2. Tätigkeitsbericht

für den Datenschutz im nicht-öffentlichen Bereich

Berichtszeitraum: 2003-2004

Impressum

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

INHALTSVERZEICHNIS

1 Einleitung

Das Sächsische Staatsministerium des Innern als oberste Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich erfüllt mit diesem Bericht die Verpflichtung, die Öffentlichkeit alle zwei Jahre über die Tätigkeit der Aufsichtsbehörden zu informieren.

Der Bericht gibt insbesondere Auskunft über die Aufgaben der Aufsichtsbehörden sowie die Schwerpunkte der Kontrolltätigkeit in den Jahren 2003 und 2004. Dabei wird auf einige ausgewählte Fälle aus der Kontrollpraxis ausführlich eingegangen.

Die im Berichtszeitraum durchgeführten Kontrollen haben immer wieder gezeigt, dass bei den Unternehmen teilweise noch beträchtliche Unsicherheiten bei der datenschutzgerechten Verarbeitung personenbezogener Daten bestehen. Die Aufsichtsbehörden sehen als Gründe dafür einerseits die verbreitete Unkenntnis über die datenschutzrechtlichen Grundlagen sowie andererseits auch mangelnde Sensibilität beim Umgang mit personenbezogenen Daten. So war in einer Vielzahl kontrollierter Unternehmen kein betrieblicher Datenschutzbeauftragter bestellt, obwohl die Voraussetzungen für die gesetzliche Pflicht zur Bestellung eines Datenschutzbeauftragten vorlagen. Aber gerade der betriebliche Datenschutzbeauftragte ist eine für den Datenschutz wichtige Institution, indem er im Unternehmen über datenschutzrechtliche Inhalte informiert, sachkundig die geplanten Datenverarbeitungsverfahren beurteilt und die Einhaltung des Datenschutzes kontrolliert.

Die Aufsichtsbehörden haben auch in diesem Berichtszeitraum im Rahmen ihrer Beratungstätigkeit wieder sehr viele Anfragen von betrieblichen Datenschutzbeauftragten, Unternehmern, Betriebsräten sowie Vereinen und Verbänden beantwortet und so dazu beigetragen, Datenschutzverstöße von vornherein vermeiden zu helfen. Wandten sich Betroffene an die Aufsichtsbehörden, so wurden sie bei der Wahrnehmung ihrer Datenschutzrechte gegenüber nicht-öffentlichen Stellen wirksam unterstützt.

Im Rahmen der Kontrolltätigkeit deckten die Aufsichtsbehörden datenschutzrechtliche Mängel auf und gaben den Unternehmen Hinweise und Empfehlungen, welche Maßnahmen zur Gewährleistung des Datenschutzes erforderlich sind. Als besonders wirksames Kontrollinstrument haben sich vor allem die so genannten „koordinierten Datenschutzkontrollen“ erwiesen, die gemeinsam von allen Sächsischen Regierungspräsidien in Abstimmung mit dem Sächsischen Staatsministerium des Innern vorbereitet und durchgeführt werden. Innerhalb

einer Branche werden dabei stichprobenartig ausgewählte Unternehmen nach einheitlichen Kriterien überprüft. Im Berichtszeitraum wurden auf diese Weise 48 Altenpflegeheime und 46 Wohnungsunternehmen kontrolliert. Die Erfahrungen zeigen, dass durch den Erfahrungsaustausch innerhalb einer Branche selbst Unternehmen, die nicht unmittelbar kontrolliert wurden, für die Belange des Datenschutzes sensibilisiert werden und Veränderungen vornehmen.

Das Zusammenwirken von Aufsichtsbehörden und Unternehmen im Berichtszeitraum wird als positiv bewertet. Die Hinweise der Aufsichtsbehörden wurden von den Unternehmen zum großen Teil beachtet und vorgeschlagene Maßnahmen zur Verbesserung des Datenschutzniveaus meist unverzüglich umgesetzt.

Auch in Zukunft wird die datenschutzrechtliche Kontrolle von Auskunfteien vor dem Hintergrund weiter fortschreitender Vernetzung von Datenübermittlungen ein wichtiges Thema bleiben. Beispielhaft seien hier die Erweiterung der SCHUFA-Geschäftsfelder (u. a. um den Bereich der gewerblichen Wohnungswirtschaft) und die Zusammenarbeit von Unternehmen der Versicherungsbranche mit Auskunfteien genannt. Auch die Anpassung des Datenschutzes an die rasante Weiterentwicklung der elektronischen Datenverarbeitung und der Kommunikationstechnik wird weiterhin einen Schwerpunkt der Arbeit im nicht-öffentlichen Bereich bilden.

2 Datenschutz und Aufsicht im nicht-öffentlichen Bereich

Das Sächsische Staatsministerium des Innern ist *oberste Aufsichtsbehörde* für den Datenschutz im nicht-öffentlichen Bereich. Damit obliegt ihm die *Fachaufsicht* über die für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden in Sachsen. Dies sind die Regierungspräsidien Chemnitz, Dresden und Leipzig. Außerdem wirkt das Sächsische Staatsministerium des Innern 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).

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 (BDSG) 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 nicht automatisierten Dateien.

Die zuständigen Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben gemäß den Bestimmungen des BDSG die folgenden Aufgaben:

- **Wahrnehmung der Kontrollkompetenzen**

- Durchführung von Anlass- und Regelkontrollen (§ 38 Abs. 1 Satz 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 Satz 3 und 4 BDSG)
- Führung des öffentlichen Registers meldepflichtiger Verarbeitungen (§ 38 Abs. 2 BDSG)
- Herausgabe regelmäßiger Tätigkeitsberichte (§ 38 Abs. 1 Satz 6 BDSG)

- **Durchsetzungs-/Sanktionsmaßnahmen nach pflichtgemäßem Ermessen**

- Durchführung von Bußgeldverfahren nach § 43 BDSG
- Eigenständiges Strafantragsrecht bei BDSG-Straftatbeständen (§ 44 Abs. 2 BDSG)
- Unterrichtung des Betroffenen und Anzeige der für den Verstoß verantwortlichen Stelle bei den zuständigen Ahndungs- und Verfolgungsbehörden (§ 38 Abs. 1 Satz 4 BDSG)
- Verhängung von Zwangsgeldern zur Durchsetzung angeordneter Maßnahmen zur Mängelbeseitigung bzw. Verbot des Einsatzes einzelner Verfahren (§ 38 Abs. 5 Satz 1 und 2 BDSG)
- Aufforderung zur Abberufung des betrieblichen Datenschutzbeauftragten (§ 38 Abs. 5 Satz 3 BDSG)

- **Auf Antrag der verantwortlichen Stelle/des Datenschutzbeauftragten**

- Allgemeine Unterstützung des Datenschutzbeauftragten (§ 4g Abs. 1 Satz 2 BDSG), Beratungstätigkeit
- Mitwirkung bei der Vorabkontrolle (§ 4d Abs. 6 Satz 3 BDSG)
- Überprüfung vorgelegter Verhaltensregelungen (§ 38a BDSG)
- Genehmigungsverfahren bei Datentransfer in Nicht-EU/EWR-Staaten ohne angemessenes Datenschutzniveau (§ 4c Abs. 2 BDSG)

Darüber hinaus ist das Regierungspräsidium Dresden auch zuständige Aufsichtsbehörde für die Verfolgung von datenschutzrechtlichen Ordnungswidrigkeiten nach dem Mediendienste-Staatsvertrag im gesamten Freistaat Sachsen (vgl. Artikel 1 des Gesetzes zur Änderung des Sächsischen Gesetzes zum Staatsvertrag über Mediendienste und zur Änderung rundfunkrechtlicher Vorschriften im Freistaat Sachsen sowie zur Änderung des Gesetzes über den privaten Rundfunk und neue Medien in Sachsen vom 21.03.03 [SächsGVBl. 2003, S. 37]).

3 Verfahrensregister (§ 38 Abs. 2 BDSG)

Die Regierungspräsidien führen ein Register über alle nach § 4d BDSG meldepflichtigen Verfahren der automatisierten Datenverarbeitung. Meldepflichtig sind 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 höchstens vier Arbeitnehmer mit der automatisierten Datenverarbeitung für eigene Zwecke beschäftigen, diese Datenverarbeitung weder durch die Einwilligung der Betroffenen noch durch die Zweckbestimmung eines Vertragsverhältnisses begründet ist, und im Übrigen auch keine Vorabkontrolle erforderlich ist.

Die bei den Regierungspräsidien geführten Verfahrensregister sind öffentlich und können von jedermann eingesehen werden. Das Einsichtsrecht erstreckt sich jedoch nicht auf die Angaben nach § 4e Satz 1 Nr. 9 BDSG (Datensicherungsmaßnahmen/Sicherheitskonzept) sowie auf die Angabe der zugriffsberechtigten Personen. Im Berichtszeitraum wurden keine entsprechenden Auskunftsbegehren an die Aufsichtsbehörden herangetragen.

Im letzten Tätigkeitsbericht wurde aufgrund der Tatsache, dass bis dahin nur wenige Markt- und Meinungsforschungsunternehmen im Register gemeldet waren, die Vermutung geäußert, dass in diesem Bereich einige Unternehmen bislang ihrer Meldepflicht noch nicht nachgekommen seien. Das Regierungspräsidium Dresden hat im Berichtszeitraum deshalb öffentlich zugängliche Quellen, wie z. B. Branchenbücher, ausgewertet. Es wurden dabei fünf Unternehmen ermittelt, die ihrer Meldepflicht bislang noch nicht nachgekommen waren. Die erforderliche Meldung wurde nach entsprechender Aufklärung der Unternehmen durch die Aufsichtsbehörde dann umgehend eingereicht.

Die folgende Übersicht gibt Aufschluss über die Anzahl der in den Regierungspräsidien gemeldeten Unternehmen im Verfahrensregister:

	Anzahl Unternehmen (Stichtag 31.12.2004)	Bemerkungen
RP Chemnitz:	**7**	
davon : - Wirtschaftsauskunfteien - Markt- und Meinungsforschungsunternehmen - Warndateibetreiber - Sonstige	5 0 1 1	
RP Dresden:	**10**	
davon : - Wirtschaftsauskunfteien - Markt- und Meinungsforschungsunternehmen	4 6	
RP Leipzig:	**16**	
davon : - Wirtschaftsauskunfteien - Markt- und Meinungsforschungsunternehmen - Adress- bzw. Datenhändler	5* 7 5*	* ein Unternehmen ist in beiden Bereichen tätig
Sachsen gesamt:	**33**	

4 Kontrolltätigkeit der Regierungspräsidien

4.1 Rechtsgrundlage

Die Sächsischen Regierungspräsidien kontrollieren gemäß § 38 Abs. 1 Satz 1 BDSG die Ausführung des Bundesdatenschutzgesetztes sowie anderer datenschutzrechtlicher Vorschriften, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln. Im Rahmen dieser Aufsichtstätigkeit werden u. a. anlassfreie Kontrollen (Regelprüfungen) und Anlasskontrollen durchgeführt.

4.2 Regelkontrollen

4.2.1 Überblick

Während bei der Anlasskontrolle regelmäßig ein konkreter Anhaltspunkt für eine mögliche Verletzung datenschutzrechtlicher Vorschriften gegeben ist, handelt es sich bei einer Regelkontrolle zunächst um eine Routineüberprüfung. Die unterschiedlichen Ansatzpunkte wirken sich auch auf den Kontrollumfang aus: Während bei Anlasskontrollen der zu überprüfende Einzelfall im Vordergrund steht, betreffen Regelkontrollen entweder ausgewählte Teilaspekte oder aber die Datenverarbeitung eines Unternehmens insgesamt.

Im Berichtszeitraum lag der Schwerpunkt der anlassfreien Kontrolltätigkeit der Aufsichtsbehörden vor allem auf den von allen drei Regierungspräsidien in Abstimmung mit dem Sächsischen Staatsministerium des Innern durchgeführten koordinierten Datenschutzkontrollen in Altenpflegeheimen und Wohnungsunternehmen.

Koordinierte Datenschutzkontrollen wurden erstmals im Jahr 2002 durchgeführt (siehe 1. TB, Pkt. 4.2.3). Sie haben sich seitdem als wirksames Instrument zur Verbesserung des Datenschutzes in den Unternehmen der für die Kontrolle ausgewählten Branchen erwiesen. Durch die stichprobenartigen, nach einheitlichen Kriterien erfolgten Überprüfungen konnten der unternehmensbezogene Prüfaufwand der Aufsichtsbehörden (Vorbereitung, Durchführung, Auswertung) erheblich reduziert und gleichzeitig eine beachtliche Breitenwirkung erzielt werden. Die Erfahrungen zeigen insbesondere, dass sich die Unternehmen einer Branche über die von den Aufsichtsbehörden durchgeführten Kontrollen untereinander austauschen und so auch Unternehmen, die nicht unmittelbar kontrolliert werden, für die Belange des Datenschutzes sensibilisiert werden und selbst Maßnahmen zur Verbesserung ihres Datenschutzniveaus ergreifen. Durch die Veröffentlichung der Auswertungen der Kontrollaktionen durch die Aufsichtsbehörden werden die Unternehmen regelmäßig auch über die Landes- und Unternehmensverbände über datenschutzrechtliche Themen informiert.

Die überwiegende Anzahl der Kontrollen wurde im schriftlichen Verfahren durchgeführt. So wurden die im Rahmen der koordinierten Datenschutzkontrollen überprüften Unternehmen zunächst aufgefordert, einen Fragebogen zu beantworten. Bei zahlreichen Kontrollen ergab sich darüber hinaus aber auch die Notwendigkeit der Prüfung vor Ort.

Vor-Ort-Kontrollen haben sich vor allem dann als effektiver und ergebnisorientierter als Kontrollen im schriftlichen Verfahren erwiesen, wenn die Einhaltung technisch-organisatorischer Maßnahmen in Unternehmen kontrolliert werden sollte, in denen vielfältige Hard- und Softwarekonfigurationen angewendet werden oder besondere räumliche Bedingungen vorherrschen.

Einige Kontrollen im Berichtszeitraum wurden auch im automatisierten Verfahren vollzogen.

Im Ergebnis der durchgeführten Kontrollen haben die Unternehmen den Empfehlungen/Beanstandungen der Aufsichtsbehörden im Wesentlichen durch entsprechende Maßnahmen Rechnung getragen. Anordnungen gem. § 38 Abs. 5 BDSG mussten durch die Aufsichtsbehörden nicht getroffen werden.

Die folgende Übersicht gibt Aufschluss über die Anzahl der von den Aufsichtsbehörden durchgeführten Regelüberprüfungen nach Branchen und verdeutlicht zugleich die Entwicklung gegenüber dem vorigen Berichtszeitraum:

Branchen	**2001 - 2002**	**2003 - 2004**	**Summe**
Altenpflegeheime	**0**	**48**	48
Wohnungsunternehmen	**0**	**46**	46
Auftragsdatenverarbeiter	**10**	**1**	11
Sparkassen/Banken	**30**	**0**	30
Verkehrsunternehmen	**56**	**3**	59
Versorgungsunternehmen	**3**	**7**	10
Sonstige	**2**	**5**	7
gesamt:	**101**	**110**	**211**

Zu den in der Übersicht aufgeführten Regelkontrollen 2003 - 2004 ist anzumerken:

- *Altenpflegeheime*

  Auf die ausführlichen Ausführungen zu dieser koordinierten Datenschutzkontrolle unter Pkt. 4.2.2 wird verwiesen.

- *Wohnungsunternehmen*

  Mit dieser koordinierten Datenschutzkontrolle wurde 2004 begonnen. Der Abschluss der Kontrollaktion ist für das Jahr 2005 vorgesehen; ein Zwischenbericht ist unter Pkt 4.2.3 enthalten.

- *Auftragsdatenverarbeiter*

  Die Kontrolle des im Bereich der Lohnabrechung tätigen Dienstleistungsunternehmens hatte ihren Ausgangspunkt in der koordinierten Datenschutzkontrolle von Altenpflegeheimen (s. u.). Im Rahmen der routinemäßigen Überprüfung der Vorgaben des § 11 BDSG (Auftragsdatenverarbeitung) bei einem Heimträger wurde der Aufsichtsbehörde u. a. ein Vertrag mit diesem Auftragsdatenverarbeiter vorgelegt. Ausschlaggebend für die Durchführung einer Vollprüfung war die Tatsache, dass dieses Unternehmen offensichtlich schon vor der Novellierung des BDSG im Jahr 2001 am Markt agiert hatte, seinerzeit jedoch entgegen der damaligen Meldepflicht nicht im Register nach § 32 BDSG90 aufgeführt war.

- *Verkehrsunternehmen*

  Die Kontrollen von drei kleineren Busunternehmen (Linien- und Reiseverkehr) erfolgten in Ergänzung der im Jahr 2002 durchgeführten Branchenkontrolle bei Verkehrsunternehmen (vgl. 1. TB, Pkt. 4.2.3) und waren als Grundprüfung angelegt. Überprüft wurden insbesondere die Problemkreise „Verpflichtung auf das Datengeheimnis“, „betrieblicher Datenschutzbeauftragter“ und „öffentliches Verfahrensverzeichnis“. Die Schwerpunkte der bereits erwähnten Branchenkontrolle bei Verkehrsunternehmen (erhöhtes Beförderungsentgelt, Videoüberwachung) waren für diese Unternehmen nicht relevant.

- *Versorgungsunternehmen*

  Hierbei handelt es sich um automatisierte Prüfungen der Websites dieser Unternehmen - für weitere Informationen wird auf Pkt. 4.2.4 verwiesen.

- *Sonstige Unternehmen*

  Bei den unter dem Punkt „Sonstige“ aufgeführten Prüfungen handelt es sich um

- drei Betreiber von Erlebnisrestaurants (Schwerpunktprüfungen - Videoüberwachung, vgl. 1. TB, Pkt. 4.3.7),
- einen Landesverband der freien Wohlfahrtspflege (Grundprüfung - §§ 4f, 4g und 5 BDSG) sowie
- ein Möbelhaus (Schwerpunktprüfung - Verarbeitung von Kundendaten).

4.2.2 Koordinierte Datenschutzkontrolle von Altenpflegeheimen

In Abstimmung mit dem Sächsischen Staatsministerium des Innern sind beginnend ab Januar 2003 durch die drei Regierungspräsidien insgesamt 48 Altenpflegeheime einer schriftlichen datenschutzrechtlichen Kontrolle ausgewählter Datenverarbeitungsbereiche unterzogen worden. Neben allgemeinen datenschutzrechtlichen Anforderungen (z. B. betrieblicher Datenschutzbeauftragter, Verpflichtung auf das Datengeheimnis, öffentliches Verfahrensverzeichnis) wurden insbesondere Fragen der Vertragsgestaltung, der Löschfristen sowie Aspekte der Videoüberwachung in die Kontrolle einbezogen.

Die wesentlichen Ergebnisse der Überprüfung sind den nachfolgenden Ausführungen zu entnehmen; eine ausführlichere Auswertung ist darüber hinaus auch von der Website des Regierungspräsidiums Dresden abrufbar:

http://www.rp-dresden.de/ds/praxis/altenpflegeheime.pdf

Datenschutzbeauftragter:

§ 4 f Abs. 1 Satz 1 und 4 BDSG regelt, dass nicht-öffentliche Stellen, die mehr als vier Arbeitnehmer mit der automatisierten Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigen, einen Datenschutzbeauftragten zu bestellen haben. Das Gleiche gilt, wenn personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 20 Personen beschäftigt sind.

Diese Pflicht trifft regelmäßig die verantwortliche Stelle (juristische Person), d. h. in diesem Fall nicht das rechtlich unselbstständige Altenpflegeheim, sondern dessen Träger. Nur in seltenen Fällen ist der Träger mit dem Altenpflegeheim identisch; im Regelfall, insbesondere bei Einrichtungen der freien Wohlfahrtspflege, betreibt der Träger noch verschiedene andere Einrichtungen (z. B. Kindertageseinrichtungen, Begegnungsstätten) und bietet weitere Dienstleistungen (z. B. Essen auf Rädern, Schuldnerberatung, Fahrdienst etc.) an. Mithin ist bei der

Ermittlung der o. g. Beschäftigtenzahlen nicht nur das Altenpflegeheim zu betrachten, vielmehr sind alle Geschäftsbereiche des Trägers maßgeblich.

Die Kontrolle ergab unter anderem, dass in vielen Einrichtungen der Inhalt des Begriffes „Personenbezogene Daten“ nicht bekannt war und auch nicht klar aufgezeigt werden konnte, an welchen Stellen bei den Heimträgern personenbezogene Daten verarbeitet werden.

