Aufsichts- und Dienstleistungsdirektion

Rheinland-Pfalz

Erster

Tätigkeitsbericht

über den Datenschutz

im nicht-öffentlichen Bereich

Erster Tätigkeitsbericht

der Aufsichts- und Dienstleistungsdirektion

als Aufsichtsbehörde für den Datenschutz im

nicht-öffentlichen Bereich in

Rheinland-Pfalz

für den Zeitraum vom 01. Juni 2001
bis zum 31. Mai 2003

(abrufbar über das Internet unter: http://www.add.rlp.de)

Herausgeber:

Aufsichts- und Dienstleistungsdirektion (ADD)
Willy-Brandt-Platz 3

54290 Trier

Tel.: 0651/9494-0
Fax: 0651/9494-170
E-Mail: poststelle@add.rlp.de
www.add.rlp.de

Inhaltsverzeichnis

Vorwort 5

I. Allgemeiner Teil

1 Organisation des Datenschutzes in Rheinland-Pfalz 6

2 Auswirkung des geänderten Bundesdatenschutzgesetzes auf die Aufgaben der Aufsichtsbehörde 7

3 Das Melderegister 9
3.1 Register der meldepflichtigen Stellen 9
3.2 Die Neuregelung der Meldepflicht 10

4 Überprüfungen im Rahmen der Regelaufsicht 12

5 Eingaben und Beschwerden 15

6 Anfragen und Auskünfte / Beratungen 17

7 Ordnungswidrigkeitsverfahren 18

8 Informationsveranstaltung 19

II. Einzelfälle aus der Praxis der Aufsichtsbehörde

1 Neue Medien / Internetanbieter 20
1.1 Fehlende Anbieterkennzeichnung bei Tele- und Mediendiensten 20
1.2 Werbung im Internet 21
1.3 Verwendung von Personalausweis-Nummern bei der Registrierung von Internet-Nutzern durch Access-Provider 24
1.4 Versendung von Kundendaten durch Provider 25

2 Handel / Auskunfteien / Inkasso-Unternehmen 25
2.1 Kopieren von Ausweisdokumenten bei Abschluss eines Beherbergungsvertrages 25
2.2 Geschäftsgeheimnis als Grund für die Verweigerung einer Auskunft 26
2.3 Verletzung von Persönlichkeitsrechten und Nichterteilung von Auskünften 27

3	Wohnen und Liegenschaften		29
	3.1	Die Eigentümergemeinschaft	29
	3.2	Mieterfragebögen	29
	3.3	Luftbildaufnahmen von Gebäuden und Grundstücken	30
4	Arbeitnehmerdatenschutz		31
	4.1	Sicherheit	32
	4.2	Streit im Betrieb	32
	4.3	Schwangerschaft	33
	4.4	Das schwarze Brett	33
	4.5	Betriebsausweise	34
	4.6	Der Systemadministrator	34
	4.7	„Datenhunger“ von Behörden	35
	4.8	Betriebliche Altersvorsorge	35
5	Datenschutz und Medizin		36
	5.1	Erteilung von Auskünften an Krankenversicherungen und Kassenärztliche Vereinigungen	37
	5.2	Die eigene Krankengeschichte	37
	5.3	Einsichtsrecht psychisch Kranker	37
	5.4	Die private Krankenversicherung	38
	5.5	Sanitätshäuser	38
	5.6	Kontrolle von Verordnungen	39
6	Videoüberwachung		39
7	Der betriebliche Datenschutzbeauftragte		40
8	Datenschutz in Vereinen		41
	8.1	Zentral- und Gliedverband	41
	8.2	Der Datenschutzbeauftragte im Verein	42
	8.3	Zweckbindung der Datenverarbeitung	42
9	Internationaler Datenverkehr		42
10	Werbung		43
11	Schlusswort		44

Vorwort

Mit Inkrafttreten des novellierten Bundesdatenschutzgesetzes (BDSG) am 23. Mai 2001 wurde den Aufsichtsbehörden für den Datenschutz erstmals gesetzlich aufgegeben, regelmäßig, spätestens alle zwei Jahre, einen Tätigkeitsbericht zu veröffentlichen.

Dieser erste Tätigkeitsbericht der Aufsichts- und Dienstleistungsdirektion (ADD) als zuständige Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich in Rheinland-Pfalz gibt einen Überblick über die wesentlichen Änderungen des Bundesdatenschutzgesetzes und informiert über die im Zeitraum vom 01. Juni 2001 bis 31. Mai 2003 wahrgenommenen Aufgaben und durchgeführten datenschutzrechtlichen Kontrollen.

Trier, im Oktober 2003

Dr. Josef Peter Mertes
Präsident

I. Allgemeiner Teil

1. Organisation des Datenschutzes in Rheinland-Pfalz

Die Aufsicht über den Datenschutz ist in Rheinland-Pfalz zweigeteilt.

Während die Aufsicht über den Datenschutz im öffentlichen Bereich dem Landesbeauftragten für den Datenschutz obliegt, ist das rheinland-pfälzische Ministerium des Innern und für Sport oberste Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich.

Seit dem 01. Januar 2000 ist die im Rahmen der Reform und Neuorganisation der Landesverwaltung neu entstandene Aufsichts- und Dienstleistungsdirektion (ADD) mit Hauptsitz in Trier die nach § 38 Bundesdatenschutzgesetz (BDSG) i.V.m. § 1 der Landesverordnung über Zuständigkeiten nach dem BDSG landesweit zuständige Behörde für die Aufsicht über den Datenschutz im nicht-öffentlichen Bereich in Rheinland-Pfalz.

Als obere Landesbehörde ist die ADD gemäß § 2 Abs. 1 Satz 1 des Landesgesetzes zu dem Mediendienste-Staatsvertrag vom 18.07.1997 (GVBl. S. 235), zuletzt geändert durch § 4 des Gesetzes vom 06.03.2003 (GVBl. S. 24) BS Anhang I 117, grundsätzlich auch zuständig für die Einhaltung der Bestimmungen des Mediendienste-Staatsvertrages (MDSV) sowie für die Verfolgung und Ahndung von Ordnungswidrigkeiten, mit Ausnahme der besonderen Regelungen für den Bereich des Jugendmedienschutzes und die Kontrolle der Beachtung der Datenschutzvorschriften bei öffentlichen Stellen.

Daneben ist die ADD zuständige Behörde für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 12 des Teledienstegesetzes (TDG) und § 9 des Teledienstedatenschutzgesetzes (TDDSG).

Weitere Informationen zur ADD und deren Zuständigkeiten sind im Internet unter www.add.rlp.de abrufbar.

2. Auswirkung des geänderten Bundesdatenschutzgesetzes auf die Aufgaben der Datenschutzaufsichtsbehörden

Mit Inkrafttreten des novellierten Bundesdatenschutzgesetzes am 23. Mai 2001 wurden den Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich zusätzliche Aufgaben übertragen und deren Befugnisse erweitert. Im Folgenden soll ein kurzer Überblick über einige wesentlichen Änderungen, soweit sie sich auf nicht-öffentliche Stellen beziehen, gegeben werden:

Nach § 38 Abs. 1 Satz 1 Bundesdatenschutzgesetz kontrollieren die Aufsichtsbehörden die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht-automatisierten Dateien regeln, einschließlich des Rechts der Mitgliedsstaaten in den Fällen des § 1 Abs. 5 BDSG.

Die Aufsichtsbehörden haben nunmehr generell das Recht, anlassunabhängige Kontrollen durchzuführen. Die Möglichkeit, im Rahmen der Initiativaufsicht solche anlassunabhängigen Kontrollen durchzuführen, war bis zur Novellierung des BDSG nur auf den Bereich der Auskunfteien, Adresshandelsunternehmen, Markt- und Meinungsforschungsinstitute sowie Auftragsdatenverarbeiter beschränkt (§ 38 Abs. 2 BDSG a.F.). In allen anderen Fällen war eine Überprüfung nur möglich, wenn der Aufsichtsbehörde hinreichende Anhaltspunkte (z.B. durch Eingaben betroffener Personen) für eine Verletzung datenschutzrechtlicher Vorschriften durch nicht-öffentliche Stellen vorlagen (§ 38 Abs. 1 BDSG a.F.).

Ungeachtet dessen waren die im Berichtszeitraum durchgeführten datenschutzrechtlichen Überprüfungen in der Mehrzahl der Fälle anlassabhängig, da sowohl berechtigte Eingaben Betroffener, Hinweise Dritter als auch eigene Erkenntnisse ein Einschreiten der Aufsichtsbehörde erforderlich machten. Die Art und Schwere der festgestellten Verstöße sowie die im Rahmen der Überprüfung gewonnenen eigenen Erkenntnisse entschieden darüber, wie vor dem Hintergrund der erweiterten Sanktionsmöglichkeiten weiter verfahren wurde. Neben

einer Erweiterung der in § 43 aufgeführten Bußgeldtatbestände wird den Aufsichtsbehörden nunmehr in § 44 Abs. 2 BDSG bei Feststellung besonderes schwerer Verstöße gegen geltendes Datenschutzrecht ein eigenes Strafantragsrecht eingeräumt. Bislang war jedoch keiner der festgestellten Verstöße so schwerwiegend, dass ein Strafantrag gestellt werden musste.

In § 1 Abs. 5 BDSG wird nunmehr ausdrücklich die Anwendbarkeit des BDSG in den Fällen geregelt, in denen verantwortliche ausländische Stellen in Deutschland personenbezogene Daten erheben, verarbeiten oder nutzen.
Danach kommt das BDSG immer zur Anwendung, wenn eine in einem anderen Mitgliedstaat der Europäischen Union bzw. in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) oder in einem Drittstaat belegene verantwortliche Stelle in Deutschland personenbezogene Daten erhebt, verarbeitet oder nutzt und dies ausschließlich durch eine in Deutschland ansässige Niederlassung erfolgt (Territorialprinzip). Werden Daten direkt durch eine im Ausland belegene verantwortliche Stelle erhoben und dort verarbeitet, ist zu unterscheiden, ob die verantwortliche Stelle ihren Sitz in einem EU/EWR-Staat oder einem Drittstaat hat. Erfolgt die Datenerhebung und weitere Verarbeitung unmittelbar durch eine verantwortliche Stelle mit Sitz in einem EU-Mitgliedstaat bzw. einem Mitgliedstaat des EWR, geht das BDSG nunmehr, die EG-Datenschutzrichtlinie (Richtlinie 95/46/EG) umsetzend, vom Vorliegen eines einheitlichen Datenschutzniveaus in diesen Staaten aus. In diesen Fällen ist anstelle des BDSG das Recht der jeweiligen Mitgliedstaaten anzuwenden. Hat die datenerhebende bzw. -verarbeitende Stelle ihren Sitz jedoch in einem Drittstaat, findet bei Datenerhebungen und -verarbeitungen in Deutschland ausschließlich das BDSG Anwendung.

