3. Tätigkeitsbericht

für den Datenschutz im nicht-öffentlichen Bereich

Berichtszeitraum: 2005 - 2006

Impressum

Herausgeber:	Sächsisches Staatsministerium des Innern Referat 15 (Justiziariat, Datenschutz, Archivwesen) Wilhelm-Buck-Str. 2 01097 Dresden Telefon: (0351) 564 31 50 Telefax: (0351) 564 31 59 E-Mail: Datenschutz@smi.sachsen.de Internet: www.smi.sachsen.de
Auflagenhöhe:	1.500 Exemplare
Gestaltung (Titelbild)	agentur t.krüger kommunikation, Dresden
Druck:	JVA-Druckerei Waldheim
Kostenlose Bestelladresse:	Zentraler Broschürenversand der Sächsischen Staatsregierung Hammerweg 30, 01127 Dresden Telefon: (0351) 210 36 71 und (0351) 210 36 72 Telefax: (0351) 210 36 81 E-Mail: publikationen@sachsen.de

Inhaltsverzeichnis

Abkürzungsverzeichnis 4

1 Datenschutz im nicht-öffentlichen Bereich 6

2 Verfahrensregister 8

3 Regelaufsicht 8

3.1 Übersicht 8
3.2 Automatisiertes Abrufverfahren aus dem elektronischen Grundbuch 11
3.3 Koordinierte Datenschutzkontrolle von Wohnungsunternehmen 11
3.3.1 Rückblick 11
3.3.2 Mieterselbstauskünfte 12
3.3.2.1 Datenschutzrechtlicher Bewertungsmaßstab 12
3.3.2.2 Detailbetrachtungen 12
3.3.3 Fremdauskünfte/Bonitätsfragen 18
3.3.3.1 Ergebnisse der Stichprobenkontrollen 18
3.3.3.2 SCHUFA-Abfragen 19
3.3.3.3 Auskünfte von Wirtschaftsauskunfteien und Brancheninternen Warnsystemen 20
3.3.4 Datenschutzrechtliche Vereinbarungen im Mietvertrag 21
3.3.4.1 Ergebnisse der Stichprobenkontrollen 21
3.3.4.2 Regelungsbedarf 22
3.4 Erfolgskontrolle bei Wohnungsunternehmen 22
3.5 Erfolgskontrolle bei Wohlfahrtsverbänden 23

4 Anlassaufsicht 24

4.1 Überblick 24
4.2 Ausgewählte Sachverhalte 28
4.2.1 Videoüberwachung 28
4.2.1.1 Überwachungsmonitore in einem Freizeitbad 28
4.2.1.2 Webcams in Einzelhandelsgeschäften 31
4.2.1.3 Videoüberwachung von Hauseingang, Gehweg und Straße 33
4.2.1.4 Videoüberwachung im Massage-Studio 34
4.2.1.5 Die Kamera im Bratwurststand 35
4.2.2 Datenverarbeitung und -nutzung für Werbezwecke 36
4.2.2.1 Werbeprospekt statt Löschbestätigung 36
4.2.2.2 Versand von E-Mail-Newslettern 37
4.2.2.3 Haushaltsumfrage 37
4.2.2.4 Werbeschreiben trotz Eintrags in der Robinsonliste 38
4.2.2.5 Auskunft über die Herkunft der Daten 38
4.2.3 Arbeitnehmerdatenschutz 39
4.2.3.1 Erhebung von Bewerberdaten durch einen Personaldienstleister 39
4.2.3.2 Übermittlung von Personaldaten bei Einschaltung eines Privatdetektivs 41
4.2.4 Einzelhandel 41
4.2.4.1 Personalausweiskopien bei Barzahlung mit 500-€-Scheinen 41
4.2.5 Sparkassen/Banken 43
4.2.5.1 Bekanntgabe vertraulicher Daten im Sichtfenster eines Briefumschlages 43

4.2.5.2 Anzeige personenbezogener Daten am Kontoauszugdrucker 44
4.2.5.3 Anonymität bei Kundenumfragen 44
4.2.6 Betrieblicher Datenschutzbeauftragter 45
4.2.6.1 Unterbringung des Datenschutzbeauftragten im Großraumbüro 45
4.2.7 Freiberufler 46
4.2.7.1 Datenübermittlung durch einen Steuerberater 46
4.2.7.2 Verarbeitung und Nutzung von Kundendaten nach Beendigung eines Handelsvertretervertrages 47
4.2.8 Gesundheits- und Sozialwesen 47
4.2.8.1 Weitergabe von Patientendaten nach Praxisaufgabe 47
4.2.8.2 Dienstleistungen im Pflegeheim 48
4.2.9 Versicherungen 49
4.2.9.1 Weitergabe von Daten Unfallgeschädigter an Mietwagen- und Reparaturfirmen 49
4.2.10 Verkehrswesen 49
4.2.10.1 Datenerhebung bei erhöhtem Beförderungsentgelt 49

5 Beratungstätigkeit/Anfragen an die Behörde 50

6 Prüfung der Verhaltensregeln von Berufsverbänden 52

7 Genehmigung von Datenübermittlungen in Drittstaaten 52

8 Öffentlichkeitsarbeit 52

9 Ordnungswidrigkeitenverfahren 54

10 Zusammenarbeit mit anderen Aufsichtsbehörden 56

11 Beendigung der Kontrolltätigkeit 56

Abkürzungsverzeichnis

AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
AGG	Allgemeines Gleichbehandlungsgesetz
ASB	Arbeiter-Samariter-Bund
Berufsordnung - BO	Berufsordnung der Sächsischen Landesärztekammer
BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGBl	Bundesgesetzblatt
BGH	Bundesgerichtshof
BZRG	Bundeszentralregistergesetz
DDV	Deutscher Direktmarketing Verband e. V.
Erfa-Kreis	Erfahrungsaustausch-Kreis
GBV	Grundbuchverfügung
GDD	Gesellschaft für Datenschutz und Datensicherung e. V.
GenG	Genossenschaftsgesetz
GG	Grundgesetz
HGB	Handelsgesetzbuch
MDStV	Mediendienste-Staatsvertrag
OLG	Oberlandesgericht
ÖPNV	Öffentlicher Personennahverkehr
SächsPersPassG	Sächsisches Gesetz über Personalausweise und zur Ausführung des Passgesetzes
SächsDSG	Sächsisches Datenschutzgesetz
SächsGVBl	Sächsisches Gesetz- und Verordnungsblatt

SächsMG	Sächsisches Meldegesetz
SGB X	Zehntes Sozialgesetzbuch
StGB	Strafgesetzbuch
TB	Tätigkeitsbericht
WuM	Wohnungswirtschaft und Mietrecht

1 Datenschutz im nicht-öffentlichen Bereich

Das Sächsische Staatsministerium des Innern (SMI) war bis zum Ende des Berichtszeitraums oberste Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich. In dieser Funktion wirkte das SMI an der Fortentwicklung der datenschutzrechtlichen Regelungen auf EU- und Bundesebene mit. Als oberster Aufsichtsbehörde oblag ihm auch die Fachaufsicht über die für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden in Sachsen. Gemäß der Verordnung der Sächsischen Staatsregierung über die Regelung der Zuständigkeit der Aufsichtsbehörden nach § 38 Abs. 6 des Bundesdatenschutzgesetzes (BDSG) vom 27. August 1991 (SächsGVBl. 1991, S. 324) waren dies die Regierungspräsidien Chemnitz, Dresden und Leipzig. Diese überwachten die Durchführung des Datenschutzes bei nicht-öffentlichen Stellen und öffentlich-rechtlichen Wettbewerbsunternehmen und kontrollierten dabei die Einhaltung der Regelungen des BDSG sowie anderer Datenschutzvorschriften, soweit sie die automatisierte Verarbeitung personenbezogener Daten oder aber die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht-automatisierten Dateien regeln.

Die Datenschutzaufsichtsbehörden haben gemäß den Vorschriften des BDSG folgende Aufgaben zu erfüllen:

- **Registerführung (§ 38 Abs. 2 BDSG)**

  Die Aufsichtsbehörden führen das Register der nach § 4d BDSG meldepflichtigen automatisierten Verarbeitungen mit den Angaben nach § 4e Satz 1 BDSG.

- **Anlass- und Regelkontrollen (§ 38 Abs. 1 BDSG)**

  Die Datenschutzaufsichtsbehörden dürfen, soweit die grundsätzlichen Anwendungsvoraussetzungen des BDSG erfüllt sind, alle nicht-öffentlichen Stellen kontrollieren, auch, wenn keine Anhaltspunkte für eine Datenschutzverletzung gegeben sind.

- **Beratungstätigkeit (§§ 4g, 4d, 38 Abs. 1 BDSG)**

  Betriebliche Datenschutzbeauftragte können sich in Zweifelsfällen an die Aufsichtsbehörde wenden. Darüber hinaus regelt § 38 Abs. 1 Satz 2 BDSG seit August 2006 auch, dass die Aufsichtsbehörde die Datenschutzbeauftragten und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse berät.

- **Prüfung der Verhaltensregeln von Berufsverbänden (§ 38a BDSG)**

  Auch Berufs- und Unternehmensverbände können sich an die Aufsichtsbehörde wenden, um von ihnen erarbeitete Verhaltensregeln zur Förderung der Durchführung von daten-

schutzrechtlichen Regelungen auf die Vereinbarkeit mit geltendem Datenschutzrecht prüfen zu lassen.

- **Genehmigung von Datenübermittlungen in Drittstaaten (§ 4c Abs. 2 BDSG)**

  § 4b BDSG regelt die Übermittlung personenbezogener Daten ins Ausland. Für den Fall, dass personenbezogene Daten in Drittstaaten ohne angemessenes Datenschutzniveau übermittelt werden sollen, stellt § 4c BDSG einen Ausnahmekatalog bereit, der vermeiden soll, dass der Wirtschaftsverkehr mit diesen Staaten unangemessen beeinträchtigt wird. Über diesen Katalog hinausgehende Ausnahmen sind von der Aufsichtsbehörde zu genehmigen.

- **Öffentlichkeitsarbeit (§ 38 Abs. 1 Satz 6 BDSG)**

  Die Aufsichtsbehörden für den nicht-öffentlichen Bereich haben regelmäßig, spätestens jedoch alle zwei Jahre, einen Tätigkeitsbericht zu veröffentlichen.

- **Durchführung von Ordnungswidrigkeitenverfahren**

  Die Zuständigkeit zur Ahndung von Ordnungswidrigkeiten nach dem BDSG ergab sich aus der Verordnung der Sächsischen Staatsregierung über die Regelung der Zuständigkeit der Aufsichtsbehörden nach § 38 Abs. 6 des BDSG vom 27. August 1991 (SächsGVBl. 1991, S. 324). Darüber hinaus war das Regierungspräsidium Dresden auch Verwaltungsbehörde für die Verfolgung von (datenschutzrechtlichen) Ordnungswidrigkeiten nach dem Mediendienste-Staatsvertrag (MDStV), wobei sich hier die örtliche Zuständigkeit auf den gesamten Freistaat Sachsen erstreckte (vgl. Artikel 1 des Gesetzes zur Änderung des Sächsischen Gesetzes zum Staatsvertrag über Mediendienste und zur Änderung rundfunkrechtlicher Vorschriften im Freistaat Sachsen sowie zur Änderung des Gesetzes über den privaten Rundfunk und neue Medien in Sachsen vom 21. März 2003 [SächsGVBl. 2003, S. 37]).

- Die Aufsichtsbehörden konnten außerdem im Rahmen ihrer Tätigkeit von folgenden **Durchsetzungs- und Saktionsbefugnissen** Gebrauch machen:

  - Eigenständiges Strafantragsrecht bei BDSG-Straftatbeständen (§ 44 Abs. 2 BDSG),
  - Unterrichtung des Betroffenen und Anzeige der für den Verstoß verantwortlichen Stelle bei den zuständigen Ahndungs- und Verfolgungsbehörden (§ 38 Abs. 1 Satz 6 BDSG),
  - Verhängung von Zwangsgeldern zur Durchsetzung angeordneter Maßnahmen zur Mängelbeseitigung bzw. Verbot des Einsatzes einzelner Verfahren (§ 38 Abs. 5 Sätze 1 und 2 BDSG),

- Aufforderung zur Abberufung des betrieblichen Datenschutzbeauftragten (§ 38 Abs. 5 Satz 3 BDSG).

2 Verfahrensregister

Die Aufsichtsbehörde führt ein Register der nach § 4d BDSG meldepflichtigen automatisierten Verarbeitungen mit den Angaben gemäß § 4e Satz 1 BDSG (§ 38 Abs. 2 BDSG).

§ 4d BDSG definiert eine Meldepflicht für automatisierte Verarbeitungen. Diese Meldepflicht trifft alle Unternehmen, die personenbezogene Daten geschäftsmäßig zum Zweck der (gegebenenfalls auch anonymisierten) Übermittlung speichern (z. B. Wirtschaftsauskunfteien, Adresshändler, Markt- und Meinungsforschungsinstitute). Darüber hinaus sind auch Unternehmen von der Meldepflicht betroffen, die höchstens neun Arbeitnehmer mit der automatisierten Datenverarbeitung für eigene Zwecke beschäftigen.

Zum Stichtag 31. Dezember 2006 lagen den Regierungspräsidien insgesamt 30 Registermeldungen vor, die

- in zehn Fällen Verfahren von Handels- und Wirtschaftsauskunfteien,

- in 14 Fällen Verfahren von Markt- und Meinungsforschungsinstituten,

- in vier Fällen Verfahren von Adress- bzw. Datenhändlern sowie

- in je einem Fall den Betrieb eines Verfügungszentralregisters und einer Warndatei

betrafen.

Die bei den Datenschutz-Aufsichtsbehörden geführten Verfahrensregister sind in dem in § 38 Abs. 2 BDSG beschriebenen Umfang öffentlich und können von jedem eingesehen werden. Innerhalb des Berichtszeitraums wurden keine Einsichtnahme- bzw. Auskunftsbegehren an die Regierungspräsidien herangetragen.

3 Regelaufsicht

3.1 Übersicht

Die Aufsichtsbehörde kontrolliert die Ausführung des BDSG 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 Mitgliedstaaten in den Fällen des § 1 Abs. 5

(§ 38 Abs. 1 Satz 1 BDSG).

Im Berichtszeitraum lag ein Schwerpunkt der anlassfreien Kontrolltätigkeit der Regierungspräsidien bei den meldepflichtige Verfahren betreibenden Unternehmen. Weitere Schwerpunkte waren die Erfolgskontrollen bei Wohnungsunternehmen und Vereinen sowie Verbänden der Freien Wohlfahrtspflege. Außerdem erfolgten erstmals Stichprobenkontrollen bei zum Abruf aus dem elektronischen Grundbuch berechtigten Stellen. Die folgende Übersicht zeigt, welche Branchen überprüft wurden und verdeutlicht zugleich die Entwicklung im Vergleich zu den vorangegangenen Berichtszeiträumen:

Jahr **Branchen**	**2001/2002**	**2003/2004**	**2005/2006**
Auskunfteien	0	0	4
Markt-/Meinungsforschung	1	0	4
Auftragsdatenverarbeiter	10	1	0
Wohnungsunternehmen	0	46	19
Sparkassen/Banken	30	0	0
Verkehrsunternehmen	57	3	0
Versorgungsunternehmen	4	7	1
Altenpflegeheime	0	48	0
Wohlfahrtsverbände	0	0	10
Sonstige	2	5	7
Anzahl/Jahr	**104**	**110**	**45**

Tab. 1: Übersicht zu durchgeführten Regelüberprüfungen

Zu den durchgeführten Regelkontrollen ist Folgendes anzumerken:

Meldepflichtige Unternehmen (vgl. Pkt. 2):

- Wirtschaftsauskunfteien

  Hierbei handelt es sich um Wiederholungsüberprüfungen von aktuell im Register enthaltenen Unternehmen.

- Markt- und Meinungsforschungsunternehmen

  Die im vorangegangenen Berichtszeitraum neu angemeldeten Unternehmen wurden 2006 einer Erstüberprüfung unterzogen. Soweit in diesem Zusammenhang Mängel in der Datenschutzorganisation festgestellt worden waren, betrafen diese vor allem die Einhaltung allgemeiner datenschutzrechtlicher Anforderungen (Verpflichtung auf das Datengeheimnis, betrieblicher Datenschutzbeauftragter, öffentliches Verfahrensverzeichnis).

- Sonstige Unternehmen

  Eine Kontrolle betraf ein Unternehmen, das ein Verfügungszentralregister betreibt .