Nach § 3 Abs. 1 BDSG sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Im Bereich von Altenpflegeheimen sind dies nicht nur die Daten der Heimbewohner, sondern die Daten aller natürlichen Personen, mit denen der Träger in Berührung kommt, also auch die Daten über

- Mitarbeiter des Heimes bzw. dessen Trägers (Beschäftigte),
- Mitglieder des Trägers (soweit als Verein organisiert),
- Gesellschafter des Trägers (soweit als GmbH organisiert),
- Kunden (aller stationären/ambulanten Einrichtungen bzw. Dienstleistungen, z. B. Heimbewohner, Beratungskunden, Nutzer von Kindertageseinrichtungen),
- ehrenamtlich tätige Personen,
- Sponsoren (soweit keine juristischen Personen),
- Geschäftspartner (soweit keine juristischen Personen, z. B. Handwerker).

Die Voraussetzungen für die Pflicht zur Bestellung eines Datenschutzbeauftragten dürften somit fast immer erfüllt sein. So bestand nach Prüfung der Fragebögen für alle 15 im Regierungsbezirk Dresden kontrollierten Heime die Pflicht zur Bestellung eines Datenschutzbeauftragten. Die Auswertung der ersten eingegangenen Stellungnahmen ergab jedoch, dass nur in fünf Heimen bzw. bei deren Trägern tatsächlich ein Datenschutzbeauftragter bestellt war. Auf Betreiben der Aufsichtsbehörde ist inzwischen in allen 15 Einrichtungen bzw. bei deren Trägern ein Datenschutzbeauftragter bestellt worden.

Die durchgeführten Kontrollen hat ein sächsischer Landesverband der Freien Wohlfahrtspflege zum Anlass genommen, alle sächsischen Kreisverbände sowie ausgegliederten Gesellschaften daraufhin zu überprüfen, ob ein betrieblicher Datenschutzbeauftragter bestellt werden muss. Dabei wurde auch auf die Möglichkeit der Bestellung eines externen Datenschutzbeauftragten hingewiesen.

Von einem anderen Landesverband ist die Aufsichtsbehörde auf dessen Geschäftsführerkonferenz eingeladen worden, um den dort anwesenden Verantwortlichen der Orts- und Kreis-

verbände die datenschutzrechtlichen Grundanforderungen an Einrichtungen der freien Wohlfahrtspflege zu verdeutlichen sowie unmittelbar auftretende Fragen zu beantworten. Bei dieser Gelegenheit wurde die Aufsichtsbehörde auch darüber unterrichtet, dass verbandsintern bereits zentrale Weiterbildungsveranstaltungen für betriebliche Datenschutzbeauftragte anberaumt worden waren.

Öffentliches Verfahrensverzeichnis/Interne Verarbeitungsübersicht:

Gemäß § 4 g Abs. 2 Satz 1 BDSG ist dem Datenschutzbeauftragten für jedes automatisierte Verfahren eine Übersicht über die Angaben nach § 4e Satz 1 BDSG sowie über die zugriffsberechtigten Personen zur Verfügung zu stellen (interne Verarbeitungsübersicht). Diese Dokumentation ist ein wesentliches Kontrollinstrument des betrieblichen Datenschutzbeauftragten. Auf ihrer Basis

- realisiert er seine Überwachungsaufgaben hinsichtlich der ordnungsgemäßen Anwendung von Datenverarbeitungsprogrammen,
- prüft er, ob eine Vorabkontrolle erforderlich ist und führt diese gegebenenfalls durch,
- erstellt und aktualisiert er das öffentliche Verfahrensverzeichnis.

Der Datenschutzbeauftragte hat dann die Angaben nach § 4e Satz 1 Nr. 1 - 8 BDSG auf Antrag jedermann in geeigneter Weise verfügbar zu machen. Ziel dieser Regelung ist es, jedem Bürger das Recht zu gewähren, ohne großen Aufwand klar definierte Informationen über das Unternehmen, dessen Verantwortliche sowie dessen Verfahren zur automatisierten Verarbeitung personenbezogener Daten zu erlangen.

Im Bereich der Heimbetreiber könnten z. B. folgende Verfahren zu einem Eintrag in die beiden o. g. Übersichten führen:

- Pflegedokumentation,
- Heimabrechnung,
- Lohnabrechnung,
- Personalverwaltung,
- Finanzbuchhaltung,
- Videoüberwachung Begegnungszentrum,
- Schwesternnotruf,
- Telefonabrechnung,
- Mitgliederverwaltung/Beitragseinzug.

Zusätzliche Hinweise zur Erstellung und Führung des öffentlichen Verfahrensverzeichnisses können von der Website des RP Dresden abgerufen werden:

http://www.rp-dresden.de/ds/praxis/verfvrz.pdf

Die Heime bzw. Träger, bei denen es Mängel bei der Führung des öffentlichen Verfahrensverzeichnisses gab, wurden auf ihre gesetzlichen Pflichten hingewiesen und aufgefordert, die gesetzliche Umsetzungsfrist (22.05.2004) einzuhalten. Die im zweiten Halbjahr 2004 erneut aufgenommene Kontrolle hat jedoch gezeigt, dass die Mehrzahl der Heimträger erhebliche Schwierigkeiten bei der Erstellung eines gesetzeskonformen öffentlichen Verfahrensverzeichnisses hat. Zum Stichtag 31.12.2004 stand die Aufsichtsbehörde in diesem Punkt immer noch mit verschiedenen Heimträgern in der Diskussion.

Verpflichtung auf das Datengeheimnis:

Die fehlende Verpflichtung auf das Datengeheimnis (§ 5 BDSG) erwies sich als ein weiterer Mängelschwerpunkt bei der durchgeführten Branchenkontrolle. In mehreren Fällen berief man sich auf die im Arbeitsvertrag festgehaltene allgemeine Verschwiegenheitspflicht, die jedoch nicht mit dem Datengeheimnis identisch ist.

Die allgemeinen Verschwiegenheitspflichten beziehen sich in der Regel nur auf die so genannten Betriebs- und Geschäftsgeheimnisse (wozu allerdings auch personenbezogene Daten gehören können). Das Datengeheimnis nach § 5 BDSG enthält aber mehr als eine bloße Verschwiegenheitspflicht, denn es enthält das gesetzliche Verbot jedweder unbefugten Verarbeitung und Nutzung personenbezogener Daten. Eine Verletzung des Datengeheimnisses ist nicht immer auch ein Bruch der Verschwiegenheitspflichten. Unter das dem Datengeheimnis zugrunde liegende Verbot fallen z. B. auch:

- Auswertungen für private Zwecke,
- unzulässige Datenabrufe,
- Entwendung oder Herausgabe von Datenträgern an Unbefugte,
- Manipulation von Daten,
- Unterstützung Unbefugter beim Zugriff auf Daten etc.

Auch wenn § 5 BDSG nicht ausdrücklich eine *schriftliche* Verpflichtung fordert, ist die Verwendung schriftlicher Verpflichtungserklärungen zu empfehlen. Dies erleichtert einerseits den gegebenenfalls gegenüber der Aufsichtsbehörde erforderlichen Nachweis der vorgenommenen Verpflichtung, andererseits sichert sich der Unternehmer damit auch gegen individuelles

Fehlverhalten seiner Mitarbeiter ab.

Ein Muster für eine Verpflichtungserklärung ist unter

http://www.rp-dresden.de/service/formulare/1/14/par5_3.pdf

abrufbar. Das Original der Erklärung ist für die Personalunterlagen bestimmt. Der bzw. die Verpflichtete erhält eine Kopie.

Die Notwendigkeit der Verpflichtung der Mitarbeiter auf das Datengeheimnis wurde den Heimen bzw. deren Trägern von den Aufsichtsbehörden begründet und von diesen auch akzeptiert.

Datenerhebung, -verarbeitung und –nutzung:

a) Heimvertrag und Einwilligung

Da es sich bei der Betreuung in einer Altenpflegeeinrichtung um eine vertragliche Beziehung zwischen Heimbetreiber und Bewohner handelt, ist gemäß § 28 Abs. 1 Nr. 1 BDSG die Erhebung, Verarbeitung und Nutzung der Bewohnerdaten immer dann und nur soweit zulässig, wie dies der Zweckbestimmung des abgeschlossenen Heimvertrages dient und für dessen Erfüllung erforderlich ist.

Auf der Grundlage des Heimvertrages dürfen nur Angaben über den Heimbewohner selbst erhoben und verarbeitet werden. Angaben über Dritte (Betreuer, Vertrauenspersonen) erfordern entweder deren Einwilligung oder sind an den in § 28 Abs. 1 Nr. 2 BDSG genannten Kriterien zu messen.

Ob die Datenverarbeitung erforderlich und damit zulässig ist, beurteilt sich insbesondere auch nach den für die Altenpflege (in Heimen) geltenden spezialgesetzlichen Regelungen, wie Sozialgesetzbuch Elftes Buch (SGB XI) und Heimgesetz (HeimG), die Inhalte und Rahmenbedingungen der Datenverarbeitung im Pflegebereich regeln.

Eine gesetzliche Verpflichtung zur Aufnahme von Regelungen zum Datenschutz in den Heimvertrag besteht zwar nicht, es empfiehlt sich jedoch zur Klarstellung, das Recht auf Einsichtnahme in die Pflegedokumentation in den Vertrag aufzunehmen. Falls die Aufnahme weiterer Datenschutzregelungen dazu dienen soll, dem Vertragspartner zu verdeutlichen, dass die Datenschutzproblematik bekannt ist und auch beachtet wird, sollte darauf geachtet werden, dass dieser Teil kurz und für den Heimbewohner verständlich gehalten wird. Ausreichend wäre z. B. die Aussage, dass beim Heimträger ein Datenschutzbeauftragter benannt ist und dieser für Rückfragen zur Verfügung steht.

Häufig fanden sich im Heimvertrag persönliche Erklärungen, insbesondere von Schweigepflichtentbindungen (Hausarzt, MDK). Derartige Verarbeitungen sind nicht vom Vertragszweck abgedeckt, so dass sie nur auf der Grundlage der Einwilligung des Betroffenen gemäß § 4a BDSG in Betracht kommen. Die Einwilligung muss auf einer freien Entscheidung des Betroffenen beruhen, ist mit besonderen Unterrichtungspflichten verbunden, bedarf der Schriftform und ist gegebenenfalls besonders hervorzuheben. Die Einwilligung kann außerdem jederzeit für die Zukunft widerrufen werden.

Die gleichzeitige Unterzeichnung von Vertrag und Einwilligungserklärung in einem Dokument ist deshalb grundsätzlich unzulässig. Die Regelung des § 4a BDSG soll den Betroffenen vor einer unbedachten Preisgabe seiner Daten bewahren. Damit ist nicht vereinbar, dass gesetzliche Zulässigkeitsregelungen zur Datenverarbeitung (hier: Zweckbestimmung des Vertragsverhältnisses) mit der freiwillig zu erteilenden Erlaubnis zur Datenverarbeitung verknüpft werden. Die Auswertung der vorgelegten Musterverträge zeigt, dass in den betreffenden Fällen die Einwilligung regelmäßig nur durch Unterzeichnung des Vertrages insgesamt erteilt werden konnte. Selbst wenn man die grundsätzliche Verhandelbarkeit des Heimvertrages in diesem Punkt unterstellt, wird ein potentieller Bewohner dies kaum erkennen, geschweige denn durch eine diesbezügliche Diskussion seinen Heimplatz gefährden wollen. Mithin handelt es sich weder um eine tatsächlich freiwillige Zustimmung, noch wird auf diese Weise den Unterrichtungs- und Hervorhebungspflichten ausreichend entsprochen.

Die Einwilligung sollte daher grundsätzlich außerhalb des Vertrages in einem getrennten, besonders zu unterzeichnenden Formular erteilt werden. Wird dann eine Einwilligung widerrufen, bleibt das Vertragsverhältnis bestehen.

In Bezug auf die inhaltliche Gestaltung von Einwilligungen sind insbesondere die bestehenden Hinweispflichten zu beachten. Damit der Betroffene seine Entscheidung vorher ausreichend abwägen kann, ist eine Aufklärung über die Bedeutung und die Folgen der Einwilligung erforderlich. Rechtswirksam einwilligen kann nur jemand, der hinreichend darüber informiert ist. Neben dem Zweck der Erhebung, Verarbeitung oder Nutzung müssen insbesondere auch die von der Einwilligung betroffenen personenbezogenen Daten genannt werden. Da es sich im Regelfall um Daten über den Gesundheitszustand der Bewohner und damit um besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG handelt, muss sich die Einwilligung speziell auf diese Gesundheitsdaten beziehen.

Die im Rahmen der Kontrolle vorgelegten Musterverträge unterschieden sich in Bezug auf datenschutzrechtliche Regelungen zum Teil beträchtlich voneinander. Einige Verträge enthielten keine Regelungen zum Datenschutz, in anderen Verträgen fanden sich viel zu pauschal

gehaltene Einwilligungserklärungen ebenso wie umfangreiche, unverständliche und für den Betroffenen verwirrende Klauseln.

b) Einsichtnahme in die Pflegedokumentation

- *Pflegekasse und MDK*

Aus dem Urteil des Bundessozialgerichtes vom 23.07.2002 (Az.: B3 KR 64/01 R - Unzulässigkeit der Anforderung von Krankenhausentlassungsberichten durch Krankenkassen) und den Ausführungen des BfD zur Einsichtnahme in Pflegedokumentationen (19. TB, Pkt. 24.2.2) lassen sich folgende Grundsätze ableiten:

- Pflegedokumentation und Abrechnungsunterlagen (Leistungsnachweise) sind unbedingt sorgfältig zu trennen. Dies ist auch ein wichtiges Auswahlkriterium bei der Neuanschaffung von Heimsoftware.
- Das Einsichtnahmerecht der Pflegekasse im Rahmen der Überprüfung der Abrechnung der Pflegeleistungen (§§ 84 - 91, 105 SGB XI) beschränkt sich auf die Abrechnungsunterlagen und erstreckt sich nicht auf die Pflegedokumentation.
- Eine Einsichtnahme der Pflegekassen in die Pflegedokumentation ist auch nicht im Rahmen der Überwachung der Wirtschaftlichkeit und Qualität der Leistungserbringung zulässig (§§ 79, 80, 112 - 115, 117, 118 SGB XI), entsprechende Befugnisse haben ausschließlich der MDK bzw. bestellte Sachverständige.
- Auch die weiteren in § 94 Abs. 1 SGB XI genannten Datenverarbeitungszwecke erfordern keine Einsichtnahme in die Pflegedokumentation, so dass die Pflegekassen nicht befugt sind, Daten aus der Pflegedokumentation zu erheben. Im Umkehrschluss ergibt sich daraus die Unzulässigkeit einer derartigen Datenübermittlung selbst dann, wenn eine Einwilligung des Bewohners vorliegt.

- *Heimaufsicht*

Gemäß § 15 Abs. 2 Nr. 3 HeimG ist die Heimaufsicht im Rahmen ihres Überwachungsauftrages befugt, Einsicht in die Aufzeichnungen nach § 13 HeimG zu nehmen. Von Bedeutung sind dabei insbesondere die Aufzeichnungen nach § 13 Abs. 1 Nr. 4 - 9 HeimG, die in der Pflegedokumentation enthalten sind.

- *Bewohner*

Ein Einsichtnahmerecht besteht für Patienten unstreitig in Bezug auf ihre Krankenunterlagen (Urteil des BGH vom 23.11.1982, NJW 1983, 328 ff.). Danach ergibt sich das Einsichtnahmerecht als zusätzlicher Behandlungsvertragsanspruch aus dem durch grundrechtliche Wertung geprägten Selbstbestimmungsrecht und der Würde des Patienten, die es verbieten, ihm im Rahmen der Behandlung die Rolle eines bloßen Objekts zuzuweisen. Bei der Pflegedokumentation handelt es sich zwar nicht um Krankenunterlagen im eigentlichen Sinne, jedoch sind die darin enthaltenen Unterlagen den Krankenunterlagen sehr ähnlich (Angaben über den Betreuungsbedarf des Betroffenen, Verabreichung von Arzneimitteln, Pflegeverläufe), so dass hierfür das Einsichtsrecht ebenfalls gilt.

Darüber hinaus besteht ein Auskunftsanspruch auch nach § 34 BDSG. Der Betroffene hat die Möglichkeit, Auskunft über die zu seiner Person in der Pflegedokumentation enthaltenen Daten zu verlangen. Die Auskunft ist im Regelfall schriftlich zu gewähren. Dabei ist zu beachten, dass nicht *alle* Inhalte einer zum Betroffenen geführten Akte der Auskunftspflicht unterliegen müssen.

Zur Klarstellung bietet es sich an, im Heimvertrag das Recht auf Einsichtnahme in die Pflegedokumentation aufzunehmen.

c) Löschfristen

Für die in der Pflegedokumentation bzw. den Abrechnungsunterlagen gespeicherten personenbezogenen Daten gelten unterschiedliche Löschfristen.

Die Aufbewahrungsfrist für die Daten in der Pflegedokumentation ergibt sich aus dem Heimgesetz. § 13 Abs. 2 HeimG legt eine fünfjährige Aufbewahrungsfrist fest; danach sind die Daten zu löschen. Dies kann bei laufenden Verträgen natürlich nur für die Aufzeichnungen des Pflegeverlaufs und der verwalteten Gelder oder Wertsachen gelten. Die für die aktuelle Pflege weiterhin erforderlichen und gültigen Angaben, insbesondere die Stammdaten und der Pflegebedarf der Bewohner, die Pflegeplanung, Förder- und Hilfepläne sowie angeordnete freiheitsbeschränkende und -entziehende Maßnahmen sind davon nicht betroffen. Über ehemalige Bewohner dürfen zu Beginn des sechsten Kalenderjahres nach Vertragsende keine Pflegedaten mehr vorhanden sein.

Für die Abrechnungsunterlagen gelten die Bestimmungen der Abgabenordnung (AO) bzw. der Pflege-Buchführungsverordnung (PBV) in Verbindung mit dem Handelsgesetzbuch (HGB). Sowohl § 147 Abs. 3 AO als auch § 6 PBV i. V. m. § 257 HGB bestimmen, dass für

Abrechnungsunterlagen eine sechs- bzw. zehnjährige Aufbewahrungsfrist zu beachten ist. Demnach sind Buchungsunterlagen und -belege sowie Jahresabschlüsse und Bilanzen zehn Jahre, Geschäftsbriefe sechs Jahre aufzubewahren. Als Geschäftsbrief gilt dabei jegliche Korrespondenz, die der Vorbereitung, Durchführung oder Rückgängigmachung eines Geschäftes dient. Buchungsbelege sollen nachweisen, dass einem gebuchten Sachverhalt auch ein tatsächlich existierender Vorgang zugrunde liegt. Externe Buchungsbelege sind oftmals zugleich auch Geschäftsbriefe. Personenbezogene Daten werden sich dabei in erster Linie in Geschäftsbriefen und Buchungsbelegen finden.

Die datenschutzrechtliche Kontrolle hat ergeben, dass bei vielen Heimträgern Unsicherheiten über die gesetzlichen Aufbewahrungsfristen bestehen, weil die Rechtsgrundlagen der Datenverarbeitung nicht ausreichend bekannt sind.

d) Auftragsdatenverarbeitung/Wartungsverträge

Einige Heimträger bedienen sich zur Verarbeitung personenbezogener Daten externer Dienstleister, welche die Daten in deren Auftrag verarbeiten (vgl. § 11 BDSG). Wesentliches Merkmal einer Auftragsdatenverarbeitung ist die Auslagerung von lediglich technischen Hilfsaufgaben im Bereich der personenbezogenen Datenverarbeitung an externe Stellen. Das Auftragsverhältnis muss konkret einzelne Datenverarbeitungsphasen oder aber einen kompletten (technischen) Verarbeitungsvorgang zum Inhalt haben. Der Auftragnehmer hat diese Aufgaben nach fest vorgegebenen Kriterien ohne eigenen Entscheidungs- oder Beurteilungsspielraum abzuarbeiten, d. h. die Verantwortung für die Zulässigkeit der Datenverarbeitung bleibt beim Auftraggeber und Betroffene haben ihre Rechte gegebenenfalls auch weiterhin gegenüber diesem geltend zu machen.

Typische Anwendungsfelder für eine Auftragsdatenverarbeitung sind z. B.

- die Lohn- und Gehaltsabrechnung,
- die Akten- und Datenträgervernichtung oder auch
- die Systemadministration.

