Datenschutz im nicht-öffentlichen Bereich

1. Tätigkeitsbericht 2001/2002

Freistaat Sachsen

Staatsministerium des Innern

Glaube & Macht

Sachsen im Europa der Reformationszeit

2. Sächsische Landesausstellung
Torgau – Schloss Hartenfels
24. Mai bis 10. Oktober 2004

Info-Telefon: 01805-1547 00
www.Landesausstellung.
Sachsen.de

1. Tätigkeitsbericht

für den Datenschutz im nicht-öffentlichen Bereich

Berichtszeitraum: 2001-2002

Impressum

Herausgeber:	Sächsisches Staatsministerium des Innern Referat 42 (Datenschutz) Wilhelm-Buck-Str. 2 01097 Dresden Telefon: (0351) 564 32 60 Telefax: (0351) 564 34 09 E-Mail: Datenschutz@smi.sachsen.de Internet: www.smi.sachsen.de/datenschutz
Auflagenhöhe:	1.000 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

1 EINLEITUNG 4

2 DATENSCHUTZ UND AUFSICHT IM NICHT-ÖFFENTLICHEN BEREICH 5

2.1 Aufgaben des Sächsischen Staatsministeriums des Innern auf dem Gebiet des Datenschutzes im nicht-öffentlichen Bereich 5

2.2 Aufgaben der Regierungspräsidien auf dem Gebiet des Datenschutzes im nicht-öffentlichen Bereich 6

3 VERFAHRENSREGISTER (§ 38 ABS. 2 BDSG) 8

4 KONTROLLTÄTIGKEIT DER REGIERUNGSPRÄSIDIEN 10

4.1 Rechtsgrundlage 10

4.2 Regelkontrolle

4.2.1 Überblick 11

4.2.2 Videoüberwachung von Geldautomaten 14

4.2.3 Koordinierte Datenschutzkontrolle von Verkehrsunternehmen 16

4.2.4 Online-Prüfung von Versorgungsunternehmen 22

4.3 Anlasskontrolle

4.3.1 Überblick 23

4.3.2 Datenübermittlung im Rahmen eines Gruppenversicherungsvertrages 27

4.3.3 Übermittlung von Hotel-Buchungsdaten 29

4.3.4 Herausgabe von Unterlagen an Vereinsmitglieder 31

4.3.5 Kundenkarten von der Wohnungsbaugesellschaft 31

4.3.6 Selbstauskünfte von Mietbewerbern 32

4.3.7 Videoüberwachung in einem Erlebnisrestaurant 36

4.3.8 Webcam auf dem Parkplatz eines Supermarktes 38

4.3.9 Schwarzes Brett für zahlungsunwillige Kunden im Internet 39

4.3.10 Stempel-Musterkataloge mit Echtdaten 41

4.3.11 Veröffentlichung personenbezogener Daten bei Erlöschen der Prokura 42

4.3.12 Datenerhebung durch eine Kurklinik mittels Fragebogen 43
4.3.13 Prüfangebote zur Nettolohnerhöhung 44
4.3.14 Erhebung von Einkommensdaten von Mitgliedern eines Tierschutzvereins 46
4.3.15 Datenverarbeitung für Werbezwecke 47
4.3.16 Werbeschreiben einer Bank 49
4.3.17 Personalausweiskopien bei Rabattaktionen 50
4.3.18 Personalausweiskopien bei Bankgeschäften 51
4.3.19 Kontostandsanzeige an Geldautomaten 52
4.3.20 Aufbewahrung von Belegen bei Zahlung mit EC-Karte 53

5 BERATUNGSDIENST / ANFRAGEN AN DIE BEHÖRDE 53

6 PRÜFUNG DER VERHALTENSREGELN VON BERUFSVERBÄNDEN 57

7 GENEHMIGUNG VON DATENÜBERMITTLUNGEN IN DRITTSTAATEN 58

8 ÖFFENTLICHKEITSARBEIT 58

9 ORDNUNGSWIDRIGKEITEN 60

10 ZUSAMMENARBEIT DER AUFSICHTSBEHÖRDEN 61

11 AUSBLICK 65

1 Einleitung

Datenschutz - ein wichtiger Teil des Persönlichkeitsrechts – gewährleistet das Recht auf informationelle Selbstbestimmung, d. h. das Recht, selbst über die Erhebung, Verwendung und Weitergabe personenbezogener Daten zu bestimmen (Artikel 33 der Sächsischen Verfassung). Durch die ständige Weiterentwicklung der Informations- und Kommunikationstechnik wird dieser Schutz immer wichtiger. Vor allem in der Wirtschaft sind die Bestände personenbezogener Daten mit dem Fortschreiten der Technik rasant angewachsen. Man denke nur an die vielfältigen Angebote von Firmen, die ihre Dienste über das Internet anbieten. Die Nutzung dieser Dienste ist für den Bürger zwar vorteilhaft und wird deshalb immer mehr angenommen, aber sie birgt andererseits auch ein erhebliches Risiko für das vom Grundgesetz geschützte Persönlichkeitsrecht eines jeden Nutzers.

Der Gesetzgeber hat mit der Novellierung des Bundesdatenschutzgesetzes (BDSG), die am 23.05.2001 in Kraft getreten ist, die Vorgaben der EG-Datenschutzrichtlinie umgesetzt. Die Neuregelungen berücksichtigen insbesondere die durch den Fortschritt der Technik veränderten Rahmenbedingungen in datenschutzrechtlicher Hinsicht. Zum Beispiel wirkt die Regelung zum Systemdatenschutz (§ 3 a BDSG) auf eine datensparende bzw. datenvermeidende Technikgestaltung hin. Neuerdings wird die Zulässigkeit und Transparenz der Vidoeoüberwachung öffentlicher Räume (§ 6 b BDSG) sowie auch die Transparenz der Datenverarbeitung beim Einsatz von Chipkarten (§ 6 c BDSG) geregelt. Datenschutzrechtliche Produkte und Konzepte sollen durch das Datenschutzaudit (§ 9 a BDSG) gefördert werden.

Das Sächsische Staatsministerium des Innern ist oberste sächsische Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich. Nicht-öffentliche Stellen sind natürliche Personen, juristische Personen des Privatrechts (hauptsächlich Wirtschaftsunternehmen) und Personenvereinigungen des Privatrechts (z. B. Vereine). Ausgenommen sind diejenigen Stellen, die Aufgaben der öffentlichen Verwaltung erfüllen. Seit der Novellierung des BDSG besteht gemäß § 38 Abs. 1 die Verpflichtung, spätestens alle zwei Jahre einen Bericht über die Tätigkeit der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich zu veröffentlichen. Der Bericht bezieht sich auf die aufsichtsbehördliche Tätigkeit im Freistaat Sachsen in den Jahren 2001 bis 2002.

Das konstruktive Zusammenwirken von Aufsichtsbehörden und Unternehmen hat zu einer weiteren Verbesserung der Einhaltung des Datenschutzes im Freistaat Sachsen im Berichtszeitraum geführt. Besonderes Augenmerk galt der Stärkung der Eigenkontrolle der Unternehmen durch die betrieblichen Datenschutzbeauftragten, die im BDSG als Grundsatz verankert ist. Im Ergebnis der durchgeführten Prüfungen konnten überwiegend einvernehmliche Lösungen zwischen Aufsichtsbehörden und geprüften Unternehmen gefunden werden bzw. wurden die von den Aufsichtsbehörden bemängelten datenschutzrechtlichen Verstöße meist unverzüglich abgestellt.

Die hohe Anzahl der im Berichtszeitraum an die Aufsichtsbehörden gerichteten Anfragen aus den verschiedensten Bereichen ist Indiz für die Aktualität und Bedeutung des Datenschutzes in der Praxis. Sie spricht auch für das Vertrauen in die solide Beratungskompetenz der Aufsichtsbehörden.

Der vorliegende Tätigkeitsbericht dient der Unterrichtung der Öffentlichkeit. Schwerpunkte sind dabei ausgewählte Fälle aus der Kontrollpraxis der Aufsichtsbehörden. Daneben gibt statistisches Material Auskunft über die Registermeldungen und Prüfmaßnahmen im Berichtszeitraum. Außerdem wird auf Entwicklungstendenzen des Datenschutzes im nicht-öffentlichen Bereich eingegangen, die sich für Sachsen als bedeutsam abzeichnen.

Der Bericht soll die Bürger sensibilisieren, ihre gesetzlich garantierten Rechte auch wahrzunehmen. Ein guter Selbstdatenschutz ist die beste Vorsorge dafür, dass datenschutzrechtliche Probleme erst gar nicht entstehen. Der sächsischen Wirtschaft gibt der Bericht Aufschluss über Verbesserungsmöglichkeiten beim Datenschutz, um so die Eigenkontrolle durch die Unternehmen zu fördern.

2 Datenschutz und Aufsicht im nicht-öffentlichen Bereich

2.1 Aufgaben des Sächsischen Staatsministeriums des Innern auf dem Gebiet des Datenschutzes im nicht-öffentlichen Bereich

Dem Sächsischen Staatsministerium des Innern obliegt die *Fachaufsicht* über die für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden in Sachsen. Dies sind

die Regierungspräsidien der drei Sächsischen Regierungsbezirke Chemnitz, Dresden und Leipzig.

Außerdem wirkt das Sächsische Staatsministerium des Innern in der Funktion als oberste Aufsichtsbehörde daran mit, die datenschutzrechtlichen Regelungen auf EU- und Bundesebene fortzuentwickeln.

Das Sächsische Staatsministerium des Innern arbeitet mit Aufsichtsbehörden anderer Länder zusammen und gehört dem „Düsseldorfer Kreis“ an (vgl. Pkt.10 Zusammenarbeit der Aufsichtsbehörden).

2.2 Aufgaben der Regierungspräsidien auf dem Gebiet des Datenschutzes im nicht-öffentlichen Bereich

Die Regierungspräsidien im Freistaat Sachsen sind gemäß der Verordnung der Sächsischen Staatsregierung über die Regelung der Zuständigkeit der Aufsichtsbehörden nach § 38 Abs. 6 des Bundesdatenschutzgesetzes vom 27.08.1991 (SächsGVBl. 1991, S. 324) zuständige Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich. Sie überwachen die Durchführung des Datenschutzes bei nicht-öffentlichen Stellen und öffentlich-rechtlichen Wettbewerbsunternehmen.

Sie kontrollieren die Einhaltung der Regelungen des BDSG sowie anderer Datenschutzvorschriften einschließlich derjenigen, die in Mitgliedsstaaten der Europäischen Union gelten. Kontrolliert wird sowohl die automatisierte Verarbeitung als auch die Verarbeitung in oder aus nichtautomatisierten Dateien.

Die Aufgaben und Befugnisse der Aufsichtsbehörden wurden durch die Novelle des Bundesdatenschutzgesetzes erweitert. Unter Berücksichtigung der Neuregelung ergeben sich für die Regierungspräsidien folgende Aufgaben:

- **Wahrnehmung der Kontrollkompetenzen**
  - Anlassunabhängige Kontrolle (§ 38 Abs. 1 S. 1 BDSG)

- Informations-, Betretungs-, Besichtigungs-, Prüfungs- und Einsichtsrechte (§ 38 Abs. 3 und 4 BDSG)
- Datenübermittlungen an andere Aufsichtsbehörden und Amtshilfe innerhalb der EU (§ 38 Abs. 1 S. 3 und 4 BDSG)
- Führung des öffentlichen Registers meldepflichtiger Verarbeitungen (§ 38 Abs. 2 BDSG)
- Herausgabe regelmäßiger Tätigkeitsberichte (§ 38 Abs. 1 S. 6 BDSG)

- **Durchsetzungs-/Sanktionsmaßnahmen nach pflichtgemäßem Ermessen**
- Durchführung von Bußgeldverfahren nach § 43 BDSG
- Eigenständiges Strafantragsrecht bei BDSG-Straftatbeständen (§ 44 Abs. 2 BDSG)
- Anzeige und Unterrichtung des Betroffenen bei den zuständigen Ahndungs- und Verfolgungsbehörden (§ 38 Abs. 1 S. 5 BDSG) und
- Zwangsgeld zur Durchsetzung angeordneter Maßnahmen zur Mängelbeseitigung bzw. Verbot des Einsatzes einzelner Verfahren (§ 38 Abs. 5 S. 1 und 2 BDSG)
- Aufforderung zur Abberufung des betrieblichen Datenschutzbeauftragten (§ 38 Abs. 5 S. 3 BDSG)

- **Auf Antrag der verantwortlichen Stelle/des Datenschutzbeauftragten (DSB)**
- Allgemeine Unterstützung des Datenschutzbeauftragten (§ 4 g Abs. 1 S. 2 BDSG)
- Mitwirkung bei der Vorabkontrolle (§ 4 d Abs. 6 S. 3 BDSG)
- Überprüfung vorgelegter Verhaltensregelungen (§ 38 a BDSG)
- Genehmigungsverfahren bei Datentransfer in Nicht-EU/EWR-Staaten ohne angemessenes Datenschutzniveau (§ 4 c Abs. 2 BDSG)

3 Verfahrensregister (§ 38 Abs. 2 BDSG)

„Die Aufsichtsbehörde führt ein Register der nach § 4 d meldepflichtigen automatisierten Verarbeitungen mit den Angaben gemäß § 4 e Satz 1." (§ 38 Abs. 2 Satz 1 BDSG).
§ 4 d BDSG definiert eine *Meldepflicht für automatisierte Verarbeitungen*. Diese Meldepflicht trifft zunächst 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 solche Unternehmen von der Meldepflicht betroffen, die mehr als vier Arbeitnehmer mit der automatisierten Datenverarbeitung für eigene Zwecke beschäftigen, wenn diese Datenverarbeitung weder durch die Einwilligung der Betroffenen noch durch die Zweckbestimmung eines Vertragsverhältnisses gedeckt ist und im Übrigen auch keine Vorabkontrolle erforderlich ist.

Die Regierungspräsidien Chemnitz, Dresden und Leipzig führen das Register der insoweit meldepflichtigen automatisierten Verarbeitungen jeweils für ihren Regierungsbezirk.

Infolge der im Berichtszeitraum erfolgten Novellierung des BDSG mussten die bis dato nach den Kriterien des § 32 BDSG 90 geführten Register auf die neuen Regelungen zur Meldepflicht umgestellt werden. Im Wesentlichen waren dabei folgende Änderungen zu berücksichtigen:

- Für Unternehmen, die geschäftsmäßig personenbezogene Daten im Auftrag als Dienstleistungsunternehmen *(„Auftragsdatenverarbeiter"*) verarbeiten oder nutzen (§ 32 Abs. 1 Nr. 3 BDSG 90), ist die *Meldepflicht entfallen*.
- *Art und Umfang* der Angaben gegenüber der Aufsichtsbehörde sind neu geregelt worden. Die Meldepflicht ist nun nicht mehr auf Unternehmen ausgerichtet, sondern auf Verfahren. Das heißt, ein Unternehmen kann durchaus mit mehreren Einträgen im Register vertreten sein.

Bereits im Vorfeld der BDSG-Novellierung war durch die Datenschutz-Aufsichtsbehörden ein bundesweit einheitliches Meldeformular (§ 4 e BDSG) sowie ein Erläuterungsblatt zur Meldepflicht (§ 4 d BDSG) erarbeitet worden, welches anlässlich der Registerumstellung sofort eingesetzt werden konnte.
Durch die Regierungspräsidien wurden alle registrierten Unternehmen angeschrieben, über die neue Rechtslage informiert und um Prüfung und Rückäußerung gebeten, ob auch weiterhin von einer Meldepflicht auszugehen ist. Den registrierten Wirtschaftsauskunfteien wurden

die neuen Meldeformulare unmittelbar mit der Bitte um Aktualisierung der Meldung übersandt. Das Regierungspräsidium Dresden konnte bundesweit als eine der ersten Aufsichtsbehörden die Registerumstellung bereits im August 2001 abschließen.

Der Wegfall der Meldepflicht wurde allerdings nicht überall positiv aufgenommen. So betrachteten einige Unternehmen aus dem Bereich der Datenträger- und Aktenvernichtung die bisherige Meldung bei der Aufsichtsbehörde offensichtlich als werbewirksames Gütesiegel. Dementsprechend gingen bei der Aufsichtsbehörde Anfragen ein, ob ein „freiwilliger Verbleib“ im Verfahrensregister möglich wäre. Da dies vom Gesetzgeber jedoch nicht vorgesehen ist, mussten die Anfragen ablehnend beantwortet werden.

Folgende Übersicht gibt Aufschluss über die Anzahl der vor bzw. nach der Registerumstellung in den Regierungspräsidien gemeldeten Unternehmen im Verfahrensregister:

	Vor Registerumstellung (Stichtag 22.05.01)	**Nach Registerumstellung (Stichtag 31.12.02)**	**Bemerkungen**
RP Chemnitz:	**83**	**5**	
davon :			
- Wirtschaftsauskunfteien	6	5	- Wegfall von einer Wirtschaftsauskunftei wegen Geschäftsaufgabe
- Markt- und Meinungsforschungsunternehmen	1	0	- Wegfall wegen Geschäftsaufgabe
- Auftragsdatenverarbeiter	76	0	- Wegfall der Meldepflicht
RP Dresden:	**71**	**6**	
davon :			
- Wirtschaftsauskunfteien	4	4	
- Markt- und Meinungsforschungsunternehmen	0	1	
- Auftragsdatenverarbeiter	67	0	- Wegfall der Meldepflicht
- Warndateibetreiber	0	1	
RP Leipzig:	**67**	**12**	
davon :			
- Wirtschaftsauskunfteien	6	3	
- Markt- und Meinungsforschungsunternehmen	8	5	
- Auftragsdatenverarbeiter	51	0	- Wegfall der Meldepflicht
- Adress- bzw. Datenhändler	2	4	
Sachsen gesamt:	**221**	**23**	

Die erhebliche Verkleinerung des Verfahrensregisters entspricht dem bundesweiten Trend und ist eine logische Folge des Wegfalls der Meldepflicht für die sogenannten Auftragsdatenverarbeiter, die vorher regelmäßig den größten Anteil an den Registereintragungen hatten.

Darüber hinaus ist aber auch davon auszugehen, dass gerade im Bereich der Markt- und Meinungsforschung einige Unternehmen bislang ihrer Meldepflicht nicht nachgekommen sind. Die Regierungspräsidien werden sich daher zukünftig verstärkt dieser Problematik widmen.

Die bei den Datenschutz-Aufsichtsbehörden geführten Verfahrensregister sind in dem in § 38 Abs. 2 BDSG beschriebenen Umfang öffentlich und können folglich von jedem eingesehen werden, wobei sich das Einsichtsrecht jedoch nicht auf die Angaben nach § 4 e Satz 1 Nr. 9 BDSG (Datensicherungsmaßnahmen/Sicherheitskonzept) sowie auf die Angabe der zugriffsberechtigten Personen erstreckt. Diesbezügliche Einsichts- bzw. Auskunftsbegehren wurden innerhalb des Berichtszeitraums in drei Fällen an die Regierungspräsidien herangetragen.

4 Kontrolltätigkeit der Regierungspräsidien

4.1 Rechtsgrundlage

„Die Aufsichtsbehörde kontrolliert die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln, einschließlich des Rechts der Mitgliedstaaten in den Fällen des § 1 Abs. 5.“ (§ 38 Abs. 1 Satz 1 BDSG – Anmerkung: anders als das SächsDSG unterscheidet das BDSG terminologisch zwischen Verarbeitung und Nutzung personenbezogener Daten).