Nutzer des Elektronischen Grundbuchs:

Erstmals durchgeführt wurden Stichprobenkontrollen bei Unternehmen, die durch das Oberlandesgericht Dresden (OLG) zum Abruf von Daten aus dem Elektronischen Grundbuch zugelassen worden sind (vgl. Pkt. 3.2). Hierbei handelt es sich um zwei Wohnungs-, ein Versorgungs- sowie zwei sonstige Unternehmen.

Wohlfahrtsverbände, Wohnungsunternehmen:

Die in diesen Branchen durchgeführten Überprüfungen dienten vorrangig der Kontrolle der Einhaltung allgemeiner datenschutzrechtlicher Anforderungen. Außerdem wurde überprüft, inwieweit die in der Vergangenheit in dieser Branche durchgeführten koordinierten Datenschutzkontrollen zu einem datenschutzgerechteren Umgang mit personenbezogenen Daten geführt haben (vgl. Pkte. 3.4 und 3.5).

Im Berichtszeitraum wurden 45 Kontrollverfahren durchgeführt.

3.2 Automatisiertes Abrufverfahren aus dem elektronischen Grundbuch

Unternehmen, die im Rahmen ihrer Geschäftstätigkeit aktuelle Grundbuchauszüge benötigen, können diese mit Hilfe des automatisierten Abrufverfahrens kostengünstig erhalten. Genutzt wird diese Möglichkeit insbesondere von Firmen aus der Immobilien-, Wohnungs- und Telekommunikationsbranche sowie von Energieversorgern. Über die Zulassung der Teilnehmer entscheidet das OLG.

§ 83 Abs. 1 Satz 3 Grundbuchverfügung (GBV) sieht vor, dass das Grundbuchamt die Abrufprotokolle für stichprobenartige Überprüfungen durch die aufsichtsführenden Stellen bereitzuhalten hat. Die Kontrollzuständigkeit für die Datenschutzaufsichtsbehörden ergibt sich aus der Generalklausel des § 38 Abs. 1 Satz 1 BDSG.

Im Berichtszeitraum sind fünf der an dem Verfahren teilnehmenden Unternehmen einer örtlichen Überprüfung unterzogen worden. Schwerpunkt dieser Kontrollen war die Zulässigkeit der Abrufe aus dem elektronischen Grundbuch. Geprüft wurden einerseits das Einsatzumfeld (z. B. grundsätzliches Abrufinteresse, lokal getroffene Sicherheitsmaßnahmen, Verwendung der vom OLG bereitgestellten Bearbeiterkennzeichen) wie auch die Durchführung des Stichprobenverfahrens. Aus den Abrufprotokollen wurden jeweils 10 bis 30 Abrufe für die Überprüfung ausgewählt. Die Auswahl sollte möglichst Abrufe aller Bearbeiter, alle Aktionen und alle Abrufgründe umfassen.

Die durch die Aufsichtsbehörde vom OLG zum Zweck der stichprobenartigen Überprüfung abgeforderten Abrufprotokolle wurden gemäß § 83 Abs. 3 Satz 2 GBV fristgemäß innerhalb eines Jahres nach Eingang vernichtet.

3.3 Koordinierte Datenschutzkontrolle von Wohnungsunternehmen

3.3.1 Rückblick

Beginnend ab Februar 2004 wurden insgesamt 46 Wohnungsunternehmen einer schriftlichen datenschutzrechtlichen Kontrolle ausgewählter Datenverarbeitungsbereiche unterzogen.

Neben allgemeinen datenschutzrechtlichen Anforderungen (z. B. betrieblicher Datenschutzbeauftragter, Verpflichtung auf das Datengeheimnis, öffentliches Verfahrensverzeichnis) wurden insbesondere Fragen zur Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung (Mieter und Mietbewerber) sowie der Kooperation mit SCHUFA, Auskunfteien und Warnsystemen in die Kontrolle einbezogen. Eine erste Zwischenauswertung wurde bereits im letzten Tätigkeitsbericht unter Pkt. 4.2.3 vorgenommen. Eine ausführliche Auswertung dieser

Punkte wurde auf der Website des Regierungspräsidiums Dresden veröffentlicht und den betroffenen Unternehmen sowie deren Verbänden zur Verfügung gestellt.

3.3.2 Mieterselbstauskünfte

3.3.2.1 Datenschutzrechtlicher Bewertungsmaßstab

Mietbewerbern werden regelmäßig Fragebögen („Mieterselbstauskünfte“) vorgelegt.

Die Zulässigkeit der von Vermietern an Mietinteressenten ausgegebenen Fragebögen beurteilt sich nach § 28 Abs. 1 Nr. 1 BDSG, wonach das Erheben, Speichern und Nutzen personenbezogener Daten zulässig ist, soweit dies der Zweckbestimmung des Mietvertrages oder eines vertragsähnlichen Vertrauensverhältnisses (hier: Bewerbung um eine Wohnung) dient.

Das Informationsinteresse des Vermieters resultiert aus seinem Interesse an einem zahlungsfähigen Mieter und dient damit der Absicherung gegenüber Zahlungsausfällen. Dem gegenüber steht das Persönlichkeitsrecht des Mietinteressenten, welches vor Eingriffen in die Intim- und Privatsphäre und auch vor Diskriminierungen zu schützen ist. Diese gegenläufigen Interessen sind gegeneinander abzuwägen. Im Ergebnis treffen den potenziellen Mieter Aufklärungspflichten nur für solche Umstände, die für den Vermieter bei objektiver Bewertung und Berücksichtigung schutzwürdiger Belange des Mietinteressenten der Auskunft bedürfen.

3.3.2.2 Detailbetrachtungen

Bei der datenschutzrechtlichen Bewertung der Fragebögen ist zwischen den Personen, über die Daten erfragt werden, und den Datenarten zu unterscheiden.

a) **Betroffene**

- **Vertragspartner (Mieter, Mitmieter)**

  Grundsätzlich dürfen nur über den Vertragspartner detaillierte Angaben erfragt werden und nicht über andere Personen, da ein Vermieter keine Forderungen diesen gegenüber geltend machen oder durchsetzen kann.

  Grundsätzlich sind die Fragebögen von allen Vertragspartnern zu unterzeichnen (Umsetzung des Direkterhebungsprinzips).

- **Mitziehende Kinder**

  Um beurteilen zu können, ob eine Wohnung bestimmungsgemäß genutzt wird, reichen

Angaben zur Familiengröße bzw. zur Anzahl der Kinder, die mit einziehen, aus.

Nicht zulässig sind somit insbesondere folgende Angaben über Kinder:

- Name und Vorname,
- Staatsangehörigkeit/Nationalität,
- Geburtsort, -datum, Alter,
- Verwandtschaftsverhältnis zum Vertragspartner,
- Beruf/Tätigkeit.

- **Mitziehende erwachsene Personen**

  Detaillierte Angaben zu mitziehenden Personen sind lediglich bei Tod des Mieters (Fortsetzung des Mietverhältnisses) oder aber bei Räumungsklagen (eigenständiges Besitzrecht von Nichtmietern) von Bedeutung:

  Ehepartner bzw. Lebensgefährten

  Eine Abfrage von Name, Vorname und Geburtsdatum des Ehepartners bzw. Lebenspartners wird als zulässig erachtet.

  Die Frage nach dem Verhältnis zum Mieter sollte unterbleiben.

  Ein nach den Bestimmungen des Datenschutzes gestalteter Fragebogen muss unter Beachtung des Direkterhebungsgrundsatzes Unterschriftsfelder für mitziehende Personen enthalten.

b) **Datenarten**

Die Bewertung der Kontrollen ergab Folgendes:

- **Name, Vorname, Geburtsdatum, Anschrift, Angaben zur gewünschten Wohnung:**

  Eine Abfrage dieser Daten ist zulässig.

- **Telefon/E-Mail:**

  Die Frage des Vermieters nach einer Möglichkeit der telefonischen Erreichbarkeit ist zulässig (hilfreich z. B. bei eventuellen Rückfragen oder Terminabsprachen). Jedoch sollte es dem Mietinteressenten überlassen bleiben, welche Telefonnummer (dienstlich, privat, mobil) er auf dem Fragebogen angibt. Bei der Abfrage der E-Mail-Adresse erscheint eine Kennzeichnung als freiwillige Angabe angemessen.

- **Geburtsort, Geburtsname:**

  Die Angabe des Namens, des Vornamens, des Geburtsdatums, der gegenwärtigen (vor Mietvertragsabschluss) und der zukünftigen (nach Mietvertragsabschluss) Wohnanschrift im Mietvertrag ist ausreichend. Die Erhebung und Speicherung von Geburtsname und -ort ist für die Durchführung des Mietverhältnisses bzw. die Durchsetzung daraus resultierender Ansprüche nicht erforderlich und deshalb nicht zulässig.

- **Legitimation:**

  Nach § 4 Abs. 1 des Sächsischen Gesetzes über Personalausweise und zur Ausführung des Passgesetzes (SächsPersPassG) können Personalausweise auch im nicht-öffentlichen Bereich zur Legitimation genutzt werden. Unzulässig hingegen sind die Erhebung und Speicherung der Ausweisnummer, der ausstellenden Behörde, des Ausstellungsdatums, der Gültigkeitsdauer oder gar die Anfertigung von Personalausweiskopien.

- **Genossenschaftsmitgliedschaft:**

  Der Bezug einer Genossenschaftswohnung ist an eine Mitgliedschaft in der Genossenschaft geknüpft. Eine Abfrage ist in diesen Fällen zulässig. Dies trifft darüber hinaus auch auf die Abfrage der Mitgliedschaft in einer anderen Wohnungsgenossenschaft zu (Konkurrenzregel des § 68 Genossenschaftsgesetz [GenG]).

- **Behinderungen:**

  Die Frage nach dem Vorliegen einer Behinderung ist grundsätzlich unzulässig.

- **Nationalität/Staatsangehörigkeit/Aufenthaltsgenehmigung:**

  Grundsätzlich ist die Abfrage dieser Daten unzulässig (so auch AG Wiesbaden, WuM 1992, S. 597 sowie Sternel, Mietrecht 3. Aufl. 1988, Rdnr. I S. 262). Vor dem Hintergrund des im Berichtszeitraum am 18. August 2006 in Kraft getretenen Allgemeinen Gleichbehandlungsgesetzes (AGG) gilt dies auch für Daten über die Rasse und ethnische Herkunft des Mietbewerbers; vgl. §§ 19 Abs. 3, 33 Abs. 2 AGG i. V. m. Artikel 5 der Antirassismus-Richtlinie 2000/43/EG. Allenfalls könnten die Daten vom Mietbewerber dann erhoben werden, wenn Wohnraum in Gebieten angeboten wird, in denen eine stabile und ausgewogene Bewohner- und Siedlungsstruktur bereits gefährdet oder gar nicht mehr vorhanden ist. Rechtsgrundlage für die Datenerhebung ist in dem Fall § 28 Abs. 1 Nr. 2 BDSG.

  Klarstellend sei in dem Zusammenhang darauf hingewiesen, dass das im AGG genannte

Merkmal „ethnische Herkunft“ EG-rechtlich auszulegen und damit in einem weiten Sinne zu verstehen ist. Dazu zählen insbesondere auch Benachteiligungen infolge der Hautfarbe, der Abstammung, des nationalen Ursprungs und des Volkstums.

- **Arbeitgeber/Beruf/Tätigkeit:**

  Bereits 1986 stellte das Amtsgericht Stuttgart fest, dass seitens des Vermieters kein Sicherungsbedürfnis dahingehend bestehe, dass der Mieter an einem bestimmten Arbeitsplatz seinen Lebensunterhalt verdienen müsse. Insofern bestehe auch keine Pflicht des Mietinteressenten mitzuteilen, wer sein Arbeitgeber sei (WuM 1986, S. 331).

  Demnach ist die Abfrage zum Arbeitgeber, zum Beruf bzw. zur aktuellen Tätigkeit unzulässig. Entscheidend für den Vermieter ist, dass dem Mieter ein ausreichendes Einkommen zum Bestreiten der Mietkosten zur Verfügung steht und ggf., dass der Mietbewerber diese aus seinem Einkommen bestreiten kann.

- **Einkommenshöhe und -bestandteile, finanzielle Verpflichtungen:**

  Die Frage nach dem monatlich zur Verfügung stehenden Geldbetrag und deren Zusammensetzung ist zulässig. Dem Vermieter wird es so ermöglicht abzuschätzen, ob die Zahlung der Miete gewährleistet ist.

  Nicht zulässig hingegen sind Abfragen zu eventuell bestehenden Bürgschaften.

- **Einkommensnachweise:**

  Diese Problematik betrifft die Vorlage von Verdienstbescheinigungen, Renten- oder Steuerbescheiden bzw. Bescheinigungen des Steuerberaters als Nachweis des im Fragebogen angegebenen Einkommens. Diese Bescheinigungen enthalten aber neben der Summe des Einkommens auch Daten, deren Kenntnis nicht im berechtigten Interesse des Vermieters liegt, z. B. die Kenntnis der Daten auf einem Steuerbescheid, auf dessen Vorlage Selbständige zurückgreifen müssten. Auch die Kenntnis des Arbeitgebers bzw. der ausgeübten Tätigkeit ist für das Mietverhältnis nicht erforderlich.

  Darüber hinaus ist fraglich, ob die Vorlage eines Einkommensnachweises z. B. zum Schutz vor so genannten „Mietnomaden“ überhaupt geeignet ist. (Als Mietnomaden werden Personen bezeichnet, die von einer Mietwohnung in die nächste ziehen, mit dem Vorsatz, keine Miete zu zahlen.) In den meisten Fällen ist hierbei jedoch nicht von einer Zahlungsunfähigkeit, sondern einer Zahlungsunwilligkeit auszugehen.

- **Eidesstattliche Versicherung, Privatinsolvenz:**

  Die Frage nach der Abgabe einer eidesstattlichen Erklärung innerhalb der letzten drei Jahre ist ebenso zulässig wie die Frage, ob der Mietbewerber von einer Privatinsolvenz (Verbraucherinsolvenz) betroffen war. Beides hätte zweifellos erhebliche Auswirkungen auf das zukünftige Mietverhältnis, die der Vermieter bei weiteren Vertragsverhandlungen entsprechend berücksichtigen müsste.

- **Aktuelle(s)/Frühere(s) Mietverhältnis(se):**

  Von Seiten der Vermieter wird meist nach den Beweggründen für den Wohnungswechsel gefragt. Unter anderem können folgende Angaben von Interesse sein:

  - Name, Anschrift des derzeitigen Vermieters,
  - Gründe für Wohnungswechsel (Kündigung [Grund], Freilenkung, Miethöhe, Wohnungsmängel, Familienzuwachs, Familientrennung, Gründung eines eigenen Hausstandes etc.),
  - Kündigungsfrist,
  - Schuldenfreiheitserklärung des Vorvermieters,
  - Zeitdauer des Mietverhältnisses,
  - Anschriften der letzten drei Jahre,
  - derzeitiger Mieterstatus (Haupt- oder Untermieter, wohnhaft bei Eltern),
  - derzeitiger Mietzins,
  - derzeitige Wohnungsgröße/Zimmeranzahl,
  - Mietrückstände,
  - Räumungsverfahren.

  Für das angestrebte Mietvertragsverhältnis wesentlich und dem Mietinteressenten zumutbar sind dabei Fragen, die Rückschlüsse auf das Zahlungsverhalten des Mietinteressenten erlauben. Dazu gehören Aussagen zu Mietrückständen ebenso wie zu Räumungsverfahren. Auch eine Schuldenfreiheitserklärung des Vorvermieters wird als zulässig erachtet. Für eine Abfrage des derzeitigen Vermieters muss die Einwilligung des Betroffenen eingeholt werden. Eine Abfrage darüber hinausgehender Sachverhalte ist nicht erforderlich und damit unzulässig. Die Frage nach dem Bestehen eines Mietverhältnisses mit dem gleichen Vermieter zu einem früheren Zeitpunkt hingegen ist zulässig.

- **Haustiere:**

  Ist die Haustierhaltung laut Mietvertrag grundsätzlich erlaubt, erübrigt sich die Fragestellung. In Mietverträgen ohne Regelungen zur Haltung von Haustieren dürfen Kleintiere gehalten werden, von denen nach der Rechtsprechung „weder Störungen noch Schäden ausgehen“ (Beispiele: Haltung von Hamstern, Meerschweinchen, Fischen, Ziervögeln und Zwergkaninchen). Diese gehören zum vertragsgemäßen Gebrauch der Mietsache. Erfahrungsgemäß bestehen jedoch unterschiedliche Auffassungen darüber, was als Kleintier zu betrachten ist (Beispiel: Hund/Katze). Die Abfrage nach der Haltung von Haustieren wird deshalb als zulässig erachtet.

- **Musikinstrumente:**

  Grundsätzlich ist Musikausübung in einem Mietshaus Teil des normalen Wohngebrauchs. Das Spielen von Musikinstrumenten in angemessenem zeitlichem Umfang ist somit kein Kündigungsgrund für den Vermieter. Die Frage nach gespielten Musikinstrumenten ist daher grundsätzlich unzulässig.