Werden diese oder vergleichbare Tätigkeiten im Rahmen der Auftragsdatenverarbeitung ausgelagert, sind insbesondere die Anforderungen des § 11 Abs. 2 BDSG zu beachten. Dies betrifft zum einen die Anforderungen an Form und Inhalt des Auftrags sowie zum anderen auch die Pflicht des Auftraggebers, sich von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Datensicherungsmaßnahmen zu überzeugen. Handlungsbedarf besteht erfahrungsgemäß bezüglich der schriftlichen Festlegung der technischen und

organisatorischen Maßnahmen (vgl. Anlage zu § 9 BDSG) und des Ausschlusses von Subauftragnehmern.

Auch Wartung und Fernwartung unterfallen dem Geltungsbereich des § 11 BDSG, d. h. für derartige Vertragsverhältnisse sind die Vorschriften für die Auftragsdatenverarbeitung analog anzuwenden.

Im Heimbereich sehr häufig praktiziert wird das Outsourcing von Hilfsaufgaben der Datenverarbeitung sowie von Administrations- und Wartungstätigkeiten. Dies betrifft sowohl den Betrieb des lokalen Netzes an sich als auch und vor allem die genutzte Heimsoftware.

In keinem Fall lag ein den Anforderungen des § 11 BDSG genügender Vertrag vor, insbesondere fehlte es regelmäßig an den in § 11 Abs. 2 Satz 2 BDSG geforderten Inhalten.

Videoüberwachung

Das BDSG trifft in § 6b spezielle Regelungen zur Videobeobachtung und -aufzeichnung in öffentlichen Räumen. Unter öffentlichen Räumen in diesem Sinne sind öffentlich zugängliche Bereiche zu verstehen, die entweder dem öffentlichen Verkehr gewidmet sind oder nach erkennbarem Willen der Berechtigen von jedermann benutzt oder betreten werden können.

Die Beobachtung eines Patienten im Wachkomazimmer beurteilt sich deshalb nicht nach § 6b BDSG, weil es sich hier nicht um einen öffentlichen Raum handelt. Auch Klingelkameras unterfallen in der Regel nicht dem Anwendungsbereich des § 6b BDSG, da es im Allgemeinen an der Beobachtung eines Raumes fehlt. Stattdessen wird nur der unmittelbar vor der Tür befindliche Bereich im Rahmen der Zugangskontrolle erfasst, und die Kamera ist in den meisten Fällen auch nur kurzzeitig während des Einlassvorganges in Betrieb.

Anders sieht es bei der permanenten Videoüberwachung ganzer Eingangs- bzw. Einfahrtsbereiche aus. Die Türen/Tore sind im Normalfall verschlossen und werden bei Bedarf durch den Pförtner oder Wachdienst geöffnet. Dies ist oft bei Wirtschaftseinfahrten (ganztägig) sowie bei Gebäudeeingängen (abends/nachts) der Fall. Für die Einordnung derartiger Bereiche als öffentlich zugängliche Räume ist einerseits der Erfassungsbereich von Bedeutung, andererseits die Bestimmung des jeweiligen Objektes.

Altenpflegeheime sind zunächst vom Grundsatz her nicht öffentlich zugängliche Räume. Bestimmungsgemäß ist der Zugang dieser Objekte nicht jedermann erlaubt, sondern eben nur dem dort tätigen Personal, den Bewohnern und deren Gästen. Insoweit besteht also eine Vergleichbarkeit mit Wohngebäuden. Anders ist die Sachlage aber immer dann, wenn sich öffentliche Einrichtungen im gleichen Objekt befinden und diese Einrichtungen keinen eigenen Zu-

gang besitzen. Für Altenpflegeheime typisch sind etwa Arztpraxen, Friseurgeschäfte, Apotheken oder Physiotherapie-Praxen. Diese Einrichtungen stehen auch der Öffentlichkeit zur Verfügung, so dass der überwachte Eingangsbereich zumindest während der Sprech- oder Öffnungszeiten als öffentlich zugänglich angesehen werden muss.

Sind derartige Einrichtungen nicht vorhanden, ist § 6b BDSG anwendbar, wenn durch die jeweiligen Kameras über den Eingangsbereich hinaus größere Flächen öffentlicher Gehwege/Straßen erfasst werden und eine Beschränkung des Erfassungsbereiches (Veränderung der Kameraeinstellung) nicht möglich ist.

Als Zweck aller dem BDSG unterfallenden Videoüberwachungsanlagen wurde von den Heimen die Zugangskontrolle angegeben. Damit werden berechtigte Interessen für einen konkret festgelegten Zweck wahrgenommen (§ 6b Abs. 1 Nr. 3 BDSG). Schutzwürdige Interessen der Betroffenen überwiegen zumindest dann nicht, wenn sich die Überwachung auf die Zeiten beschränkt, in denen das Tor bzw. die Tür verschlossen ist und der Erfassungsbereich so gering wie möglich gehalten wird. Insbesondere muss eine Erfassung anderer Passanten ohne Zutrittsbegehren möglichst ausgeschlossen werden. Hinzuweisen ist außerdem darauf, dass die Einsatzzwecke der Videoüberwachung vorab schriftlich - etwa in Form eines Einsatz- und Nutzungskonzeptes - festzulegen sind.

Auf die Tatsache der Videoüberwachung ist außerdem deutlich hinzuweisen, damit für den Betroffenen erkennbar ist, dass er sich in einem videoüberwachten Bereich aufhält. Dazu sollten Hinweisschilder angebracht werden, auf denen auch die verantwortliche Stelle zu benennen ist, damit der Betroffene weiß, wohin er sich im Beschwerdefall wenden kann.

Sofern die Kamerabilder auch aufgezeichnet werden sollen, ist hierfür die Erforderlichkeit zu prüfen und dann eine nochmalige Abwägung mit den schutzwürdigen Interessen der Betroffenen vorzunehmen. Für den Zweck der Zugangskontrolle/Türöffnung ist die Notwendigkeit der Aufzeichnung zu verneinen, diese ist deshalb unzulässig.

Datensicherungsmaßnahmen

Die in den Heimen überprüften technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit ergaben häufig Mängel in folgenden Punkten:

- mangelhafte Passwortgestaltung,
- Passwortvergabe durch andere Personen,
- Hinterlegung von Nutzerpasswörtern,
- zeitliche Gültigkeit von Passwörtern,

- Möglichkeit des nutzerinitiierten Passwortwechsels,
- Umsetzung des Generationsprinzips bei der Datensicherung,
- ungesicherte Aufbewahrung von Sicherungsdatenträgern,
- Möglichkeit von Gast- und Gruppenlogins,
- inaktive Accounts,
- kein Passwortschutz des Bildschirmschoners,
- keine Dokumentation der Zugriffsrechte,
- fehlendes Virenschutzkonzept,
- mangelnde Zutrittskontrolle Serverraum,
- ungesicherte Diskettenlaufwerke,
- unsachgemäße bzw. fehlende Aktenvernichtung.

4.2.3 Koordinierte Datenschutzkontrolle von Wohnungsunternehmen

Nachdem sich das Kontrollinstrument „koordinierte Datenschutzkontrolle“ im Bereich der Verkehrsunternehmen (vgl. 1. TB, Pkt. 4.2.3) sowie der Altenpflegeheime (vgl. Pkt. 4.2.2) in der Praxis bewährt hat, ist im Februar 2004 mit einer weiteren Kontrolle dieser Art, diesmal bei großen Wohnungsunternehmen, begonnen worden. Überprüft wurden dabei insgesamt 46 Wohnungsunternehmen.

Um im Bereich der Wohnungsunternehmen datenschutzrechtliche Schwerpunkte herauszuarbeiten und den Fragebogen für das Prüfverfahren zu erstellen, setzte sich die Aufsichtsbehörde zunächst mit einem Wohnungsunternehmen in Verbindung und führte dort eine Vor-Ort-Kontrolle durch. Bei dem so geprüften Wohnungsunternehmen wurden die folgenden Schwachstellen festgestellt:

- Mängel bei der Löschung und Sperrung personenbezogener Daten nach § 35 BDSG.
- Das Fehlen der Verpflichtung der mit der Datenverarbeitung befassten Mitarbeiter auf das Datengeheimnis.
- Von Mietinteressenten ausgefüllte Fragebögen wurden in elektronischer Form in einer Interessentendatenbank gespeichert. Dies war bedenklich, da diese zunächst intern in Stahlschränken gelagert und später in einem externen Brandbereich des Unternehmens ausgelagert wurden. Eine Vernichtung der Datenträger erfolgte bis dahin nicht.

Alle Beanstandungen wurden von dem Wohnungsunternehmen jedoch im Nachgang beseitigt.

Die für die koordinierte Kontrolle verwendeten Fragebögen behandelten daraufhin schwerpunktmäßig folgende datenschutzrechtliche Aspekte:

- betrieblicher Datenschutzbeauftragter,
- öffentliches Verfahrensverzeichnis,
- Verpflichtung auf das Datengeheimnis,
- Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung (Mieter und Mietbewerber),
- Kooperation mit SCHUFA, Auskunfteien und Warnsystemen sowie
- technische und organisatorische Maßnahmen zur Datensicherung.

Eine kurze Zusammenfassung der bis jetzt feststehenden Ergebnisse kann wie folgt vorgenommen werden:

Betrieblicher Datenschutzbeauftragter:

Ein großer Teil der Wohnungsunternehmen hatte trotz bestehender Verpflichtung keinen betrieblichen Datenschutzbeauftragten bestellt (vgl. § 4f BDSG). Zwischenzeitlich wurden die Verstöße in den meisten Fällen behoben. In drei Fällen jedoch musste die Aufsichtsbehörde ein Ordnungswidrigkeitenverfahren einleiten (vgl. Pkt. 9).

Verpflichtung auf das Datengeheimnis:

Soweit die Unternehmen ihre Mitarbeiter nicht auf das Datengeheimnis verpflichtet hatten, wurde dies nachgeholt. Bei einigen Unternehmen war die Anpassung des verwendeten Verpflichtungsformulars an das im Jahr 2001 novellierte BDSG erforderlich.

Öffentliches Verfahrensverzeichnis:

Bei den kontrollierten Wohnungsunternehmen hat sich wie bereits bei den Altenpflegeheimen (vgl. Pkt. 4.2.2) gezeigt, dass die Erarbeitung eines gesetzeskonformen öffentlichen Verfahrensverzeichnisses in der Praxis erhebliche Probleme bereitet. Trotz detaillierter Hinweise der Aufsichtsbehörden war bis zum Stichtag 31.12.2004 bei einem großen Teil der Unternehmen ein öffentliches Verfahrensverzeichnis noch immer nicht vorhanden bzw. entsprach nicht den

gesetzlichen Anforderungen.

Videoüberwachung:

Die Thematik Videoüberwachung war in der Praxis bei den kontrollierten Unternehmen insgesamt nur von untergeordneter Bedeutung. Die wenigen der Aufsichtsbehörde bekannt gewordenen Fälle betrafen die Videoüberwachung eines Verwaltungsgebäudes, der Kellerbereiche von Hochhäusern sowie einer Tiefgarage.

Auftragsdatenverarbeitung:

Die den Aufsichtsbehörden vorgelegten Vertragsauszüge bzw. -ergänzungen erfüllen nur in wenigen Fällen die gesetzlichen Anforderungen des § 11 Abs. 2 Satz 2 BDSG. Im Regelfall fehlen konkrete Festlegungen zu den technischen und organisatorischen Maßnahmen sowie zu Subauftragsverhältnissen.

In vielen Fällen werden in den Vereinbarungen lediglich allgemeine pauschale Aussagen zum Datenschutz getroffen bzw. wird die Einhaltung der Vorgaben des BDSG zugesichert. Zwar kann ein Auftraggeber aus einer naturgemäß allgemein gehaltenen „Datenschutz-Leitlinie" des Auftragnehmers ableiten, dass die Thematik „Datenschutz" dort bekannt ist und einen entsprechenden Stellenwert besitzt. Allerdings ermöglicht ihm dies keine Aussage darüber, ob die vorhandenen Datensicherungsmaßnahmen für seinen speziellen Fall ausreichend oder gegebenenfalls zusätzliche Maßnahmen erforderlich sind. Der Auftraggeber muss im Rahmen seiner datenschutzrechtlichen Verantwortung jedoch dafür Sorge tragen, dass die Daten entsprechend den gesetzlichen Vorschriften beim Auftragnehmer verarbeitet werden. Er muss sich also über das Sicherungskonzept des Auftragnehmers Klarheit verschaffen. Es genügt nicht, dass sich der Auftraggeber auf nicht nachgewiesene Aussagen bzw. allgemein zugesicherte Maßnahmen des Auftragnehmers verlässt. Er muss sicherstellen, dass die Datenverarbeitung beim Auftragnehmer genauso sicher erfolgt, wie dies bei eigener Erledigung der Fall wäre.

Die an die Auftraggeber gerichteten Forderungen der Aufsichtsbehörden zeigen inzwischen Wirkung. Es liegen mehrere Anfragen von Auftragnehmern vor, die an einer Abstimmung zu gesetzeskonformer Vertragsgestaltung, insbesondere zur Gestaltung von Musterverträgen, interessiert sind.

Selbstauskünfte von Mietbewerbern:

Regelmäßig werden Bewerbern für Mietwohnungen mehr oder weniger umfangreiche Fragebögen („Selbstauskünfte“) vorgelegt, auf deren Basis dann eine Entscheidung getroffen werden soll, ob mit den Bewerbern ein Mietverhältnis eingegangen wird. Die von den Unternehmen vorgelegten Fragebögen zu Selbstauskünften zeigten eine breite Vielfalt innerhalb der Branche.

Die Zulässigkeit der von Vermietern an Mietinteressenten gestellten Fragen beurteilt sich nach § 28 Abs. 1 Nr. 1 BDSG, 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. Bewerbungsphase) dient. Danach ist der potentielle Mieter nur zur Auskunft verpflichtet, wenn die Umstände für den Vermieter bei objektiver Bewertung und Berücksichtigung schutzwürdiger Belange des Mietinteressenten der Auskunft bedürfen. Das ist zu bejahen, wenn die Angaben 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, WuM 1992, 597).

Häufig wurden Auskünfte über so genannte „weiche“ Daten von den potentiellen Mietern gefordert. Beispielhaft hierfür sind Fragen nach der Kreditwürdigkeit und nach Privatinsolvenzen. Es liegt zwar ein nachvollziehbares Interesse der Vermieter vor, liquide Mieter zu finden, jedoch steht das Recht des Mietinteressenten auf informationelle Selbstbestimmung dem gegenüber. Demnach muss eine verhältnismäßige Datenerhebung erfolgen, die kollidierenden Interessen sind gegeneinander abzuwägen.

Sollte nach der Datenerhebung kein Mietverhältnis zu Stande kommen, müssen die erhobenen Daten gelöscht werden. Eine weitere Nutzung und Übermittlung der Daten ist bei fehlender Einverständniserklärung der potentiellen Mieter unzulässig.

In Auswertung der Kontrolle planen die Aufsichtsbehörden, gemeinsam einen Katalog der Datenarten zu erarbeiten, deren Abfrage bei der Anbahnung eines Mietvertragsverhältnisses im Rahmen der Selbstauskunft nicht zulässig ist.

Fremdauskünfte

Im Verlauf der weiteren Auswertung der Kontrolle werden sich die Aufsichtsbehörden auch noch mit der Problematik der Zulässigkeit des Einholens von Fremdauskünften über Mietbe-

werber befassen. So haben von den achtzehn im Regierungsbezirk Dresden kontrollierten Unternehmen sieben Unternehmen angegeben, mit der SCHUFA zusammenzuarbeiten. Weitere vier Unternehmen holen Einkünfte bei Wirtschaftsauskunfteien ein.

4.2.4 Online-Prüfung von Versorgungsunternehmen

Ende des Jahres 2002 hatte das Regierungspräsidium Dresden eine Kontrollaktion in der Branche der Energieversorgungsunternehmen begonnen (vgl. 1. TB, Pkt. 4.2.4), die im Berichtszeitraum fortgesetzt worden ist. Schwerpunkt dieser unter Einsatz eines Online-Prüftools vorgenommenen Kontrollen war die datenschutzgerechte Gestaltung der Internetseiten dieser Unternehmen.

Bisher wurden zehn Unternehmen kontrolliert. Eine erste Zwischenauswertung der Kontrollen ergab folgendes:

Betrieblicher Datenschutzbeauftragter:

Lediglich die Hälfte der bislang kontrollierten Unternehmen hatte ordnungsgemäß einen Datenschutzbeauftragten bestellt. In drei Fällen war die als Datenschutzbeauftragte bestellte Person wegen der Wahrnehmung sonstiger Aufgaben im Unternehmen nicht als Datenschutzbeauftragter geeignet, weil die Tätigkeiten kollidierenden Interessen dienten. So ist z. B. die Bestellung eines Personalleiters oder Leiters der Datenverarbeitungsabteilung zum Datenschutzbeauftragten nicht zulässig.

Verpflichtung auf das Datengeheimnis:

Beanstandet wurden in fünf Fällen Mängel bei der Verpflichtung auf das Datengeheimnis. Ursache war entweder die nicht erfolgte Anpassung der Verpflichtungserklärung an das novellierte BDSG oder aber die Reduzierung der Verpflichtung auf die Verschwiegenheitspflicht.

Öffentliches Verfahrensverzeichnis:

Das gemäß § 4g Abs. 2 BDSG vorzuhaltende öffentliche Verfahrensverzeichnis war in acht Fällen entweder nicht vorhanden oder zu allgemein gehalten, d. h. auf ein dem Unternehmenszweck entsprechendes Verfahren reduziert.

Anbieterkennzeichnung:

Es wurde überprüft, ob das Angebot eine Anbieterkennzeichnung nach § 6 TDG bzw. eine Information über die für die Datenverarbeitung verantwortliche Stelle gemäß § 4 Abs. 3

Satz 1 Nr. 1 BDSG aufweist.

Der Einordnung der Websites von Versorgungsunternehmen als Teledienst liegen die Regelungen des § 2 Abs. 2 Nr. 1, 2 TDG zu Grunde. Auf den geprüften Internetseiten wurden vielfältige Dienste angeboten, z. B. Bestellmöglichkeiten, Zählerstandmeldungen, An-, Um- und Abmeldungen und Informationen über Warenangebote (Energie). Gem. § 6 TDG sind folgende Informationen leicht erkennbar, unmittelbar erreichbar sowie ständig verfügbar vorzuhalten:

- Namen und Anschrift des Anbieters, bei juristischen Personen der Name des Vertretungsberechtigten,
- Angaben, die eine schnelle elektronische Kontaktaufnahme ermöglichen (E-Mail-Adresse),
- Angaben zur zuständigen Aufsichtsbehörde (soweit im Rahmen einer Tätigkeit, die der behördlichen Zulassung bedarf),
- Register, in das der Anbieter eingetragen ist und Registernummer,
- die Kammer, der der Anbieter angehört, die gesetzliche Berufsbezeichnung und der Staat, in dem die Berufsbezeichnung verliehen worden ist sowie die Bezeichnung der berufsrechtlichen Regelungen und wie diese zugänglich sind (bei bestimmten Berufen) sowie
- die Umsatzsteueridentifikationsnummer (falls vorhanden).

Nicht in allen Fällen wurden von den Unternehmen diese Anforderungen an die Anbieterkennzeichnung beachtet.

Datenschutz-Unterrichtung:

Gemäß § 4 Abs. 1 (TDDSG) ist der Nutzer eines Teledienstes zu Beginn des Nutzungsvorganges über die Verarbeitung seiner personenbezogenen Daten zu unterrichten, damit auch der technisch nicht so versierte Nutzer erkennen kann, dass bereits mit dem Aufrufen der Internetseite personenbezogene Daten erhoben werden (z. B. IP-Nummer, Browsertyp, Uhrzeit und Dauer der Nutzung).

Die sich aus § 4 Abs. 3 BDSG ergebenden Unterrichtungspflichten sind zu beachten. Das

bedeutet insbesondere, dass die Identität der verantwortlichen Stelle, Zweckbestimmung der Erhebung, Verarbeitung und Nutzung sowie Empfänger der Daten anzugeben sind. Die Auswertung der bisher durchgeführten Kontrollen hat ergeben, dass in neun von zehn Fällen eine Datenschutzunterrichtung fehlte.

