automatisierte Datei dem BDSG. Bei Abrechnungen werden zumeist sei es bei Kassenpatienten gegenüber der Kasse oder bei Privatpatienten Patientendaten durch Erstellung einer Rechung auf dem Praxiscomputer oder durch Weitergabe der Daten an eine gewerbliche Abrechnungsstelle automatisiert verarbeitet. Unter dem im Gesundheitswesen herrschenden Kostendruck ist die Ärzteschaft zudem bestrebt, Kosten durch eine elektronische Vernetzung der Arztpraxen zu senken, ohne dabei das Niveau der ärztlichen Leistungen zu gefährden. Durch die Vernetzung können z. B. Mehrfachuntersuchungen entfallen.

Für den Datenschutz im Gesundheitsbereich ist nicht nur das BDSG einschlägig. Datenschutzrechtliche Regelungen für die Krankenhäuser in öffentlicher und privater Trägerschaft befinden sich auch im LKHG.

Die Aufsichtsbehörde ist zuständig für den *Datenschutz in Arztpraxen*, privaten *Krankenhäusern* und Krankenhäusern öffentlicher Träger, die in privatwirtschaftlicher Rechtsform betrieben werden. So sind in den vergangenen Jahren die Krankenanstalten mehrerer Landkreise in gemeinnützige GmbH‘s überführt worden. Da durch die freie Krankenhauswahl der Patienten zwischen den Krankenanstalten eine Wettbewerbssituation besteht, unterliegen sie nach § 2 Abs. 4 LDSG den Vorschriften des Datenschutzes im nichtöffentlichen Bereich und somit der Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich.

Strafrechtlichen Schutz genießen Patientendaten durch § 203 des Strafgesetzbuches (StGB), der die unbefugte Offenbarung eines zum persönlichen Lebensbereich gehörenden Geheimnisses durch einen Angehörigen eines Heilberufs unter Strafe stellt. Diese Vorschrift ist unbeschadet der datenschutzrechtlichen Vorschriften zu beachten, d. h. auch bei einer datenschutzrechtlich zulässigen Datenübermittlung an einen Dritten kann gegen § 203 StGB verstoßen werden.

9.1 Elektronische Vernetzung der Ärzte

Ein Schwerpunktthema war die elektronische Vernetzung der niedergelassenen Ärzte. Der Aufsichtsbehörde lag das Projekt eines elektronischen Ärztenetzwerks zur Beurteilung vor. Im Rahmen dieses Projekts ist beabsichtigt, dass Ärzte ihren *patientenbezogenen Schriftverkehr* – etwa Facharztüberweisungen, Befundberichte, Laborergebnisse aus der Praxissoftware heraus mit *E-Mail* versenden. In einem späteren Abschnitt soll den Krankenhäusern und den medizinischen Hilfsberufen der Zugang zum Netzwerk eröffnet werden.

Ursprünglich war das Projekt zweistufig angelegt. Als zweite Stufe war angedacht, eine zentrale Befunddatenbank einzurichten, in die die Ärzte einen „Befundextrakt“ eines jeden Patienten einstellen, aus dem ein nachbehandelnder Arzt oder ein Notfallarzt Grundinformationen über den Patienten entnehmen kann. Von dieser Planung wurde jedoch, auch wegen erheblicher datenschutzrechtlicher Anforderungen, zwischenzeitlich Abstand genommen.

Für die Durchführung der Kommunikation über das Netz ist beabsichtigt, dass alle Projektteilnehmer bei *einem Zugangsdiensteanbieter* aus dem medizinischen Bereich angeschlossen werden. Ein E-Mailverkehr über einen anderen Zugangsdiensteanbieter und damit über das Internet wird nicht akzeptiert. Die E-Mails sollen verschlüsselt und signaturgesetzkonform signiert werden. Die elektronische Signatur wird über die sog. HCP-Karte des Arztes erfolgen. Die E-Mails werden aus der Praxissoftware heraus versandt. Diese Software wird so konfiguriert, dass ein Versenden unverschlüsselter Mails nicht möglich ist.

Bewertung der Aufsichtsbehörde

Die Aufsichtsbehörde hat die Planung der Vernetzung grundsätzlich positiv beurteilt. Da sich alle „Netzärzte“ beim selben Zugangsdiensteanbieter anschließen müssen, verlassen die E-Mails bei der Arzt-zu-Arzt Kommunikation den geschützten Bereich des Mailservers nicht und sind daher nicht dem Gefährdungspotenzial des Internets ausgesetzt. Da aber über den Zugangsdiensteanbieter zu-

gleich auch der Zugang zum Internet möglich ist, durch den unbemerkt Viren und schädigende Programme, die Patientendaten ausspähen oder verändern, auf den Arztrechner gelangen könnten, forderte die Aufsichtsbehörde die Entwicklung eines Datenschutz- und Sicherheitskonzepts, das den Vorschriften über den technisch-organisatorischen Datenschutz der Anlage zu §9 BDSG entspricht. Dieses Konzept muss insbesondere Regelungen zu den folgenden Punkten treffen:

– Von einem Rechner, auf dem sich Patientendaten befinden, darf nur dann ein Zugang zum Internet eröffnet werden, wenn die Patientendaten zumindest mit einem, dem jeweiligen Stand der Technik entsprechenden, aktuellen Firewall und Virenschutz vor Einwirkungen aus dem Internet geschützt sind (Ziff. 2 und 3 der Anlage zu § 9 BDSG).

– Die Problematik von ActiveX und Java, d. h. dass diese Programme auf dem PC unkontrolliert aktiv werden, muss gelöst werden; der sicherste Weg ist das Deaktivieren beider Komponenten im Browser (Ziff. 3 der Anlage zu § 9 BDSG).

– Es muss ausgeschlossen werden, dass auf dem Praxissystem ein weiterer Internetzugang eingerichtet wird und damit die Sicherungen umgangen werden (Ziff. 5 der Anlage zu § 9 BDSG).

Das Projekt befindet sich derzeit noch in der Planungsphase. Die Aufsichtsbehörde wird das weitere Vorhaben kritisch begleiten.

9.2 Weitergabe von Patientendaten

Ein Patient einer fachärztlichen Gemeinschaftspraxis wandte sich an die Aufsichtsbehörde, weil er von einer ambulanten Therapieeinrichtung, zu der er noch nie Kontakt hatte, Informationsmaterial erhalten hatte, das genau auf seine Erkrankung zugeschnitten war. Er vermutete, dass von der Facharztpraxis Informationen über seinen Gesundheitszustand an die Therapieeinrichtung gelangt waren.

Die Überprüfung durch die Aufsichtsbehörde ergab, dass ein Arzt der Gemeinschaftspraxis Daten von Patienten, bei denen er eine Therapie für sinnvoll hielt, an die gemeinnützige Therapieeinrichtung, deren Vorstand er angehört, übermittelt hatte, damit der Patient von dort individuell informiert werden konnte. Bei dem Arzt handelte es sich nicht um den behandelnden Arzt des Beschwerdeführers.

Ergebnis der Überprüfung, ausgesprochene Beanstandung

Die Tatsache, Patient einer Arztpraxis zu sein, ist ein personenbezogenes Datum i. S. v. § 3 Abs. 1 BDSG. Die Patientendaten in der Gemeinschaftspraxis wurden in einer DV-Anlage verarbeitet. Damit war das BDSG anwendbar. Ein Arzt der Gemeinschaftspraxis hat nach der Rechtsprechung des BGH grundsätzlich das Zugriffsrecht auf alle in der Praxis-DV gespeicherten Patientenakten (Urteil vom 29. Juni 1999, NJW 1999, 2731).

Die *Weitergabe der Daten* von der Praxis an das Therapiezentrum ist eine Datenübermittlung nach § 3 Abs. 5 Nr. 3 BDSG. Zwar mag ein berechtigtes Interesse des Arztes und des Therapiezentrums an der Übermittlung bestanden haben. Da es sich bei Gesundheitsdaten jedoch um besonders sensible Daten handelt, die zudem dem besonderen gesetzlichen Schutz des § 203 StGB unterliegen, bestand Grund zu der Annahme, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Übermittlung überwiegt. Die Übermittlung war somit nach § 28 Abs. 1 Nr. 2 und Abs. 2 Nr. 1 a BDSG unzulässig. Dass die Information des Patienten eventuell in dessen gesundheitlichem Interesse und deshalb medizinisch begründet war, kann datenschutzrechtlich zu keinem anderen Ergebnis führen. Zudem fehlte es auch an der erforderlichen Schweigepflichtentbindungserklärung. Ausschlaggebend ist, dass der *Patient selbst darüber entscheiden kann, ob seine Gesundheitsdaten einem Dritten offenbart* werden.

Die Weitergabe der Patientendaten wurde von der Aufsichtsbehörde beanstandet. Der Arzt, der bei der Information des Therapiezentrums von einer Handlung im Interesse des Patienten ausgegangen war, hat zugesagt, künftig die Übermittlung von Patientendaten ohne deren Einwilligung zu unterlassen.

9.3 Bonitätsprüfung vor ärztlicher Behandlung

Bei umfangreichen ärztlichen, insbesondere zahnärztlichen Behandlungen – z. B. unter Beteiligung von Zahntechnikern – können *Vorleistungen* des behandelnden Arztes erforderlich werden, die für ihn wegen des hohen Eigenanteils des Patienten mit einem finanziellen Risiko verbunden sind. Der vorleistende Arzt kann daher ein Interesse haben, sich der *Bonität* des von ihm zu behandelnden Patienten durch eine Anfrage bei einer Kreditschutzorganisation oder einer Auskunftei zu versichern.