  Soweit der Vermieter mit dieser Abfrage bezweckt, Mieter mit ähnlichen Interessen (z. B. Musikstudenten) in einzelnen Mietobjekten unterzubringen, sollte dem Mietinteressenten die Angabe zum Betreiben von Musikinstrumenten freigestellt bleiben (Kennzeichnung).

- **Familienstand, Sozialstatus:**

  Ohne Relevanz für das zukünftige Mietverhältnis ist der Familienstand des Mietbewerbers bzw. das Verwandtschaftsverhältnis zu einem eventuellen Mitmieter. Gleiches gilt für den Sozialstatus (Einzelperson, Ehepaar mit Kindern, Lebensgemeinschaft, Alleinerziehende, Großfamilie, Seniorenehepaar). Für den Vermieter ist zunächst entscheidend, wer als Vertragspartner (Mieter, Mitmieter) auftritt; ferner kann von Bedeutung sein, welche erwachsenen Personen mit in die Wohnung ziehen.

- **Bankverbindung:**

  Die Bankverbindung ist ein Datum, welches frühestens bei Abschluss eines Mietvertrages erforderlich wird. Die Abfrage im Rahmen der Selbstauskunft eines Mietinteressenten ist unzulässig, da zu diesem Zeitpunkt nicht abzusehen ist, ob es zu einem Mietverhältnis kommen wird.

- **Wohnberechtigungsschein, Wohngeldanspruch:**

  Soweit die Förderbedingungen für im Rahmen von Förderprogrammen gebaute Objekte

die Vorlage eines Wohnberechtigungsscheines vorsehen, ist diese Abfrage zulässig.

Die Information, ob ein Mietinteressent ggf. Anspruch auf Wohngeld hat oder dieses bezieht, ist für den Vermieter dagegen nur mittelbar von Bedeutung. Das heißt, dieser Betrag ist durch den Mietinteressenten bei der Ermittlung seines Einkommens zu berücksichtigen.

- **Vorstrafen, laufende Ermittlungsverfahren:**

  Der Mietinteressent ist nicht verpflichtet, gegen ihn anhängige staatsanwaltschaftliche Ermittlungsverfahren zu offenbaren oder darauf abzielende Nachfragen des Vermieters wahrheitsgetreu beantworten zu müssen (AG Hamburg, WuM 1992, S. 598). Ebenso wenig umfasst die Aufklärungspflicht eines Mietinteressenten eventuelle Vorstrafen (AG Rendsburg, WuM 1990, S. 507).

Fragen nach

- Mitgliedschaft im Mieterverein,
- Parteizugehörigkeit,
- Religionszugehörigkeit,
- Familienplanung/Kinderwunsch,
- bestehenden Schwangerschaften,
- Hobbys,
- Wohnstil oder
- Rechtsschutzversicherung

sind unzulässig.

3.3.3 Fremdauskünfte/Bonitätsfragen

3.3.3.1 Ergebnisse der Stichprobenkontrollen

Neben Mieterselbstauskünften holen Vermieter zur weiteren Bonitätsprüfung mitunter auch Fremdauskünfte über Mietinteressenten ein. Bei 29 von 46 in Sachsen kontrollierten wohnungswirtschaftlichen Unternehmen wurde keine Bonitätsabfrage bei der SCHUFA bzw. bei Wirtschaftsauskunfteien durchgeführt. In zehn Fällen hingegen haben sich Vermieter vor Abschluss eines Mietvertrages mit einer SCHUFA-Abfrage über die Bonität des Mietinteressen-

ten rückversichert bzw. sich diese Möglichkeit offen gehalten und dies mit einer SCHUFA-Klausel legitimiert. In neun Fällen wurde gelegentlich (alternativ oder ergänzend) auf Wirtschaftsauskunfteien (Bürgel, Creditreform) zurückgegriffen. Eine Information der Betroffenen erfolgte dabei nicht. In zwei Fällen wurden in unzulässiger Weise Generalklauseln verwendet, mit denen die Betroffenen ihre Einwilligung zum Einholen von Auskünften von nicht näher bezeichneten Stellen erteilen sollten.

3.3.3.2 SCHUFA-Abfragen

Seit 2001 können Vermieter wieder als so genannte „B-Vertragspartner“ Auskünfte zu Mietinteressenten durch die SCHUFA erhalten. Im Gegensatz zum „A-Verfahren“, das überwiegend für Banken gedacht ist, gibt die SCHUFA hierbei ausschließlich Negativdaten, also Informationen über nicht-vertragsgemäßes Verhalten des Betroffenen, heraus. Aus datenschutzrechtlicher Sicht problematisch ist, dass die SCHUFA diese Daten aus ihrem gesamten Datenbestand beauskunftet, d. h., dass der Vermieter z. B. auch über vergleichsweise geringe Zahlungsrückstände des Betroffenen - z. B. eine nicht bezahlte Handy-Rechnung - informiert werden kann. Dies führt unter Umständen dazu, dass der Vermieter einem Mietvertragsverhältnis mit dem Betroffenen aus dem Wege geht.

Die aktuell verwendete SCHUFA-Klausel (Stand: August 2005) hat folgenden Inhalt:

„Ich willige ein, dass der Vermieter[1] der SCHUFA Holding AG, Kormoranweg 5, 65201 Wiesbaden, Daten über die Beantragung dieses Mietvertrages übermittelt und Auskünfte über mich von der SCHUFA erhält.

Unabhängig davon wird die Firma[1] auch Daten aufgrund nichtvertragsgemäßen Verhaltens (z. B. Forderungsbetrag nach Titulierung im Anschluss einer Kündigung gemäß §§ 543 Abs. 2 Nr. 3, 569 Abs. 3 BGB bzw. wegen Zahlungsverzug nach § 573 Abs. 2 Nr. 1 BGB) übermitteln. Diese Meldungen dürfen nach dem Bundesdatenschutzgesetz nur erfolgen, soweit dies nach Abwägung aller betroffenen Interessen zulässig ist.

Die SCHUFA speichert und übermittelt die Daten an ihre Vertragspartner im EU-Binnenmarkt, um diesen Informationen zur Beurteilung der Kreditwürdigkeit von natürlichen Personen zu geben. Vertragspartner der SCHUFA sind vor allem Kreditinstitute, Kreditkarten- und Leasinggesellschaften. Daneben erteilt die SCHUFA Auskünfte an Handels-, Telekommunikations- und sonstige Unternehmen, die Leistungen und Lieferungen gegen Kredit gewähren. Die SCHUFA stellt personenbezogene Daten nur zur Verfügung, wenn ein berechtigtes Inte-

resse hieran im Einzelfall glaubhaft dargelegt wurde. Zur Schuldnerermittlung gibt die SCHUFA Adressdaten bekannt. Bei der Erteilung von Auskünften kann die SCHUFA ihren Vertragspartnern ergänzend einen aus ihrem Datenbestand errechneten Wahrscheinlichkeitswert zur Beurteilung des Kreditrisikos mitteilen (Score-Verfahren).

Ich kann Auskunft bei der SCHUFA über die mich betreffenden gespeicherten Daten erhalten. Weitere Informationen über das SCHUFA-Auskunfts- und Score-Verfahren enthält ein Merkblatt, das auf Wunsch zur Verfügung gestellt wird. Die Adresse der SCHUFA lautet

SCHUFA Holding AG, Verbraucherservice, Postfach 5640, 30056 Hannover.

Unterschrift

---

[1] zu personalisieren“

Bei der Formulierung der SCHUFA-Klausel wurden die datenschutzrechtlichen Hinweise und Empfehlungen der Aufsichtsbehörden weitestgehend berücksichtigt. Vor allem die Transparenz des Verfahrens ist für den Betroffenen damit gewährleistet. Vermieter sollten deshalb prüfen, ob die von ihnen ggf. verwendete SCHUFA-Klausel dem aktuellen Stand entspricht.

3.3.3.3 Auskünfte von Wirtschaftsauskunfteien und Brancheninternen Warnsystemen

Wirtschaftsauskunfteien erteilen auf der Grundlage der §§ 28 bzw. 29 BDSG grundsätzlich allen berechtigten Interessenten Vollauskünfte. Grundsätzlich gilt auch hier, dass die schutzwürdigen Interessen der Betroffenen (hier: existenzielle Bedeutung der Wohnung für die private Lebensgestaltung des Mietinteressenten) gegen die berechtigten Interessen des Vermieters abzuwägen sind.

Die Tatsache, dass Wirtschaftsauskunfteien Vermietern den gesamten Datenkatalog zum Betroffenen übermitteln, ist aus datenschutzechtlicher Sicht problematisch. Nach Auffassung der Aufsichtsbehörden dürfen neben Daten aus allgemein zugänglichen Quellen nur so genannte harte, d. h. objektiv feststehende Negativdaten beauskunftet werden. Dies wäre z. B. das Vorliegen eines vollstreckbaren Titels oder einer Privatinsolvenz. Das Auskunftsmerkmal „Zahlungsverhalten“ hingegen wäre nicht im Datenkatalog der zu übermittelnden Daten enthalten.

Brancheninterne Warnsysteme haben gegenüber Wirtschaftsauskunfteien den Vorteil, dass branchenfremde Informationen weitestgehend von der Übermittlung ausgeschlossen sind und sich diese Systeme somit innerhalb des Rechtskreises Mietverhältnis bewegen. Ausnahmen

bilden lediglich Daten aus den öffentlichen Schuldnerverzeichnissen, die regelmäßig mit in die Datenbestände derartiger Warnsysteme einfließen. Der Bonitätsprüfung von Mietbewerbern wird damit nur das bisherige Zahlungsverhalten im Zusammenhang mit Mietverhältnissen zugrunde gelegt. Dabei sollte jedoch berücksichtigt werden, dass etwaige Zahlungsrückstände nicht unbedingt auf ein generell schlechtes Zahlungsverhalten des Mietbewerbers schließen lassen. Die verarbeiteten Datenkataloge müssen sich auf harte Negativmerkmale (mietrechtliche Gerichtsentscheidungen) beschränken.

Folgende Daten dürfen durch brancheninterne Warnsysteme an Vermieter übermittelt werden:

- Daten aus öffentlichen Schuldnerverzeichnissen,
- rechtskräftige Titel zu Zahlungsverzug im Mietbereich,
- rechtskräftige Urteile zur fristlosen Kündigung wegen Zahlungsverzug oder sonstiger mietrechtlicher Vertragsverletzungen,
- rechtskräftige Räumungsurteile wegen fristloser Kündigung sowie
- Zahlungsrückstände von zwei Monatsmieten innerhalb der ersten drei Monate nach Mietbeginn, soweit bereits ein Strafantrag gestellt worden ist (Mietnomadentum).

Im Übrigen erfordert das Einholen von Wirtschaftsauskünften durch den Vermieter die vorherige Information der Mietinteressenten (z. B. im Rahmen der Selbstauskunft). Die Mietinteressenten können sich so rechtzeitig auf diesen Umstand einstellen. Eine nachträgliche Benachrichtigung des Betroffenen durch den Vermieter (§ 33 Abs. 1, Abs. 2 Nr. 1 BDSG) ist dann nicht mehr erforderlich.

3.3.4 Datenschutzrechtliche Vereinbarungen im Mietvertrag

3.3.4.1 Ergebnisse der Stichprobenkontrollen

Geprüft wurden unter anderem (Muster-)Mietverträge der von der Kontrolle betroffenen Unternehmen. In der deutlichen Mehrzahl der Fälle wurden keinerlei datenschutzrechtlich relevante Regelungen im Mietvertrag getroffen. Lediglich drei der 18 vom Regierungspräsidium Dresden eingesehenen Mietverträge enthielten eine Klausel, mit der die Mieter der Speicherung ihrer zur Erfüllung des Mietvertrages erforderlichen Daten zustimmen sollten.

3.3.4.2 Regelungsbedarf

Gemäß § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zulässig, wenn dies eine Rechtsvorschrift (inkl. des BDSG selbst) erlaubt oder der Betroffene eingewilligt hat (Verbot mit Erlaubnisvorbehalt).

Für die Datenverarbeitung im Rahmen des Mietvertragsverhältnisses bietet § 28 Abs. 1 Nr. 1 BDSG eine ausreichende Rechtsgrundlage. Demnach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten bzw. deren Nutzung grundsätzlich zulässig, wenn es der Zweckbestimmung des Mietverhältnisses mit dem Betroffenen dient. Zwischen dem Mietverhältnis und der Datenverarbeitung muss ein unmittelbarer sachlicher Zusammenhang bestehen. Zulässig ist nur die Verarbeitung und Nutzung der Daten, die zur Abwicklung des Vertrages, also der Wahrnehmung der Rechte hieraus, erforderlich sind.

Spezielle Regelungen zum Datenschutz im Mietvertrag sind nicht erforderlich. Auch einer Einwilligung des Betroffenen in die Verarbeitung seiner Daten bedarf es nicht. Diese käme als Grundlage ohnehin nicht in Betracht, da die Freiwilligkeit der Einwilligung nicht gewährleistet wäre.

3.4 Erfolgskontrolle bei Wohnungsunternehmen

Die Ergebnisse der koordinierten Datenschutzkontrolle bei Wohnungsunternehmen wurden im Internet veröffentlicht und auch den sächsischen Verbänden der Wohnungswirtschaft zur Verfügung gestellt. Auf diese Weise gelang es, die Landes- und Unternehmensverbände für datenschutzrechtliche Probleme zu sensibilisieren und sie anzuhalten, durch gezielte Information ihrer Mitglieder letztlich zur Verbesserung des Datenschutzniveaus bei den verbandsangehörigen Genossenschaften bzw. Unternehmen beizutragen.

Im Nachgang zur koordinierten Datenschutzkontrolle wurde eine Erfolgskontrolle bei solchen Wohnungsunternehmen durchgeführt, die vorher noch keiner datenschutzrechtlichen Überprüfung unterzogen worden waren. Im Rahmen dieser Kontrollaktion wurden innerhalb des Regierungsbezirkes Dresden alle Wohnungsgenossenschaften mit mehr als 1000 Wohneinheiten (WE) um Auskunft zu

- der Bestellung und Fachkunde eines betrieblichen Datenschutzbeauftragten,
- der Verpflichtung der Mitarbeiter auf das Datengeheimnis sowie
- dem Öffentlichen Verfahrensverzeichnis

gebeten. Die Auswertung der Überprüfung der 16 Genossenschaften ergab Folgendes:

Vier Genossenschaften waren aufgrund ihrer zu geringen Beschäftigtenzahlen nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. In den verbleibenden Genossenschaften war jeweils ein Datenschutzbeauftragter bestellt. Bei fünf Genossenschaften erfolgte die Bestellung bereits vor der koordinierten Datenschutzkontrolle; bei den übrigen Genossenschaften erst im Jahr 2005 bzw. Anfang 2006.

15 Genossenschaften hatten ihre Mitarbeiter auf der Grundlage ordnungsgemäßer Verpflichtungserklärungen zur Einhaltung des Datengeheimnisses verpflichtet.

Eine Genossenschaft (ohne Datenschutzbeauftragten) konnte kein öffentliches Verfahrensverzeichnis vorweisen; die Verzeichnisse der übrigen Genossenschaften wiesen teilweise erhebliche Mängel auf. Wesentliche Kritikpunkte waren dabei vor allem

- die lediglich unternehmensbezogene Darstellung der Zweckbestimmung der Datenverarbeitung (keine Definition einzelner Verfahren),
- die fehlende Abgrenzung der Angaben nach § 4e Satz 1 Nr. 5 bis 7 BDSG einzelner Verfahren (zusammengefasste Darstellung für alle Verfahren),
- die fehlende Angabe der mit der Leitung der Datenverarbeitung beauftragten Personen,
- die zu weite Verallgemeinerung der Angaben nach § 4e Satz 1 Nr. 5 bis 7 BDSG.

Die notwendige Überarbeitung der Verfahrensverzeichnisse wird durch die Aufsichtsbehörde entsprechend begleitet.

Die dargestellten Ergebnisse verdeutlichen, mit welchen gesetzlichen Vorgaben die Unternehmen besondere Umsetzungsschwierigkeiten haben. Die Aufsichtsbehörde hat daraus die entsprechenden Schwerpunkte für die zukünftige Beratungstätigkeit sowie für die Erarbeitung unterstützender Arbeitsmaterialien abgeleitet.

3.5 Erfolgskontrolle bei Wohlfahrtsverbänden

Auch bei Vereinen und Verbänden der Freien Wohlfahrtspflege wurde eine vergleichbare Erfolgskontrolle durchgeführt. Anlass dazu gab eine in den Jahren 2003/2004 durchgeführte koordinierte Datenschutzkontrolle in Altenpflegeheimen (vgl. 2. TB: Pkt. 4.2.2), deren Endauswertung veröffentlicht und auch den sächsischen Spitzenverbänden der freien Wohlfahrtspflege zur Verfügung gestellt wurde.