Für die Unterrichtung nach dem TDDSG ist es zweckmäßig, eine mit der Anbieterkennzeichnung vergleichbare Anordnung zu wählen, um so insbesondere die rechtzeitige Unterrichtung sicherzustellen. Hingegen ist es für die Unterrichtung nach dem BDSG besser, wenn diese erst dann erfolgt, wenn die Daten tatsächlich erhoben werden, also z. B. auf den Seiten des dafür vorgesehenen Direktservice-Bereiches. Andernfalls bestehen Bedenken, dass diese Unterrichtung den Nutzer nicht tatsächlich erreicht.

Unterrichtung über die Verwendung von Cookies[1]:

Kommen Cookies zum Einsatz, die nicht lediglich temporär gespeichert werden, ist der Nutzer davon zu unterrichten. Auch dies ergibt sich aus § 4 Abs. 1 TDDSG, denn insoweit handelt es sich um ein Verfahren, welches die spätere Identifizierung des Nutzers ermöglicht. Sofern Cookies im Zusammenhang mit der Speicherung von Nutzungsprofilen verwendet werden, hat der Nutzer zudem das Widerspruchsrecht nach § 6 Abs. 3 TDDSG. Auf dieses Widerspruchsrecht ist der Nutzer hinzuweisen.

Bei den geprüften Internetpräsenzen wurden nur Session-Cookies verwendet, die kurzfristig gespeichert werden. Dennoch empfahl die Aufsichtsbehörde den Unternehmen, zur Vermeidung von Missverständnissen zumindest einen klarstellenden Hinweis zu geben, dass lediglich temporäre Cookies zum Einsatz kommen.

Einsatz von Weitervermittlungstechniken:

Über Links und eingebettete Objekte können im Internet verteilte Informationen miteinander verknüpft und in Zusammenhang gebracht werden. Ein Nutzer geht dann oftmals davon aus, dass alle Teile eines Angebots durch den ursprünglich von ihm angewählten Anbieter zu verantworten sind und wundert sich, wenn er plötzlich auf Seiten eines ganz anderen Anbieters gelangt. Anbieter von Telediensten müssen dem Nutzer daher gem. § 4 Abs. 5 TDDSG die Weitervermittlung an Dritte anzeigen. Dies gilt für jede Form der Weitervermittlung, so insbesondere bei externen Links, automatisch geladenen Elementen anderer Anbieter oder auch

[1] Cookies („Kekse“) sind kleine Informationseinheiten, die Webseiten per JavaScript auf dem Rechner des Anwenders (Client-Rechner) ablegen und später wieder auslesen können.

bei Weiterleitung der Startseite.

Die in bislang drei Fällen festgestellten Mängel betrafen die fehlende Kennzeichnung externer Links. Behoben werden können die Mängel durch eine klare Linkbezeichnung, eine Zusatzkennzeichnung als „externer Link“ oder durch Öffnen eines zu quittierenden Informationsfensters vor der tatsächlichen Weiterleitung an den externen Anbieter.

Veröffentlichung personenbezogener Daten:

Die Veröffentlichung personenbezogener Daten auf Internetseiten beurteilt sich nach den Vorschriften des BDSG.

In Anwendung der §§ 4 und 28 BDSG (Datenverarbeitung für eigene Zwecke) sowie des § 22 Kunsturheberrechtsgesetz (Recht am eigenen Bild) ist eine Veröffentlichung über reine Kontaktangaben hinausgehender personenbezogener Daten im Regelfall nur mit schriftlicher Einwilligung der Betroffenen zulässig.

Insbesondere bei der häufig zu Präsentationszwecken erfolgenden Veröffentlichung von Mitarbeiterfotos, die in acht Fällen vorlag, ist dies durch die Aufsichtsbehörde entsprechend hinterfragt worden. Bei der Veröffentlichung von Kontaktdaten gilt der Grundsatz, dass funktionsbezogenen Kontaktangaben (Telefon, E-Mail) der Vorzug vor personalisierten Angaben zu geben ist.

Erhebung personenbezogener Daten durch Online-Formulare:

Online-Formulare dienen zur Erhebung von Daten eines Nutzers. Die Zulässigkeit der Erhebung richtet sich ebenfalls nach dem BDSG. Von der Aufsichtsbehörde wird in Analogie zu Offline-Formularen insbesondere die Erforderlichkeit der Datenerhebung im Rahmen der angegebenen Zweckbestimmung geprüft. Besonderes Augenmerk wird auf die Kennzeichnung der oft im Übermaß abgefragten Kontaktdaten als „freiwillige Angaben“ gerichtet. Dahingehend waren bislang acht Verstöße festzustellen.

Verschlüsselung:

Bei acht der kontrollierten Versorgungsunternehmen wurden die in Online-Formulare eingegebenen Daten unverschlüsselt übertragen. Nur eine qualitativ hochwertige verschlüsselte Übertragung garantiert jedoch, dass diese Daten nicht von Dritten zur Kenntnis genommen

werden können. Zumindest bei sensiblen personenbezogenen Daten oder bei Authentisierungsdaten - praktisch also im gesamten Direktservice-Bereich - sollte daher eine Verschlüsselung erfolgen. Nach § 4 Abs. 4 Nr. 3 TDDSG hat der Diensteanbieter durch geeignete Vorkehrungen sicherzustellen, dass der Nutzer Teledienste gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann. Ein Hinweis auf die unverschlüsselte Übertragung der eingegebenen Daten an den Nutzer erfüllt die Vorgaben des § 4 Abs. 4 Nr. 3 TDDSG nicht.

Unverschlüsselte Datenübertragungen im Direktservice-Bereich sind durch die Aufsichtsbehörde regelmäßig beanstandet worden.

4.3 Anlasskontrollen

4.3.1 Überblick

Anlasskontrollen werden im Gegensatz zu Regelkontrollen (vgl. Pkt. 4.2) immer dann durchgeführt, wenn der Aufsichtsbehörde konkrete Anhaltspunkte für eine Datenschutzverletzung vorliegen. In den meisten Fällen ergeben sich derartige Anhaltspunkte aus Beschwerden Betroffener. In der Regel können diese Vorgänge schriftlich bearbeitet werden. Wenn dies jedoch nicht zweckmäßig oder nicht ausreichend ist, wird eine Vor-Ort-Kontrolle durchgeführt.

Anlasskontrollen finden ihren Abschluss in einer datenschutzrechtlichen Würdigung des untersuchten Sachverhalts, die sowohl der verantwortlichen Stelle als auch dem Betroffenen bzw. dem Petenten zur Kenntnis gegeben wird. Werden dabei Verletzungen materiellrechtlicher Datenschutzbestimmungen festgestellt, kann dies der Betroffene dann als Grundlage für weitere rechtliche Schritte (z. B. Schadensersatzforderungen) nehmen.

Gelegentlich kommt es vor, dass die kontrollierte Stelle gegen die durch die Aufsichtsbehörde vorgenommene abschließende Sachverhaltsbewertung Widerspruch einlegt. Dabei wird jedoch nicht erkannt, dass es sich bei der Feststellung des Prüfungsergebnisses nicht um einen Verwaltungsakt handelt und somit auch nicht die Möglichkeit eines Widerspruchs besteht (vgl. BVerwG, Beschluss vom 05.02.1992 - 7 B 15.92).

Seitens der Aufsichtsbehörde wird mit einer Beanstandung nicht in die Rechte der verantwortlichen Stelle eingegriffen, d. h. es bleibt letztlich dem Unternehmen überlassen, ob es der Auffassung der Aufsichtsbehörde folgt oder nicht. Sollte die vorgenommene Bewertung in einen Rechtsstreit mit dem Betroffenen einfließen, obliegt dem dann zuständigen Gericht die

Entscheidung darüber, ob und in welcher Weise die Feststellungen der Aufsichtsbehörde zu berücksichtigen sind.

Unabhängig davon hat die Aufsichtsbehörde die Möglichkeit, bei Vorliegen der entsprechenden Voraussetzungen den Verstoß als Ordnungswidrigkeit zu ahnden. In diesem Fall ist die Sachlage eine andere, da mit dem Erlass eines Bußgeldbescheides in die Rechte der verantwortlichen Stelle bzw. seiner vertretungsberechtigten Personen eingegriffen wird und somit auch entsprechende Rechtsmittel (Einspruch, Rechtsbeschwerde) eingelegt werden können.

Die Übersicht zeigt die Entwicklung der von den Aufsichtsbehörden durchgeführten Anlasskontrollen gegenüber dem letzten Berichtszeitraum:

Anlässe	2001 - 2002	**2003 - 2004**
Eingang	116	**147**
Übernahme aus vorherigem Berichtszeitraum	5	**9**
Kontrollen vor Ort	18	**24**
Schriftliches Verfahren	103	**132**
Begründet	50	**65**
Abgewiesen	36	**53**
Keine Zuständigkeit	27	**26**
Noch in Bearbeitung	8	**12**

Die Kontrollen betrafen insbesondere die folgenden Branchen:

- Einzelhandel
- Vermieter/Hausverwaltungen
- Industrieunternehmen
- Markt- und Meinungsforschungsunternehmen
- Banken/Sparkassen
- Internet Content Provider
- Vereine
- Hotels, Gaststätten

- Ärzte, Privatkliniken
- Rechtsanwälte, Steuerberater.

Die bei den Kontrollen festgestellten Verstöße betrafen unter anderem die folgenden Sachverhalte:

- Verstöße gegen die Meldepflichten gem. § 4d BDSG,
- Interessenkollisionen beim betrieblichen Datenschutzbeauftragten,
- Datenschutzverstöße durch Auftragsdatenverarbeiter,
- Unregelmäßigkeiten bei der Ausgabe und dem Versand von SparkassenCards,
- Auskunftserteilung durch eine Sparkasse (vgl. 4.3.15),
- Übermittlung von Schuldnerdaten an Verwandte eines Schuldners,
- Nutzung und Übermittlung von Kundendaten durch Außendienstmitarbeiter nach Beendigung des Vertretervertrages,
- Übermittlung der Daten von Vereinsmitgliedern im Rahmen eines Gruppenversicherungsvertrages
- Umgang mit Mitgliederdaten durch einen Insolvenzhilfeverein
- nachträgliche Abforderung von Personalausweiskopien bei Bankgeschäften,
- Erhebung von Personalausweisdaten bei bargeldlosem Bezahlen (vgl. Pkt. 4.3.10),
- Personalausweiskopien zur Überprüfung von Manipulationsvorwürfen im Fußball (vgl. Pkt. 4.3.9),
- Löschung personenbezogener Daten bei einem Unternehmensberater nach Auftragsende,
- Nutzung personenbezogener Daten für Werbezwecke durch nebenberufliche Lehrkräfte,
- unverlangte Zusendung von Werbe-E-Mails,
- Veröffentlichung personenbezogener Daten im Internet,
- automatische Weiterleitung aller auf einem persönlichen Account eingehenden E-Mails an den Vorgesetzten (vgl. Pkt. 4.3.3),
- Auskunftsverweigerung bei elektronischer Verbrauchsdatenerfassung,
- heimliche Installation von Überwachungssoftware durch Arbeitgeber (vgl. Pkt. 4.3.4),
- fehlende Kennzeichnung der Videoüberwachung in öffentlichen Tiefgaragen,
- Videoüberwachung eines auch für Wohn- und Freizeitzwecke genutzten Gebäudeensembles (vgl. Pkt. 4.3.5),
- Videoüberwachung einer Werkhalle (vgl. Pkt. 4.3.2),

- Videoüberwachung des Gehweges vor einem Hotel,
- Videoüberwachung des Einganges eines privaten Wohnhauses,
- unzureichende Trennung von Warte- und Empfangsbereich in einer Arztpraxis,
- Unterrichtung der Ehefrau über die Krankheitsgeschichte ihres Ehemannes durch den Arzt (vgl. Pkt. 4.3.6),
- Umgang mit Patientendaten in einer ärztlichen Gemeinschaftspraxis (vgl. 4.3.7),
- Auskunftsersuchen einer Betriebskrankenkasse an eine Klinik (vgl. 4.3.14),
- Auskünfte an Betroffene durch Wirtschaftsauskünften (vgl. Pkt 4.3.8),
- Bekanntgabe der Endergebnisse von Betriebskostenabrechnungen an Mitmieter (vgl. Pkt, 4.3.11),
- Selbstauskünfte von Mietbewerbern,
- Speicherung von Besucherdaten bei einem Wachunternehmen,
- Rücksendung von Bewerbungsunterlagen an falschen Bewerber (vgl. 4.3.12),
- Entsorgung von Bewerbungsunterlagen in Müllcontainer (vgl. 4.3.13),
- Beschäftigtendaten am „Schwarzen Brett“,
- Weitergabe von Kundendaten durch ein Energieversorgungsunternehmen (vgl. 4.3.16),
- Aushang eines Hausverbots (vgl. 4.3.17),
- mangelnde Sorgfalt bei Adressrecherchen durch einen Rechtsanwalt,
- Nichtbeachtung der Auskunftspflicht durch einen Finanzdienstleister.

4.3.2 Videoüberwachung einer Werkhalle

Die Aufsichtsbehörde hatte ein von mehreren Beschäftigten unterzeichnetes Schreiben erhalten, in dem diese um die datenschutzrechtliche Überprüfung einer kürzlich in der Werkhalle ihres Arbeitgebers installierten Videoüberwachung baten.

Die daraufhin durchgeführte örtliche Überprüfung ergab folgende Sachlage:

Inner- und außerhalb der Werkhalle waren insgesamt zwölf Videokameras installiert worden. Vier dieser Kameras befanden sich im Gebäudeinneren, wobei drei Kameras innerbetriebliche Transportwege (Hauptgänge) erfassten. Die vierte Kamera diente der Beobachtung eines unter Arbeitsschutzaspekten besonders gefährlichen Einzelarbeitsplatzes.

Die verbleibenden acht Kameras dienten der Außenhautüberwachung bzw. der Überwachung des Werkgeländes. Bis auf ein Aufnahmegerät erfassten alle Kameras eindeutig erkennbares und umfriedetes Betriebsgelände. Die verbleibende Kamera erfasste darüber hinaus aber auch Teile der öffentlichen Straße, des öffentlichen Gehweges sowie angrenzende, frei zugängliche Teile des Betriebsgeländes.

Die Kameras waren offen angebracht und besaßen einen statischen Erfassungsbereich.

Der Zweck der Überwachung war auf einer Betriebsversammlung erläutert worden. Die Kameras sollten dem Nachweis der ordnungsgemäßen Objektsicherung gegenüber der Kredit gebenden Bank bzw. der vertraglich gebundenen Versicherungsgesellschaft dienen.

Auf diese Weise sollten die materiellen Werte geschützt, eventuelle Einbrüche dokumentiert und damit der Versicherungsschutz garantiert werden. Die Überwachung des Einzelarbeitsplatzes sollte darüber hinaus der Erhöhung der Arbeitssicherheit dienen.

Das Geschehen in den überwachten Bereichen wurde permanent und digital in einem Ringspeicher mit einer Kapazität von sechs Tagen aufgezeichnet. Der Monitor befand sich im Büro des Firmeninhabers; zugriffsbefugt war neben ihm nur sein Stellvertreter. Der Zugriff war passwortgeschützt. Am Monitor bestand die Möglichkeit, entweder die Aufnahmen von sechs Kameras gleichzeitig in verkleinerter Darstellung oder die Aufnahme einer Kamera in großformatiger Darstellung zur Anzeige zu bringen. Eventuell im Erfassungsbereich befindliche Personen waren deutlich identifizierbar; eine Auswertung nur im Schadenfall beabsichtigt.

Die Zulässigkeit der Videoüberwachung hat die Aufsichtsbehörde wie folgt bewertet:

Außenhautsicherung:

§ 6b BDSG regelt die Zulässigkeit der Videoüberwachung von öffentlich zugänglichen Räumen. Für Bereiche, die in einem deutlich abgegrenzten Betriebsgelände überwacht werden, ist diese Regelung nicht einschlägig. Dies führte zu dem Ergebnis, dass nur die auf den Gehweg bzw. die Straße gerichtete Kamera nach dieser Vorschrift zu prüfen war.

Gemäß § 6b ist eine Videoüberwachung solcher Bereiche dann zulässig, wenn dies zur Wahrnehmung des Hausrechtes oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erfolgt und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen (hier: Passanten) überwiegen.

Der Firmeninhaber berief sich insoweit zwar auf sein Hausrecht, dies galt allerdings angesichts des Erfassungsbereiches der Kamera in dem Fall nicht. Zum Kontrollzeitpunkt war neben dem öffentlichen Gehweg auch ein Teil der Straße von der Kamera erfasst. Aufgrund weiterer, unmittelbar an den Gehweg anschließender Parkflächen war nicht klar erkennbar, wo das Firmengelände und damit der Geltungsbereich des Hausrechts beginnt.

Abhilfe konnte hier nur eine veränderte Kameraeinstellung bringen - ggf. in Verbindung mit einer deutlichen Abgrenzung des Firmengeländes durch entsprechende Kennzeichnung (z. B. als Privat- oder Firmenparkplatz mit Hinweis auf die praktizierte Videoüberwachung). Der Firmeninhaber hat die Empfehlungen der Aufsichtsbehörde unverzüglich umgesetzt.

Videoüberwachung im Betriebsgelände bzw. in den Werkhallen:

Rechtsgrundlage für die Videoüberwachung im Betriebsgelände bzw. in den Werkhallen ist § 28 Abs. 1 Nr. 2 BDSG. Danach ist die Datenerhebung und -verarbeitung zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stellen erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Eine permanente Videoüberwachung am Arbeitsplatz erzeugt grundsätzlich einen mit den Persönlichkeitsrechten des Arbeitnehmers nicht zu vereinbarenden Überwachungsdruck. Eine solche Videoüberwachung ist deshalb nur ausnahmsweise durch besondere Sicherheitsinteressen des Arbeitgebers zu rechtfertigen. Die Rechtsprechung besagt sogar, dass ein Arbeitnehmer unter Wahrnehmung des Zurückbehaltungsrechts solange seiner Arbeitspflicht nicht nachkommen muss, wie der ihm zugewiesene Arbeitsplatz ständig im Blickfeld einer unzulässig installierten Kamera liegt. Sicherlich muss bei der Abwägung der Zulässigkeit auch die Intensität der Beobachtung berücksichtigt werden. Der Eingriff in das Persönlichkeitsrecht wird demnach weniger schwerwiegend sein, wenn der Arbeitnehmer nur gelegentlich (z. B. beim Betreten eines Hauptganges) erfasst wird.

Vor diesem Hintergrund hat die Aufsichtsbehörde zumindest in Bezug auf die Überwachung des Einzelarbeitsplatzes ein deutliches Überwiegen der schutzwürdigen Interessen der dort beschäftigten Mitarbeiter gesehen. Ein weiterer Grund für die Unzulässigkeit ist, dass die dort installierte Kamera weder Arbeitsunfälle verhindert noch dazu führt, dass in einem solchen Fall sofort eine Alarmierung der verantwortlichen Stellen erfolgt. Sie ist allenfalls dazu ge-

eignet, gegebenenfalls den Hergang eines Arbeitsunfalls aufklären zu helfen. Dies allein kann aber nicht zur Zulässigkeit der Überwachung führen.

Der Firmeninhaber ist dieser Argumentation gefolgt und hat die betreffende Kamera neu installiert, so dass nur noch die Fensterfront im Bereich dieses Arbeitsplatzes erfasst wird.

Die Überwachung der Hauptgänge in der Werkhalle war zum Schutz der Firmenressourcen vor Einbrüchen nach Auffassung der Aufsichtsbehörde nicht ständig erforderlich. Es hätte ausgereicht, die Kamera nur außerhalb der Arbeitszeiten bzw. angesichts des 3-Schicht-Betriebes nur an den Wochenenden zu aktivieren. Dieser Lösung stimmte der Firmeninhaber nicht zu.

Die vom Firmeninhaber für eine ständige Überwachung vorgebrachten Gründe, nämlich die ganztägige Belieferung des Unternehmens mit Waren und die unvermeidbare Anwesenheit Dritter (Besucher, Kunden, Spediteure etc.), rechtfertigen keine ständige Videoüberwachung. Auch die Wahrung von Betriebsgeheimnissen oder die Verhinderung des (unbefugten) Technologietransfers sind keine ausreichenden Gründe.

Schließlich konnten sich Aufsichtsbehörde und Firmeninhaber darüber einigen, dass zumindest die Innenkameras in der Kernarbeitszeit, d. h. von Montag bis Freitag, jeweils von 7.00 Uhr bis 17.00 Uhr, deaktiviert sind.

Der Firmeninhaber wurde gebeten, seine Mitarbeiter über die geänderte Verfahrensweise im Unternehmen zu unterrichten.