Neu ist ebenfalls der in § 3a BDSG formulierte Grundsatz der Datenvermeidung und Datensparsamkeit. Danach haben sich Gestaltung und Auswahl von Datenverarbeitungssystemen an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist, sofern möglich und angemessen, von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen.

Zusätzliche Aufgaben ergeben sich ferner aus § 4c Abs. 2 BDSG, wonach die Aufsichtsbehörden Datenübermittlungen in Staaten außerhalb der Europäischen Union und des Europäischen Wirtschaftsraumes zu genehmigen haben, in denen kein angemessenes Datenschutzniveau besteht und die Ausnahmetatbestände des § 4c Abs. 1 BDSG nicht erfüllt sind. Der Aufsichts- und Dienstleistungsdirektion (ADD) wurden im Berichtszeitraum keine diesbezüglichen Anträge auf Genehmigung vorgelegt.

Hauptaufgabe der Aufsichtsbehörde war und wird auch zukünftig die Durchführung datenschutzrechtlicher Prüfungen sowie die Beratung und Information der verantwortlichen Stellen sein. Vor allem im letztgenannten Bereich ist im Berichtszeitraum eine stetige Zunahme der entsprechenden Anfragen zu verzeichnen gewesen.

3. Das Melderegister

3.1 Register der meldepflichtigen Stellen (§ 32 Abs. 2 BDSG a.F.)

Mit der Auflösung der ehemaligen Bezirksregierungen wurden die bis zum 31.12.1999 jeweils gem. § 38 Abs. 2 BDSG a.F. geführten Register der meldepflichtigen Stellen bei der ADD zusammengeführt.

Zu Beginn des Berichtszeitraumes waren noch insgesamt 159 Stellen, die gem. § 32 Abs. 1 Nr. 1 bis 3 BDSG a.F. personenbezogene Daten geschäftsmäßig zum Zwecke der personenbezogenen Übermittlung bzw. der anonymisierten Übermittlung speichern bzw. im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen, gemeldet.

Von den gemeldeten 159 Stellen waren:

- 20 Stellen, die Daten zum Zwecke der Übermittlung speichern (Auskunfteien und Adresshandelsunternehmen), § 32 Abs. 1 Nr. 1 BDSG a.F.,

- 2 Stellen, die Daten zum Zwecke der anonymisierten Übermittlung speichern (Markt- und Meinungsforschungsinstitute), § 32 Abs. 1 Nr. 2 BDSG a.F., sowie

- 137 Stellen, die Auftragsdatenverarbeitung betrieben haben (Konzern- und Dienstleistungsrechenzentren, Akten- und Datenträgervernichter, Datenerfassungsbetriebe, Schreibdienste, Lettershops, Direktmarketingunternehmen, usw.), § 32 Abs. 1 Nr. 3 BDSG a.F..

3.2 Die Neuregelung der Meldepflicht (§ 4d BDSG n.F.)

Die Neuregelung der Meldepflicht führte zu einer grundlegenden Änderung des Melderegisters. § 4d Abs. 1 BDSG sieht als Grundsatz vor, dass Verfahren automatisierter Verarbeitungen vor ihrer Inbetriebnahme von den nichtöffentlichen verantwortlichen Stellen der Aufsichtsbehörde zu melden sind. Danach muss ein Unternehmen alle zur Anwendung kommenden Verfahren, die eine Verarbeitung personenbezogener Daten zum Gegenstand haben, jeweils einzeln melden.

Die Meldepflicht entfällt, wenn die verantwortliche Stelle einen betrieblichen Datenschutzbeauftragten bestellt hat (§ 4d Abs. 2 BDSG). Die Meldepflicht entfällt ferner, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei höchstens vier Arbeitnehmer mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt und entweder eine Einwilligung der Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder eines vertragsähnlichen Vertrauensverhältnisses mit den Betroffenen dient (§ 4d Abs. 3 BDSG).

Ungeachtet dieser Ausnahmeregelung bleiben nach § 4d Abs. 4 BDSG weiterhin alle Stellen meldepflichtig, die personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung oder zum Zwecke der anonymisierten Übermittlung speichern (§§ 29, 30 BDSG). Dies betrifft somit alle Handels- und Wirt-

schaftsauskunfteien, Adresshandelsunternehmen sowie Markt- und Meinungsforschungsinstitute.

Gleichzeitig mit der Meldepflicht hat sich der Inhalt der gegenüber der Aufsichtsbehörde abzugebenden Meldungen verändert. Beinhalteten die bisherigen Meldungen zum Register überwiegend Angaben zur meldepflichtigen Stelle, wie z.B. Name, Anschrift, Inhaber oder Geschäftsführer, zum Geschäftszweck der Stelle und der Datenverarbeitung, zum betrieblichen Datenschutzbeauftragten und zur Art der Datenverarbeitungsanlagen, müssen die meldepflichtigen Stellen nun gem. § 4e Nr. 9 BDSG zusätzlich konkrete Angaben über die nach § 9 BDSG getroffenen technischen und organisatorischen Schutzmaßnahmen machen. Diese zusätzlichen detaillierten Angaben sind gemäß § 38 Abs. 2 Satz 3 BDSG nur für die Aufsichtsbehörden bestimmt, so dass sich das für jedermann bestehende Einsichtsrecht in das nun nach § 38 Abs. 2 Satz 1 zu führende Register lediglich auf die Angaben nach § 4e Satz 1 Nr. 1 – 8 BDSG bezieht.

Angesichts dieser Neuregelungen war es erforderlich, alle bisher im Register der meldepflichtigen Stellen eingetragenen Unternehmen auf ihre weitere Meldepflicht hin zu überprüfen. Zunächst wurden alle diejenigen Unternehmen, die aus Sicht der Aufsichtsbehörde weiterhin meldepflichtig waren (Auskunfteien, Warndienste, Adresshandelsunternehmen, Markt- und Meinungsforschungsinstitute), angeschrieben und um Überprüfung ihrer Meldepflicht gebeten. Danach wurden alle Unternehmen, die gem. § 32 Abs. 2 Nr. 3 BDSG a.F. Auftragsdatenverarbeitung betreiben, schriftlich über den Wegfall der Meldepflicht informiert und aus dem Register gestrichen. Dadurch reduzierte sich die Anzahl der meldepflichtigen Unternehmen erheblich.

Aktuell sind zum Register der meldepflichtigen Stellen gemeldet:

- 22 Stellen, die geschäftsmäßig Daten zum Zwecke der Übermittlung speichern (§ 29 BDSG), sowie

- 2 Stellen, die geschäftsmäßig Daten zum Zwecke der anonymen Übermittlung speichern (§ 30 BDSG).

Im Zusammenhang mit der Überprüfung der Meldepflicht der einzelnen verantwortlichen Stellen ist das bisher manuell geführte Register nun auf ein entsprechendes automatisiertes Verfahren umgestellt worden.

4. Überprüfungen im Rahmen der Regelaufsicht

Im Berichtszeitraum wurden insgesamt sechs Handels- und Wirtschaftsauskunfteien und ein Adresshandels-Unternehmen einer datenschutzrechtlichen Überprüfung unterzogen.

Gegenstand der Prüfungen bei den Auskunfteien waren neben einer Besichtigung der Geschäftsräume (Räumlichkeiten, Arbeitsplätze, EDV-Einrichtungen) unter anderem

- die Fachkunde und Zuverlässigkeit der betrieblichen Datenschutzbeauftragten (§ 4f BDSG),
- die Ausführung der den betrieblichen Datenschutzbeauftragten gemäß § 4g BDSG übertragenen Aufgaben,
- das von der verantwortlichen Stelle zu erstellende Verfahrensverzeichnis (§ 4g Abs. 2 BDSG),
- die Verpflichtung der Mitarbeiter auf das Datengeheimnis (§ 5 BDSG),
- die Überprüfung des dargelegten berechtigten Interesses bei Datenübermittlungen nach § 29 Abs. 2 Nr. 1a BDSG,
- die Beachtung der Erfordernisse für automatisierte Abrufverfahren gem. § 10 BDSG,
- die Trennung des Inkassobereiches vom Auskunfteibereich und
- die getroffenen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten gem. § 9 BDSG.

Im Ergebnis bleibt festzuhalten, dass keine der überprüften Auskunfteien das nach § 4g Abs. 2 BDSG geforderte Verfahrensverzeichnis erstellt und den betrieblichen Datenschutzbeauftragten zur Verfügung gestellt hat. Demzufolge war es den betrieblichen Datenschutzbeauftragten auch nicht möglich, die darin enthaltenen Angaben für jedermann in geeigneter Weise verfügbar zu machen. Den Verantwortlichen wurde aufgegeben, das Verfahrensverzeichnis unverzüglich zu erstellen und den betrieblichen Datenschutzbeauftragten zur weiteren Veranlassung zu überlassen.

Eine Auskunftei wurde aufgrund einer eingegangenen anonymen Anzeige einer unangemeldeten datenschutzrechtlichen Kontrolle unterzogen. Dabei wurden einzelne Mängel hinsichtlich der Beachtung der datenschutzrechtlichen Anforderungen festgestellt. So wurde z. B. ein nur durch ein Fahrradschloss gesicherter „Verschlag“ im Untergeschoss der zum Geschäftshaus gehörenden und frei zugänglichen Tiefgarage als Lagerplatz für abgeschlossene Inkasso-Fälle genutzt. Die Unterlagen lagerten in offenen Umzugskartons und waren nach Angaben des Prokuristen „schlicht und einfach“ dort vergessen worden. Den Verantwortlichen wurde aufgegeben, die Unterlagen umgehend aus diesem Verschlag zu entfernen und – sofern die gesetzlichen Aufbewahrungsfristen abgelaufen waren – der ordnungsgemäßen Vernichtung zuzuführen. Des Weiteren wurde wegen eines Verstoßes gegen § 43 Abs. 1 Nr. 1 BDSG ein Bußgeldverfahren eingeleitet.

Erhebliche Mängel in Bezug auf die gemäß § 9 BDSG zu treffenden Schutzmaßnahmen waren bei einer weiteren durchgeführten unangemeldeten Kontrolle einer anderen Auskunftei zu verzeichnen. Das Unternehmen wurde überprüft, nachdem deren betriebliche Datenschutzbeauftragte es seit Juni 2001 versäumt hatte, die von der Aufsichtsbehörde geforderte Neuanmeldung zum Register der meldepflichtigen Stellen abzugeben. Bereits beim Betreten der Geschäftsräume war erkennbar, dass die EDV-Anlage nicht in einem ausreichend geschützten Raum, sondern in einer ca. 1,5 qm großen Abstellkammer untergebracht ist, deren Tür bedingt durch deren bauliche Anordnung sowie einer fehlenden Klimaanlage nicht geschlossen werden konnte. So hatten Besucher beim Betreten der Geschäftsräume Zugang zu dieser Anlage und wie jeder Mit-

arbeiter die Möglichkeit, in einem unbeachteten Moment die Anlage abzuschalten oder Datenträger an sich zu nehmen. Eine Notstromversorgung für den Betrieb des Rechners sowie eine Alarmanlage zum Schutz der Geschäftsräume waren aus Kostengründen nicht installiert worden. Die Überprüfung dieser Auskunftei war bis zum Ende des Berichtszeitraumes noch nicht abgeschlossen.