Diese seit der Novellierung des BDSG geltende Regelung bedeutet, dass den Aufsichtsbehörden nun eine *generelle anlassunabhängige Kontrolle* obliegt. Eine Dauer- bzw. Initiativkontrolle mit anlassunabhängigen Überprüfungen war vom Gesetzgeber bislang nur für bestimmte Bereiche vorgesehen - für Auskunfteien, Adress-Handelsunternehmen, Markt- und Meinungsforschungsinstitute, Service-Rechenzentren und sonstige Auftragsdatenverarbeiter gemäß § 38 Abs. 2 BDSG a.F. sowie für Tele- und Mediendiensteanbieter gemäß Teledienste-Datenschutzgesetz und Mediendienste-Staatsvertrag. In allen anderen Bereichen oblag den Behörden nur eine Anlassaufsicht, so dass sie Prüfungen lediglich vornehmen konnten, wenn

Beschwerden oder sonstige konkrete Anhaltspunkte für Datenschutzverstöße vorlagen (§ 38 Abs. 1 BDSG a.F).

Seit der BDSG-Novellierung im Mai 2001 sind nun also bei allen nicht-öffentlichen Stellen *neben Anlass- auch Regelkontrollen* möglich.

4.2 Regelkontrolle

4.2.1 Überblick

Bei der Regelkontrolle braucht gegenüber der Anlasskontrolle *kein* Anhaltspunkt für eine Datenschutzverletzung vorzuliegen. Eine Regelkontrolle ist außerdem im Allgemeinen wesentlich breiter als eine Anlasskontrolle angelegt. Es bleibt der Entscheidung der Aufsichtsbehörde vorbehalten, ob sie bei einer Regelkontrolle die Datenverarbeitung eines Unternehmens *insgesamt* einer Prüfung unterzieht oder sich dabei auf ausgewählte *Teilaspekte* konzentriert.

Der Regelkontrolle liegen im Wesentlichen folgende variable Elemente zu Grunde:

- der Kontrollbereich (Branchen- bzw. Unternehmensauswahl),
- der Kontrollumfang (Prüfgegenstand),
- die Kontrolltiefe (Intensität der Kontrolle),
- das Kontrollverfahren (Ressourcen-Einsatz, Prüftechnik).

Zu den Mitteln der Kontrolle zählen insbesondere:

- Aufsichtsgespräche (Großunternehmen, Fachverbände),
- Grundprüfungen (branchenübergreifende datenschutzrechtliche Regelungen),
- Schwerpunktprüfungen (Teilbereiche der Datenverarbeitung),
- Vollprüfungen (z. B. bei meldepflichtigen Unternehmen),
- Vergleichsprüfungen (innerhalb einer Branche),
- Automatisierte Prüfungen (Internet),
- Koordinierte Datenschutzkontrollen (parallele oder gemeinsame Prüftätigkeit verschiedener Aufsichtsbehörden).

Im Berichtszeitraum wurden insbesondere Schwerpunktprüfungen, Vollprüfungen, Vergleichsprüfungen, automatisierte Prüfungen sowie koordinierte Datenschutzkontrollen durchgeführt.

Die folgende Übersicht gibt Aufschluss über die durchgeführten Regelüberprüfungen nach Schwerpunktbranchen und verdeutlicht zugleich die Entwicklung seit 1998:

Branchen	1998	1999	2000	**2001**	**2002**	**gesamt 2001-2002**
Auskunfteien	1	3	0	**0**	**0**	0
Markt-/Meinungsforschung	0	0	0	**0**	**1**	1
Auftragsdatenverarbeiter	16	26	27	**9**	**1**	10
Sparkassen/Banken	0	0	0	**30**	**0**	30
Verkehrsunternehmen	0	0	0	**1**	**56**	57
Versorgungsunternehmen	0	0	0	**1**	**3**	4
Sonstige	0	0	0	**0**	**2**	2
gesamt:	17	29	27	**41**	**63**	**104**

Die ersten beiden Zeilen betreffen die sowohl nach altem als auch nach neuem BDSG meldepflichtigen Branchen: Handels- und Wirtschaftsauskunfteien sowie Markt- und Meinungsforschungsunternehmen.

Unternehmen, die personenbezogene Daten im Auftrag als Dienstleistungsunternehmen verarbeiten (Auftragsdatenverarbeiter), waren nur nach dem alten BDSG meldepflichtig. Die für das Jahr 2001 angegebene Zahl beinhaltet insoweit ausschließlich nach altem Recht, d. h., bis 22. Mai 2001 durchgeführte Regelüberprüfungen. Branchenmäßig teilen sich die im Berichtszeitraum bei *Auftragsdatenverarbeitern* durchgeführten Prüfungen folgendermaßen auf:

- 2 Rechenzentren,
- 1 Aktenvernichtungsunternehmen,

- 1 Datenträgervernichtungsunternehmen,
- 1 Letter-Shop,
- 5 Telefon-Marketingunternehmen (davon 1 in 2002).

Die Zeilen 4 bis 7 betreffen *Unternehmen ohne Meldepflicht*; hier haben die Regierungspräsidien von ihrer durch die BDSG-Novellierung erweiterten Kontrollbefugnis Gebrauch gemacht. Konkret handelt es sich dabei um

- 2 Gastronomieunternehmen (Schwerpunktprüfungen hier: Videoüberwachung). Diese Kontrollen waren bei Redaktionsschluss noch nicht abgeschlossen. Es handelt sich dabei um die Betreiber von Gewölberestaurants. Deren Gasträume sind durch das August-Hochwasser stark in Mitleidenschaft gezogen worden, so dass die Kontrolle bis auf Weiteres ausgesetzt worden ist. Eine Wiederaufnahme/Fortführung wurde für das zweite Halbjahr 2003 vorgesehen.
- 30 Banken bzw. Sparkassen (Vergleichsprüfungen, vgl. 4.2.2),
- 1 Taxigenossenschaft (Vollprüfung),
- 57 Bus- bzw. Straßenbahnunternehmen (koordinierte Datenschutzkontrolle, vgl. 4.2.3),
- 3 Versorgungsunternehmen (automatisierte Prüfungen, vgl. 4.2.4).

Zum größten Teil wurden die Kontrollen im *schriftlichen Verfahren* durchgeführt. Der Grund dafür liegt in erster Linie in den neuen Prüfbefugnissen der Aufsichtsbehörden (anlassfrei bzw. unabhängig von der Meldepflicht) und der damit verbundenen Vergrößerung der Anzahl der zu kontrollierenden Unternehmen. Wird das schriftliche Verfahren so angelegt, dass eine ganze Branche stichprobenartig nach einheitlichen Kriterien geprüft werden kann, reduziert dies den Prüfaufwand hinsichtlich Vorbereitung, Durchführung und Auswertung in erheblichem Maße und versetzt die Aufsichtsbehörden so in die Lage, mit dem gleichen Personalaufwand eine wesentlich größere Breitenwirkung zu erzielen.

Soweit erforderlich, sind die schriftlichen Kontrollen durch örtliche Kontrollen ergänzt worden. Dies war insbesondere dann der Fall, wenn es den Rückläufen an Aussagefähigkeit gemangelt hatte oder aber wenn grundlegend fehlerhafte Bewertungen getroffen worden waren.

In geringem Maße wurden auch automatisierte Kontrollen durchgeführt.

Die Reaktionen der überprüften Unternehmen auf die Prüftätigkeit der Aufsichtsbehörden waren konstruktiv. Den Empfehlungen/Beanstandungen der Aufsichtsbehörde ist im Wesentlichen durch entsprechende Maßnahmen Rechnung getragen worden. Anordnungen gem. § 38 Abs. 5 BDSG waren demzufolge nicht erforderlich.

4.2.2 Videoüberwachung von Geldautomaten

Ausgehend von einem konkreten Beschwerdefall – es wurde die Videoaufzeichnung der PIN-Eingabe am Geldautomaten vermutet - sind im Herbst 2001 im Regierungsbezirk Dresden alle Sparkassen, Volks- und Raiffeisenbanken sowie Privatbanken mit eigenen Geldautomaten, insgesamt 30 zzgl. des Beschwerdefalles, einer datenschutzrechtlichen Vergleichskontrolle unterzogen worden. Ziel der Kontrolle war die Feststellung, ob und inwieweit sich aus den im novellierten BDSG erstmals enthaltenen Regelungen zur Videoüberwachung entsprechender Handlungsbedarf für die Betreiber der Geldautomaten ergibt.
Um eine möglichst große Breitenwirkung bei vertretbarem Aufwand zu erzielen, wurde die Form der schriftlichen Vergleichskontrolle gewählt. Alle Stellen erhielten mit einem im Wesentlichen gleichlautenden Anschreiben einen 11 Punkte umfassenden Fragekatalog mit der Bitte, diesen innerhalb von vier Wochen zu beantworten. Inhaltlich ging es daher *nicht* um die flächendeckend praktizierte Raumüberwachung, vielmehr erfolgte eine *Beschränkung auf die in die Geldautomaten integrierte, durch den Kunden kaum erkennbare Videoüberwachungstechnik (Porträt- und Geldfachkameras)*.

Die wesentlichen Ergebnisse der Überprüfungen lassen sich wie folgt zusammenfassen:

- Die mit den Porträt- und Geldfachkameras praktizierte Videoüberwachung dient dem berechtigten Interesse der Geldautomatenbetreiber (z. B. Beweissicherung bei Kartenmissbrauch) und ist vom Grundsatz her zulässig. Bei entsprechender Ausgestaltung des Verfahrens stehen dem keine (überwiegenden) schutzwürdigen Betroffeneninteressen entgegen.

- Im Gegensatz zu den Raumüberwachungskameras sind die Geldfach- und Porträtkameras nicht ohne Weiteres erkennbar, so dass ein expliziter Hinweis auf die Aufzeichnung mit diesen Kameras erforderlich ist. Der Hinweis „*Dieser Raum ist videoüberwacht“* ist insoweit nicht ausreichend. Ergänzend muss mindestens darüber informiert

werden, dass auch „*bei der Bedienung der Automaten Bilder aufgezeichnet werden“*.

- Die der schnellen Auswertung sowie der eindeutigen Zuordnung dienende Verknüpfung der Videoaufnahmen mit den dazugehörigen Transaktionsdaten steht zwar unter Umständen (Art und Umfang der Daten) zu dem im BDSG programmatisch enthaltenen Grundsatz der Datenvermeidung und Datensparsamkeit in Konflikt, begegnet jedoch letztendlich keinen gravierenden datenschutzrechtlichen Bedenken.

- Die im Rahmen der Kontrolle ermittelte Regelfrist (90 Tage) für die Löschung der Videoaufzeichnungen orientiert sich an der Erforderlichkeit der Datenspeicherung und ist daher nicht zu beanstanden.

- Die in § 6 b Abs. 4 BDSG geforderte Benachrichtigung der Betroffenen gilt zwar vom Grundsatz her schon bei der Verknüpfung der Aufzeichnungen mit den Transaktionsdaten, kann aber durch entsprechende inhaltliche Ausgestaltung der Hinweise auf die Videoüberwachung weitgehend aufgehoben werden.

- Für die Videoüberwachung ist ein schriftliches Sicherheits- bzw. Einsatzkonzept erforderlich, welches den Einsatz der Überwachungsanlage detailliert beschreibt und regelt und darüber hinaus auch die notwendigen technischen und organisatorischen Maßnahmen enthält. Eine detaillierte Überprüfung/Bewertung der einzelnen Maßnahmen, insbesondere im technischen Bereich, hätte einerseits den Rahmen der Kontrolle gesprengt, andererseits sind zu treffende Maßnahmen auch stark von den örtlichen Gegebenheiten abhängig. Eine effektive und sinnvolle Kontrolle kann insoweit nur vor Ort erfolgen. Dies war aber bei dieser Aktion von vornherein nicht beabsichtigt, auch haben sich im Rahmen der Überprüfung keine Anhaltspunkte für die Notwendigkeit einer örtlichen Kontrolle im Einzelfall ergeben.

- Insgesamt ist festzustellen, dass ca. 60 % aller Kreditinstitute (im Regierungsbezirk Dresden) auch Porträt- und Geldfachkameras einsetzen, dabei 100 % aller Sparkassen. Bezogen auf die Gesamtheit aller vorhandenen Geldautomaten ist dessen ungeachtet davon auszugehen, dass der Ausstattungsgrad noch unter 50 % liegt.

- Die Beantwortung der Auskunftsersuchen der Aufsichtsbehörden erfolgte zumindest bei den (lediglich regional tätigen) Sparkassen sowie den Volks- und Raiffeisenban-

ken ohne Probleme und im Wesentlichen auch fristgemäß. Bei den Privatbanken musste allerdings in 5 von 13 Fällen die Beantwortung wegen erheblicher Fristüberschreitung angemahnt werden. Dies war in erster Linie auf Probleme bei der internen Weiterleitung der Schreiben an die zuständige Stelle bzw. den Datenschutzbeauftragten der betroffenen Banken zurückzuführen.

Eine ausführliche Auswertung ist von der Web-Seite des Regierungspräsidiums Dresden (http://www.rp-dresden.de) abrufbar.

4.2.3 Koordinierte Datenschutzkontrolle von Verkehrsunternehmen

In Abstimmung mit dem Sächsischen Staatsministerium des Innern haben die drei Regierungspräsidien - federführend war insoweit das RP Dresden - im Laufe des Jahres 2002 insgesamt *56 Verkehrsunternehmen* einer schriftlichen datenschutzrechtlichen Kontrolle ausgewählter Datenverarbeitungsbereiche unterzogen. Je nach Erfordernis erfolgte zudem eine Vor-Ort-Kontrolle.

Neben *allgemeinen datenschutzrechtlichen Anforderungen* (z. B. betrieblicher Datenschutzbeauftragter, Verpflichtung auf das Datengeheimnis, öffentliches Verfahrensverzeichnis) wurden insbesondere Fragen der Verarbeitung von *Schwarzfahrerdaten* sowie Aspekte der *Videoüberwachung* (Fahrzeuge, Haltestellen) in die Kontrolle einbezogen.

Bezüglich des Prüfpunktes *„Allgemeine datenschutzrechtliche Anforderungen“* wurden mehrfach die folgenden Verstöße festgestellt:

- **Entgegen der gesetzlichen Pflicht war kein *betrieblicher Datenschutzbeauftragter* bestellt.**
  Auffällig war vor allem, dass in zahlreichen Unternehmen nicht bekannt war, was sich hinter dem Begriff „Personenbezogene Daten“ verbirgt und an welchen Stellen in den Unternehmen überall personenbezogene Daten verarbeitet werden. Bei den durchgeführten Vor-Ort-Kontrollen zeigten sich die Geschäftsführer oftmals überrascht, an wie vielen Stellen dies in ihrem Unternehmen der Fall war.

Bei den größeren Verkehrsunternehmen, insbesondere bei den in den Verkehrsverbünden als Partner fungierenden Unternehmen, kann im Regelfall davon ausgegangen werden, dass ein betrieblicher Datenschutzbeauftragter zu bestellen ist. Eine Ausnahme bilden insoweit möglicherweise die sogenannten Managementgesellschaften (ohne eigenes Fahrpersonal). Nur bei den kleineren Unternehmen, die oftmals lediglich als Subauftragnehmer eines Verkehrsverbundpartners am Markt agieren, wird häufiger die Konstellation zu erwarten sein, dass ein Datenschutzbeauftragter wegen zu geringer zu berücksichtigender Beschäftigtenzahl nicht bestellt werden muss.

- **Es war kein *öffentliches Verfahrensverzeichnis* vorhanden.**
  Den einzelnen Verkehrsunternehmen weitgehend unbekannt waren die nach dem BDSG zu erstellenden Verzeichnisse. Dies gilt nicht nur für die im BDSG 2001 neu beschriebenen Verzeichnisse, sondern ebenso für das bereits nach § 37 Abs. 2 BDSG 90 vorgeschriebene Dateiregister. Für *Verkehrsunternehmen* in erster Linie relevant sind das *öffentliche Verfahrensverzeichnis* sowie die *interne Verarbeitungsübersicht*.

  - Öffentliches Verfahrensverzeichnis:
  Der Datenschutzbeauftragte (alternativ: das Unternehmen) hat die Angaben nach § 4 e Satz 1 Nr. 1-8 BDSG auf Antrag jedermann in geeigneter Weise verfügbar zu machen. Ziel dieser Regelung ist es, jedermann das Recht zu gewähren, auf Antrag und ohne großen Aufwand an klar definierte Informationen über das Unternehmen, dessen Verantwortliche sowie dessen Verfahren zur automatisierten Verarbeitung personenbezogener Daten zu gelangen.

  - Interne Verarbeitungsübersicht:
  Dem Datenschutzbeauftragten ist eine Übersicht über die in § 4 e Satz 1 BDSG genannten Angaben sowie über die zugriffsberechtigten Personen zur Verfügung zu stellen. Diese Dokumentation ist ein wesentliches Kontrollinstrument des betrieblichen Datenschutzbeauftragten, d.h. auf dessen Basis realisiert er seine Überwachungsaufgaben hinsichtlich der ordnungsgemäßen Anwendung von Datenverarbeitungsprogrammen, prüft er, ob eine Vorabkontrolle erforderlich ist, und erstellt und aktualisiert er das öffentliche Verfahrensverzeichnis. Ist kein Da-

tenschutzbeauftragter zu bestellen, entfällt die Pflicht zur Bereitstellung einer internen Verarbeitungsübersicht.

- Umsetzungsfristen

Hinsichtlich der Erstellung bzw. Bereithaltung der internen Verarbeitungsübersicht sowie des öffentlichen Verfahrensverzeichnisses gilt die dreijährige Umsetzungsfrist des § 45 BDSG, d.h. spätestens zum 22.05.2004 müssen die genannten Übersichten verfügbar sein. Dies gilt allerdings nicht für Verfahren, die erst nach dem 22.05.2001 neu eingeführt worden sind - hier sind die entsprechenden Verzeichnisse bereits jetzt vorzuhalten.

- **Die Mitarbeiter waren nicht auf das *Datengeheimnis* verpflichtet.**

  Zunächst ist festzustellen, dass die Verpflichtung auf das Datengeheimnis nur dann relevant ist, wenn infolge der Verarbeitung *personenbezogener Daten* das BDSG zur Anwendung kommt. In einigen Fällen berief man sich insoweit auf die im Arbeitsvertrag festgehaltene *allgemeine Verschwiegenheitspflicht*, die sich jedoch in aller Regel auf die sogenannten Betriebs- und Geschäftsgeheimnisse - wozu allerdings auch personenbezogene Daten gehören können - bezieht. Darüber hinaus erstreckt sich das Datengeheimnis aber insgesamt auf die Datenerhebung, -verarbeitung und -nutzung und besitzt damit eine wesentlich größere Reichweite als die Geheimhaltungspflicht. Es schließt zum Beispiel auch aus, dass tätigkeitsbedingt zugängliche Daten zweckfremd für persönliche Angelegenheiten genutzt werden, was insoweit keine Verletzung der Verschwiegenheitspflicht bedeuten muss. Auch wenn § 5 BDSG keine schriftliche Verpflichtung fordert, ist jeder Unternehmer gut beraten, wenn er entsprechende Verpflichtungserklärungen verwendet. Dies erleichtert einerseits den gegebenenfalls gegenüber der Aufsichtsbehörde erforderlichen Nachweis der vorgenommenen Verpflichtung, andererseits sichert sich der Unternehmer damit gegenüber individuellem Fehlverhalten seiner Mitarbeiter entsprechend ab.