Bewertung der Aufsichtsbehörde

Die Bonitätsanfrage bei einer Auskunftei muss personenbezogene Daten des Patienten enthalten, die ihn eindeutig identifizieren lassen. Mit der Anfrage wird deshalb zwangsläufig die Tatsache offenbart, dass sich der Patient in ärztlicher Behandlung befindet. Die Anfrage des behandelnden Arztes schließt die Angabe ein, bei welchem Arzt die Behandlung stattfindet. Nach der *Rechtsprechung* ist die Mitteilung an einen Dritten, dass sich eine Person in ärztlicher Behandlung befindet, die Mitteilung eines fremden Geheimnisses im Sinne von § 203 StGB (Urteil des OLG Düsseldorf vom 20. August 1996 – 20 U 139/95). Die Zulässigkeit dieser Mitteilung und damit die Übermittlung personenbezogener Daten des Patienten bedarf nach einhelliger Auffassung der Aufsichtsbehörden im Düsseldorfer Kreis der *Einwilligung* des Patienten. Nur dann ist sie „befugt“ im Sinne des § 203 StGB.

Rechnet der Arzt bzw. Zahnarzt mit dem Patienten (bzw. bei minderjährigen Patienten mit deren Erziehungsberechtigten) ab, wird es zweckmäßig sein, sofern nicht die Einwilligung angesichts einer kostenintensiven Behandlung im Einzelfall eingeholt wird, eine *Einwilligungserklärung des Patienten* in eine denkbare Bonitätsanfrage in den Patientenerhebungsbogen aufzunehmen. Die Erklärung könnte – bezogen auf Zahnärzte – folgenden Wortlaut haben:

„Ich bin damit einverstanden, dass bei umfangreichen zahnärztlichen oder zahntechnischen Leistungen, für die mein(e) Zahnarzt/Zahnärztin gegenüber dem Zahntechniker in finanzielle Vorleistungen treten muss, ggf. eine Bonitätsanfrage bei einem Kreditschutzunternehmen oder einer Auskunftei eingeholt wird.“

Die Aufsichtsbehörden im Düsseldorfer Kreis haben der Rechtsauffassung der Aufsichtsbehörde *zugestimmt*. Sie wird von der Bundesärztekammer und der Bundeszahnärztekammer mitgetragen und wurde von den beiden Organisationen den Ärzten mitgeteilt.

9.4 Verarbeitung und Archivierung von Patientendaten außerhalb des Krankenhauses

Ein Krankenhaus beabsichtigte, Patientenakten aus seinem Archiv aus Platz- und Kostengründen an einen gewerblichen Archivierungsbetrieb in einem anderen Bundesland zur Einlagerung, Überwachung der 30-jährigen Aufbewahrungsfrist und anschließender Vernichtung abzugeben.

Ergebnis der Überprüfung, Beanstandung

Nach dem Grundsatz des § 48 Abs. 1 LKHG sind *Patientendaten im Krankenhaus* selbst oder im Auftrag des Krankenhauses durch ein anderes Krankenhaus zu verarbeiten. Die Ausnahmeregelung des § 48 Abs. 2 LKHG bezieht sich nur auf die automatisierte Verarbeitung in externen Rechenzentren. Die Patientenunterlagen sollten in dem fremden Archiv eingelagert (Datenspeicherung) und nach Ablauf der Aufbewahrungszeit vernichtet (Datenlöschung) werden. Die Übertragung dieser Verarbeitungsvorgänge an einen Dritten ist nach § 48 LKHG unzulässig. Das Vorhaben wurde daher von der Aufsichtsbehörde beanstandet.

Die externe Verarbeitung von Patientendaten beinhaltet noch eine weitergehende Problematik. Patientendaten genießen im Krankenhaus einen strafprozessualen Beschlagnahmeschutz. Dieser Schutz gilt jedoch nicht, wenn sich die Daten im Gewahrsam eines Dritten befinden.

Datenschutzgerechte Lösung

Da das Krankenhaus die ausgelagerten Akten wegen Baumaßnahmen nicht mehr bei sich aufnehmen konnte, wurde eine Regelung getroffen, wonach das Kranken-

haus bei dem Archivierungsdienstleister eigene, abgeschlossene Räume anmietet, darin mit eigenen Mitarbeitern die Akten archiviert und nach Zeitablauf dort selbst vernichtet. Dadurch wurde eine *Krankenhausfiliale* der Krankenhausverwaltung geschaffen, in der die Patientendaten weiterhin intern verarbeitet werden und auch Beschlagnahmeschutz genießen.

Grundsätzlich ist anzumerken, dass § 48 LKHG auch die *Verarbeitung* von Patientendaten *außerhalb des Krankenhauses* durch externe Schreibbüros sowie externe Firmen zur Mikroverfilmung und der Vernichtung von Patientenakten *nicht ermöglicht*. In diesen Fällen ist Zulässigkeitsvoraussetzung vielmehr die ausdrückliche und schriftliche Einwilligung des betroffenen Patienten im Einzelfall (§ 50 LKHG).

9.5 Schutz der Patientendaten in der Apotheke

Ein Bürger beschwerte sich bei der Aufsichtsbehörde, dass er, nach dem Kauf von Diabetesmedikamenten in einer Apotheke von dieser Rundschreiben mit Diabetesinformationen erhielt. Die Aufsichtsbehörde überprüfte den Vorgang und stellte fest, dass die Apotheke die Adressdaten aller Kunden mit Diabetesverordnungen speicherte, um ihnen entsprechende Informationen zu senden. Die Apotheke war von Pharmaherstellern für die Betreuung von Diabetikern besonders zertifiziert.

Ergebnis der Überprüfung, Beanstandung

Die Speicherung bzw. Nutzung dieser *Kundenadressen* zu Informations- beziehungsweise zu *Werbezwecken* wurde beanstandet. Die Speicherung einer Kundenadresse mit dem Merkmal „Diabetiker“ ist ein personenbezogenes Datum. Die Apotheke erhält das Rezept zur Abgabe des verordneten Medikaments, bei Kassenpatienten zusätzlich zur Abrechnung mit der Kasse. Die Apotheke hat bei einem verordnungspflichtigen Medikament lediglich zu prüfen, ob eine entsprechende Verordnung vorliegt, und die Abgabe darauf zu vermerken, damit sie nicht nochmals vorgelegt werden kann. Bei *Kassenpatienten* ist die Apotheke zur elektronischen Erfassung der Verordnungsdaten verpflichtet, da sie die Daten den gesetzlichen Krankenkassen in maschinenlesbarer Form übermitteln muss. Bei *Privatpatienten* ist bereits das Speichern der Adresse im Rahmen der Zweckbestimmung des Vertragsverhältnisses (§ 28 Abs. 1 Nr. 1 BDSG) nicht erforderlich. Einer Nutzung dieser Daten für andere Zwecke wie z. B. Werbung stehen nach § 28 Abs. 1 Nr. 2 BDSG überwiegende schutzwürdige Interessen der Privat- und Kassenpatienten entgegen. Dies gilt insbesondere auf Grund des besonderen Vertrauensverhältnisses zwischen Arzt und Patient.

Will die Apotheke die Kundendaten zu Informations- oder Werbezwecken nutzen, so benötigt sie dazu die *informierte schriftliche Einwilligung* des Kunden nach § 4 Abs. 2 BDSG.

Für diese schriftliche Einwilligung hat die Aufsichtsbehörde im Berichtszeitraum mit der Apothekerkammer einen Musterinformationstext zur pharmazeutischen Betreuung mit Einwilligungserklärung ausgearbeitet, der nach Zustimmung der Aufsichtsbehörden im Düsseldorfer Kreis über die Bundesapothekerkammer allen Apotheken zur Kenntnis gebracht wurde. Im vorliegenden Beschwerdefall wurde die Apotheke auf den Mustertext verwiesen, mit dessen Hilfe sie die Adressen der einwilligenden Kunden datenschutzgerecht sammeln kann.

9.6 Einsicht in Patientenunterlagen

Mehrere Patienten fragten bei der Aufsichtsbehörde an, ob sie die vom Arzt geführten Patientenunterlagen einsehen dürfen und bei einem Arztwechsel die Unterlagen und die Röntgenbilder mitnehmen können.

Ein Arzt hat auf Grund standesrechtlicher Vorschriften die Behandlung eines Patienten zu dokumentieren. Diese *Dokumentation* ist von ihm zehn Jahre aufzubewahren. Die Dokumentation erfolgt in Form von Karteikarten oder im Praxisrechner. Bei der Dokumentation in Form von Karteikarten, die nach verschiedenen Merkmalen ausgewertet werden können, liegt eine nicht automatisierte Datei vor, für die ebenfalls das BDSG anwendbar ist.

Einsichtsrecht des Patienten

Unabhängig von den Regelungen des BDSG hat der Patient nach der Rechtsprechung des BGH grundsätzlich ein Einsichtsrecht in seine Patientenakte. Da die Akte im Eigentum des Arztes steht, hat der Patient jedoch keinen Herausgabeanspruch. Ähnlich verhält es sich bei *Röntgenbildern*. Ein Röntgenbild ist keine Datei. Es enthält personenbezogene Daten des Patienten und steht nach den Vorschriften des Urheberrechts im Eigentum des Arztes, der es angefertigt hat. Auch hier hat der Patient ein Einsichtsrecht, jedoch keinen Herausgabeanspruch.

9.7 Information von Angehörigen durch den Krankenhausarzt

An die Aufsichtsbehörde wurde der Streitfall zweier Töchter über die Auskunft eines Krankenhausarztes zu dem Gesundheitszustand ihres Vaters herangetragen. In der Familie bestanden Spannungen, die dem Arzt nicht bekannt waren. Der Krankenhausarzt hatte auf Nachfrage beide Töchter über den Gesundheitszustand ihres Vaters informiert. Die Tochter, die die Pflege des Vaters übernehmen wollte, bestritt die datenschutzrechtliche Zulässigkeit der Auskunft an ihre Schwester.

Ergebnis der Überprüfung

Die *Unterrichtung von Angehörigen* über den Gesundheitszustand ist eine Übermittlung personenbezogener Daten des Patienten. Rechtsgrundlage für die Datenübermittlung ist § 46 Abs. 1 Ziff. 3 d und § 47 Abs. 3 LKHG. Danach ist die Information von Angehörigen und sonstigen Bezugspersonen zulässig, soweit dies im Versorgungsinteresse des Patienten geboten ist, wenn er nicht widersprochen hat oder – wenn er dazu nicht in der Lage ist – sein *erkennbarer Wille* der Übermittlung nicht entgegensteht. Eine Auswahl, welchem der Angehörigen die Informationen erteilt werden, braucht das Krankenhaus bei gleichrangigen Verwandtschaftsverhältnissen nicht zu treffen, solange ihm kein entgegenstehender Patientenwille bekannt ist. So lag der Sachverhalt auch in diesem Fall.