Voraussetzung für die Übermittlung personenbezogener Daten durch eine Auskunftei an einen Kunden ist ein berechtigtes Interesse des Datenempfängers an der Kenntnis dieser Daten (§ 29 Abs. 2 Nr. 1a BDSG). Zur Darlegung des berechtigten Interesses muss die anfragende Stelle der Auskunftei jeweils den Grund für die Anfrage mitteilen. Die Auskunfteien haben das Vorliegen des berechtigten Interesses der anfragenden Stellen zu dokumentieren und stichprobenartig zu überprüfen. Dazu übersenden die Auskunfteien entsprechend der mit dem Düsseldorfer Kreis (Gremium der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich) getroffenen Regelung, wonach in zwei von tausend Fällen eine umfassende Überprüfung der Auskunftserteilung zu erfolgen hat, ihren Kunden ein Formblatt, in dem substantiierte Angaben zum berechtigten Interesse gemacht werden müssen. Im Rahmen der durchgeführten datenschutzrechtlichen Überprüfungen wurde bei allen Auskunfteien Einsicht in die Dokumentationen genommen. Dabei wurde u.a. festgestellt, dass anfragende Stellen häufig das berechtigte Interesse an einer Auskunft mit „Geschäftsanbahnung“ bzw. „Bonitätsprüfung“ begründeten. Zwei der überprüften Auskunfteien sahen nach Erhalt solcher Begründungen keine Notwendigkeit, entsprechende weitere Nachfragen zu stellen bzw. weitere Unterlagen anzufordern und gaben sich mit dieser Begründung zufrieden. Aus Sicht der Aufsichtsbehörde genügt dies nicht den Anforderungen an die Überprüfung des berechtigten Interesses, da Auskunfteien eine substantielle Überprüfung des berechtigten Interesses ihrer Kunden durchzuführen haben. Dies wurde entsprechend bemängelt und die betreffenden wurden Auskunfteien aufgefordert, künftig in diesen Fällen entsprechende schriftliche Unterlagen anzufordern, die das berechtigte Interesse für die Anfrage belegen.

Alle Auskunfteien betreiben neben ihrer eigentlichen Tätigkeit – der Erteilung von Bonitätsauskünften über Unternehmen und Privatleute – einen Inkasso-

dienst. In jeder der geprüften Auskunfteien befindet sich zu diesem Zweck ein separater Bereich, in dem nur Mitarbeiter beschäftigt sind, die nicht gleichzeitig mit der Wahrnehmung auskunfteispezifischer Tätigkeiten betraut sind. Die Inkasso-Akten werden, wie festgestellt, mehrheitlich in Räumen aufbewahrt, zu denen alle Mitarbeiter der Auskunftei Zugang haben. Ferner wurde festgestellt, dass Daten aus dem Inkasso-Bereich an den Auskunfteibereich übermittelt und bei der Berechnung des Bonitätsindex mit berücksichtigt werden. Da es sich bei den Bereichen Inkasso und Auskunftei um zwei selbständige Bereiche handelt, ist zwischen Aufsichtsbehörden und Auskunfteien die Frage umstritten, unter welchen Voraussetzungen Negativdaten aus dem Inkasso-Bereich an den Auskunftei-Bereich übermittelt werden dürfen. Dabei sind die berechtigten Interessen der Auskunftei und potentieller Gläubiger gegen die schutzwürdigen Interessen der Schuldner abzuwägen (§§ 28 Abs. 3 Nr. 1, 29 Abs. 1 Nr. 1 BDSG). Es wurde jeweils versichert, dass nur Angaben über berechtigte Forderungen bzw. abgeschlossene Inkasso-Verfahren (sog. harte Negativdaten) an den Auskunftei-Bereich weitergemeldet werden.

5. Bearbeitung von Eingaben und Beschwerden

Im Berichtszeitraum wurden insgesamt 119 Eingaben und Beschwerden bearbeitet. Statistisch erfasst wurden dabei nur die Fälle, die aktenmäßig bearbeitet wurden. Es handelte sich in der überwiegenden Zahl der Fälle um konkrete Beschwerden betroffener Personen, um Hinweise auf vermeintliche Datenschutzverstöße sowie um eigene Feststellungen.

Nicht enthalten in dieser Fallzahl sind die Eingaben und Beschwerden, die aufgrund der Unzuständigkeit der Aufsichts- und Dienstleistungsdirektion an den Bundesbeauftragten für den Datenschutz oder an Aufsichtsbehörden anderer Bundesländer abgegeben wurden.

In den 119 bearbeiteten Fällen richteten sich die Beschwerden

- in 19 Fällen gegen Anbieter geschäftsmäßiger Tele- und Mediendienste,

- in 15 Fällen gegen Finanz- und sonstige Dienstleistungsunternehmen,
- in 11 Fällen gegen Internetanbieter (Provider),
- in 11 Fällen gegen verantwortliche Stellen im Gesundheitswesen,
- in 9 Fällen gegen Groß- und Einzelhandelsunternehmen,
- in 8 Fällen gegen Handels- Wirtschaftsauskunfteien / Warndienste,
- in 6 Fällen gegen Versicherungsunternehmen,
- in 5 Fällen gegen Werbe- und Direktmarketingunternehmen,
- in 5 Fällen gegen Kreditinstitute,
- in 5 Fällen gegen Inkasso-Unternehmen,
- in 5 Fällen gegen Arbeitgeber,
- in 5 Fällen gegen Zeitungs- und Zeitschriftenverlage,
- in 4 Fällen gegen Unternehmen der Freizeit- und Tourismusbranche,
- in 3 Fällen gegen die Videoüberwachung von Grundstücken,
- in 2 Fällen gegen Versandhandelsunternehmen,
- in 2 Fällen gegen Wohnungsunternehmen und Vermieter,
- in 2 Fällen gegen Vereine und
- in 2 Fällen gegen Parteien.

In etwa 30 % der genannten Fälle sind unzulässige Datenverarbeitungen bzw. andere Verstöße gegen datenschutzrechtliche Bestimmungen festgestellt worden.

Im Rahmen der Bearbeitung der Eingaben und Beschwerden wurden in einer Reihe von Fällen teilweise unangemeldete Vor-Ort-Kontrollen vorgenommen. Die betroffenen verantwortlichen Stellen reagierten entweder über längere Zeit hinweg nicht auf Schreiben der Aufsichtsbehörde, oder der Sachverhalt konnte auf schriftlichem Wege nicht geklärt werden. In einigen wenigen Fällen bestand im Übrigen die Befürchtung, dass die beanstandeten Verstöße bei einer angemeldeten Vor-Ort-Kontrolle nicht mehr hätten festgestellt werden können.

6. Anfragen und Auskünfte / Beratungen

Im Berichtszeitraum wurden von der Aufsichtsbehörde insgesamt 53 schriftliche und 61 telefonische Anfragen von Bürgern, Gewerbetreibenden, Unternehmen, Vereinen und Verbänden beantwortet.

Einen Schwerpunkt der Anfragen bildeten die gesetzlichen Anforderungen zur datenschutzgerechten Ausgestaltung von Tele- und Mediendiensten. Dabei wurden Fragen zur Form und Platzierung der gesetzlich geforderten Anbieterkennzeichnung (§ 6 Teledienstegesetz, § 10 Mediendienste-Staatsvertrag) auf Internetseiten beantwortet und Empfehlungen zur Ausgestaltung von Datenschutzhinweisen ausgesprochen. Daneben wurden die von den Diensteanbietern ausgearbeiteten Unterrichtungen der Nutzer von Telediensten (§ 4 TDDSG) datenschutzrechtlich überprüft.

Vielfach sind von Arbeitgebern und Arbeitnehmern Fragen zum Datenschutz im Arbeitsverhältnis an die Aufsichtsbehörde herangetragen worden. Hier wurden insbesondere Fragen zur Übermittlung von Arbeitnehmerdaten ins Ausland (Konzerndatenverarbeitung), zur privaten Internetznutzung am Arbeitsplatz bis hin zur Videoüberwachung von Geschäfts- und Betriebsräumen beantwortet.

Von Betrieben und betrieblichen Datenschutzbeauftragten sind in einer Reihe von Fällen auch Fragen zur Neuregelung der Meldepflicht, der Pflicht zur Bestellung betrieblicher Datenschutzbeauftragter oder dem zu erstellenden Verfahrensverzeichnis an die Aufsichtsbehörde herangetragen worden.

Weitere Anfragen betrafen Fragen zum Datenschutz in Verbänden und Vereinen, in Arztpraxen, zur Tätigkeit von Handels- und Wirtschaftsauskunfteien oder zu geplanten Videoüberwachungen.

7. Bußgeldverfahren

In einer Reihe von Fällen haben sich die verantwortlichen Stellen erst aufgrund der Androhung eines Bußgeldes veranlasst gesehen, der Aufsichtsbehörde gegenüber die erforderlichen Auskünfte zu erteilen. Da einige Firmen trotz Androhung eines Bußgeldes der ihnen gem. § 38 Abs. 3 Satz 1 BDSG obliegenden Auskunftspflicht nicht nachkamen, wurde in diesen Fällen ein Verfahren nach dem Gesetz über Ordnungswidrigkeiten eingeleitet.

Im Einzelnen wurden

- in sechs Fällen wegen eines Verstoßes gegen § 43 Abs. 1 Nr. 10 BDSG (Auskunftspflicht) und
- in einem Fall wegen eines Verstoßes gegen § 43 Abs. 1 Nr. 2 (Nichtbestellung eines betrieblichen Datenschutzbeauftragten) und eines Verstoßes gegen § 43 Abs. 1 Nr. 10 BDSG

ein Bußgeld verhängt.

Keines der Bußgeldverfahren war bis zum Ende des Berichtszeitraumes abgeschlossen.
Von drei – teilweise schon seit Anfang 2002 – vor Gericht anhängigen Verfahren sind zwei bislang noch nicht terminiert worden. In einem weiteren Verfahren wurde die Rechtsauffassung der Aufsichtsbehörde durch das zuständige Amtsgericht bestätigt, die Höhe des verhangenen Bußgeldes aber verringert; die Entscheidung ist noch nicht rechtskräftig. Die übrigen Bußgeldbescheide erlangten Bestandskraft und befanden sich zum Ende des Berichtszeitraumes noch in der Vollstreckung.

Über den Ausgang der Verfahren wird im nächsten Tätigkeitsbericht berichtet werden.

8. Informationsveranstaltung zum „Datenschutz in der Arztpraxis“

Auf Initiative der Aufsichts- und Dienstleistungsdirektion (ADD) lud die Bezirksärztekammer Trier ihre Mitglieder im Herbst 2002 zu einer Informationsveranstaltung zum Thema „Datenschutz in der Arztpraxis“ ein.