Von den acht bis zum Ende des Berichtszeitraums überprüften Vereinen war in drei ord-

nungsgemäß ein Datenschutzbeauftragter bestellt. Zwei der übrigen Vereine waren gesetzlich nicht zur Bestellung verpflichtet. Die Kontrolle in den restlichen Fällen ergab, dass entweder kein Datenschutzbeauftragter bestellt war oder dessen Bestellung schwerwiegende Mängel aufwies. Die Verpflichtung der Mitarbeiter auf das Datengeheimnis war lediglich in der Hälfte der Fälle ordnungsgemäß vorgenommen worden. Bei drei Vereinen beschränkte sich die Verpflichtung auf die Forderung nach Verschwiegenheit; in einem Fall fehlte sie ganz. Lediglich ein Verein wies ein ordnungsgemäßes öffentliches Verfahrensverzeichnis nach und blieb insoweit frei von Beanstandungen. Die Verzeichnisse von zwei weiteren Vereinen wiesen erhebliche Mängel auf; in den übrigen Fällen war noch kein Verfahrensverzeichnis angelegt worden.

Die betreffenden Vereine sind aufgefordert worden, die festgestellten Mängel zu beseitigen und die Aufsichtsbehörde hierüber zu unterrichten.

4 Anlassaufsicht

4.1 Überblick

„Die Aufsichtsbehörde kontrolliert die Ausführung des BDSG 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 Mitgliedstaaten in den Fällen des § 1 Abs. 5“ (§ 38 Abs. 1 Satz 1 BDSG).

Anlasskontrollen werden immer dann durchgeführt, wenn der Aufsichtsbehörde Anhaltspunkte für eine Datenschutzverletzung vorliegen, z. B. auf Grund der Eingabe eines Bürgers. Im Rahmen der Anlasskontrolle wird auch kontrolliert, ob die allgemeinen datenschutzrechtlichen Bestimmungen durch die zu überprüfende Stelle eingehalten werden. Dazu gehören zum Beispiel die Pflicht zur Bestellung eines Datenschutzbeauftragten, die Verpflichtung der Mitarbeiter auf das Datengeheimnis und die Führung eines öffentlichen Verfahrensverzeichnisses.

Im Berichtszeitraum nahmen die Aufsichtsbehörden branchenübergreifend insgesamt 173 Anlasskontrollen vor. Im Vergleich zu den vorangegangenen Berichtszeiträumen hat sich die Anzahl weiter erhöht. Die Kontrollen erfolgten vor Ort oder im schriftlichen Verfahren.

Berichtszeitraum	**2001/2002**	**2003/2004**	**2005/2006**
Eingang	116	147	164
Übernahme Vorjahr	3	6	9
- Kontrollen vor Ort	18	24	17
- schriftliches Verfahren	101	129	156
Begründet	50	65	62
Abgewiesen	36	53	65
Keine Zuständigkeit	27	26	31
Noch in Bearbeitung	6	9	15

Die durch die Aufsichtsbehörde festgestellten Verstöße betrafen im Wesentlichen folgende Sachverhalte:

Videoüberwachung

- Überwachungsmonitore in einem Freizeitbad (vgl. Pkt. 4.2.1.1),
- Webcams in Einzelhandelsgeschäften (vgl. Pkt. 4.2.1.2),
- Überwachung von Hauseingängen, Gehwegen und Straßen (vgl. Pkt. 4.2.1.3),
- Überwachung im Massage-Studio (vgl. Pkt. 4.2.1.4),
- Überwachung eines Bratwurststandes (vgl. Pkt. 4.2.1.5),
- Überwachung von Außensitzplätzen eines Restaurants.

Datenverarbeitung für Werbezwecke

- Werbeprospekt statt Löschungsbestätigung (vgl. Pkt. 4.2.2.1),
- Versand von E-Mail-Newslettern (vgl. Pkt. 4.2.2.2),
- Auskunft über die Datenherkunft (vgl. Pkt. 4.2.2.5),

- Beachtung von Widersprüchen (§ 28 Abs. 4 Satz 2 BDSG),
- Anrufe zu Werbezwecken ohne Einwilligung der Betroffenen,
- Unterrichtung über das Widerspruchsrecht (§ 28 Abs. 4 Satz 2 BDSG).

Arbeitnehmerdatenschutz

- Erhebung von Bewerberdaten durch einen Personaldienstleister (vgl. Pkt. 4.2.3.1),
- Übermittlung von Personaldaten bei Einschaltung eines Privatdetektivs (vgl. Pkt. 4.2.3.2),
- Archivierung von Bewerbungsunterlagen bei Ablehnung,
- Entsorgung von Bewerbungs- und Kundenunterlagen in Müllcontainer,
- Vernichtung von Bewerbungsunterlagen ohne Kenntnis des Betroffenen,
- Veröffentlichung personenbezogener Daten im Betriebsjournal.

Einzelhandel

- Personalausweiskopien bei Barzahlung mit 500-€-Scheinen (vgl. Pkt. 4.2.4),
- Erhebung von Personalausweisdaten bei Bezahlung mit EC-Karte (vgl. 2. TB, Pkt. 4.3.10).

Sparkassen/Banken

- Bekanntgabe vertraulicher Daten im Sichtfenster eines Briefumschlages (vgl. Pkt. 4.2.5.1),
- Anzeige personenbezogener Daten am Kontoauszugsdrucker (vgl. Pkt. 4.2.5.2).

Betrieblicher Datenschutzbeauftragter

- Datenschutzbeauftragter im Großraumbüro (vgl. Pkt. 4.2.6),
- Abberufung eines betrieblichen Datenschutzbeauftragten.

Freiberufler

- Datenübermittlung durch einen Steuerberater (vgl. Pkt. 4.2.7.1),
- Verarbeitung und Nutzung von Kundendaten nach Beendigung eines Handelsvertreterver-trages (vgl. Pkt. 4.2.7.2).

Freie Wohlfahrtspflege

- Schweigepflichtentbindungsklauseln in Nebenverdienst-Verträgen,
- Fragebögen zur Erfassung von Besucherdaten in Suchtberatungsstellen.

Verfahrensverzeichnis

- Änderungsmeldungen gegenüber der Aufsichtsbehörde (s. Pkt. 9),
- Verfügbarmachen des Öffentlichen Verfahrensverzeichnisses (§ 4g Abs. 2 BDSG).

Wohnungswirtschaft

- Inhalt von Mieterselbstauskunftsformularen (s. Pkt. 3.3.2).

Gesundheitswesen

- Datenübermittlung durch Fehlfunktionen eines Medizin-Management-Programms (vgl. Pkt. 4.2.8.1),
- Weitergabe von Patientendaten nach Praxisaufgabe (vgl. Pkt. 4.2.8.2).

Handels- und Wirtschaftsauskunfteien

- Datenspeicherung und -übermittlung trotz Auskunftssperre nach § 34 SächsMG.

Versicherungen

- Datenweitergabe an Abschlepp- und Reparaturfirmen (vgl. Pkt. 4.2.9).

Verkehrswesen

- Datenerhebung bei erhöhtem Beförderungsentgelt (vgl. Pkt. 4.2.10).

Sonstiges

- Veröffentlichung personenbezogener Daten im Internet,
- Auskunftsgewährung nach § 34 BDSG,
- Unterrichtungspflichten bei formularmäßiger Datenerhebung (§ 4 Abs. 3 BDSG),
- Inhaltliche und formale Anforderungen an Einwilligungsklauseln (§ 4a BDSG).

Zahlreiche Eingaben betrafen vor allem Videoüberwachungsmaßnahmen durch nichtöffentliche Stellen. Die Kontrollen ergaben, dass die meisten verantwortlichen Stellen datenschutzgerecht mit personenbezogenen Daten umgehen. Auch den Betroffenen selbst kommt eine wichtige Rolle beim Schutz ihrer personenbezogenen Daten zu. Indem sie aktiv ihre Rechte wahrnehmen, bewusst und restriktiv mit ihren eigenen Daten umgehen, insbesondere auch Datenerhebungen kritisch hinterfragen, können viele Probleme von Beginn an vermieden werden.

4.2 Ausgewählte Sachverhalte

4.2.1 Videoüberwachung

4.2.1.1 Überwachungsmonitore in einem Freizeitbad

Eine Petentin beschwerte sich über die von einem Freizeitbad durchgeführte Videoüberwachung. Sie war mit einer Gruppe von jungen Müttern und deren Kindern nach dem Bad unbekleidet gefilmt worden. Aus Platzmangel und weil sich die Frauen unbeobachtet wähnten, nutzten sie zum Ankleiden nicht die vorhandenen Umkleidekabinen, sondern zogen sich direkt vor den Garderobenschränken im Gang um. Dieser Bereich des Bades wurde jedoch von Videokameras überwacht, wobei die Bilder der Kamera auf einen von den Besuchern des Bades gut einsehbaren Monitor im stark frequentierten Kassenbereich des Freizeitbades übertragen wurden. Beim Verlassen des Bades entdeckte eine der Mütter, dass sie auf dem Bildschirm einige Personen aus der Gruppe beobachten konnte, die sich zu der Zeit noch ankleideten.

Die Aufsichtsbehörde nahm den geschilderten Vorfall zum Anlass für eine Kontrolle der Videoüberwachung in diesem und anderen Freizeitbädern. Dabei stellte sich heraus, dass von den zehn kontrollierten Freizeitbädern nur eines ganz auf Videoüberwachungsmaßnahmen verzichtete. Überwacht werden vor allem die Gänge vor den Garderobeschränken sowie unfallgefährdete bzw. schlecht einsehbare Badebereiche. Darüber hinaus sind Kameras zum Teil auch im Eingangs- und Kassenbereich, in Einzelfällen auch an der Außenfront sowie auf dem Besucherparkplatz zu finden.

Die Videoüberwachung dient vor allem dem Schutz des Eigentums des Badbetreibers und der Badbesucher vor Schrankaufbrüchen und Diebstählen. Die Installation der Kameras habe zu einem massiven Rückgang, in vielen Fällen sogar zum Ausbleiben derartiger Vorkommnisse geführt.

Darüber hinaus sei die Videoüberwachung auch eine Maßnahme zur Gewährleistung der Sicherheit beim Badebetrieb. Im Gegensatz zu Freibädern, in denen es oft nur ein großes und überschaubares Becken gibt, sind in Freizeitbädern zahlreiche Becken, Badelandschaften und entsprechende technische Anlagen zu finden, die für das Aufsichtspersonal teilweise nicht oder nur schwer von deren Standort aus einsehbar sind. Durch die Videoüberwachung wird in diesen Bereichen die Aufrechterhaltung eines ordnungsgemäßen Badebetriebes und im Falle eines Unfalles eine schnelle Hilfeleistung ermöglicht.

Der Allgemeinheit offen stehende Einrichtungen wie Freizeit- und Erlebnisbäder sind grundsätzlich öffentlich zugängliche Räume im Sinne von § 6b BDSG. Zulässig ist die Videoüberwachung dann, wenn sie zur Wahrnehmung des Hausrechts (hier: Schutz der Schrankanlagen vor Beschädigungen) oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (hier: Schutz der in den Schrankanlagen eingeschlossenen persönlichen Gegenstände der Besucher vor Diebstahl sowie Gewährleistung der Sicherheit beim Badebetrieb) erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Dies wäre insbesondere dann anzunehmen, wenn sich die Überwachung auch auf Bereiche wie die Umkleidekabinen oder auch auf Bereiche wie z. B. Liege- und Ruhezonen erstrecken würde.

Soweit auch eine Aufzeichnung der Videoaufnahmen erfolgen soll, müssen besondere Gründe für die Erforderlichkeit einer solchen Maßnahme vorliegen. Die Aufzeichnung darf auch nur in angemessenem Umfang erfolgen.

Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. In der Regel werden Badeunfälle unverzüglich gemeldet und Diebstähle so-

fort beim Öffnen des Umkleideschrankes bemerkt. Deshalb ist eine Speicherdauer der Aufnahmen von ein bis zwei Tagen für die o. g. Zwecke ausreichend.

Hinweise und Empfehlungen für die Videoüberwachung verschiedener Bereiche in Freizeitbädern:

Umkleidebereiche:

- Zweck der Videoüberwachung ist der Schutz vor Diebstählen und Inventarbeschädigungen und dient ggf. zur Beweissicherung.
- Die Überwachung der Umkleidekabinen sowie von Dusch- oder Toilettenräumen ist nicht zulässig.
- Die Überwachung ist auf die Bereiche der Umkleidespinde zu beschränken.
- Es sind offen installierte Kameras mit statischem Erfassungsbereich einzusetzen.
- Die Monitore sind so aufzustellen, dass sie nicht für Besucher einsehbar sind.
- In den Umkleidekabinen sollte ein nochmaliger Hinweis auf die Überwachung der Schrankanlagen angebracht werden.

Badebereiche:

- Zweck der Videoüberwachung ist die Gewährleistung der Sicherheit des Badebetriebes und der ordnungsgemäßen Funktion der technischen Einbauten in nicht einsehbaren oder unfallgefährdeten Bereichen; sie dient ggf. der Rekonstruktion des Unfallherganges/Beweissicherung bei Schadensersatzforderungen.
- Monitore sollten sich ausschließlich in den Diensträumen der Bademeister befinden.
- Die Videoüberwachung ist auf schwer oder nicht einsehbare Badebereiche bzw. Unfallschwerpunkte zu beschränken.
- Es sind offen installierte Kameras mit statischem Erfassungsbereich einzusetzen.
- Eine Aufzeichnung sollte nur erfolgen, wenn besondere Gefahrenbereiche überwacht werden.

Sonstige Bereiche:

- Eine Überwachung des Kassenbereiches zum Schutz vor Überfällen ist zulässig.
- Übersichtsaufnahmen des Bades (beispielsweise für eine Webcam oder einen Besuchermonitor im Foyer) sind nur zulässig, wenn die Identifikation einzelner Badbesucher ausgeschlossen ist.
- Eine Überwachung von speziellen Zugangsbereichen wie Drehkreuzen, Saunazugängen etc. ist nur zulässig, wenn diese Bereiche durch das (Kassen-)Personal nicht einsehbar sind und spezielle Zugangsvoraussetzungen bestehen.
- Bei der Überwachung der Außenfront sowie von Neben- bzw. Wirtschaftseingängen ist die Erfassung öffentlicher Gehwege/Straßen zu vermeiden.
- Eine Parkplatzüberwachung erfordert deutliche, rechtzeitig erkennbare Hinweise.

Grundsätzliche Anforderungen:

- Ein schriftliches Einsatzkonzept (Festlegung der Zwecke der Überwachung) ist zu erstellen.
- Eine Dienstanweisung für das Bedienpersonal der Videoüberwachungstechnik ist ebenso notwendig wie ein Sicherheitskonzept, das insbesondere die Zutritts-, Zugriffs- und Auswertungsbefugnisse festlegt.
- Im Eingangs- oder Kassenbereich sind deutlich erkennbare Schilder mit Hinweisen auf die Videoüberwachung anzubringen.

Bei dem eingangs geschilderten Fall war die Videoüberwachungsmaßnahme nicht datenschutzgerecht durchgeführt worden. Eine rechtzeitige, deutlich wahrnehmbare Unterrichtung der Betroffenen hätte diesen Vorfall ebenso verhindern können wie die Aufstellung des Überwachungsmonitors an einem anderen - von Besuchern nicht einsehbaren - Ort. Der Betreiber des Freizeitbades wurde von der Aufsichtsbehörde auf die datenschutzrechtlichen Mängel hingewiesen und aufgefordert, diese abzustellen.

4.2.1.2 Webcams in Einzelhandelsgeschäften

Ein Telekommunikationsfachhändler mit mehreren Filialen in Sachsen und Sachsen-Anhalt ließ seine Verkaufsräume, nachdem bereits mehrere Diebstähle begangen worden waren, mit

je einer Videokamera (Webcam) überwachen. Neben Verkaufspersonal und Kunden wurden von den Kameras teilweise auch Passanten durch die Schaufenster hindurch erfasst. Die Videoüberwachung war für die Kunden nicht erkennbar, es waren keine entsprechenden Hinweisschilder vorhanden.