  Geeignete Verpflichtungserklärungen sind z. B. zu finden unter
  http://www.rp-dresden.de/service/formulare/1/14/par5_3.pdf

Die Überprüfung der *Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Fahrgästen ohne gültigen Fahrausweis* („Schwarzfahrer“) hat gleichfalls eine Vielzahl von

Mängeln offenbart. Um sowohl den kontrollierten Verkehrsgesellschaften als auch den nicht in die Kontrolle einbezogenen Unternehmen die Auslegung der datenschutzrechtlichen Vorschriften zu erleichtern und eine weitgehende Vereinheitlichung der Verarbeitungspraxis zu erreichen, wurden eine Reihe von Grundsätzen erarbeitet, die sich wie folgt zusammenfassen lassen:

- **Datenschutzrechtliche Einordnung**

  In der Frage der Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Fahrgästen ohne gültigen Fahrausweis ist nach den verfolgten Zwekken zu unterscheiden. Soweit das erhöhte Beförderungsentgelt (EBE) nicht sofort bar bezahlt worden ist, wird man sich hinsichtlich des Inkassos der EBE-Forderung auf § 28 Abs. 1 Nr. 1 BDSG (Beförderungsvertrag) berufen können. Für eine darüber hinausgehende Datenspeicherung mit dem Ziel der Erkennung von Wiederholungstätern und der Erstattung von Strafanzeigen hingegen ergibt sich die Zulässigkeit statt dessen aus § 28 Abs. 1 Nr. 2 BDSG ergeben.

- **Hinweispflichten der Verkehrsunternehmen**

  Im Ergebnis der Kontrollen war zum einen festzustellen, dass häufig Fremdunternehmen mit der Fahrausweiskontrolle beauftragt werden, zum anderen ist die für die EBE-DV verantwortliche Stelle nicht in jedem Fall mit dem die Beförderungsleistung bereitstellenden Unternehmen identisch. Für die Betroffenen ist die verantwortliche Stelle nicht immer gleich erkennbar. Darüber hinaus differieren auch die *Zwecke* der Datenerhebung, -verarbeitung und -nutzung und ggf. kommen auch Übermittlungen in Frage. Deshalb kommt den Hinweispflichten besondere Bedeutung zu.

  Werden im Rahmen der Fahrausweiskontrolle Fahrgäste ohne gültigen Fahrausweis angetroffen, sind diese bei der nachfolgenden Datenerhebung auf geeignete Weise über

  - die *Identität* des Verkehrsunternehmens,
  - die *Zweckbestimmungen* der Datenerhebung, -verarbeitung oder -nutzung und
  - die *Kategorien von Empfängern* (nur, soweit der Betroffene nach den Umständen des Einzelfalls nicht mit der Übermittlung an diese rechnen muss),

  zu unterrichten.

Aus Sicht der Aufsichtsbehörde sind diese Hinweispflichten am besten durch *Erhebungsvordrucke* mit mindestens einem Durchschlag zu realisieren, da der Betroffene dann zugleich einen Beleg über die von ihm erhobenen Daten hat.

- **Art der von Fahrgästen ohne gültigen Fahrschein erhobenen Daten**

Folgende Angaben sind für das EBE-Inkasso erforderlich und dürfen somit für diesen Zweck erhoben, verarbeitet und genutzt werden:

- Name, Vorname
- Anschrift
- Geburtsdatum
- Tatsache der Überprüfung anhand eines zu bezeichnenden Ausweisdokumentes
- Name, Anschrift der Erziehungsberechtigten (bei Minderjährigen)
- Daten zum Vorkommnis (z.B. Datum, Uhrzeit, Linie/Haltestelle, Art des Verstoßes)
- lfd. Nummer
- Kontrolleur

Ist über das EBE-Inkasso hinaus auch die Ermittlung von Mehrfachtätern beabsichtigt, so ist dies in erster Linie eine Frage der Lösch- bzw. Aufbewahrungsfristen, d. h. zusätzliche Daten sind dafür nicht erforderlich.

- **Aufbewahrungs- bzw. Löschfristen**

Durch geeignete organisatorische Maßnahmen ist sicherzustellen, dass die EBE-Unterlagen bzw. die betreffenden Datensätze, insbesondere auch die Erhebungsformulare nach Erledigung der Forderung (Zahlungseingang bzw. Einstellung/Stornierung) umgehend gelöscht bzw. vernichtet und nur die finanztechnisch erforderlichen Belege (Zahlungsaufforderung, Zahlungsnachweis) aufbewahrt werden.

Anders ist die Sachlage zu betrachten, wenn auch Strafanzeige gegen die Betroffenen gestellt werden soll. Da dies generell nur bei Wiederholungstätern praktiziert wird, müssen Betroffene zunächst als solche identifiziert werden. Angesichts der insoweit

bestehenden Verjährungsfristen wird hierfür eine Speicherdauer von maximal drei Jahren als zulässig erachtet.

- **Verfahrensweise bei Minderjährigen**

  Bei Kindern/Jugendlichen, die nicht im Besitz eines gültigen Fahrausweises angetroffen werden, ist hinsichtlich der Zulässigkeit der Datenspeicherung das Alter der Betroffenen zu berücksichtigen.

  Von Kindern unter 6 Jahren werden grundsätzlich keine Daten erhoben, da diese gemäß den Tarifbestimmungen der Verkehrsverbünde kostenlos zu befördern sind.

  Für die Altersgruppe bis 14 Jahre ist die Speicherung zum Zweck der Erhebung des EBE nicht zulässig. Möglich ist die Information der Eltern durch die Verkehrsunternehmen.

  Bei Jugendlichen ab 14 Jahren ist darüber hinaus und davon unabhängig von der Zulässigkeit der Datenspeicherung auszugehen, wenn diese zwecks Erkennung von Wiederholungstätern/Strafanzeige erfolgt.

- **Verfahrensweise bei „Graufahrern“**

  „Graufahrer“ sind Fahrgäste, die zwar eine gültige (übertragbare) Zeitkarte besitzen, diese aber zum Zeitpunkt der Kontrolle nicht vorweisen können, oder auch Fahrgäste, die den räumlichen Geltungsbereich ihrer Zeitkarte überschritten haben.

  Hinsichtlich der Erhebung, Verarbeitung und Nutzung der Daten von „Graufahrern“ ist zunächst grundsätzlich auf die Ausführungen zur Verfahrensweise bei den klassischen „Schwarzfahrern“ zu verweisen. Maßgebliche Unterschiede bestehen in erster Linie in der Höhe des EBE - dies stellt jedoch kein Datenschutzproblem dar - sowie gegebenenfalls im Verzicht auf die weitere Speicherung zum Zwecke der Ermittlung von Wiederholungstätern, die im Ermessen des Verkehrsunternehmens liegt.

- **Datenschutzrechtliche Einordnung von externen Kontrolleuren**
  Bezüglich der Verpflichtung externer Stellen zur Fahrausweiskontrolle ist davon auszugehen, dass es sich um eine Form der Auftragsdatenverarbeitung handelt. Die Auftragserteilung richtet sich nach den Vorgaben des § 11 BDSG.

- **Videoüberwachung**
  Bezüglich des letzten Kontrollpunktes *„Videoüberwachung von Fahrzeugen und Haltestellen"* war festzustellen, dass derartige Verfahren insgesamt noch wenig verbreitet sind. Dies hat seine Ursache vor allem in den hohen Kosten, der unzuverlässigen Technik (z. B. Kälteempfindlichkeit) sowie der schlechten Aufzeichnungsqualität (mangelnde Identifizierbarkeit von Personen).

Die Verkehrsunternehmen, bei denen nach Auswertung der Kontrolle Mängel vorlagen, wurden aufgefordert, diese innerhalb einer bestimmten Frist zu beseitigen. Die bereits vorliegenden Rückläufe lassen erkennen, dass den Empfehlungen/Forderungen der Aufsichtsbehörden durch die Verkehrsunternehmen gefolgt worden ist. Abschließend kann festgestellt werden, dass die koordinierte Datenschutzkontrolle insgesamt erfolgreich und konstruktiv verlaufen ist und zu einer spürbar verbesserten Umsetzung der datenschutzrechtlichen Regelungen in den kontrollierten Unternehmen geführt hat.

Eine ausführliche Auswertung ist von der o. g. Website des RP Dresden abrufbar.

4.2.4 Online-Prüfung von Versorgungsunternehmen

Zum Ende des Berichtszeitraumes hat das Regierungspräsidium Dresden eine weitere Kontrollaktion begonnen. Ausgewählt worden ist die Branche der Energieversorgungsunternehmen; inhaltlich geht es um die *datenschutzgerechte Gestaltung ihrer Webpräsenzen*.
Das Regierungspräsidium Dresden setzt hierfür ein Prüftool ein, welches es ermöglicht, auch große und komplexe Internet-Angebote vollständig zu analysieren. Dazu werden die Seiten des Angebots einer *automatischen Prüfung* auf eine Vielzahl von datenschutzrelevanten Anforderungen (BDSG, TDG/TDDSG, MDStV) unterzogen. Die Ergebnisse werden anschließend durch einen Mitarbeiter bewertet und gegebenenfalls durch weitere Recherchen ergänzt. Im Gegensatz zu allen anderen Prüfverfahren liegt damit das Prüfergebnis bei der ersten Kontaktaufnahme mit den kontrollierten Unternehmen bereits vor.

Die Kontrolle erstreckt sich in diesem Zusammenhang auf folgende Sachverhalte:

- Anbieterkennzeichnung,
- Datenschutz-Unterrichtung,
- Verwendung von Cookies (Unterrichtung),
- Einsatz von Weitervermittlungstechniken (Links, automatisch geladene Elemente anderer Anbieter, Weiterleitung von der Startseite, Anzeige der Weitervermittlung),
- Veröffentlichung personenbezogener Daten,
- Erhebung personenbezogener Daten mittels Formular (Verschlüsselung),
- Protokollierung von Nutzungsdaten.

Darüber hinaus und davon unabhängig wird auch diese Kontrolle auf allgemeine datenschutzrechtliche Aspekte ausgedehnt, d. h., zusätzlich in die Prüfung einbezogen wird die Umsetzung der gesetzlichen Forderungen

- zum betrieblichen Datenschutzbeauftragten,
- zur Verpflichtung auf das Datengeheimnis,
- zum öffentlichen Verfahrensverzeichnis.

Im Rahmen dieser Kontrollaktion sollen insgesamt 15 Unternehmen geprüft werden. Bis zum 31.12.2002 sind bereits drei derartige Prüfungen durchgeführt worden. Eine ausführliche Auswertung wird nach Abschluss aller vorgesehenen Prüfungen vorgenommen.

4.3 Anlasskontrolle

4.3.1 Überblick

Anlasskontrollen werden dann durchgeführt, wenn der Aufsichtsbehörde Anhaltspunkte für eine Datenschutzverletzung vorliegen. Derartige Anhaltspunkte können sich außer aus Beschwerden Betroffener z. B. auch aus Pressemeldungen, Hinweisen anderer Personen, Prüfungsergebnissen anderer Unternehmen (der gleichen Branche) oder u. U. selbst aus anonymen Hinweisen ergeben.

Meist handelt es sich bei den Vorgängen zunächst um die Klärung von Rechtsfragen, wie etwa die Zulässigkeit einer Datenübermittlung bzw. -nutzung. Hält die Aufsichtsbehörde die

Bearbeitung „vom Schreibtisch aus“ nicht für zweckmäßig bzw. ausreichend, wird als Kontrollinstrument die Vor-Ort-Kontrolle gewählt (z. B. bei besonderer Eilbedürftigkeit des Vorgangs oder wenn eine Prüfung vor Ort einen langwierigen Schriftwechsel zu vermeiden verspricht bzw. in den Fällen, in denen konkret das Vorhandensein bestimmter Daten vor Ort geklärt werden muss). Gleiches gilt, wenn die bekannt gewordenen Tatsachen größere Datenschutzverletzungen vermuten lassen.

Sieht man von den Fällen ab, bei denen eine eindeutige Bewertung des Sachverhalts bereits anhand der Aktenlage möglich ist, werden die betroffenen Stellen zur Sachverhaltsklärung zunächst unter Fristsetzung und Hinweis auf Ihre Auskunftspflichten (§ 38 Abs. 3 Satz 1 BDSG) zu einer Stellungnahme aufgefordert, wobei insbesondere auch eine Aufklärung über bestehende Auskunftsverweigerungsrechte erfolgt (§ 38 Abs. 3 Satz 2 BDSG).

Je nach Sachlage werden danach weitere Informationen eingeholt oder Recherchen angestellt. Den Abschluss bildet eine datenschutzrechtliche Würdigung des Sachverhalts, die sowohl das betroffene Unternehmen als auch - soweit vorhanden - der Beschwerdeführer erhalten. Fallen weitere datenschutzrechtliche Verstöße auf, so werden diese in die Würdigung einbezogen.

Die Übersicht zeigt die Entwicklung in Sachsen durchgeführter Anlasskontrollen seit 1998:

Anlässe	**Jahr**				
	1998	1999	2000	**2001**	**2002**
Eingang	36	33	44	**47**	**69**
Übernahme Vorjahr	2	0	2	**3**	**2**
Kontrollen vor Ort	6	2	6	**13**	**5**
Schriftliches Verfahren	32	31	40	**37**	**66**
Begründet	15	11	18	**21**	**29**
Abgewiesen	18	12	20	**17**	**19**
Keine Zuständigkeit	3	8	5	**10**	**17**
Noch in Bearbeitung	0	2	3	**2**	**6**

Betrafen die möglichen Datenschutzverletzungen Unternehmen außerhalb der örtlichen oder sachlichen Zuständigkeit der Regierungspräsidien, wurden die Eingaben entweder an die zu-

ständige Behörde weitergeleitet oder aber der Betroffene wurde auf den Zivilrechtsweg verwiesen.

Die weiter untersuchten Sachverhalte betrafen vielfach Banken bzw. Sparkassen sowie den Einzelhandelsbereich. Daneben waren folgende Stellen bzw. Branchen in mehr als einem Fall betroffen:

- Vermieter
- Zeitungen/Verlage
- Wirtschaftsauskunfteien
- Privatkliniken/Ärzte
- Verkehrsunternehmen
- Vereine
- Anwälte/Steuerberater
- Bauunternehmen
- Privatpersonen
- Telemarketingunternehmen
- Industrieunternehmen
- Vermögensberater
- Hotels/Gaststätten
- Hausverwaltungen
- Versicherungen

Je *einmal* betroffen waren folgende Branchen bzw. Stellen: Autohaus, Energieversorger, Flexografen, Handwerker, Internet Content Provider, Marktforscher, Vertriebsunternehmen, Wohnungsunternehmen, Wettbewerbszentrale, Wohlfahrtsverband, Wachunternehmen, Wirtschaftsberater, Zeitarbeitsfirma, sowie ein Unternehmen, welches sich mit der Teilnahme an Gewinnspielen befasst.

Die durch die Aufsichtsbehörde festgestellten Verstöße betrafen (teilweise mehrfach) im Wesentlichen folgende Sachverhalte:

- Übermittlung der Daten von Vereinsmitgliedern im Rahmen eines Gruppenversicherungsvertrages (vgl. 4.3.2),
- Übermittlung von Hotel-Buchungsdaten (vgl. 4.3.3),

- mangelnde Sorgfalt bei der Herausgabe von Unterlagen an Vereinsmitglieder (vgl. 4.3.4),
- Selbstauskünfte von Mietbewerbern (vgl. 4.3.6),
- Löschung/Sperrung der Daten ehemaliger Mieter,
- Anprangerung vermeintlicher Mietschuldner durch Aufkleber an den Wohnungstüren,
- Videoüberwachung in einem Erlebnisrestaurant (vgl. 4.3.7),
- Webcam auf einem Supermarkt-Parkplatz (vgl. 4.3.8),
- Schwarzes Brett über zahlungsunwillige Kunden im Internet (vgl. 4.3.9),
- Stempel-Muster-Kataloge mit Echtdaten (vgl. 4.3.10),
- Veröffentlichung personenbezogener Daten bei Erlöschen der Prokura (vgl. 4.3.11),
- Datenerhebung durch eine Kurklinik mittels Fragebogen (vgl. 4.3.12),
- Prüfangebote zur Nettolohnerhöhung,
- Nutzung personenbezogener Daten für Werbezwecke,
- fehlende Unterrichtung über das Widerspruchsrecht bei Werbeschreiben (vgl. 4.3.15),
- fehlende Unterrichtung in Werbeschreiben einer Bank (vgl. 4.3.16),
- Erhebung und Nutzung von Schülerdaten für Werbezwecke,
- Personalausweiskopien im Rahmen von Rabattaktionen (vgl. 4.3.17),
- Personalausweiskopien bei Eröffnung eines Wertpapierdepots,
- Personalausweiskopien bei Bankgeschäften (vgl. 4.3.18),
- nicht beeinflussbare Kontostandsanzeige an Geldautomaten (vgl. 4.3.19),
- Aufbewahrung von Belegen bei Zahlung mit EC-Karte (vgl. 4.3.20),
- Abfrage früherer Wohnsitze durch Arbeitgeber,
- Arbeitnehmerbefragungen zur Potenzialanalyse,
- Weitergabe von Bewerbungsunterlagen,
- Entsorgung von Bewerbungsunterlagen über öffentliche Papiercontainer,
- Verstöße gegen die Auskunftspflicht sowie das Löschungsgebot,
- Akten mit personenbezogenen Daten auf einem ehemaligen Betriebsgelände,
- unerlaubter Umgang mit Patientendaten durch einen Arzt,
- mangelnde Sorgfalt bei Adressrecherchen per Telefonbuch,
- unverlangte Telefonwerbung,
- unverlangte Zusendung von Werbe-SMS,
- Datenspeicherung durch eine Wirtschaftsauskunftei/Ermittlung des Bonitätsindexes
- Auskunftserteilung durch eine Wirtschaftsauskunftei,
- Warndatei für das Baugewerbe,
- Erhebung personenbezogener Daten im Beschwerdeverfahren,

- Speicherung der Daten von minderjährigen „Schwarzfahrern“,
- Veröffentlichung von E-Mails in öffentlich zugänglichen Schaukästen,
- Übermittlung von Abo-Vertragsdaten durch einen Zeitungsverlag an einen Zusteller,
- unterlassene Bestellung eines Datenschutzbeauftragten,
- Verstöße gegen die Meldepflichten gem. § 4 d BDSG

4.3.2 Datenübermittlung im Rahmen eines Gruppenversicherungsvertrages

Im Rahmen einer Presseanfrage hat die Aufsichtsbehörde Kenntnis davon erhalten, dass ein Versicherungsvertreter bei einem älteren Vereinsmitglied vorstellig geworden war und dieses bewegen wollte, einem mit dem Verein abgeschlossenen Gruppenversicherungsvertrag beizutreten. Gegenstand der Anfrage an die Aufsichtsbehörde war die Zulässigkeit dieser Vorgehensweise, insbesondere der damit verbundenen Datenweitergabe vom Verein an die Versicherung.

Die daraufhin vorgenommenen Nachforschungen ergaben, dass zwischen dem Bundesverband des Vereins und der Versicherung seit 1990 ein Gruppenversicherungsvertrag besteht. Danach erhalten die Vereinsmitglieder die Möglichkeit, als Versicherungsnehmer für sich und ihre Ehegatten Sterbegeldversicherungen sowie optional auch Unfall-Zusatzversicherungen zu günstigen Konditionen (Beitrittsalter bis 80 Jahre, keine Gesundheitsfragen) abzuschließen. Voraussetzung ist, dass mindestens 50 % des Versicherungsvolumens des betroffenen Personenkreises versichert werden kann. Der gesamte Geschäftsverkehr inkl. Beitragseinzug und -abführung wird dabei grundsätzlich zwischen dem Bundesverband und der Versicherung geführt; Versicherungsleistungen werden an den Anspruchsberechtigten gezahlt.

