Datenschutz im nicht - öffentlichen Bereich

Erster Tätigkeitsbericht des Regierungspräsidiums Halle als Aufsichtsbehörde des Landes Sachsen-Anhalt nach § 38 Bundesdatenschutzgesetz (Berichtszeitraum: 23.05.2001-31.05.2003)

Inhaltsverzeichnis **2**

1. Das Regierungspräsidium Halle als Datenschutzaufsichtsbehörde im nicht – öffentlichen Bereich

1.1 Aufgabeninhalte und Rechtsgrundlagen

Die Datenschutzaufsicht im Bereich der Privatunternehmen und der sonstigen **nicht-öffentlichen Stellen** im Land Sachsen-Anhalt ist Aufgabe des Regierungspräsidiums Halle.

Der Beschluss der Landesregierung über die Bestimmung der zuständigen Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich, der am 01. Oktober 2002 in Kraft trat, führte zu einer **Zuständigkeitskonzentration** beim Regierungspräsidium Halle. Seither übt das Regierungspräsidium Halle im nicht – öffentlichen Bereich für das Land Sachsen-Anhalt die Kontrolle aus über die Einhaltung des Bundesdatenschutzgesetzes (BDSG) und anderer Bestimmungen über den Datenschutz, wie z.B. des Gesetzes über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz – TDDSG) und des Staatsvertrages über Mediendienste (MDStV). Mit Ende diesen Jahres geht die Zuständigkeit auf das Landesverwaltungsamt über, das seinen Sitz in Halle haben wird. Im vorliegenden Bericht sind Tätigkeiten der drei Regierungspräsidien Halle, Magdeburg und Dessau, die bis zum Inkrafttreten des Beschlusses als Datenschutzaufsichtsbehörden des jeweiligen Regierungsbezirkes fungierten, dargestellt.

Die Datenschutzaufsicht ist angesichts der Vielzahl der steuernden Rechtsnormen mit schwierigen rechtlichen und nicht minder komplexen informationstechnischen Fragestellungen befasst, die sich nicht selten nur im Wege zeitaufwendiger Prüfungen und Vor-Ort-Besichtigungen in Abstimmung mit den datenverarbeitenden Stellen lösen lassen.

1.2 Abgrenzung zum öffentlichen Bereich

Nicht zu den Aufgaben des Regierungspräsidiums Halle zählt die Datenschutzaufsicht über die **öffentlichen Stellen des Landes**, d.h. die Behörden, Organe der Rechtspflege und anderen öffentlich-rechtlich organisierten Einrichtungen des Landes einschließlich der Gemeinden und Gemeindeverbände. Auf die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch diese Stellen findet das Gesetz zum Schutz personenbezogener Daten der Bürger

(DSG-LSA) Anwendung. Wer sich durch eine öffentliche Stelle des Landes in seinen Rechten verletzt fühlt, wendet sich an den **Landesbeauftragten für den Datenschutz**, der seine Aufgaben nach §§ 20 ff. DSG-LSA wahrnimmt.

Nicht selten erreichen die Aufsichtsbehörde Anfragen und Beschwerden, die den Schutz von **Sozialdaten** zum Gegenstand haben. Sozialdaten sind personenbezogene Daten über Empfänger sozialer Leistungen oder Versicherte der Sozialversicherung bzw. deren Familienangehörige, Arbeitgeber, Ärzte etc., die durch Leistungsträger im Sinne von § 35 des Ersten Buches des Sozialgesetzbuches (SGB I) zur Erfüllung ihrer Aufgaben erhoben, verarbeitet oder genutzt werden. Leistungsträger sind z.B. Behörden, die Sozialleistungen erbringen (z.B. Sozialamt, Arbeitsamt), oder die gesetzliche Krankenkassen. Von Leistungsträgern verarbeitete Daten unterliegen einem besonderen Schutz, dem Sozialdatenschutz. Wer der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung von Sozialdaten in seinen Rechten verletzt worden zu sein, wendet sich an den Bundesbeauftragten für den Datenschutz, wenn es sich um eine öffentliche Stelle des Bundes handelt. Dazu gehören auch gesetzliche Krankenkassen, die über den Bereich des Landes hinaus tätig werden. Ist der Leistungsträger eine öffentliche Stelle des Landes, z.B. die AOK Sachsen-Anhalt, kann man sich an den Landesbeauftragten für den Datenschutz wenden.

1.3 Zielstellung eines Datenschutzberichts

Die Aufsichtsbehörden über den Datenschutz im nicht-öffentlichen Bereich sind seit der Novellierung des Bundesdatenschutzgesetzes durch § 38 Abs. 1 Satz 6 BDSG verpflichtet, regelmäßig, spätestens alle zwei Jahre, über ihre Tätigkeiten zu berichten. Es handelt sich vorliegend um den Ersten Datenschutzbericht im nicht-öffentlichen Bereich für das Land Sachsen-Anhalt. Seine Zielstellung erschöpft sich nicht darin, Rechenschaft über die zurückliegenden zwei Jahre zu geben. Darüber hinaus soll er den interessierten und betroffenen Bürger informieren, wie er sein **Recht auf informationelle Selbstbestimmung**, das als Bestandteil des allgemeinen Persönlichkeitsrechts (Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG) durch das Grundgesetz) garantiert wird und das ihn gegen eine unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe von Daten aus seinem persönlichen Lebensbereich schützt, wirkungsvoll wahrnehmen kann. Der Bericht soll dazu dienen, Antworten auf die am häufigsten wiederkehrenden Bürgeranfragen zu geben. Mit diesem Ziel wurden bestimmte Themenschwerpunkte aus der Arbeit der Aufsichtsbehörde ausgewählt. Natürlich sind jederzeit neue Gefährdungssituationen vorstellbar, die von den Themengruppen nicht erfasst werden. Nicht zuletzt sollen datenverarbeitende Stellen im Vorfeld Hinweise für einen datenschutzkonfor-

men, den Anforderungen der Aufsichtsbehörde entsprechenden Umgang mit personenbezogenen Daten erhalten, bevor Prüfungen und Beanstandungen notwendig werden.

2. Novellierung des Bundesdatenschutzgesetzes

Die am 23. Mai 2001 in Kraft getretene BDSG-Novelle, mit der die EU-Datenschutzrichtlinie (RL 95/46/EG) des Europäischen Parlaments und des Rats vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Warenverkehr in deutsches Recht umgesetzt wurde, hat zu grundlegenden Veränderungen geführt. Die Arbeit der Aufsichtsbehörde betreffen vor allem die Neugestaltung der Meldepflicht zum Register und die **Ausweitung der Kontroll- und Sanktionsbefugnisse der Aufsichtsbehörde**:

- Nach § 4 d Abs. 1 unterliegen nun Verfahren automatisierter Verarbeitungen vor ihrer Inbetriebnahme grundsätzlich vor ihrer Inbetriebnahme der **Meldepflicht**. § 4 d Abs. 2 BDSG sieht allerdings weitreichende Ausnahmen hiervon vor. Ausnahmslos meldepflichtig sind nach § 4 d Abs. 4 BDSG automatisierte Verfahren, in denen von verantwortlichen Stellen personenbezogene Daten zum Zweck der Übermittlung nach § 29 BDSG (z.B. Auskunfteientätigkeit, Adresshandel) oder der anonymisierten Übermittlung nach § 30 BDSG (z.B. Markt- und Meinungsforschung) verarbeitet werden. Für Verarbeitungen, die anderen Zwecken dienen, entfällt die Meldepflicht dann, wenn die verantwortliche Stelle einen betrieblichen Datenschutzbeauftragten bestellt hat oder wenn die Voraussetzungen des § 4 d Abs. 3 BDSG erfüllt sind. Dies wird sich in der Praxis so auswirken, dass fast nur noch die o.g. Verarbeitungen nach § 4 d Abs. 4 BDSG im Datenschutzregister gemeldet sein werden.

- Die Aufsichtsbehörde darf nun nach § 38 Abs. 1 BDSG die Einhaltung datenschutzrechtlicher Vorschriften jederzeit, auch ohne konkreten Anhaltspunkt für einen Datenschutzverstoße kontrollieren. **Anlassfreie Prüfungen** waren vom Gesetzgeber bislang nur für bestimmte Bereiche vorgesehen, wie z.B. für Auskunfteien, Adresshandelsunternehmen, Markt- und Meinungsforschungsinstitute, Service-Rechenzentren und sonstige Auftragsdatenverarbeitungsunternehmen (§ 38 Abs. 2 BDSG a.F.) sowie für Tele- und Mediendiensteanbieter gemäß Teledienstedatenschutzgesetz und Mediendienstestaatsvertrag. Sonstige Stellen konnten einer Prüfung nur bei Vorhandensein konkreter Anhaltspunkte für einen Datenschutzverstoß unterzogen werden (§ 38 Abs. 1 BDSG a.F.). Hinsichtlich der Einleitung einer anlassfreien Prüfung besteht allerdings ein weiterer Ermessensspiel-

raum, als wenn konkrete Anhaltspunkte für Datenschutzverstöße vorliegen. Es ist daher auch zukünftig zu erwarten, dass die Aufsichtsbehörde schwerpunktmäßig Anlassprüfungen durchführen wird.

- Die **Bußgeldtatbestände** wurden erweitert. Im Gegenzug erfuhr der Bereich des mit Strafe bedrohten Verhaltens eine Einschränkung. Während bislang nur Verstöße gegen bestimmte Verfahrensvorschriften (z.B. Nichtbeachtung der Meldepflicht, Auskunftsverweigerung gegenüber der Aufsichtsbehörde) als Ordnungswidrigkeiten mittels eines Bußgeldes geahndet werden konnten, kann nun auch bei Verstößen gegen materielle Schutzvorschriften des BDSG und anderer Datenschutzbestimmungen, die unmittelbar den Umgang mit personenbezogenen Daten regeln, ein Bußgeld durch die Behörde verhängt werden (§ 43 Abs. 2 BDSG). Eine Straftat stellen die in § 43 Abs. 2 BDSG aufgezählten Tatbestände nur noch dann dar, wenn sie vorsätzlich, gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begangen werden.

- Die Aufsichtsbehörde hat ein eigenes **Strafantragsrecht**, das bis zur Gesetzesänderung nach § 77 Strafgesetzbuch (StGB) nur der Verletzte selbst besaß.

- Durch **§ 38 a BDSG** wurde der Aufsichtsbehörde die Aufgabe zugewiesen, Entwürfe von Verhaltensregeln, die Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten, erarbeitet haben, auf ihre Vereinbarkeit mit dem geltenden Datenschutzrecht zu überprüfen. Auf diese Weise werden auf bestimmte Unternehmensbranchen zugeschnittene Datenschutzkonzepte mit einer Art behördlichem „Gütesiegel“ versehen. Die neu hinzugetretene Aufgabe verfolgt das Ziel, die Aufstellung solcher Datenschutzkonzepte im Interesse einer branchenspezifischen Konkretisierung des Gesetzes zu fördern und entsprechende gesetzgeberische Bemühungen entbehrlich zu machen.

- **§ 4 c Abs. 2 BDSG** weist der Aufsichtsbehörde die Aufgabe zu, **Genehmigungen** zu erteilen für **Datenübermittlungen** an Stellen in einem Drittstaat oder an eine zwischen-oder überstaatliche Stelle, wenn diese kein angemessenes Datenschutzniveau aufweist und keine der in § 4 c Abs. 1 BDSG aufgezählten Ausnahmeerlaubnisse eingreift. Die praktische Bedeutsamkeit der neuen Aufgabe ist allerdings gering. Zum einen hat die Kommission der Europäischen Union Standardvertragsklauseln verabschiedet und die Mitgliedsstaaten verpflichtet anzuerkennen, dass Unternehmen, die diese Vertragsklauseln verwenden, einen „angemessenen Schutz“ der Daten bieten. Eine Genehmigung der Aufsichtsbehörde ist in diesem Fall entbehrlich. Zum anderen hat die Kommission bereits mehrere Feststel-

lungen über ein angemessenes Datenschutzniveau in Drittstaaten getroffen. Nähere Informationen zu Entscheidungen der Kommission hinsichtlich der Standardvertragsklauseln und zur Angemessenheit des Schutzes persönlicher Daten in Drittstaaten sind im Internet beim Bundesbeauftragten für den Datenschutz (www.bfd.bund.de/europa/rubrik1.htm) und beim Berliner Beauftragten für Datenschutz und Informationsfreiheit (europa.eu.int/comm/internal/market/privacy/index.de.htm) zu finden.