9.8 Erhebung und Verarbeitung von Praxisdaten

Die Aufsichtsbehörde wurde darauf aufmerksam gemacht, dass ein Unternehmen mit Sitz in Baden-Württemberg bundesweit in Arztpraxen Behandlungsdaten erhebt, diese Daten auswertet und Dritten zur Verfügung stellt. Der Sachverhalt wurde von der Aufsichtsbehörde überprüft.

Ergebnis der Überprüfung

Das Unternehmen ist in der Erhebung und Auswertung von Marktforschungsdaten im Gesundheitswesen tätig. Das Unternehmen erfasst auf den Praxiscomputern der niedergelassenen Ärzte mittels eines Zusatzprogramms zur Praxissoftware automatisch die verordneten Medikamente nach Pharmazentralnummern kumuliert und aufgeschlüsselt nach Leistungsträgern, Geschlecht und Altersgruppe der Patienten. Ein auf dem Praxiscomputer implementiertes Schnittstellenprogramm erstellt eine Monatsauswertung und kopiert die Daten in verschlüsselter Form auf eine Diskette, die der Arzt per Post an das Unternehmen verschickt. Die Erhebung der Daten erfolgt im Hinblick auf die Patienten anonym, im Hinblick auf die Ärzte zu deren Verschreibungspraxis jedoch personenbezogen. Ein Patientenbezug durch das Unternehmen ist nicht herstellbar. Die von den Ärzten übermittelten Daten werden von dem Unternehmen zusammengefasst, arztbezogen für die Pharmaunternehmen und anonymisiert für Marktforschungszwecke ausgewertet. Der Arzt erhält eine besondere Auswertung zur Budgetkontrolle. Zwischen dem Arzt und dem Unternehmen wird ein Vertrag über die Datenübermittlung und die Gegenleistung abgeschlossen. Der *Arzt willigt* darin in die arztbezogene Auswertung und in die Weitergabe seiner personenbezogenen Daten an Pharmaunternehmen *ein*.

Das Verfahren, das zwischenzeitlich bundesweit eingesetzt wird, ist datenschutzrechtlich zulässig, da *keine personenbezogenen Patientendaten* verarbeitet werden und für die Verarbeitung der Arztdaten die schriftliche Einwilligung vorliegt.

Wie die Untersuchung weiter ergab, ist jedoch geplant, die Daten zukünftig auch über das Internet aus den Praxiscomputern abzurufen. Hiergegen hat die Auf-

sichtsbehörde *Bedenken* geltend gemacht. Auf einem Praxiscomputer befinden sich hochsensible Patientendaten, die zudem dem Schutz des § 203 StGB unterliegen. Wenn dieser Praxiscomputer Verbindung zum Internet hat, besteht die Gefahr, dass von dort unbemerkt Software geladen wird, die den Datenbestand ausspähen oder verändern kann. Deshalb hält die Aufsichtsbehörde einen Internetzugang an einem Praxiscomputer grundsätzlich für datenschutzrechtlich äußerst bedenklich und nur mit umfangreichen und wirkungsvollen Schutzmaßnahmen ausgerüstet, unter anderem Firewall und Virenschutzsoftware, für zulässig.

10. Verbände, Vereine, Parteien und Gewerkschaften

10.1 Wohnungswesen und Mieterdatenschutz

Der Schwerpunkt der Aufsichtstätigkeit in diesem Bereich lag bei der Klärung der Frage, ob für die Benennung einer Vergleichswohnung im Rahmen eines Mieterhöhungsverfahrens die Einwilligung des Mieters dieser Vergleichswohnung in die Weitergabe der Wohnungsdaten erforderlich ist. Häufig wurde auch von Eigentümern und Verwaltern von Eigentumswohnungen angefragt, welche Daten ein Verwalter an Miteigentümer und Dritte weitergeben darf. Ferner gingen mehrere Anfragen dazu ein, ob ein Hauseigentümer von den Energieversorgungsunternehmen Auskünfte über den Energieverbrauch seiner Mieter erhalten kann.

10.1.1 Benennung einer Wohnung als Vergleichsobjekt im Mieterhöhungsverfahren

Der Aufsichtsbehörde lagen mehrere Eingaben von Mietern vor, die sich darüber beschwerten, dass ihre Mietwohnungen *beim Mieterhöhungsverfahren* anderer Vermieter *als Vergleichsobjekt* herangezogen wurden. Die Daten der Wohnungen (wie Lage, Baujahr, Ausstattung) waren aus einem beim örtlichen Haus- und Grundbesitzerverein geführten Verzeichnis (Vergleichsmietenkataster) entnommen. Die Aufsichtsbehörde hat zur Klärung der Sach- und Rechtsfragen Gespräche mit den betroffenen Vereinen geführt und ihre Rechtsauffassung mit den beiden Landesverbänden der Haus- und Grundbesitzervereine erörtert.

Bewertung der Aufsichtsbehörde

Nach § 2 Abs. 1 des Gesetzes zur Regelung der Miethöhe (MHG) ist für eine Mieterhöhung die ortsübliche Vergleichsmiete maßgebend. Das Erhöhungsverlangen ist zu begründen. Eine der in § 2 Abs. 2 MHG vorgesehenen Begründungsmöglichkeiten ist die Benennung dreier vergleichbarer Wohnungen. Nach der Rechtsprechung des Bundesgerichtshofs müssen die Vergleichswohnungen im Erhöhungsverlangen so genau beschrieben werden, dass sie vom Mieter identifiziert werden können, damit dieser die Vergleichbarkeit überprüfen kann.

Die Daten einer Wohnung sind zweifellos personenbezogene Daten des Vermieters. Durch die im Mieterhöhungsverfahren erforderliche Identifizierbarkeit der Vergleichswohnung entsteht jedoch auch ein Personenbezug zum Mieter. Durch die Anschrift ist er bestimmbar und durch die genaue Beschreibung der Wohnung kann auf seine Lebensumstände geschlossen werden. Bei einem Mieterhöhungsverlangen, das mit der Benennung von drei vergleichbaren Wohnungen begründet wird, werden deshalb an den Mieter, an den das Mieterhöhungsverlangen gerichtet ist, personenbezogene Daten der Mieter der Vergleichswohnungen übermittelt.

§ 2 Abs. 2 MHG ist keine „andere Rechtsvorschrift“ i. S. von § 4 Abs. 1 BDSG, die die Nutzung und Verarbeitung personenbezogener Daten erlaubt. Der Gesetzgeber wollte im MHG, das vor dem BDSG erlassen wurde, keine datenschutzrechtliche Regelung treffen. Vielmehr ist die Problematik alleine nach den Regelungen des BDSG zu bewerten.

Bei der datenschutzrechtlichen Beurteilung der Frage, inwieweit die Daten anderer Wohnungen für die Begründung einer Mieterhöhung ohne Einwilligung der Mieter der Vergleichswohnungen herangezogen werden dürfen, ist zwischen vier Fallgruppen zu unterscheiden:

– Der Vermieter lässt sein Mieterhöhungsverlangen von seinem Haus- und Grundbesitzerverein durchführen, der über eine Sammlung von Vergleichsmieten verfügt.

  Viele Haus- und Grundbesitzervereine erstellen für ihre Mitglieder individuell ausgearbeitete Mietvertragsentwürfe und führen Mieterhöhungsverfahren durch. Diese Tätigkeit ist keine Datenverarbeitung im Auftrag, sondern eine eigenständige Verarbeitung von Daten. Daher können die Vereine bestimmte Wohnungsdaten insbesondere über Größe, Lage, Ausstattung und Miethöhe der von ihnen erstellten und abgeschlossenen Verträge ohne die Namen der Mieter in einem Vergleichsmietenkataster nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG zur Erfüllung eigener Geschäftszwecke speichern.

Erhält ein Verein von einem Vermieter den Auftrag, für dessen Wohnung eine Mieterhöhung durchzuführen, so greift der Verein zu deren Begründung auf die Daten des Katasters zurück. Obwohl das Kataster keine Mieternamen enthält, übermittelt er mit der Benennung der Vergleichswohnung personenbezogene Daten der Mieter. Die Zulässigkeit dieser Übermittlung ist nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG zu beurteilen. Zwar hat der Verein ein berechtigtes Interesse, das Mieterhöhungsverfahren durchzuführen, jedoch besteht Grund zur Annahme, dass das schutzwürdige Interesse der Mieter der Vergleichswohnungen an der Geheimhaltung ihrer Daten überwiegt, da

- durch die Übermittlung der Wohnungsdaten Rückschlüsse auf ihre persönlichen Verhältnisse gezogen werden können und
- durch mögliche Anfragen und Besuche des von der Mieterhöhung betroffenen Mieters, der die Vergleichbarkeit überprüfen will, Belästigungen entstehen können.

Die Übermittlung von Wohnungsdaten aus dem Kataster ist deshalb nur mit Einwilligung des Mieters der Vergleichswohnung zulässig. Die Einwilligung ist nach § 4 Abs. 1 BDSG schriftlich einzuholen. Dabei ist der Mieter über den vorgesehenen Verwendungszweck der Daten zu informieren, sowie darüber, dass die Einwilligung widerruflich ist.

– Der gewerbliche Vermieter greift bei der Begründung des Mieterhöhungsverlangens auf seinen eigenen Wohnungsbestand zu.

  Wohnungsdaten sind personenbezogene Daten des Vermieters und des Mieters. Aus diesem Grund muss der gewerbliche Vermieter bei der Benennung eigener Vergleichswohnungen in Mieterhöhungsverlangen die eingangs dargestellten, schutzwürdigen Interessen der Mieter gegenüber seinem berechtigten Interesse an der Mieterhöhung abwägen. Dazu wird er dann in der Lage sein, wenn er die aktuellen persönlichen Lebensumstände des betreffenden Mieters kennt. Ist dies nicht der Fall, muss er dem Mieter vorher Gelegenheit geben, seine Interessen darzulegen, die der Benennung seiner Wohnung als Vergleichswohnung entgegenstehen.