Die Verwendung der Videokameras ist im vorliegenden Fall außerdem im Rahmen der Datenverarbeitung für eigene Zwecke (§ 4d BDSG) meldepflichtig. Die Meldepflicht ist u. a. dann gegeben, wenn

- personenbezogene Daten automatisiert verarbeitet werden (hier: Videoaufzeichnung),
- dies ausschließlich für eigene Zwecke erfolgt,
- kein Datenschutzbeauftragter bestellt ist,
- höchstens vier Arbeitnehmer mit der automatisierten Datenverarbeitung beschäftigt sind,
- weder eine Einwilligung der Betroffenen vorliegt noch
- die Datenverarbeitung der Zweckbestimmung eines Vertragsverhältnisses mit den Betroffenen dient und

- auch keine Vorabkontrolle erforderlich ist.

Im Falle des oben genannten Unternehmens ergibt sich die Zulässigkeit der Videoüberwachung nicht aus § 28 Abs. 1 Nr. 1 BDSG (Zweckbestimmung des Arbeitsverhältnisses), sondern aus § 28 Abs. 1 Nr. 2 BDSG (berechtigte Interessen der verantwortlichen Stelle in Abwägung mit den schutzwürdigen Interessen der Betroffenen).

Auf seine Meldepflicht hingewiesen, hat es das Unternehmen dann vorgezogen, auf freiwilliger Basis einen Datenschutzbeauftragten zu bestellen. Damit entfiel die Meldepflicht.

4.3.3 Automatische E-Mail-Weiterleitung an Vorgesetzte

Ein mittelständisches, weltweit agierendes Industrieunternehmen hatte seine 18 Verwaltungsarbeitsplätze mit einem Internetzugang ausgestattet und den dort tätigen Mitarbeitern eine eigene personenbezogene E-Mail-Adresse zugewiesen.

In den Bereichen „Kundenservice“ und „Auftragsbearbeitung“ waren insgesamt vier Mitarbeiter tätig, wovon ein Mitarbeiter Mitglied im Betriebsrat war und darüber hinaus auch gewerkschaftlich agierte.

Eine Voreinstellung im Computer regelte, dass grundsätzlich alle dort eingehenden E-Mails an den Leiter Kundenservice weitergeleitet wurden. Die zuständigen Mitarbeiter hatte man hiervon in Unkenntnis gelassen.

Die Weiterleitung betraf neben dienstlichen auch interne Nachrichten, E-Mails mit gewerkschaftlichem Inhalt, für den Betriebsrat bestimmte sowie und private E-Mails.

Als Begründung für diese Vollkontrolle eingehender E-Mails wurde angegeben, dass es sich ein Exportunternehmen nicht leisten könne, eingehende E-Mails länger als 24 Stunden unbearbeitet zu lassen, sollte der zuständige Bearbeiter abwesend sein. Darüber hinaus berief sich das Unternehmen auf die Veröffentlichung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur datenschutzgerechten Nutzung von E-Mail- und anderen Internet-Diensten am Arbeitsplatz, wonach der Arbeitgeber von dienstlichen E-Mails seiner Beschäftigten im selben Maße Kenntnis nehmen darf, wie von deren dienstlichem Schriftverkehr.

Die Verfahrensweise des Unternehmens hat die Aufsichtsbehörde als unzulässig bewertet und dies wie folgt begründet:

1. Die durch einen Vorgesetzten erfolgende Vollkontrolle (Kenntnisnahme und Speicherung) aller auf bestimmten personengebundenen Accounts eingehenden E-Mails ist weder verhältnismäßig noch erforderlich und stellt einen unzulässigen Eingriff in das Persönlichkeitsrecht der betroffenen Arbeitnehmer dar. Dies gilt umso mehr, als die Weiterleitung ohne Wissen der Betroffenen erfolgte.

2. Auch die Sicherstellung einer umgehenden Reaktion auf eingehende dienstliche E-Mails kann die Vollkontrolle in der praktizierten Form nicht rechtfertigen. Für diesen Zweck existieren alternative Lösungen, die weniger in das Persönlichkeitsrecht der Arbeitnehmer eingreifen. Zum Beispiel können (zusätzliche) funktionsbezogene E-Mail-Accounts nach dem Muster *kundenservice@firma.de* eingerichtet werden. Die Weiterleitung von auf derartigen Accounts eingehenden E-Mails - auch an mehrere Nutzer - ist aus datenschutzrechtlicher Sicht unbedenklich. Bei personenbezogenen Accounts hingegen ist selbst ein bestehendes Verbot privater Mitbenutzung des E-Mail-Systems nicht geeignet, die Zulässigkeit der automatischen Weiterleitung der E-Mails zu begründen. Der Absender einer E-Mail, der seine Nachricht nicht allgemein an das Unternehmen, sondern an einen Mitarbeiter schickt, muss nicht davon ausgehen, dass andere Personen von dieser E-Mail Kenntnis erlangen.
   Da E-Mail-Systeme bzw. -Dienste dem Telekommunikationsbereich zuzuordnen sind, kann zudem auf die Analogie zu Telefongesprächen verwiesen werden.

3. Für den Fall der Abwesenheit besteht zudem die Möglichkeit, eine automatische Antwortfunktion („Abwesenheits-Assistent“) zu aktivieren, mit der die Absender von E-Mails auf die Abwesenheit des Mitarbeiters hingewiesen und alternative Ansprechpartner benannt werden können.

4. Die Aussage, wonach ein Arbeitgeber verfügen kann, dass ihm jede ein- und ausgehende E-Mail seiner Mitarbeiter zur Kenntnis zu geben ist, bedeutet nicht, dass alle eingehenden E-Mails automatisch an den Vorgesetzten weitergeleitet werden dürfen.

5. Ein Arbeitgeber hat unabhängig davon zwar grundsätzlich das Recht, den dienstlichen Zweck des E-Mail-Verkehrs seiner Beschäftigten zu prüfen, jedoch darf dies für Präventi-

onszwecke zunächst nur stichprobenartig erfolgen. Eine automatisierte Vollkontrolle durch den Arbeitgeber hingegen ist nur bei Vorliegen eines konkreten Missbrauchsverdachtes im Einzelfall zulässig.

6. Ungeachtet dessen darf auch der Arbeitnehmer selbst seine E-Mail-Adresse nicht für Zwecke privater Kommunikation (darunter fällt auch die Gewerkschaft) an Dritte herausgeben. Grundsätzlich handelt es sich auch beim E-Mail-System um ein betriebliches Arbeitsmittel, welches ausschließlich der dienstlichen Kommunikation dient.

7. Bei Beschäftigten, denen besondere Verschwiegenheitspflichten obliegen (z. B. Betriebsrat), ist sicherzustellen, dass der Arbeitgeber keine Kenntnis von Nachrichten sowie deren Absendern erlangen kann. Er darf die Nutzungs- und Verbindungsdaten von Betriebsratsmitgliedern nur insoweit kontrollieren, als dies im Einzelfall aus Gründen der Kostenkontrolle erforderlich ist.

Nur funktionsbezogene E-Mail-Adressen können eine datenschutzgerechte automatische Weiterleitung eingehender E-Mails (Kopien) an weitere Empfänger ermöglichen.
Viele Unternehmen haben das bereits erkannt und praktizieren diese Verfahrensweise - insbesondere im Bereich der Kundenbetreuung.

In dem eingangs dargestellten Fall wird nun ebenso verfahren. Darüber hinaus hat auch der Betriebsrat eine eigene funktionsbezogene E-Mail-Adresse erhalten. Zur Schaffung der notwendigen Transparenz sind alle Mitarbeiter zudem über den Umgang mit den auf den funktionsbezogenen Accounts eingehenden E-Mails informiert worden. Dem Betriebsrat wurde der Abschluss einer Betriebsvereinbarung zur Nutzung von E-Mail- und anderen Internetdiensten empfohlen.

4.3.4 Arbeitnehmerüberwachung mittels Spyware[2]

„Spector Pro“ ist eine Überwachungssoftware zur Aufnahme aller Computer- und Internetaktivitäten. Das Programm verfügt über eine ausgereifte Tarnfunktion und kombiniert mehrere leistungsfähige Monitoring Tools; dazu gehört die permanente Aufnahme aller Bildschirmin-

[2] Als „Spyware“ wird üblicherweise Software bezeichnet, die persönliche Daten des Benutzers ohne dessen Wissen oder gar Zustimmung an den Hersteller der Software (das so genannte „Call Home“) oder an Dritte sendet. Oft wird Spyware verwendet, um Produkte scheinbar kostenlos anzubieten.

halte und Tastenanschläge. Das Arbeitsverhalten des jeweiligen Nutzers am PC wird detailgetreu aufgezeichnet und kann im Nachgang lückenlos nachvollzogen werden. Damit handelt es sich um eine Vollkontrolle der PC-Tätigkeiten des jeweiligen Nutzers. Die mit dieser Software erhobenen und gespeicherten Daten dokumentieren den Umgang des Nutzers mit seinem PC und sind damit personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG.

Diese Überwachungssoftware hatten zwei Geschäftsführer nach Dienstschluss auf dem Arbeitsplatz-PC eines ihrer Arbeitnehmer ohne dessen Wissen durch eine Dienstleistungsfirma installieren lassen. Der Betroffene entdeckte dies am Folgetag und informierte anschließend die Aufsichtsbehörde darüber.

Die Zulässigkeit des Einsatzes der Überwachungssoftware ist zunächst nach § 28 Abs. 1 Nr. 1 BDSG zu beurteilen. Danach ist das Erheben, Speichern oder Nutzen personenbezogener Daten im Rahmen der Zweckbestimmung des Arbeitsverhältnisses zulässig. Maßgebend für die Zulässigkeit der Verwendung von Überwachungssoftware ist, dass der Arbeitgeber die Daten zur Wahrnehmung der ihm aus dem Arbeitsverhältnis zustehenden Kontrollbefugnisse benötigt. Eine Grenze wird dieser Kontrolle allerdings durch den Persönlichkeitsrechtsschutz des Arbeitnehmers gesetzt: Die berechtigten Interessen des Arbeitgebers sind gegen die schutzwürdigen Belange des Arbeitnehmers abzuwägen. Der Grundsatz der Verhältnismäßigkeit ist hierbei zu beachten.

Wird wie im vorliegenden Fall die Sicherstellung der ordnungsgemäßen und reibungslosen Funktion des Unternehmensnetzes als berechtigtes Interesse angeführt, muss dies zunächst zwar anerkannt werden, jedoch nur in dem Fall, wenn ein begründeter Verdacht gegen den Betroffenen vorgelegen hätte. Dies war jedoch hier nicht der Fall.

Es fehlt bereits an der Erforderlichkeit der Überwachungsmaßnahme zur Durchsetzung der berechtigten Interessen. Außerdem muss bei einer heimlichen Überwachung, die lückenlos und ohne begründeten Verdacht erfolgt, in jedem Fall ein Überwiegen der schutzwürdigen Interessen des Betroffenen angenommen werden.

Die Installation von Überwachungssoftware auf dem Computer des Mitarbeiters war also unzulässig. Die Geschäftsführer waren jedoch bis zuletzt nicht bereit, dies anzuerkennen. Die in diesem Zusammenhang erlassenen Bußgeldbescheide sind durch das Amtsgericht bestätigt worden (vgl. Pkt. 9).

4.3.5 Videoüberwachung eines Wohn- und Gewerbegebietes

In einer an die Aufsichtsbehörde gerichteten Beschwerde wurde auf diverse Videokameras in einem städtischen Wohn- und Gewerbegebiet aufmerksam gemacht. Der Beschwerdeführer war Mieter eines Wohnhauses, welches sich im Erfassungsbereich einer der insgesamt vier an Gebäuden installierten Videokameras befand.

Drei dieser Kameras waren fest montiert und auf die Einfallstraßen gerichtet. Sie erfassten den gesamten Fahrzeug- und einen großen Teil des Fußgängerverkehrs in und aus dem Gebiet. Die Kameras waren mit den Monitoren eines vertraglich gebundenen Wachunternehmens verbunden. Die Videobilder wurden durch den Betreiber aufgezeichnet.

Die vierte, mit einer Zoom-Funktion versehene Kamera war schwenkbar und wurde durch Mitarbeiter des Wachunternehmens bedient. Von der Kamera wurden der gesamte zentrale Platz des Gebietes, wesentliche Teile der dort entlang führenden Straßen und Wohngebäude erfasst.

Für die Aufzeichnung wurde ein digitaler Ringspeicher mit einer Speicherkapazität von ca. 1,5 Tagen genutzt. Im Falle besonderer Vorkommnisse sollten die entsprechenden Aufzeichnungen auf ein Videoband zur weiteren Auswertung durch die Polizei oder durch betroffene Mieter gesichert werden.

Der Zweck der Videoüberwachung war durch die verantwortliche Stelle wie folgt beschrieben worden:

- Erhöhung der Sicherheit im Wohn- und Gewerbegebiet,
- Unterstützung der Polizei bei Aufklärung von Gesetzesverstößen (Beweissicherung),
- Unterstützung der Mieter bei Vorkommnissen (Beweissicherung),
- Sicherung des Gebäudeeigentums des Betreibers,
- Unterstützung der Arbeit des Wachdienstes.

Das Wohn- und Gewerbegebiet mit seinen öffentlichen Straßen, Wegen und Plätzen ist als öffentlich zugänglicher Raum zu betrachten. Die Zulässigkeit ist folglich nach § 6b BDSG zu beurteilen. Von den Erlaubnistatbeständen des § 6b Abs. 1 BDSG (reine Beobachtung) kam

allenfalls Nr. 3 „Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke“ in Betracht. Dabei gilt jedes wirtschaftliche und ideelle Interesse als berechtigt, das auch objektiv begründbar ist

Werden die o. g. Zwecke der Videoüberwachung unter diesem Aspekt betrachtet, so wird deutlich, dass es dem Betreiber in erster Linie um die Förderung der öffentlichen Sicherheit und Ordnung und damit um eine Attraktivitätsverbesserung des Gebietes für die Mieter ging.

Ein weiteres Kriterium ist die Erforderlichkeit der Videoüberwachung für den beabsichtigten Zweck (Gewährleistung der Sicherheit, Attraktivitätserhöhung). Diese ist nur gegeben, wenn dieser Zweck nicht mit einem anderen zumutbaren, weniger in die Rechte der Betroffenen eingreifenden Mittel erreicht werden kann. Hier war bereits ein Wachunternehmen verpflichtet, welches regelmäßige Kontrollgänge durchgeführt hat. Allerdings kann eine Videoüberwachung effektiver und umfassender zur Gewährleistung der Sicherheit beitragen als Kontrollgänge eines Wachdienstes. Bis auf vereinzelte Vorkommnisse in der Vergangenheit war eine besondere Gefährdungslage (Häufung von Einbrüchen, Überfälle auf Personen, Kriminalitätsschwerpunkt) in diesem Fall nicht gegeben.

Bei der Abwägung der schutzwürdigen Interessen der Betroffenen war zu berücksichtigen, dass private Wohnungen im Überwachungsbereich lagen. Einige der Mieter fühlten sich beim Aufenthalt auf dem Balkon durch die permanente Beobachtung belästigt. Selbst das Verlassen und Aufsuchen ihrer Wohnungen geschah unter der Beobachtung der Kameras. Von jedem, der sich in diesem Gebiet aufhielt (Besucher, Mitarbeiter dort ansässiger Unternehmen etc.) wurden zwangsläufig personenbezogene Daten erhoben. Ein Hinweis auf die permanente Videoüberwachung des Gebietes fehlte.

Ebenso wurden der zentral gelegene Platz und gastronomische Einrichtungen teilweise lückenlos erfasst und aufgezeichnet.

Auf öffentlichen Wegen hat grundsätzlich das Recht des Bürgers Vorrang, sich in der Öffentlichkeit ohne Überwachung durch private Stellen frei bewegen zu können (BGH, Urteil vom 25.04.1995, RDV 1996, 26). Das Amtsgericht Berlin-Mitte hat in seinem Urteil vom 18.12.2003 (DuD 2004, 309 ff.) festgestellt, dass die Schutzbedürftigkeit der Betroffenen regelmäßig in solchen Bereichen besonders groß ist, in denen sich Menschen länger aufhalten und/oder typischerweise miteinander kommunizieren. Den Betroffenen ist dabei die Video-

überwachung eines öffentlichen Fußgängerüberweges allenfalls in einem einen Meter breiten Randstreifen zur Hauswand (des zu sichernden Gebäudes) zuzumuten.

Im Ergebnis musste die Aufsichtsbehörde damit die Rechtswidrigkeit der Videoüberwachung des Wohn- und Gewerbegebietes feststellen. Insbesondere war davon auszugehen, dass die Bebauung (Wohngebäude) und die Zweckbestimmung des Gebietes (in erster Linie die Freizeiteinrichtungen) dazu führten, dass das schutzwürdige Interesse der Betroffenen, sich frei und unbeobachtet in der Öffentlichkeit bewegen zu können, das Sicherheitsinteresse der verantwortlichen Stelle klar überwog.

Die Aufsichtsbehörde empfahl die Erarbeitung eines Einsatz- und Nutzungskonzeptes, in das u. a. folgende Maßnahmen aufgenommen werden sollen:

- Die steuerbare Kamera wird fest arretiert und ohne Zoommöglichkeit auf einen dem Hausrecht unterliegenden Bereich ausgerichtet.
- Die Überwachung der Zufahrtsstraßen wird aufgegeben.
- Die gewerblichen Hausfronten der Gebäude des Betreibers werden inkl. eines schmalen Gehwegstreifens durch fest installierte, nicht zoombare Kameras überwacht.
- Wohngebäude werden nicht in die Überwachung einbezogen.
- Die Aufzeichnungszeiten werden auf den Zeitraum 17.00 Uhr - 05.00 Uhr begrenzt.
- Eine ausreichende Anzahl von Hinweisschildern soll so angebracht werden, dass jeder, der das Gebiet betritt oder befährt, rechtzeitig über die Überwachung in Kenntnis gesetzt wird.

4.3.6 Ärztliche Schweigepflicht gegenüber Ehepartnern

Ein Ehemann hatte erhebliche gesundheitliche Probleme, woraufhin seine Frau einige Medikamente in der Apotheke besorgen wollte. Dort wurde ihr nach Schilderung des Krankheitsbildes geraten, sofort einen Arzt aufzusuchen. Auf Nachfrage der erst kürzlich zugezogenen Frau wurde ihr ein Arzt in der Nähe empfohlen, der kurzfristig Hausbesuche durchführen würde. Nach Darstellung der Ehefrau weigerte sich der Arzt nach der Namensnennung des Patienten, einen Hausbesuch durchzuführen. Auf Nachfrage der Ehefrau gab er den Namen des Ehemanns in seinen PC ein und begann, der Frau aus dessen Krankheitsgeschichte zu berichten. Dies betraf Informationen über vor mehreren Jahren erfolgte Behandlungen und Befindlichkeiten des Ehemannes (Selbstmordversuche, weiterbehandelnde Ärzte, Trunken-

heit, Unberechenbarkeit, Arbeitslosigkeit, psychische Störungen etc.). Diese Sachverhalte waren der Ehefrau bislang nicht bekannt und ihr von ihrem Mann verschwiegen worden.

Nach dieser Darstellung bestand Grund zu der Annahme, dass der Arzt gegen die in § 203 Strafgesetzbuch (StGB) verankerte Schweigepflicht verstoßen hat. Ein Verstoß gegen die ärztliche Schweigepflicht wird gem. § 205 StGB nur auf Antrag verfolgt. Den Betroffenen hat die Aufsichtsbehörde empfohlen, umgehend Strafanzeige bei der Polizei zu stellen, was anschließend erfolgt ist.

Ungeachtet des durch die Staatsanwaltschaft eingeleiteten Ermittlungsverfahrens beurteilt die Aufsichtsbehörde den Sachverhalt abschließend wie folgt:

Schutzzweck der ärztlichen Schweigepflicht ist die Geheim- und Individualsphäre des Einzelnen. Vom umfassenden Schutzbereich werden nicht nur Details einer ärztlichen Behandlung, wie Diagnosen, Behandlungsmaßnahmen oder Ähnliches erfasst. Auch Informationen zu einer ärztlichen Behandlung als solche dürfen nicht unbefugt an Dritte weitergegeben werden. Hierzu gehören insbesondere Umstände, die sich auf den persönlichen Lebensbereich beziehen wie z. B. Erkenntnisse und Informationen über familiäre und partnerschaftliche Probleme. Ausnahmen bedürfen einer besonderen Begründung und Rechtfertigung.