Über die beschriebenen Neuregelungen hinaus hat die Novellierung des BDSG zu weiteren wesentlichen Änderungen geführt. Als Beispiele sollen an dieser Stelle die Einführung des Begriffs der **„besonderen Arten personenbezogener Daten“** (z.B. Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) durch **§ 3 Abs. 9 BDSG**, das Einfügen einer Vorschrift zur **Videoüberwachung (§ 6 b BDSG)** sowie die Begründung einer **Unterrichtungspflicht des Betroffenen** im Falle einer Ansprache zum Zwecke der Werbung oder der Markt- oder Meinungsforschung **(§ 28 Abs. 4 Satz 2 BDSG)** genannt werden. Auf diese und weitere Änderungen wird bei der Erörterung der einzelnen Themenschwerpunkte unter Ziff. 4 dieses Berichts näher eingegangen.

3. Kontrolltätigkeit der Aufsichtsbehörde im Berichtszeitraum - ein Überblick mit statistischer Auswertung -

3.1 Registerführung

Das Regierungspräsidium Halle führt gemäß § 38 Abs. 2 BDSG das Register der nach § 4 d BDSG meldepflichtigen nicht-öffentlichen Stellen, die im automatisierten Verfahren personenbezogene Daten verarbeiten. Seit der Novellierung des Bundesdatenschutzgesetzes hat sich die Anzahl der meldepflichtigen Unternehmen erheblich reduziert.

Am 1. April 2003 waren im Regierungsbezirk Halle nur noch 7, im Regierungsbezirk Dessau 5 und im Regierungsbezirk Magdeburg nicht mehr als 3 datenverarbeitende Stellen zum Register der Datenschutzaufsichtbehörden gemeldet. In allen Fällen handelt es sich um Unternehmen, die im automatisierten Verfahren Daten gemäß § 29 BDSG geschäftsmäßig zum Zweck der Übermittlung (Auskunfteien, Adresshandel) oder gemäß § 30 BDSG zum Zweck der anonymisierten Übermittlung (Markt-, Meinungs- und Sozialforschungsinstitute) verarbeiten.

3.2 Anlassfreie Prüfungen; Schwerpunkte im Berichtszeitraum: Handels- und Wirtschaftsauskunfteien und Auftragsdatenverarbeitungsfirmen

Die BDSG-Novelle vom 23. Mai 2001 hat die Durchführung von routinemäßigen anlassfreien Datenschutzprüfungen erleichtert. Seit der Gesetzesänderung können alle nicht-öffentlichen Stellen, die personenbezogene Daten im automatisierten Verfahren bzw. in oder aus nicht automatisierten Dateien verarbeiten oder nutzen, geprüft werden, ohne dass die Beschwerde eines Betroffenen vorliegen oder sonstige Anhaltspunkte gegeben sein müssen, die auf eine Datenschutzverletzung hindeuten (§ 38 Abs. 1 Satz 1 BDSG).

Eine anlassfreie Überprüfung beginnt grundsätzlich mit der schriftlichen Ankündigung einer **Vor-Ort-Kontrolle** und dem Übersenden eines Fragebogens, auf dem allgemeine Angaben zum Tätigkeitsfeld und zur Organisationsstruktur des Unternehmens zu machen sind. Zu der Ortsbegehung wird – wenn erforderlich - ein technischer Mitarbeiter des Landesinformationszentrums Sachsen-Anhalt hinzugezogen. Die Vor-Ort-Kontrolle wird mit Hilfe eines detaillierten Fragenkatalogs absolviert und durch eine stichprobenweise Überprüfung der Datenverarbeitungsanlagen ergänzt. Die Aufsichtsbehörde überprüft zuerst die Einhaltung der allgemeinen rechtlichen Anforderungen an eine datenverarbeitende Stelle. So wird beispielsweise kontrolliert, ob alle mit der Datenverarbeitung in Berührung kommenden Personen auf das Datengeheimnis nach § 5 BDSG verpflichtet wurden, ob - soweit gesetzlich erforderlich - ein mit dem notwendigen Fachwissen ausgestatteter Datenschutzbeauftragter bestellt wurde und eine Meldung zum Register erfolgte. Es schließt sich eine detaillierte Abfrage der getroffenen technischen und organisatorischen Maßnahmen i. S. v. § 9 BDSG zum Schutz des ordnungsgemäßen Ablaufs der Datenverarbeitung durch Sicherung von Hard- und Software sowie von Daten vor Verlust, Beschädigung und Missbrauch an. Beispiele für technische und organisatorische Maßnahmen sind bauliche Vorkehrungen zum Schutz gegen den Zutritt oder Eingriff durch Unbefugte wie z.B. das Einrichten besonders gesicherter Räume und Behältnisse für Datenverarbeitungsanlagen, der Einbau von Überwachungstechnik, Zugriffsschranken in Form von Passwörtern, die gezielte Verteilung von Aufgaben und Befugnissen und die Zuweisung von Verantwortlichkeiten. Verlauf und Ergebnis der Prüfung werden in einem abschließenden **Protokoll** festgehalten. Stellt die Aufsichtsbehörde einen Verstoß gegen Datenschutzvorschriften fest, rügt sie diesen und fordert das Unternehmen auf, den Mangel innerhalb einer bestimmten Frist zu beseitigen. Selbst in Fällen, in denen die Prüfung ohne Bean-

standungen endet, hat die Aufsichtsbehörde die Möglichkeit, Empfehlungen zur Verbesserung des Datenschutzniveaus in dem Betrieb auszusprechen.

In Sachsen-Anhalt wurden im Berichtszeitraum insgesamt 4 nicht-öffentliche Stellen einer umfassenden anlassfreien Überprüfung unterzogen. Bei den betroffenen Betrieben handelte es sich in zwei Fällen um eine Handels- und Wirtschaftsauskunftei, in einem Fall um ein Auftragsdatenverarbeitungsunternehmen und in einem weiteren Fall um einen Verein.

Handels- und Wirtschaftsauskunfteien sammeln Informationen über die wirtschaftliche Betätigung, Kreditwürdigkeit und Zahlungsfähigkeit von Unternehmen und Privatpersonen. Erhoben und gespeichert werden z. B. Beruf, Arbeitgeber, ausgeübte Tätigkeit, Verdienst, Umsatz, Grundbesitz, Bankverbindung, Schulden, Zahlungsweise, Abgabe einer eidesstattlichen Versicherung, Zwangsversteigerungsverfahren, Mahn- oder Vollstreckungsbescheide. Die Daten stammen teilweise aus der Öffentlichkeit zugänglichen Quellen, z. B. Telefon- und Adressbüchern, dem Bundesanzeiger, öffentlichen Registern wie dem Handels- und Vereinsregister und Schuldnerverzeichnissen. Auch Geschäftspartner der Auskunftei übermitteln mitunter personenbezogene Daten aus ihren Geschäftsbeziehungen.

Ohne Einwilligung des Betroffenen ist die Erhebung, Speicherung und Weitergabe dieser Daten nach § 29 BDSG erlaubt. Voraussetzung für eine Übermittlung ist, dass der Dritte, an den übermittelt wird, ein berechtigtes Interesse glaubhaft darlegt und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. Der Interessent muss ein spezielles Interesse an bestimmten Daten für im einzelnen zu benennende Ziele oder Geschäftszwecke glaubhaft darlegen (Vertrag, Darlehensgewährung). Auskunfteien tragen den gesetzlichen Anforderungen von § 29 Abs. 2 Satz 1
Nr. 1 a BDSG zum Teil dadurch Rechnung, dass sie Mitgliedernummern und Kennwörter vergeben. Eine Auskunft erhält nur, wer Mitgliedernummer und Kennwort nennt und ein berechtigtes Interesse glaubhaft machen kann.

Handels- und Wirtschaftsauskunfteien unterliegen ohne Einschränkung nach § 4 d Abs. 4 BDSG der Meldepflicht. Die Betroffene hat nach § 34 BDSG einen **Rechtsanspruch auf Auskunft** über die zu seiner Person gespeicherten Daten, den Zweck der Speicherung und die Kategorien von Empfängern, an die die Daten im Allgemeinen weitergegeben werden. Auskunft über Herkunft und Empfänger der Daten kann nur verlangt werden, wenn nicht das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt. Nach § 33 Abs. 1 BDSG müssen Handels- und Wirtschaftsauskunfteien den Betroffenen über die erstmalige Übermittlung und

die Art der übermittelten Daten benachrichtigen, sofern die Speicherung der Daten ohne seine Kenntnis erfolgte.

Bei den im Berichtszeitraum geprüften Auskunfteien wurden **keine Datenschutzverstöße** festgestellt. Es wurden lediglich einzelne Empfehlungen zur Optimierung des Datenschutzes im Betrieb erteilt.

Prüft die Aufsichtsbehörde ein Unternehmen der **Auftragsdatenverarbeitung** i. S. v. § 11 BDSG, kontrolliert sie neben den allgemeinen Anforderungen und den technisch-organisatorischen Maßnahmen nach § 9 BDSG zusätzlich, ob die Datenverarbeitung sich im Rahmen der Weisungen des Auftraggebers hält. Durch Vorlage entsprechender Verträge muss das Unternehmen nachweisen, dass ein schriftliches Auftragsverhältnis existiert und vom Auftraggeber Weisungen betreffend den Leistungsumfang, Ort und Zeitpunkt der Datenverarbeitung erteilt wurden.

Die Geschäftstätigkeit des im Berichtszeitraum durch die Aufsichtsbehörde geprüften Auftragsdatenverarbeitungsunternehmens erstreckt sich auf die Durchführung von Lohn- und Gehaltsabrechnungen sowie die Finanzbuchhaltung für auftraggebende Firmen. Personenbezogene Daten werden im Zusammenhang mit den Lohn- und Gehaltsabrechnungen verarbeitet. Bei dem geprüften Unternehmen konnte im Ergebnis **kein Datenschutzverstoß** festgestellt werden. Da das Unternehmen nicht mehr als 4 Arbeitnehmer mit der Verarbeitung personenbezogener Daten beschäftigt, unterliegt es nicht der Pflicht, einen Datenschutzbeauftragten zu bestellen. Wegen des großen Umfangs der verarbeiteten personenbezogenen Daten wies die Aufsichtsbehörde darauf hin, dass die Bestellung eines Datenschutzbeauftragten ungeachtet der gesetzlichen Regelung von Vorteil ist.

3.3 Anlasskontrollen

Die auf die Beschwerde eines Betroffenen hin oder wegen sonstiger **konkreter Anhaltspunkte** für das Bestehen einer Datenschutzverletzung eingeleiteten Anlasskontrollen bildeten im Berichtszeitraum einen Schwerpunkt der Tätigkeiten der Aufsichtsbehörde. Ist der Verdacht eines Datenschutzverstoßes begründet, wird die datenverarbeitende Stelle regelmäßig schriftlich zu einer Stellungnahme aufgefordert. Ergänzend wird ggf. ein Kontrollbesuch in dem Unternehmen durchgeführt. Die Aufsichtsbehörde ist gemäß § 38 Abs. 4 Satz 1 BDSG berechtigt, während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. Hierbei kann sie

geschäftliche Unterlagen sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme einsehen. Festgestellte Datenschutzverstöße werden der Stelle mitgeteilt, verbunden mit der Aufforderung, den Mangel innerhalb einer bestimmten Frist zu beseitigen. Kommt die datenverarbeitende Stelle den Anforderungen nicht freiwillig nach, besteht die Möglichkeit, ein Bußgeldverfahren gemäß § 43 BDSG einzuleiten. § 38 Abs. 5 BDSG räumt der Aufsichtsbehörde unter bestimmten Voraussetzungen auch Anordnungs- und Untersagungsbefugnisse ein. Diese setzen das Vorliegen technischer bzw. organisatorischer Mängel im Sinne von § 9 BDSG bei der Anwendung der Datenverarbeitungsverfahren voraus, die eine Gefahr von Verlust, Beschädigung oder Missbrauch personenbezogener Daten begründen.

Im Land Sachsen-Anhalt wurden im Berichtszeitraum insgesamt 81 Prüfungen aufgrund von Beschwerden eingeleitet, wobei sich 35 Beschwerden auf dieselbe verantwortliche Stelle bezogen. Auf den Regierungsbezirk Halle entfielen 65 Beschwerden, im Regierungsbezirk Dessau wurden 9, im Regierungsbezirk Magdeburg 7 Beschwerden erhoben.