  Da es nach Auffassung der Aufsichtsbehörde häufig schwierig ist, eine solche Abwägung sachgerecht durchzuführen, wird auch bei gewerblichen Vermietern die Einholung einer vorherigen Einwilligung der Mieter der praktikablere Weg sein.

– Der gewerbliche oder private Vermieter greift für sein Mieterhöhungsverlangen auf fremde Wohnungsbestände zu.

  Speichert eine nichtöffentliche Stelle geschäftsmäßig Wohnungsdaten zu dem Zweck, diese an Vermieter zur Begründung von Mieterhöhungsverlangen zu übermitteln, handelt es sich um eine geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung nach § 29 BDSG. Von einer rechtmäßigen Speicherung ausgehend ist in diesen Fällen die Übermittlung nur dann zulässig, wenn der Vermieter, der die Daten erhalten will, ein berechtigtes Interesse glaubhaft darlegt und kein Grund zur Annahme besteht, dass der Mieter, dessen Daten übermittelt werden, ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. Von einem schutzwürdigen Interesse muss nach Ansicht der Aufsichtsbehörde jedoch regelmäßig ausgegangen werden. Daher ist auch in diesen Fällen eine Übermittlung von Wohnungsdaten ohne die Einwilligung des betroffenen Mieters nach § 29 BDSG nicht zulässig.

– Der private Vermieter erhält Angaben über Vergleichsmieten von anderen privaten Vermietern.

  Die Datenverarbeitung ist bei privaten Vermietern weder geschäftsmäßig noch gewerblich, solange sie keinen berufsmäßigen Umfang annimmt. Das BDSG gilt nicht für den privaten Umgang mit personenbezogenen Daten.

Mit einem Landesverband konnte eine Einigung erzielt werden. Dieser hat seine Mitgliedsvereine über die Rechtslage informiert und eine mit der Aufsichtsbehörde abgestimmte Einwilligungserklärung zur Verwendung empfohlen. Ein anderer Landesverband konnte bislang von der datenschutzrechtlichen Bewertung nicht überzeugt werden.

10.1.2 Übermittlung von Daten durch den Wohnungsverwalter an die Wohnungseigentümer

Von der Aufsichtsbehörde war die Frage zu beantworten, ob der Verwalter einer Wohnanlage mit Eigentumswohnungen den prozentualen Anteil jeder Wohnung an den Gesamtheizkosten in der Wohnungseigentümerversammlung bekannt geben darf.

Bewertung der Aufsichtsbehörde

Personenbezogene Daten sind nach § 3 Abs. 1 BDSG Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren Person. Die Heizkosten beschreiben sachliche Verhältnisse. Somit sind sie personenbezogene Daten des Eigentümers bzw. Mieters der Wohnung.

Ob die *Daten den Miteigentümern in der Wohnungseigentümerversammlung* bekannt gegeben, das heißt übermittelt werden dürfen, hängt davon ab, ob ihre Kenntnis für die ordnungsgemäße Beschlussfassung durch die Versammlung erforderlich ist. Dies könnte beispielsweise der Fall sein bei einer Beratung und Beschlussfassung über die Verbesserung der Wärmeisolierung oder Optimierung der Heizungsanlage. Ist die Kenntnis erforderlich, so liegt ein berechtigtes Interesse der Eigentümerversammlung vor. Die Datenübermittlung ist dann nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig, sofern nicht Grund zur Annahme besteht, dass ein schutzwürdiges Interesse eines Eigentümers oder Mieters am Ausschluss der Übermittlung überwiegt. Ob ein solches schutzwürdiges Interesse zum Tragen kommt, lässt sich aber immer nur im Einzelfall klären.

10.1.3 Übermittlung von Verbrauchsdaten des Mieters durch Energieversorgungsunternehmen an den Vermieter

Verschiedene Vermieter richteten an die Aufsichtsbehörde die Frage, ob die Energieversorgungsunternehmen ihnen zu Recht die Auskunft über den Energieverbrauch ihrer Mieter verweigert hatten. Die Energielieferungsverträge waren zwischen den Mietern und den Energieversorgungsunternehmen abgeschlossen.

Bewertung der Aufsichtsbehörde

Angaben über den Energieverbrauch des Mieters sind als Einzelangaben über persönliche oder sachliche Verhältnisse personenbezogene Daten des Mieters. Ohne die Einwilligung des Mieters darf das Energieversorgungsunternehmen die Verbrauchsdaten nur dann an den Vermieter übermitteln, wenn dies nach § 28 BDSG zulässig ist. Nach § 28 Abs. 2 Satz 1 Nr. 1 a BDSG ist das Übermitteln personenbezogener Daten zulässig, soweit es zur Wahrung berechtigter Interessen des Vermieters erforderlich ist und kein Grund zur Annahme besteht, dass der Mieter ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. Die Aufsichtsbehörde hat Bedenken, ob der Vermieter ein berechtigtes Interesse geltend machen kann. Im Regelfall dürfte zudem auch ein Grund zur Annahme eines schutzwürdigen Interesses des Mieters bestehen. Eine andere Beurteilung könnte sich z. B. dann ergeben, wenn Mieter und Vermieter über verbrauchsabhängige Umlagen streiten; dann könnte der Vermieter zum Erhalt der Auskunft berechtigt sein.

Davon zu unterscheiden ist der Fall, dass der Vermieter den Energielieferungsvertrag abgeschlossen hat. Dann erhält er nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG die Daten im Rahmen der Zweckbestimmung des Vertragsverhältnisses und übermittelt sie an die Mieter weiter.

10.2 Datenverarbeitung in Vereinen

Ein fester Bestandteil unserer gesellschaftlichen Struktur sind die Vereine. Die Vielfalt der Zwecke, zu denen sie gegründet wurden, und der Themenfelder, in denen sie sich betätigen, führt dazu, dass beinahe jeder Bürger und jede Bürgerin in einem oder mehreren Vereinen Mitglied ist. Ob die Vereine sich nun dem Sport, dem Umwelt- und Naturschutz, der Bildung oder der Kultur widmen, ob sich nun Kleintierzüchter, Schachspieler, Briefmarkensammler oder Zauberer zusammengeschlossen haben, ob die Vereine die Interessen von Mietern und Haus-

und Grundbesitzern wahrnehmen oder sich im sozialen oder gesundheitlichen Bereich zu Selbsthilfegruppen organisiert haben, ob sie als Parteien, Verbände oder Gewerkschaften aktiv sind, sie haben immer Mitglieder, deren *Daten verwaltet* werden müssen.

Erfolgt die *Verarbeitung oder Nutzung der Mitgliederdaten* oder der Daten sonstiger Personen mithilfe der automatisierten Datenverarbeitung oder in Mitgliederkarteien, sind für die Datenverarbeitung die Bestimmungen des BDSG maßgebend, obwohl dieses Gesetz auf den ersten Blick auf Vereine nicht anwendbar zu sein scheint. Nach § 1 BDSG ist nämlich der Anwendungsbereich konkret auf die geschäftsmäßige oder für berufliche oder gewerbliche Zwecke ausgerichtete Verarbeitung und Nutzung von personenbezogenen Daten in oder aus Dateien beschränkt. Bei der Vereinsdatenverarbeitung ist aber von einer Geschäftsmäßigkeit auszugehen, da sie in der Regel auf eine gewisse Dauer und Wiederholung angelegt ist. Im novellierten BDSG wird der Anwendungsbereich wesentlich umfassender geregelt, sodass die Vereinsdatenverarbeitung darunter fallen wird.

Bewertung der Aufsichtsbehörde

Die Mitgliedschaft in einem Verein ist im Sinne des BDSG als vertragsähnliches Vertrauensverhältnis anzusehen, dessen Rahmen und Inhalt im Wesentlichen durch die Vereinssatzung und – soweit vorhanden – die Vereinsordnung vorgegeben wird. Aus dem Vertrauensverhältnis folgt, dass der Verein bei der Erhebung, Verarbeitung und Nutzung von Daten das Persönlichkeitsrecht seiner Mitglieder angemessen berücksichtigen muss. Unerheblich ist dabei, ob der Verein ins Vereinsregister eingetragen ist und eigene Rechtspersönlichkeit besitzt oder ob es sich um einen nicht rechtsfähigen Verein handelt.

Für *eigene Zwecke des Vereins* dürfen Mitgliederdaten nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG im Rahmen der Vereinsmitgliedschaft als vertragsähnlichem Vertrauensverhältnis und damit des Vereinszwecks verarbeitet oder genutzt werden. Dabei ist maßgeblich auf den in der Satzung festgelegten Vereinszweck abzustellen. Auf Grund des Vereinszwecks dürfen nicht nur Mitgliederdaten verarbeitet oder genutzt werden, die für die Vereinsmitgliedschaft unbedingt erforderlich sind (wie etwa Name und Anschrift des Mitglieds und bei Lastschrifteinzug der Mitgliedsbeiträge: Bankverbindung, Bankleitzahl und Kontonummer), sondern darüber hinaus auch sonstige Mitgliederdaten, die im Rahmen des Vereinszwecks liegen, d. h. die geeignet sind, diesen zu fördern (z. B. Übungsleiterlizenz, Funktion im Verein). Darüber hinaus dürfen Mitgliederdaten, bei denen kein ausreichender Sachzusammenhang mit dem Vereinszweck besteht (etwa Telefon- oder Faxnummern von Mitgliedern) sowie Daten von Nichtmitgliedern nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG verarbeitet oder genutzt werden, wenn dies zur Wahrung der berechtigten Interessen des Vereins erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein überwiegendes schutzwürdiges Interesse am Ausschluss der Verarbeitung oder Nutzung hat. Dabei sind die Interessen des Vereins und die schutzwürdigen Belange des Betroffenen allgemein gegeneinander abzuwägen, wobei vor allem auf die Art und Schutzbedürftigkeit der Daten sowie den geplanten Verwendungszweck der Daten abzustellen ist. Wegen des vertragsähnlichen Vertrauensverhältnisses zwischen dem Verein und seinen Mitgliedern kann es angemessen sein, entgegenstehende schutzwürdige Interessen einzelner Mitglieder auch dann zu berücksichtigen, wenn sie das Vereinsinteresse nicht überwiegen.