Die Aufsichtsbehörde bemängelte dies als unzulässige Datenerhebung und -verarbeitung und begründete ihre Entscheidung wie folgt:

Gemäß § 6b BDSG ist die Videoüberwachung öffentlich zugänglicher Bereiche nur zulässig, wenn hierfür berechtigte Interessen geltend gemacht werden können und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Da es sich im vorliegenden Fall jedoch um Aufnahmen handelte, die über das Internet der Allgemeinheit zugänglich gemacht worden waren, sah die Aufsichtsbehörde die schutzwürdigen Interessen der Betroffenen in besonderem Maße verletzt. Denn Videoaufnahmen im Internet können weltweit unbegrenzt und unkontrolliert verarbeitet und genutzt werden. Dies wäre jedoch ein nicht zu rechtfertigender Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen.

Darüber hinaus sind die Verkaufsmitarbeiter durch die Webcam einem ständigen Überwachungsdruck ausgesetzt, dem sie sich nicht entziehen können. Nach § 28 Abs. 1 Nr. 1 BDSG ist die Datenerhebung und -verarbeitung nur zulässig, wenn sie der Zweckbestimmung des Arbeitsverhältnisses, d. h. der Wahrnehmung der Rechte bzw. der Erfüllung der Pflichten hieraus, dient. Eine Veröffentlichung der Aufnahmen im Internet ist aber hierfür weder erforderlich noch angemessen. Auch eine Einwilligung der Mitarbeiter kann diese Datenverarbeitung nicht rechtfertigen, denn diese muss auf freiwilliger Basis erfolgen. Das heißt, der Betroffene darf sich nicht in einer Situation befinden, die ihn faktisch dazu zwingt, sich mit der Verarbeitung seiner Daten einverstanden erklären zu müssen. Dies ist aber bei einem Abhängigkeitsverhältnis, wie es das Arbeitsverhältnis ist, regelmäßig anzunehmen.

Die Überwachung der Verkaufsräume kann zum Zweck der Verhinderung bzw. Aufklärung von Diebstählen auf zulässige Weise erfolgen, indem der Firmeninhaber dafür Sorge trägt, dass die Aufnahmen der Videokameras nicht veröffentlicht werden und die Einstellung der Kamera so vorgenommen wird, dass das Verkaufspersonal nicht ständig erfasst wird. Außerdem ist die Videoüberwachung durch entsprechende Hinweisschilder für die Kunden erkennbar zu machen, um die Transparenz der Datenverarbeitung zu gewährleisten.

4.2.1.3 Videoüberwachung von Hauseingang, Gehweg und Straße

Häufig hatten die Aufsichtsbehörden die Zulässigkeit der Videoüberwachung von Hauseingängen, Gehwegen und Straßen durch Hauseigentümer zu beurteilen. Der folgende Fall steht somit stellvertretend für eine ganze Reihe von Fällen.

Der Eigentümer eines Mehrfamilien- oder Wohn- und Geschäftshauses installiert an der Hauswand eine Videokamera zur Überwachung des Hauseinganges bzw. der Außenfassade. Die Kamera ist schräg nach unten auf den Eingang bzw. die Fassade ausgerichtet und erfasst somit auch Teile des öffentlichen Gehweges bzw. der Straße. Mieter bzw. Passanten, die die Kamera bemerken, wenden sich an die Aufsichtsbehörde.

Die Überprüfung der Eingaben vor Ort ergibt meist, dass die Videoüberwachung in unzulässiger Weise erfolgt. So werden oft nicht nur Hauseingang und/oder die Fassade, sondern auch ein Teil des Gehweges und/oder der Straße, der sich direkt vor dem Hauseingang befindet, erfasst. Nach § 6b Abs. 1 Nr. 3 BDSG ist eine Videoüberwachung jedoch nur zulässig, wenn sie zur Wahrnehmung berechtigter Interessen oder zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen.

Meist werden Überwachungskameras installiert, um Straftaten wie Beschädigungen der Hauswände (bspw. durch Graffitis) oder Einbrüchen vorzubeugen. Doch das Recht des Hauseigentümers, Schutzmaßnahmen für sein Eigentum zu treffen, darf nicht in unverhältnismäßiger Weise das Recht auf informationelle Selbstbestimmung unbeteiligter Dritter beeinträchtigen. Im oben genannten Beispiel können Personen das Haus nicht betreten oder verlassen, ohne dass sie dabei gefilmt werden. Die Betroffenen, insbesondere Mieter und Besucher, können der Überwachung somit nicht entgehen und auch nicht überprüfen, wie lange die Aufzeichnungen tatsächlich gespeichert und für welche Zwecke sie weiterverwendet werden. Darüber hinaus besteht die Gefahr des Missbrauchs der Daten, denn die ständige Beobachtung ermöglicht z. B. die Erstellung einzelner Bewegungsprofile. Dies ist insbesondere für die Mieter nicht zumutbar.

Der Bundesgerichtshof stellte bereits 1995 fest, dass auf öffentlichen Wegen regelmäßig das Recht des Bürgers, sich ohne Überwachung durch private Stellen frei bewegen zu können, Vorrang hat. Dem Eigentümer ist es zuzumuten, dass er sein Eigentum auf andere Weise schützt, etwa durch nächtliche Beleuchtung des Hausflurs oder die Installation von Glasbruch- bzw. Einbruchsmeldern. Auch eine Wechselsprechanlage oder Klingelkamera wären geeignete Alternativen.

4.2.1.4 Videoüberwachung im Massage-Studio

Ein Petent berichtete der Aufsichtsbehörde von einem Massagestudio, in dem ihm ein Wäscheschrank aufgefallen sei, worin sich ein Videorekorder und diverse mit Tagesdaten beschriftete Videokassetten befunden hätten. An der Decke des Flures bemerkte er eine Domkamera[1].

Die vor Ort durchgeführte Kontrolle bestätigte die Angaben des Petenten. Als Gründe für die Kamerainstallation wurde seitens des Massagestudios angegeben, die Kundenfluktuation so besser nachvollziehen und die eigenen Mitarbeiter kontrollieren zu können. Die Inhaberin des Studios wollte auf diese Weise überprüfen, ob ihre Mitarbeiter die Tageseinnahmen korrekt abrechneten.

Nach Aussage der Inhaberin habe nur sie Zugriff auf das Videomaterial, und die Bänder seien in einem unzugänglichen Schrank eingeschlossen. Die durch die Aufsichtsbehörde durchgeführte Kontrolle ergab jedoch, dass Videorekorder und auch die Videobänder sich in einem für das Personal frei zugänglichen Wäscheschrank befanden.

Beim Flur bzw. Empfangsbereich des Massagestudios handelte es sich um einen nach § 6b BDSG öffentlich zugänglichen Raum. § 6b Abs. 1 Nr. 3 BDSG regelt die Zulässigkeit der Videoüberwachung, die nur dann gegeben ist, wenn sie zur Wahrnehmung berechtigter Interessen erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Die Aufsichtsbehörde stellte die Unzulässigkeit der Videoüberwachungsmaßnahmen fest. Es überwogen die schutzwürdigen Interessen der Kunden des Massagesalons, nämlich die vertrauliche und diskrete Behandlung ihres Besuchs. Aus der Art der in dem Massagesalon angebotenen Dienstleistung ergibt sich, dass ein Missbrauch der Videoaufnahmen unangenehme Folgen für die Betroffenen haben könnte. Die Gefahr des Missbrauchs war deshalb hoch, weil die Videobänder in einem für das Personal frei zugänglichen Wäscheschrank aufbewahrt wurden.

Im Übrigen rechtfertigt ein pauschaler Betrugsverdacht der Inhaberin gegen ihre Mitarbeiter nicht deren permanente Videoüberwachung bei der Arbeit. Nur wenn konkrete Anhaltspunkte für ein treuewidriges Verhalten gegeben sind, ist eine Videoüberwachungsmaßnahme in engen Grenzen erlaubt.

[1] Kamera für den Einsatz im Innenbereich mit Super-Weitwinkel-Objektiv (90°), das die komplette Überwachung eines Raumes mit einer Kamera ermöglicht.

Die Maßnahme war überdies von vorn herein nicht zur Erreichung der o. g. Zwecke geeignet und somit auch nicht erforderlich. Denn die Höhe der tatsächlichen Einnahmen sowie die durch den Kunden in Anspruch genommene Dienstleistung konnte durch die stichprobenartige Auswertung der Videobänder nicht ermittelt werden. Die Bänder hätten wegen der unverschlossenen Aufbewahrung außerdem ohne Weiteres unbemerkt durch das Personal ausgetauscht werden können. Somit war eine Kontrolle der Abrechnung durch die Mitarbeiter auf diese Weise gar nicht möglich.

Die Videoüberwachung des Massagestudios wurde daraufhin durch die Inhaberin eingestellt.

4.2.1.5 Die Kamera im Bratwurststand

Die Aufsichtsbehörde wurde durch einen telefonischen Hinweis auf die Videoüberwachung in einem mobilen Bratwurststand aufmerksam. Der Anrufer gab an, die Kamera sei so angebracht, dass sie auf die Kundschaft ausgerichtet sei, und vermutete daher deren Überwachung.

Der Unternehmer teilte der Aufsichtsbehörde auf deren Nachfrage hin mit, dass er die Videokamera nicht zum Zweck der Beobachtung der Kundschaft, sondern zur Kontrolle des Grillgerätes angebracht habe. Vor der Installation der Kamera hätte ein Mitarbeiter seine mitgebrachte Ware auf eigene Rechnung verkauft. Erst nach diesem Vorfall installierte der Inhaber des Standes die Kamera, die seitdem ständig das Grillgerät und damit indirekt alle an dem Stand arbeitenden Beschäftigten überwacht.

Bei dem mobilen Grillstand handelt es sich nicht um einen der Öffentlichkeit zugänglichen Raum im Sinne des § 6b BDSG, sondern um einen eng begrenzten Geschäftsraum, zu dem nur Mitarbeiter Zutritt haben. Da somit § 6b BDSG als Ermächtigungsgrundlage nicht anwendbar ist, war die Zulässigkeit der Videoüberwachung anhand der Regelungen in § 28 BDSG zu prüfen. Danach ist das Erheben und Speichern personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Im vorliegenden Fall sind die Intensität des Eingriffs und die ihn rechtfertigenden Gründe gegeneinander abzuwägen. Weiterhin müssen bei der Ermittlung der Eingriffsintensität das Recht auf Eigentum (Art. 14 GG) und das allgemeine Persönlichkeitsrecht (Art. 2 GG) berücksichtigt werden.

Mit der der Videokamera im Bratwurststand wurden neben dem beschuldigten Mitarbeiter auch alle anderen Mitarbeiter überwacht und kontrolliert. Für sie war es unmöglich, dieser Kontrolle zu entgehen. Gründe für eine Rechtfertigung lagen nicht vor. Der Betreiber hätte hingegen durch regelmäßige persönliche Kontrollen und anhand vergleichender Auswertungen der Verkaufszahlen bzw. der diversen Tagesumsätze den Betrug seines Mitarbeiters aufdecken können.

Die Persönlichkeitsrechte der Betroffenen überwiegen hier gegenüber dem Eigentumsrecht des Unternehmers; die Videoüberwachung ist damit unzulässig. In einem ähnlichen Fall hat das Bundesarbeitsgericht die Videoüberwachung am Arbeitsplatz ebenso für unzulässig erklärt (Beschluss vom 29. Juni 2004, 1 ABR 21/03).

Der Betreiber hat nach entsprechender Aufforderung umgehend die Kamera vom Bratwurststand entfernt.

4.2.2 Datenverarbeitung und -nutzung für Werbezwecke

4.2.2.1 Werbeprospekt statt Löschbestätigung

Eine Bürgerin bestellte bei einer Versandapotheke Medikamente. Da sie anschließend keine weiteren Bestellungen vornehmen wollte, bat sie um Löschung ihrer bei dem Unternehmen gespeicherten Daten und um eine schriftliche Bestätigung hierfür. Dazu fügte die Frau ihrem Schreiben einen frankierten Rückumschlag bei. Der Bitte der Kundin um Löschung ihrer Daten kam die Versandapotheke allerdings nicht nach; stattdessen erreichte die Kundin in deren eigenem Briefumschlag ein weiteres Werbeprospekt. Auf die von ihr daraufhin unternommenen mehrmaligen telefonischen Versuche, die Löschung ihrer Daten zu erreichen, erfolgte keine Reaktion seitens des Unternehmens.

Die Aufsichtsbehörde bat daraufhin die Geschäftsleitung der Versandapotheke zu dem Fall um Stellungnahme.

Das Unternehmen führte aus, dass es in Bezug auf das Anliegen der Betroffenen unternehmensintern zu einer unternehmensinternen Verwechslung gekommen sei. Deshalb habe sie anstatt der erbetenen Bestätigung über die Löschung ihrer Daten ein Werbeprospekt erhalten. Das Unternehmen hat sich für den Fehler entschuldigt und die Löschung der Daten der Betroffenen aus der Datenbank bestätigt.

4.2.2.2 Versand von E-Mail-Newslettern

Ein Petent erhielt wiederholt unerwünschte Werbe-E-Mails von einem ihm unbekannten Internet Content Provider. Daraufhin bat er die Aufsichtsbehörde um Prüfung dieses Sachverhaltes. Der Petent habe bereits mehrfach erfolglos versucht, seine E-Mail-Adresse bei diesem Provider löschen zu lassen. Die Aufsichtsbehörde bat den Betreiber der Website um Stellungnahme hierzu. Der verantwortliche Anbieter teilte mit, er habe nie unaufgefordert - das heißt ohne vorherige Anmeldung des Nutzers - Newsletter versandt. Das Unternehmen konnte stattdessen eine Anmeldung unter der E-Mail-Adresse des betroffenen Petenten mit Datum und Uhrzeit nachweisen. Das vom Anbieter verwandte einfache Anmeldeverfahren konnte einen Missbrauch fremder E-Mail-Adressen für die Anmeldung nicht ausschließen.

Um derartigen Problemen vorzubeugen, sollten Anbieter von Newslettern für die Anmeldung vorzugsweise auf das so genannte „Double-Opt-In“ zurückgreifen. Hierbei wird eine Anmeldung erst dann wirksam, wenn sie vom Betroffenen ein zweites Mal bestätigt wird (bspw. durch Anklicken eines speziellen Links in der E-Mail des Anbieters).

Weiterhin teilte der Anbieter mit, dass man das Newsletter-Abonnement jederzeit bedingungslos kündigen könne. Jedoch sei von dem Betroffenen bislang keine entsprechende Anfrage eingegangen.

Der Provider kam schließlich dem Wunsch des Betroffenen nach, dessen E-Mail-Adresse aus der Liste der Newsletter-Empfänger zu löschen.

4.2.2.3 Haushaltsumfrage

Eine an Osteoporose leidende Rentnerin erhielt ein Aktionspaket zur Thematik „Bedeutung einer calciumreichen Ernährung in der Osteoporose-Therapie“ und fragte sich, woher der Absender Kenntnis von ihrer Krankheit hatte. Sie vermutete, dass entweder ihre Krankenkasse, Apotheke oder ihre Physiotherapie Daten an die für diese Aktion verantwortliche Stelle weitergegeben haben könnten.

Es stellte sich jedoch heraus, dass die Betroffene durch die Teilnahme an einer Haushaltsumfrage selbst dafür gesorgt hatte, dass ihre Daten durch Marketingunternehmen für Werbezwecke genutzt werden durften. Die Auswahl der Konsumenten für die Informationskampagne war tatsächlich auf Basis der Daten einer solchen Konsumentenbefragung erfolgt, wobei allerdings ausschließlich Geschlecht und Altersgruppe als Auswahlkriterium herangezogen worden waren. Eine rechtswidrige Datenverarbeitung lag dieser Aktion nicht zugrunde.

4.2.2.4 Werbeschreiben trotz Eintrags in der Robinsonliste

Der Deutsche Direktmarketing Verband e.V. (DDV) bietet Verbrauchern zum Schutz vor adressierter Werbung seit vielen Jahren die Aufnahme in die sog. Robinsonliste an. In diese Liste kann sich jeder eintragen lassen, der keine an ihn adressierten Werbebriefe von Unternehmen erhalten möchte. Die Beachtung der Robinsonliste geschieht freiwillig; ungewollte Werbeschreiben lassen sich dadurch zwar nicht vollständig vermeiden, jedoch zumindest maßgeblich reduzieren.

Eine Petentin ließ sich in die Liste aufnehmen, stellte einige Zeit später jedoch fest, dass die Zusendung unerwünschter Werbeschreiben trotz Eintragung in die Robinsonliste zunahm, so dass sie sich veranlasst sah, sich an die Aufsichtsbehörde zu wenden.

Der Petentin war entgangen, dass jeder Eintrag in die Robinsonliste nur fünf Jahre Gültigkeit besitzt und danach im Bedarfsfall wieder erneuert werden muss. So wird verhindert, dass Namens- und Adressenangaben veralten. Der Petentin wurde empfohlen, ihre Angaben neu in die Liste aufnehmen zu lassen.