Die Beschwerden betrafen

→ unverlangte Fax-Werbung	38
→ unverlangte E-Mail-Werbung	8
→ sonstige Nutzung von Adressen zu Werbezwecken	4
→ Verarbeitung personenbezogener Daten aus Vertragsverhältnis	8
→ Umgang mit personenbezogenen Daten durch Vereine	5
→ Kopieren von Personalausweisen	4
→ Videoüberwachung	3
→ Datenschutzverletzungen im Arbeitsverhältnis durch den Arbeitgeber	2
→ Datenschutzverletzungen im Gesundheitswesen	3
→ Veröffentlichung personenbezogener Daten im Internet	4
→ Nichterteilung einer Auskunft i. S. v. § 34 BDSG	1
→ Verletzung des Berufsgeheimnisses durch einen Rechtsanwalt.	1

Die erhobenen Beschwerden erwiesen sich in insgesamt **59 Fällen als begründet**, wobei 35 Beschwerden gegen dasselbe Unternehmen gerichtet waren:
Die begründeten Beschwerden betrafen:

→ unzulässige Fax-Werbung	35
→ unzulässige E-Mail-Werbung	9

→ Veröffentlichung von Schuldnerdaten im Internet	3
→ Kopieren von Personalausweisdokumenten	3
→ Datenschutzverletzungen durch den Arbeitgeber	2
→ Nichterteilung einer Auskunft i. S. v. § 34 BDSG gegenüber dem Betroffenen	1
→ Datenschutzverletzungen im Gesundheitswesen	2
→ Datenschutzverstöße durch Vereine	2
→ Erhebung personenbezogener Daten in Vertragsverhältnissen	2

In insgesamt 10 Prüfungsverfahren wurden ergänzende **Ortsbesichtigungen** durchgeführt.

3.4 Beratung auf Anfrage

Das Regierungspräsidium Halle nimmt als Datenschutzaufsichtsbehörde Beratungsaufgaben wahr. Die Beratung von datenverarbeitenden Stellen und Betroffenen macht einen wesentlichen Bestandteil ihrer Tätigkeiten aus. Die gesetzliche Regelung weist die Beratungstätigkeit allerdings in erster Linie dem **betrieblichen Datenschutzbeauftragten** zu (§ 4 g Abs. 1 Satz 1, § 4 d Abs. 6 BDSG). Dieser kann sich aber in Zweifelsfällen an die Aufsichtsbehörde wenden (§ 4 g Abs. 1 Satz 2, § 4 d Abs. 6 BDSG). Häufig wiederkehrende Fragen des betrieblichen Datenschutzbeauftragten beziehen sich z. B. auf den Erwerb der erforderlichen Sachkunde sowie auf das Problem, welche konkreten Anforderungen an die Betriebsorganisation aus dem BDSG abzuleiten sind. Die Aufsichtsbehörde wird auch außerhalb dieser ausdrücklich gesetzlich zugewiesenen Hilfsaufgabe beratend tätig. Anfragende sind z. B. Geschäftsführer und Betriebsleiter von datenverarbeitenden Firmen, aber auch Betroffene, die sich in ihren Rechten verletzt fühlen, die Beschwerde gegen eine bestimmte Stelle jedoch scheuen und stattdessen die Klärung der Rechtsfrage vorziehen, um selbst über das weitere Vorgehen in dieser Angelegenheit entscheiden zu können. Wenden sich Angehörige von datenverarbeitenden Stellen an die Aufsichtsbehörde, so geschieht dies meistens in der Absicht, vor der Einführung eines neuen Datenverarbeitungssystems oder vor der Eröffnung eines neuen Geschäftsfeldes eine Rechtssicherheit zu erlangen, um späteren Kontrollen und Beanstandungen zuvorzukommen.

Im Berichtszeitraum gingen insgesamt 18 schriftliche Beratungsersuchen von Gewerbetreibenden und Privatpersonen bei der Aufsichtsbehörde ein. Die Anfragen hatten u.a. Datenschutzprobleme bei der Videoüberwachung öffentlich zugänglicher Räume, der Einrichtung von Schuldnerwarndateien im Internet, im Gesundheitswesen (z.B. externe Archivierung von

Patientendaten durch Arztpraxen und Krankenhäuser, datenschutzkonforme Vernichtung von Patientenakten), ferner im Arbeitsleben und im Verein zum Gegenstand.

3.5 Bußgeldverfahren

Ist einer der Bußgeldtatbestände des § 43 BDSG erfüllt, kann die Aufsichtsbehörde ein Bußgeld verhängen. Die Höhe richtet sich danach, ob ein Verstoß gegen **Verfahrensvorschriften** gemäß **§ 43 Abs. 1 BDSG**, z.B. wegen einer Verletzung der Meldepflicht, eines Verstoßes gegen die Verpflichtung zur Bestellung eines Datenschutzbeauftragten oder zur Unterrichtung des Betroffenen im Falle der Ansprache zu Werbe-, Markt- oder Meinungsforschungszwecken, oder ein solcher gegen **materielle Schutzvorschriften** des BDSG gemäß **§ 43 Abs. 2 BDSG** festgestellt wurde. Im ersten Fall kann ein Bußgeld bis zu 25.000,00 Euro, im zweiten Fall ein Bußgeld bis zu 250.000 Euro verhängt werden.

Von der rechtlichen Möglichkeit, Datenschutzverstöße mittels Bußgeldern zu sanktionieren, machte die Aufsichtsbehörde bislang in zurückhaltender Weise Gebrauch, weil sich die festgestellten Verletzungen meistens in Absprache mit der datenverarbeitenden Stelle beseitigen ließen. In einigen Fällen wurde aber die Einleitung eines Bußgeldverfahrens als notwendig erachtet, um eine Rechtsverletzung in einer für die Betroffenen spürbaren Weise zu sanktionieren und Wiederholungen abzuwenden. Bußgeldverfahren wurden im Berichtszeitraum eingeleitet bei wiederholten, hartnäckigen Verstößen gegen Bestimmungen des Datenschutzrechts, die eine große Anzahl von Eingaben auslösten und die zudem als wesentlicher Bestandteil der wirtschaftlichen Betätigung der datenverarbeitenden Stelle auf ein unlauteres Gewinnstreben schließen ließen. Ferner wurde die Einleitung eines Bußgeldverfahrens erforderlich, wenn die durch den Verstoß ausgelöste Persönlichkeitsverletzung beim betroffenen Bürger als schwerwiegend eingestuft wurde, so z. B. im Falle der öffentlichen Bloßstellung einer Person mittels unzulässiger Veröffentlichung ihrer persönlichen Daten im Internet.

Im Berichtszeitraum wurde durch die Aufsichtsbehörde in vier Fällen ein Bußgeld verhängt, drei der Bußgeldbescheide sind bestandkräftig, weil die datenverarbeitenden Stellen keinen Rechtsbehelf einlegten. Die Verfahren richteten sich gegen drei Firmen der Werbewirtschaft und gegen ein Dienstleistungsunternehmen. Die Summe der verhängten Bußgelder beträgt 3.200 Euro. Bußgeldmindernd wirkte sich in der Regel aus, wenn die verantwortliche Stelle unverzüglich nach Erteilung eines rechtlichen Hinweises durch die Aufsichtsbehörde freiwillig die Rechtsverletzung beseitigte. In zwei

Fällen verhängte die Aufsichtsbehörde bereits wegen der **verweigerten Auskunftserteilung** gegenüber der Aufsichtsbehörde gemäß **§ 38 Abs. 3 BDSG** jeweils ein Bußgeld in Höhe von 1.000 Euro. Es lagen hier aufgrund zahlreicher Beschwerden Anhaltspunkte vor, die den Verdacht mehrfacher erheblicher Verstöße von Werbefirmen gegen das Datenschutzrecht begründeten. Da alle Aufforderungen zur Stellungnahme trotz Hinweises der Aufsichtsbehörde auf die Rechtsverpflichtung unbeantwortet blieben, musste von einer vorsätzlichen Auskunftsverweigerung ausgegangen werden.

4. Ausgewählte Themen aus Beschwerden und Anfragen

4.1 Werbung und Marketing

4.1.1 Unerwünschte Werbung per Fax und E-Mail (Spamming)

Spamming ist die Bezeichnung für unverlangte Werbesendungen per E-Mail oder Fax, die in großen Mengen und wahllos verschickt werden. Diese Art von Werbung ist lästig und kostspielig für den Empfänger der Werbung. Im Falle der Werbe-Mails gilt dies auch für den Provider, dem Kosten entstehen, weil Massen-Mails Leitungen belegen, Kapazitäten binden und hierdurch Kosten verursachen. Nach den einschlägigen Urteilen zur Telefax- und mittlerweile auch zur E-Mail-Werbung kann der Zivilrechtsweg durch die Betroffenen beschritten werden. Die unerlaubte Werbung stellt einen **Wettbewerbsverstoß** im Sinne von § 1 des Gesetzes über den unlauteren Wettbewerb (UWG) dar, gegen den sich konkurrierende Betriebe wehren können. Aus Sicht des Empfängers stellt sich die Werbung im Hinblick auf die Verursachung von Aufwand und Kosten als **Eigentumsstörung** dar, die einen Unterlassungs- und Schadensersatzanspruch nach §§ 823 Abs. 1 und Abs. 2, 1004 Bürgerliches Gesetzbuch (BGB) auslösen kann.

Aber auch das BDSG unterwirft das unerwünschte Versenden von Werbemitteilungen nicht unerheblichen Schranken. So ist gemäß § 28 Abs. 1 das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke außerhalb von vertraglichen oder vertragsähnlichen Beziehungen nur zulässig, soweit es zur Wahrung **berechtigter Interessen der verantwortlichen Stelle** erforderlich ist und kein Grund zu der Annahme besteht, dass das **schutzwürdige Interesse des Betroffenen** an dem Ausschluss der Verarbei-

tung oder Nutzung **überwiegt** (§ 28 Abs. 1 Nr.. 2 BDSG). Selbst in Fällen, in denen die personenbezogenen Daten allgemein zugänglich sind, ist das Erheben, Verarbeiten oder Nutzen der Daten unzulässig, wenn das schutzwürdige Interesse des Betroffenen **offensichtlich überwiegt** (§ 28 Abs. 1 Nr. 3 BDSG). Bei einer Verarbeitung personenbezogener Daten, die nach der einschlägigen Rechtsprechung wettbewerbswidrig ist bzw. eine Eigentumsverletzung i. S. v. § 823 BGB darstellt, nimmt die Aufsichtsbehörde an, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung i. S. d. § 28 Abs. 1 Satz 1 Nr. 2 und Nr. 3 BDSG überwiegt bzw. offensichtlich überwiegt.

In einem durch die Aufsichtsbehörde geprüften Fall gingen insgesamt 35 Beschwerden wegen unverlangter, mehrere Monate andauernder Faxwerbung ein. Angeboten wurden zum Abruf unter 0190-er Nummern Verbraucherinformationen zu verschiedenen Themenbereichen. Die Faxe enthielten keine Absenderangabe. Genannt wurden lediglich zwei Telefonnummern, unter denen allerdings niemand zu erreichen war. Die Betroffenen gaben allerdings an, dass unter diesen Nummern niemand zu erreichen gewesen sei. Viele der Betroffenen erklärten der Aufsichtsbehörde gegenüber, ihre Faxnummern nicht veröffentlicht zu haben. Häufig wurde trotz eines Werbewiderspruchs gemäß § 28 Abs. 4 BDSG weiterhin Werbung an die betroffenen Personen versandt.

Die schriftliche Aufforderung der Aufsichtsbehörde zur Stellungnahme wurde nicht beantwortet. Auch die konkrete Androhung eines Bußgeldes blieb ohne Reaktion.. Mit dem Ziel der Aufklärung des Sachverhalts führte die Aufsichtsbehörde schließlich eine Besichtigung vor Ort durch. Hierbei stellte sich heraus, dass sich hinter der als Geschäftsadresse angegebenen Anschrift das private Wohnhaus des Inhabers verbirgt. Dieser erwies sich als nicht bereit, an der Aufklärung des Sachverhalts mitzuwirken, insbesondere Auskünfte zu erteilen zum Inhalt seiner Geschäftstätigkeit und zur Herkunft der Privatadressen.