In Vorbereitung des Vertragsabschlusses übermitteln die Ortsverbände die Mitgliederdaten listenmäßig (Name, Anschrift, Geburtsjahr) in gewissen Abständen an die örtlich zuständigen Filialdirektionen der Versicherung. Die Benachrichtigung der Mitglieder über diese Übermittlung erfolgt mit entsprechenden Avisschreiben sowie darüber hinaus auch durch regelmäßige Informationen in den Verbandsorganen. Die Avisschreiben enthalten eine Information über das Widerspruchsrecht der Mitglieder, d. h., diese müssen der Weitergabe ihrer Daten unverzüglich beim Verein widersprechen, andernfalls werden die Daten nach einer nicht näher bezeichneten Frist weitergegeben. Speziell für Gruppenversicherungsverträge geschulte

Versicherungsmitarbeiter suchen daraufhin die Vereinsmitglieder auf und bieten ihnen den Beitritt zu dem Gruppenversicherungsvertrag an.

Nach den zwischen den Datenschutzaufsichtsbehörden und den Verbänden der Versicherungswirtschaft getroffenen Absprachen dürfen Vereine auf der Basis eines Gruppenversicherungsvertrages dem betreffenden Versicherungsunternehmen Mitgliederdaten nur unter folgenden Voraussetzungen übermitteln:

- Von **Neumitgliedern** (Mitgliedschaft erst **nach** Abschluss des Gruppenversicherungsvertrages) ist die Einwilligung zur Datenweitergabe einzuholen (z. B. im Aufnahmeantrag), wobei darüber zu informieren ist, welche Daten an welchen Versicherer weitergegeben werden.

- Bei **Altmitgliedern** (Mitgliedschaft bereits **vor** Abschluss des Gruppenversicherungsvertrages) genügt ein entsprechendes Avisschreiben, in welchem über Art und Empfänger der zu übermittelnden Daten sowie über die Widerspruchsmöglichkeit zu informieren ist. Dem Mitglied ist ausreichend Zeit für einen Widerspruch einzuräumen; darüber hinaus ist bekannt zu geben, dass andernfalls mit einem Vertreterbesuch zu rechnen ist.

Die im untersuchten Fall von dem Verein praktizierte Verfahrensweise entsprach der zweiten Alternative. Während dies für die sogenannten Altmitglieder, wie dargestellt, nicht zu beanstanden war, war der Verzicht auf eine Einwilligungslösung bei den Neumitgliedern nicht korrekt. Schutzwürdige Interessen dieser Mitglieder können dadurch beeinträchtigt werden, dass sie aktiv handeln müssen, um eine Datenweitergabe zu verhindern, obwohl sie regelmäßig darauf vertrauen dürften, dass ihre Daten nicht zu vereinsfremden Zwecken verwendet werden.

Die Aufsichtsbehörde hat die bei Neumitgliedern praktizierte Verfahrensweise gegenüber dem Landesverband bemängelt und insoweit eine Umstellung von der Widerspruchs- auf die Einwilligungslösung gefordert. Der vom Landesverband daraufhin informierte Bundesverband ist den Vorschlägen der Aufsichtsbehörde gefolgt und hat neue, bundesweit eingesetzte Aufnahmeanträge entwickelt, die folgende explizite Einwilligungserklärung enthalten:

Der <Name des Vereins> hat für seine Mitglieder einen Gruppenversicherungsvertrag abgeschlossen. Um die Vergünstigungen aus diesem Gruppenversicherungsvertrag zu erhalten, willige ich ein, dass hierfür mein Name, meine Anschrift und mein Geburtsjahr an die <Name der Versicherung> weitergegeben werden.

Die vereinfachte Verfahrensweise für Altmitglieder ist ein Zugeständnis der Aufsichtsbehörden und trägt dem Umstand Rechnung, dass es oftmals erhebliche Schwierigkeiten bereitet, nachträglich die erforderlichen Einwilligungserklärungen einzuholen. Außerdem ist davon auszugehen, dass Altmitglieder in die Entscheidungsfindung zum eventuellen Abschluss eines Gruppenversicherungsvertrages einbezogen werden (z. B. im Rahmen einer Mitgliederversammlung) und daher auf eine zweckgebundene Verwendung ihrer Daten für vereinsfremde Zwecke entsprechend vorbereitet sind, während dies bei Neumitgliedern gerade nicht der Fall ist.

4.3.3 Übermittlung von Hotel-Buchungsdaten

Ein Geschäftsmann hatte im Dezember 2001 dreimal je eine Übernachtung in einem Hotel gebucht. Im März 2002 erhielt das Hotel den Anruf einer Werbeagentur, die sich als Auftraggeberin des Geschäftsmannes ausgab und zwecks Überprüfung von Spesenabrechnungen um die Übermittlung der Buchungsdaten bat. Die drei Termine wurden noch am gleichen Tag von einer Hotelangestellten per Fax an die Werbeagentur übermittelt. In seiner Beschwerde führte nun der Betroffene aus, dass die Faxauskunft nachfolgend dazu verwendet worden sei, ihn zu erpressen. Die Werbeagentur gäbe es im Übrigen gar nicht.

Der Leiter des Hotels geht von der Zulässigkeit der Datenübermittlung aus und begründet dies mit § 28 Abs. 3 Nr. 1 BDSG. Demnach habe die (vermeintliche) Auftraggeberin des Betroffenen ein berechtigtes Interesse (Rechnungskontrolle) geltend gemacht, welches die Datenweitergabe insoweit rechtfertigen könne.

Die Aufsichtsbehörde hat diesen Erlaubnistatbestand geprüft, ist dabei allerdings zum entgegengesetzten Ergebnis gekommen. Allein das Drittinteresse ist für die Zulässigkeit der Auskunftserteilung nicht ausreichend, vielmehr ist darüber hinaus auch zu prüfen, ob möglicherweise schutzwürdige Interessen des Betroffenen einer Übermittlung entgegenstehen (§ 28 Abs. 3 letzter Halbsatz BDSG). Dies musste in diesem Fall angenommen werden.

Zunächst ist regelmäßig davon auszugehen, dass Hotelübernachtungen mit einem Beleg nachgewiesen werden können. Sind Belege nicht verfügbar, ist es Aufgabe des Betroffenen, entsprechende Bestätigungen des Hotels einzuholen. Dies ist insbesondere aus dem durch den Auftraggeber zu beachtenden Direkterhebungsgrundsatz des § 4 Abs. 2 BDSG abzuleiten. Davon abgewichen werden darf nur bei einer entsprechenden Rechtsvorschrift oder wenn die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordert. Für einen Auftrag- oder Arbeitgeber ist es jedoch kein Problem, sich die entsprechenden Informationen (Übernachtungsdaten bzw. -belege) vom Betroffenen direkt zu besorgen. Wird statt dessen eine dem Direkterhebungsgrundsatz widersprechende Datenerhebung bei Dritten – hier dem Hotel - bevorzugt, so muss das bei der übermittelnden bzw. angefragten Stelle (Hotel) dazu führen, entgegenstehende schutzwürdige Interessen des Betroffenen anzunehmen und eine Auskunftserteilung folgerichtig abzulehnen.

Darüber hinaus sind weitere Gründe für ein entgegenstehendes schutzwürdiges Betroffeneninteresse erkennbar. Zunächst sind ausschließlich telefonisch eingegangene Anfragen Dritter wegen der damit verbundenen Missbrauchsgefahr (falsche Identitäten, falsche Gründe, fehlender schriftlicher Nachweis) regelmäßig besonders restriktiv zu behandeln. Unabhängig von der Frage der Zulässigkeit der Datenabfrage ist zu berücksichtigen, dass dem Hotel als übermittelnder Stelle nicht bekannt ist, welche Buchungsdaten für den angegebenen Zweck relevant sind. Neben geschäftlichen können auch private Übernachtungen erfolgt sein, die dann jedoch gleichfalls beauskunftet würden. Üblicherweise würde also ein Auftraggeber um Bestätigung der von ihm vorgelegten Buchungsdaten bitten, nicht jedoch um Mitteilung ihm nicht bekannter Daten.

Damit ist also davon auszugehen, dass die Übermittlung rechtswidrig erfolgt ist, insbesondere lagen ausreichend Anhaltspunkte für die Annahme vor, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Auskunftserteilung hatte. Für eventuell entstandene Schäden könnten auf zivilrechtlichem Weg entsprechende Schadenersatzforderungen geltend gemacht werden; Anspruchsgrundlage wäre der § 7 BDSG: Schadenersatz.

Seitens des Hotels wurde versichert, dass zukünftig generell keine telefonischen Auskünfte über Gäste mehr erteilt werden. Darüber hinaus sollen anderweitige Anfragen nur nach Rückfrage mit dem Gast beantwortet werden.

Abschließend zu klären war noch die Identität des Datenempfängers. Dem Vernehmen nach war dem Betroffenen weder die Anruferin bekannt, noch sollte eine Werbeagentur mit dem angegebenen Namen existieren, so dass zu vermuten war, dass es sich um ein Auskunftsersuchen unter falscher Identität handelte, was wiederum die Verwirklichung eines Bußgeldtatbestandes (§ 43 Abs. 2 Nr. 4 BDSG – Erschleichen personenbezogener Daten) bzw. sogar eines Straftatbestandes (§ 44 Abs. 1 BDSG – Schädigungsabsicht) bedeuten würde.

Die Identität des Faxempfängers wurde über eine Anfrage bei der Deutschen Telekom (§ 89 Abs. 6 TKG) in Erfahrung gebracht. Dabei stellte sich heraus, dass die von der vermeintlichen Werbeagentur für die Antwort des Hotels angegebene Faxnummer an den Betroffenen selbst vergeben ist. Da nunmehr alles auf innerfamiliäre Streitigkeiten hindeutete, wurde die Angelegenheit nicht weiterverfolgt.

4.3.4 Herausgabe von Unterlagen an Vereinsmitglieder

In dem an die Aufsichtsbehörde herangetragenen Fall begehrte ein Vereinsmitglied vom Verein die Herausgabe bestimmter persönlicher Unterlagen. Nachdem der Betroffene die erhaltenen Unterlagen in Augenschein genommen hatte, stellte er fest, dass sich darin Schriftstücke befanden, die zu einem anderen Vorgang gehörten. Die der Aufsichtsbehörde übergebenen Schriftstücke enthielten zahlreiche personenbezogene Daten Dritter, darunter Angaben zu gesundheitlichen Verhältnissen.

Die Aufsichtsbehörde leitete die Schriftstücke an den Verein weiter mit der Aufforderung, zukünftig u. a. bei der Aushändigung von Unterlagen an Vereinsmitglieder oder Dritte durch geeignete organisatorische Maßnahmen sicherzustellen, dass keine personenbezogenen Daten unbefugt weitergegeben werden.

4.3.5 Kundenkarten von der Wohnungsbaugesellschaft

Gegenstand einer Bürgereingabe war ein Artikel in einer Mieterzeitung einer größeren Wohnungsbaugesellschaft. Hierin bot der Vermieter seinen Mietern sogenannte Kundenkarten an, mit denen diese bei ausgewählten Dienstleistern und Geschäften Rabatte erhalten würden. Die

Mieter sollten unaufgefordert derartige Kundenkarten zugeschickt bekommen. Es wurde mitgeteilt, dass personenbezogene Daten wie Name, Anschrift und Bankverbindung zur Herstellung der Kundenkarte an Dritte weitergereicht werden sollten. In der Mieterzeitschrift war eine vorbereitete Widerspruchserklärung abgedruckt. Es wurde darauf hingewiesen, dass das Wohnungsunternehmen bei Nichtvorliegen einer unterschriebenen Widerspruchserklärung vom Einverständnis zur Datenweitergabe und zur Herstellung der Kundenkarte ausgeht.

Diese Vorgehensweise hat die Aufsichtsbehörde datenschutzrechtlich beanstandet. Die Datenverarbeitung setzt eine Erlaubnisnorm voraus. Eine Widerspruchslösung, wie sie § 28 Abs. 4 BDSG vorsieht, war hier nicht zulässig. Durch die Aufsichtsbehörde wurde eine schriftliche Einwilligung nach § 4 a BDSG gefordert.

Folgende Lösung wurde gefunden: Im Auftrag des Wohnungsunternehmens werden Karten hergestellt, die lediglich den Namen und die Adresse enthalten. Die Karten werden mit einer umfassenden Einverständniserklärung versandt. Den Mietern wurde mitgeteilt, dass erst nach Rückübersendung der unterschriebenen Einverständniserklärung die „Aktivierung“ der Karte erfolgt.

4.3.6 Selbstauskünfte von Mietbewerbern

Regelmäßig werden Bewerbern für Mietwohnungen umfangreiche Fragebögen („Selbstauskünfte“) vorgelegt, auf deren Basis dann eine Entscheidung getroffen werden soll, ob mit den Bewerbern ein Mietverhältnis eingegangen werden kann oder nicht.

Im Berichtszeitraum hat sich die Aufsichtsbehörde in zwei Fällen mit derartigen Selbstauskunftsbögen befasst. Grundsätzlich kann zunächst Folgendes festgehalten werden:

Die Zulässigkeit der von Vermietern an Mietinteressenten ausgegebenen Fragebögen beurteilt sich nach § 28 Abs. 1 Nr. 1 Bundesdatenschutzgesetz, wonach das Erheben, Speichern und Nutzen personenbezogener Daten zulässig ist, soweit dies der Zweckbestimmung eines Vertragsverhältnisses (z. B. Mietvertrag) oder eines vertragsähnlichen Vertrauensverhältnisses (hier: Anbahnung eines Mietvertrages, d. h. Bewerberphase) dient.

Danach treffen den potentiellen Mieter Aufklärungspflichten nur für solche Umstände, die für den Vermieter bei objektiver Bewertung und Berücksichtigung schutzwürdiger Belange des Mietinteressenten der Auskunft bedürfen. Das ist bei solchen Umständen der Fall, die für das angestrebte Mietvertragsverhältnis wesentlich sind und deren Offenbarung dem Mieter zuzumuten ist. Fragen nach dem persönlichen Status des Mieters sind unzulässig, soweit sie sich nicht auf besondere Qualifikationsmerkmale beziehen, die den Mietgebrauch betreffen (Amtsgericht Wiesbaden, Wohnungswirtschaft und Mietrecht 1992, S. 597).

Das Informationsinteresse des Vermieters ergibt sich aus seinem Interesse an einem zahlungsfähigen Mieter und dient damit der Absicherung gegenüber Zahlungsausfällen. Dem entgegen steht das Interesse des Mietinteressenten, seine Privatsphäre zu schützen und nur die für ein eventuelles Mietverhältnis erforderlichen Informationen über sich preiszugeben. Diese gegenläufigen Interessen sind gegeneinander abzuwägen, wobei zu berücksichtigen ist, dass preiswerter Wohnraum knapp ist. Die Tatsache, dass auf dem Wohnungsmarkt Privatautonomie, d. h. Vertragsfreiheit, herrscht, darf jedoch nicht dazu führen, dass das Recht auf informationelle Selbstbestimmung der Mietbewerber in den Vertragsverhandlungen ignoriert bzw. ungenügend beachtet wird.

Zu ausgewählten Datenfeldern, die in Fragebögen häufig zu finden sind, wird folgende grundsätzliche Auffassung vertreten:

- **Nationalität/Staatsangehörigkeit**

Es ist in der Regel kein Grund erkennbar, durch den die Erhebung dieses Datums gerechtfertigt werden könnte. In den meisten Fällen wird man deshalb von der Rechtswidrigkeit dieser Abfrage ausgehen müssen. Insbesondere verhindert eine derartige Abfrage weder, dass ein Mieter in ausländerfeindlichen Gegenden gefährdet ist, noch werden dadurch ethnische Konflikte innerhalb eines Hauses ausgeschlossen.

- **Einkommenshöhe**

Die Frage nach dem monatlich zur Verfügung stehenden Geldbetrag (Bonität) ist datenschutzrechtlich nicht zu beanstanden, wobei jedoch nur die Gesamtsumme von Bedeutung ist. Ohne Belang ist, wie sich dieses Einkommen zusammensetzt.

- **Geburtsort**

Durch Name, Vorname, Geburtsdatum, gegenwärtige (vor Mietvertragsabschluss) und zukünftige (nach Mietvertragsabschluss) Wohnanschrift ist der Mieter für den Geschäftsverkehr im Rahmen des Mietvertrages ausreichend genau bezeichnet. Dies gilt auch für den gelegentlich von Vermietern angeführten Fall, dass eine Melderegisterauskunft erforderlich wird. Es ist selbst in größeren Wohnblocks sehr unwahrscheinlich, dass zwei oder mehr Personen bei allen fünf Angaben identische Daten aufweisen. Die Erhebung und Speicherung von Geburtsort und -name ist folglich für die Durchführung des Mietverhältnisses bzw. die Durchsetzung daraus resultierender Ansprüche nicht erforderlich und somit gem. § 28 Abs. 1 Nr. 1 BDSG auch nicht zulässig.

- **Legitimation**

Es ist nicht bekannt, inwieweit durch Mieter bei Abschluss eines Mietvertrages wissentlich falsche Daten angegeben werden. Unabhängig davon bestehen keine Einwände, wenn die Adress- und Geburtsdaten anhand eines Ausweises überprüft werden. Dies ergibt sich schon aus § 4 Abs. 1 Personalausweisgesetz (PersAuswG) bzw. § 18 Abs. 1 Passgesetz (PassG), wonach Personalausweise bzw. Pässe auch im nicht-öffentlichen Bereich als Ausweis- und Legitimationspapier benutzt werden können.
Nicht erforderlich ist jedoch die Erhebung und Speicherung der Ausweisnummer. Zum einen sind private Stellen gemäß dem PassG bzw. PersAuswG grundsätzlich nicht befugt, Auskünfte aus dem Pass- bzw. Personalausweisregister zu erlangen. Andererseits sind Ausweisnummern auch nicht für die Beantragung von Melderegisterauskünften erforderlich, da die eindeutige Identifikation bereits durch die unter dem Diskussionspunkt ‚Geburtsdatum_ erwähnten Daten sichergestellt ist. Nach den melderechtlichen Vorschriften benötigt ein Vermieter also weder Personalausweis- noch Passnummer, um - etwa zum Auffinden ehemaliger Mieter mit Mietrückständen - Auskunft über die gegenwärtige Anschrift ehemaliger Mieter zu erlangen.

- **Telefon**

Die telefonische Erreichbarkeit eines Mieters ist für die Durchführung des Mietverhältnisses allenfalls nützlich, nicht jedoch erforderlich. Mit § 28 Abs. 1 Nr. 1 BDSG (Zweckbestimmung des Mietverhältnisses) kann die Erhebung, Verarbeitung und Nutzung der Telefonnummer folglich nicht begründet werden. Darüber hinaus ist zu berücksichtigen, dass sich z. B. die private Telefonnummer in vielen Fällen allein schon durch den Umzug wieder ändert und dass Anrufe des Vermieters zu dienstlichen Anschlüssen oftmals nicht erwünscht sind. Eine für Vermieter- und Mieterinteressen gleichermaßen gerechte Lösung ist die Kennzeichnung als freiwillige Angabe.

- **Haustiere**

Wird die Haustierhaltung per Mietvertrag generell erlaubt, erübrigt sich eine derartige Frage.
In den Fällen, in denen im Mietvertrag keine Aussage zu Haustieren enthalten ist, dürfen nach einschlägiger Rechtsprechung solche Kleintiere gehalten werden, von denen weder Störungen noch Schäden ausgehen, d. h., die Haltung von Hamstern, Meerschweinchen, Fischen, Ziervögeln und Zwergkaninchen gehört zum vertragsgemäßen Gebrauch der Mietsache. Die Frage nach Haustieren wird als zulässig erachtet.