Für *fremde Zwecke* darf ein Verein nach § 28 Abs. 2 Satz 1 Nr. 1 a BDSG Daten seiner Mitglieder übermitteln oder nutzen, soweit dies zur Wahrung berechtigter Interessen eines Dritten oder öffentlicher Interessen erforderlich ist oder wenn es sich um die in § 28 Abs. 2 Satz 1 Nr. 1 b BDSG aufgeführten listenmäßigen Daten handelt (insbesondere Angaben über die Zugehörigkeit zu einer Personengruppe, z. B. Mitglied des Sportvereins X, Name, Anschrift, Geburtsjahr). In beiden Fällen ist die Übermittlung oder Nutzung der Daten nur zulässig, wenn bei allgemeiner Abwägung kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der betroffenen Mitglieder entgegenstehen. Da der Verein grundsätzlich verpflichtet ist, die Interessen seiner Mitglieder zu wahren, wird eine Datenübermittlung an außenstehende Dritte oder die Nutzung der Daten für deren Zwecke nach den genannten Vorschriften nur ausnahmsweise in Betracht kommen.

Kann die Verarbeitung oder Nutzung personenbezogener Daten nicht auf eine Vorschrift des BDSG gestützt werden, ist sie nur zulässig, wenn der Betroffene einge-

willigt hat. Die *Einwilligung* ist nach §4 Abs. 2 BDSG nur wirksam, wenn der Betroffene zuvor ausreichend klar darüber informiert worden ist, welche Daten für welchen Zweck vom Verein gespeichert und genutzt werden bzw. an wen sie ggf. übermittelt werden sollen, sodass er die Folgen seiner Einwilligung auf der Grundlage dieser Information konkret abschätzen kann; sie bedarf regelmäßig der Schriftform. Insbesondere bei kleineren Vereinen kann in Ausnahmefällen bei Vorliegen besonderer Umstände (beispielsweise bei weniger bedeutsamen oder eilbedürftigen Vorgängen) eine mündliche oder konkludente Einwilligung ausreichen. Die Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Vereinsinterne Regelungen

Die Vereine sollten *vereinsinterne Regelungen* für eine ordnungsgemäße Datenverarbeitung treffen und darin auch technische und organisatorische Sicherheitsmaßnahmen vorsehen, etwa um zu verhindern, dass die Mitgliederdaten missbräuchlich verwendet werden, Unbefugte hiervon Kenntnis erlangen oder Daten auf Grund unzureichender Datensicherung verloren gehen. Dies ist beispielsweise auch erforderlich, wenn die Datenverarbeitung von Mitgliedern ehrenamtlich zu Hause mit eigener DV-Ausstattung erledigt wird. Geregelt werden sollte auch, welche Mitgliederdaten wie lange gespeichert werden und wann Daten ausgeschiedener Mitglieder gelöscht werden. Wird die Verwaltung der Mitgliederdaten von einem Funktionsträger auf einen Nachfolger übertragen, ist dafür zu sorgen, dass sämtliche Mitgliederdaten übergeben werden und keine Kopien beim bisherigen Funktionsträger verbleiben.

Zur Datenverarbeitung in Vereinen hat die Aufsichtsbehörde ein Merkblatt erstellt, das auf Anfrage an Vereine herausgegeben wird.

Im Zusammenhang mit der Aufsichtstätigkeit sind die nachfolgenden Fälle zur Datenverarbeitung bei Vereinen erwähnenswert.

10.2.1 Bekanntgabe von Mitgliederdaten innerhalb des Vereins

Innerhalb eines Vereins sind die Aufgaben in der Regel abgegrenzt und bestimmten Funktionsträgern zugewiesen. Wer wofür zuständig ist, wird durch die Satzung des Vereins bzw. durch seine satzungsmäßigen Organe (Vorstand, Mitgliederversammlung, ggf. Vertreterversammlung, Ausschüsse) bestimmt. Für den *vereinsinternen Umgang mit Mitgliederdaten* gilt, dass jeder Funktionsträger die für die Ausübung seiner Funktion notwendigen Mitgliederdaten verarbeiten und nutzen darf. So darf beispielsweise der Vorstand auf alle Mitgliederdaten zugreifen, wenn er diese zur Aufgabenerledigung benötigt. Alle Mitgliederdaten müssen regelmäßig auch der Vereinsgeschäftsstelle für die Mitgliederverwaltung zur Verfügung stehen. Für den Schatzmeister oder Kassierer genügen hingegen die für die Beitragsfestsetzung und den Beitragseinzug relevanten Mitgliederdaten (Namen, Anschrift, Bankverbindung usw.), für den Leiter einer Vereinsabteilung Namen, Anschrift und Telefonnummer der Mitglieder seiner Abteilung.

Abgrenzung zwischen speichernder Stelle und Dritten

Der *Verein* ist für seine Mitgliederdaten *speichernde Stelle*. Dem Verein zuzurechnen sind unselbstständige Organisationen – z. B. Ortsvereine oder Ortsgruppen eines überregionalen Vereins – und seine Funktionsträger, Auftragnehmer und gegebenenfalls – vom Verein beschäftigte Mitarbeiter, soweit diese im Rahmen der Aufgabenerfüllung für den Verein tätig werden. Die Weitergabe von Mitgliederdaten durch den Verein an diese Stellen oder Personen ist ein *vereinsinterner Vorgang* und keine Datenübermittlung. Im Unterschied hierzu sind selbstständige Organisationen des Vereins (beispielsweise selbstständige Kreisverbände) sowie Vereinsmitglieder, die keine Funktionen ausüben, datenschutzrechtlich im Verhältnis zum Verein *Dritte.* Die Weitergabe von Mitgliederdaten durch den Verein an solche Organisationen und Mitglieder ist daher eine Datenübermittlung, die nur zulässig ist, wenn die rechtlichen Voraussetzungen vorliegen.

Zulässigkeit der Datenübermittlung

In der Vereinspraxis stellt sich häufig die Frage, inwieweit es zulässig ist, *Daten von Mitgliedern anderen Vereinsmitgliedern zu übermitteln*. So wurde der Aufsichtsbehörde folgender Fall vorgetragen:

Einzelne Mitglieder eines größeren Vereins wollten eine *außerordentliche Mitgliederversammlung* einberufen. Dies war nach der Satzung nur möglich, wenn dazu dem Vorstand Unterschriften von mindestens einem Drittel der Vereinsmitglieder vorgelegt werden. Ohne eine Namensliste der Vereinsmitglieder war aber die Durchführung der Unterschriftensammelaktion nicht möglich. Der Vorstand lehnte die Herausgabe einer Mitgliederliste unter Hinweis auf den Datenschutz ab.

Bewertung der Aufsichtsbehörde

Die Aufsichtsbehörde hielt aus nachstehenden Gründen die Rechtsauffassung des Vorstandes für unzutreffend und eine Datenübermittlung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG für zulässig.

Regelungen in Vereinssatzungen sehen vielfach vor, dass beispielsweise Anträge auf Einberufung einer außerordentlichen Mitgliederversammlung oder auf Ergänzung der Tagesordnung der Mitgliederversammlung davon abhängig gemacht werden, dass eine bestimmte Mindestzahl von Mitgliedern die Einberufung bzw. Ergänzung verlangt. Wenn der Verein nicht generell eine Mitgliederliste oder ein Mitgliederverzeichnis herausgibt, kann es erforderlich sein, dass er Mitgliedern beispielsweise durch Einsicht in diese Unterlagen ermöglicht, eine ausreichende Anzahl anderer Mitglieder für die Unterstützung eines solchen Minderheitsantrags zu erreichen. Die Offenbarung von Mitgliederdaten für diesen Zweck ist wegen der Pflicht des Vereins, die Ausübung satzungsmäßiger Minderheitsrechte zu ermöglichen, regelmäßig im Vereinsinteresse erforderlich, ohne dass überwiegende schutzwürdige Interessen der betroffenen Mitglieder entgegenstehen. So lag der Fall auch hier.

Ausnahmsweise können jedoch überwiegende schutzwürdige Belange der Mitglieder einer Bekanntgabe ihres Namens und ihrer Anschrift entgegenstehen, beispielsweise wenn ein Interesse der Mitglieder besteht, dass ihre Daten vertraulich behandelt werden oder wenn die Zugehörigkeit zum Verein ein besonders sensibles Datum darstellt (z. B. Parteien, Gewerkschaften). Dann sollte der Verein eine entsprechende Regelung in der Satzung treffen oder die Mitglieder ausreichend informieren, ohne ihre Daten bekannt zu geben. Dies kann etwa dadurch geschehen, dass in einer Vereinspublikation auf den beabsichtigten Antrag, die Gründe und den Antragsteller hingewiesen und so interessierten Mitgliedern die Möglichkeit der Kontaktaufnahme zur Unterstützung eröffnet wird.

Im Übrigen beurteilt sich die Zulässigkeit der Datenübermittlung an Mitglieder, die im Einzelfall den Verein um Auskunft über Daten anderer Mitglieder ersuchen, nach § 28 Abs. 2 Satz 1 Nr. 1 a BDSG danach, *ob das auskunftsersuchende Vereinsmitglied ein berechtigtes Interesse an der Kenntnis der Daten hat* und ob bei allgemeiner Abwägung keine schutzwürdigen Interessen der betroffenen Mitglieder der Datenübermittlung entgegenstehen. Dabei kommt es auf die Umstände des konkreten Einzelfalles an, beispielsweise ob es sich um einen kleinen Verein handelt, dessen Mitglieder sich im Wesentlichen kennen, oder um einen großen Verein, bei dem dies nicht der Fall ist, und darauf, ob die Kenntnis der Mitgliederdaten für den beabsichtigten Zweck erforderlich ist. Zu berücksichtigen ist auch, um welche Art von Verein es sich handelt, ob sich im Verein in der Vergangenheit eine bestimmte allgemein akzeptierte Praxis herausgebildet hat und ob einzelne Mitglieder bereits früher Einwände gegen die Übermittlung ihrer Daten erhoben haben.