Gegen den Firmeninhaber wurde ein Bußgeld verhängt wegen mehrfachen Verstoßes gegen Verfahrensvorschriften, d.h. wegen Nichterteilung der erforderlichen Auskünfte gegenüber der Aufsichtsbehörde (§ 43 Abs. 1 Nr.. 10, § 38 Abs. 3 Satz 1 BDSG), wegen unterbliebener Unterrichtung der Betroffenen über die verantwortliche Stelle anlässlich der Werbeansprache sowie über deren Widerspruchsrecht und über die Herkunft der Daten (§ 28 Abs. 4 Satz 2 BDSG). Neben den aufgezählten Verfahrensverstößen war überdies die materielle Verletzung des BDSG wegen vorsätzlicher unbe-

fugter Erhebung oder Verarbeitung personenbezogener Daten, die nicht allgemein zugänglich sind (§ 43 Abs. 2 Nr. 1), zu ahnden.

Gegen den Bußgeldbescheid legte die Firma keinen Widerspruch ein, sodass dieser mittlerweile bestandskräftig ist. Das zuständige Gewerbeaufsichtsamt wurde informiert.

Ein weiterer der Aufsichtsbehörde angezeigter Fall betraf das Versenden von Werbe-E-Mails. Auch hier gingen mehrere Beschwerden sowohl aus Deutschland als auch aus dem europäischen Ausland bei der Aufsichtsbehörde ein. Nach eigenen Angaben des Firmeninhabers wurde an über 84 Mio. Leser in der ganzen Welt, in Deutschland allein an 5 Mio. Leser Werbung gemailt. Geworben wurde für Webshops, z. B. Berufsbekleider, Uhrenhändler etc.

Die Beschwerden richteten sich nicht nur gegen das unaufgeforderte Zusenden der Werbemails, sondern ebenso dagegen, dass die einschlägigen Verfahrensvorschriften ignoriert wurden. Die Aufforderung zur Offenlegung, welche Daten außer Name und E-Mail-Adresse über die betreffende Person gespeichert wurden und aus welcher Quelle diese Daten stammen, sowie die Aufforderung zur Löschung der gespeicherten Daten blieben unbeantwortet.

Auch hier verhängte die Aufsichtsbehörde ein Bußgeld wegen Nichterteilung der erforderlichen Auskünfte gegenüber der Aufsichtsbehörde, wegen unterbliebener Unterrichtung über das Widerspruchsrecht des Betroffenen und Sicherstellung, dass der Betroffene Kenntnis von der Herkunft seiner Daten erhält sowie in materieller Hinsicht wegen unbefugter Erhebung und Verarbeitung personenbezogener Daten, die nicht allgemein zugänglich sind. Der Bußgeldbescheid ist mittlerweile bestandskräftig.

4.1.2 Telefon-Marketing

Firmen, die Telefon-Marketing betreiben, erhalten die Adressen meistens aus den Kundenbeständen ihrer Auftraggeber. Bei den Telefongesprächen mit den beworbenen Personen werden beispielsweise Produktinformationen erteilt und Bestellungen aufgenommen. Stammen die Adressen nicht aus Kundendateien, werden sie von Adresshandelsunternehmen angemietet oder gekauft. Die Rechtsprechung beurteilt Telefonanrufe zu Werbezwecken, die vom Angerufenen nicht veranlasst wurden, restriktiv. Nach Ansicht des Bundesgerichtshofes verstoßen Telefonanrufe zu Werbezwecken

wegen der hierdurch verursachten Beeinträchtigung der Privatsphäre gegen die guten Sitten und damit gegen § 1 des Gesetzes gegen den unlauteren Wettbewerb. Die Beurteilung des unerwünschten Telefon-Marketing als sittenwidrig wirkt sich auf die Auslegung und Anwendung des BDSG aus. Ebenso wie im Falle der unverlangten Werbung per Fax und E-Mail muss auch in diesem Fall davon ausgegangen werden, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung seiner persönlichen Daten überwiegt (§ 28 Abs. 1 Nr. 2 BDSG) bzw. offensichtlich überwiegt (§ 28 Abs. 1 Nr. 3 BDSG), soweit sich die Werbemaßnahme als Wettbewerbsverstoß im Sinne von § 1 des Gesetzes gegen den unlauteren Wettbewerb darstellt.

In dem von der Aufsichtsbehörde zu beurteilenden Fall rief eine Telefon-Marketing-Firma eine Person auf deren privatem Telefonanschluss an und teilte ihr mit, dass sie einen Hotelaufenthalt gewonnen habe. Es stellte sich allerdings im nachhinein heraus, dass der vermeintliche Gewinn mit dem Abschluss eines Zeitschriftenabonnements verbunden war. Die angerufene Person stellte klar, dass sie den Abschluss eines Abonnements nicht wünsche. Dennoch erhielt der Angerufene kurze Zeit später den Hotelgutschein sowie die Bestätigung des Zeitschriftenabonnements und die Mitteilung, dass der Halbjahrespreis von seinem Konto eingezogen werde. Der Betroffene forderte daraufhin die Firma auf, ihm schriftlich darüber Auskunft zu erteilen, welche seine Person betreffenden Daten gespeichert wurden und woher diese Daten stammen. Darüber hinaus wurde die unverzügliche und vollständige Löschung aller gespeicherten Daten sowie die schriftliche Bestätigung der Löschung verlangt. Das Auskunftsersuchen des Betroffenen wurde nicht beantwortet. Die 2-fache Aufforderung der Aufsichtsbehörde, zum Sachverhalt Stellung zu nehmen, blieb ohne Resonanz. Nachdem über insgesamt 5 Monate hinweg keinerlei Reaktionen auf die behördlichen Schreiben zu verzeichnen waren und der Firmeninhaber erst nach Androhung eines konkreten Bußgeldes mitteilte, die Schreiben nie erhalten zu haben, verhängte die Aufsichtsbehörde ein Bußgeld wegen vorsätzlicher Nichterteilung der erforderlichen Auskünfte gegenüber der Aufsichtsbehörde gemäß § 43 Abs. 1 Nr. 10, § 38 Abs. 3 Satz 1 BDSG und wegen unterbliebener Unterrichtung des Betroffenen und der Sicherstellung, dass dieser Kenntnis von der Herkunft seiner Daten erhält (§ 43 Abs. 1 Nr. 3, § 28 Abs. 4 Satz 2 BDSG). Der Bescheid ist bestandskräftig.

4.2 Bloßstellung von Personen durch Veröffentlichung personenbezogener Daten im Internet

Mit einem Offenbaren rufschädigender privater Lebensumstände gegenüber jedermann im Internet lässt sich eine **Prangerwirkung** erzielen, die vom Betreiber der Internetseite zumeist beabsichtigt ist. Im Berichtszeitraum hatte sich die Aufsichtsbehörde wiederholt mit Datenschutzverstößen dieser Art zu beschäftigten. Einen thematischen Schwerpunkt bildete hierbei die Veröffentlichung von **Schuldnerdaten** im Internet.

Beschwerden gingen bei der Aufsichtsbehörde ein, weil die Geschäftsführung eines Dienstleistungsunternehmens persönliche Daten eines ihrer Schuldner in das Internet eingestellt hatte. Insbesondere wurden Name, Vorname, Geburtsdatum, die aktuelle und die frühere Wohnungsanschrift, zwei Funktelefonnummern, die Bankverbindung und der Arbeitgeber bekannt gegeben. Als Anlage wurde u.a. die Mitteilung der Staatsanwaltschaft über die Einleitung eines Ermittlungsverfahrens gegen die betreffende Person angefügt. Der Schuldner war seiner Zahlungsverpflichtung aus einem Vertragsverhältnis nicht nachgekommen. Auf ihrer Internetseite erläuterte die Geschäftsführung, dass die Veröffentlichung im Internet dazu dienen solle, andere Gläubiger vor der Eingehung schädigender Geschäftsbeziehungen zu warnen.

Die Aufsichtsbehörde wies die Geschäftsführerin auf den Rechtsverstoß hin und stellte die Verhängung eines Bußgeldes in Aussicht. Darauf hin wurden die Internetseiten mit den personenbezogenen Schuldnerangaben aus dem Netz entfernt. Aufrechterhalten wurde im Internet eine Seite, auf der die Nutzer Gelegenheit erhielten, über das Vorgehen gegen die nunmehr nur noch mit dem Nachnamen bezeichneten Person per Maus-Taste unter Auswahl einer der aufgelisteten Alternativen (*Was sollen wir mit Herrn X machen ? Russisch Inkasso schicken ? Noch einmal nett mit ihm reden ? Alles pfänden, was möglich ist etc.*) abzustimmen. Mittlerweile wurden durch das Unternehmen alle den Schuldner betreffenden Internetseiten aus dem Netz entfernt.

Die Aufsichtsbehörde sieht in der Veröffentlichung eine durch das BDSG nicht erlaubte Verarbeitung personenbezogener Daten. Der Vorgang ist nach § 28 BDSG zu beurteilen.

Da das Unternehmen die persönlichen Daten seines Schuldners nicht für die Erfüllung eigener Geschäftszwecke speicherte und übermittelte, kommt als Erlaubnistatbestand nur § 28 Abs. 3 Satz 1 Nr. 1 BDSG. 1 in Betracht gekommen. Danach ist die Übermittlung oder Nutzung für einen anderen Zweck auch zulässig, soweit dies 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 oder Nutzung hat.

Es ist der verantwortlichen Stelle zuzugestehen, dass derjenige, der andere Gläubiger vor der Eingehung einer nachteiligen Geschäftsbeziehung warnt, ein berechtigtes Interesse verfolgt. Allerdings stellt das Aussprechen dieser Warnung gegenüber jedermann im Internet nicht das erforderliche Mittel dar. Es existieren durchaus andere Möglichkeiten, die zur Erzielung eines Gläubigerschutzes ebenso geeignet sind, das Persönlichkeitsrecht des Schuldners aber weniger beeinträchtigen. So gibt es Wirtschaftsauskunfteien i. S. v. § 29 BDSG, die bei Nachweis eines berechtigten Interesses, so bei einem bevorstehenden konkreten Vertragsabschluss, Auskunft erteilen über Tatsachen, die mit der Kreditwürdigkeit einer Person in unmittelbarem Zusammenhang stehen, wie beispielsweise die Abgabe einer eidesstattlichen Versicherung. Darüber hinaus verletzt das Vorgehen ein berechtigtes Interesse des Schuldners, da die mit einer Veröffentlichung im Internet herbeigeführten nachteiligen Auswirkungen für seine Person über das verfolgte Ziel hinaus gehen. Das Einstellen von Daten ins Internet hat zur Folge, dass diese von jedermann global abrufbar sind, mit anderen im Internet anzutreffenen Angaben über die betreffende Person problemlos verknüpft und losgelöst von dem Zweck der ursprünglichen Veröffentlichung verwendet werden können.

Entgegen dem Vorbringen des Unternehmens waren die Mitteilungen über den Schuldner im Wesentlichen als nicht allgemein zugängliche Daten zu werten. Dies gilt für die Angaben über die Bankverbindung, die Funktelefonnummern, Haustiere, Wohnungsgröße und die Einleitung eines strafrechtlichen Ermittlungsverfahrens. Auch die Angabe von Beruf und Arbeitgeber, die der Schuldner freiwillig gegenüber seinem Vertragspartner tätigte, sind Daten, die nicht jedermann zugänglich sind.

Bei der Bußgeldbemessung fiel zu Gunsten der verantwortlichen Stelle ins Gewicht, dass nach dem rechtlichen Hinweis durch die Aufsichtsbehörde alle persönlichen Angaben über den Schuldner enthaltenden Seiten geschlossen wurden. Die weiterhin betriebene Internetseite mit dem Abstimmungsforum ermöglichte nicht die Herstellung eines Bezugs zur konkreten Person und vermittelte auch kein Hintergrundwissen für

eine Beteiligung an der Abstimmung. Auch diese Seite wurde mittlerweile entfernt. Insgesamt wurde ein Bußgeld in Höhe von 200,00 € als angemessen erachtet und von dem Unternehmen akzeptiert.