4.2.2.5 Auskunft über die Herkunft der Daten

In zwei Fällen wurde die Datenschutzaufsichtsbehörde durch Eingaben auf Unternehmen aufmerksam gemacht, die mit Werbeansprachen an die Betroffenen herantraten und keine Auskunft darüber gaben, woher sie die Kontaktdaten bezogen hatten.

In einem Fall wandte sich eine Versicherung an einen Petenten - erst telefonisch in seiner Dienststelle, später per E-Mail -, um ihm Angebote zu unterbreiten. Der Betroffene erhielt auf seine Frage nach der Herkunft seiner Daten vom Unternehmen keine klare Antwort. Auf Bitten der Aufsichtsbehörde teilte die Geschäftsleitung mit, dass das Versicherungsunternehmen öfter Kunden-Empfehlungen zu möglichen Interessenten erhalte. Der Name des Empfehlenden wird von der Versicherung nur notiert, wenn dieser es wünscht. Im Fall des betroffenen Bürgers war dies jedoch nicht geschehen.

Im zweiten Fall erhielt ein Petent einen Anruf, bei dem ihm ein Gewinn aus einem Gewinnspiel und ein anschließender Hausbesuch des werbenden Unternehmens angekündigt wurden. Auf seine Nachfrage hin, woher das Unternehmen die Kontaktdaten bezogen habe, teilte ihm der Geschäftsführer des werbenden Unternehmens mit, man würde nur Interessenten bzw. Kunden ansprechen, die an Messeständen oder in einer Umfragekarte ihr Interesse an den angebotenen Produkten bekundet und daher dem Unternehmen ihre Adresse bekannt gegeben

hätten. Der Petent legte jedoch dar, dass weder er noch seine Familienangehörigen seine Kontaktdaten dem Unternehmen gegeben hatten. Trotz mehrmaliger Aufforderung der Aufsichtsbehörde konnte das betreffende Unternehmen die Herkunft der Telefonnummer und der Adresse des Betroffenen nicht nachweisen.

§ 28 Abs. 4 Satz 2 BDSG bestimmt, dass das werbende Unternehmen sicherzustellen hat, dass der Betroffene Kenntnis über die Herkunft seiner Daten erhält. Dies gilt insbesondere dann, wenn diese Daten bei einer ihm nicht bekannten Stelle gespeichert sind. Diese Regelung soll gewährleisten, dass von Werbeansprachen betroffene Bürger auf einfache Weise den Übermittler ihrer personenbezogenen Daten in Erfahrung bringen können.

In den beiden dargestellten Fällen wurde gegen diese Pflicht verstoßen. Die Aufsichtsbehörde verhängte gegen beide Unternehmen Bußgelder (vgl. Pkt. 9). Der Tatbestand der Ordnungswidrigkeit ist vorliegend insbesondere auch dann erfüllt, wenn die entsprechenden Vorkehrungen zur Beantwortung solcher Anfragen in einem Unternehmen fehlen oder unzureichend sind.

4.2.3 Arbeitnehmerdatenschutz

4.2.3.1 Erhebung von Bewerberdaten durch einen Personaldienstleister

Ein Arbeit Suchender bewarb sich bei einem Personaldienstleister um eine Arbeitsstelle. Der vom Bewerber auszufüllende Personalbogen enthielt Fragen, die ihm in datenschutzrechtlicher Hinsicht bedenklich erschienen. Er erkundigte sich daher bei der Aufsichtsbehörde nach der Rechtslage:

Im Rahmen der Anbahnung eines Arbeitsverhältnisses ist der Arbeitgeber bemüht, möglichst umfassende Informationen über den Bewerber zu erhalten, auf deren Grundlage er seine Personalentscheidung treffen kann. Der Arbeitgeber ist jedoch bei der Auswahl seiner Fragen nicht völlig frei, sondern muss dabei das Persönlichkeitsrecht des Bewerbers besonders berücksichtigen. Dies ist Teil der vorvertraglichen Pflichten des Arbeitgebers. Zum Fragerecht des Arbeitgebers gibt es bereits eine umfangreiche arbeitsgerichtliche Rechtsprechung (Bundesarbeitsgericht). Danach sind nur Fragen zulässig, an deren wahrheitsgemäßer Beantwortung der Arbeitgeber ein berechtigtes und schutzwürdiges Interesse hat, aufgrund dessen die Belange des Bewerbers zurücktreten müssen. Ein solches Interesse ist regelmäßig nur anzunehmen, wenn die Beantwortung der Frage für den angestrebten Arbeitsplatz und die zu verrichtende Tätigkeit selbst von Bedeutung ist. Betrifft die Frage dagegen die Privat- oder In-

timsphäre des Bewerbers, ohne dass ein Zusammenhang mit der zu übernehmenden Aufgabe besteht, ist die gestellte Frage unzulässig.

Die Zulässigkeit einzelner Fragen wird von der Aufsichtsbehörde wie folgt bewertet:

- *Gewerkschaftszugehörigkeit*

Die Frage nach der Gewerkschaftszugehörigkeit ist aufgrund der verfassungsrechtlich garantierten Koalitionsfreiheit (Art. 9 Abs. 3 GG) unzulässig.

- *Vorstrafen*

Die Frage nach Vorstrafen ist nur zulässig, wenn und soweit die zu besetzende Arbeitsstelle oder die zu leistende Arbeit dies erfordert. So darf etwa ein Kassierer nach vermögensrechtlichen Vorstrafen oder ein Kraftfahrer nach Verkehrsdelikten befragt werden. Vorstrafen dürfen verschwiegen werden, wenn sie gemäß § 51 Bundeszentralregistergesetz (BRZG) nicht (mehr) in ein polizeiliches Führungszeugnis aufzunehmen sind.

- *Laufende Gerichtsverfahren*

Es darf grundsätzlich nach laufenden Gerichtsverfahren gefragt werden, die im Zusammenhang mit der angestrebten Tätigkeit stehen. Relevant kann zudem sein, ob die Verfügbarkeit des Bewerbers durch das Verfahren eingeschränkt ist, wenn mit umfangreichen Ermittlungen oder gar mit Untersuchungshaft oder der Verurteilung zu einer Freiheitsstrafe zu rechnen ist. Hier ist das Einstellungs- und Beschäftigungsrisiko so groß, dass dem Arbeitgeber ein Fragerecht zugebilligt werden muss.

- *Krankheitstage in den letzten zwölf Monaten*

Diese Frage ist unzulässig. Eine Aussage zu der Anzahl der Krankheitstage in den letzten zwölf Monaten gibt keine verlässlichen Hinweise auf eine etwaige zukünftige Arbeitsunfähigkeit des Arbeitnehmers.

- *Letzter Vorgesetzter und dessen Telefonnummer*

Nach der Rechtsprechung des Bundesarbeitsgerichtes (BAG) darf ein neuer Arbeitgeber beim bisherigen Arbeitgeber Auskünfte über den Bewerber - auch ohne dessen Zustimmung - einholen. Das Auskunftserteilungsrecht findet jedoch seine Grenze im Fragerecht des neuen Arbeitgebers beim Einstellungsgespräch. Die Frage nach dem letzten Vorgesetzten und dessen Telefonnummer steht im Zusammenhang mit dem Arbeitsverhältnis und ist daher zulässig.

- *Art und Weise der Beendigung der Arbeitsverhältnisse*

Für den neuen Arbeitgeber dürfte von Bedeutung sein, ob die früheren Arbeitsverhältnisse durch eine fristlose Kündigung aufgrund eines Verschuldens des Bewerbers beendet worden sind. An dieser Auskunft hat der neue Arbeitgeber ein berechtigtes Interesse.

4.2.3.2 Übermittlung von Personaldaten bei Einschaltung eines Privatdetektivs

Zwei Mitarbeiter eines Unternehmens standen im Verdacht, ihren Arbeitspflichten nicht ausreichend nachgekommen zu sein. Die leitenden Angestellten beauftragten einen Privatdetektiv mit deren außerdienstlicher Überwachung. Dem Detektiv wurden die kompletten Personalbögen, in einem Fall auch der Lebenslauf, übermittelt.

Die Beurteilung der Zulässigkeit der Weitergabe persönlicher Daten richtet sich nach § 28 Abs. 1 Nr. 2 BDSG. Danach ist zu prüfen, ob die Übermittlung der umfangreichen Datenbestände (Personalbogen + Lebenslauf) zur Wahrung eines berechtigten Interesses erforderlich war.

Kann der Arbeitgeber einem Arbeitnehmer vertragswidriges Verhalten nachweisen, genügen für eine Überwachung durch einen Privatdetektiv in der Regel die Weitergabe der Anschrift und eines Fotos. Die Übermittlung weiterer Angaben aus dem Personalbogen, so etwa von Angaben zur Familie des betroffenen Mitarbeiters, dessen Aus- und Fortbildung, dem beruflichen Werdegang, sonstigen Fähigkeiten und Kenntnissen oder gar des Lebenslaufes ist unzulässig. In diesem Fall überwiegen die schutzwürdigen Interessen des Betroffenen. Diesem ist es – auch bei begründetem Verdacht eines schwerwiegend vertragswidrigen Verhaltens – nicht zuzumuten, dass seine persönlichen Lebensverhältnisse einem Privatdetektiv im Detail offengelegt werden.

Gegen die verantwortlichen leitenden Angestellten des Unternehmens ist wegen unbefugter Datenübermittlung ein Ordnungswidrigkeitenverfahren eingeleitet worden, welches zum Ende des Berichtszeitraumes noch nicht abgeschlossen war.

4.2.4 Einzelhandel

4.2.4.1 Personalausweiskopien bei Barzahlung mit 500-€-Scheinen

Die Aufsichtsbehörde wurde auf die Vorgehensweise eines großen Elektronikfachmarktes aufmerksam gemacht, in dem man von Kunden, die mit 500-€-Scheinen bezahlen wollten,

den Personalausweis verlangte und diesen mit den Geldscheinen zusammen kopierte. Auf Nachfrage wurde dies vom Unternehmen mit dem Schutz vor Zahlungsausfällen durch Falschgeld begründet. Anhand der Ausweiskopien könne gegebenenfalls nachträglich eine personelle Zuordnung der von der Bank nicht eingelösten Bargeldbeträge vorgenommen werden.

Die Überprüfung der einzelnen Sicherheitsmerkmale von Euro-Banknoten ist Aufgabe jedes/r Kassierers/Kassiererin. Das Unternehmen hat dafür Sorge zu tragen, das Personal im Hinblick auf die Erfüllung seiner Aufgaben ausreichend zu schulen. Auch der Einsatz technischer Hilfsmittel ist möglich, wenn Zweifel an der Echtheit von Geldscheinen bestehen. Zum Schutz vor der Bezahlung mit falschen Banknoten ist es deshalb nicht erforderlich, Ausweiskopien anzufertigen. Im Übrigen war den Kassierern die Überprüfung der Echtheit von 50- und 100-Euroscheinen auch ohne Ausweiskopie möglich.

Die vom Fachmarkt praktizierte Verfahrensweise ist auch nicht angemessen, denn es überwiegen die schutzwürdigen Interessen der Betroffenen an der Nichtverarbeitung ihrer Personalausweisdaten. Es ist nicht gerechtfertigt, Kunden, die mit 500-Euro-Scheinen bezahlen, durch das Kopieren von deren Ausweis unter pauschalen Betrugsverdacht zu stellen.

Die Verbreitung von falschen 500-Euro-Scheinen ist außerdem äußerst gering. Sie betrug in Deutschland im 2. Halbjahr 2004 gerade 0,9 % aller Falschgeldfälle. Demgegenüber lag der Anteil von falschen 50-Euro-Scheinen bei 47,8 % und der von 100-Euro-Scheinen bei 34,9 %. Angesichts des raren Vorkommens falscher 500-Euro-Scheine und der Tatsache, dass diese nur äußerst selten zur Zahlung verwendet werden, war das Schadensrisiko durch andere falsche Banknoten um ein Vielfaches höher.

Die mit der Anfertigung der Ausweiskopien verbundene Datenerhebung und -speicherung verstößt gegen § 28 BDSG. Die Anfertigung von Personalausweiskopien war daher unzulässig.

Die Geschäftsführung des Elektronikfachmarktes ist der Aufforderung der Aufsichtsbehörde, diese Verfahrensweise umgehend einzustellen, nachgekommen.

4.2.5 Sparkassen/Banken

4.2.5.1 Bekanntgabe vertraulicher Daten im Sichtfenster eines Briefumschlages

Eine Kundin erhielt von ihrer Sparkasse einen Brief, bei dem im Sichtfenster des Briefumschlages neben dem Namen und der Anschrift die Worte „Kreditnehmer (persönliche Angaben der Verpflichteten)“ erkennbar waren.

Die Betroffene beschwerte sich zunächst bei ihrer Sparkasse über die Verletzung ihrer Persönlichkeitsrechte. Die Sparkasse begründete die Bekanntgabe der in Rede stehenden Daten im Sichtfenster des Briefumschlages mit fehlerhafter Faltung des Anschreibens. Einen datenschutzrechtlichen Verstoß bzw. eine Verletzung der Persönlichkeitsrechte der Betroffenen sah die Bank dabei jedoch nicht. Daraufhin wandte sich die Betroffene an die Aufsichtsbehörde, die nach Prüfung der Angelegenheit Folgendes feststellte:

Das Schreiben ging der Betroffenen im Rahmen einer Kampagne zur Kundenbetreuung zu, mit der die Sparkasse ihre Kunden in unregelmäßigen Abständen auf Produkte hinweist, die bisher nicht von ihnen genutzt werden. Im vorliegenden Fall handelte es sich um einen Kreditantrag. In diesem von der Sparkasse vorbereiteten Formular waren Name und Anschrift der Kundin bereits eingetragen. Durch die falsche Faltung des Formulars war die Zeile „Kreditnehmer (persönliche Angaben der Verpflichteten)“ im Sichtfenster des Briefumschlages sichtbar geworden.

Die Sparkasse war der Ansicht, bei der Angabe „Kreditnehmer“ handele es sich nicht um ein personenbezogenes Datum, da das Produkt vom Kunden nicht genutzt wird. Nach § 3 Abs. 1 BDSG sind jedoch personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Es ist somit bereits ausreichend, wenn bei Außenstehenden der Eindruck erweckt wird, der Empfänger des Briefes (die Kundin der Sparkasse) sei Kreditnehmer. Derartige Kennzeichnungen sind geeignet, den Betroffenen in seinem Persönlichkeitsrecht zu beeinträchtigen und damit unzulässig.

Die Aufsichtsbehörde forderte die Sparkasse auf sicherzustellen, dass bei Anschreiben im Rahmen der Kundenbetreuung zukünftig nur noch die für die Zustellung des Briefes erforderlichen Angaben (Anrede, ggf. Titel, Name, Vorname, Anschrift) im Sichtfenster des Briefumschlages erscheinen.

4.2.5.2 Anzeige personenbezogener Daten am Kontoauszugdrucker

Ein Kunde der Sparkasse wollte mit seiner Kundenkarte Kontoauszüge am Kontoauszugdrucker ausfertigen lassen und bemerkte nach dem Einführen der Karte, dass auf dem Flachbildschirm des Automaten die Worte „Guten Tag, sehr geehrter Herr *Max Mustermann*[2]! Sind Sie am Kauf einer Immobilie interessiert?“ erschienen. Auf diese Weise wurde für andere im Raum befindliche Personen sein vollständiger Name erkennbar. Der Betroffene vermutete einen Verstoß gegen den Datenschutz und wandte sich an die Aufsichtsbehörde. Die Prüfung des Sachverhaltes ergab Folgendes:

Der betreffende Kontoauszugsdrucker ist neben einem Flachbildschirm mit sog. „Softkeys“ (Tasten, die abhängig von der jeweiligen Anwendung mit verschiedenen Funktionen belegt werden können) ausgestattet. Das Gerät kann so auch zur personalisierten und internaktiven Kundenansprache eingesetzt werden. Nach Erscheinen der Begrüßung und eines Werbetextes kann der Kunde über die Softkeys zwischen den Antworten „Ja“, „Nein“ und „Abbruch“ wählen. Mit der Betätigung eines Softkeys erlischt die Anzeige auf dem Bildschirm sofort, ansonsten nach ca. zehn Sekunden.

Weil die Namensangaben des Kunden für andere im Raum befindliche Personen deutlich erkennbar waren, war diese personenbezogene Ansprache datenschutzrechtlich unzulässig.

Die Sparkasse reagierte auf den Hinweis der Aufsichtsbehörde und ersetzte die personenbezogene Anzeige auf dem Bildschirm des Kontoauszugsdruckers durch eine anonyme.