Mitgliederlisten

Häufig besteht bei Vereinen auch die Unsicherheit, ob *Mitgliederlisten* an die Vereinsmitglieder herausgegeben und welche Daten darin aufgenommen werden dürfen.

Besteht bei Vereinen vom Vereinszweck her eine *persönliche Verbundenheit* und kennen sich die Mitglieder gegenseitig oder stellt die Pflege des persönlichen oder geschäftlichen Kontakts der Mitglieder einen wichtigen Bestandteil des Vereinszwecks dar, ist die Herausgabe einer Mitgliederliste im Rahmen des Vereinsverhältnisses als vertragsähnlichem Vertrauensverhältnis nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG zulässig. Welche Angaben dabei in die Mitgliederliste aufgenommen werden dürfen, hängt vom jeweiligen Vereinszweck ab, wobei die Interessen der Mitglieder angemessen zu berücksichtigen sind.

Bei *anderen Vereinen*, bei denen diese Voraussetzungen nicht vorliegen, aber dennoch der Verein oder die meisten Vereinsmitglieder ein Interesse an der Herausgabe einer Mitgliederliste haben, ist dieses Interesse nach § 28 Abs. 1 Satz 1 Nr. 2 und Abs. 2 Satz 1 Nr. 1 b BDSG mit etwaigen entgegenstehenden Interessen anderer Vereinsmitglieder abzuwägen. Dabei ist insbesondere zu berücksichtigen, ob die Mitglieder ein schutzwürdiges Interesse daran haben, dass ihre Adressen vertraulich behandelt und nicht offengelegt werden. Dies kann beispielsweise bei großen Vereinen ohne persönliche Verbundenheit der Mitglieder oder bei Selbsthilfevereinen der Fall sein. Ist nach *Abwägung der Interessen* die Herausgabe einer Mitgliederliste zulässig, empfiehlt es sich, einen Mitgliederbeschluss oder einen Beschluss des Vorstands über die Herausgabe der Mitgliederliste herbeizuführen und diesen den Vereinsmitgliedern bekannt zu geben. Mitglieder, die ihre schutzwürdigen Interessen durch die Herausgabe der Mitgliederliste beeinträchtigt sehen, können dann Einspruch gegen die Aufnahme ihrer Adresse in die Mitgliederliste erheben und sollten unabhängig davon, ob ihre schutzwürdigen Interessen überwiegen, nicht in die Liste aufgenommen werden.

Die Daten in der Mitgliederliste sollten sich möglichst auf die zur *Kontaktaufnahme* notwendigen Angaben wie Namen, Anschrift und ggf. Telefonnummer der Mitglieder, soweit diese im Telefonbuch enthalten ist oder die Mitglieder der Aufnahme ihrer dort nicht enthaltenen Telefonnummer in die Mitgliederliste zugestimmt haben, beschränken. Sollen in die Liste darüber hinaus noch weitere Angaben aufgenommen werden wie z. B. Beruf, Familienstand, Geburtstag, ist dies bei der Abwägung der einer Bekanntgabe entgegenstehenden schutzwürdigen Interessen von Mitgliedern im Rahmen des § 28 Abs. 1 Satz 1 Nr. 2 BDSG zu berücksichtigen. Dies kann dazu führen, dass eine Bekanntgabe nur mit Einwilligung der Betroffenen zulässig ist. In Zweifelsfällen empfiehlt es sich, die Einwilligung der Vereinsmitglieder in die Herausgabe der Mitgliederliste einzuholen. Bei der Herausgabe der Mitgliederliste ist nach § 28 Abs. 4 BDSG darauf hinzuweisen, dass diese nur für Vereinszwecke verwendet werden darf und eine Verwendung für andere Zwecke sowie die Überlassung der Liste an außenstehende Dritte nicht zulässig ist.

10.2.2 Bekanntgabe von Mitgliederdaten für Werbezwecke

Vereine sollten bei der *Übermittlung von Mitgliederdaten an Wirtschaftsunternehmen zu Werbezwecken* grundsätzlich zurückhaltend verfahren. Anders als bei Vertragsbeziehungen mit Wirtschaftsunternehmen handelt es sich bei einer Mitgliedschaft in einem Verein um ein personenrechtliches Rechtsverhältnis, aus dem sich für den Verein besondere *Rücksichtnahmepflichten* in Bezug auf die schutzwürdigen Belange seiner Mitglieder ergeben, die je nach Art des Vereins unterschiedlich stark sind. Besonders Mitglieder örtlicher Vereine vertrauen regelmäßig darauf, dass der Verein ihre Daten grundsätzlich nicht für vereinsfremde Zwecke verwendet. Bei größeren, überregional tätigen Vereinen hingegen könnte eine andere Situation gegeben sein.

So hat sich beispielsweise folgender Fall zugetragen:

Ein Kreisverband einer Partei hat Namen und Anschrift von Parteimitgliedern zum Teil ohne deren Einwilligung an einen Zeitschriftenverlag zur Übersendung eines Probeabonnements weitergegeben. Die Geschäftsstelle des Kreisverbandes ging davon aus, dass den datenschutzrechtlichen Anforderungen dadurch Genüge getan wurde, dass das Angebot zum Zeitschriftenbezug nicht unmittelbar durch den Zeitschriftenverlag, sondern durch die Kreisverbandsgeschäftsstelle an die Betroffenen herangetragen worden ist und den Betroffenen ein angemessener Reaktionszeitraum eingeräumt wurde, innerhalb dessen sie sich gegen eine Weitergabe ihrer Daten aussprechen konnten. Bei der Kreisverbandsgeschäftsstelle ging man davon aus, dass die Betroffenen, die sich innerhalb dieses Zeitraums nicht gegen eine Weitergabe ihrer Daten ausgesprochen hatten, durch Schweigen in die Datenübermittlung an den Zeitschriftenverlag eingewilligt hätten.

Ergebnis der Überprüfung, Beanstandung

Die Auffassung der Kreisverbandsgeschäftsstelle musste von der Aufsichtsbehörde beanstandet werden. Der Kreisverband ist für die Speicherung und Übermittlung der Daten seiner Mitglieder die verantwortliche Stelle, die die Schutzrechte

der Betroffenen zu wahren hat. Soweit die Datenübermittlung nicht im Rahmen der Mitgliedschaft nach den satzungsgemäßen Zielen der Partei zulässig ist, sind die Übermittlungsvorschriften des § 28 Abs. 2 BDSG zu beachten. Namen und Anschriften von Parteimitgliedern dürfen danach nur dann an andere Unternehmen und Organisationen übermittelt werden, wenn kein Grund zu der Annahme besteht, dass die betroffenen Mitglieder ein schutzwürdiges Interesse am Ausschluss der Übermittlung haben. Ein solches der Übermittlung entgegenstehendes Interesse ist nach der gesetzlichen Vermutung des § 28 Abs. 2 Satz 2 BDSG in Bezug auf politische Anschauungen im Allgemeinen immer gegeben, weshalb die Weitergabe von Parteimitgliederdaten grundsätzlich als unzulässig angesehen werden muss, wenn nicht ausnahmsweise die Einwilligung der Betroffenen vorliegt. Anders verhält es sich lediglich, wenn Daten weitergegeben werden sollen, die auch aus allgemein zugänglichen Quellen zu entnehmen sind, wie beispielsweise Orts- oder Kreisvorstände der Partei, Fraktionsmitglieder u. ä. Wegen der besonderen Sensibilität der Information über die Mitgliedschaft in einer Partei reicht die mutmaßliche Einwilligung des Mitglieds in die Übermittlung seiner Daten nicht aus. Der Kreisverband der Partei konnte daher nicht davon ausgehen, dass jedes Mitglied mit der Weitergabe seiner Adresse an den Zeitschriftenverlag zur Zusendung von Probeexemplaren einer Tageszeitung dann einverstanden ist, wenn es sich nicht ausdrücklich gegen die Weitergabe gewandt hat. Vielmehr wäre es erforderlich gewesen, nur solche Adressen von Mitgliedern weiterzugeben, die sich positiv dazu geäußert haben. Der Kreisverband sagte zu, künftig nur noch Mitgliederdaten weiterzugeben, wenn eine ausdrückliche Einwilligung der Mitglieder vorliegt.

Geheimhaltungsinteressen der Mitglieder

Allgemein gilt, dass Vereine, soweit sie ihren Mitgliedern gegenüber zur Rücksichtnahme verpflichtet sind, Mitgliederdaten nur mit Einwilligung der betroffenen Mitglieder an Wirtschaftsunternehmen (z. B. Versicherungen, Banken, Zeitschriftenverlage) übermitteln dürfen. Dies gilt in besonderem Maße, wenn es sich um besonders schutzbedürftige Daten handelt. Oft ergibt sich das *Geheimhaltungsinteresse der Mitglieder* schon aus dem Vereinszweck, so beispielsweise bei einer Suchtkranken-Selbsthilfegruppe oder einer Elterninitiative verhaltensgestörter Kinder. Darüber hinaus kann sich die besondere Sensibilität und damit die erhöhte Schutzwürdigkeit der Daten auch aus der Vereinsmitgliedschaft ergeben, wenn sich daraus etwa Rückschlüsse auf gesundheitliche Verhältnisse, politische oder religiöse Anschauungen, die rassische oder ethnische Herkunft sowie die Zugehörigkeit zu einer Gewerkschaft ziehen lassen. Nur dann, wenn Interessen von Vereinsmitgliedern offensichtlich nicht entgegen stehen, können die in § 28 Abs. 2 Satz 1 Nr. 1 b BDSG aufgeführten listenmäßigen Daten an Wirtschaftsunternehmen weitergegeben werden. Dabei muss jedoch der Umstand berücksichtigt werden, dass der Datenempfänger diese Daten wiederum für Werbezwecke anderer Unternehmen weitergeben oder nutzen kann. Deshalb sollte die Verwendung der übermittelten Daten auf den konkreten Werbezweck des Datenempfängers beschränkt und eine Nutzung oder Übermittlung der Daten für fremde Werbezwecke vertraglich ausgeschlossen werden. Daten von Mitgliedern, bei denen ein entgegenstehendes Interesse erkennbar ist, dürfen auf keinen Fall weitergegeben werden.