4.3 Handelsregisterauskunftsdienste im Internet

Ein Unternehmen, das Eintragungen im öffentlichen Handelsregister sammelt und speichert, um sie dann über das Internet der Öffentlichkeit zugänglich zu machen, wird im Regelfall als Auskunftei tätig und unterliegt den Anforderungen des § 29 BDSG, der das geschäftsmäßige Erheben, Speichern oder Verändern personenbezogener Daten zum Zwecke der Übermittlung regelt. Auch Presseunternehmen bieten mitunter einen solchen Auskunftsdienst im Internet an. Es stellt sich dann die Frage, ob sie in diesem Fall dem in § 41 BDSG verankerten und durch § 10 des Landespressegesetzes ausgefüllten **„Medienprivileg“** unterliegen und von der staatlichen Datenschutzaufsicht befreit sind oder ob sie wie eine Auskunftei i. S. v. § 29 BDSG behandelt werden müssen.

Ist der Anwendungsbereich des BDSG eröffnet, ist die gesetzliche Zulässigkeit eines solchen Auskunftsdienstes in Frage gestellt. Zwar ist das Handelsregister nach §§ 9, 9a Handelsgesetzbuch (HGB) jedermann zugänglich. Werden die in ihm enthaltenen personenbezogenen Daten aber in Datenverarbeitungsanlagen oder nicht – automatisierten Dateien verarbeitet, unterliegen sie den Anforderungen von § 29 BDSG. Nach § 29 Abs. 1 Satz 1 Nr. 2 BDSG ist das geschäftsmäßige Speichern oder Verändern personenbezogener Daten zum Zwecke der Übermittlung zulässig, wenn die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Speicherung oder Veränderung offensichtlich überwiegt. Die Übermittlung im Rahmen dieser Zwecke ist nach § 29 Abs. 2 Satz 1
Nr. 1 a und Nr. 2 BDSG nur zulässig, wenn der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Werden Handelsregistereintragungen über das Internet jedermann zugänglich gemacht, fehlt es an der glaubhaften Darlegung eines berechtigten Interesses des Empfängers im Einzelfall.

In dem von der Aufsichtsbehörde zu beurteilenden Fall bietet ein Presseunternehmen, das eine regionale Tageszeitung herausgibt, auf seiner Homepage im Internet die Möglichkeit an, Handelsregistereintragungen aus einzelnen Amtsgerichtsbezirken abzufragen. Das Unternehmen wertet zuvor die im Bundesanzeiger veröffentlichten Handelsregistereintragungen im Hinblick auf ihren Regionalbezug aus, stellt die ausgewählten Daten in eine Datenbank ein, um sie über das Internet der Öffentlichkeit zugänglich zu machen. Es handelt sich um ein kostenloses Serviceangebot für den Leser, welches auf der Homepage unter derselben Rubrik wie z. B. „An- und Verkauf“, „Reisen“ etc. erscheint.

§ 10 a des Landespressegesetzes nimmt Unternehmen oder Hilfsunternehmen der Presse von den wesentlichen Vorschriften des BDSG aus, wenn sie personenbezogene Daten ausschließlich zu eigenen **journalistisch-redaktionellen Zwecken** verarbeiten oder nutzen. In diesen Fällen gelten lediglich §§ 5, 7, 9 und 38 a BDSG. Das Landespressegesetz schützt die im Grundgesetz verankerte Pressefreiheit (Art. 5 Abs. 1 GG). Adressaten des Medienprivilegs sind somit alle Hersteller von Druckwerken, die Aufgaben im Rahmen des gesellschaftlichen Kommunikationsprozesses wahrnehmen und die sich auf Art. 5 Abs. 1 GG berufen können. Eine Datenverarbeitung erfolgt zu journalistisch-redaktionellen Zwecken, wenn sie auf eine Verbreitung in der Öffentlichkeit gerichtet ist. Allerdings muss die Publikation eine **redaktionelle Bearbeitung** widerspiegeln, die es rechtfertigt, diese als Beitrag zur Berichterstattung und öffentlichen Meinungsbildung zu werten. Der journalistisch-redaktionelle Zweck ist fraglich, wenn ausschließlich aus fremden Quellen entnommenes Material übermittelt wird, wie dies bei einer Entnahme von Daten aus dem öffentlichen Handelsregister der Fall ist.

Die Aufsichtsbehörde bejahte im Ergebnis die journalistisch – redaktionelle Zielsetzung. Der hier zu bewertende Fall unterscheidet sich von anderen rein kommerziellen Auskunftsdiensten insoweit, als die Eintragungen im Handelsregister vor ihrer Veröffentlichung im Internet nach dem Kriterium ihrer Regionalbedeutsamkeit ausgewählt werden. Darüber hinaus handelt es sich um einen kostenlosen Leserservice, der dem Informationsinteresse der Öffentlichkeit dienen soll, und somit nicht um eine Datenübermittlung zu rein kommerziellen Zwecken. Da insoweit das „Medienprivileg“ eingreift, unterliegt das Presseunternehmen nicht der Datenschutzaufsicht, insbesondere nicht der Meldepflicht nach § 4 d BDSG.

4.4 Ablichtung von Personalausweisen im Geschäfts- und Rechtsverkehr

In datenschutzrechtlicher Hinsicht stellt das Kopieren eines Personalausweisdokuments die Erhebung und Speicherung aller in diesem Dokument enthaltenen Daten dar. Gemäß § 28 Abs. 1 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln nicht allgemein zugänglicher personenbezogener Daten oder ihre Nutzung als Mittel für eigene Geschäftszwecke nur zulässig, wenn dies der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen dient (§ 28 Abs. 1 Nr. 1 BDSG) oder dies zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

4.4.1 Einfahrtserlaubnis für Betriebsgelände nur bei Kopie des Personalausweises

In einem Fall richtete sich die Beschwerde gegen einen produzierenden Gewerbebetrieb, der beim Einfahren der Lastkraftwagen in sein Betriebsgelände von dem jeweiligen Fahrer den Personalausweis verlangte und diesen anschließend kopierte. Die auf diese Weise angefertigten Kopien wurden anschließend in Ordnern abgelegt und aufbewahrt. Zur Stellungnahme aufgefordert erläuterte die Geschäftsleitung, dass die Kopien nur von Mitarbeitern der Speditionsfirmen bei einer erstmaligen geschäftlichen Kontaktaufnahme angefertigt würden. Die Aufbewahrung erfolge in verschlossenen Ordnern Die Räume, in denen die Unterlagen gelagert würden, seien nur dem Personal der Straßenwaage zugänglich. Dieses sei nach § 5 BDSG auf das Datengeheimnis verpflichtet worden. Sobald die Vertragsbeziehung zu der jeweiligen Spedition beendet sei, würden die angefertigten Kopien vernichtet. Als Zweck der Maßnahme wurde die Verhinderung von Diebstählen bzw. eine Beweissicherung bei geschehenen Diebstählen angegeben. Es seien bereits in nicht unerheblichem Umfang Fertigerzeugnisse vom Betriebsgelände durch als Spediteure getarnte Täter entwendet worden. Das Kopieren der Personalausweisdokumente wurde durch die Aufsichtsbehörde beanstandet. Das Unternehmen wurde darüber informiert, dass zum Zwecke der Verhinderung bzw. Aufklärung von Straftaten ein Kopieren der Personalausweisdokumente nicht erforder-

lich ist und insoweit eine Einsichtnahme in den Ausweis und das Festhalten der erforderlichen personenbezogenen Angaben ausreicht. Durch das Kopieren des gesamten Ausweisdokuments werden Daten erlangt, die nicht erforderlich zur Wahrung der Interessen des Unternehmens sind. Zur Wahrung der berechtigten Interessen an einer Verhinderung bzw. Aufklärung von Straftaten genügt die Erfassung von Name, Vorname, Wohnanschrift und Geburtsjahr. Bei einer Beratung vor Ort sicherte das Unternehmen zu, in Zukunft in entsprechender Weise zu verfahren.

4.4.2 Personalausweiskopien in Mietverhältnissen

In einem weiteren Fall beschwerte sich ein Bürger darüber, dass eine Wohnungsvermittlungsfirma bei der Übergabe eines Schlüssels zwecks Wohnungsbesichtigung bzw. beim späteren Abschluss des Mietvertrages eine Kopie seines Personalausweises angefertigt hatte. Dieses Vorgehen wurde ebenfalls von der Aufsichtsbehörde beanstandet. Das Unternehmen wurde darauf hingewiesen, dass eine solche Verfahrensweise nicht durch § 28 Abs. 1 Satz 1 Nr. 2 BDSG gerechtfertigt ist, weil es nicht zur Erfüllung eigener Geschäftszwecke erforderlich ist. Zur Identifizierung von Personen bei Rechtsverstößen reicht es aus, Einsicht in das Personaldokument zu nehmen und Name, Vorname und Wohnanschrift des zukünftigen Mieters festzuhalten. Das Unternehmen wurde aufgefordert, das Kopieren in Zukunft zu unterlassen und alle bereits angefertigten Personalausweiskopien zu vernichten. Der Betrieb akzeptierte die Rechtslage und teilte schriftlich mit, dass sämtliche Mitarbeiter über den Verfahrensweg belehrt und alle angefertigten Personalausweiskopien aus den Akten entfernt und vernichtet wurden.

4.5 Datenverarbeitung in Vereinen, Verbänden, Genossenschaften

Mehrere Bürgereingaben betrafen den Umgang von Vereinen, Verbänden oder Genossenschaften mit personenbezogenen Daten. Häufig wiederkehrende Fragen in diesem Zusammenhang sind, welche Daten von Mitgliedern oder sonstigen Personen zu welchem Zweck erhoben oder gespeichert werden dürfen, unter welchen Voraussetzungen Mitgliederdaten an andere Mitglieder oder an Empfänger außerhalb des Vereins, des Verbandes oder der Genossenschaft übermittelt werden dürfen und welche Anforderungen das Gesetz an eine ordnungsgemäße Verarbeitung und Aufbewahrung der Da-

ten stellt, die vor einer missbräuchlichen Verwendung, einer Kenntnisnahme durch Unbefugte und vor einem Datenverlust schützen.

Für **eigene Zwecke des Vereins** dürfen Mitgliederdaten nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG nur erhoben, verarbeitet oder genutzt werden, soweit es dem Vereinszweck dient, der sich maßgeblich nach der Vereinssatzung und - soweit vorhanden der Vereinsordnung beurteilt. Die Mitgliedschaft in einem Verein ist als vertragsähnliches Vertrauensverhältnis im Sinne von § 28 Abs. 1 Nr. 1 BDSG zu beurteilen, aus dem u. a. folgt, dass der Verein beim Umgang mit Daten das Recht auf informationelle Selbstbestimmung seiner Mitglieder in angemessener Weise berücksichtigen muss. Erhoben, verarbeitet oder genutzt werden dürfen nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG nicht nur die für eine Vereinsmitgliedschaft unbedingt erforderlichen Daten, sondern auch solche, die noch im Rahmen des Vereinszwecks liegen und geeignet sind, diesen zu fördern, wie z. B. die Angabe über besondere Qualifikationen der Vereinsmitglieder.

Für **fremde Zwecke** darf ein Verein Daten seiner Mitglieder übermitteln oder nutzen, soweit dies nach § 28 Abs. 3 Satz 1 Nr. 1 BDSG zur Wahrung berechtigter Interessen eines Dritten oder öffentlicher Interessen erforderlich ist oder wenn es sich um die in § 28 Abs. 3 Satz 1 Nr. 3 BDSG aufgeführten listenmäßigen Daten handelt (insbesondere Angaben über die Zugehörigkeit zu einer Personengruppe, z. B. Mitglied des Vereins X, Name, Anschrift, Geburtsjahr). In beiden Fällen ist eine Übermittlung oder Nutzung der Daten unzulässig, wenn die Aufsichtsbehörde zu der Annahme gelangt, dass ein schutzwürdiges Interesse des Betroffenen entgegensteht. Wegen des vertragsähnlichen Vertrauensverhältnisses, welches den Verein, den Verband oder die Genossenschaft zur Wahrung des Persönlichkeitsrechts der Mitglieder verpflichtet, wird eine Datenübermittlung bzw. -nutzung für fremde Zwecke auf Ausnahmefälle beschränkt bleiben.

Ergibt sich die Zulässigkeit der Datenverarbeitung nicht aus § 28 BDSG, ist sie nur erlaubt, wenn der Betroffene **eingewilligt** hat, nachdem er darüber **informier**t wurde, welche seiner Daten für welchen Zweck verarbeitet und an wen sie übermittelt werden. Die Einwilligung bedarf gemäß § 4a Abs. 1 Satz 3 BDSG der **Schriftform**, soweit nicht wegen besonderer Umstände eine andere Form, z. B. eine mündliche oder eine konkludente, durch schlüssiges Verhalten erklärte Einwilligung angemessen ist.