Dies können sein:

- die ausdrückliche Einwilligung des Patienten,
- bestimmte, ansteckende Krankheiten, die der gesetzlichen Meldepflicht unterliegen,
- Fälle, in denen polizeilich ermittelt werden muss (Kapitalverbrechen) und
- im Sozialrecht verankerte Mitwirkungs- und Auskunftspflichten.

Die ärztliche Schweigepflicht gilt umfassend. Demnach dürfen Dritte (auch Ehepartner) nicht ohne weiteres über Patientendaten informiert werden. Anders verhält es sich, wenn der Patient die Anwesenheit eines Verwandten bei einem ärztlichen Gespräch ausdrücklich wünscht oder zu erkennen gibt, dass eine Entbindung von der Schweigepflicht gewollt ist.

Vor diesem Hintergrund war die Information der Ehefrau durch den Arzt unzulässig und stellt eine Verletzung der ärztlichen Schweigepflicht dar. Es ist nicht erkennbar, dass einer der o. g. Ausnahmetatbestände erfüllt ist. Soweit geltend gemacht worden war, dass zur Klärung der Akutsituation Fragen zu stellen waren, begründet dies weder die Notwendigkeit noch die Zulässigkeit dieser derart umfassenden Unterrichtung der Ehefrau.

Die Familie stellte Strafanzeige, so dass die Aufsichtsbehörde von weiteren Schritten in dieser Angelegenheit absah.

4.3.7 Umgang mit Patientendaten in einer ärztlichen Gemeinschaftspraxis

In einem von der Aufsichtsbehörde zu untersuchenden Fall vermutete die Betroffene einen Verstoß gegen die ärztliche Schweigepflicht.

Die Betroffene war bei ihrem Hausarzt, der zusammen mit seiner Frau eine Gemeinschaftspraxis betreibt, in Behandlung. Der Hausarzt hatte die Betroffene zur weiteren Untersuchung in ein Krankenhaus überwiesen. Wenige Tage später war die Betroffene von einer Bekannten daraufhin angesprochen worden, wie es ihr gehe und warum sie ins Krankenhaus musste. Da die Betroffene niemandem davon erzählt hatte, hätte die Bekannte gar nichts davon wissen dürfen. Die Bekannte hatte auf entsprechende Nachfrage bestätigt, dies von ihrer Ärztin, der Frau des Hausarztes der Betroffenen, erfahren zu haben.

Die beiden Ärzte der Gemeinschaftspraxis bestritten, derartige Gespräche mit bzw. über jeweils andere Patienten geführt und auf diese Weise unbefugt personenbezogene Daten weitergegeben zu haben.

Die Aufsichtsbehörde hat den Vorgang jedoch zum Anlass genommen, die Arztpraxis einer allgemeinen datenschutzrechtlichen Kontrolle zu unterziehen.

Es wurde zunächst festgestellt, dass in der Arztpraxis entgegen der gesetzlichen Pflicht kein Datenschutzbeauftragter (§ 4f BDSG) bestellt war.

Des Weiteren wurde festgestellt, dass die Beschäftigten der Arztpraxis nicht auf das Datengeheimnis gemäß § 5 BDSG verpflichtet worden waren, obwohl diese mit der Erhebung, Verarbeitung und Nutzung der Patientendaten betraut sind. Die in den Arbeitsverträgen enthaltene Bestimmung zur Geheimhaltungs- bzw. Verschwiegenheitspflicht, auf die sich die Ärzte beriefen, ersetzt die Verpflichtung gemäß § 5 BDSG nicht, da das Datengeheimnis eine wesentlich größere Reichweite als die Verschwiegenheitspflicht besitzt.

Die Ärzte wurden aufgefordert, einen (gemeinsamen) Datenschutzbeauftragten für die Gemeinschaftspraxis zu bestellen und die erforderlichen Belehrungen und Verpflichtungen auf das Datengeheimnis durchzuführen. Diese Maßnahmen wurden seitens der Arztpraxis umgesetzt.

Darüber hinaus hat die Aufsichtsbehörde beide Ärzte gebeten, in ihrer Praxis zukünftig dafür Sorge zu tragen, dass nur der aus medizinischer Sicht erforderliche Informationsaustausch erfolgt. Die Aufsichtsbehörde hat in diesem Zusammenhang darauf hingewiesen, dass die ärztliche Schweigepflicht auch gegenüber anderem medizinischen Personal, das seinerseits der ärztlichen Schweigepflicht unterliegt, also auch gegenüber dem anderen Arzt der Gemeinschaftspraxis, der nicht in die Behandlung des Patienten eingebunden ist, gilt.

4.3.8 Auskünfte an die Betroffenen durch Wirtschaftsauskunfteien

Bei den Aufsichtsbehörden häufen sich Beschwerden, die die Tätigkeit von Handels- und Wirtschaftsauskunfteien betreffen. Auslöser sind regelmäßig die Benachrichtigungsschreiben der Auskunfteien, die diese bei erstmaliger Übermittlung personenbezogener Daten an die Betroffenen versenden.

Das BDSG erlaubt Wirtschaftsauskunfteien - auch ohne Kenntnis und ohne Einwilligung der Betroffenen -, personenbezogene Daten zu speichern und an Dritte zu übermitteln, wenn diese ein berechtigtes Interesse an der Kenntnis dieser Daten glaubhaft dargelegt haben. Als berechtigtes Interesse sind wirtschaftliche Interessen anerkannt. So fällt hierunter die Anbahnung und Erweiterung geschäftlicher Beziehungen, wie die Einräumung von Krediten, der Abschluss von Raten-, Leasing- oder Versicherungsverträgen, der Kauf oder die Bestellung auf Rechnung (bei Versandhäusern), die Übernahme einer Bürgschaft oder die Realisierung bestehender Forderungen. Ziel dieser Regelung ist es, den Unternehmen, die gegenüber ihren Kunden in Vorleistung treten müssen, eine Abschätzung des damit verbundenen wirtschaftlichen Risikos zu ermöglichen.

Ein berechtigtes Interesse muss dargelegt werden. Darüber hinaus darf kein Grund zu der Annahme bestehen, der Betroffene habe ein schutzwürdiges Interesse am Ausschluss der Übermittlung, d. h., die Persönlichkeitsrechte des Betroffenen sind gegen die Interessen der anfragenden Stelle abzuwägen. Schutzwürdige Interessen überwiegen jedenfalls dann, wenn die Angaben nicht der Beurteilung der Zahlungsfähigkeit/Kreditwürdigkeit dienen (z. B. Gesundheitsdaten oder Vermögensangaben über Bekannte oder Verwandte). Es kann davon ausgegangen werden, dass schutzwürdige Interessen Betroffener nicht überwiegen, wenn wahrheitsgemäße, objektive und aussagekräftige Informationen über die Bonität bzw. über die bestehenden wirtschaftlichen Verhältnisse weitergegeben werden.

Auskunfteien werten für Ihre Tätigkeit in erster Linie öffentlich zugängliche Quellen, z. B. Telefon- und Adressbücher, Schuldnerverzeichnisse der Amtsgerichte und sonstige öffentliche Register aus. Darüber hinaus werden auch die Betroffenen um freiwillige Selbstauskünfte (beispielsweise im Zusammenhang mit der unten erläuterten Auskunftserteilung an den Betroffenen selbst) ersucht. Die anfragenden Stellen geben auch Daten über Geschäftsbeziehungen weiter.

Gemäß § 33 Abs. 1 Satz 2 BDSG sind Wirtschaftsauskunfteien verpflichtet, die Betroffenen von der erstmaligen Übermittlung von Daten zu ihrer Person zu unterrichten. Diese Unterrichtung hat zeitnah (innerhalb von zwei bis vier Wochen) zu erfolgen und dient dem Zweck, die Betroffenen von der Speicherung und Übermittlung von Daten zu ihrer Person in Kenntnis zu setzen und ihnen so zu ermöglichen, ihre Rechte nach dem BDSG wahrzunehmen.

Betroffene sollten daher zunächst ein formloses schriftliches Auskunftsersuchen gem. § 34 BDSG an die Auskunftei richten, um zu erfahren, welche Daten über sie gespeichert und an wen sie übermittelt worden sind. Der Betroffene kann dann weitere Rechte geltend machen, z. B. die Berichtigung unrichtiger Daten oder die Löschung seiner Daten verlangen.

Für die Aufsichtsbehörde problematisch ist die Information der Betroffenen über die bei den Wirtschaftsauskunfteien anfragenden Stellen. Die Wirtschaftsauskunfteien beschränken sich auf die Angabe von Empfängerkategorien und vermeiden die genaue Angabe der Empfänger. Die Auskunft über Herkunft und Empfänger der Daten kann gem. § 34 Abs. 1, 2 BDSG jedoch nur dann verweigert werden, wenn das Interesse der Auskunftei an der Wahrung des Geschäftsgeheimnisses überwiegt. Dies muss zunächst dem Betroffenen gegenüber geltend gemacht und ggf. später der Aufsichtbehörde nachgewiesen werden.

Um die genannte Regelung praxisfähig zu gestalten und eine Benachteiligung der Betroffenen zu vermeiden, haben sich die obersten Aufsichtsbehörden für den Datenschutz auf eine Reihe von Fallkonstellationen geeinigt, bei denen grundsätzlich eine Information des Betroffenen über den Empfänger der Daten zu erfolgen hat.

Dazu gehören:

- Der Betroffene trägt begründete Zweifel an der Richtigkeit der Daten vor.
- Der Betroffene beabsichtigt - ausgehend von unzutreffenden Daten -, Schadensersatz- oder Richtigstellungsansprüche geltend zu machen.

- Der Betroffene gibt an, der Auskunftsempfänger habe den Auskunftsdatensatz unberechtigterweise an Dritte weitergegeben.
- Der Betroffene trägt vor, der Auskunftsempfänger könne unter keinen Umständen ein berechtigtes Interesse an der Auskunft gehabt haben.
- Der Empfänger gehört einer der folgenden Branchen an: Versicherungen, Versandhandel, Telekommunikation, Banken, Leasing-/Factoringgesellschaften, Konzerngesellschaften.

Ansonsten ist jeweils eine Einzelabwägung zwischen dem Auskunftsinteresse des Betroffenen und dem Geschäftsgeheimnis der Auskunftei vorzunehmen. Eine Ablehnung der Auskunft ohne diese Einzelfallprüfung ist nicht zulässig.

Im Berichtszeitraum ist das Regierungspräsidium Dresden in zwei Fällen wegen einer unterbliebenen Unterrichtung des Betroffenen über den Empfänger der Daten eingeschaltet worden:

Der erste Fall betraf die Anfrage eines Versicherungsunternehmens (s. o.). Hier hat die Auskunftei den Betroffenen nach Aufforderung durch die Aufsichtsbehörde selbst über den Empfänger unterrichtet.

Im zweiten Fall hatte die Wirtschaftsauskunftei auf der Wahrung des Geschäftgeheimnisses bestanden und dabei angeführt, dass das im Bereich der Baustofftechnik tätige Unternehmen als langjähriger Großkunde der Auskunftei auf deren Diskretion vertraut. Die Aufsichtsbehörde hat diese Auffassung nicht akzeptiert und den Betroffenen nachfolgend selbst über den Auskunftsempfänger unterrichtet. Dafür waren die folgenden Erwägungen maßgebend:

Das anfragende Unternehmen ist eines der führenden europäischen Unternehmen für den professionellen Schutz und die Werterhaltung von Bauwerken und Kulturdenkmälern in Zusammenarbeit mit Handwerk und Industrie; direkte Geschäftsbeziehungen zu nicht im Handwerk tätigen Personen dürften die Ausnahme darstellen. Es ist nicht davon auszugehen, dass die Offenlegung dieses Empfängers gegenüber dem Betroffenen zu einer nachhaltigen Störung der Geschäftstätigkeit des Unternehmens führt. Einerseits besteht kein besonderes Verhältnis zwischen dem Baustofflieferanten und dem Betroffenen, andererseits kann bei Unternehmen dieser Größenordnung mit europaweiten Geschäftsaktivitäten davon ausgegangen werden, dass zur Minimierung des unternehmerischen Risikos auch Anfragen bei Wirtschaftsauskunfteien die Regel sind. Anders verhielte es sich bei einem Handwerker aus der unmittelbaren Umgebung des Betroffenen.

4.3.9 Aufdeckung von Spielerpass-Manipulationen im Fußball

Ein in der Kreisklasse aktiver Fußballverein wandte sich an die Aufsichtsbehörde mit der Bitte, die im Rahmen eines Sportgerichtsverfahrens ihm gegenüber erhobene Forderung zur Übergabe von Identitätsnachweisen für alle aktiven Mitglieder datenschutzrechtlich prüfen zu lassen. Die Recherchen der Aufsichtsbehörde ergaben zunächst folgenden Sachverhalt:

Beim Vereinswechsel eines Spielers wurden Abweichungen bei dessen Geburtsdatum festgestellt. Dies führte im Verein zum Verdacht einer Datenmanipulation. Hintergrund ist die anhand des Geburtsdatums vorzunehmende Einteilung der Spieler in Altersklassen, welche insbesondere im Nachwuchsbereich die Spielstärke einer Mannschaft oftmals entscheidend beeinflussen kann. Der Einzelfall wurde durch das beim Kreisverband Fußball (KVF) angesiedelte Sportgericht zum Anlass genommen, von diesem Fußballverein zwecks Ausschluss weiterer Missbrauchsfälle Kopien der Spielerpässe sowie Identitätsnachweise aller Spieler (10 Mannschaften = ca. 250 Aktive) abzufordern. Die von einigen Mitgliedern/Eltern vorgetragenen datenschutzrechtlichen Bedenken wurden mit Verweis auf das Zweckbindungsgebot zurückgewiesen.

Datenschutzrechtlich ist die pauschale Abforderung der Kopien von Identitätsnachweisen aller aktiven Mitglieder des Vereins unverhältnismäßig und damit unzulässig.

Mitglieder des KVF sind die Vereine selbst. Als Rechtsgrundlage für die Tätigkeit des Sportgerichts kommt nur § 28 Abs. 1 Nr. 2 BDSG in Betracht, wenn die Datenerhebung und -speicherung zur Wahrung berechtigter Interessen des KVF erforderlich ist. Es darf kein Grund zu der Annahme bestehen, dass entgegenstehende schutzwürdige Interessen der Betroffenen überwiegen.

Der Satzung des KVF war zu entnehmen, dass das Sportgericht als erste Rechtsprechungsinstanz in allen Streitigkeiten der Satzung und der Ordnungen fungiert. Für die Aufsichtsbehörde ergibt sich daraus zunächst eine Zuständigkeit für die Klärung von Einzelfällen, nicht aber eine unabhängige Kontrollbefugnis aller Vereinsmitglieder bzw. einer Vereinsabteilung. Ungeachtet dessen ist davon auszugehen, dass die schutzwürdigen Interessen von Betroffenen einer pauschalen Anforderung von Identitätsnachweisen aller Vereinsmitglieder entgegenstehen.

Angesichts der berechtigten KVF-Interessen wurde auf einen entsprechenden Prüfauftrag des KVF-Vorstandes verwiesen, in dem der beabsichtigte Ausschluss weiterer Missbrauchsfälle, der Verlust des Versicherungsschutzes und der Betrug an den Spielgegnern angeführt wurden. Die schutzwürdigen Interessen der Betroffenen stehen denen der KVF entgegen. Eine Anfertigung von Kopien der Spielerpässe und die Erbringung von Identitätsmerkmalen widerspricht dem Erforderlichkeits- und Verhältnismäßigkeitsprinzip.

Die vom Verein angeführte strenge Zweckbindung der abgeforderten Daten ist durch die Aufsichtsbehörde nicht angezweifelt worden. Es wurde jedoch klargestellt, dass die Relevanz einer Zweckbindung erst nach Klärung der Zulässigkeit der Datenerhebung gegeben ist. Bei entsprechenden Änderungen der grundsätzlichen Verfahrensweise bestehen durchaus Kontrollmöglichkeiten, die die schutzwürdigen Interessen der Betroffenen in ausreichendem Maß berücksichtigen.

Die von der Aufsichtsbehörde vorgeschlagene Alternative, schriftliche Bestätigungen durch die Eltern der Kinder- und Jugendlichen einzuholen, ist vom KVF abgelehnt worden. Auch eine Regelung in der Spielordnung (Passkontrolle im Nachwuchsbereich) erwies sich als untauglich (Angabe eines falschen Geburtsdatums durch betreffende Spieler).

Eine datenschutzgerechte Lösung ist die Einsichtnahme in die Identitätsnachweise vor Ort. Die Mitglieder könnten sich gegenüber Vertretern des Sportgerichts ausweisen (Sichtkontrolle der Geburtsurkunde, des Personal- oder Schülerausweises). So könnte ohne Anfertigung einer Kopie ein Identitätsnachweis gegenüber dem Sportgericht erbracht werden.

Dem Betroffenen kann angeboten werden, freiwillig eine Ausweiskopie vorzulegen (z. B. für den Fall der Abwesenheit). Hierbei sollte klar darauf hingewiesen werden, dass nicht erforderliche Angaben (z. B. Angaben zu Eltern, Geburtsort, Ausweisnummer etc.) geschwärzt werden können. Für die ordnungsgemäße Bekanntgabe dieser Verfahrensweise an die Mitglieder ist ausschließlich der Verein verantwortlich.

Minderjährige Vereinsmitglieder mit Spielerpässen mit Ausstellungsdatum ab Juli 2004 sind von einer Überprüfung ausgeschlossen. Der Sächsische Fußballverband nimmt seitdem eine Überprüfung der Spielerpassdaten auf wahrheitsgemäße Angaben mittels eines ihm vorzulegenden Identitätsnachweises selbst vor (§ 7 Jugendordnung). Vor diesem Hintergrund dürften in den unteren Altersklassen keine Überprüfungen durch das Sportgericht nötig sein.

4.3.10 Erhebung von Personalausweisdaten bei bargeldlosem Bezahlen

Das weit verbreitete bargeldlose Bezahlen mit EC-Karte im Lastschriftverfahren birgt auch die Gefahr des Missbrauchs in sich. Immer öfter kommt es zu erheblichen Zahlungsausfällen im Handel, weil Bankkonten nicht gedeckt sind oder der Lastschrift seitens des Kunden widersprochen wird. Letzteres ist insbesondere dann der Fall, wenn mit gestohlenen EC-Karten bezahlt wird. Die auf den Lastschriftbelegen enthaltene Einwilligungsklausel erlaubt es den kontoführenden Banken, im Fall der Rücklastschrift die Anschrift des Kontoinhabers an den Händler zu übermitteln. Die Banken sind dadurch zwar ermächtigt, aber nicht verpflichtet, die Daten zu übermitteln. Oft verweigern deshalb Banken die Auskunft über den Kontoinhaber oder verlangen für die Auskunft eine erhebliche Gebühr vom Händler, die zum Teil den Wert der bezahlten Ware übersteigt. In diesen Fällen hat der Einzelhändler dann praktisch keine Möglichkeit mehr, den Kunden zu ermitteln und muss die fehlenden Gelder als Verlust verbuchen.

Bei der Zahlung mit EC-Karte unter Eingabe der persönlichen PIN besteht dieses Risiko nicht, doch dieses Verfahren wird insbesondere von kleineren Händlern wegen der damit verbundenen höheren Kosten größtenteils abgelehnt.

Um den Missbrauch von EC-Karten weitgehend zu minimieren, wird von den Händlern oft stichprobenartig die Identität des Kunden durch Einsichtnahme in den Personalausweis überprüft. In zunehmendem Maße werden aber auch Ausweisdaten der Kunden auf separaten Formularen oder dem Transaktionsbeleg erhoben. Dass dies nicht immer im Einklang mit den datenschutzrechtlichen Vorschriften erfolgt, zeigen die bei den Aufsichtsbehörden eingegangenen Beschwerden.

So wandte sich eine Kundin an die Aufsichtsbehörde, die sich durch ein Möbelhaus in ihren Rechten verletzt sah. Die Kundin wollte ihren Einkauf per EC-Karte bezahlen. Als die Kassiererin ihre Kartendaten einlas, ertönte plötzlich ein Signalton. Auf Nachfrage der Kundin erklärte die Kassiererin, dass sie deren Personalausweis für eine Kontrolle benötige. In der Annahme, es handele sich hier um einen bloßen Vergleich von Lichtbild, Name und Unterschrift, übergab die Kundin ihren Ausweis. Die Kassiererin notierte sich jedoch Name, Vorname, Anschrift, Geburtsdatum, Ort der Ausstellung sowie Ausweisnummer auf einem separaten Beleg und legte diesen neben der Kasse ab. Dies begründete die Kassiererin der Kundin gegenüber damit, dass es ja möglich sein könne, dass ihr Konto überzogen sei und das Mö-

belhaus in dem Fall irgendwie an sein Geld kommen müsse.