- **Musikinstrumente**

Die Frage nach vorhandenen Musikinstrumenten geht im Regelfall am eigentlichen Problem vorbei. Von Interesse sind vielmehr die Lärmgewohnheiten des Mietbewerbers, die aber mit einer derartig eingeschränkten Fragestellung nicht zufriedenstellend in Erfahrung gebracht werden können. Weit verbreitete Ursachen für Lärmstörungen sind beispielsweise auch Heimwerktätigkeiten, Schichtarbeit, lautes Musikhören etc.. Im Übrigen sind Musikinstrumente kein Kündigungsgrund und können - gerade bei jungen Familien - jederzeit nachträglich erworben werden. Soweit mit dieser Abfrage bezweckt wird, Mieter mit ähnlichen Interessen und einer damit verbundenen erhöhten Toleranzschwelle (z. B. Musikstudenten) in einzelnen Mietobjekten zu konzentrieren, so steht einer Abfrage auf freiwilliger Basis (Kennzeichnung) nichts entgegen.

4.3.7 Videoüberwachung in einem Erlebnisrestaurant

Durch einen anonymen Hinweis wurde die Aufmerksamkeit der Aufsichtsbehörde auf ein Gewölberestaurant gelenkt, welches in seinen Gasträumen sowie in einem so genannten Schminkzimmer mehrere Videokameras installiert und auch im Einsatz hat.

Die vor Ort geführten Ermittlungen ergaben, dass es sich dabei um eine reine Beobachtung handelt, d. h. Aufzeichnungsgeräte sind nicht vorhanden. Mehrere Kameras sind jedoch im Restaurant verteilt; an verschiedenen Standorten befinden sich dazugehörige Monitore. Durch die offen installierten Kameras werden ausgewählte Gänge des Restaurants, die Essensausgabe, die Bar, der ebenerdige Restaurant-Eingangsbereich bzw. die Außensitzplätze sowie das erwähnte „Schminkzimmer“ erfasst. Die Kameras sind allenfalls manuell schwenkbar und haben keine Zoomfunktion.

§ 6 b Bundesdatenschutzgesetz (BDSG) regelt die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen und erfasst auch die reine Beobachtung. Die Zulässigkeit der Videobeobachtung kann sich daher gem. § 6 b Abs. 1 Nr. 3 BDSG aus berechtigen Interessen für konkret festgelegte Zwecke ergeben, die gegenüber den schutzwürdigen Interessen der Gäste abzuwägen sind.

Als berechtigte Interessen wurden folgende Sachverhalte angeführt:

- Koordinierung des Bedien- und Künstlerpersonals angesichts verzweigter und verwinkelter Restauranträume und -gänge,
- Vermeidung unnötiger Wege des Bedienpersonals, insbesondere was die Essenausgabe und die Außensitzplätze betrifft.

Angesichts der besonderen Lage (Gewölbe) des Restaurants sowie der weit verzweigten und verwinkelten Räume können die oben angeführten Interessen zunächst durchaus als berechtigt angesehen werden. Allerdings existiert insoweit keine schriftliche Festlegung der konkret verfolgten Zwecke.

Andererseits stehen schutzwürdige Interessen der Gäste einer Videoüberwachung entgegen. Restaurants sind üblicherweise Orte, an denen sich die Besucher frei bewegen wollen und nicht einer Überwachung ausgesetzt werden wollen.

Im Regelfall wird die erforderliche Abwägung in Restaurants daher zuungunsten einer Videoüberwachung ausgehen. Die konkrete Konstellation in dem kontrollierten Restaurant wird jedoch angesichts letztlich doch eher geringer Gefährdung des Persönlichkeitsrechts (keine Aufzeichnung, Tische weitgehend außerhalb des Erfassungsbereiches, keine Fernsteuerung der Kameras) und angesichts der räumlichen Besonderheiten dennoch zur Zulässigkeit führen. In diesem Zusammenhang zu fordern war allerdings, dass die wenigen von der Videoüberwachung erfassten Sitzplätze durch eine modifizierte Kamera- oder Tischstellung aus dem Erfassungsbereich der Kameras genommen werden.

Was davon unabhängig zu bemängeln war, ist die fehlende, in § 6 b Abs. 2 BDSG zwingend geforderte Kennzeichnung der Videoüberwachung: Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen. Die offene Installation der Kameras reicht - nicht zuletzt wegen der ohnehin unübersichtlichen, mit vielen Details ausgestatteten Räume - keinesfalls aus.

Der Restaurantbetreiber wurde aufgefordert, die Videoüberwachung innerhalb des Übergangszeitraumes des § 45 BDSG, d. h. bis 22.05.2004, mit den neuen gesetzlichen Vorgaben in Übereinstimmung zu bringen.

Der „Schminkraum“ ist nur Restaurantmitarbeitern zugänglich bzw. Künstlern, die sich für einen Auftritt im Restaurant vorbereiten. § 6 b BDSG regelt jedoch die Beobachtung öffentlich zugänglicher Räume und ist daher in diesem Fall nicht einschlägig. Weil darüber hinaus auch keine Aufzeichnung mittels automatisierter Verfahren erfolgt, ist auch die alternative Bewertung auf der Grundlage des § 28 Abs. 1 Nr. 1 BDSG ausgeschlossen, d. h. das BDSG ist insgesamt nicht anwendbar. Der Betreiber konnte daher durch die Aufsichtsbehörde lediglich darauf aufmerksam gemacht werden, dass durch den Betrieb dieser Kamera eine Beeinträchtigung der Persönlichkeitsrechte der sich dort vorbereitenden Künstler bzw. auch der eigenen Mitarbeiter anzunehmen ist. Veränderungen können insoweit aber nur die Betroffenen selbst bewirken.

4.3.8 Webcam auf dem Parkplatz eines Supermarktes

Im Rahmen einer Presseanfrage erhielt die Aufsichtsbehörde Kenntnis davon, dass an einem Einkaufsmarkt eine Videokamera installiert ist, die Bilder vom Standort der Einkaufswagen auf dem Parkplatz ins Internet überträgt. „Private Scherzkekse wollten damit wohl das tägliche Trinkerleben einiger sich dort aufhaltender örtlicher Penner weltweit erlebbar machen", so die Formulierung der Presse.

Eine Webcam (Videokamera, die Bilder ins Internet überträgt) ist genau dann datenschutzrechtlich relevant, wenn Personen (oder personenbezogene Daten, z. B. Autokennzeichen) so detailliert wiedergegeben werden, dass eine Identifikation von Personen möglich ist. Diese Voraussetzung war in dem geschilderten Fall zweifelsfrei gegeben, so dass die Zulässigkeit des Betriebs der Webcam nach § 6 b BDSG zu beurteilen war.

Da die Webcam auf einem benachbarten Grundstück installiert war und insbesondere auch nicht durch den Supermarkt selbst betrieben wurde, war von den drei in § 6 b Abs. 1 BDSG angegebenen Erlaubnistatbeständen

- Wahrnehmung berechtigter Interessen für vorab festgelegte Zwecke
- Wahrnehmung des Hausrechts
- Aufgabenerfüllung öffentlicher Stellen

offensichtlich nur der zuerst genannte Erlaubnistatbestand überhaupt zu prüfen. Allerdings stellt sich dabei die Frage, ob der der Website zu entnehmende Zweck, weltweit bekannt zu machen, welche „Gestalten" sich auf dem Parkplatz – aus welchen Gründen auch immer - aufhalten, einem berechtigten Interesse dient. *(„Da isse nun, unsere Assicam, die nichts weiter zeigt als einen öffentlichen Parkplatz und den darauf zu findenden Gestalten, die nur eins im Sinne haben: Schlucken, Schlucken und nochmals Schlucken.")* Durch die Aufsichtsbehörde konnte ein solches Interesse nicht erkannt werden; die Aufforderung an den Domaininhaber, der Aufsichtsbehörde mitzuteilen, worin dessen berechtigte, d. h. von der Rechtsordnung gebilligte Interessen bestehen, ist unbeantwortet geblieben.

Selbst wenn man davon ausginge, dass solche berechtigten Interessen bestünden, dürfen nach § 6 b Abs. 1 BDSG keine Anhaltspunkte dafür vorliegen, dass schutzwürdige Interessen der Betroffenen überwiegen. Schon die Tatsache der Bezeichnung der Website als „Assicam" und

die damit verbundene gesellschaftliche Einordnung der von der Webcam erfassten Personen ist jedoch ausreichend, um überwiegende schutzwürdige Betroffeneninteressen zu bejahen. Darüber hinaus ist zu berücksichtigen, dass auch jeder Kunde des Marktes, der einen Einkaufswagen benötigt, zwangsläufig in den Erfassungsbereich der Kamera gerät. Schließlich liegt das Problem der Webcams auch noch in der weltweiten Verbreitung der Bilder und der nahezu unbegrenzten Verfügbarkeit und Weiterverwendungsmöglichkeit durch jeden Internet-Nutzer. Die Bilder können heruntergeladen und gespiegelt, d. h. im Internet vervielfältigt werden, spezielle Software ermöglicht auch Vergrößerungen. Es besteht also keine Kontrollmöglichkeit mehr über die weitere Verwendung der Bilder. Offensichtlich ist auch, dass das Löschungsgebot des § 6 b Abs. 5 BDSG nicht erfüllt werden kann.

Der Betrieb der Webcam mit dem geschilderten Erfassungsbereich ist damit nach § 6 b BDSG unzulässig und rechtswidrig. Das gleiche Resultat ergibt sich auch aus § 22 des Kunsturheberrechtsgesetzes (Recht am eigenen Bild). Insoweit ist auch der Bußgeldtatbestand des § 43 Abs. 2 Nr. 1 BDSG (unbefugte Erhebung und Übermittlung personenbezogener Daten) erfüllt.

Des Weiteren schreibt § 6 b BDSG auch eine Kennzeichnungspflicht für derartige Überwachungsmaßnahmen vor.

Die betreffende Website ist nicht mehr im Netz; gegen den Betreiber wurde ein Ordnungswidrigkeitenverfahren durchgeführt (vgl. 9 Ordnungswidrigkeiten).

4.3.9 Schwarzes Brett für zahlungsunwillige Kunden im Internet

Auch Warndateien sowie schwarze Listen sind ein „Dauerbrenner“ in der Prüfpraxis der Datenschutz-Aufsichtsbehörden. So ist die Aufsichtsbehörde im Berichtszeitraum auf die Webpräsenz eines Kleinunternehmers aufmerksam gemacht worden, der auf einer speziellen Webseite ein „Schwarzes Brett für alle zahlungsunwilligen Kunden“ eingerichtet hatte. Diese Seite nutzte er, um allen Surfern, die zufällig oder zielgerichtet diese Seite aufgerufen hatten, mitzuteilen, wer (Name, Anschrift) bei ihm bislang zwar Waren/Leistungen bezogen, dafür jedoch nicht bezahlt hatte. Soweit bekannt, waren ergänzende Informationen zum Zahlungsverhalten bzw. zur Zahlungsfähigkeit der jeweiligen Schuldner angegeben.

Grundlage der datenschutzrechtlichen Beurteilung des beschriebenen „Schwarzen Brettes“ ist § 28 BDSG, Datenerhebung, -verarbeitung und -nutzung für eigene Zwecke.

Gemäß § 28 Abs. 1 Nr. 1 BDSG ist die Datenverarbeitung zulässig, wenn dies der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen dient. Auch wenn im konkreten Fall ein Kauf- oder Dienstleistungsvertrag als Grund für die wohl bislang nicht beglichenen finanziellen Forderungen anzusehen ist, ergibt sich daraus nicht die datenschutzrechtliche Zulässigkeit der Veröffentlichung der Daten von Kunden im Falle der Zahlungsverweigerung. Zweck des abgeschlossenen Vertrages ist es also nicht, Angaben zum Vertragspartner zu veröffentlichen.

Hierfür kommen allenfalls § 28 Abs. 1 Nr. 2 BDSG (berechtigte Eigeninteressen) oder aber § 28 Abs. 3 Nr. 1 BDSG (berechtigte Fremdinteressen) in Betracht. Berechtigte Eigeninteressen erfordern keine Veröffentlichung, insoweit genügt es, wenn intern eine Liste von Kunden geführt wird, mit denen schlechte Zahlungserfahrungen gemacht worden sind. Im Fall der Annahme berechtigter Fremdinteressen (Warnfunktion) ist zunächst festzustellen, dass diese Informationen allen Besuchern der Website zugänglich gemacht werden, also unabhängig davon, ob das gesetzlich geforderte berechtigte Interesse besteht oder nicht. Darüber hinaus darf aber gem. § 28 Abs. 3 BDSG auch kein Grund zu der Annahme bestehen, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung oder Nutzung hat. Angesichts der Prangerwirkung des schwarzen Brettes sowie in Anbetracht der Tatsache, dass es sich lediglich um subjektive Angaben des Gläubigers handelt - die Zahlungsverweigerung kann ihre Ursache beispielsweise auch in Qualitäts- oder Leistungsmängeln haben - muss davon ausgegangen werden, dass die im Gesetz benannten schutzwürdigen Betroffeneninteressen bestehen und die Veröffentlichung der Daten somit unzulässig ist.

Ergänzend kann auf eine vergleichbare Entscheidung des Oberlandesgerichtes Rostock (Urteil vom 21.03.01, Az.: 2 U 55/00, RDV 2001, 285) verwiesen werden, wonach die Veröffentlichung eines Schuldnerspiegels im Internet ohne Einwilligung der Betroffenen unzulässig ist.

Der Kleinunternehmer hat auf die Beanstandung hin unverzüglich das schwarze Brett aus seiner Internetpräsentation entfernt.

4.3.10 Stempel-Musterkataloge mit Echtdaten

Der Aufsichtsbehörde ist ein auch in elektronischer Form (Internet) verteilter Stempel-Musterkatalog mit der Bitte um datenschutzrechtliche Überprüfung vorgelegt worden.

Sämtliche im Katalog enthaltenen Schriftmuster stimmten mit auftragsgemäß gefertigten Stempeln eins zu eins überein. Bezüglich der darunter befindlichen Stempel von Privatpersonen bestätigte der Firmeninhaber, dass diese weder ihre Einwilligung zur Veröffentlichung erteilt, noch überhaupt davon Kenntnis hätten. Dies würde seit Generationen so gemacht und sei im Übrigen auch absolut branchenüblich. Darüber hinaus habe er die Daten stets als offenkundig angesehen und sei sich daher eines Datenschutzverstoßes nie bewusst gewesen.

Die Aufsichtsbehörde vertritt hingegen die Auffassung, dass die Aufnahme originaler Schriftmuster in einen Werbekatalog eine unzulässige Übermittlung personenbezogener Daten darstellt. Grundlage dieser Bewertung bildet § 28 Abs. 1 Nr. 1 BDSG, wonach die Übermittlung personenbezogener Daten dann zulässig ist, wenn dies der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen dient. Der dem Sachverhalt zugrunde liegende Vertrag betrifft jedoch ganz konkret die Anfertigung eines Stempels, nicht jedoch die Veröffentlichung der darauf abzubildenden Informationen. Dabei kann auch nicht davon ausgegangen werden, dass es sich um allgemein zugängliche Daten handelt, denn aus der Tatsache der Anfertigung eines Stempels ist nicht abzuleiten, dass der Betroffene auch in öffentlich zugänglichen Übersichten wie Telefon- oder Adressbüchern aufgeführt ist.

Eine vergleichende Betrachtung verschiedener Lösungsmöglichkeiten (vorsorgliche oder nachträgliche Einwilligung, Anonymisierung, Verfremdung) führt zu dem Ergebnis, dass eine Verfremdung der Stempelbilder am besten den Interessen aller Beteiligten gerecht wird (Aufrechterhaltung der Attraktivität des Katalogs, Vermeidung von Persönlichkeitsrechtsbeeinträchtigungen der Betroffenen).

Eine Einwilligung ist in diesem Fall nicht praktikabel, weil der weitaus größte Teil der gefertigten Stempel über Wiederverkäufer abgesetzt wird. Diese legen die Tatsache, dass sie einen Subunternehmer mit der Herstellung der Stempel beauftragen, dem Endkunden gegenüber jedoch nicht offen, so dass eine Einwilligungslösung bezüglich der Veröffentlichung im Katalog des Subunternehmers ausscheidet.

Da der ermittelte Sachverhalt nicht nur die kontrollierte Firma betrifft, sondern vielmehr ein branchenweites Problem darstellt, hat sich die Aufsichtsbehörde auf einen Hinweis zur Rechtswidrigkeit und zur Möglichkeit der nachträglichen Legalisierung beschränkt und im Übrigen von Einzelmaßnahmen abgesehen. Nicht zuletzt musste berücksichtigt werden, dass die Herstellung des seit Mitte 2001 im Umlauf befindlichen Katalogs äußerst kostenintensiv war und der Katalog bereits eine große Verbreitung gefunden hat. Die Unterbindung der weiteren Verbreitung des Kataloges bzw. der Rückruf der im Umlauf befindlichen Exemplare im Fall eines einzelnen Unternehmens wäre sowohl unverhältnismäßig als auch wettbewerbsverzerrend gewesen. Gleiches würde für eine Unterrichtung der Betroffenen gelten.

Statt dessen wird versucht, eine branchenweite Lösung zu finden. Diese könnte in einer Informations- bzw. Sensibilisierungsaktion bestehen. Damit könnten alle betroffenen Unternehmen auf dieses branchenspezifische Problem reagieren; zu einem späteren Zeitpunkt sind auch Einzelmaßnahmen gegen uneinsichtige Branchenvertreter denkbar. Ein möglicher Ansatzpunkt für eine solche Kampagne wäre die in Wiesbaden ansässige Bundesinnung für das Flexografenhandwerk. Der Bundesinnung (ca. 150 Mitglieder) gehören zwar nicht alle, aber zumindest die bedeutendsten der bundesweit etwa 750 Stempelhersteller an. Es kann davon ausgegangen werden, dass sich Aktionen dieser Art auch zu nicht in der Bundesinnung vertretenen Flexografen herumsprechen werden. Die Katalogproblematik wird jedoch in erster Linie für die größeren Branchenvertreter von Bedeutung sein. Das RP Darmstadt als die für Wiesbaden zuständige Aufsichtsbehörde ist gebeten worden, in dieser Angelegenheit mit der Bundesinnung Kontakt aufzunehmen.

4.3.11 Veröffentlichung personenbezogener Daten bei Erlöschen der Prokura

Ein mittelständisches Unternehmen hatte sowohl im Rahmen seines Internetauftrittes als auch in einer selbst herausgegebenen Kundenzeitschrift (Auflage ca. 12.000 Stück) darüber informiert, dass die Prokura für einen Mitarbeiter ab einem konkret genannten Zeitpunkt erloschen ist. Datenschutzrechtlich bedenklich war dabei, dass dieser Mitarbeiter in den genannten Veröffentlichungen jeweils mit vollständiger Privatanschrift sowie dem genauen Geburtsdatum bezeichnet war.

Die Aufsichtsbehörde hat den Sachverhalt geprüft und ist zu dem Ergebnis gekommen, dass diese Übermittlung personenbezogener Daten weder durch § 28 Abs. 1 Nr. 1 BDSG (Arbeits-

vertrag) noch durch § 28 Abs. 1 Nr. 2 BDSG (berechtigte Interessen der verantwortlichen Stelle) oder gar Nr. 3 (allgemein zugängliche Daten) gedeckt ist. Insbesondere in den letzten beiden Fällen stehen einer Veröffentlichung jeweils überwiegende schutzwürdige Betroffeneninteressen gegenüber. Auch wenn die genannten Angaben grundsätzlich beim Amtsgericht eingesehen werden können, beschränken sich die amtlichen Bekanntmachungen beim Erlöschen einer Prokura regelmäßig auf die namentliche Nennung der (ehemaligen) Prokuristen. Das Geburtsdatum wird allenfalls dann veröffentlicht, wenn eine Prokura neu eingeführt wird. Die Privatanschrift schließlich wird grundsätzlich nicht veröffentlicht und ist auch nicht über telefonische Registerauskünfte in Erfahrung zu bringen.