4.5.1 Datenschutz in Genossenschaften: Bekanntgabe des Namens eines Beschwerdeführers

Die Aufsichtsbehörde hatte sich wiederholt mit der Frage auseinander zu setzen, inwieweit der Vorstand einer Wohnungsbaugenossenschaft berechtigt ist, den Namen eines Beschwerdeführers anderen Wohnungsbaugenossenschaftsmitgliedern bekannt zu geben. In einem Fall hatte sich ein Mitglied gegen die Durchführung einer Sanierungsmaßnahme, in einem anderen Fall gegen die Umlage von Betriebskosten für die Rasenpflege beschwert. Der Vorstand der Genossenschaft hatte auf das Beschwerdeschreiben mit der namentlichen Benennung des betreffenden Mitglieds, in einem Fall im Einladungsschreiben zu einer Mitgliederversammlung, im anderen Fall im Wege eines Aushangs in den verschiedenen Hauseingängen, reagiert.

Die namentliche Benennung der Beschwerdeführer bedeutet im Regelfall eine durch § 28 Abs. 1 BDSG nicht erlaubte Übermittlung von personenbezogenen Daten i. S. v. § 3 Abs. 4 Ziff. 3 BDSG. Auch die Weitergabe der Daten an andere Genossenschaftsmitglieder kann eine Übermittlung an Dritte im Sinne von § 3 Abs. 8 Satz 2 BDSG darstellen. Innerhalb der verantwortlichen Stelle würden die Daten nur dann verbleiben, wenn sie den Funktionsträgern der Genossenschaft bzw. deren Mitarbeitern bekannt gemacht würden. Genossenschaftsmitglieder, die keine Funktion ausüben, stehen außerhalb der verantwortlichen Stelle und sind damit Dritte. Nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist die Übermittlung der Daten nur zulässig, wenn sie zur Wahrung berechtigter Interessen der Wohnungsbaugenossenschaft erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Übermittlung überwiegt. Das Interesse des Vorstandes der Wohnungsgenossenschaft könnte darin liegen, dass er den Genossenschaftsmitgliedern und dem Aufsichtsrat gegenüber rechenschaftspflichtig und somit an einer Aufklärung des Inhalts von Beschwerdeschreiben interessiert ist. Zur Wahrung dieses Interesses ist allerdings die namentliche Benennung der Beschwerdeführer weder geeignet noch erforderlich. Eine Wahrnehmung der satzungsgemäßen Aufgaben kann der Vorstand der Genossenschaft durch eine sachbezogene, auf den Inhalt der Beschwerdeschreiben konzentrierte Prüfung erreichen. Zudem beeinträchtigt die namentliche Nennung der Beschwerdeführer in Einladungsschreiben zu Mitgliederversammlungen und in öffentlichen Aushängen deren schutzwürdige Belange, weil durch eine solche Verfahrens-

weise eine bloßstellende bzw. anprangernde Wirkung erzielt wird, die durch die Genossenschaft zumeist beabsichtigt sein wird.

4.5.2 Nicht ordnungsgemäße Aufbewahrung personenbezogener Daten in Kindervereinen

Das BDSG unterwirft nicht nur die Erhebung, Speicherung, Veränderung oder Übermittlung personenbezogener Daten einer Beschränkung, sondern stellt auch Anforderungen an die ordnungsgemäße Aufbewahrung der Daten zum Schutz vor unbefugten Zugriffen. Auch Vereine müssen die erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen im Sinne von § 9 BDSG treffen, um Missbrauch, unbefugte Kenntnisnahme und Verlust personenbezogener Daten zu verhindern.

Der Aufsichtsbehörde wurde eine nicht datenschutzgerechte Aufbewahrung personenbezogener Daten in Kindervereinen angezeigt. Es handelte sich hierbei um zwei Vereine, die Freizeitaktivitäten sowie Ferienreisen für Kinder organisierten und durchführten. Als die Beschwerde gegenüber der Aufsichtsbehörde erhoben wurde, war über das Vermögen der beiden Vereine bereits das Insolvenzverfahren eröffnet worden. Eine Ortsbegehung bestätigte den Inhalt der Beschwerden. Lediglich der Eingangsbereich war gesichert worden, während ein großer Teil der Fensterreihe an der Rückseite des Gebäudes zerstört war. In der näheren Umgebung des Gebäudes wurden Fotos von Kinderreisen, Listen mit Namen und Anschriften etc. aufgefunden. Im Inneren der ehemaligen Vereinsräume befanden sich Akten mit Personalunterlagen und Gehaltsabrechnungen der Mitarbeiter sowie Listen mit Namen, Anschriften und Telefonnummern der Kinder, die an diversen Aktivitäten der Vereine teilgenommen hatten. Wegen des baulichen Zustandes der Liegenschaft konnte die Aufsichtsbehörde ein Betreten durch Unbefugte nicht ausschließen.

Die verantwortlichen Stellen müssen gemäß § 9 BDSG die technischen und organisatorischen Maßnahmen treffen, die erforderlich sind, um die Ausführungen der Vorschriften des BDSG, insbesondere die in der Anlage zu § 9 BDSG genannten Anforderungen, z.B. Zutritts-, Zugangs-, Zugriffskontrolle zu gewährleisten. § 9 Satz 1 BDSG bezieht sich ausdrücklich nur auf eine automatisierte Datenverarbeitung und -nutzung. Wie sich aus dem Wort „insbesondere“ ergibt, handelt es sich bei den in der Anlage aufgeführten Anwendungsfällen nur um eine nicht abschließende Aufzählung von Beispielen. Auch

bei nicht automatisierten Verfahren sind geeignete technische und organisatorische Maßnahmen zum Schutz der Daten vor unbefugten Zugriffen zu treffen. Die Maßnahmen sind unter Abwägung aller Umstände des Einzelfalles unter Berücksichtigung der konkreten Gefährdungslage zu treffen. Gemäß **§ 38 Abs. 5 BDSG** ist die Aufsichtsbehörde berechtigt, die erforderlichen Anordnungen zum Abstellen festgestellter technischer und organisatorischer Mängel zu treffen.

Die Aufsichtsbehörde hielt im vorliegenden Fall eine konkrete Gefahr für das Persönlichkeitsrecht der ehemaligen Mitarbeiter des Vereins, der in die Vereinstätigkeit involvierten Kinder sowie weiterer Personen, die in Kontakt zu den Vereinen standen, für gegeben. Als Verantwortlicher war in diesem Fall der Insolvenzverwalter heranzuziehen, auf den mit Eröffnung des Insolvenzverfahrens die Aufgabe übergeht, das Vereinsvermögen einschließlich der aus der Vereinstätigkeit resultierenden Geschäftsunterlagen zu verwalten. Er wurde aufgefordert, die Aktenbestände bis zum Abschluss des Insolvenzverfahrens in einer den Anforderungen des § 9 BDSG entsprechenden Weise aufzubewahren und nach § 9 BDSG zu vernichten, sobald sie für die Durchführung des Insolvenzverfahrens nicht mehr benötigt werden.

4.5.3 Veröffentlichung personenbezogener Daten von Kindern im Internet

Vereine, die aufgrund des vertragsähnlichen Vertrauensverhältnisses zu einem vorsichtigen Umgang mit personenbezogenen Daten seiner Mitglieder verpflichtet sind, sollten sorgfältig prüfen, inwieweit sie zu Zwecken der Außendarstellung von Veröffentlichungen im Internet Gebrauch machen. Für eine Veröffentlichung personenbezogener oder personenbeziehbarer Daten im Internet bedarf es einer vorhergehenden **schriftlichen** und **informierten Einwilligung** im Sinne von **§ 4 a Abs. 1 BDSG**.

In einem Fall hatte die Aufsichtsbehörde die Beschwerde mehrerer Eltern gegen einen Kinderverein zu prüfen, der Reisen in Kinderferiencamps organisiert. Auf seiner Homepage hatte er mehrere Reisefotos veröffentlicht, auf denen auch die mitreisenden Kinder in identifizierbarer Weise abgebildet waren. Das Vorgehen wurde von der Aufsichtsbehörde beanstandet, da eine Veröffentlichung dieser Daten nur mit vorheriger **schriftlicher Einwilligung der Eltern** erlaubt ist.

4.6 Datenschutz im Gesundheitswesen

4.6.1 Verwendung von Rezeptdaten durch Apothekenrechenzentren

Die Apotheken führen die Abrechnung mit den Krankenkassen in der Regel nicht selbst aus, sondern bedienen sich für die Erfüllung dieser Aufgabe eines Apotheken-Rechenzentrums. Die Rechenzentren sind allerdings in den letzten Jahren dazu übergegangen, die Rezeptdaten nicht nur für die Abrechnung mit den Krankenkassen, sondern auch für vielfältige andere Auswertungen durch die jeweilige Apotheke aufzubereiten. Die Daten werden versicherten- und arztbezogen auf einer CD, die meist als Apotheken - CD bezeichnet wird, gespeichert und an die Apotheken geliefert und/oder die Daten werden online für die Apotheken angeboten.

Eines dieser Rechenzentren wurde durch die Aufsichtsbehörde im Berichtszeitraum geprüft. Dieses erstellt u.a. für die Apotheken monatlich eine Arztstatistik, die den Umsatz der 30 umsatzstärksten Ärzte sowie die häufigsten Indikationen und verschriebenen Produkte der 4 umsatzstärksten Ärzte in einem Abrechnungsmonat ausweist. Ferner stellt es den Vertragsapotheken auf Wunsch eine Apotheken - CD und einen Online-Abrufdienst zur Verfügung, mittels dessen die Apotheke alle von ihr selbst zum Zweck der Abrechnung eingereichten Rezeptdaten des Vormonats abrufen kann, so z.B. die Rezeptnummer, die Arztnummer, Anschrift und Geburtsdatum des Patienten, verordnetes Medikament und ähnliche Daten.

Eine Aufbereitung von Rezeptdaten in dieser Form ist mit dem Datenschutzrecht nicht zu vereinbaren, weil die verfolgten Interessen über die im Sozialgesetzbuch bestimmten Zwecke hinausgehen. Die Rechenzentren dürfen nach § 300 Abs. 2 Satz 2 des Fünften Buches des Sozialgesetzbuches (SGB V) Rezeptdaten nur für die im Sozialgesetzbuch bestimmten Zwecke und ab dem 1. Januar 2003 aufgrund des Arzneimittelausgaben-Begrenzungsgesetzes – AABG – nur in einer auf diese Zwecke ausgerichteten Weise verarbeiten und nutzen, soweit sie dazu von einer berechtigten Stelle beauftragt worden sind. Für andere Zwecke als solche des SGB dürfen nur anonymisierte Daten verarbeitet werden, wobei die Anonymisierung sowohl versicherten- als auch arztbezogen zu verstehen ist. Die im Apotheken-Rechenzentrum verarbeiteten Daten

dürfen, soweit sie nicht anonymisiert wurden, nur zu den im SGB V bestimmten Zwecken an die Apotheken weitergeleitet werden. Bei diesen Zwecken handelt es sich insbesondere um

- die Erstellung von Zuzahlungsbescheinigungen für die Patienten
- Möglichkeiten der Rezeptrecherche für Patienten, Ärzte und Krankenkassen und
- Die Nachvollziehbarkeit der Berechtigung einer Retaxation.

Die Rechenzentren haben deshalb die Funktionen der durch sie auf CD gespeicherten und online bereit gehaltenen Rezeptdaten auf diese Zwecke zu begrenzen. Diese Auffassung entspricht derjenigen, die von der Mehrheit der Mitglieder des Düsseldorfer Kreises, dem Gremium der obersten Aufsichtsbehörden der Bundesländer über den Datenschutz im nicht – öffentlichen Bereich, vertreten wird.

4.6.2 Outsourcing – externe Archivierung von Patientenakten aus Krankenhäusern und Arztpraxen

Zwei an die Aufsichtsbehörde gerichtete Anfragen betrafen die **Einlagerung von Patientenakten** aus Krankenhäusern und Arztpraxen. Ein Logistikcenter und ein IT-Dienstleistungsunternehmen teilten mit, dass sie die Eröffnung eines neuen Geschäftsfeldes – Lagerung von Patientendaten - planten, und baten um Beratung hinsichtlich der einzuhaltenden Datenschutzbestimmungen.