Im Rahmen dieser Veranstaltung informierte die Vertreterin der ADD die anwesende Ärzteschaft unter anderem über die Grundzüge des novellierten Bundesdatenschutzgesetzes, der Pflicht zur Bestellung betrieblicher Datenschutzbeauftragten sowie über einen datenschutzgerechten Umgang mit Patientenunterlagen einschließlich deren Aufbewahrung. Die Teilnehmer nutzten die Möglichkeit, um in der Praxis aufgetretene Probleme mit der Aufsichtsbehörde zu schildern und nach Lösungsmöglichkeiten zu fragen.

II. Einzelfälle aus der Praxis der Aufsichtsbehörde

1. Neue Medien / Internetanbieter

1.1 Fehlende Anbieterkennzeichnung bei Tele- und Mediendiensten

Mehrere Beschwerden richteten sich im Berichtszeitraum gegen die Betreiber von Mediendiensten und geschäftsmäßigen Telediensten, die bei ihren Internetauftritten ihren Informationspflichten nicht oder nicht ausreichend nachgekommen waren. Beschwerdeführer waren neben Privatpersonen auch Rechtsanwälte, die aufgrund eigener Feststellungen oder im Auftrag ihrer Mandanten die fehlende Anbieterkennzeichnung zur Anzeige brachten.

Da für den jeweiligen Nutzer erkennbar sein muss, mit welchen natürlichen oder juristischen Personen er es auf Seiten der Diensteanbieter zu tun hat, sind diese nach den einschlägigen Bestimmungen des Teledienstegesetzes (TDG) und des Mediendienste-Staatsvertrages (MDSV) verpflichtet, entsprechende Angaben zu machen, die leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sein müssen (z.B. durch ein Impressum auf der Homepage oder einen Verweis auf das Impressum auf jeder Web-Seite oder auf der Homepage). Es ist keinesfalls ausreichend, nur den Namen eines Verantwortlichen ohne dessen Anschrift oder einen Verantwortlichen in den AGB zu benennen. Ein Verstoß gegen die Verpflichtung zur Anbieterkennzeichnung stellt eine Ordnungswidrigkeit dar, die mit einer Geldbuße von bis zu 50.000 Euro geahndet werden kann.

In den überprüften Fällen wurden die Domaininhaber angeschrieben und auf die fehlende oder unvollständige Anbieterkennzeichnung hingewiesen. Gleichzeitig erging eine Aufforderung, die Internetseiten um die fehlenden Angaben zu ergänzen. Da die Betroffenen dieser Aufforderung binnen der gesetzten Frist nachkamen, wurde bislang von der Verhängung von Bußgeldern abgesehen. Ferner zeigte sich, dass es immer noch Firmen gibt, die Internetauftritte für Unternehmen erstellen und dabei keine Kenntnis von den Bestimmungen des TDG

oder des MDSV haben. In diesem Zusammenhang ist von Seiten der Aufsichtsbehörde regelmäßig auf die „Orientierungshilfe Tele- und Mediendienste“ des Hamburgischen Datenschutzbeauftragten hingewiesen worden, die im Internet unter www.datenschutz-hamburg.de abrufbar ist.

Seit Ende 2002 steht der Aufsichtsbehörde zudem ein Prüftool zur Verfügung, welches es ermöglicht, auch große und komplexe Internetangebote umfassend auf eine Vielzahl von datenschutzrelevanten Aspekten hin zu analysieren. Dazu werden die jeweiligen Seiten auf einen Prüfserver geladen und dort einer automatischen Überprüfung unterzogen. Die Ergebnisse werden anschließend von einem Prüfer bewertet und ggf. durch weitere Funde und Aussagen ergänzt.

1.2 Werbung im Internet

Im Berichtszeitraum häuften sich die Beschwerden von Betroffenen über den Erhalt unverlangter eMail-Werbung (Spammails). In den der Aufsichtsbehörde vorgelegten Fällen war der Absender der eMail entweder bereits aufgrund der im „Header“ (Kopfzeile jeder eMail) enthaltenen wahrheitsgemäßen Angaben bekannt oder er konnte ermittelt werden. In den Fällen, in denen der Absender bekannt war, waren die Auskunftsersuchen der Betroffenen über die zu ihrer Person gespeicherten Daten als auch über deren Herkunft unbeantwortet geblieben. Auch wurde deren Forderung, das Zusenden weiterer Spammails zu unterlassen, vielfach ebenso wenig nachgekommen wie der Forderung auf Löschung bzw. Sperrung ihrer eMail-Adressen.

Die Fälle, in denen der Absender der eMail bekannt ist, sind jedoch die Ausnahme. Überwiegend handelt es sich bei den in Massen verschickten Spammails um unseriöse Angebote für Geschäftsideen, die per Fax unter 0190er-Nummern abgerufen werden können oder um Werbung für Erotikseiten im Internet, bei deren Besuch dann ein 0190er-Dialer auf dem PC des Nutzers installiert wird. Die Absender dieser Spammails geben in den überwiegenden Fällen gefälschte Absenderadressen an oder nutzen die eMail-Adressen unbeteiligter Dritter. Im Berichtszeitraum wandten sich daher auch viele Bürger mit der

mit der Frage an die Aufsichtsbehörde, wie man sich vor der Zusendung dieser unverlangten Spammails schützen kann.

Unternehmen sehen in der Versendung von eMail-Werbung eine kostengünstige und schnelle Möglichkeit, potentielle Kunden für Ihre Produkte zu gewinnen. Sie ist besonders effektiv, da Personen oder Personengruppen nach bestimmten Merkmalen ausgewählt und daher gezielt angesprochen werden können. Für den Empfänger werden diese Spammails aber immer öfter zu einem Problem. Sie führen zu einer Erhöhung der Telefonkosten, da sie nur gelesen werden können, wenn der Empfänger online ist und der Provider dem Empfänger die Kosten für die Nutzung seines Servers in Rechnung stellt, die anteilmäßig auch auf die Zeit entfällt, in denen die Werbe-eMails gelesen werden.

Die bisherigen Entscheidungen der Gerichte haben – analog zu den bisher ergangenen Urteilen zur unverlangten Telefon- und Telefaxwerbung – entschieden, dass diese Form des Direktmarketings, privat wie gewerblich, unzulässig ist und gegen § 1 des Gesetzes gegen den unlauteren Wettbewerb verstößt (u.a. LG Traunstein, Beschluss vom 18.02.1997 – 2 HK O 3755/97; LG Berlin, Beschluss vom 02.04.1998 – 16 O 201/98; LG Berlin, Beschluss vom 14.05.1998 – 16 O 301/98).

Grundsätzlich bedarf der Versender einer Werbe-eMail vorab einer ausdrücklichen vorherigen Einwilligung des Empfängers. Ansonsten ist die Nutzung der eMail-Adresse eines Empfängers nur zulässig, wenn sie im Rahmen der Begründung, inhaltlichen Ausgestaltung oder zur Änderung eines Vertragsverhältnisses genutzt wird (§ 5 TDDSG). Auch bei Anwendung des weniger strengen Offline-Rechts ist die werbliche Nutzung von eMail-Adressen ohne vorherige Einwilligung der Betroffenen nur unter den in § 28 Abs. 1 Nr. 1 – 3 und Abs. 3 BDSG genannten Voraussetzungen zulässig, es sei denn, der Betroffene hat gemäß § 28 Abs. 4 Satz 1 BDSG der Nutzung seiner personenbezogenen Daten zu Zwecken der Werbung oder der Markt- und Meinungsforschung ausdrücklich widersprochen.

Die betroffenen Unternehmen teilten auf Anfrage der Aufsichtsbehörde in der überwiegenden Zahl der Fälle mit, nicht mehr nachvollziehen zu können, wie man in den Besitz der eMail-Adresse gelangt sei. Andere wiederum teilten mit,

- die eMail-Adresse einem öffentlichen Verzeichnis (z.B. DeTeMedien-eMail-Verzeichnis) entnommen zu haben oder
- die eMail-Adresse von einem Anbieter erworben zu haben, der beim Kauf bescheinigte, dass die Adressaten zuvor in die Zusendung von Werbe-eMails eingewilligt hätten.

Auf die Frage, warum die berechtigten Auskunftsbegehren der Betroffenen nicht beantwortet wurden, war die Antwort jedoch in allen Fällen gleich: es handelte sich entweder um ein bedauerliches Versehen oder es konnte nicht mehr nachvollzogen werden, warum den Beschwerdeführern nicht geantwortet wurde.

Allen Unternehmen wurde unter Hinweis auf die ihnen gemäß § 34 Abs. 1 BDSG obliegende Auskunftspflicht aufgegeben, Auskunftsersuchen Betroffener zukünftig umgehend und umfassend zu beantworten und den Forderungen auf Löschung bzw. Sperrung der eMail-Adressen der Beschwerdeführer nachzukommen. Gleichzeitig wurde auf die bereits zur Versendung unangeforderter eMail-Werbung ergangene Rechtsprechung und die möglichen Folgen hingewiesen.

Anfragenden Bürgern wurde als Schutzmaßnahme empfohlen,

- bei der Weitergabe ihrer eMail-Adresse zurückhaltend zu sein und sich nicht in Adressverzeichnisse einzutragen oder eintragen zu lassen,
- bei der Teilnahme an Newsgroups oder Webforen, soweit erforderlich, eine gesonderte eMail-Adresse anzugeben, die von vielen Anbietern (z.B. yahoo, web.de, oder freemail) kostenlos angeboten wird,
- eingegangene Werbe-eMails nicht zu beantworten, sondern direkt zu löschen, um zu vermeiden, dass Unternehmen in Erfahrung bringen, dass ihre eMail-Adresse noch existiert und
- sog. eMail-Filter auf ihrem PC zu installieren.

1.3 Verwendung der Personalausweisnummer bei der Registrierung von Internet- Nutzern durch Access-Provider

Ein Petent beschwerte sich über einen Access-Providers, der den Zugang zu eigenen und verlinkten Internetseiten, die erotische, pornographische oder jugendgefährdende Inhalte haben können, erst dann freigibt, wenn der Nutzer bei seiner Anmeldung die vollständige und richtige Personalausweis-Nummer angegeben hat. Nach Auffassung des Petenten verstoße die Registrierung der Personalausweis-Nummer gegen geltendes Datenschutzrecht, da er diese Internetseiten anonym sichten wolle.

Die Überprüfung des Sachverhaltes ergab, dass der Provider – mit Genehmigung des Bundesministerium des Innern – über ein System verfügt, welches das Lebensalter einer Person online, unter Wahrung der Anonymität, anhand der Personalausweis-Nummer feststellt.