10.2.3 Veröffentlichung von Daten

Die Veröffentlichung von Daten ist datenschutzrechtlich eine Übermittlung von Daten an einen üblicherweise unbekannten Personenkreis. In einer Regelung in der Satzung oder Vereinsordnung kann eine *Veröffentlichung* von personenbezogenen Daten für eigene Zwecke des Vereins vorgesehen werden. Für die Veröffentlichung müssen die Zulässigkeitsvoraussetzungen des § 28 BDSG erfüllt sein. Andernfalls ist nur mit Einwilligung der Betroffenen zulässig.

An die Aufsichtsbehörde wurden *folgende Fälle* herangetragen:

– Ein Beschwerdeführer wandte sich gegen die Veröffentlichung zweier *Listen* von Namen und Wohnort der Mitglieder einer Gewerkschaft, die nach der geltenden Regelung *über die Abführung von Aufsichtsratsvergütungen* diese korrekt bzw. nicht korrekt abgeführt haben. Der Veröffentlichung vorangestellt

war die Beschlusslage des Gewerkschaftstages, wonach die Veröffentlichung in der geschehenen Form erfolgen soll. Die Veröffentlichung erfolgt jährlich in der gewerkschaftseigenen Publikation. Der Beschwerdeführer war der Meinung, dass einer Veröffentlichung schutzwürdige Belange der Betroffenen entgegenstehen.

Ergebnis der Überprüfung

Die Überprüfung durch die Aufsichtsbehörde ergab die Zulässigkeit einer solchen Veröffentlichung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Nach einem Beschluss des Bundesvorstands der gewerkschaftlichen Dachorganisation ist vonseiten des Bundesvorstands und der Gewerkschaften sicherzustellen, dass die Erfüllung der Abführungsverpflichtung durch die jeweils zuständige Gewerkschaft wirksam kontrolliert wird. Über die Kontrolle der Erfüllung der Abführungspflicht wurde ein Beschluss des Gewerkschaftstags der betroffenen Gewerkschaft gefasst. Dem Beschluss entsprechend soll die Kontrolle der Erfüllung der Abführungsverpflichtung nicht nur intern erfolgen, sondern besonders wirksam durch gewerkschaftsöffentlichen Druck sichergestellt werden. Das gegen die Abführungspflicht verstoßende Mitglied soll sich gerade der Kritik aller Mitglieder stellen müssen und nicht nur einer Auseinandersetzung mit dem Vorstand. Daraus lassen sich aber keine Einwände gegen die Veröffentlichung in der gewerkschaftseigenen Publikation ableiten, insbesondere wenn man das Auswahlverfahren der Aufsichtsratsmitglieder bedenkt. Die Kandidaten der Gewerkschaft werden öffentlich nominiert und übernehmen ebenso öffentlich die Verpflichtung, einen Teil ihrer Vergütung abzuführen. Zu keinem Zeitpunkt können daher weder bei den Betroffenen noch bei allen anderen Mitgliedern der Gewerkschaft Zweifel über die Konsequenzen der Wahl zum Aufsichtsrat bestehen. Es besteht deshalb kein Grund für die Annahme, dass schutzwürdige Belange der einzelnen Aufsichtsratsmitglieder die berechtigten Interessen der Gewerkschaft an der Veröffentlichung der Daten überwiegen. Durch den auf dem Gewerkschaftstag gefassten Beschluss haben die Mitglieder ihren Wunsch zum Ausdruck gebracht, die Kontrolle nicht allein dem Vorstand zu überlassen, sondern sie als eine den Gewerkschaftsmitgliedern unmittelbar obliegende Angelegenheit anzusehen. Das jeweils betroffene Gewerkschaftsmitglied muss infolgedessen die Publikation ebenso in Kauf nehmen wie jede andere aus der Zugehörigkeit zur Gewerkschaft folgende Pflicht. Mögliche Bedenken hinsichtlich einer allgemeinen Persönlichkeitsrechtsverletzung einzelner betroffener Gewerkschaftsmitglieder dürften an dem gewichtigeren berechtigten Interesse der Gewerkschaft und ihrer Mitglieder, die Einhaltung der jedem zum Aufsichtsrat gewählten Gewerkschaftsmitglied obliegenden Verpflichtung zu kontrollieren, scheitern.

– In einem anderen Fall hatte ein Bürger auf einen entsprechenden Spendenaufruf anlässlich eines Heimatfestes in seinem Wohnort die zur Festorganisation eingesetzte Kommission mit einer Spende unterstützt. Kurze Zeit später erschien in der örtlichen Tagespresse eine Auflistung aller Spender mit Namen und genauer Anschrift, nicht aber des Spendenbetrags. Der Bürger vertrat die Auffassung, dass es niemand etwas angehe, ob er etwas spende, und dass durch die Veröffentlichung ein Zwang ausgeübt werde, das jährlich stattfindende Fest regelmäßig mit einer Spende zu unterstützen.

Ergebnis der Überprüfung

Spenden bilden eine wichtige finanzielle Grundlage vieler Vereine. Vereine haben deshalb ein nicht unerhebliches Interesse an dieser finanziellen Unterstützung ihrer regelmäßigen Arbeit oder einzelner Aktionen. Neben persönlichen Ansprachen von Vereinsmitgliedern werden auch Nichtvereinsmitglieder über persönlich adressierte Werbung oder über allgemeine Aufrufe um Spenden gebeten. Wenn es sich um eine öffentlichkeitswirksame Aktion handelt, die durch Spenden unterstützt werden soll, ist es den Vereinen oft auch ein Bedürfnis, den Spendern öffentlich und persönlich zu danken. Dies geschieht häufig durch Nennung des Namens und teilweise sogar des Wohnorts und/oder des Spendenbetrags beispielsweise in der örtlichen Tagespresse, in entsprechenden Fachzeitschriften oder in den Vereinsnachrichten.

Die Veröffentlichung von *Spenderlisten* ist datenschutzrechtlich eine Übermittlung von personenbezogenen Daten für eigene Zwecke und nach § 28 Abs. 1

Satz 1 Nr. 2 BDSG ohne Einwilligung der Betroffenen zulässig, soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Nutzung überwiegt. Zweifellos liegt es im berechtigten Interesse eines Vereins, die Spender, die etwa ein Fest finanziell unterstützen, namentlich zu erwähnen und ihnen öffentlich zu danken. Ob eine Veröffentlichung der einzelnen Spender zur Wahrung dieses berechtigten Interesses erforderlich ist, bedarf der Abwägung. Führt die Abwägung zu dem Ergebnis, dass es an der Erforderlichkeit mangelt, ist eine Veröffentlichung nur mit einer Einwilligung der Betroffenen möglich. Zwar ist für eine Einwilligung grundsätzlich die Schriftform vorgeschrieben, bei Vorliegen besonderer Umstände können aber auch andere Formen angemessen sein. Soll auch die *Spendenhöhe* bekannt gegeben werden, so ist dazu jedoch eine *schriftliche Einwilligung* einzuholen, da mit einer Bekanntgabe dieses Datums ein tiefer Einblick in die Privatsphäre verbunden ist.

In dem schriftlichen Spendenaufruf, der an die einzelnen Haushalte verteilt wurde, ist im letzten Absatz ausdrücklich für den Fall um Mitteilung gebeten worden, dass eine Veröffentlichung der Spenderdaten nicht gewünscht wird. Im Spendenwesen in örtlichen bzw. begrenzten regionalen Bereichen ist die Einholung einer Einwilligung in Form einer solchen Negativerklärung durchaus üblich und auch zulässig, da erfahrungsgemäß die meisten Spender mit der Veröffentlichung einverstanden sind und diese gegebenenfalls erwarten. Es ist deshalb nicht unangemessen, wenn die Darstellungslast für entgegenstehende Interessen den Spendern auferlegt wird, die nicht veröffentlicht werden wollen. Bei denjenigen Spendern, die auf die ausdrückliche Aufforderung nicht reagiert haben, konnte die veranstaltende Kommission deshalb davon ausgehen, dass sie mit der Veröffentlichung einverstanden waren. Der Beschwerdeführer hatte sich jedoch nicht bei der Kommission gemeldet, sodass sie zu Recht von der Zulässigkeit der Veröffentlichung ausgegangen war.

– In zunehmendem Maße sind auch die Verbände, Vereine und Parteien daran interessiert, ihre Arbeit im Internet darzustellen. Eine Vielzahl von mündlichen Anfragen betrafen die Frage nach der Zulässigkeit der *Veröffentlichung von Daten einzelner Mitglieder oder von Mitgliederlisten im Internet.*

Bewertung der Aufsichtsbehörde

Für die Zulässigkeit der Veröffentlichung von Mitgliederdaten im *Internet* gelten vom Grundsatz her dieselben datenschutzrechtlichen Bestimmungen wie für eine *sonstige Veröffentlichung*. Für eine zulässige Veröffentlichung von Daten einzelner Mitglieder oder von Mitgliederlisten kommen im Allgemeinen nur § 28 Abs. 1 Satz 1 Nr. 2 und Abs. 2 Satz 1 Nr. 1 b BDSG als Rechtsgrundlagen oder eine Einwilligung der Betroffenen in Betracht. Wegen der besonderen *Rücksichtnahmepflichten* des Vereins in Bezug auf die schutzwürdigen Belange seiner Mitglieder ist bei einer Veröffentlichung im Internet bei der erforderlichen Abwägung aber ein *strengerer Maßstab* anzulegen als bei der Bekanntgabe von Mitgliederdaten innerhalb des Vereins (vgl. Ziff. 10.2.1). Zu berücksichtigen ist zudem, dass eine wesentlich größere Anzahl von Personen von den Daten Kenntnis erlangen kann als bei internen Vereinspublikationen.