Bei einer Besichtigung des Logistikunternehmens stellte sich heraus, dass vor der Auslagerung der Akteninhalt durch Mitarbeiter des Krankenhauses mittels Datenverarbeitungsanlagen elektronisch erfasst (gescannt) werden sollte. Die Patientenakten sollten anschließend in verklebten Kartons zusammen mit medizinischen Geräten in großen Lagerhallen des Unternehmens aufbewahrt werden. Es war geplant, die Lagerhalle durch einen Streckzaun mit eingebautem Tor von der benachbarten Werkstatt abzugrenzen. Zum Lagerbereich sollten nur 4 bis 5 Mitarbeiter Zugang haben, die vorhandenen Tore zur Be- und Entladung stets verschlossen bleiben.

Die Aufsichtsbehörde teilte den Unternehmen mit, dass ein Outsourcing in dieser Form mit den geltenden Datenschutzvorschriften nicht vereinbar ist.

Gegen das Scannen von Patientenakten bestehen zunächst keine datenschutzrechtlichen Bedenken, wenn es in den Räumen des Arztes bzw. des Krankenhauses durch eigenes, d.h. vom Auftraggeber eingesetztes Personal erfolgt, das eine Gehilfenstellung im Sinne des § 203 Abs. 3 Satz 2 StGB innehat.

Die nach dem Scannen vorgesehene externe Aufbewahrung der Originalunterlagen ist jedoch weder mit dem zwischen dem Arzt bzw. dessen Berufsgehilfen und dem Patienten bestehende, strafrechtlich durch § 203 Strafgesetzbuch (StGB) geschützten Vertrauensverhältnis noch mit dem strafprozessualen Beschlagnahmeschutz nach § 97 Strafprozessordnung (StPO) zu vereinbaren.

Nach § 203 Abs. 1 Satz 1 StGB macht sich strafbar, *„wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- und Geschäftsgeheimnis, offenbart, das ihm als 1. Arzt, Zahnarzt...anvertraut worden ist...“* Nach § 203 Abs. 3 StGB stehen den in Absatz 1, S. 1 Genannten ihre *„berufsmäßig tätigen Gehilfen und die Personen gleich, die bei ihnen zur Vorbereitung auf den Beruf tätig sind.“* Diese Strafvorschrift ist bei der Anwendung und Auslegung des BDSG zu beachten, denn ein nach dem Strafgesetzbuch verbotenes Verhalten kann datenschutzrechtlich nicht erlaubt sein.

Die Auslagerung von Patientendaten ist somit nur zulässig, wenn hierfür eine gesetzliche Befugnis besteht oder wenn der Patient seine ausdrückliche Einwilligung hierzu erteilt hat oder wenn die Übergabe des Datenmaterials im Einzelfall nicht das Merkmal des Offenbarens erfüllt.

Anders als in anderen Bundesländern enthält das Krankenhausgesetz des Landes Sachsen-Anhalt keine auf den Patientendatenschutz zugeschnittenen Befugnisnormen. Die Weitergabe der Daten an einen Auftragnehmer kann somit nur durch eine Einwilligung des Patienten im Sinne von § 4 a BDSG gerechtfertigt werden, die z. B. im Behandlungsvertrag mit dem Krankenhaus enthalten sein kann. Da es vorliegend allerdings um die Auslagerung archivierter Akten ging, war eine nachträgliche Einholung sämtlicher Patienteneinwilligungen praktisch nicht realisierbar. Ohne Einwilligung des Patienten ist eine Auslagerung nur zulässig, wenn durch die Maßnahme keine personenbezogenen Daten offenbart werden, indem durch ausreichende technische und organisatorische Maßnahmen (§ 9 BDSG) sichergestellt ist, dass Unbefugte keine Kenntnis nehmen können. Praktisch kann eine unbefugte Kenntnisnahme in der Regel bereits dadurch wirkungsvoll ausgeschlossen werden,

dass Behältnisse in einer Weise verschlossen werden, die jede unbefugte Öffnung sichtbar macht. Mit einer solchen Lösung wird allerdings nicht dem durch **§ 97 StPO** gewährleisteten **strafprozessualen Beschlagnahmeschutz** Rechnung getragen. Dieser besteht gemäß § 97 Abs. 2 StPO nur dann, wenn sich die Gegenstände im Gewahrsam der zeugnisverweigerungsberechtigten Personen, d. h. des Arztes und seiner Berufsgehilfen, befinden. Es ist deshalb erforderlich, dass die Krankenakten in Schließfächern, Containern oder verschlossenen Räumen verwahrt werden, die nur von Bediensteten des Krankenhauses bzw. der Arztpraxis geöffnet bzw. betreten werden können. Bei dieser Unterbringung besteht der Gewahrsam des Krankenhauses oder Arztes fort. Würden die Akten wie geplant zusammen mit weiteren Gegenständen in der Lagerhalle der Firma aufbewahrt werden, ginge trotz des vorgesehenen Verschlusses der Kartons der Gewahrsam des Krankenhauses bzw. des Arztes mit der Auslagerung unter.

Die aus § 203 StGB bzw. § 97 StPO hergeleiteten Anforderungen lassen sich auch nicht dadurch erreichen, dass Mitarbeiter der Unternehmen zur Verschwiegenheit verpflichtet werden bzw. einen Arbeits- oder Dienstvertrag mit dem Krankenhaus oder dem Arzt abschließen. Hierdurch erlangen sie noch nicht die Stellung eines Berufsgehilfen im Sinne von § 203 Abs. 3 Satz 2 StGB, weil die Behandlung der Patienten zum Zeitpunkt der Archivierung abgeschlossen ist und einer Archivierung und Lagerung der erforderliche sachliche und räumliche Zusammenhang mit dem Behandlungsgeschehen fehlt.

4.6.3 Verwahrung von Patientenakten nach Auflösung einer Arztpraxis durch Tod, Verkauf oder Insolvenzverfahren

Die Auflösung einer Arztpraxis durch Verkauf, Tod des Arztes oder durch die Eröffnung des Insolvenzverfahrens wirft in Bezug auf das Schicksal der Patientendateien datenschutzrechtliche Fragen auf, wenn die nach der Berufsordnung der Ärzte oder anderen gesetzlichen Bestimmungen vorgesehene Aufbewahrungsfrist noch nicht abgelaufen ist, so dass einer Vernichtung der Unterlagen und damit einer Löschung der Patientendaten § 35 Abs. 2 Satz 1 i. V. m. Abs. 3 Nr. 1 BDSG entgegensteht.

Beim **Verkauf einer Arztpraxis** stellt die Übergabe der Patientenakten an den Nachfolgearzt ohne Einwilligung der Patienten eine durch das Gesetz nicht erlaubte Übermittlung besonderer Arten personenbezogener Daten dar. Der Sachverhalt erfüllt den Tatbestand des § 203 Abs. 1 Nr. 1 StGB. Keine Rolle spielt in Bezug auf die Tatbestandsmäßigkeit des Verhaltens, dass die Weitergabe an eine Person erfolgt, die gleichfalls der ärztlichen Schweigepflicht unterliegt. Die Einwilligung muss sich bereits auf die Übergabe der Patien-

tendateien beziehen. Erst recht bedarf es einer Einwilligung in die Einsichtnahme durch den Nachfolgearzt. Aus § 28 Abs. 6 BDSG folgt, dass sich die Patienteneinwilligung ausdrücklich auf die übermittelten Daten beziehen muss (§ 4 a Abs. 3 BDSG), da es sich bei den Patientendateien um sensitive Daten i. S. v. § 3 Abs. 9 BDSG handelt.

Im Fall des **Todes des Arztes** sind dessen Erben, auch wenn sie nicht Ärzte sind, zur Aufbewahrung und zur Verschwiegenheit in Bezug auf die Patientengeheimnisse verpflichtet. Die Erben unterliegen zwar nicht der Berufsordnung der Ärzte, sind aber Gesamtrechtsnachfolger des Verstorbenen gemäß § 1922 BGB und haben die dem Arzt nach § 9 Abs. 1 und § 10 Abs. 3 Berufsordnung der Ärztekammer Sachsen-Anhalt obliegende Pflicht zur Aufbewahrung und zur Verschwiegenheit als Nachlassverbindlichkeit zu erfüllen (§ 1967 BGB). Auch die strafrechtlich sanktionierte Schweigepflicht des Arztes geht mit dessen Tod nicht unter. Gemäß § 203 Abs. 3 Satz 2 StGB trifft diese diejenigen Personen, die die Geheimnisse vom Verstorbenen oder aus dessen Nachlass erlangt haben. Der Gesetzgeber geht von einem Fortwirken der besonderen Vertrauensbeziehung zwischen Arzt und Patient aus, die nach dessen Tod durch die Erben gewährleistet werden muss.

Die Aufsichtsbehörde hatte sich im Berichtszeitraum mit der Eingabe der Erben eines verstorbenen Arztes zu beschäftigen, über dessen Vermögen das Nachlassinsolvenzverfahren eröffnet worden war. Die Beschwerde richtete sich gegen den Insolvenzverwalter, der beabsichtigte , die Patientenakten aus einer langjährigen ärztlichen Tätigkeit einem Großhandelsunternehmen zu übergeben. Die Patientendaten sollten mittels Datenverarbeitungsanlagen elektronisch erfasst und die Karteikarten in Archivschachteln gelagert werden. Zum Leistungsangebot der Firma gehörte über die bloße Erfassung und Aufbewahrung hinaus die Erteilung von Auskünften an Patienten, Krankenhäuser und Versicherungen.

Die beabsichtigte Übergabe der Patientenakten wurde als eine unzulässige Übermittlung sensitiver Daten an Dritte beanstandet. Die Rüge richtete sich in diesem Fall gegen den Insolvenzverwalter, nicht gegen die Erben, weil mit Eröffnung des Insolvenzverfahrens die Verwaltungs- und Verfügungsbefugnis auf den Verwalter übergeht und bis zur Beendigung des Insolvenzverfahrens bei diesem verbleibt, solange er nicht die Freigabe erklärt.

Der Insolvenzverwalter selbst ist nicht unumschränkt berechtigt, Einsicht in Patientenunterlagen zu nehmen. Infolge seiner Verwaltungs- und Verfügungsbefugnis als Insolvenzverwalter ist er allerdings zur Prüfung der Karteien insoweit berechtigt, als dies zur Beurteilung der Frage erforderlich ist, ob die gesetzliche Aufbewahrungsfrist abgelaufen ist und die Unterlagen vernichtet werden können. Grund für das eingeschränkte Einsichtsrecht ist, dass der

Insolvenzverwalter nicht der strafbewehrten Schweigepflicht nach § 203 Abs. 1 StGB unterliegt. Wird ein Rechtsanwalt als Insolvenzverwalter bestellt, gilt für diesen Teil seiner Tätigkeit nicht die strafrechtlich sanktionierte Schweigepflicht, weil er kraft hoheitlichen Auftrag und nicht im Rahmen eines persönlichen Vertrauensverhältnisses tätig wird. Die Patientengeheimnisse wurden ihm nicht anvertraut, wie dies in § 203 Abs. 1 StGB vorausgesetzt wird. Selbstverständlich ist der Insolvenzverwalter aber an die Vorschriften des BDSG gebunden. Gesundheitsdaten sind „besondere Arten personenbezogener Daten“ und unterliegen einem besonderen Schutz (§ 3 Abs. 9 BDSG). Ihre Erhebung, Verarbeitung und Nutzung für eigene Geschäftszwecke ist nach § 28 Abs. 6 BDSG nur mit Einwilligung des Betroffenen nach § 4 a BDSG zulässig, wenn nicht einer der in § 28 Abs. 6 Nr. 1-4 aufgezählten Ausnahmefälle vorliegt. Die Voraussetzungen dieser Erlaubnisnorm waren im hier untersuchten Fall nicht erfüllt.