4.2.5.3 Anonymität bei Kundenumfragen

Ein Kreditinstitut stellte seinen Kunden einen Fragebogen zur Ermittlung der Kundenzufriedenheit zu und teilte darin mit, dass alle Teilnehmer der Befragung nach dem Zufallsprinzip aus dem Kundenbestand ausgewählt worden seien. Eine anonyme Auswertung des Fragebogens, die keine Rückschlüsse auf den Befragten zulässt, wurde zugesichert.

Einem der Empfänger fiel auf, dass Anschreiben und Fragebogen eine dreistellige Nummer aufwiesen. Es stellte sich heraus, dass auch die Mutter des Kunden ein analoges Schreiben, jedoch mit einer anderen Nummer, erhalten hatte. Seine daraus resultierenden Zweifel an der tatsächlichen Anonymität dieser Kundenumfrage teilte er der Aufsichtbehörde mit. Die Bedenken des Petenten schienen der Aufsichtsbehörde durchaus berechtigt. Individuelle Kenn-

[2] Name geändert

zeichnungen von Kundenschreiben sind aus dem Marketingbereich bekannt und haben eine wichtige Funktion. Durch diese Kennzeichnung kann die werbetreibende Stelle bei einem Werbewiderspruch oder Auskunftsersuchen der Kunden feststellen, aus welchem Datenbestand die Daten des Adressaten stammen. Da es sich in diesem Fall um eine als „anonym“ deklarierte Kundenumfrage handelte, war die Zulässigkeit der Nummernkennzeichnung zu hinterfragen.

Das Kreditinstitut versicherte der Aufsichtsbehörde, dass die Anonymität der Befragten - trotz der unterschiedlichen Kennzeichnungen - gewahrt gewesen sei. Es handelte sich hierbei nach Angaben des Kreditinstitutes um die Codierung der Filiale. Die Nummerierung im Adressfeld der Anschreiben sollte die Arbeit der zentralen Poststelle des Kreditinstituts erleichtern, damit ggf. Rücksendungen mit Unzustellbarkeitsvermerk problemlos einer Umfrageaktion zugeordnet und der Marktforschungsabteilung ungeöffnet zugeleitet werden könnten.

Ein Datenschutzverstoß konnte nicht festgestellt werden; allerdings hätte eine kurze Erläuterung zum Grund der Kennzeichnung im Anschreiben an die Kunden Missverständnissen vorbeugen können.

4.2.6 Betrieblicher Datenschutzbeauftragter

4.2.6.1 Unterbringung des Datenschutzbeauftragten im Großraumbüro

Ein Unternehmen plante, seinen Datenschutzbeauftragten zusammen mit anderen Mitarbeitern in einem Büroraum unterzubringen. Der Datenschutzbeauftragte ersuchte daraufhin die Aufsichtsbehörde, da er hierin einen Verstoß seines Arbeitgebers gegen die Unterstützungspflicht vermutete und seine Stellung als Vertrauensperson für Mitarbeiter, Geschäftsleitung, Kunden und Geschäftspartner gefährdet sah.

Nach Einschätzung der Aufsichtsbehörde ist die Absicht des Arbeitgebers, den innerbetrieblichen Datenschutzbeauftragten zusammen mit anderen Mitarbeitern in einem Büroraum unterzubringen, mit den datenschutzrechtlichen Bestimmungen (Unterstützungs- und Verschwiegenheitspflicht) nicht vereinbar.

Gemäß § 4f Abs. 5 Satz 1 BDSG ist die verantwortliche Stelle verpflichtet, den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen. Dazu gehört es auch, ihm u. a. einen geeigneten separaten Raum, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. Es muss dem Datenschutzbeauftragten insbesondere möglich sein, vertrauliche Gesprä-

che führen zu können. Die Verschwiegenheitspflicht nach § 4f Abs. 4 BDSG gilt gegenüber allen Mitarbeitern des Unternehmens.

Im vorliegenden Fall musste auch berücksichtigt werden, dass der Datenschutzbeauftragte gleichzeitig auch als externer Datenschutzbeauftragter der Tochterunternehmen seines Arbeitgebers bestellt war und somit die Gefahr der unbefugten Datenübermittlung bestanden hätte.

Die Aufsichtsbehörde bemängelte deshalb die gemeinsame Unterbringung des Datenschutzbeauftragten mit anderen Mitarbeitern. Das Unternehmen hat daraufhin von diesem Plan Abstand genommen.

4.2.7 Freiberufler

4.2.7.1 Datenübermittlung durch einen Steuerberater

Ein Steuerberater sandte einigen seiner Mandanten eine Anlage zum Kammerbrief der Steuerberaterkammer des Freistaates Sachsen mit der Überschrift „Bekämpfung des unlauteren Wettbewerbs - Unterlassungserklärungen im II. und III. Quartal …“ zu. In dieser Anlage waren Buchhalter aufgeführt, die Unterlassungserklärungen abgegeben hatten. Dadurch erhielten die Adressaten nicht nur Kenntnis vom Text der jeweiligen Unterlassungsverpflichtungserklärung, es wurden ihnen auch Namen, Vornamen und genaue Anschriften der Betroffenen mitgeteilt. Ein Betroffener informierte die Aufsichtsbehörde über diesen Sachverhalt.

Die Prüfung ergab, dass die durch den Steuerberater vorgenommene Übermittlung personenbezogener Daten ohne Rechtsgrundlage erfolgte und somit unzulässig war. Die in dem Kammerbrief enthaltenen Namen und Adressen der Personen, die eine Unterlassungserklärung abgegeben hatten, hätten durch den Steuerberater unkenntlich gemacht (geschwärzt) werden müssen. Nach einem entsprechenden Hinweis durch die Aufsichtsbehörde wurde die Versendung der Briefe am darauffolgenden Tag eingestellt.

Der Steuerberater räumte die Datenschutzverletzung ein und sicherte zu, dass sich derartige Vorkommnisse künftig nicht wiederholen werden. Die Aufsichtsbehörde beließ es bei einer Beanstandung und einem Hinweis auf geeignete personelle und organisatorische Maßnahmen zur Einhaltung des Datenschutzes.

4.2.7.2 Verarbeitung und Nutzung von Kundendaten nach Beendigung eines Handelsvertretervertrages

Ein Kunde einer Vermögensberatungsfirma erhielt einen Anruf einer Consulting-Firma, die angeblich im Auftrag seiner Hausbank Depotprüfungen durchführte. In einem ersten Gespräch zeigte sich, dass die Consulting-Firma detaillierte Kenntnisse über das Depot des Kunden hatte. Eine Rückfrage bei seiner Hausbank ergab jedoch, dass diese weder Kundendaten an Beratungsunternehmen übermittelt noch diese mit Depotprüfungen beauftragt hatte.

Die Aufsichtsbehörde stellte fest, dass es sich beim Inhaber der Consulting-Firma um einen ehemaligen Handelsvertreter des Vermögensberatungsunternehmens handelte. Bereits vor Beendigung seines Handelsvertreter-Vertrages gründete er ein Consulting-Unternehmen und nutzte dabei ihm im Rahmen seiner Tätigkeit als Vermögensberater bekannt gewordene Kundendaten (z. B. über bestehende Geldanlagen und Depotstände) für Zwecke seines neuen Unternehmens. Die Nutzung der Kundendaten war jedoch ausschließlich im Rahmen seiner Tätigkeit für die Vermögensberatungsfirma zulässig. Nach § 90 HGB darf ein Handelsvertreter Geschäfts- und Betriebsgeheimnisse, die ihm anvertraut oder als solche durch seine Tätigkeit bekannt geworden sind, auch nach Beendigung des Vertragsverhältnisses nicht verwerten oder anderen mitteilen. Außerdem waren darüber hinaus auch im Handelsvertretervertrag Verschwiegenheitspflichten, Wettbewerbsverbote sowie die Pflicht zur Wahrung des Datengeheimnisses gemäß § 5 BDSG geregelt.

Vor diesem Hintergrund war die weitere Verarbeitung und Nutzung der Kundendaten nach Beendigung des Handelsvertretervertrages unzulässig. Die noch bei der Consultingfirma vorhandenen Daten waren zu löschen bzw. entsprechende Unterlagen zu vernichten.

4.2.8 Gesundheits- und Sozialwesen

4.2.8.1 Weitergabe von Patientendaten nach Praxisaufgabe

Eine Patientin erfuhr durch ein Informationsschreiben einer Klinik von der Praxisaufgabe ihrer ehemaligen Ärztin. Die Patientenakten wurden von ihr zur weiteren Betreuung der Patienten an die Klinik übergeben. Offensichtlich wurden aber die Betroffenen durch die Ärztin darüber nicht informiert und die Einholung einer Einwilligung zur Weitergabe der Patientendaten versäumt.

Bei der Schließung einer ärztlichen Praxis ist das Patientengeheimnis hinsichtlich der zu diesem Zeitpunkt vorhandenen und im Rahmen der gesetzlichen Fristen aufzubewahrenden Pati-

entenakten zu beachten. § 10 Abs. 4 der Berufsordnung der Sächsischen Landesärztekammer (Berufsordnung - BO) schreibt vor, dass der Arzt nach Aufgabe der Praxis seine Aufzeichnungen für die Dauer von mindestens zehn Jahren nach Abschluss der Behandlung aufzubewahren oder dafür Sorge zu tragen hat, dass diese in gehörige Obhut gegeben werden. Eine Übertragung der Patientenunterlagen an einen anderen Arzt zur weiteren Betreuung der Patienten ist nur mit der eindeutigen und unmissverständlichen Einwilligung der betroffenen Patienten zulässig. Die Weitergabe der Patientendaten ohne eine den Anforderungen des § 4a BDSG genügende Einwilligung hingegen verletzt das informationelle Selbstbestimmungsrecht der Patienten sowie die ärztliche Schweigepflicht nach § 203 Strafgesetzbuch (StGB). Die Arzt-Patienten-Vertrauensbeziehung (§ 28 Abs. 1 Nr. 1 BDSG) lässt sich nicht ohne Weiteres auf einen anderen Arzt oder gar eine Klinik übertragen.

Für die Aufsichtsbehörde stellte die erfolgte Datenübermittlung einen Verstoß gegen die in § 203 Strafgesetzbuch (StGB) geregelte ärztliche Schweigepflicht dar. Eine Ahndung durch die Staatsanwaltschaft scheiterte jedoch an dem zu spät gestellten Strafantrag der Betroffenen.

Gegen die verantwortliche Ärztin wurde durch die Aufsichtsbehörde ein Bußgeld festgesetzt (vgl. Pkt. 9).

4.2.8.2 Dienstleistungen im Pflegeheim

Eine Unternehmerin, die in einem Alten- und Pflegeheim Dienstleistungen anbietet, fragte die Aufsichtsbehörde, inwieweit die Heimleitung ihr die Adressen von Betreuern derjenigen Personen herausgeben dürfe, die ihre Dienstleistungen zwar in Anspruch nehmen, aber nicht mehr selbst bezahlen können. Da der Frau in den meisten Fällen kein Ansprechpartner zur Begleichung ihrer Rechnungen bekannt sei, waren bereits erhebliche Außenstände aufgelaufen.

In diesem Fall ist nach den Bestimmungen des § 28 Abs. 3 Nr. 1 BDSG eine Übermittlung der Betreuerdaten von der Heimleitung an die Unternehmerin zulässig. Danach ist eine Datenübermittlung erlaubt, wenn sie zur Wahrung berechtigter Interessen eines Dritten erforderlich ist und kein Grund zu der Annahme besteht, dass Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung haben.

Die Daten der Heimbewohner und deren Betreuer werden zwar zunächst nur für eigene Zwecke des Heimes verarbeitet. Die Unternehmerin benötigt jedoch die Adressen der Betreuer ihrer Kunden zur Abwicklung der Rechnungslegung. Insoweit ist ein wirtschaftliches Interes-

se an der Übermittlung der Daten gegeben. Da die Betroffenen im vorliegenden Fall gesetzlich bestellte Betreuer sind, die von Berufs wegen alle Angelegenheiten einschließlich des Bezahlens von Rechnungen der zu Betreuenden abwickeln, besteht auch kein Grund zu der Annahme, dass sie ein schutzwürdiges Interesse am Ausschluss der Übermittlung haben.

4.2.9 Versicherungen

4.2.9.1 Weitergabe von Daten Unfallgeschädigter an Mietwagen- und Reparaturfirmen

Eine Fahrzeugführerin erhielt unmittelbar nach einem unverschuldeten Unfall den Anruf einer Mietwagenfirma, die ihr ein Mietangebot unterbreitete. Kurze Zeit später rief eine Karosseriewerkstatt bei ihr an, die gleichfalls ihre Dienste anbot. Die Betroffene vermutete eine Datenweitergabe von Seiten der Versicherung des Unfallverursachers, die allerdings ohne ihr Einverständnis erfolgt sein musste.

Die Ermittlungen der Aufsichtsbehörde ergaben, dass es in der Versicherungsbranche üblich ist, Daten (Name, Anschrift, Telefonnummer sowie Fahrzeugdaten) Unfallgeschädigter an Reparatur- und Mietwagenfirmen weiterzureichen, jedoch grundsätzlich nur mit dokumentiertem Einverständnis der Betroffenen. Das Einverständnis der Betroffenen war in diesem Fall jedoch nicht eingeholt worden.

Nach Hinweis durch die Aufsichtsbehörde wurden die Daten der Betroffenen bei der Mietwagenfirma und bei der Karosseriewerkstatt gelöscht. Die Mitarbeiter der Versicherung wurden in dem Zusammenhang nochmals zum datenschutzgerechten Umgang mit personenbezogenen Daten belehrt.

4.2.10 Verkehrswesen

4.2.10.1 Datenerhebung bei erhöhtem Beförderungsentgelt

Ein Petent wurde bei einer Fahrausweiskontrolle in einem öffentlichen Verkehrsmittel ohne gültigen Fahrausweis angetroffen. Das Kontrollpersonal bat ihn daraufhin um seinen Personalausweis, um u. a. die Ausweisnummer zu notieren. Der Bitte des Petenten, ihm eine Kopie der erfassten Daten auszuhändigen, kam das Kontrollpersonal nicht nach. Der Betroffene sah sich in seinem Recht auf Datenschutz verletzt und wandte sich daraufhin an die Aufsichtsbehörde, die den Sachverhalt prüfte.

Personalausweis- oder Passnummern sind für den Einzug eines erhöhten Beförderungsentgelts nicht erforderlich und deren Erhebung nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG unzulässig. Dem Unternehmen wurde mitgeteilt, welche personenbezogenen Daten für den Einzug des erhöhten Beförderungsentgelts und ggf. für die Erstattung von Strafanzeigen verarbeitet werden dürfen und welche Hinweispflichten nach § 4 Abs. 3 Satz 1 BDSG bestehen (vgl. hierzu 1. TB, Pkt. 4.2.3).

Das Unternehmen wurde aufgefordert, die Personalausweis- oder Passnummer von „Schwarzfahrern“ künftig nicht mehr zu erfassen. Die Aufsichtsbehörde schlug dem Unternehmen vor, stattdessen auf dem Erhebungsbogen zu vermerken, dass die Überprüfung der Angaben mittels eines Ausweisdokumentes erfolgt. Der Betroffene soll außerdem eine Kopie des Erhebungsbogens erhalten.

5 Beratungstätigkeit/Anfragen an die Behörde

Die Aufsichtsbehörde berät und unterstützt die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse. (vgl. § 38 Abs. 1 Satz 2 BDSG).

Die Beratung von Datenschutzbeauftragten, aber auch von Geschäftsführern von Unternehmen, Betriebsräten und Betroffenen in datenschutzrechtlichen Fragen bildete im Berichtszeitraum einen großen Teil der Tätigkeit der Regierungspräsidien als Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich. Schwerpunkte der Anfragen an die Aufsichtsbehörde waren u. a.:

- Bestellung/Tätigkeit des betrieblichen Datenschutzbeauftragten,
- Verarbeitung von Kundendaten, Kundenkarten,
- Arbeitnehmerdatenschutz,
- medizinischer Datenschutz, Pflegedienste, Beratungsstellen,
- Videoüberwachung,
- Verbände, Vereine,
- Datenverarbeitung für Marketingzwecke,
- Datenschutz im Mietverhältnis,
- Aspekte der Auftragsdatenverarbeitung,

- Informationsmaterial, aktuelle gesetzliche Regelungen,
- Meldepflicht, Verfahrensverzeichnis,
- Umgang mit Bewerberdaten,
- Internet/neue Medien,
- Tätigkeit von Wirtschaftsauskunfteien,
- Unterrichtungen nach § 7 Abs. 3 SächsDSG,
- Erfassung von Ausweisdaten/Personalausweiskopien (Handel, Banken),
- Aufbewahrungs- bzw. Löschfristen, Datenträgervernichtung,
- Datenschutzklauseln in Verträgen/Formularen,
- Zulässigkeit von Datenübermittlungen,
- Aushändigung von Unterlagen/Akteneinsicht,
- Schadensersatz.