Soweit es bei den Veröffentlichungen um Informationen geht, die in engem *Zusammenhang* mit dem Verein stehen, kann die Bekanntgabe von Daten einzelner Mitglieder als zulässig angesehen werden, wenn keine überwiegenden schutzwürdigen Interessen der Mitglieder entgegenstehen, beispielsweise bei der Veröffentlichung von Daten der Mitglieder, die auch in anderen Medien genannt werden, also quasi öffentlich sind. Anders zu beurteilen sind jedoch Daten über Vereinsjubiläen von Mitgliedern oder von neu beigetretenen Mitgliedern, da denkbar ist, dass einzelne Mitglieder eine Bekanntgabe nicht wünschen. In solchen Fällen empfiehlt es sich, die Mitglieder generell oder im Einzelfall über die vorgesehene Bekanntmachung zu informieren und ihnen Gelegenheit zu geben, Einwände hiergegen vorzubringen. Diese sollten unabhängig von einer Interessenabwägung berücksichtigt werden.

Problematisch ist auch die Bekanntgabe von Daten aus dem *persönlichen Lebensbereich* der Mitglieder (etwa Angaben über runde Geburtstage, Eheschließungen, Geburt von Kindern, Abschluss von Schul- oder Berufsaus-

bildungen). Bei der Veröffentlichung solcher Daten, insbesondere im Internet, besteht ein Grund für die Annahme eines überwiegenden schutzwürdigen Interesses. Auch bei der Einstellung von Mitgliederlisten ins Internet ist in aller Regel davon auszugehen, dass schutzwürdige Belange einzelner Betroffener berührt sind. In den vorgenannten Fällen ist somit eine Einwilligung der Betroffenen zur Veröffentlichung ihrer Daten erforderlich. Diese *Einwilligung* sollte zur Absicherung und auch um den Betroffenen das Vorhaben nochmals deutlich vor Augen zu führen grundsätzlich schriftlich eingeholt werden.

10.2.4 Wahrung des Datengeheimnisses

Auch für die Vereinsdatenverarbeitung gilt das *Datengeheimnis* nach § 5 BDSG. Den mit der Verarbeitung der Mitgliederdaten betrauten Personen ist es demnach untersagt, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen, auch nach Beendigung dieser Tätigkeit. Hierzu sind entsprechende Verpflichtungserklärungen abzugeben.

Der Aufsichtsbehörde wurde ein Fall vorgetragen, in dem der Vorsitzende eines Bundesverbands von Selbsthilfegruppen, dem die Mitgliederverwaltung oblag, für sich Kopien der Mitgliederdaten gefertigt und diese nach seiner Abwahl und Austrittserklärung für private Zwecke verwendet hat.

Ergebnis der Überprüfung

Die weitere geschäftliche und private Nutzung der personenbezogenen Mitgliederdaten ist schlicht unzulässig. Das BDSG sieht für diesen datenschutzrechtlichen Verstoß aber keine Sanktionsmöglichkeit der Aufsichtsbehörde vor. Im angesprochenen Fall wurden die Daten vor der Verwendung gespeichert. Wer aber unbefugt durch das BDSG geschützte personenbezogene Daten, die nicht offenkundig sind, speichert, erfüllt den Straftatbestand des § 43 BDSG. Offenkundig sind Daten dann, wenn sie einer beliebig großen Anzahl von Menschen bekannt oder ohne Weiteres wahrnehmbar sind. Dies war vorliegend auszuschließen. Die Aufsichtsbehörde hat die Betroffenen auf die Rechtslage und die Möglichkeit, bei der Staatsanwaltschaft oder der Polizei Anzeige zu erstatten, hingewiesen. Das novellierte BDSG verbessert die Position der Aufsichtsbehörde, da ihr danach das Recht eingeräumt wird, Verstöße selbst bei den für die Verfolgung zuständigen Stellen anzuzeigen.

Anhang: Begriffsbestimmungen

Bannerwerbung

Als „Banner“ werden kleine Bildelemente auf dem Bildschirm bei einer Internetverbindung bezeichnet. Klickt der Nutzer auf das Banner, wird er sofort auf die Seite des Banneranbieters weitergeleitet. Banner werden häufig zu Werbezwecken eingesetzt (Werbebanner). Der Anbieter einer Internetseite erhält vom Banneranbieter einen Pfennigbetrag pro Nutzer, bei dem das Werbebanner eingeblendet wird oder der das Banner anklickt. Damit finanzieren sich viele für den Nutzer kostenlose Angebote im Internet.

Bonitätsprüfung

Bonitätsprüfungen werden von Unternehmen, die einem Kunden einen Geld- oder Warenkredit einräumen, vorgenommen, um die Zahlungsfähigkeit und -willigkeit und damit die Kreditwürdigkeit der Kunden vorab zu prüfen. Dazu werden insbesondere Anfragen bei Auskunfteien oder Kreditschutzorganisationen wie z. B. die SCHUFA durchgeführt. Diese sammeln und speichern Daten über Personen und Firmen, die über deren Zahlungsverhalten in der Vergangenheit Aufschluss geben (z. B. Angaben über Vollstreckungsmaßnahmen oder aus den Schuldnerverzeichnissen).

Browser

Der Browser ist ein Programm für die Bildschirmoberfläche, das zur Kommunikation für die Teilnahme am WWW-Dienst erforderlich ist. Der Browser wird auf dem PC installiert. Auf die WWW-Seiten des Internets kann durch die unmittelbare Eingabe der Internet-Adresse der gewünschten Seite bzw. der übergeordneten Startseite oder über so genannte Internet-Portale (z. B. Telediensteanbieter) zugegriffen werden.

Cookies

Cookies sind kleine Textdateien, die auf dem PC des Internet-Nutzers abgelegt werden. Cookies können von jedem Betreiber einer Internet-Seite eingespielt und ausgewertet werden. Der Datenaustausch erfolgt im Hintergrund zwischen PC und Internet-Server. Der Inhalt der Cookie-Datei und die Speicherdauer werden vom Betreiber der Internet-Seite bestimmt. In der Regel sind sie mit einem Verfallsdatum versehen, nach dessen Ablauf sie vom Browser selbstständig gelöscht werden.

Hyperlinks

Das Verweisen von einer auf eine andere Internet-Seite erfolgt mithilfe von Hyperlinks. Das Verweisen kann im Text oder durch speziell gekennzeichnete Verweisungen in einer gesonderten Rubrik erfolgen.

Listbroker

Entsprechend dem vom Werbekunden angeforderten Kundenprofil wählt er aus verschiedenen Adresslisten die dem Werbeprofil entsprechenden Kunden (z. B. Senioren mit Eigenheim in den Postleitzahlbereichen 6x, 7x und 8x) aus und stellt eine Adressliste zusammen, die er an den Werbekunden zur Nutzung vermietet. Im Regelfall erhält der Werbekunde die Liste nicht direkt, sondern nur die von ihm beauftragte Druckerei (Lettershop), die die Werbepost erstellt und versendet. Anhand des neben dem Adressfeld angebrachten Codes kann oftmals die Zusammensetzung der Liste beim Listbroker zurückverfolgt werden.

Mediendienste

Mediendienste sind an die Allgemeinheit gerichtete Informations- und Kommunikationsdienste. Dabei handelt es sich im Gegensatz zum Teledienst um rein redaktionell zum Abruf über das Internet gestaltete Seiten.

Routing

Das Routing versucht, die Nachrichten aus Netzauslastungsgründen möglichst optimal durch das Netzwerk zu senden. So kann es sein, dass ein Teil einer Nachricht von Stuttgart über Frankfurt nach Berlin gelangt, der andere Teil über die

Verbindung München nach Berlin. Am Empfangsort werden die einzelnen Nachrichtenteile wieder zusammengesetzt. Der Nutzer merkt davon nichts.

Scoring

Das Scoring ist ein Verfahren, in dem mit statistisch-mathematischen Methoden durch Auswertung eines vorhandenen Datenbestandes eine Punktzahl als Score-Wert ermittelt wird. Der Score-Wert stellt eine zusätzliche Entscheidungshilfe für Kreditgeber bei ihrer Entscheidung über eine Kreditvergabe dar. Zur Ermittlung des Score-Wertes werden Profile von Personengruppen erstellt, aus denen sich ableiten lässt, bei welcher Personengruppe mit einem bestimmten Datenbestand sich in der Vergangenheit welches Kreditausfallrisiko realisiert hat. Der Score-Wert ist also ein personengruppenbezogener Wert, der aussagt, mit welcher Wahrscheinlichkeit mit dem Eintreten eines Kreditausfalls bei einer bestimmten Personengruppe zu rechnen ist.

TCP/IP-Protokoll

Bei dem TCP/IP-Protokoll (TCP/IP = Transmission Control Protocoll / Internet Protocoll) handelt es sich um ein Netzwerkprotokoll, das für die Kommunikation in verzweigten Computer-Netzwerken zwischen Computern (u. a. Servern, PC-Netzwerke) mit verschiedenen Betriebssystemen (z. B. Unix, NT, Windows 2000) eingesetzt wird. *TCP/IP* umfasst Standards, die festlegen, wie Computer Daten austauschen, sowie Regeln für das Verbinden von Netzwerken und das Leiten des Datenverkehrs.

Teledienste

Teledienste sind Angebote zur Information und Kommunikation, soweit nicht die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht. Während es sich beim Anwendungsbereich des Mediendienstes um das Angebot und die Nutzung von an die Allgemeinheit gerichteten Informationsdiensten handelt, beziehen sich die Teledienste auf die individuelle Nutzung von Informations- und Kommunikationsdiensten (z. B. Internet-Dienste, E-Mail).

Webhosting

Für Privatleute, Vereine oder kleinere Unternehmen ist es wirtschaftlich nicht sinnvoll, einen eigenen Web-Server ständig im Internet zu betreiben. Hierfür haben sich Firmen etabliert, die einen entsprechenden Web-Speicherplatz mit zusätzlichen Internet-Diensten (z. B. E-Mailing, Gestaltung der Web-Seite, Anmeldung des Domain-Namens u. a. bei DENIC) anbieten. Das Anbieten dieses Dienstes wird Webhosting genannt.