Bedingt durch die Tatsache, dass der Inhalt der angebotenen Internetseiten nur für Erwachsene bestimmt ist, hat der Provider sicherzustellen, dass nur volljährige Personen darauf zugreifen können (vgl. § 184 Abs. 1 StGB). Das einzig existierende Personaldokument, das das Alter eines deutschen Staatsangehörigen eindeutig dokumentiert, ist der Personalausweis. Nach Eingabe der auf dem Personalausweis abgedruckten vier Nummernblöcke (Personalausweis-Nummer) kann die eingesetzte Software das Alter des Nutzers feststellen und gleichzeitig überprüfen, ob die übrigen angegebenen Zahlenkombinationen des Personalausweises richtig sind. Bei einer fehlerhaften / falschen Angabe der Personalausweis-Nummer bleibt der Zugang zu den einzelnen geschützten Seiten gesperrt. Damit kommt der Provider in vollem Umfang den Bestimmungen des Jugendschutzgesetzes nach.

Ein Verstoß gegen datenschutzrechtliche Bestimmungen konnte nicht festgestellt werden, insbesondere auch deshalb nicht, da die Nutzer vorab vollständig über die Nutzungsbedingungen sowie den Zweck und die Dauer der Datenspeicherung informiert werden.

1.4 Versendung von Kundendaten durch Provider

Ein Kunde führte Beschwerde über die Art und Weise seines Providers, wie dieser seine Kunden über einen neuen Internettarif informierte. Der Provider schrieb die Kunden einzeln per Post an und informierte sie – bedingt durch den Wegfall eines Kooperationspartners – über die Möglichkeit, den bisherigen Vertrag auf einen neu geschaffenen Tarif umstellen zu können. Einhergehend mit dieser Unterrichtung wurden sie gebeten, die dem Provider vorliegenden und ebenfalls im Anschreiben abgedruckten Bankdaten auf ihre Richtigkeit hin zu überprüfen. Für den Fall, dass die Bankdaten nicht mehr aktuell sein sollten, wurden die Kunden gebeten, diese auf einer entsprechenden Internetseite abzuändern. Dazu wurde den Kunden auch deren bisherige Nutzerkennung und Passwort mitgeteilt. Der Petent war über den leichtfertigen Umgang des Providers mit den personenbezogenen Daten seiner Kunden sehr befremdet und wandte sich deshalb an die Aufsichtsbehörde.

Ein Verstoß gegen datenschutzrechtliche Bestimmungen konnte nicht festgestellt werden. Der Provider nahm die Eingabe jedoch zum Anlass, die bisher praktizierte Verfahrensweise bei der Versendung der Kundendaten entsprechend den von der Aufsichtsbehörde unterbreiteten Vorschlägen umgehend abzuändern.

2. Handel / Auskunfteien / Inkasso-Unternehmen

2.1 Kopieren von Ausweisdokumenten bei Abschluss eines Beherbergungsvertrages

Ein Petent führte Beschwerde über ein Hotel, das bei Abschluss des Beherbergungsvertrages ohne sein Einverständnis eine Kopie seines Personalausweises anfertigte. Die Inhaberin des Hotel sah sich – eigenen Angaben zufolge – durch die steigende Anzahl von Gästen, die bewusst falsche Personalien in die Anmeldeformulare eintrugen und ohne Begleichung der Übernachtungskosten ab-

reisten, gezwungen, zur Sicherung ihrer Rechtsansprüche Kopien der Ausweispapiere anzufertigen.

Grundsätzlich ist das Kopieren von Ausweisdokumenten zum Zwecke der Identitätsfeststellung datenschutzrechtlich nur dann nicht zu beanstanden, wenn der Betroffene vor dem eigentlichen Kopiervorgang seine ausdrückliche Einwilligung erteilt hat (§ 4 Abs. 1 BDSG). Im vorliegenden Fall wurde die Inhaberin des Hotels aufgefordert, das Kopieren der Ausweisdokumente zu unterlassen und darauf hingewiesen, dass es ihr lediglich erlaubt ist, anhand des vorzulegenden Ausweisdokumentes die von den Gästen im Meldeformular eingetragenen Angaben zur Person abzugleichen (§ 4 Abs. 1 des Gesetzes über Personalausweise).

2.2 Geschäftsgeheimnis als Grund für Verweigerung einer Auskunft

Eine minderjährige Petentin beschwerte sich bei der Aufsichtsbehörde über eine Handels- und Wirtschaftsauskunftei, die ihr gegenüber unter Berufung auf das Geschäftsgeheimnis die gewünschte Auskunft über die Herkunft und Empfänger der zu ihrer Person gespeicherten Daten verweigert hatte.

Bis zum Inkrafttreten des novellierten BDSG konnten betroffene Personen von Auskunfteien nach § 34 Abs. 2 BDSG (alt) nur dann eine Auskunft über Herkunft und Empfänger von Daten verlangen, wenn begründete Zweifel an der Richtigkeit der Daten geltend gemacht wurden. Mit der Umsetzung der Richtlinie 95/46 EG sollte eine Stärkung und Erweiterung der Auskunftsrechte der Betroffenen erreicht werden. Nunmehr dürfen Auskunfteien eine Auskunft über Herkunft und Empfänger der Daten nur noch dann verweigern, wenn deren Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt.

Diese Regelung führte zu einer kontroversen Diskussion zwischen dem Verband der Handelsauskunfteien (VdH) und der Arbeitsgruppe „Auskunfteien“ des Düsseldorfer Kreises, bei der bislang noch keine Einigung erzielt werden konnte. Während nach Auffassung des Verbandes der Handelsauskunfteien der

Kundenstamm einer jeden Auskunftei unter das Geschäftsgeheimnis fällt, so ist aus Sicht der Aufsichtsbehörden bei einer fehlerhaften Auskunft immer den Betroffenen gegenüber Auskunft zu erteilen. In diesen Fällen hat die Interessenabwägung zwischen dem Anspruch des Betroffenen auf Bekanntgabe und der Wahrung des Geschäftsgeheimnis der Auskunftei immer zugunsten des Betroffenen auszugehen.

Sofern jedoch eine Auskunftei eine Auskunft über den Empfänger der Daten verweigert, muss diese ausführlich begründen, warum überwiegende Geschäftsgeheimnisse der Auskunftserteilung entgegenstehen. Der alleinige Verweis auf das Geschäftsgeheimnis reicht insoweit nicht aus.

2.3 Verletzung von Persönlichkeitsrechten / Verweigerung von Auskünften durch ein Inkasso-Unternehmen

Im Berichtszeitraum beschwerten sich mehrere betroffene Bürger über die Arbeitsweise eines Inkasso-Unternehmens.

In einem Fall wurden dem Beschwerdeführer binnen kurzer Zeit insgesamt 33 Mahn- und 7 Vollstreckungsbescheide zugestellt. Nachdem er umgehend nach Erhalt der ersten Mahnbescheide form- und fristgerecht Widerspruch dagegen eingelegt hatte, wandte er sich an das Inkasso-Unternehmen und forderte die Vorlage von Nachweisen, die die ihm gegenüber geltend gemachten Forderungen belegen sollten, eine Kopie der zu seiner Person beim zuständigen Einwohnermeldeamt eingeholten Auskunft sowie um Mitteilung über die zu seiner Person gespeicherten Daten (§ 34 Abs. 1 BDSG). Anstelle der gewünschten Auskünfte teilte das Inkasso-Unternehmen dem Beschwerdeführer lediglich mit, aus welchen Einkäufen die Forderungen angeblich resultierten und forderte die umgehende Begleichung der noch offenstehenden Forderungen. Auf die Einlassung des Petenten, er könne die Einkäufe aufgrund urlaubsbedingter Abwesenheit nicht getätigt haben, wurde nicht eingegangen.

Nachdem sich der Beschwerdeführer Hilfe suchend an die Aufsichtsbehörde gewandt hatte, wurde eine unangemeldete Vor-Ort-Kontrolle des Inkasso-Unternehmens durchgeführt. Die Vor-Ort-Kontrolle konnte jedoch nicht, wie beabsichtigt, durchgeführt werden, da der Inhaber des Inkasso-Unternehmens jegliche Akteneinsicht und Auskunftserteilung verweigerte. Gleichzeitig sprach der telefonisch hinzugezogene Rechtsanwalt den Mitarbeitern der Aufsichtsbehörde das ihnen durch § 38 Abs. 4 BDSG eingeräumte Recht zum Betreten des Grundstückes und auf Einsicht in die entsprechenden Unterlagen ab. Die Kontrolle wurde daraufhin abgebrochen.

Im Rahmen der weiteren Überprüfung stellte sich später heraus, dass es beim zuständigen Einwohnermeldeamt aufgrund einer unvollständigen Meldeamtsanfrage sowie eines Schreibfehlers zu einer Personenverwechslung gekommen war. Auf die Verletzung der Persönlichkeitsrechte der Betroffenen und deren unabdingbares Recht auf Auskunft (§ 34 Abs. 1 BDSG) hingewiesen, teilte das Inkasso-Unternehmen lediglich mit, bei Anfragen an das Einwohnermeldeamt das Geburtsdatum der Schuldner grundsätzlich nicht anzugeben und „Einwände der betroffenen Personen nur im Rahmen des gerichtlichen Mahnverfahrens vor Gericht überprüfen zu lassen.“

Wegen weiterer, nicht fristgerecht erteilter Auskünfte gegenüber der Aufsichtsbehörde sowie wegen Nichtbestellung eines betrieblichen Datenschutzbeauftragten wurde ein Bußgeldverfahren gegen den Inhaber des Inkasso-Unternehmens eingeleitet und ein Bußgeld festgesetzt. Das Bußgeldverfahren war zum Ende des Berichtszeitraumes noch beim zuständigen Amtsgericht anhängig.

Kurz darauf musste die Aufsichtsbehörde erneut tätig werden, da das Inkasso-Unternehmen aufgrund einer erneuten Personenverwechslung bei einem 5-jährigen Kind versuchte, eine noch offenstehende Forderung beizutreiben. Auch in dem Fall hatte das Inkasso-Unternehmen gegenüber den Erziehungsberechtigten jegliche Auskünfte verweigert.

3. Wohnen und Liegenschaften

3.1 Die Eigentümergemeinschaft

Telefonisch fragte eine Bürgerin an, ob in einer Eigentümerversammlung die Personen namhaft gemacht werden dürfen, die die Umlage noch nicht bezahlt haben. Ihr wurde geraten, zunächst die Vereinbarungen in der Teilungserklärung und dem Vertrag mit der Hausverwaltung zu lesen. Nach den Regeln des BDSG ist eine solche allgemeine Mitteilung über die Schuldner der Umlage unzulässig. Gerechtfertigt ist die Mitteilung nur, wenn die Forderung so hoch ist, dass die Eigentümergemeinschaft wirtschaftlich gefährdet wird. In diesem Fall müssten Beschlüsse über gezielte Maßnahmen getroffen werden. Die Bekanntgabe der Schuldner ist dann im Rahmen einer vertragsähnlichen Beziehung zwischen den Wohnungseigentümern notwendig und erlaubt (vgl. § 28 Abs. 1 Nr. 1 BDSG).