Sehr zahlreiche Anfragen wurden zur Bestellung des betrieblichen Datenschutzbeauftragten, zu seiner Fachkunde, Zuverlässigkeit, Tätigkeit und zu Abberufungsmöglichkeiten an die Regierungspräsidien gerichtet. Die von den Aufsichtsbehörden in den Unternehmen regelmäßig durchgeführten Kontrollen haben dabei wesentlich zu einer Sensibilisierung der verantwortlichen Stellen in Bezug auf die Einhaltung der Bestellungspflicht beigetragen. Hinzuweisen ist in diesem Zusammenhang auch auf die Änderung des BDSG im August 2006. § 4f Abs. 1 sieht nun vor, dass nicht-öffentliche Stellen dann einen betrieblichen Datenschutzbeauftragten zu bestellen haben, wenn sie mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Das Maß der erforderlichen Fachkunde bestimmt sich nach dem Umfang der Datenverarbeitung der verantwortlichen Stelle und dem Schutzbedarf der personenbezogenen Daten, die die verantwortliche Stelle erhebt oder verarbeitet (vgl. § 4f Abs. 2 BDSG).

Häufig wurde auch um Beratung zur Auftragsdatenverarbeitung sowie zum Führen des öffentlichen Verfahrensverzeichnisses gebeten. In diesen Bereichen zeigten sich oft noch erhebliche Probleme der verantwortlichen Stellen bei der Umsetzung der gesetzlichen Bestimmungen.

Verantwortliche Stellen und Betroffene stellten außerdem häufig Anfragen zur Kundendatenverarbeitung, Datenverarbeitung im Rahmen des Marketings, Arbeitnehmerdatenschutz, Umgang mit Bewerberdaten und Videoüberwachung.

6 Prüfung der Verhaltensregeln von Berufsverbänden

Die Aufsichtsbehörde überprüft die ihr von Berufsverbänden und anderen - bestimmte Gruppen verantwortlicher Stellen vertretenden - Vereinigungen unterbreiteten Entwürfe für interne datenschutzrechtliche Verhaltensregeln auf ihre Vereinbarkeit mit dem geltenden Datenschutzrecht (§ 38a BDSG).

Im Berichtszeitraum sind an die Regierungspräsidien keine derartigen Anliegen herangetragen worden.

7 Genehmigung von Datenübermittlungen in Drittstaaten

Sofern personenbezogene Daten in Drittstaaten ohne angemessenes Datenschutzniveau übermittelt werden sollen und keiner der in § 4c Abs. 1 BDSG aufgeführten Ausnahmetatbestände greift, kann die Aufsichtsbehörde entsprechende Datenübermittlungen genehmigen, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist (§ 4c Abs. 2 BDSG).

Als Garantien für den Schutz des Persönlichkeitsrechts und die Ausübung der damit verbundenen Rechte sind entsprechende Vertragsklauseln oder verbindliche Unternehmensregelungen vorzulegen. Werden insoweit die von der Europäischen Kommission erarbeiteten Standardvertragsklauseln verwendet, erübrigt sich die Einschaltung der Aufsichtsbehörde, d. h., eine Genehmigung der Datenübermittlungen ist dann nicht mehr erforderlich.

Im Berichtszeitraum sind bei den Regierungspräsidien keine Genehmigungsanträge gestellt worden.

8 Öffentlichkeitsarbeit

Die Aufsichtsbehörden für den nicht-öffentlichen Bereich haben regelmäßig, spätestens jedoch alle zwei Jahre, einen Tätigkeitsbericht zu veröffentlichen (§ 38 Abs. 1 Satz 7 BDSG).

Mit der Veröffentlichung dieses Tätigkeitsberichtes kommt das Sächsische Staatsministerium des Innern letztmalig seiner Pflicht nach, die Öffentlichkeit alle zwei Jahre über die Tätigkeit der Aufsichtsbehörden zu informieren.

Darüber hinaus bieten auch die Internetseiten des Sächsischen Staatsministeriums des Innern und des Regierungspräsidiums Dresden eine Vielzahl von Informationen zum Datenschutz, die einerseits Einblicke in die Kontrolltätigkeit der Aufsichtsbehörde, andererseits aber auch Hilfestellung bei der Lösung datenschutzrechtlicher Probleme in den Unternehmen geben sollen. Erwähnt sei dabei insbesondere die Dokumentation der Endauswertung der koordinierten Datenschutzkontrolle bei Wohnungsunternehmen (vgl. Pkt. 3.3).

Die Zusammenarbeit mit der Gesellschaft für Datenschutz und Datensicherung e. V. (GDD) bildete einen weiteren wesentlichen Schwerpunkt der Öffentlichkeitsarbeit der Aufsichtsbehörden im Freistaat Sachsen. Die viermal jährlich stattfindenden Tagungen des ERFA-Kreises Sachsen der GDD bieten sehr gute Möglichkeiten eines direkten und effektiven Meinungsaustausches und ermöglichen es der Aufsichtsbehörde, den Unternehmen neben umfangreichem Fachwissen wesentliche Aspekte der Aufsichtstätigkeit zu vermitteln - z. B. in persönlichen Gesprächen, in Diskussionen oder bei diversen Fachvorträgen. Stellvertretend sei hier der gemeinsam durch die Regierungspräsidien Chemnitz und Dresden gestaltete Vortrag „Aus der Prüfpraxis der Aufsichtsbehörde“ zur ERFA-Kreis-Tagung am 8. September 2005 in Waldenburg/OT Franken genannt.

Auf Wunsch der Veranstalter wurden darüber hinaus durch das Regierungspräsidium Dresden auch andere Tagungen und Konferenzen mit Fachvorträgen bereichert, so die ASB-Geschäftsführerkonferenz im März 2005 in Ottendorf-Okrilla, die ÖPNV-Datenschutzfachtagung im Mai 2005 in Dresden und das Regionaltreffen Dresden des Baustoff-Fachhandelsverbandes Ost im September 2005.

Zur Erweiterung des Serviceangebotes wurden von den Aufsichtsbehörden zudem Informationsbroschüren, Formulare und Musterdokumente/-verträge zum Datenschutz vorgehalten. Das Sächsische Staatsministerium des Innern hat im Jahr 2005 einen Leitfaden zum Datenschutz im nicht-öffentlichen Bereich für Bürger herausgegeben, der neben nützlichen Hinweisen und Empfehlungen zum Datenschutz u. a. auch praktische Musterschreiben zu den Bereichen SCHUFA, Handels- und Wirtschaftsauskunfteien, Versicherungsunternehmen und Kreditinstituten enthält.

9 Ordnungswidrigkeitenverfahren

Die Zuständigkeit der Regierungspräsidien zur Ahndung von Ordnungswidrigkeiten ergab sich aus der Verordnung der Sächsischen Staatsregierung über die Regelung der Zuständigkeit der Aufsichtsbehörden nach § 38 Abs. 6 BDSG vom 27. August 1991 (SächsGVBl. 1991, S. 324).

Im Berichtszeitraum wurden durch die Regierungspräsidien 24 Ordnungswidrigkeitenverfahren eingeleitet. Drei Verfahren befanden sich Ende 2006 noch in der Anhörungsphase; vier weitere sind eingestellt worden. In einem Fall konnte während der Ermittlungen zwar rechtswidriges Handeln nachgewiesen werden, jedoch entsprach dies nicht dem Tatbestand einer Ordnungswidrigkeit. In einem anderen Fall setzte sich der Betroffene während des Verfahrens ins Ausland ab. Ein Verfahren musste eingestellt werden aufgrund der zwischenzeitlich eingetretenen Verjährung, ein anderes aufgrund des nicht bestätigten Tatvorwurfes.

Damit sind im Berichtszeitraum 17 Verfahren mit einem Bußgeldbescheid und ein Verfahren mit einem Verwarnungsgeld abgeschlossen worden; die Bußgeldsumme belief sich auf insgesamt 5.035 €.

Mit acht Bußgeldbescheiden (4 x 100 €, je 1 x 200 €, 300 €, 500 € und 1.000 €) sowie einem Verwarnungsgeld in der maximalen Höhe von 35 € wurden Verstöße gegen die Auskunftspflichten gemäß § 38 Abs. 3 BDSG sanktioniert (§ 43 Abs. 1 Nr. 10 BDSG).

Zum Beispiel kam ein Restaurantbetreiber sieben Aufforderungen der Aufsichtsbehörde nach Auskunftserteilung (inkl. einer Vorortkontrolle) nicht nach. Erst nach Einleitung eines Ordnungswidrigkeitenverfahrens konnten die noch offenen Punkte abgearbeitet werden. Geahndet wurde dieser Verstoß mit einem Bußgeld in Höhe von 1.000 €.

Verstöße gegen die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten wurden in drei Fällen geahndet (§ 43 Abs. 1 Nr. 2 BDSG).

Einen Bußgeldbescheid in Höhe von 600 € erhielt die Geschäftsführerin eines im Bereich der sozialpsychiatrischen Versorgung tätigen Unternehmens. Als Gründe des (bereits mehrjährigen) Verstoßes führte sie aktuelle Gespräche zur Bestellung eines gemeinsamen betrieblichen Datenschutzbeauftragten mit anderen Trägern bzw. ihrem eigenen Spitzenverband an. Die Geschäftsführerin war sich offensichtlich der Pflicht zur Bestellung bewusst, so dass von einer vorsätzlichen Pflichtverletzung ausgegangen wurde. Das Amtsgericht bestätigte den Gesetzesverstoß, warf der Unternehmerin aber lediglich Fahrlässigkeit vor, so dass das vormals verhängte Bußgeld auf 300 € reduziert wurde.

Der Geschäftsführer eines kleinen Unternehmens der Wohnungswirtschaft bestellte sich selbst zum Datenschutzbeauftragten. § 4f Abs. 3 BDSG fordert jedoch, dass der Datenschutzbeauftragte dem Leiter der nicht-öffentlichen Stelle unmittelbar zu unterstellen ist. Ein Datenschutzbeauftragter darf somit nicht selbst Mitglied der Geschäftsführung sein. Diese Anforderung an einen Datenschutzbeauftragten ist regelmäßig auch Inhalt datenschutzrechtlicher Grundlagenseminare. Der Geschäftsführer hatte selbst ein solches Seminar besucht. So wurde trotz der Tatsache, dass unmittelbar nach dem Tätigwerden der Aufsichtsbehörde eine geeignete Person zum Datenschutzbeauftragten bestellt worden war, ein Bußgeld in Höhe von 200 € verhängt.

In einem mittelständischen, 1992 gegründeten Handelsunternehmen der Telekommunikationsbranche war von Gründung an kein Datenschutzbeauftragter bestellt gewesen. Der Geschäftsführer wurde jedoch nur für die letzten beiden Jahre zur Verantwortung gezogen. Geahndet wurde dieser Verstoß mit der Zahlung eines Bußgeldes in Höhe von 500 €. Die Entscheidung über den eingelegten Einspruch stand zum Ende des Berichtszeitraumes noch aus.

Mit Bußgeldern in Höhe von 200 € und 350 € sind Verstöße gegen § 28 Abs. 4 Satz 2 BDSG geahndet worden (§ 43 Abs. 1 Nr. 3 BDSG). In beiden Fällen wurde die Datenschutzaufsichtsbehörde durch Eingaben von Betroffenen darauf aufmerksam gemacht, dass Unternehmen mit Werbeansprachen an die Betroffenen herantraten, die keine Auskunft darüber geben konnten, woher sie die Kontaktdaten bezogen (vgl. Pkt. 4.2.2.5).

Gegen ein Kleinunternehmen wurde wegen der Verletzung von Meldepflichten ein Bußgeldbescheid in Höhe von 50 € erlassen (§ 43 Abs. 1 Nr. 1 BDSG). Zwar war das Unternehmen im bei der Aufsichtsbehörde geführten Verfahrensregister gemeldet; jedoch hatten sich zwischenzeitlich Firmenname, Firmensitz und der Name des Geschäftsführers geändert, ohne dass die Aufsichtsbehörde hierüber informiert worden war.

Zwei Bußgeldverfahren betrafen materielle Rechtsverletzungen (§ 43 Abs. 2 Nr. 1 BDSG):

Die ehemalige Vorsitzende der Revisionskommission eines Vereins war der Auffassung, die Geschäftsführung und weitere Angestellte bezögen überhöhte Gehälter. Nachdem ihre Bemühungen zur Herbeiführung einer vereinsinternen Klärung vom Vorstand zurückgewiesen worden waren, gab sie Informationen über die Gehälter dieser Personen an die Presse weiter. Die unbefugte Datenübermittlung wurde mit einem Bußgeld in Höhe von 200 € geahndet; die gerichtliche Entscheidung über den Einspruch stand zum Ende des Berichtszeitraumes noch aus.

Eine Ärztin gab nach Praxisaufgabe Patientenakten zur weiteren Betreuung der Patienten an eine Klinik (vgl. Pkt. 4.2.8.2), versäumte jedoch, die dazu notwendige Einwilligung der Pati-

enten zur Schweigepflichtentbindung einzuholen. Dieser Verstoß gegen § 4 Abs. 1 BDSG wurde mit einem Bußgeld in Höhe von 500 € geahndet.

10 Zusammenarbeit mit anderen Aufsichtsbehörden

Die im Sächsischen Staatsministerium des Innern halbjährlich durchgeführten gemeinsamen Dienstberatungen der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich des Freistaates Sachsen dienten der Abstimmung in datenschutzrechtlichen Grundsatzfragen, dem Austausch aktueller Prüferfahrungen sowie der Festlegung von Kontrollschwerpunkten.

Die Zusammenarbeit mit den Aufsichtsbehörden anderer Bundesländer bestand im Berichtszeitraum im Wesentlichen aus gegenseitigen Unterrichtungen (vgl. § 38 Abs. 1 Satz 4 BDSG) und dem Meinungsaustausch zu speziellen fachlichen Problemstellungen. Die jährlich durchgeführten Workshops der Datenschutzaufsichtsbehörden waren hierbei von besonderer Bedeutung. Im Jahr 2005 fand ein Workshop der Aufsichts- und Dienstleistungsdirektion in Trier (Rheinland-Pfalz) und 2006 im Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein in Kiel statt.

Hinsichtlich der bundesweiten Abstimmung zu datenschutzrechtlichen Grundsatzfragen ist der Düsseldorfer Kreis von Bedeutung. Dieses Gremium der obersten Datenschutzaufsichtsbehörden kommt zweimal jährlich zusammen. Der Düsseldorfer Kreis ist in mehrere Arbeitsgruppen untergliedert, die sich jeweils mit speziellen Fragestellungen zu Themen wie Telekommunikation/Tele- und Mediendienste, Versicherungen, Internationaler Datenverkehr, Kreditwirtschaft oder Auskunfteien beschäftigen. Der Freistaat Sachsen wurde in diesen Gremien durch das Sächsische Staatsministerium des Innern vertreten.

11 Beendigung der Kontrolltätigkeit

Der Sächsische Landtag beschloss am 13. Dezember 2006 das Gesetz zur Änderung des Sächsischen Datenschutzgesetzes, welches zum 1. Januar 2007 in Kraft trat (SächsGVBl. 2006, S. 530 f.). Die Aufsicht über den Datenschutz im nicht-öffentlichen Bereich nimmt seitdem der Sächsische Datenschutzbeauftragte wahr.

Die Regierungspräsidien haben seit der Aufgabenübertragung im August 1991 einen anerkennenswerten, wesentlichen Beitrag zur Verbesserung des Datenschutzniveaus bei privaten Unternehmen, Vereinen und sonstigen nicht-öffentlichen Stellen innerhalb des Freistaates Sachsen geleistet.

Verteilerhinweis:

Diese kostenlose Informationsschrift wird von der Sächsischen Staatsregierung im Rahmen ihrer verfassungsmäßigen Verpflichtung zur Unterrichtung der Öffentlichkeit herausgegeben. Sie darf weder von Parteien noch von deren Kandidaten oder Helfern im Zeitraum von sechs Monaten vor einer Wahl zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für alle Wahlen.

Missbräuchlich sind insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken oder Aufkleben parteipolitischer Informationen oder Werbemittel.

Untersagt ist auch die Weitergabe an Dritte zur Verwendung bei der Wahlwerbung.

Auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl darf die vorliegende Druckschrift nicht so verwendet werden, dass dies als Parteinahme der Herausgeber zugunsten einzelner politischer Gruppen verstanden werden könnte.

Diese Beschränkungen gelten unabhängig vom Vertriebsweg, also unabhängig davon, auf welchem Wege und in welcher Anzahl diese Informationsschrift dem Empfänger zugegangen ist.

Erlaubt ist es jedoch den Parteien, diese Informationsschrift zur Unterrichtung ihrer Mitglieder zu verwenden.