Unabhängig davon ist der beim Registergericht nur durch zielgerichtetes Handeln (Studium der amtlichen Bekanntmachungen, explizite unternehmensbezogene Auskunftsersuchen an das Amtsgericht) erreichbare Erkenntnisgewinn (Geburtsdatum, Privatanschrift) hinsichtlich seiner Eingriffstiefe in die Privatsphäre in keiner Weise zu vergleichen mit einer Veröffentlichung in einer Zeitschrift oder gar im Internet, wodurch jedermann unaufgefordert und ohne erkennbare Notwendigkeit über Geburtstag und Privatwohnsitz eines ehemaligen Prokuristen informiert wird.

Es ist offensichtlich, dass eine auf den Namen und Vornamen beschränkte Veröffentlichung den Informationszweck in gleichem Maße erfüllt hätte. Abschließend ist festzustellen, dass die Veröffentlichung des Geburtsdatums sowie der Privatanschrift im Internet bzw. in der Kundenzeitschrift rechtswidrig erfolgt ist. Sollte dem Betroffenen dadurch ein Schaden entstanden sein, kann er gegenüber seinem ehemaligen Arbeitgeber auf der Basis von § 7 BDSG entsprechende Ansprüche geltend machen.

4.3.12 Datenerhebung durch eine Kurklinik mittels Fragebogen

Ein Betroffener bat die Aufsichtsbehörde zu prüfen, ob eine Kurklinik von ihren Patienten im Rahmen der Aufnahme in die Einrichtung verlangen kann, einen Fragebogen zu einer Vielzahl personenbezogener Daten auszufüllen, und ob der entsprechende Fragebogen mit dem Datenschutz vereinbar ist.

Die Zulässigkeit der seitens des Unternehmens durchgeführten Datenerhebung beurteilt sich nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG. Danach ist das Erheben personenbezogener Daten oder

ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke u. a. zulässig, wenn es der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen dient.

Gegen die grundsätzliche Zulässigkeit der Datenerhebung im Rahmen des Behandlungsvertrages bestanden keine datenschutzrechtlichen Bedenken. Einzelne auf dem Fragebogen enthaltene Datenfelder waren jedoch für den Klinikaufenthalt nicht erforderlich (Religion, Geburtsdatum des Ehepartners).

Die Aufsichtsbehörde forderte das Unternehmen auf, die betreffenden Datenfelder mit einem * zu versehen und als freiwillige Angaben zu kennzeichnen. Darüber hinaus wurde das Unternehmen gebeten, direkt auf dem Fragebogen zu vermerken, dass der Fragebogen in den Patientenunterlagen der Klinik verwahrt wird und ausschließlich ärztlichen bzw. therapeutischen Zwecken dient und dass er nicht an Dritte weitergegeben wird.

Das Unternehmen hat den Fragebogen überarbeitet und dabei die Forderungen und Anregungen der Aufsichtsbehörde berücksichtigt.

4.3.13 Prüfangebote zur Nettolohnerhöhung

Der Aufsichtsbehörde ist ein mit „Prüfantrag zur Nettolohnerhöhung“ überschriebenes Formular einer „Wirtschaftskanzlei“ vorgelegt worden. Beigefügt war eine „Wichtige Mitteilung“ für alle Arbeitnehmer, Angestellten und Beamten, die sich mit ihrem Einkommen über der Bemessungsgrenze 3.000 DM/4.300 DM (ledig/verheiratet) befinden. Demnach wurde auf Grund von nicht näher bezeichneten Gesetzesänderungen und Sonderregelungen eine kostenlose Erstellung eines Antrags zur Prüfung einer Nettolohnerhöhung angeboten, womit zwischen 35 und 70 % der Lohnsteuer parallel zum Lohnsteuerausgleich zurückgeführt werden könnten. Der Prüfantrag enthielt eine allgemeine Zusicherung, dass alle Daten entsprechend dem BDSG behandelt werden; ergänzend waren die §§ 1, 3 des BDSG 77 (!) abgedruckt. Im eigentlichen Erhebungsteil wurden umfangreiche Angaben zur persönlichen Situation (Anschrift, Geburtsdatum, Arbeitgeber, Familienverhältnisse etc.), zum monatlichen Einkommen (Brutto/Netto, Kindergeld, Kirchensteuer etc.), zu monatlichen Ausgaben (Miete, Unterhalt, Krankenversicherung etc.), zum Haus- und Grundbesitz sowie zu sonstigen Verbindlichkeiten abverlangt.

Da es sich unzweifelhaft um ein Angebot auf freiwilliger Basis handelte, lag der primäre Ansatzpunkt für die Aufsichtsbehörde in der unzureichenden sowie überholten, inzwischen jedoch entsprechend aktualisierten Datenschutzerklärung. In diesem Zusammenhang wurden der Zweck der Datenverarbeitung sowie die Herkunft der Daten hinterfragt. Demnach handelt es sich bei den durch die Wirtschaftkanzlei zugesandten Unterlagen um ein Angebot zur Prüfung, ob durch geeignete steuerrechtliche Abschreibungsmodelle eine Erhöhung des jeweiligen Nettolohnes möglich ist. Ob derartige Abschreibungsmodelle anwendbar sind und welche finanziellen Vorteile sich daraus ergeben, kann natürlich nur ermittelt werden, wenn der Interessent die dafür notwendigen persönlichen Daten bereitstellt. Rechtsgrundlage für die damit verbundene Datenverarbeitung wäre dann § 28 Abs. 1 Nr. 1 BDSG (Zweckbestimmung eines Vertragsverhältnisses, hier: Prüfauftrag).

Voraussetzung für das Zustandekommen des Vertragsverhältnisses ist, dass der Adressat des Schreibens tatsächlich daran interessiert ist, eine derartige Prüfung durch die Wirtschaftskanzlei durchführen zu lassen, und diesen Prüfauftrag dann mit der Rücksendung des ausgefüllten Formulars auch erteilt. An dieser Stelle ist also der Betroffene selbst gefragt. Es steht außer Frage, dass die Annahme dieses Angebots – wie bei jeder Werbesendung – vollkommen freiwillig ist und dass keine Auskunftspflicht besteht.

Datenschutzrechtlich unzulässig ist daher ein solches Angebot sicherlich nicht, jedoch ist darauf hinzuweisen, dass jedermann gut beraten ist, sich vor der (zweckgebundenen) Weitergabe seiner (sensiblen) personenbezogenen Daten einen persönlichen Eindruck von der Seriosität des zu beauftragenden Unternehmens zu verschaffen und den Inhalt des Prüfvorgangs näher zu hinterfragen.

Wesentlich kritischer zu sehen ist die dem Versand der Prüfanträge vorausgehende telefonische Akquise. Der Inhaber der Wirtschaftskanzlei gab zwar an, sich insoweit auf den gewerblichen/geschäftlichen Bereich (Verwendung von Branchentelefonverzeichnissen) zu beschränken; dennoch bestehen Zweifel an der Zulässigkeit der Telefonakquise. Die von den Mitarbeitern getätigten Akquisitionsanrufe erfolgen zwar über geschäftliche Telefonanschlüsse, jedoch werden die kontaktierten Geschäftsleute bzw. Mitarbeiter dann als Privatpersonen angesprochen, d. h. der eigentliche Geschäftsbereich des Unternehmens bzw. Gewerbetreibenden ist vom Anruf nicht betroffen. Rechtswidriges „kaltes Telefonmarketing“ liegt nach der Rechtsprechung des BGH (NJW 1991, 2087 „Telefonwerbung IV“) jedoch auch dann vor, wenn geschäftliche Telefonnummern für eindeutig auf private Verfügungszwecke zielendes

Marketing genutzt werden. Damit soll grundsätzlich das auch am Arbeitsplatz dem Betroffenen zustehende Recht auf Nichtbeeinträchtigung durch werbende Telefonanrufe geschützt werden, das als Teil des Persönlichkeitsrechts einen hohen grundgesetzlich geschützten Rang hat.

Da also offensichtlich keine der von der Rechtsprechung für den gewerblichen Bereich aufgestellten Zulässigkeitskriterien

- bestehende Geschäftsbeziehung oder
- Betroffenheit des eigentlichen Geschäftsbereiches oder
- Betroffenheit eines Hilfsgeschäftes i. V. m. konkreten Anzeichen für ein Interesse des Angerufenen

zutrifft, ist die Rechtmäßigkeit der praktizierten Telefonakquise in der Tat fraglich. Allerdings ist dies vordergründig ein wettbewerbsrechtliches Problem (möglicher Verstoß gegen § 1 UWG); Betroffene sollten sich diesbezüglich daher an die zuständige Verbraucherzentrale wenden.

4.3.14 Erhebung von Einkommensdaten von Mitgliedern eines Tierschutzvereins

Auf Grund einer Bürgereingabe nahm die Aufsichtsbehörde eine anlassbezogene Betriebskontrolle bei einem Tierschutzverein, insbesondere hinsichtlich dessen automatisierter Mitgliederverwaltung vor.

Der Tierschutzverein fragte in seinem Beitrittsformular Einkommensdaten von Mitgliedern ab. Die Abfrage der Einkommensdaten wurde vom Einwender als Verstoß gegen das BDSG betrachtet, da seiner Ansicht nach die Zulässigkeit der Datenverarbeitung nicht gegeben war.

Bei den Recherchen durch die Aufsichtsbehörde stellte sich heraus, dass Zweck der Einkommenserhebung die Verteilung von Futterspenden für wildlebende Katzen war. In Anbetracht der Tatsache, dass engagierte Tierfreunde hierbei in der Regel zusätzlich mit ihrem eigenen Einkommen Tierfutter hinzukauften, sollten einkommensschwache Personen bevorzugt bezuschusst werden.

Eine Erlaubnisnorm im BDSG oder in anderen speziellen datenschutzrechtlichen Regelungen in anderen Gesetzen, welche die private Verarbeitung der Einkommensdaten erlauben würde,

besteht nicht. Dem Verein wurde mitgeteilt, dass die Angabe von Einkommensdaten im Beitrittsformular nur auf Basis einer freiwilligen, schriftlich zu erteilenden Einwilligungserklärung des Betroffenen nach § 4 a BDSG erfolgen kann. Auf die Freiwilligkeit muss außerdem besonders hingewiesen werden.

Der Tierschutzverein sicherte daraufhin schriftlich die Löschung der ohne Einwilligung erhobenen Einkommensdaten zu. Das Formular wird im Hinblick auf die Einkommensdaten mit einer Einverständniserklärung gemäß § 4 a BDSG versehen. Außerdem werden die Angaben auf dem Beitrittsformular durch den Verein auf die zur Vereinsführung notwendigen Daten beschränkt.

4.3.15 Datenverarbeitung für Werbezwecke

Unerwünschte Werbeschreiben, insbesondere von Unternehmen, mit denen vorher zu keiner Zeit irgendein Kontakt bestanden hat, sind ein weiterer „Dauerbrenner“ in der Kontrolltätigkeit der Aufsichtsbehörden.

Ein besonderes Problem ist dabei die Tatsache, dass das BDSG - im Interesse der werbetreibenden Wirtschaft – gewisse Erleichterungen bei der Datenübermittlung vorsieht. So können zusammengefasste Daten über eine Vielzahl von Personen, so sie sich auf

- Berufs-, Branchen- oder Geschäftsbezeichnung,
- Namen,
- Titel,
- Akademische Grade,
- Anschrift,
- Geburtsjahr sowie
- eine Angabe über die Personengruppe als Ganzes

beschränken, für Zwecke der Werbung oder der Markt- und Meinungsforschung übermittelt und genutzt werden (§ 28 Abs. 3 Nr. 3 BDSG), ohne dass die Betroffenen hierüber informiert werden oder gar ihre Zustimmung erteilen müssen. Die Betroffenen haben insoweit jedoch zumindest ein Widerspruchsrecht, welches sie vorsorglich oder nachträglich bei den Stellen geltend machen können, die ihre Daten für die genannten Zwecke verwenden (§ 28 Abs. 4

Satz 1 BDSG). Abgesehen davon, dass die Betroffenen hierbei selbst aktiv werden müssen, war in der Vergangenheit ein erhebliches Informationsdefizit zu verzeichnen. Den Betroffenen war die Möglichkeit des Widerspruchs vielfach nicht bekannt.

Insoweit hat die Novellierung des BDSG Verbesserungen gebracht, denn die verantwortlichen Stellen treffen nunmehr Unterrichtungspflichten: Gemäß § 28 Abs. 4 Satz 2 BDSG ist der Betroffene bei der Ansprache zu Zwecken der Werbung oder der Markt- und Meinungsforschung über die verantwortliche Stelle sowie über das Widerspruchsrecht zu unterrichten.

Die Kontrollpraxis zeigt, dass bei den Unternehmen vielerorts noch Umsetzungsdefizite bestehen. Dies verdeutlichen auch die Eingaben bei der Aufsichtsbehörde. In den seltensten Fällen erfolgt eine Unterrichtung über das Widerspruchsrecht, mitunter ist noch nicht einmal die verantwortliche Stelle ersichtlich.

So verwundert es denn auch nicht, dass Betroffene auch weiterhin nur zögerlich von ihrem Widerspruchsrecht Gebrauch machen. Im Regelfall verlangen sie lediglich die Löschung ihrer Daten bei der jeweiligen verantwortlichen Stelle. Dabei ist ihnen allerdings nicht bewusst, dass gerade die Löschung dazu führen kann, dass sie kurzfristig erneut Werbeschreiben des gleichen Absenders erhalten. Mit dem Löschen der Daten geht auch die Kenntnis der ablehnenden Haltung gegenüber Werbeschreiben verloren. Beschränkt sich der Betroffene hingegen auf die Geltendmachung seines Widerspruchsrechtes, so muss die verantwortliche Stelle nunmehr geeignete Maßnahmen treffen, dass erneute Werbesendungen an diesen Empfänger ausgeschlossen sind. Üblicherweise werden dazu sogenannte Sperrdateien angelegt. Da in der Werbebranche sehr häufig mit externen Adressdatenbeständen gearbeitet wird, ist nur so, d. h. durch einen Abgleich der angemieteten bzw. erworbenen Datenbestände mit der eigenen Sperrdatei zu vermeiden, dass Personen gegen ihren ausdrücklich geäußerten Willen erneut zu Werbezwecken angeschrieben werden.

Bislang waren die Aufsichtsbehörden bei Verstößen gegen die im Rahmen der Novellierung neu in das BDSG aufgenommenen Unterrichtungspflichten noch entsprechend zurückhaltend und haben es bei einem rechtlichen Hinweis bzw. der Forderung nach zukünftiger Beachtung belassen. Nachdem jedoch das novellierte BDSG nunmehr zwei Jahre in Kraft ist, sollte diese Regelung bekannt sein, so dass zukünftig mit einem härteren Durchgreifen zu rechnen ist, zumal diesbezügliche Verstöße explizit als Bußgeldtatbestand im BDSG verankert sind (§ 43 Abs. 1 Nr. 3 BDSG).

4.3.16 Werbeschreiben einer Bank

Ein Betroffener hatte von einer Bank unaufgefordert ein persönliches Kreditangebot erhalten. Da mit dem Unternehmen bisher keinerlei geschäftliche oder sonstige Kontakte bestanden, bat er telefonisch um Auskunft über die Herkunft seiner bei der Werbung verwendeten personenbezogenen Daten. Er wurde mit seinem Auskunftsbegehren an die Unternehmenszentrale verwiesen.

Der Betroffene wandte sich daraufhin an die Datenschutz-Aufsichtsbehörde. Im Ergebnis der Ermittlungen konnte Folgendes festgestellt werden:

Die Überprüfung der gesamten Kundendatei der Bank durch deren Datenschutzbeauftragten hat ergeben, dass unter dem Namen des Betroffenen kein Kunde gespeichert war. Mit der Fertigung von Werbeanschreiben an Nichtkunden beauftragt die Bank Fremdfirmen. Die Daten von Nichtkunden werden bei der Bank nicht gespeichert.

Damit zurückverfolgt werden kann, woher die Anschrift stammt und welche Firma die Werbeaktion für die Bank durchgeführt hat, enthält jedes Werbeanschreiben einen sogenannten Werbecode, und zwar in der linken oberen Ecke des Anschreibens. Anhand des Werbecodes konnte die beauftragte Firma ermittelt werden.

Der Datenschutzbeauftragte veranlasste, dass dem Betroffenen in Zukunft keine Werbung mehr von der Bank zugehen wird. Die Aufsichtsbehörde hat die Bank aufgefordert, durch geeignete Maßnahmen zukünftig die Einhaltung der Informationspflichten aus § 28 Abs. 4 Satz 2 BDSG sicherzustellen.

Gemäß § 28 Abs. 4 Satz 1 BDSG kann der Betroffene jederzeit bei der verantwortlichen Stelle der Nutzung oder Übermittlung seiner personenbezogenen Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung widersprechen mit der Folge, dass eine Nutzung oder Übermittlung der Daten für diese Zwecke unzulässig ist. Bereits nach dem alten BDSG (vgl. § 28 Abs. 3 Satz 1 BDSG a. F.) hatte der Betroffene ein solches Widerspruchsrecht.

Wie der geschilderte Fall zeigt, bestehen hinsichtlich der Beachtung der Informationspflichten seitens der Unternehmen noch erhebliche Defizite.

4.3.17 Personalausweiskopien bei Rabattaktionen

Das Augusthochwasser 2002 hat in Sachsen auch zu datenschutzrechtlichen Problemen geführt. So boten viele Handelseinrichtungen einen speziellen Rabatt für Flutoper an, um auf diese Weise einen Beitrag zur schnellen Beseitigung der Flutschäden zu leisten.

Anfangs erfolgte die Rabattgewährung mehr oder weniger auf Vertrauensbasis, wobei festgestellt werden musste, dass es zahlreiche Trittbrettfahrer gab, d. h., es wurden Rabatte von Personen in Anspruch genommen, die gar nicht vom Hochwasser betroffen waren.

Da einerseits die Verwaltung nicht so schnell in der Lage war, für die Betroffenen entsprechende Bescheinigungen auszustellen, andererseits aber schnelles Handeln geboten war, ging man in einem Baumarkt dazu über, von den Betroffenen, die (noch) keine Bescheinigung vorlegen konnten, die Personalausweise zu kopieren. Anschließend erhielten diese Personen ebenso wie die Personen mit Bescheinigung (und ohne Ausweiskopie) eine sogenannte Nachlassberechtigung, mit der sie dann den Rabatt in Anspruch nehmen konnten. Sobald die Bescheinigung (nachträglich) vorgelegt wird, sollte die Vernichtung oder Rückgabe der angefertigten Kopien erfolgen.

Die Aufsichtsbehörde hat den Vorgang geprüft und ist zu dem Ergebnis gekommen, dass die Anfertigung von Ausweiskopien unzulässig und damit rechtswidrig ist:

Gemäß § 28 Abs. 1 Nr. 1 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten (hier: Anfertigung von Ausweiskopien) oder ihre Nutzung als Mittel für eigene Geschäftszwecke zulässig, wenn dies der Zweckbestimmung eines Vertragsverhältnisses (hier: Rabattgewährung) mit dem Betroffenen dient. Unter dem Aspekt, dass für die Rabattgewährung die Erhebung und Speicherung der auf der Nachlassberechtigung vorgesehenen (und durch Einsichtnahme in den Personalausweis zu überprüfenden) Daten ausreichend ist, fehlt es an der Erforderlichkeit für die Anfertigung der Kopien. Datenschutzrechtlich entspricht die Kopie eines Ausweises der Erhebung und Speicherung aller in diesem Dokument enthaltenen Daten. Dies ist jedoch nur dann zulässig, wenn hierfür eine explizite gesetzliche Grundlage besteht bzw. wenn nachgewiesen werden kann, dass diese Daten auch tatsächlich für den beabsichtigten Zweck benötigt werden. Den Ausführungen des Marktleiters zufolge diente diese Maßnahme jedoch ausschließlich dazu, Kunden ohne behördliche

Schadensbestätigung von der missbräuchlichen Inanspruchnahme der Rabattregelung abzuhalten (Abschreckung). Dies unterstreicht aber die hinsichtlich der Rabattgewährung fehlende Erforderlichkeit der erhobenen Daten, womit die Anfertigung der Kopien insgesamt unzulässig ist. Auch für den gegebenenfalls (erkennbaren Missbrauch) notwendigen Widerruf der Nachlassberechtigung ist eine Personalausweiskopie in keinem Fall notwendig.