Die Aufsichtsbehörde prüfte den Fall und stellte fest, dass das Möbelhaus nicht nur zu viele Daten erhoben hatte, sondern auch das Verfahren den Kunden gegenüber nicht ausreichend transparent dargestellt hatte.

Die Erhebung personenbezogener Daten ist nur zulässig, wenn es der Zweckbestimmung eines Vertragsverhältnisses (hier also des Kaufvertrages) mit dem Betroffenen dient. Zur Feststellung der Identität des Käufers würde es zwar ausreichen, *Einsicht* in dessen Ausweis zu nehmen, doch muss auch anerkannt werden, dass einerseits durch die Datenerhebung die Hemmschwelle des Käufers für einen Kartenmissbrauch steigt und andererseits das Kassenpersonal in diesem Fall eine genaue Prüfung des Ausweises vornehmen *muss*, was bei einer bloßen Einsichtnahme unter dem meist bestehenden Zeitdruck (Warteschlangen etc.) nicht unbedingt gewährleistet ist. Zum Schutz vor Kartenmissbrauch und Forderungsausfall darf der Händler deshalb Ausweisdaten erheben. Dabei müssen jedoch die folgenden Bedingungen eingehalten werden:

- Es dürfen nur solche Ausweisdaten erhoben werden, die für das Vertragsverhältnis erforderlich sind. Als erforderlich werden anerkannt: Name, Vorname, Straße, Postleitzahl, Wohnort und Geburtsdatum des Ausweisinhabers. Nicht zulässig ist dagegen die Erhebung der Personalausweisnummer, des Ausstellungsdatums sowie der ausstellenden Behörde, da diese Angaben nicht für die Erfüllung der o. g. Zwecke erforderlich sind. Somit ist auch das Kopieren von Ausweisen nicht zulässig.

- Durch den Händler ist sicherzustellen, dass die zur Verarbeitung der Daten erforderlichen technischen und organisatorischen Maßnahmen eingehalten werden, insbesondere sind die Daten sicher aufzubewahren und gegen unbefugten Zugriff zu schützen. Die Daten dürfen nur genutzt werden, wenn es im konkreten Fall erforderlich ist und sie sind spätestens dann zu löschen, wenn ihre Kenntnis nicht mehr zur Erfüllung der o. g. Zwecke erforderlich ist (in der Regel nach drei Monaten).

- Außerdem ist vom Händler im Kassenbereich ein Schild mit dem Hinweis anzubringen, dass bei Bezahlung mit EC-Karte der Ausweis vorgelegt werden muss und stichprobenartig Personalausweisdaten (Name, Vorname, Anschrift, Geburtsdatum) auf dem Transaktionsbeleg notiert werden, dass diese Daten nicht elektronisch erfasst und auch nicht weitergegeben und im Übrigen nach drei Monaten bzw. nach endgültiger Lastschrifteinlösung vernichtet werden. Der Kunde kann dann entscheiden, ob er diese Zahlungsart wählen

möchte oder die Barzahlung vorzieht. Durch den Händler ist im Rahmen seiner Informationspflicht außerdem sicherzustellen, dass vom Kassenpersonal auf Nachfrage ausreichend über die Gründe und die weitere Verwendung der Daten Auskunft gegeben werden kann.

4.3.11 Bekanntgabe der Ergebnisse von Betriebskostenabrechnungen

Neben der eigenen Betriebskostenabrechnung erhielten alle Mieter in einer Wohnanlage von ihrem Vermieter auch eine Übersicht der Nachzahlungen/Gutschriften aller anderen Mieter. Dadurch wollte der Vermieter eine Disziplinierung der Mieter untereinander sowie eine höhere Zahlungsmoral der Mieter erreichen. Dies kam insbesondere durch die folgende Anmerkung in seinem Schreiben an die Mieter zum Ausdruck:

Diese Übersicht dient der allgemeinen Information. Gutschriften an Mieter können erst nach Eingang der Nachzahlungen der anderen Mieter ausgezahlt werden. Es wird deshalb zum einen um Geduld, zum anderen um Einflussnahme auf die Kostenschuldner gebeten.

Nach § 28 Abs. 1 Nr. 1 BDSG ist das Erheben, Speichern, Verändern, Übermitteln oder Nutzen personenbezogener Daten dann zulässig, wenn dies der Zweckbestimmung eines Vertragsverhältnisses (hier: Mietverhältnis) mit den Betroffenen dient. Die Unterrichtung eines Mieters über Guthaben oder Nachzahlungen anderer Mieter ist für dessen Mietverhältnis jedoch nicht erforderlich, so dass die Übermittlung dieser Liste unzulässig und damit rechtswidrig ist.

Der Vermieter hat der Aufsichtsbehörde gegenüber versichert, dass es sich bei der in Rede stehenden Datenweitergabe um einen einmaligen, auf diese Wohnanlage beschränkten Vorfall gehandelt habe, der sich nicht wiederholen wird. Er wollte die Mieter lediglich darauf aufmerksam machen, dass die Summe der Nachzahlungen höher als die der Gutschriften gewesen sei, er damit entsprechend in Vorkasse gehen musste und sich nicht etwa in irgendeiner Form bereichert habe.

Diese Begründung rechtfertigt sein Vorgehen nicht. Die Aufsichtsbehörde hat es jedoch bei einem deutlichen Hinweis auf die Rechtswidrigkeit dieser Verfahrensweise belassen.

4.3.12 Rücksendung von Bewerbungsunterlagen an falschen Bewerber

Ein Petent hatte sich bei einem Steuerberater um eine Arbeitsstelle beworben. Nachdem er mit der Absage nicht seine eigenen Bewerbungsunterlagen, sondern die eines anderen Bewerbers zurückbekommen hatte, wandte er sich an die Aufsichtsbehörde.

Es stellte sich heraus, dass der Steuerberater die Bewerbungsunterlagen des Betroffenen mit denen eines anderen Bewerbers bei der Rücksendung vertauscht hatte. So erhielt der Betroffene Kenntnis von personenbezogenen Daten (u. a. Lebenslauf, Lichtbild, Zeugnisse) eines anderen Bewerbers und umgekehrt. Letztendlich konnte jedoch geklärt werden, an wen welche Unterlagen geschickt worden waren, so dass jeder Bewerber wieder in den Besitz seiner Unterlagen gelangte.

Die Verarbeitung von Bewerberdaten ist im Rahmen der Zweckbestimmung des vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen zulässig (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Ist das Bewerbungsverhältnis beendet, d.h. hat der Arbeitgeber seine Einstellungsentscheidung getroffen, so sind die vertragsähnlichen Beziehungen grundsätzlich beendet. Der Arbeitgeber ist verpflichtet, die Daten der nicht berücksichtigten Bewerber zu löschen und die eingereichten Bewerbungsunterlagen entweder dem Bewerber zurückzugeben oder zu vernichten (siehe auch unten 4.3.13).

Werden die Bewerbungsunterlagen nicht an den jeweiligen Bewerber, sondern an einen anderen Bewerber gesandt, liegt eine Datenübermittlung vor. In diesem Fall erfolgten auf die Weise zwei unzulässige Datenübermittlungen.

Derartige Vorfälle sollten sich normalerweise nicht ereignen; gleichwohl können sie aber nicht mit absoluter Gewissheit ausgeschlossen werden. Da die Ursache für den Vorfall auf die Unachtsamkeit des Steuerberaters bzw. eines seiner Mitarbeiter zurückzuführen war und nicht das Resultat unzureichender innerbetrieblicher Organisation war, waren weitergehende aufsichtsbehördliche Maßnahmen nicht erforderlich.

4.3.13 Entsorgung von Bewerbungsunterlagen in Müllcontainer

Auf der Straße vor einem Restaurant waren in einem Müllcontainer Bewerbungsunterlagen gefunden und der Aufsichtsbehörde übergeben worden. Es handelte sich hierbei um insgesamt 36 Mappen mit Bewerbungsunterlagen. Die Bewerbungen für eine Tätigkeit als Köchin/Koch

waren alle an ein bestimmtes Restaurant gerichtet und stammten größtenteils von März/April 2003.

Der Inhaber des Restaurants gab an, im besagten Zeitraum insgesamt ca. 120 Bewerbungen erhalten zu haben. Einige seien in dem provisorischen Briefkasten oder vor der Tür abgelegt worden. Die Unterlagen der nicht berücksichtigten Bewerber seien teilweise persönlich abgeholt worden, die restlichen Unterlagen habe er im Ofen verbrannt. Wie die 36 Bewerbungsmappen in den Müllcontainer gelangt sind, könne er sich nicht erklären.

Die Aufsichtsbehörde hat dem Restaurantinhaber zunächst mitgeteilt, wie mit Bewerbungsunterlagen von nicht erfolgreichen Bewerbern umzugehen ist:

Entweder die Unterlagen werden an den Bewerber zurückgesandt oder sie werden datenschutzgerecht vernichtet oder es wird vereinbart, dass die Unterlagen bis zu einem bestimmten Zeitpunkt persönlich abgeholt werden können (unter Hinweis darauf, dass diese bei Nichtabholung datenschutzgerecht vernichtet werden).

Des Weiteren hat die Aufsichtsbehörde den Restaurantinhaber aufgefordert, die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Hierzu gehört insbesondere, für eine datenschutzgerechte Vernichtung von Unterlagen mit personenbezogenen Daten zu sorgen (z. B. Anschaffung eines Aktenvernichters oder Beauftragung eines Vernichtungsunternehmens) sowie einen ausreichend großen, abschließbaren Briefkasten zu installieren.

Der Restaurantinhaber hat die von der Aufsichtsbehörde geforderten Maßnahmen umgehend getroffen. Die Aufsichtsbehörde hat die ihr übergebenen Bewerbungsmappen an die Betroffenen zurückgesandt. Dem Restaurantinhaber konnte die vorsätzliche Entsorgung der Bewerbungsunterlagen im Müllcontainer nicht zweifelsfrei nachgewiesen werden, so dass von der Verhängung eines Bußgeldes abgesehen wurde.

4.3.14 Auskunftsersuchen einer Betriebskrankenkasse an eine Klinik

Der externe Datenschutzbeauftragte einer Klinik informierte die Aufsichtsbehörde darüber, dass die Klinik zunehmend Auskunftsersuchen von einer Betriebskrankenkasse erhält, die nicht mit den Vorgaben des § 301 SGB V vereinbar sind.

§ 301 Abs. 1 SGB V regelt, dass die Krankenhäuser verpflichtet sind, den Krankenkassen bei Krankenhausbehandlung die in der Vorschrift genannten Daten zu übermitteln. Die Betriebskrankenkasse verlangte jedoch auch darüber hinausreichende Daten.

Die Aufsichtsbehörde hat die Betriebskrankenkasse darauf hingewiesen, dass die Krankenkassen grundsätzlich nicht berechtigt sind, zur Überprüfung ihrer Leistungspflicht im Einzelfall von den Krankenhäusern Einsichtnahme in die Behandlungsunterlagen bzw. die Übermittlung der betreffenden Versichertendaten zu verlangen. Vielmehr ist in den §§ 275, 276 SGB V geregelt, dass sich die Krankenkassen in derartigen Fällen an den Medizinischen Dienst der Krankenversicherung zu wenden haben. Ein eigenständiges Datenerhebungsrecht sehen die den Umgang mit Sozialdaten abschließend regelnden Bestimmungen des SGB nicht vor (vgl. Bundessozialgericht, Urteil vom 23.07.2002, DuD 4/2003, 244 ff).

Die Betriebskrankenkasse wurde aufgefordert, die gesetzlichen Bestimmungen einzuhalten.

4.3.15 Auskunftserteilung durch eine Sparkasse

Ein Betroffener wandte sich an die Aufsichtsbehörde und bat zu prüfen, ob die seitens einer Sparkasse an Dritte erteilte Auskunft zulässig war.

Im Zusammenhang mit Erbschaftsauseinandersetzungen hatten zwei Erben als Pflichtteilberechtigte von der betreffenden Sparkasse Auskünfte über sämtliche Konten und Kontenbewegungen des Erblassers verlangt und auch erhalten. In der Sparkasse war man davon ausgegangen, dass eine Berechtigung zur Auskunftserteilung bestand. Die geforderten Auskünfte waren daher ohne rechtliche Prüfung des Auskunftsbegehrens erteilt worden.

Die Aufsichtsbehörde hat den Vorgang geprüft und kam zu dem Ergebnis, dass die Sparkasse die Auskünfte hätte nicht erteilen dürfen, da es für diese Datenübermittlung keine Rechtsgrundlage gab.

Der Datenübermittlung stand zunächst das bankvertraglich geschützte Bankgeheimnis entgegen.

Aber auch nach den datenschutzrechtlichen Bestimmungen war die Datenübermittlung unzulässig. Die Erlaubnisnormen des § 28 BDSG waren vorliegend nicht einschlägig. Insbesondere war die Datenübermittlung nicht zur Wahrung berechtigter Interessen der Sparkasse erfor-

derlich (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG). Im Falle der Annahme berechtigter Interessen der Dritten (§ 28 Abs. 3 Satz 1 Nr. 1 BDSG) war festzustellen, dass einer Datenübermittlung das schutzwürdige Interesse des Erblassers am Unterbleiben dieser Übermittlung entgegen stand.

Die Aufsichtsbehörde hat die unzulässige Auskunftserteilung beanstandet. Sie geht jedoch davon aus, dass es sich hierbei um einen Einzelfall gehandelt hat. Die Sparkasse hat den Fehler eingeräumt und zugesichert, künftig in allen Geschäftsstellen zu gewährleisten, dass Auskünfte erst nach einer rechtlichen Prüfung des Auskunftsbegehrens erteilt werden.

4.3.16 Weitergabe von Kundendaten durch ein Energieversorgungsunternehmen

Im Rahmen eines gerichtlichen Verfahrens erhielt ein Betroffener Kenntnis davon, dass die gegnerische Partei Auskünfte über ihn von einem Energieversorgungsunternehmen, bei dem er als Stromkunde gemeldet ist, verlangt und auch erhalten hatte. Die anfragende Stelle hatte gegenüber dem Energieversorgungsunternehmen angegeben, die Daten zur Durchsetzung privatrechtlicher Ansprüche zu benötigen. Der Betroffene vermutete hierin einen Datenschutzverstoß und wandte sich an die Aufsichtsbehörde.

Die Aufsichtsbehörde hat den Vorgang geprüft und kam zu dem Ergebnis, dass die Auskunftserteilung durch das Energieversorgungsunternehmen unzulässig und damit rechtswidrig war.

Einschlägige Vorschrift ist hier § 28 Abs. 3 Satz 1 Nr. 1 BDSG (Datenübermittlung im Drittinteresse). Danach ist die Datenübermittlung für einen anderen Zweck (als den eigenen) zulässig, soweit es zur Wahrung berechtigter Interessen eines Dritten erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Zwar konnte von einem berechtigten Interesse seitens der anfragenden Stelle an der Auskunft ausgegangen werden, jedoch bestand in diesem Fall Grund zu der Annahme, dass der Auskunftserteilung das schutzwürdige Interesse des Betroffenen entgegensteht.

Zunächst folgt aus dem Direkterhebungsgrundsatz des § 4 Abs. 2 BDSG, dass die betreffenden Daten grundsätzlich beim Betroffenen zu erheben sind. Wird stattdessen – wie in diesem Fall – seitens der anfragenden Stelle ohne nähere Angabe von Gründen eine dem Direkterhebungsgrundsatz widersprechende Datenerhebung bei Dritten (hier: dem Energieversorgungs-

unternehmen) bevorzugt, so muss dies in der Regel bei der angefragten Stelle (hier: dem Energieversorgungsunternehmen) dazu führen, entgegenstehende schutzwürdige Interessen des Betroffenen anzunehmen und eine Auskunftserteilung abzulehnen.

Eine sorgfältige Interessenabwägung durch das Energieversorgungsunternehmen hätte folgerichtig dazu führen müssen, die Auskünfte nicht zu erteilen.

Die Aufsichtsbehörde hat die Vorgehensweise des Energieversorgungsunternehmens beanstandet und das Unternehmen aufgefordert, seine Mitarbeiter regelmäßig zum Datenschutz zu belehren und insbesondere mit den Voraussetzungen der Auskunftserteilung/Weitergabe von Daten an Dritte vertraut zu machen bzw. entsprechend zu sensibilisieren.

Seitens des Energieversorgungsunternehmens wurde aus diesem Anlass umgehend eine entsprechende Datenschutzunterweisung durchgeführt.

4.3.17 Aushang eines Hausverbots

Einem Betroffenen war Hausverbot für ein Wohnhaus und eine Gaststätte erteilt worden. Der Hauseigentümer hatte das entsprechende Schreiben (enthielt Name, Vorname und Anschrift des Betroffenen) an mehreren Stellen im Haus und in der Gaststätte ausgehängt. Der Betroffene sah hierin einen datenschutzrechtlichen Verstoß und informierte die Aufsichtsbehörde.

Bei einem derartigen Aushang handelt es sich datenschutzrechtlich um eine Übermittlung personenbezogener Daten an eine unbestimmte Anzahl von Dritten.

Der Grundstückseigentümer ist aufgrund seines Hausrechts grundsätzlich befugt, Hausverbote gegen Personen auszusprechen, die bestimmte festgelegte Verhaltensregeln nicht einhalten. Hierbei hat er jedoch das allgemeine Persönlichkeitsrecht des Betroffenen zu beachten.

Dies ist in dem vorliegenden Fall nicht erfolgt. Für die Datenübermittlung durch die Bekanntgabe des Hausverbots an alle das Wohnhaus bzw. die Gaststätte betretenden Personen gab es keine Rechtsgrundlage. Dem Aushang kam indes eine prangerähnliche Wirkung zu. Der Aushang war daher aus datenschutzrechtlicher Sicht unzulässig.

Dem Grundsatz der Verhältnismäßigkeit hätte es entsprochen, wenn das Hausverbot lediglich vollzogen worden wäre. Hierzu hätte die Bekanntgabe an den Betroffenen durch ein entspre-

chendes Schreiben und eine ausschließlich interne Information an die Mitarbeiter der Gaststätte genügt.

4.3.18 Videoüberwachung einer Wohnanlage

Durch Zufall stieß ein Mieter einer Wohnanlage auf ein Bild des benachbarten Hauseinganges auf einem Fernsehkanal der Hausfernsehanlage. Er entdeckte dann noch auf weiteren Kanälen Bilder, die verschiedene Hauseingänge und den Spielplatz der Wohnanlage zeigten. Diese Bilder konnten von allen Bewohnern der Wohneinheit über den Kabelanschluss empfangen werden. Darüber hinaus wurden auch Tonaufnahmen gesendet. Es bestand für jeden Mieter die Möglichkeit, diese Bilder über ein Videogerät aufzuzeichnen.

Der Mieter fühlte sich in seiner Freiheit beeinträchtigt, sich unbeobachtet bewegen zu können und äußerte der Aufsichtsbehörde gegenüber Bedenken über die Zulässigkeit dieser Überwachungsmaßnahmen. Er verwies darauf, dass es die in den Treppenhäusern installierten Kameras ermöglichten, den Gehweg und die öffentliche Straße einzusehen. Außerdem seien weder im Innen- noch im Außenbereich Schilder angebracht, die auf die Videoüberwachung hinweisen. In einem Gespräch mit dem Petenten stellte sich heraus, dass die sich unter der Wohnanlage befindliche Tiefgarage ebenfalls noch mit Videokameras versehen werden sollte. Außerdem sei in einer Privatwohnung eine Art „Schaltzentrale“ installiert. Die Videoüberwachungsanlage sei nach Beschluss der Wohnungseigentümerversammlung durch die Hausverwaltung eingerichtet worden.

In einem späteren Schreiben informierte der Mieter die Aufsichtsbehörde darüber, dass ein weiterer Durchgang nun ebenfalls überwacht werde und die Kamera die volle Einsicht zu dem Balkon im Erdgeschoss ermögliche.

Nach Kontaktaufnahme mit der zuständigen Wohnungsverwaltungsgesellschaft wurde die Anlage daraufhin in Augenschein genommen. Durch die in der Wohnanlage installieren Kameradome konnten Briefkästen, Gehweg, Parkbucht, Straße, sowie Durchgänge und der gesamte Innenhof eingesehen werden. Darüber hinaus waren Mikrofone für Tonaufnahmen installiert. In der Tiefgarage sollten die Eingänge nur von innen erfasst werden. Ein Schaltraum befand sich in einem verschlossenen Kellerraum der Wohnanlage. Die Bilder konnten an einem Monitor betrachtet werden.