3.2 Mieterfragebögen

Vor der Vermietung einer Wohnung versuchen Vermieter, sich umfangreiche Kenntnisse über künftige Mieter zu verschaffen. Einige Wohnungsbaugesellschaften legen deshalb Mietinteressenten Fragebögen vor, in denen unter anderem Angaben zur Person erfragt werden, die für eine Wohnungsbewerbung nicht erforderlich sind. Um die Chancen für die Anmietung der Wohnung zu wahren, sind die potentiellen Mieter dennoch bereit, die gewünschten Auskünfte zu erteilen.

Da eine Wohnungsbewerbung erfahrungsgemäß nur bei komplett ausgefülltem Fragebogen angenommen wird, liegt eine echte Einwilligung in die Datenverarbeitung nicht vor. Eine Einwilligung ist nur dann wirksam, wenn sie auf der freien Entscheidung der befragten Person beruht (§ 4a Abs. 1 BDSG). Die Datenerhebung und Verarbeitung muss durch den Zweck des künftigen Mietverhältnisses gerechtfertigt werden. Es dürfen nur Daten erhoben werden, an deren Erkenntnis der Vermieter ein berechtigtes Interesse hat.

Das berechtigte Interesse des Vermieters und das schutzwürdige Interesse des künftigen Mieters am Ausschluss der Datenverarbeitung müssen gegeneinander abgewogen werden. Demnach sind Fragen nach Vorstrafen, Größe und Preis der früheren Wohnung, dem früheren Vermieter oder dem Arbeitgeber unstatthaft. Vor Abschluss des Mietvertrages ist die Frage nach der Bankverbindung unzulässig. Die Bankverbindung wird erst nach Vertragsabschluss für die Abbuchungen bedeutsam. Nur Interessenten für Wohnungen in großen Anlagen dürfen nach der Staatsangehörigkeit gefragt werden. Hier dient die Frage der Vermeidung von Gettobildungen und sozialen Problemstrukturen.

Zulässig hingegen sind Fragen nach der Einkommenshöhe, der Zahl der einziehenden Personen und nach Haustieren. Sie stehen unmittelbar mit der reibungslosen Abwicklung eines Mietverhältnisses in Verbindung.

3.3 Luftbildaufnahmen von Gebäuden und Grundstücken

Mehrmals wurde im Berichtszeitraum Beschwerde gegen ein Unternehmen geführt, das Luftbildaufnahmen von Gebäuden und Grundstücken anfertigt und diese den jeweiligen Eigentümern zum Kauf anbietet. Die betroffenen Grundstückseigentümer sahen in der Anfertigung der Luftbildaufnahmen einen Verstoß gegen den Datenschutz.

Das Luftbildunternehmen teilte mit, die mittlerweile nicht mehr genehmigungspflichtigen Luftbildaufnahmen in Serie anzufertigen und in Form von Rohkopien den Eigentümern bzw. Nutzungsberechtigten der jeweiligen Objekte zum Kauf anzubieten. Die Objekte selbst werden in den jeweiligen Orten durch die Rohkopien ausfindig gemacht. Nicht verkaufte Bilder werden umgehend vernichtet. Die Archivierung der Negative erfolgt nach Film- und Seriennummern, wobei zu jeder Serie ein Flugplan mit Einzeichnung und Name des Ortes gehört. Eine Auswertung der archivierten Negative ist daher nicht möglich; nach Ablauf von 4 Jahren werden die Negative vernichtet.

Sofern die Aufnahmen nur den Betroffenen zum Kauf angeboten werden (Datenverarbeitung zur Erfüllung eigener Geschäftszwecke, § 28 Abs. 1 BDSG), bestehen aus datenschutzrechtlicher Sicht keine Bedenken. Die Luftbildaufnahmen enthalten zunächst lediglich grundstücks- oder gebäudebezogene Daten, nicht aber personenbezogenen Daten i.S.v. § 3 Abs. 1 BDSG. Die „Personalisierung“ der Aufnahmen erfolgt erst dann, wenn sie vor Ort im Rahmen der Kontaktaufnahme mit den Betroffenen einer bestimmten Person zugeordnet werden. Schutzwürdige Interessen Betroffener stehen der Anfertigung der Luftaufnahmen somit nicht entgegen.

Werden digitale Luftbildaufnahmen jedoch zum Online-Abruf bereitgehalten (Datenverarbeitung zum Zwecke der Übermittlung, § 29 Abs. 1 BDSG) und kann durch eine Verknüpfung mit anderen Datenbanken ein Personenbezug hergestellt werden (z.B. Datenbanken mit Angaben über wirtschaftliche oder finanzielle Verhältnisse von Grundstückseigentümern), überwiegt in diesen Fällen das schutzwürdige Interesse der betroffenen Personen. Eine Speicherung, Verarbeitung oder Nutzung dieser Daten ohne vorherige Einwilligung der betroffenen Grundstückseigentümer ist unzulässig.

4. Arbeitnehmerdatenschutz

Ein spezielles Arbeitnehmerdatenschutzgesetz gibt es nicht. Im politischen Raum wird seit Jahren darüber diskutiert, ob ein solches Gesetz erlassen werden soll. Derzeit gelten die allgemeinen Vorschriften des Bundesdatenschutzgesetzes. Bei der Dauer der Speicherung von Daten müssen Aufbewahrungspflichten aus anderen Gesetzen beachtet werden. Lohndaten beispielsweise dürfen erst gelöscht werden, wenn die zivilrechtlichen Verjährungsfristen abgelaufen sind. Auch steuerrechtliche Pflichten gegenüber der Finanzverwaltung können die Dauer der Speicherung von Daten bestimmen.

Daten von Bewerbern müssen nach Abschluss der Stellenbesetzung gelöscht werden. Falls ein Unternehmen Daten für künftig frei werdende Stellen speichern möchte, müssen die Bewerber auf eine fortdauernde Speicherung ihrer

Daten hingewiesen werden. Ein Widerspruch gegen die fortdauernde Speicherung der Daten muss berücksichtigt werden.

Anfragen zum Arbeitnehmerdatenschutz stellten Arbeitgeber und Arbeitnehmer. Bei der Auslegung der Normen des BDSG muss das Arbeitsrecht beachtet werden.

4.1 Sicherheit

Im Zuge der verschärften Sicherheitsmaßnahmen nach dem 11. September 2001 lassen militärische Stellen nur noch sicherheitsüberprüftes Personal von beauftragten Unternehmen auf ihrem Gelände arbeiten. Eine echte Entscheidungsmöglichkeit hat ein Privatunternehmen in dieser Lage nicht. An die Aufsichtsbehörde wurde die Frage herangetragen, wie die Maßnahmen datenschutzkonform durchgeführt werden können. Der Abschluss einer Betriebsvereinbarung, die die Erhebung und Verwendung der Daten regelt, wurde empfohlen. In der Betriebsvereinbarung kann insbesondere festgelegt werden, dass die Daten nur für sicherheitserhebliche Arbeiten in militärischem Gelände benutzt werden dürfen. Zu einer sonstigen Verhaltens- und Leistungskontrolle dürfen sie bei einer entsprechenden Betriebsvereinbarung nicht eingesetzt werden.

4.2 Streit im Betrieb

Nach einer Auseinandersetzung trat ein Betriebsrat zurück, ohne bis zur Neuwahl als geschäftsführender Betriebsrat tätig zu sein. Um die Aufbewahrung der Unterlagen des zurückgetretenen Betriebsrates stritten Arbeitgeber und ehemaliger Betriebsrat.

Aus datenschutzrechtlicher Sicht war der Vorschlag des Arbeitgebers zu begrüßen, die Unterlagen so zu verpacken, dass der ehemalige Betriebsrat und der Arbeitgeber nur gemeinsam Zugang zu den Unterlagen haben. So wird die Zweckbindung der Daten nach § 28 Abs. 2 BDSG und die Vollständigkeit des

Materials gesichert. Dem neu gewählten Betriebsrat werden sie zur weiteren Bearbeitung ausgehändigt werden.

4.3 Schwangerschaft

Eine schwangere Arbeitnehmerin legte ihrem Arbeitgeber ein Attest über ein Beschäftigungsverbot vor. Der Arbeitgeber nahm daraufhin Kontakt zur Frauenärztin auf. Diese stellte eine Krankmeldung aus, die die Krankenkasse anzweifelte. Die Krankenkasse war ebenso wie die Betroffene der Ansicht, dass sie nicht krank sei. Eine neuerliche ärztliche Untersuchung kam gleichfalls zu dem Ergebnis eines Beschäftigungsverbotes. Der Arbeitgeber bezweifelte auch das zweite Beschäftigungsverbot und wollte Einblick in die Krankenakte nehmen.

In dieser Situation wandte sich die Arbeitnehmerin an die Aufsichtsbehörde. Die Anfrage wurde dahin beantwortet, dass ein Arzt ohne Einwilligung des Patienten keine Einsicht in eine Krankenakte gewähren darf. Auch habe ein Arbeitgeber kein Recht auf Einsichtnahme in eine Patientenakte. Die Abgabe einer Einwilligungserklärung darf vom Arbeitnehmer nicht gefordert werden.

4.4 Das schwarze Brett

Ein Betrieb veröffentlichte krankheitsbedingte Fehlzeiten der einzelnen Mitarbeiter im Intranet. Ein betroffener Mitarbeiter wandte sich daraufhin an die Aufsichtsbehörde.

Ihm wurde erläutert, dass die reine Bekanntgabe der Abwesenheit von Mitarbeitern aus organisatorischen Gründen für den Betrieb erforderlich sei. Im Arbeitsverhältnis gibt es aber keinen Grund, allgemein bekannt zu machen, warum ein Mitarbeiter abwesend ist. Die allgemeine Bekanntgabe des Abwesenheitsgrundes ist für die Erfüllung des Arbeitsvertrages nicht erforderlich.

Das Unternehmen nahm aufgrund der Beschwerde des Mitarbeiters die Daten aus dem Intranet. So hat eine Beratung – ohne Beanstandung – zum Erfolg geführt.

4.5 Betriebsausweise

Ein großes Unternehmen mit mehreren Betriebsstätten in Deutschland möchte die vorhandenen Betriebsausweise mit Lichtbildern versehen. Die Ausweise sollen nur innerbetrieblich genutzt werden, damit das Wachpersonal die Mitarbeiter leichter identifizieren kann. Eine Veröffentlichung der Lichtbilder in der Hauszeitung, im Inter- und Intranet erfolgt nicht.

Die Lichtbilder der Ausweise dienen der Erfüllung der Arbeitsverträge. Das Sicherheitsinteresse des Unternehmens überwiegt die Beeinträchtigung der Persönlichkeit durch ein unerwünschtes Bild. Die Beeinträchtigung ist sehr gering und datenschutzrechtlich nicht zu beanstanden.