Der Baumarkt hat die datenschutzrechtliche Bewertung der Aufsichtsbehörde akzeptiert und die Anfertigung von Ausweiskopien eingestellt. Vorhandene Ausweiskopien wurden vernichtet.

4.3.18 Personalausweiskopien bei Bankgeschäften

Auch Banken und Sparkassen greifen, insbesondere wenn es um den Nachweis geht, dass die Identität des Kunden ordnungsgemäß überprüft worden ist, oft und gern auf Personalausweiskopien zurück. Selbst bei Bankgeschäften durfte aber nach bisheriger Rechtslage nur in Ausnahmefällen ohne Einverständnis des Kunden eine Personalausweiskopie erstellt werden.

Nach dem in § 154 Abgabenordnung (AO) verankerten Grundsatz der Kontenwahrheit sind Kreditinstitute bei der Kontoeröffnung verpflichtet, sich Gewissheit über die Person und die Anschrift des Verfügungsberechtigten zu verschaffen. Diese Gewissheit besteht, wenn dem Bankangestellten der vollständiger Name, die Anschrift und gegebenenfalls noch das Geburtsdatum mitgeteilt worden sind, und dieser die Angaben anhand eines vorgelegten Personalausweises überprüft hat. Gem. § 154 Abs. 2 AO besteht darüber hinaus die Verpflichtung, diese Angaben in geeigneter Form (schriftlich) festzuhalten. Eine Berechtigung oder gar Verpflichtung zum Kopieren des Personalausweises enthält die Abgabenordnung nicht.

Neben der AO sind unter bestimmten Voraussetzungen noch die Bestimmungen des Geldwäschegesetzes (GWG) zu beachten. Danach sind Kreditinstitute verpflichtet, ihre Kunden bei jeder Transaktion (z. B. Ein- oder Auszahlung) ab 15.000 € zu identifizieren (§ 2 GWG). Gemäß § 9 Abs. 1 GWG sind diesbezüglich erfolgte Identifizierungen durch eine Kopie der zur Feststellung der Identität vorgelegten Ausweise zu dokumentieren, d. h. in diesen Fällen wäre die Anfertigung einer Personalausweiskopie also zulässig.

Zusammengefasst bedeutet dies, dass ein Kreditinstitut dann eine Ausweiskopie fordern dürfte, wenn eine Finanztransaktion in einer Größenordnung ab 15.000 € durchgeführt würde. War der bewegte Geldbetrag (Bargeld, Wertpapiere, Edelmetalle) kleiner oder handelte es sich um Vorgänge ohne finanzielle Transaktionen (z. B. Kontoeröffnung), war nach bisheriger Rechtslage die Anfertigung von Ausweiskopien nur mit ausdrücklicher Einwilligung des Kunden, mithin auf freiwilliger Basis, zulässig.

Am Ende des Berichtszeitraumes ist jedoch eine Änderung der Rechtslage eingetreten. Gemäß § 2 GWG besteht die Identifizierungspflicht nun auch bei Abschluss eines Vertrages zur Begründung einer auf Dauer angelegten Geschäftsbeziehung, wozu auch die Führung eines Kontos gehört.

4.3.19 Kontostandsanzeige an Geldautomaten

Der Aufsichtsbehörde lag eine Beschwerde vor, wonach seit einiger Zeit an allen Geldautomaten eines Geldinstitutes nach Identifikation/Authentifizierung des Kunden grundsätzlich der aktuelle Kontostand angezeigt wird.

Nach Kenntnis der Aufsichtsbehörde ist eine Kontostandsanzeige zwar auch bei anderen Geldinstituten möglich, jedoch obliegt es dort der Entscheidung des Kunden, ob er diese Funktion aufruft oder nicht. Bedingt durch die oftmals ungünstige räumliche Aufstellung der Geldautomaten sowie der Größe und Anordnung des Bildschirms (wird durch den Kunden nicht ausreichend verdeckt), ist es in den meisten Fällen nicht vermeidbar, dass wartende Kunden den aktuellen Kontostand des am Geldautomaten tätigen Kunden einsehen können. Genau dies war auch Gegenstand der an die Aufsichtsbehörde herangetragenen Bedenken. Wenn eine Kenntnisnahme des Kontostandes durch Dritte nicht durch eine geeignete räumliche Anordnung (z. B. Aufstellung des Geldautomaten in einer Weise, dass hinter dem Geld abhebenden Kunden keine weiteren Kunden warten können) vermieden werden kann, so muss durch anderweitige technische Maßnahmen eine derartige Kenntnisnahme ausgeschlossen (Kontostandsanzeige deaktiviert) bzw. die Entscheidung darüber, ob unter diesen Umständen der Kontostand angezeigt werden soll, dem Kunden überlassen werden (explizit aufzurufende Funktion).

Der Vorstand des Geldinstitutes hat diesen Standpunkt der Aufsichtsbehörde akzeptiert und die kritisierte obligatorische Kontostandsanzeige zeitnah unterbunden. Die Möglichkeit einer kundengesteuerten Kontostandsabfrage bleibt von dieser Entscheidung unberührt.

4.3.20 Aufbewahrung von Belegen bei Zahlung mit EC-Karte

Ein Betroffener beschwerte sich bei der Aufsichtsbehörde über den unsachgemäßen Umgang eines Einzelhandelsunternehmens mit Kundendaten.

Der Betroffene hatte bei dem Unternehmen eingekauft und mit EC-Karte bezahlt. Der für die Abwicklung der Zahlung per elektronischem Lastschriftverfahren erstellte Originalbeleg mit der Bankverbindung und der Unterschrift des Betroffenen war von der Kassiererin in einem offenen Schuhkarton - für jedermann zugänglich und sichtbar - auf dem Verkaufstresen abgelegt worden. Der Aufforderung des Betroffenen, den Beleg aus dem Schuhkarton zu entfernen und sicher aufzubewahren, kam die Kassiererin nicht nach.

Nachdem sich die Aufsichtbehörde eingeschaltet hatte, änderte das Unternehmen diese Verfahrensweise. Die Belege werden nunmehr bis zum täglichen Geschäftsschluss in der Kasse gesammelt.

5 Beratungsdienst / Anfragen an die Behörde

„Der betriebliche Datenschutzbeauftragte wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin. Zu diesem Zweck kann sich der Beauftragte für den Datenschutz in Zweifelsfällen an die für die Datenschutzkontrolle bei der verantwortlichen Stelle zuständige Behörde wenden.“ (§ 4 g Abs.1 Satz 1 BDSG).

Der betriebliche Datenschutzbeauftragte ist außerdem für die Vorabkontrolle zuständig. Auch im Hinblick darauf hat er sich in Zweifelsfällen an die Aufsichtsbehörde zu wenden (§ 4 d Abs. 6 BDSG).

Gesetzlich vorgesehen ist eine datenschutzrechtliche Beratung durch die Aufsichtsbehörde also zunächst nur für betriebliche Datenschutzbeauftragte. Darüber hinaus wenden sich aber in vielen Fällen auch andere Personen an die Aufsichtsbehörde. Dazu gehören sowohl Firmeninhaber, Geschäftsführer als auch Betriebsräte sowie natürlich Betroffene. Ungeachtet der fehlenden gesetzlichen Verankerung dieser Beratungstätigkeit werden selbstverständlich auch deren Anfragen ohne Ausnahme beantwortet, da auf diese Weise ein wesentlicher Beitrag zur Erhöhung des Datenschutzbewusstseins einerseits wie auch des Datenschutzniveaus im nichtöffentlichen Bereich andererseits geleistet werden kann. Nicht zuletzt entlastet dies perspektivisch auch die Aufsichtsbehörde selbst durch die mittelbare Verringerung der Anlasskontrollen.

Sofern sich Betroffene selbst an die Aufsichtsbehörde gewandt haben, ging es diesen in erster Linie darum, das eigene Misstrauen von kompetenter Seite her bestätigt bzw. widerlegt zu bekommen, um dann gegebenenfalls mit den notwendigen Argumenten die Lösung des jeweiligen Problems in eigener Regie zu bewältigen. Haben sich hingegen Firmen, Vereine oder sonstige speichernde Stellen an die Aufsichtsbehörde gewandt, so erfolgte dies im Regelfall zum Zweck der Abklärung von Zulässigkeitsfragen und damit der Vermeidung von Datenschutzverstößen.

Die je nach Sachlage telefonisch oder schriftlich erfolgte Beratungstätigkeit bei der Bearbeitung von Anfragen der verschiedensten Art bildete also auch 2001/2002 einen wesentlichen Bestandteil der Tätigkeit der Aufsichtsbehörden. Das Spektrum der Anfragen war äußerst vielfältig; inhaltlich konzentrierten sich die Anfragen vor allem auf die Zulässigkeit der Datenverarbeitung, -erhebung und -nutzung. Folgende Schwerpunkte waren im Berichtszeitraum zu erkennen:

- Bestellung / Tätigkeit des betrieblichen Datenschutzbeauftragten
- Datenschutz im Mietverhältnis / Fragerecht des Vermieters
- Tätigkeit von Wirtschaftsauskunfteien / Benachrichtigungen gem. § 33 BDSG
- Arbeitnehmerdatenschutz
- Nachfrage von Informationsmaterial, aktuellen gesetzlichen Regelungen
- Kopieren von Ausweisdokumenten, Erfassung von Ausweisdaten (Handel, Banken)
- Zulässigkeit von Datenübermittlungen
- Internet / neue Medien
- Verbände, Vereine

- Gesprächsaufzeichnung, Lauthören, Videoüberwachung
- Erfassung von Daten bei der EC- Scheckkartenzahlung
- Register nach § 32 BDSG 90, § 4 d BDSG 01 / Meldepflicht
- Datenverarbeitung für Werbezwecke
- Markt- und Meinungsforschung
- Aufbewahrungsfristen, Archivierung, Vernichtung
- Akteneinsicht
- Öffentliches Verfahrensverzeichnis
- Schwarzfahrerdaten
- Warndateien, Schuldnerlisten
- Schufa
- Aspekte der Auftragsdatenverarbeitung
- Datengeheimnis
- Datenschutzaudit / Zertifizierung
- unerbetene Faxwerbung
- Anfragen ohne Datenschutzbezug

Außerordentlich häufig waren vor allem Anfragen zum Problemkreis *„Betrieblicher Datenschutzbeauftragter“*. Neben der Klärung der Bestellungspflicht ging es dabei um Fragen der Auswahl einer geeigneten Person, um den Erwerb der Fachkunde sowie die Anforderungen an die Arbeitsbedingungen des betrieblichen Datenschutzbeauftragten.

Stark zugenommen haben die Anfragen im *Bereich des Wohnungswesens*. Unumstrittener Schwerpunkt sind hier die im Rahmen der Wohnungssuche vom Mietbewerber abgeforderten Selbstauskünfte (vgl. auch 4.3.6). Daneben waren Mieter an Informationen zu ihrem Auskunftsrecht sowie zu datenschutzrechtlichen Aspekten der Betriebskostenabrechnung interessiert.

Die Anfragen zur *Tätigkeit von Wirtschaftsauskunfteien* beruhen in den meisten Fällen auf dem Erhalt einer Benachrichtigung gem. § 33 Abs. 1 BDSG und sind damit eher Zeichen einer datenschutzgerechten Geschäftstätigkeit und nicht Anhaltspunkte für Datenschutzverstöße. Betroffene reagieren in diesem Zusammenhang zumeist mit Unverständnis, wenn ihnen die Auskunft darüber verweigert wird, wer ohne ihr Wissen Informationen über sie eingeholt hat. Eine derartige Auskunft kann die Auskunftei seit der BDSG-Novellierung nach einer Einzelfallabwägung mit dem Argument der Wahrung von Geschäftsgeheimnissen ablehnen

(§ 34 Abs. 1, 2 BDSG). Klarstellend muss hinzugefügt werden, dass auch nach dem BDSG 90 nur dann ein diesbezügliches Auskunftsrecht bestanden hatte, wenn begründete Zweifel an der Richtigkeit der übermittelten Daten geltend gemacht werden konnten.

Daneben stehen Anfragen zum *Arbeitnehmerdatenschutz* zahlenmäßig im Vordergrund.

Ein verschiedene Bereiche umfassendes Dauerthema sind *Ausweisdaten und Ausweiskopien*. Die Erhebung umfangreicher Ausweisdaten, insbesondere der Dokumentennummer, wird vielerorts als Garantie dafür angesehen, den Betroffenen bei nichtvertragsgemäßem Verhalten jederzeit wieder aufspüren und die zur Durchsetzung der eigenen Ansprüche erforderlichen Maßnahmen durchsetzen zu können. Dabei wird regelmäßig übersehen, dass private Stellen gemäß dem PassG bzw. PersAuswG grundsätzlich nicht befugt sind, Auskünfte aus dem Pass- bzw. Personalausweisregister zu erlangen. Andererseits sind Ausweisnummern auch nicht für die Beantragung von Melderegisterauskünften erforderlich, da die eindeutige Identifikation bereits durch die gleichfalls erhobenen Angaben wie Namen, Anschrift und ggf. Geburtsdatum sichergestellt ist. Nach den melderechtlichen Vorschriften benötigt ein Unternehmen also weder Personalausweis- noch Passnummer, um weitere Informationen mittels einer Melderegisterauskunft in Erfahrung zu bringen. Der Hang zur Anfertigung von Ausweiskopien im Einzelhandel hat nach hiesigen Erfahrungen deutlich nachgelassen; im Bankenbereich gibt es diesbezüglich jedoch immer wieder Probleme. Diesbezüglich wird auf die Ausführungen unter Pkt. 4.3.18 verwiesen.

Die Anfragen zur *Tätigkeit von Vereinen* betreffen vorwiegend die Vereine, Verbände sowie sonstigen Einrichtungen der freien Wohlfahrtspflege. Die Zuordnung dieser Stellen zum öffentlichen bzw. nicht-öffentlichen Bereich erfolgt aufgabenbezogen.

Im Berichtszeitraum hat es auch Anfragen von Bürgern gegeben, bei denen das datenverarbeitende Unternehmen seinen Sitz in einem anderen Bundesland hat und deshalb nicht unter die Zuständigkeitsbereiche der Aufsichtsbehörden des Freistaates Sachsen fällt, wie z. B. bei folgendem Fall:

Es ging um nicht verlangte Werbung für Informationsdienste über gebührenpflichtige 0190-Nummern. Bis die Aufsichtsbehörde ermittelt hatte, wer ursächlich für diese unerwünschte Faxwerbung war, gingen die Petenten davon aus, es handele sich um ein in Sachsen ansässiges Unternehmen. Sie fühlten sich durch diese Art der Werbung belästigt. Die an die Auf-

sichtsbehörde gerichtete datenschutzrechtliche Fragestellung betraf die Herkunft von Faxnummern, die teilweise nicht in öffentlichen Verzeichnissen vorzufinden waren, deren Verwaltung und die mögliche Weitergabe. Erst nach längeren Recherchen konnte die versendende Firma und deren Geschäftsführer ausgemacht werden. Hierauf sprach deren Geschäftsführer persönlich bei der Aufsichtsbehörde vor. Er teilte mit, er miete von verschiedenen Anbietern 0190er-Nummern an. Diese würden dann weiter an verschiedene Interessenten vermietet. Er stelle hierbei Dienstleistungen zur Verfügung, die die Vermittlung der technischen Abwicklung des Versendens von Werbefaxen für 0190er-Nummern als auch des Faxabrufdienstes mit verschiedenen Inhalten durch kostenpflichtige 0190er-Nummern zum Inhalt haben. Mit den Inhalten der abzurufenden Faxe habe er nichts zu tun. Diese seien auf eine in Sachsen-Anhalt ansässige Firma zurückzuführen. Er legte hierzu einen Datenträger mit einer dBASE-Datei vor. Der Datenträger enthielt die Bezeichnung 02.08.2002. Auf diesem Datenträger waren unsortiert 17.000 Telefon/Telefaxnummern bundesweit gespeichert. Außer den Nummern waren keine weiteren Daten in der Datei enthalten.

Der Geschäftsführer erklärte, er erhalte die Nummern aus Sachsen-Anhalt auf einem Datenträger. Der Datenträger werde ungeöffnet an eine Firma geleitet, die die technische Durchführung der Versendung vornehme. Am 02.08.2002 seien dies beispielsweise ca. 17.000 Nummern gewesen. Es wurde angeboten, die Löschung der Nummern der Petenten vorzunehmen.

Die Angelegenheit wurde an das Regierungspräsidium Halle als für diesen Fall zuständige Behörde abgegeben. Den Petenten wurde dieser Sachverhalt mitgeteilt. Das Regierungspräsidium Halle hat die Frage zu klären, ob die Daten personenbeziehbar sind und der Anwendungsbereich des Bundesdatenschutzgesetzes eröffnet ist.

6 Prüfung der Verhaltensregeln von Berufsverbänden

Die Aufsichtsbehörde überprüft gemäß § 38 a Abs. 2 BDSG die ihr von Berufsverbänden und anderen Vereinigungen unterbreiteten Entwürfe für interne datenschutzrechtliche Verhaltensregeln auf ihre Vereinbarkeit mit dem geltenden Datenschutzrecht hin. An derartige Verhaltensregeln stellen die Aufsichtsbehörden konkrete Anforderungen, d. h., es genügt insoweit nicht, nur die Bestimmungen des BDSG wiederzugeben. Statt dessen müssen die Verhaltensregeln einen über den Regelungsbereich des BDSG hinausgehenden *Mehrwert* beinhalten, was in erster Linie durch eine *Konkretisierung der materiellen Voraussetzungen des BDSG*

(z. B. Angaben zur Speicherdauer oder zur Datensparsamkeit) zu erreichen ist. Außerdem prüfen die Aufsichtsbehörden die vorgelegten Verhaltensregeln maßgeblich auch darauf, ob für die jeweilige Branche typische Fragestellungen beantwortet werden. Die Überprüfung der von Einzelunternehmen vorgelegten Verhaltensregeln ist im Rahmen des § 38 a BDSG nur dann möglich, wenn eine Branche durch das einreichende Unternehmen fast vollständig repräsentiert wird. 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 § 4 c Abs. 1 BDSG aufgeführten Ausnahmetatbestände greift, kann die Aufsichtsbehörde entsprechende Datenübermittlungen genehmigen, wenn die verantwortliche Stelle ausreichend Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist.“ (§ 4 c 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 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

- **Internetpräsenz**

Mit der wachsenden Zahl der Internetnutzer wird auch die Präsenz der Behörden im Internet immer wichtiger. Auf diesem Weg kann eine breite Wirkung der Öffentlichkeitsarbeit erzielt

werden. Auch die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben im Berichtszeitraum ihre Internetpräsenz ausgebaut, um den Bürgern und der Wirtschaft einen entsprechenden Service anbieten zu können.