Den Verantwortlichen wurde erläutert, dass gemäß § 6b BDSG die Überwachung öffentlich zugänglicher Räume durch eine Videoanlage nur zulässig ist, wenn dies zur Erfüllung öffentlicher Aufgaben, der Wahrnehmung des Hausrechtes oder der Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine schutzwürdigen Interessen der Betroffenen überwiegen.

Daraufhin erklärten die Betreiber der Anlage, dass diese Maßnahmen zum Schutz der Fassade gegen Graffiti und zum Schutz vor Diebstählen und Sachbeschädigungen nötig seien. In der Vergangenheit seien diese Delikte schon häufiger aufgetreten. Den Verantwortlichen wurden die datenschutzrechtlichen Bedenken gegen den Betrieb Anlage erläutert. Insbesondere die Aufzeichnung von Tonaufnahmen, die Einspeisung in das Fernsehnetz und die Aufnahme von Bereichen außerhalb des Grundstücks sind nicht zulässig. Es handelt sich um einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung, insbesondere durch die für alle Bewohner bestehende Möglichkeit, jederzeit Aufzeichnungen anzufertigen. In die Privatsphäre der Anwohner und Passanten würde damit unverhältnismäßig eingegriffen. Es besteht keine rechtliche Grundlage für diese Form der Überwachung.

Von den Verantwortlichen wurde zugesagt, die Anlage bis zur Klärung des zulässigen Rahmens der Videoüberwachung abzuschalten.

Zu einem späteren Termin teilten die Verantwortlichen der Aufsichtsbehörde mit, dass die beanstandeten Mängel ausgeräumt wurden. Die Zulässigkeit der Überwachung der Tiefgarage wurde auf Grund der dort schon vorgekommenen Straftaten (Diebstahl, Sachbeschädigung) von der Behörde bestätigt. Die Zulässigkeit ergibt sich aus den §§ 27 ff. BDSG, da es sich hier um einen nicht öffentlich zugänglichen Raum handelt und die Überwachung der Tiefgarage der Sicherheit dient.

Die Erforderlichkeit der Videoüberwachung in der Wohnanlage nach § 6b Abs. 1 BDSG war für die Behörde weiterhin bedenklich. Die Verantwortlichen der Hausverwaltung haben ihre Gründe für die Erforderlichkeit der Videoüberwachung gegenüber der Aufsichtsbehörde inzwischen dargelegt. Die Angelegenheit befindet sich weiterhin in Bearbeitung.

5 Beratungsdienst/Anfragen an die Behörde

Auch in diesem Berichtszeitraum wurden wieder viele Anfragen zum Datenschutz an die Aufsichtsbehörden gerichtet. Betriebliche Datenschutzbeauftragte, Geschäftsführer von Unternehmen, Betriebsräte, Vereine und andere Daten verarbeitende Stellen baten überwiegend in Fragen der Zulässigkeit der Verarbeitung von personenbezogenen Daten um Rat. Die Aufsichtsbehörden leisteten mit ihrer umfangreichen Beratungstätigkeit einen wichtigen Beitrag zur Erhöhung des Datenschutzniveaus bei den Unternehmen sowie zur Vermeidung von Datenschutzverstößen. Die Möglichkeiten der Unternehmen zur Selbstkontrolle konnten gestärkt werden.

Betroffene wandten sich in vielen Fällen an die Aufsichtsbehörden, wenn sie meinten, bei der Verarbeitung ihrer Daten durch eine nicht-öffentliche Stelle in ihren Rechten verletzt worden zu sein. Sie konnten meist nach Beratung durch die Aufsichtsbehörden ihre Datenschutzrechte gegenüber nicht-öffentlichen Stellen erfolgreicher wahrnehmen.

Die Anfragen wurden je nach Sachlage in mündlicher oder in schriftlicher Form beantwortet. Sie betrafen insbesondere folgende Themen:

- Arbeitnehmerdatenschutz,
- Videoüberwachung,
- Bestellung/Tätigkeit des betrieblichen Datenschutzbeauftragten,
- datenschutzrechtliche Aspekte der Tätigkeit von Apotheken,
- Internet/neue Medien,
- Verarbeitung von Kundendaten, Zulässigkeit von Übermittlungen,
- Informationsmaterial, aktuelle gesetzlichen Regelungen,
- Meldepflicht, Verfahrensverzeichnis,
- Datenverarbeitung für Werbezwecke,
- Datenschutz im Mietverhältnis,
- medizinischer Datenschutz,
- Unterrichtungen nach § 7 Abs. 3 SächsDSG,
- Aspekte der Auftragsdatenverarbeitung,
- Tätigkeit von Wirtschaftsauskunfteien/Benachrichtigungen gem. § 33 BDSG,
- Datenverarbeitung durch die SCHUFA,
- Datenerhebung durch Versicherungen,
- Erhebung von Personalausweisdaten bei bargeldloser Bezahlung (vgl. 4.3.10),

- Datenschutz in Vereinen,
- Aufbewahrungs-/Löschfristen, Datenträgervernichtung,
- Datenschutzklauseln in Verträgen/Formularen,
- Aushändigung von Unterlagen/Akteneinsicht,
- Warndateien.

Zahlreich waren erstmals vor allem Anfragen zum Arbeitnehmerdatenschutz. Neben der Videoüberwachung stehen in diesem Bereich vor allem Fragen der Internet-, E-Mail- und Telefonnutzung am Arbeitsplatz immer wieder im Blickpunkt des Interesses. Künftig wird sicherlich auch das Thema „Spyware“ (vgl. Pkt. 4.3.4) verstärkt Anlass zu Anfragen oder Beschwerden geben.

Nachdem immer mehr auch im privaten Bereich Videokameras für Überwachungszwecke zum Einsatz kommen, hat auch der Umfang der Anfragen zum Thema Videoüberwachung stetig zugenommen. Insbesondere Privatpersonen wollen ihr Eigentum durch den Einsatz von Videokameras schützen und geraten dabei leicht an die Grenze der gesetzlichen Zulässigkeit. Denn sobald von der Kamera auch angrenzende öffentlich zugängliche Bereiche erfasst werden, gelten die Bestimmungen des BDSG.

Auch die Zulässigkeit des Einsatzes von Kamera-Attrappen, die zu Abschreckungszwecken angebracht werden, wird nach denselben Kriterien bewertet. Für den Betroffenen ist es nicht erkennbar, ob es sich um eine aktive Kamera oder eine Attrappe handelt. Auch Attrappen beeinträchtigen das Persönlichkeitsrecht des sich im vermeintlichen Erfassungsbereich befindenden Betroffenen, indem sie bei ihm zum Beispiel Überwachungsdruck erzeugen.

Ebenso recht häufig wurde die Aufsichtsbehörde zum Thema „Betrieblicher Datenschutzbeauftragter“ befragt. Neben der Klärung des Vorliegens der Bestellungspflicht ging es dabei wie bereits im vorhergehenden Berichtszeitraum um Fragen der Auswahl einer geeigneten Person (Interessenkollisionen), um den Erwerb der Fachkunde sowie um die Arbeitsbedingungen eines betrieblichen Datenschutzbeauftragten.

Die vergleichsweise große Zahl der Anfragen von Apotheken ist auf den Artikel „Datenschutz in der Apotheke“ im Informationsblatt 4/2003 der Sächsischen Landesapothekerkammer zurückzuführen. Der von der Landesapothekenkammer erarbeitete Beitrag war im Vorfeld mit dem Regierungspräsidium Dresden abgestimmt worden und beinhaltete insbesondere die Schwerpunkte „betrieblicher Datenschutzbeauftragter“ und „öffentliches Verfahrensverzeich-

nis“. Die daraufhin an die Aufsichtsbehörde gerichteten Anfragen betrafen jedoch nicht nur diese beiden Handlungsfelder, sondern wiesen ein breites Spektrum auf. Dieses Beispiel zeigt, dass oft schon mit relativ geringem Aufwand eine spürbare Verbesserung des Datenschutzes in einer ganzen Branche erzielt werden kann. Insbesondere die auf Landesebene wirkenden Verbände und Kammern sind geeignete Multiplikatoren, um das Anliegen des Datenschutzes in ihrem Wirkungsbereich zu verbreiten.

6 Datenschutzaufsicht über die Spielbanken im Freistaat Sachsen

Dem Regierungspräsidium Leipzig obliegt gemäß § 6 Abs. 4 Satz 2 des Gesetzes über die Spielbanken im Freistaat Sachsen (SpielbG) die datenschutzrechtliche Aufsicht über die sächsischen Spielbanken. Im Berichtszeitraum wurden Vor-Ort-Kontrollen in zwei Spielbanken durchgeführt. In beiden Fällen wurden insbesondere die in den Spielbankordnungen vorgeschriebenen Videoüberwachungsanlagen einer Prüfung unterzogen.

Nach den Spielbankenordnungen müssen alle Spiel-, Abrechungs- und Kassenvorgänge aufgezeichnet werden. Kontrolliert wurden die Aufnahmebereiche der Kameras, die Zugangssicherung der Aufzeichnungen sowie deren regelmäßige zeitnahe Löschung.

Anlass zur datenschutzrechtlichen Beanstandung bot bei einem Standort die unzureichende Kenntlichmachung der Beobachtung gemäß § 6b Abs. 2 BDSG. Nachdem die Aufsichtsbehörde darauf hingewiesen hatte, wurden mehrere Hinweisschilder angebracht. Der Mangel war damit behoben.

7 Genehmigung von Datenübermittlungen in Drittstaaten

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

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

Im Berichtszeitraum sind bei den Aufsichtsbehörden keine Genehmigungsanträge gestellt worden.

8 Öffentlichkeitsarbeit

Ein wesentlicher Bestandteil der Öffentlichkeitsarbeit der Aufsichtsbehörde im Berichtszeitraum war die Zusammenarbeit mit der Gesellschaft für Datenschutz und Datensicherung e. V. (GDD), insbesondere mit dem ERFA-Kreis Sachsen der GDD.

Die vierteljährlich stattfindenden Tagungen des ERFA-Kreises bieten Möglichkeiten eines effektiven und vor allem auch persönlichen Erfahrungs- und Meinungsaustausches. Darüber hinaus eröffnen sie der Aufsichtsbehörde die Möglichkeit, ihren Ansprechpartnern in den Unternehmen wesentliche Aspekte der Aufsichtstätigkeit und Fachwissen zu vermitteln.

Auf Bitten des Landesinnungsverbandes Orthopädie-Schuhtechnik Sachsen wurde der Landesinnungstag am 30.10.2004 in Waldheim durch einen Fachvortrag zum Thema „Datenschutzbeauftragte in Betrieben“ mitgestaltet.

Zur Verwirklichung des Servicegedankens werden zudem eine Reihe von Informationsbroschüren, Formularen sowie Musterdokumenten und -verträgen zum Datenschutz vorgehalten.

9 Ordnungswidrigkeiten

Im Berichtszeitraum wurden von den Aufsichtsbehörden 17 Ordnungswidrigkeitsverfahren durchgeführt. Davon betrafen drei Verfahren Verstöße gegen die Auskunftspflichten gem. § 38 Abs. 1 Satz 6 BDSG, acht Verfahren betrafen Verstöße gegen die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten. Vier Verfahren wurden wegen unbefugter Erhebung bzw. Verarbeitung personenbezogener Daten, die nicht allgemein zugänglich sind,

durchgeführt (§ 43 Abs. 2 BDSG). Die zwei verbleibenden Verfahren betrafen die heimliche Installation von Spyware auf einem Mitarbeiter-PC (vgl. o. Ziffer 4.3.4.).

Von den 17 durchgeführten Ordnungswidrigkeitsverfahren wurden insgesamt 3 Verfahren eingestellt, weil den Betroffenen die Verstöße nicht nachgewiesen werden konnten. Ein Verfahren ist noch nicht abgeschlossen. In sechs Fällen wurde wegen Verstoßes gegen die Auskunftspflichten gem. § 38 Abs. 1 Satz 6 BDSG bzw. wegen Verstoßes gegen die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten ein Verwarnungsgeld in Höhe von jeweils 35 € verhängt.

In sieben Fällen wurde ein Bußgeld verhängt, wobei die einzelnen Bußgelder zwischen 75 € und 300 € betrugen. Die Bußgelder betrafen folgende Fälle:

- Ein Bußgeld in Höhe von 75 € musste eine Geschäftsführerin eines Kleinunternehmens zahlen, weil sie entgegen § 4f Abs. 1 Satz 2 BDSG der Verpflichtung zur Bestellung eines Datenschutzbeauftragten auch nach weit über einem Monat noch nicht nachgekommen war.

- In einem mittelständischen Beratungsunternehmen, welches zum Teil als Weiterbildungsträger fungierte, ergab eine Kontrolle der Aufsichtsbehörde, dass nach dem Ausscheiden des bisherigen Datenschutzbeauftragten drei Jahre lang kein neuer Datenschutzbeauftragter bestellt worden war. Der Geschäftsführer reagierte zwar umgehend auf den Hinweis der Aufsichtsbehörde, einen Datenschutzbeauftragten zu bestellen; dennoch wurde angesichts des langen Zeitraums bis zur Bestellung eines neuen Datenschutzbeauftragten ein Bußgeld in Höhe von 200 € verhängt.

- Der Vorstand einer Wohnungsgenossenschaft hatte sich selbst als Datenschutzbeauftragten bestellt und dies damit begründet, dass kein anderer Angestellter im Haus die erforderliche technische Fachkunde besäße. Dem steht § 4f Abs. 3 Satz 1 BDSG entgegen, wonach der Datenschutzbeauftragte *dem Vorstand* unmittelbar *zu unterstellen* ist. Dem genannten Vorstand hätte die Unvereinbarkeit beider Funktionen durch die Teilnahme an mehreren Datenschutzseminaren bekannt sein müssen. Gegen ihn wurde ein Bußgeld in Höhe von 300 € verhängt. Ein weiterer Bußgeldbescheid über 200 € erging an den anderen Vorstand dieser Genossenschaft, dem lediglich Fahrlässigkeit vorzuwerfen war.

- Ein Bußgeld in Höhe von jeweils 250 € verhängte die Aufsichtsbehörde gegen die Ge-

schäftsführer eines Ingenieurbüros, die die Installation von Spyware auf einem Mitarbeiter-PC veranlasst hatten (vgl. o. Ziffer 4.3.4). Da die Geschäftsführer die Bußgelder nicht akzeptierten, kam es zu einer Verhandlung vor dem Amtsgericht, das die Auffassung der Aufsichtsbehörde vom Grundsatz her bestätigte, das Bußgeld jedoch auf 100 € korrigierte. Die Entscheidung ist inzwischen rechtskräftig.

- Gegen zwei Mitarbeiter eines Kreditinstitutes wurde ein Bußgeld in Höhe von jeweils 75 € verhängt, weil sie eine Liste mit Namen von Bürgschaftsinhabern und den Bürgschaftsbeträgen an den Beirat einer WEG übermittelt hatten, um einen Streit zwischen der WEG und einem durch das Kreditinstitut finanzierten Bauunternehmen über die Beseitigung von Baumängeln durch eine Vergleichszahlung des Kreditinstitutes an die WEG zu beenden. Eine Einwilligung der betroffenen Bürgschaftsinhaber zur Datenübermittlung lag nicht vor. Die Datenübermittlung war deshalb unzulässig, weil das Interesse der Betroffenen an der Nichtübermittlung der Daten höher zu bewerten ist, als das Interesse des Kreditinstituts, einen Rechtsstreit zu beenden. Gegen die Mitarbeiter des Kreditinstitutes wurde deshalb eine Bußgeld in Höhe von jeweils 75 € verhängt.

10 Zusammenarbeit der Aufsichtsbehörden

Zusammenarbeit der sächsischen Aufsichtsbehörden

Zweimal jährlich finden gemeinsame Beratungen zwischen dem Sächsischen Staatsministerium des Innern als oberster Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich und den drei Regierungspräsidien statt, bei denen Erfahrungen aus der praktischen Tätigkeit ausgetauscht werden und über Neuerungen auf dem Gebiet des Datenschutzes auf Bundes- und Europaebene informiert wird.

Die Zusammenarbeit zwischen den Regierungspräsidien erfolgt darüber hinaus durch gegenseitige Unterrichtungen und fachspezifischen Erfahrungsaustausch.

Hervorzuheben sind die jährlich durchgeführten Workshops der Datenschutz-Aufsichtsbehörden für den nicht-öffentlichen Bereich, die 2003 bei der Regierung von Mittelfranken in Ansbach und 2004 beim Landesbeauftragten für den Datenschutz der Freien Hansestadt Bremen stattfanden.

Zusammenarbeit mit Aufsichtsbehörden anderer Länder

Die länderübergreifende Zusammenarbeit findet vor allem über den sog. Düsseldorfer Kreis statt. Dieses Gremium haben die Bundesländer mit dem Ziel der bundesweit möglichst einheitlichen Rechtsanwendung der datenschutzrechtlichen Vorschriften für den nicht-öffentlichen Bereich eingerichtet. Mitglieder des Düsseldorfer Kreises sind Vertreter der Aufsichtsbehörden der Länder sowie des Bundesbeauftragten für den Datenschutz.

Die Beschlüsse des Düsseldorfer Kreises haben empfehlenden Charakter. Vorbereitet werden die Beschlüsse von den fachspezifischen Arbeitsgruppen des Düsseldorfer Kreises (AG Auskunfteien, AG Telekommunikation, Tele- und Mediendienste, AG Kreditwirtschaft, AG Versicherungswirtschaft und AG Internationaler Datenverkehr).

Im Düsseldorfer Kreis wird Sachsen durch das Sächsische Staatsministerium des Innern vertreten, das auch in den ersten zwei der o. g. Arbeitsgruppen mitwirkt.

Im Berichtszeitraum wurden im Düsseldorfer Kreis insbesondere folgende Schwerpunktthemen erörtert:

- Informationsbeziehungen zwischen Auskunfteien und der Wohnungswirtschaft,
- Neufassung der Einwilligungsklausel in Verträgen der Versicherungswirtschaft,
- Bestellung von Beauftragten für den Datenschutz bei Rechtsanwaltskanzleien und bei Apotheken,
- Videoüberwachung im nicht-öffentlichen Bereich,
- Zulässigkeit der Telefonwerbung von Kreditinstituten auf der Grundlage mündlicher Einwilligungen.

11 Abkürzungsverzeichnis

AG	Arbeitsgruppe
BDSG	Bundesdatenschutzgesetz
BDSG 90	Bundesdatenschutzgesetz vom 20.12.1990 in der bis zum 22.05.2001 geltenden Fassung
BfD	Bundesbeauftragter für Datenschutz
BGH	Bundesgerichtshof
BVerwG	Bundesverwaltungsgericht
DSB	Datenschutzbeauftragte(r)
DuD	Datenschutz und Datensicherheit, Zeitschrift für Recht und Sicherheit in der Informationsverarbeitung und Kommunikation
ERFA-Kreis	Erfahrungsaustausch-Kreis
EU	Europäische Union
EWR	Europäischer Wirtschaftsraum
GDD	Gesellschaft für Datenschutz und Datensicherung e. V.
HGB	Handelsgesetzbuch
HeimG	Heimgesetz
IP	Internet Protocol
MDK	Medizinischer Dienst der Krankenversicherung
MDStV	Mediendienste-Staatsvertrag
PBV	Pflege-Buchführungsverordnung
PIN	Persönliche Identifikations-Nummer
RDV	Recht der Datenverarbeitung, Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht
RP	Regierungspräsidium
SächsGVBl.	Sächsisches Gesetz- und Verordnungsblatt
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung

SGB V	Sozialgesetzbuch Fünftes Buch (gesetzliche Krankenversicherung)
SGB XI	Sozialgesetzbuch Elftes Buch (soziale Pflegeversicherung)
StGB	Strafgesetzbuch
SpielbG	Gesetz über Spielbanken im Freistaat Sachsen
TB	Tätigkeitsbericht
TDDSG	Gesetz über den Datenschutz bei Telediensten (Teledienstedaten-schutzgesetz)
TDG	Gesetz über die Nutzung von Telediensten (Teledienstegesetz)
WEG	Wohnungseigentümergemeinschaft
WuM	Fachzeitschrift „Wohnungswirtschaft und Mietrecht“