4.6 Der Systemadministrator

In einer Firma erhielt der Systemadministrator eine Kopie jeder eingehenden eMail. Während seiner urlaubsbedingten Abwesenheit leitete er sie auf den in seiner Privatwohnung stehenden PC weiter. Eine betriebsinterne Anweisung untersagte die Nutzung des eMail-Systems für private Zwecke. Jedoch erhielt der Systemadministrator zur Überraschung der Kunden des Unternehmens Kenntnis von namentlich adressierten E-Mails.

Ein Systemadministrator darf Stichproben des eMail-Verkehrs machen. Eine solche Kontrolle dient dem Schutz des betrieblichen Computersystems. Auch die Leistungsfähigkeit eines Systems kann besser gesichert werden, wenn dem Systemadministrator die Anforderungen aus dem betrieblichen Alltag bekannt sind. Eine Lektüre jeder eMail stellt aber eine unzulässige Inhaltskontrolle dar. Besonders bedenklich ist die ungeschützte Übertragung auf einen Computer im

häuslichen Bereich. Die eMails sind vor unbefugter Veränderung oder Kenntnisnahme nicht geschützt. Der Fragesteller wurde entsprechend unterrichtet.

4.7 „Datenhunger“ von Behörden

Gelegentlich fragen Unternehmen an, ob sie – wie von einer Behörde gefordert – umfangreiche Datenbestände übermitteln dürfen. Daten dürfen nach § 28 BDSG nur übermittelt werden, wenn das Einverständnis des Betroffenen, eine gesetzliche Erlaubnis oder ein Sonderfall (die Abwehr einer Gefahr) vorliegt. Eine Datenübermittlung ist beispielsweise nicht erlaubt, wenn

- das Arbeitsamt Informationen über die Selbstzahler einer privaten Berufsfachschule oder

- eine Landesversicherungsanstalt von einer Bank Informationen über alle Kredite an Mitarbeiter wünscht.

Den Unternehmen wurde empfohlen, sich von den anfragenden Behörden eine Rechtsgrundlage für ihr Begehren nennen zu lassen. Ein allgemeiner Hinweis auf statistische Zwecke reiche nicht aus.

4.8 Betriebliche Altersvorsorge

Auch die Einführung der „Riesterrente“ hat datenschutzrechtliche Bedeutung. Ein Unternehmen bietet eine betriebliche Altersvorsorge an. Die Mitarbeiter sollen sich bei einem großen deutschen Versicherungsunternehmen versichern können.

Für diesen Zweck sollen an das Versicherungsunternehmen die nötigen Daten übermittelt werden. Der Versicherer erstellt Modellberechnungen, die den Mitarbeitern übergeben werden. Für die Mitarbeiter entstehen bis zu diesem Zeitpunkt keine Verpflichtungen. Der informierte Betriebsrat erhob keine Einwände.

Der Versicherer bearbeitet die Daten im Auftrag des Unternehmens. Nach § 11 BDSG bleibt die Verantwortung bei dem Unternehmen (Auftraggeber). Gegen das Vorhaben bestehen keine Einwände. Dem anfragenden Unternehmen wurde empfohlen, den Versicherer zu verpflichten, die Daten nur für die Modellberechnungen zu verwenden.

5. Datenschutz und Medizin

Medizinische Daten sind nach Maßgabe des § 3 Abs. 9 BDSG als besonders schützenswert anzusehen. Sie werden von niedergelassenen Ärzten, Krankenhäusern sowie privaten und gesetzlichen Krankenkassen verarbeitet. Niedergelassene Ärzte, private Krankenhäuser und private Krankenversicherungen unterliegen der Aufsicht der Datenschutzbehörden. Die gesetzlichen Krankenkassen werden vom Bundesbeauftragten für den Datenschutz bzw. den Landesbeauftragten für den Datenschutz (LfD) beaufsichtigt, öffentliche Krankenhäuser vom LfD, für Krankenhäuser in kirchlicher Trägerschaft gelten die Regeln über den Datenschutz in der evangelischen bzw. katholischen Kirche, vgl. § 1 Abs. 2 BDSG. Bei der Datenverarbeitung im medizinischen Bereich sind neben dem BDSG zu berücksichtigen: SGB V, SGB X, Landeskrankenhausgesetz, § 203 Strafgesetzbuch und die Berufsordnung der Ärzte.

In Zusammenarbeit mit der Ärztekammer Trier fand eine Fortbildungsveranstaltung zum Thema "Datenschutz in der Arztpraxis" statt. Im Rahmen des Vortrags wurde auf das umfangreiche Material des unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein hingewiesen. Es kann unter

www.datenschutzzentrum.de/medizin/arztprax/index.htm

abgerufen werden. Eingaben zu datenschutzrechtlichen Fragen stammen von Ärzten und Patienten.

5.1 Erteilung von Auskünften an Krankenversicherungen und Kassenärztliche Vereinigungen

Anfragen von Ärzten betrafen ihre Auskunftspflicht gegenüber den gesetzlichen Krankenversicherungen bzw. der kassenärztlichen Vereinigung. Entsprechende Regeln enthalten die §§ 106, 295 ff, 301 SGB V. Für das Arzt-Patienten-Verhältnis sind die §§ 27 ff. BDSG daneben zu beachten. Die Krankenkassen haben kein medizinisches Vorprüfungsrecht. Auch die kassenärztliche Vereinigung hat kein generelles Recht, Befunde oder Daten aus Arztbriefen anzufordern. Die Prüfung medizinischer Fragen übertrug der Gesetzgeber dem medizinischen Dienst der Krankenkassen, §§ 275 ff. SGB V. Das Urteil des Bundessozialgerichtes vom 23.07.2002, Az.: B 3 KR 64/01 R betrifft direkt die Krankenhäuser. Ein medizinisches Prüfungsrecht der Krankenkassen wird in dem Urteil ausdrücklich abgelehnt. Es ist zu hoffen, dass das Urteil auch im Bereich der ambulanten Versorgung klärend wirkt.

5.2 Die eigene Krankengeschichte

Anfragen von Patienten betrafen den Umgang mit Krankengeschichten. Bei einem Arztwechsel sind die Unterlagen an den neuen Arzt weiterzugeben. Ein formalisiertes Übergabeverfahren ist aus datenschutzrechtlicher Sicht nicht erforderlich. Der die Unterlagen abgebende Arzt muss lediglich sicherstellen, dass sie per Post oder per Boten an den richtigen Empfänger gelangen. Entgegen der Ansicht eines Beschwerdeführers sind Ausweiskontrollen oder ähnliche Maßnahmen bei persönlicher Abholung nicht zwingend erforderlich.

5.3 Einsichtsrecht psychisch Kranker

Eine Suchtklinik fragte an, ob sie dem Rechtsanwalt einer früheren Patientin Auskunft erteilen müsse. Eine anwaltliche Vollmacht schließt die Berechtigung zur Einsichtnahme in Krankenunterlagen nicht ein. Die betroffene Patientin muss den behandelnden Arzt gegenüber dem Anwalt von der Schweigepflicht

schriftlich und ausdrücklich entbinden. Die Klinik wurde darüber unterrichtet, dass Patienten mit Erkrankungen aus dem psychiatrischen Formenkreis die Einsicht nicht generell verweigert werden darf. Wenn nach sorgfältiger ärztlicher Prüfung wegen drohender Gesundheitsgefahren durch die Einsichtnahme diese versagt wird, muss die Ablehnung nachvollziehbar dokumentiert werden. Dann genügt eine Information durch den Arzt.

5.4 Die private Krankenversicherung

Beschwerden von Versicherungsnehmern privater Krankenversicherungen betrafen den allgemeinen Umfang mit Adressen und Daten. Eine Beschwerde zu speziell medizinischen Fragen gab es nicht.

5.5 Sanitätshäuser

Sanitätshäuser vertreiben Artikel zur Förderung der Gesundheit sowie Heil- und Hilfsmittel. Letztere werden in der Regel ärztlich verordnet. Die beim Vertrieb verordneten Heil- und Hilfsmittel anfallenden Daten sind personenbezogene Daten im Sinne des § 3 Abs. 9 BDSG. Für die Abrechnung mit den gesetzlichen Krankenkassen gelten das SGB V und das SGB X. Eine Beschwerde betraf die Weitergabe von Daten zwischen Sanitätshäusern. Nach der Auflösung einer Fachabteilung in einem kleinen Sanitätshaus übergab dieses seine Daten an ein anderes Sanitätshaus, das eine entsprechende Fachabteilung führte. Trotz intensiver Bemühungen und einer Vor-Ort-Kontrolle ließ sich nicht aufklären, ob die Daten von dem empfangenen Sanitätshaus mit oder ohne Einwilligung der Kunden ausgewertet wurden. Auch der Übergabeakt selbst konnte nicht mehr nachvollzogen werden. Die Widersprüche zwischen den Behauptungen der beiden Inhaber ließen sich nicht aufklären. Fest steht, dass dem übernehmenden Sanitätshaus durch die Begleitumstände der Übergabe Kunden verloren gingen. Diskretion und Datenschutz sollten für Sanitätshäuser umsatzfördernde Faktoren sein.

5.6 Kontrolle von Verordnungen

Durch einen Hinweis aus der Ärzteschaft erfuhr die Aufsichtsbehörde, dass einige gesetzliche Krankenversicherungen (teils aus Baden-Württemberg) die Verordnung von Kontaktlinsen generell durch eine privatrechtlich organisierte Gesellschaft von Augenoptikern überprüfen lässt. Die Augenoptikergesellschaft hat ihren Sitz in Rheinland-Pfalz. Die Krankenkassen meinen, dass bei ihnen und dem Medizinischen Dienst der Krankenkassen (MDK) die Fachkunde für solche Prüfungen fehle. Zum Zwecke der Prüfung erhielt die Gesellschaft die komplette Verordnung einschließlich Name und Anschrift des Patienten, des Arztes und ggf. des Optikers. In Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz Baden-Württemberg (23. Bericht 2002, 3. Teil), konnte erreicht werden, dass die Krankenkassen künftig pseudonymisierte Verordnungen an die Prüfgesellschaft übermitteln. Für die fachliche Kontrolle müssen Name und Anschrift der Patienten und des Arztes nicht bekannt sein. Erst bei der Krankenkasse werden bei der Bewilligung oder Ablehnung die Daten zusammengeführt. Evtl. Rückfragen werden über die Krankenkassen gestellt.

6. Videoüberwachung

Die Überwachung öffentlicher Straßen und Plätze und privater Grundstücke durch Videokameras nimmt – wie eingegangene Beschwerden zeigen – immer mehr zu.