Die inzwischen vollständig überarbeitete Internetpräsentation des Sächsischen Staatsministeriums des Innern, Referat Datenschutz, ist zu finden unter www.smi.sachsen.de/datenschutz. Dort sind zahlreiche wichtige Informationen zum Thema Datenschutz abrufbar, unter anderem das im vergangenen Jahr veröffentlichte „Datendschungelbuch-online". Das Datendschungelbuch ist ein Wegweiser für Bürger, der ihnen helfen soll, das „Dickicht" in der Privatwirtschaft zu „lichten", um besser zu durchschauen, *wer* ihre personenbezogenen Daten *mit welchem Grund* und *welcher Berechtigung* verwendet und was sie selbst unternehmen können, wenn sie mit der Verarbeitung ihrer personenbezogenen Daten nicht einverstanden sind. Außerdem sind im Datendschungelbuch eine Reihe von Musterschreiben enthalten, die von den Bürgern für die Wahrnehmung ihrer Rechte im Datenschutz verwendet werden können.

Weitere Online-Aktivitäten waren die Ergänzung der Website des Regierungspräsidiums Dresden mit einem speziellen Informations- und Kommunikationsangebot zum Thema „Datenschutz". Unter www.rp-dresden.de/ds/ ist eine eigene Homepage der Datenschutzaufsichtsbehörde erreichbar, die umfangreiche Informationen zum Datenschutz bereitstellt, Einblicke in die diesbezügliche Tätigkeit des Regierungspräsidiums Dresden gibt und darüber hinaus auch die Möglichkeiten zur Kontaktaufnahme mit der Aufsichtsbehörde quantitativ (neue Medien) und qualitativ (Vertraulichkeit) erweitert. Die für eine vertrauliche Kontaktaufnahme seitens der Internetnutzer notwendige Verschlüsselungssoftware (PGP) ist als Freeware kostenlos aus dem Internet zu beziehen.

Über die Präsentation auf der Website des RP Dresden hinaus ist noch auf zwei Veröffentlichungen in Printmedien hinzuweisen:

- IHK-Wirtschaftsdienst (Dresden), Heft 3/2001, S. 38: Was beim Auftrag an Dienstleister zu beachten ist
- RDV 2002, S. 266-270: Videoüberwachung von Geldautomaten (Abdruck der Internet-Veröffentlichung: http://www.rp-dresden.de/ds praxis/kontrolle_verkehrsbetriebe.pdf)

Die vorgehaltenen Informationsbroschüren, Formulare sowie Musterverträge und -dokumente sind ohne Ausnahme über die Website abrufbar bzw. zu ordern; die ständige Erreichbarkeit ist

durch einen Voice Mail Service sowie eine separate E-Mail-Adresse (datenschutz@rpdd.sachsen.de) gewährleistet.

- **ERFA-Kreis Sachsen**

Im Berichtszeitraum war die Zusammenarbeit mit der *Gesellschaft für Datenschutz und Datensicherung e. V. (GDD)*, insbesondere mit dem *GDD-ERFA-Kreis Sachsen (Erfahrungsaustauschkreis Sachsen der GDD)*, ein wesentlicher Schwerpunkt der Öffentlichkeitsarbeit. Die viermal jährlich stattfindenden ERFA-Kreis-Tagungen bieten Möglichkeiten eines zeitnahen und effektiven – vor allem auch persönlichen - Meinungsaustausches und eröffnen darüber hinaus die Möglichkeit für die Aufsichtsbehörden, ihren Ansprechpartnern in den Unternehmen wesentliche Aspekte der Aufsichtstätigkeit und Fachwissen zu vermitteln.

9 Ordnungswidrigkeiten

Die Zuständigkeit für die Ahndung von Ordnungswidrigkeiten nach dem BDSG ergibt sich aus der *Verordnung der Sächsischen Staatsregierung über die Regelung der Zuständigkeit der Aufsichtsbehörden i. V. m. § 38 Abs. 6 des Bundesdatenschutzgesetzes* vom 27. August 1991 (OwiZuVO, SächsGVBl. 1991, S. 324).

Im Berichtszeitraum wurden von den Aufsichtsbehörden *10 Ordnungswidrigkeitsverfahren*, jeweils wegen Verstößen gegen die Auskunftspflichten gem. § 38 Abs. 3 BDSG, durchgeführt. In einem Fall wurde ergänzend die unbefugte Erhebung und Übermittlung personenbezogener Daten geahndet.

Von den 10 Verfahren wurden
- 4 wieder eingestellt,
- 2 mit einem maximalen Verwarnungsgeld in Höhe von 75,00 DM (38,75 €) und
- 4 mit einem Bußgeld abgeschlossen.

Von den Verfahren richteten sich zwei gegen die Geschäftsführerin eines gem. § 32 BDSG 90 zum Register gemeldeten Unternehmens. Diese war durch die Aufsichtsbehörde mit der Aufforderung zur Mitteilung der nach einer Regelkontrolle getroffenen Maßnahmen angeschrie-

ben worden. Weder auf dieses Schreiben noch auf die nachfolgende Mahnung hatte die Geschäftsführerin reagiert. Erst nach Einleitung des Bußgeldverfahrens (Anhörung) wurde schließlich dem Auskunftsersuchen entsprochen. Die mit aktuellem Poststempel versehene Stellungnahme war mit einem mehrere Wochen zurückliegenden Datum (innerhalb der Frist des ersten Anschreibens) versehen und in mehreren Punkten unvollständig. Dieser Sachverhalt führte zu einem Bußgeld in Höhe von 1.000,00 DM (511,30 €). Ausgegangen wurde dabei von einer fahrlässigen Pflichtverletzung der Auskunftspflichten (weder rechtzeitige noch vollständige Auskunftserteilung). Der Bußgeldbescheid musste vollstreckt werden.

Die Aufsichtsbehörde richtete daraufhin ein insoweit aktualisiertes Auskunftsschreiben an die Geschäftsführerin. Nachdem wiederum keine Reaktion erfolgte, wurde ein weiteres Bußgeldverfahren eröffnet und - mangels Reaktion von Seiten der Adressatin - mit einem Bußgeld in Höhe von 1.500,00 € abgeschlossen. Ausgegangen wurde nunmehr von einer vorsätzlichen Pflichtverletzung der Auskunftspflichten (Unterlassen der Auskunftserteilung).
Ein Bußgeldverfahren betrifft den unter 4.3.8 geschilderten Fall (Webcam auf einem Supermarktparkplatz). Gegen den Betreiber wurden Bußgelder wegen Auskunftsverweigerung (200 €) sowie wegen unbefugter Datenerhebung und -übermittlung (500 €) verhängt. Der Bußgeldbescheid befindet sich derzeit in der Vollstreckung.

10 Zusammenarbeit der Aufsichtsbehörden

- **Zusammenarbeit der sächsischen Aufsichtsbehörden:**

In gemeinsamen Beratungen zwischen dem Sächsischen Staatsministerium des Innern und den Regierungspräsidien wurden zweimal jährlich datenschutzrechtliche Schwerpunktthemen erörtert, Erfahrungen aus der praktischen Tätigkeit ausgetauscht sowie über Neuerungen auf dem Gebiet des Datenschutzes im nicht-öffentlichen Bereich auf Bundes- und Europaebene informiert.

Auch die Regierungspräsidien untereinander haben im Berichtszeitraum den fachspezifischen Erfahrungsaustausch gesucht. Zu verweisen ist insbesondere auf die Durchführung der ersten koordinierten Datenschutzkontrolle (vgl. 4.2.3) im Jahre 2002.

- **Zusammenarbeit mit Aufsichtsbehörden anderer Länder:**

Die einzelfallbezogene Zusammenarbeit mit anderen Aufsichtsbehörden der Länder im Berichtszeitraum beschränkte sich im Wesentlichen auf gegenseitige Unterrichtungen sowie den informellen Meinungsaustausch zu speziellen fachlichen Problemstellungen.
So wurde mehrmals von der Befugnis zur Unterrichtung anderer Aufsichtsbehörden Gebrauch gemacht (§ 38 Abs. 1 Satz 3 BDSG). Dies betrifft u. a. den unter Pkt. 4.3.10 dargestellten Fall, da aus den Unterlagen hervorging, dass ein weiterer Stempelhersteller in Thüringen den gleichen Musterkatalog nutzte. Ein weiteres Beispiel ist die unter dem Aspekt „Datenverarbeitung für Werbezwecke“ (vgl. 4.3.15) in einem Möbelhaus durchgeführte Anlasskontrolle. Da in diesem Zusammenhang auch Nebenerkenntnisse über weitere Datenschutzverletzungen (unwirksame Bestellung eines Datenschutzbeauftragten, fehlende Verpflichtung auf das Datengeheimnis, nicht vorhandenes Verfahrensregister) festgestellt wurden und darüber hinaus bekannt war, dass in anderen Bundesländern gleich firmierte Möbelhäuser mit einer identischen Geschäftsführung agierten, wurden die jeweils örtlich zuständigen Aufsichtsbehörden über die bisherigen Erkenntnisse und das Vorgehen entsprechend informiert.

- **Düsseldorfer Kreis:**

Mit dem Ziel der bundesweit *möglichst einheitlichen Rechtsanwendung der datenschutzrechtlichen Vorschriften* für den nicht-öffentlichen Bereich haben die Länder ein Abstimmungsgremium - den sogenannten *Düsseldorfer Kreis* - eingerichtet.

Mitglieder des Düsseldorfer Kreises sind mehrheitlich Vertreter der obersten Aufsichtsbehörden der Länder, so auch das Sächsische Staatsministerium des Innern, teilweise entsprechend beauftragte Vertreter der Landesdatenschutzbeauftragten, soweit sie zuständige Aufsichtsbehörde für den nicht-öffentlichen Bereich sind, sowie der Bundesbeauftragte für den Datenschutz, der bundesweit für den Telekommunikationsbereich zuständig ist.

Die *Beschlüsse* des Düsseldorfer Kreises haben empfehlenden Charakter und sind für die Datenschutzkontrollen der Aufsichtsbehörden der Länder eine geeignete *Grundlage für die Anwendung der Vorschriften des BDSG im nicht-öffentlichen Bereich*.

Vorbereitet werden die Beschlüsse von den fachspezifischen *Arbeitsgruppen* des Düsseldorfer Kreises (AG Auskunfteien, AG Kreditwirtschaft, AG Telekommunikation, Tele- und Mediendienste, AG Versicherungswirtschaft und AG Internationaler Datenverkehr) unter Beteiligung der jeweiligen Spitzenverbände der Wirtschaft. Das Sächsische Staatsministerium des Innern ist in den ersten drei der o.a. Arbeitsgruppen vertreten.

Der Düsseldorfer Kreis tagt zweimal jährlich, die Arbeitsgruppen nach Bedarf ein- bis zweimal jährlich.

Im Rahmen der Umsetzung der Datenschutzrichtlinie der Europäischen Gemeinschaft im Bundesdatenschutzgesetz hat der Düsseldorfer Kreis zahlreiche Vorschläge erarbeitet. Die Novellierung des Bundesdatenschutzgesetzes sowie der Landesdatenschutzgesetze und die Entwicklung eines einheitlichen Datenschutzstandards in den EG-Mitgliedstaaten waren Schwerpunkte in den Beratungen des Düsseldorfer Kreises.

Darüber hinaus wurden insbesondere die folgenden Schwerpunktthemen erörtert und Positionen dazu erarbeitet:

- *2. Stufe der BDSG-Novellierung*

  Nach der Novellierung des BDSG 2001 steht die 2. Stufe der Novellierung des BDSG an. Im Auftrag des BMI wurde dazu ein Gutachten mit dem Titel „Modernisierung des Datenschutzrechts“ (abrufbar unter http://www.datenschutz-berlin.de als pdf Datei) erstellt.

- *Leitfaden für bankenspezifische datenschutzrechtliche Probleme nach der Novellierung des Bundesdatenschutzgesetzes*

  Im Leitfaden werden die Regelungen des BDSG erläutert, die im Zusammenhang mit dem Bankgewerbe stehen. Der Leitfaden wurde mit den Aufsichtsbehörden abgestimmt.

- *Datawarehouse, Datamining bei Banken*

  Der zunehmende technische Fortschritt in der Informations- und Kommunikationstechnik ermöglicht in weitaus größerem Maße als bisher die Sammlung und Verar-

beitung von personenbezogenen Daten in der Wirtschaft, vor allem im Kreditbereich. Dadurch ergeben sich in erheblichem Umfang datenschutzrechtliche Probleme.

Im *Datawarehouse-System* können alle verwendbaren Daten in einem einheitlichen Datenbestand, losgelöst von ihrer ursprünglichen Verwendung, zusammengeführt werden. Dies widerspricht dem Grundsatz der Zweckbindung der Verarbeitung personenbezogener Daten. *Datamining* eröffnet die Möglichkeit, scheinbar zusammenhanglose Daten nach im Einzelfall festzulegenden, wissenswerten Zusammenhängen zu durchsuchen, zu kombinieren und damit neue Informationen zu erlangen.

Datenschutzrechtliche Probleme sind je nach Einzelfall zu beurteilen und treten in Zusammenhang mit der Zweckbestimmung der Daten, der Einwilligung des Kunden und Datenübermittlung an andere Unternehmen auf.

- *Rabattkartensysteme*

  Rabattkartensysteme werden zur Kundenbindung in einer Reihe großer Unternehmen eingesetzt. Dem Kunden wird es ermöglicht, ein Guthaben anzusammeln, das später in Sachprämien oder Bargeld eingelöst werden kann. Aus datenschutzrechtlicher Sicht bedeutsam ist hier, dass aufgrund der gesammelten Verkaufsdaten detaillierte Kundenprofile erstellt werden können. Daher muss der Kunde in seiner Einwilligungserklärung darüber aufgeklärt werden, in welchen Fällen und an welche Adressaten seine Daten weitergegeben werden können und für welche Zwecke die Daten übermittelt werden.

- *Elektronisches Mediendienstegesetz*

  Bisher sind Regelungen zum Schutz personenbezogener Daten für den Bereich der elektronischen Medien in verschiedenen, inhaltlich jedoch weitgehend übereinstimmenden Regelungen auf Bundes- und Länderebene enthalten. Das Elektronische Mediendienstegesetz soll diese Bestimmungen nun in *einem* Gesetz zusammenführen.

- *Schufa-Verträge mit Wohnungsunternehmen*

  Wohnungsunternehmen können Vertragsmitglied der Schufa werden. Sofern Mietverhältnisse nicht vertragsgemäß beendet werden, z. B. wenn ein Mieter keine Miete mehr zahlt, ergeht eine Meldung an die Schufa. Gegenstand der Diskussion ist vor al-

lem, welche Kriterien an die Schufa gemeldet werden. Z. B. ist es nicht ohne weiteres gleichzusetzen, dass die Zahlung der Miete wegen Mietmängeln zu einem Teil verweigert wurde oder dass ein vom Mieter verschuldetes Zahlungsversäumnis über mehrere Monate vorliegt.

- *Unternehmensregelungen bei Datenübermittlung in Drittstaaten*

  Bei Datenübermittlung in Drittstaaten stellen sich umfangreiche Rechtsfragen, sofern im Drittstaat kein angemessenes Datenschutzniveau gegeben ist.

- *Videoüberwachung in öffentlichen Verkehrsbetrieben*

  Mit dem Verband Deutscher Verkehrsunternehmen wurde abgestimmt, unter welchen Voraussetzungen eine Videoüberwachung in Verkehrsbetrieben möglich ist.

- **Workshops der Datenschutzaufsichtsbehörden:**

Von besonderer Bedeutung sind die jährlich durchgeführten Workshops der Datenschutzaufsichtsbehörden - ein Gremium des Erfahrungsaustausches. 2001 fand der Workshop beim Berliner Beauftragten für Datenschutz und Informationsfreiheit und 2002 im Innenministerium Mecklenburg-Vorpommern statt.

11 Ausblick

Folgende Schwerpunktthemen werden auf dem Gebiet des Datenschutzes im nichtöffentlichen Bereich auch weiterhin Gegenstand der Diskussion sein:

- *Grundlegende Reform des Datenschutzrechts*
  2. Stufe der Novellierung des BDSG (vgl. S. 63)

- *Einzelfragen zur Auslegung des BDSG,*
  wie z. B. Fragen aus der Werbewirtschaft, insbesondere inwieweit auf das Widerspruchsrecht gemäß § 28 Abs. 4 S. 2 BDSG hingewiesen werden muss.

- *Neuordnung des IUK- Datenschutzrechts im Bundesrecht*

- *Erweiterung der Schufa-Geschäftsfelder*

- *Einwilligungen*
  Schweigepflichtentbindungserklärungen bei Versicherungen

- *Übermittlung personenbezogener Daten in Drittländer,*
  z. B. Übermittlung von Arbeitnehmerdaten

Abkürzungsverzeichnis:

AO	Abgabenordnung vom 16. März 1976 BGBl I 1976, 613 (1977, 269), Neugefasst durch Bekanntmachung vom 1.10.2002 I 3866; 2003 I 61, geändert durch Art. 6 G vom 31. 7.2003 I 1550
BDSG 77	Bundesdatenschutzgesetz vom 27.01.1977 (BGBl. II S. 201)
BDSG 90	Bundesdatenschutzgesetz vom 20.12.1990, zuletzt geändert durch Gesetz vom 17.12.1997, (BGBl. I S. 3108)
BDSG/ BDSG 01	Bundesdatenschutzgesetz, neugefasst durch Bekanntmachung vom 14. Januar 2003 (BGBl. 2003 S. 67-88)
BGH	Bundesgerichtshof
BMI	Bundesministerium des Innern
DV	Datenverarbeitung
EBE	Erhöhtes Beförderungsentgelt
Erfa-Kreis	Erfahrungsaustausch-Kreis
GDD	Gesellschaft für Datenschutz und Datensicherung e. V.
GWG	Geldwäschegesetz vom 25. Oktober 1993 (BGBl I 1993, 1770), geändert durch Art. 1 G v. 08.08.2002 I 3105
IHK	Industrie- und Handelskammer
MDStV	Mediendienste-Staatsvertrag, zuletzt geändert durch Artikel 3 des Sechsten Staatsvertrages zur Änderung des Rundfunkstaatsvertrages, des Rundfunkfinanzierungsstaatsvertrages und des Mediendienste-Staatsvertrages (Sechster

	Rundfunkänderungsstaatsvertrag) vom 20. Dezember 2001 (GVBl. Berlin 2002, S. 162)
NJW	Neue Juristische Wochenschrift
PassG	Passgesetz vom 3. Dezember 2001 (BGBl I 2001, 3274, 3275), Zuletzt geändert durch Art. 13 G v. 21.08.2002 I 3322
PersAuswG	Personalausweisgesetz vom 21. April 1986, geändert druch Art. 1 ÄndG vom 30.07.1996(BGBl. II S. 1182) und Art. 3 § 6 Nr. 1 G zur Reform des Staatsangehörigkeitsrechts vom 15.7.1999 (BGBl. I S. 1618)
PIN	Persönliche Identifikations-Nummer
RDV	Recht der Datenverarbeitung
RP	Regierungspräsidium
SächsDSG	Sächsisches Datenschutzgesetz Vom 11. Dezember 1991 (SächsGVBl S. 401), geändert am 7. April 1997 (SächsGVBl S. 351)
TDDSG	Teledienste-Datenschutzgesetz vom 22. Juli 1997 (BGBl I 1997, 1870, 1871), geändert durch Art. 3 und 4 Abs. 2 G vom 14.12.2001 I 3721
TDG	Teledienstgesetz vom 22. Juli 1997 (BGBl I 1997, 1870), zuletzt geändert durch Art. 1 und 4 Abs. 1 G v. 14.12.2001 I 3721
TKÜV	Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation vom 22. Januar 2002, geändert durch erste Verordnung zur Änderung der Telekommunikations-Überwachungsverordnung vom 16. August 2002 (BGBl. I S. 3317),
UWG	Gesetz gegen den unlauteren Wettbewerb vom 7. Juni 1909 (RGBl 1909, 499), zuletzt geändert durch Art. 6 G v. 23. 7.2002 I 2850

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.