§ 6 b BDSG regelt nur die Videoüberwachung öffentlich zugänglicher Räume. Nicht einschlägig ist die Norm, wenn ein Mieter seine zum Mietobjekt gehörende Terrasse im Zusammenhang mit einem Nachbarschaftsstreit von einer Videokamera überwachen lässt. Öffentlich zugänglich sind beispielsweise Banken, Einkaufszentren und Tankstellen. In solchen Fällen dient die Videoüberwachung der Wahrnehmung des Hausrechtes, der Sicherung von Rechtsansprüchen oder dem Schutz vor Diebstahl. Die Videoüberwachung ist damit zulässig im Sinne des § 6 b Abs. 1 BDSG. Häufig wird – wie die Praxis zeigt –

jedoch entgegen § 6 b Abs. 2 BDSG nicht auf die Videoüberwachung hingewiesen.

Nach dem Gesetz sind der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen. Auch auf deutlich sichtbare Kameras muss eigens hingewiesen werden. Entsprechende Aufforderungen wurden von der Aufsichtsbehörde aufgrund mehrerer eingegangener Beschwerden an verschiedene Unternehmen versandt. Sie installierten darauf hin die erforderlichen Hinweisschilder.

7. Der betriebliche Datenschutzbeauftragte

Ein betrieblicher Datenschutzbeauftragter ist nach § 4 f BDSG zu stellen, wenn mehr als vier Arbeitnehmer personenbezogene Daten automatisiert erheben, verarbeiten oder nutzen. Gleiches gilt, wenn personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 20 Personen beschäftigt sind.

Häufig fragten Inhaber von Unternehmen telefonisch oder schriftlich an, ob sie einen betrieblichen Datenschutzbeauftragten bestellen müssten.

Die Zahlenangaben im Gesetz beziehen sich auf die Anzahl der Mitarbeiter und nicht auf Stellen. Eine Halbtagskraft gilt als ganze Person im Sinne des § 4 f BDSG. Auch die Trennung zwischen Mitarbeitern in der Produktion und im handwerklichen Bereich und Mitarbeitern, die Daten verarbeiten, ist nicht in allen Unternehmen klar. Eine allgemeine Beratung zu den gesetzlichen Vorgaben ist in diesen Fällen ausreichend. Sie wird von den Anfragenden häufig positiv bewertet.

Die Vorbereitung betrieblicher Datenschutzbeauftragter auf ihre Aufgaben ist sehr unterschiedlich. Sie geht von bloßen Pro-Forma-Bestellungen über Verbands- und Kammerschulungen bis hin zur Ausbildung an der Fachhochschule Ulm. Auch der Einsatz der betrieblichen Datenschutzbeauftragten hängt stark

davon ab, ob die Leitung eines Unternehmens Datenschutz als wichtig bewertet.

8. Datenschutz in Vereinen

Das BDSG gilt auch für die Datenverarbeitung in Vereinen. Nach § 1 Bundesdatenschutzgesetz ist das Gesetz anwendbar, wenn Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben oder die Daten in oder aus nichtautomatisierten Dateien verarbeitet, genutzt oder dafür erhoben werden. Eine Ausnahme gilt nur, wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. Eine automatisierte Datenverarbeitung findet heute in vielen kleinen und allen größeren Vereinen statt. Anfragen von Vereinsmitgliedern und Vereinsvorständen belegen den wachsenden Bedarf an der Klärung von Fragen zum Datenschutz in Vereinen.

8.1 Zentral- und Gliedverband

Immer wieder tauchte die Frage auf, ob und in welchem Umfang ein Ortsverein Mitgliederdaten an den übergeordnete Dachorganisation weitergeben darf. Die Organisationsform eines Vereins spielt hier eine große Rolle. Es gibt Bundes- oder Landesverbände mit örtlichen Gruppierungen. Rechtlich selbständige Ortsverbände, die sich zu größeren Einheiten zusammenschließen, gibt es auch. Die Struktur wirkt sich auf die Art der Verarbeitung und Nutzung der Daten aus. Die nachfolgenden Ausführungen sind zwangsläufig allgemein gehalten.

Nach §§ 4, 4a BDSG setzt die Zulässigkeit der Verarbeitung personenbezogener Daten das Vorliegen einer gesetzlichen Erlaubnisnorm oder einer Einwilligung voraus. Als Grundlage für die Datenverarbeitung kommt insoweit auch die Vereinssatzung in Betracht. Einwilligungen zur vereinsinternen Datenübermittlung können auch im Aufnahmeantrag erteilt werden. Falls beide Möglichkeiten

nicht (mehr) durchführbar sind, sollte eine entsprechende Information der Mitglieder bei der Hauptversammlung oder durch die Vereinszeitschrift erfolgen. Die betroffenen Mitglieder müssen auf die Möglichkeit eines Widerspruches hingewiesen werden, vgl. §§ 4 a, 28 Abs. 2 Nr. 3 BDSG.

Allen Vereinen wird empfohlen, Regelungen über die Datenverarbeitung in die Satzung aufzunehmen, um auf diese Weise unter Berücksichtigung der Struktur und der Tätigkeit des Vereins den Umgang mit personenbezogenen Daten sachgerecht auszugestalten.

8.2 Der Datenschutzbeauftragte im Verein

Große Vereine, die Arbeitnehmer in ihrer Geschäftsstelle beschäftigen, benötigen betriebliche Datenschutzbeauftragte. Bei großen Sportvereinen trifft dies beispielsweise zu. Zum betrieblichen Datenschutzbeauftragten kann ein Mitglied des Vereins oder eine externe Person bestellt werden.

8.3 Zweckbindung der Datenverarbeitung

Vereine müssen bei ihrer Datenverarbeitung auf das Gebot der Zweckbindung beachten, vgl. § 28 Abs. 2 BDSG. Der Zweck heißt „Mitgliedschaft im Verein X". Ohne eindeutige Regelung dürfen Daten beispielsweise nicht an Adresshändler oder Sponsoren weitergegeben werden.

9. Internationaler Datenverkehr

Von der EU-Kommission ist für eine Reihe von Ländern inzwischen festgestellt worden, dass diese über ein den Anforderungen der EU-Datenschutzrichtlinie vergleichbares Datenschutzniveau verfügen. Soweit sich Datenempfänger in den USA den zwischen der Europäischen Kommission und den USA vereinbarten Safe-Habor-Absprachen angeschlossen haben, ist insoweit von einem an-

gemessenen Datenschutzniveau in Sinne von § 4e BDSG auszugehen. Die Übermittlung personenbezogener Daten ins Ausland ist nach Maßgabe des § 4c Abs. 1 BDSG auch dann zulässig, wenn beispielsweise Betroffene eingewilligt haben, die Übermittlung für die Erfüllung eines Vertrages zwischen dem Betroffenen und der verantwortlichen Stelle erforderlich ist, die Geltendmachung von Rechtsansprüchen dies erfordert oder sonstige lebenswichtige Interessen die Datenweitergabe notwendig machen.

Unabhängig von den vorgenannten Voraussetzungen kann im Einzelfall nach § 4c Abs. 2 BDSG auch die Genehmigung der Aufsichtsbehörde für eine grenzüberschreitende Datenübermittlung eingeholt werden. Von dieser Ausnahmevorschrift ist von Unternehmen in Rheinland-Pfalz bisher kein Gebrauch gemacht worden.

10. Werbung

Unverlangte Werbung ist für viele Menschen mittlerweile zu einem Ärgernis geworden. So gab es im Berichtszeitraum zahlreiche Beschwerden über diverse in- und ausländische Unternehmen, die unaufgefordert Werbeschreiben versenden und auf Auskunftsersuchen (§ 34 Abs. 1 BDSG) und Widersprüche Betroffener (§ 28 Abs. 4 Satz 1 BDSG) nicht reagierten.

Die Erfahrung zeigt, dass viele Werbetreibende, unabhängig davon, ob sie die Werbe-Mailings selbst versenden oder durch entsprechende Dienstleistungsunternehmen (Adresshandelsunternehmen, Lettershops, usw.) versenden lassen, nicht auf Auskunftsersuchen oder Widersprüche betroffener Personen reagieren. Einige Unternehmen hatten es ebenfalls nicht für notwendig erachtet, der Aufsichtsbehörde umgehend die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte zu erteilen. Erst die Androhung eines Bußgeldes brachte in diesen Fällen den gewünschten Erfolg für die Betroffenen.

Vielfach wurde auch die Frage gestellt, wie die Absender in den Besitz der Adressen kommen und ob die überwiegend unbekannten Absender dieser Werbe-Mailings die Adressen überhaupt für diese Zwecke nutzen dürfen.

Nach § 28 Abs. 3 Nr. 3 BDSG ist die Übermittlung oder Nutzung personenbezogener Daten (meistens Name und Anschrift) auch für Zwecke der Werbung oder der Markt- und Meinungsforschung zulässig, wenn kein Grund zu der Annahme besteht, dass schutzwürdige Interessen Betroffener an dem Ausschluss der Übermittlung oder Nutzung überwiegen. Das gleiche gilt, solange die Betroffenen der Nutzung ihrer personenbezogenen Daten zum Zwecke der Werbung oder der Markt- und Meinungsforschung nicht widersprochen haben (§ 28 Abs. 4 Satz 1 BDSG). Der Widerspruch kann jederzeit eingelegt werden. Nach Einlegung eines Widerspruches ist der Datensatz für jede weitere Nutzung oder Übermittlung zu sperren und in eine sog. „Sperr-Datei“ aufzunehmen.

Viele Betroffene verlangen von den werbetreibenden Unternehmen gleichzeitig die Löschung ihrer personenbezogenen Daten. Trotz Löschung der Daten kann es dennoch zu weiteren Werbesendungen kommen, wenn das Unternehmen Adressen für weitere Mailingaktionen ankauft oder anmietet und der betreffende Datensatz ebenfalls darin enthalten ist. Es ist daher sinnvoller, es bei einer Sperrung der Daten zu belassen. Beim Abgleich der neu angekauften oder angemieteten Adressdatenbestände mit der Sperr-Datei können gesperrte Datensätze dann direkt festgestellt werden.

11. Schlusswort

Der vorliegende Tätigkeitsbericht belegt, auch im Hinblick auf die Entwicklung in der Informationsgesellschaft, dass dem Schutz der persönlichen Daten Betroffener in besonderer Weise Aufmerksamkeit zu schenken ist. Insbesondere die vielfältigen Möglichkeiten der Erfassung und Verknüpfung personenbezogener Daten im Rahmen des Internets und andere Verfahren der automatisierten Datenverarbeitung stellen Gefährdungen für das vom Bundesverfassungsgericht ausdrücklich anerkannte und inzwischen auch in der Landesverfassung veran-

kerte Recht des Betroffenen dar, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Die Erfahrungen der Aufsichtsbehörde belegen, dass sowohl die verantwortlichen Stellen als insbesondere auch die Betroffenen vielfach nicht über die gesetzlichen Bestimmungen zum Schutz der personenbezogenen Daten informiert sind. Die Aufsichts- und Dienstleistungsdirektion (ADD) als Aufsichtsbehörde versteht sich insoweit als Ansprechpartner sowohl für Unternehmen als auch Betroffene, um einen effektiven Schutz der Persönlichkeitsrechte der Betroffenen zu gewährleisten.