4.7 Videoüberwachung von Gebäuden

In der Absicht, die sich ausbreitende Überwachung öffentlich zugänglicher Räume mittels optisch-elektronischer Einrichtungen an eine gesetzliche Regelung zu binden, führte der Ge setzgeber mit der BDSG-Novelle eine neue Vorschrift zur Videoüberwachung ein **(§ 6 b BDSG)**. Zuvor musste derjenige, der sich in seinen Rechten beeinträchtigt fühlte, den Zivil rechtsweg beschreiten und unter Berufung auf eine Verletzung seines allgemeinen Persön lichkeitsrechts und der gesetzlichen Vorschriften zum Schutz seines Rechts am eigenen Bild Abwehransprüche gem. §§ 823 Abs. 1, Abs. 2, 1004 BGB geltend machen, da eine Videoauf nahme grundsätzlich keine Datei i. S. v. § 3Abs. 2 BDSG darstellte und der Anwendungsbe reich des BDSG somit nicht eröffnet war. Die Beobachtung **öffentlich zugänglicher Räume**, d. h. solcher Räume, die nach dem erkennbaren oder mutmaßlichen Willen des Berechtigten von jedermann betreten werden dürfen, ist gemäß § 6 b BDSG nur zur Wahrnehmung des **Hausrechts** oder sonstiger **berechtigter Interessen** zulässig. Die Beobachtung ist unzulässig, wenn **schutzwürdige Interessen des Betroffenen** überwiegen. Die Zwecke müssen vor Beginn der Beobachtung konkret festgelegt sein. Die verantwortliche Stelle muss auf die Tatsache der Beobachtung **hinweisen**. § 6 b BDSG kommt nicht zur Anwendung, wenn eine Überwachung ausschließlich für private oder familiäre Zwecke erfolgt (§ 1 Abs. 2 Nr. 3 BDSG), d. h. wenn der Umstand der Beobachtung ausschließlich im privaten Bereich ver bleibt.

4.7.1 Videokamera in Hörgeschädigteneinrichtung

In einem durch die Aufsichtsbehörde zu prüfenden Fall richtete sich die Beschwerde gegen eine Einrichtung für Hörgeschädigte, die im öffentlich zugänglichen Flurbereich eine Videokamera angebracht hatte. Es war zu befürchten, dass die Beobachtung mit der Kamera zugleich das Verstehen von Kommunikationsinhalten ermöglicht, da der betroffene Personenkreis mittels der Gebärdensprache (visuelle Sprache) kommuniziert. Anlässlich einer Ortsbegehung wurde festgestellt, dass eine Videokamera im öffentlichen Flurbereich der Hörgeschädigteneinrichtung angebracht ist, es sich bei diesem Bereich allerdings nicht, wie behauptet wurde, um eine Sitz- bzw. Raucherecke handelt, sondern um einen reinen Durchgangsbereich. Der Bereich, in dem sich gewöhnlich Angehörige der Einrichtung zum Zweck der Kommunikation aufhalten, wird von der Kamera nicht mehr erfasst. Eine Speicherung der Bilder erfolgt nicht. Die Kamera ist mit einem in einem Büroraum des Gebäudes aufgestellten Bildschirm verbunden, welcher von dort aus überwacht wird. Seinen Angaben zufolge wurden in dem Gebäude schon mehrfach am Tag Diebstähle begangen, weshalb man sich für die Installation einer Videokamera im Eingangsbereich entschieden habe. Es wurde festgestellt, dass unterhalb der Kamera ein Schild angebracht ist, das auf die Videoüberwachung hinweist, das allerdings für Hereinkommende nicht deutlich sichtbar ist.

Von der Aufsichtsbehörde wurde zunächst angenommen, dass es sich bei dem überwachten Eingangsbereich um einen öffentlich zugänglichen Raum handelt. Die Einrichtung beherbergt verschiedene Vereine und Verbände für Hörgeschädigte. Wegen des hierdurch bedingten Publikumsverkehrs steht die Eingangstür meistens offen. Auch wenn mittels der Kamera im Durchgangsbereich keine Aufzeichnung möglich ist, so liegt dennoch eine Beobachtung im Sinne des § 6 b BDSG vor, da eine solche keine Speicherung der Bilder voraussetzt, sondern auch die reine Beobachtung zu dem Zweck, sofortige oder nachfolgende Interventionen zu ermöglichen, erfasst. Es wurde ferner anerkannt, dass ein zulässiger Beobachtungszweck vorliegt, weil die Kamera die Wahrnehmung des Hausrechts und der Verfolgung berechtigter Interessen für konkret festgelegt Zwecke (§ 6 b, Abs. 1, Ziff. 2 und Ziff. 3 BDSG), in diesem Fall der zukünftigen Verhinderung bereits geschehener Diebstähle und der Beweissicherung, dienen soll. Wenn es sich als richtig erwiesen

hätte, dass die Kamera den Ort filmt, an dem sich gewöhnlich Hörgeschädigte der Einrichtung für eine Rauchpause und eine private Unterhaltung zusammenfinden, wäre die Videoüberwachung wegen Entgegenstehens überwiegender schutzwürdiger Interessen der Betroffenen als unzulässig einzustufen gewesen. Da jedoch durch das Aufnehmen des reinen Durchgangsbereichs allenfalls Bruchstücke von Gesprächsinhalten verstanden werden können, ist die Überwachung in diesem Fall von § 6 b Abs. 1 BDSG gedeckt. Allerdings wurde von der Aufsichtsbehörde beanstandet, dass der Umstand der Beobachtung nicht in ausreichender Weise kenntlich gemacht wurde. Es erging insoweit eine Aufforderung, ein Hinweisschild bereits an der Eingangstür anzubringen. Dem Verlangen der Aufsichtsbehörde wurde entsprochen.

4.7.2 Vermeintliche Überwachung mit Kameraattrappen

Eine an die Aufsichtsbehörde gerichtete Anfrage betraf die Zulässigkeit einer lediglich vermeintlich personenbezogenen Videoüberwachung mit Hilfe einer Kameraattrappe. Der Vorgang ist datenschutzrechtlich irrrelevant, da Voraussetzung für die Anwendung von § 6 b BDSG die Beobachtung mit optisch-elektronischen Einrichtungen ist. Selbst wenn eine Attrappe denselben Überwachungsdruck erzeugen kann, fehlt es bereits am Merkmal des Beobachtens. Auch auf eine vermeintliche Beobachtung durch eine als solche nicht erkennbare Attrappe muss jedoch nach Auffassung der Aufsichtsbehörde in entsprechender Anwendung des § 6 b Abs. 2 BDSG hingewiesen werden, weil der Eindruck der Beobachtung erzeugt wird.

4.7.3 Überwachung eines Betriebsgeländes

Eine weitere Beschwerde betraf die Überwachung des Betriebsgeländes eines Verkehrsbetriebes. Ein Firmengelände ist, selbst wenn tatsächlich jedermann das Gelände betreten kann, kein öffentlich zugänglicher Raum, da der Betriebsinhaber den Zugang in der Regel nur einem begrenzten Personenkreis gestatten will. Die Beschwerde richtete sich in diesem Fall allerdings dagegen, dass die an der Rückseite des Betriebsgeländes installierte Kamera über dieses hinaus ging und die öffentliche Straße überwachte. Anlässlich einer Ortsbegehung durch die Aufsichtsbehörde erläuterte der Betriebsleiter, dass lediglich das Gewerbeobjekt und seine Grenzen beobachtet werden sollen, um regelwidriges Verhalten rechtzeitig zu erkennen. Die Beschwerde führte im Ergebnis nicht zur Rüge eines Datenschutzverstoßes, weil bei der Besichtigung deutlich wurde, dass die Beobachtungsmöglichkeit unwesentlich über das Betriebsgelände und seine Grenzen hinausreich-

te. Dennoch wurde von der Aufsichtsbehörde die Empfehlung erteilt, die Kamera im Radius zu begrenzen und zur Straßenseite hin, z. B. durch den Einbau eines Sichtschutzes, blind zu machen.

4.7.4 Videokamera auf Privatgrundstück

Schließlich ging bei der Aufsichtsbehörde die Beschwerde von zwei Grundstückseigentümern ein, die sich durch die Videokamera ihrer Nachbarn beobachtet fühlten. Die Überwachung des eigenen Privatgrundstücks eröffnet noch nicht den Anwendungsbereich des § 6 b BDSG, weil dieses keinen öffentlich zugänglichen Raum darstellt, sei denn die Kamera ist über das eigene Grundstück hinaus auf einen öffentlichen Weg bzw. angrenzende Gebäude des Grundstücks gerichtet. Eine Beobachtung, die im privaten Bereich verbleibt, weil sie ausschließlich für private oder familiäre Tätigkeiten erfolgt (§ 1 Abs. 2 Nr. 3 BDSG), begründet noch nicht die Zuständigkeit der Aufsichtsbehörde. Im konkreten Fall konnten selbst nach einer Ortsbegehung keine ausreichenden Anhaltspunkte gefunden werden, dass die Kamera überhaupt in Betrieb war und dass sie auch Bereiche außerhalb des privaten Grundstücks erfasste. Vom Grundstückseigentümer wurde dies stets verneint. Die Beschwerdeführer waren überdies mit einer auf Unterlassung gerichteten Klage vor dem Amtsgericht wegen Verletzung des allgemeinen Persönlichkeitsrechts unterlegen, da sie als Kläger nicht beweisen konnten, dass die Kamera auf das Nachbargrundstück ausgerichtet ist. Da es sich um ein privates Wohnhaus handelt, konnte die Aufsichtsbehörde eine Klärung der Verhältnisse auch nicht durch Betreten und Besichtigen des Grundstücks und der installierten Kamera herbeiführen, da § 38 Abs. 4 Satz 1 BDSG ohne Einwilligung des Berechtigten nur das Betreten von Geschäftsräumen und –grundstücken zulässt.

5. Zusammenarbeit mit anderen Aufsichtsbehörden

5.1 Der Düsseldorfer Kreis

Der Düsseldorfer Kreis wurde im Jahr 1978 auf Initiative des nordrhein-westfälischen Innenministeriums mit dem Ziel ins Leben gerufen, gemeinsame - zumindest von der Mehrheit seiner Mitglieder - getragene Positionen bei der Auslegung und Anwendung der

Bestimmungen des BDSG zu erarbeiten. Themenschwerpunkte der Diskussion sind z. B. die Kredit- und die Versicherungswirtschaft, die SCHUFA, Handelsauskunfteien, Adresshandel, Direktwerbung, Versandhandel, Arbeitnehmerdatenschutz und Schutz von Patientendaten. Darüber hinaus betrachtet es der Düsseldorfer Kreis als seine Aufgabe, einen Dialog mit den Unternehmen der Privatwirtschaft, in der Regel durch Kontaktaufnahme mit deren Spitzenverbänden, anzubahnen und zu fördern, um die Akzeptanz für den Datenschutz zu erhöhen und Konzepte zu entwickeln, die den Belangen der Beteiligten in besonderem Maße gerecht werden. Beim Düsseldorfer Kreis handelt es sich um ein Gremium der **obersten Aufsichtsbehörden** der Bundesländer über den Datenschutz im nicht-öffentlichen Bereich. Dies sind die Innenministerien der Länder, welche zugleich die ministerielle Fachaufsicht über die i. S. v. § 38 BDSG zuständigen Aufsichtsbehörden führen, sowie die Landesdatenschutzbeauftragten in den Bundesländern, in denen diese nicht nur für den Umgang öffentlicher Stellen des Landes mit personenbezogenen Daten, sondern auch für den Datenschutz im nicht-öffentlichen Bereich zuständig sind. An den Sitzungen des Düsseldorfer Kreises nimmt auch der Bundesdatenschutzbeauftragte teil. Das Land Sachsen-Anhalt ist hier durch das Ministerium des Innern vertreten.

5. 2 Workshop der Aufsichtsbehörden über den Datenschutz im nicht-öffentlichen Bereich

Jedes Jahr im September treffen sich Vertreter der **Aufsichtsbehörden** über den Datenschutz im nicht-öffentlichen Bereich zu einem Arbeitstreffen („Workshop“) jeweils in einem anderen Bundesland mit dem Ziel, die Zusammenarbeit der Aufsichtsbehörden untereinander zu intensivieren und Probleme, die bei der täglichen Arbeit auftauchen, gemeinsam zu lösen. Von Bedeutung ist ein solcher Erfahrungsaustausch vor allen Dingen in den Fällen, in denen in mehreren Bundesländern gleichzeitig bzw. bundesweit agierende Unternehmen einer datenschutzrechtlichen Prüfung zu unterziehen sind und eine einheitliche Vorgehensweise durch die Aufsichtsbehörden anzustreben ist.
Der letzte Workshop der Aufsichtsbehörden fand im September des vergangenen Jahres in Schwerin statt. Besprechungsthemen waren z. B. die praktischen Erfahrungen mit den Prüftätigkeiten, d. h. den Anlass unabhängigen Prüfungen, die Datenübermittlung von Auskunfteien in Drittländer, die datenschutzrechtlichen Probleme im Zusammenhang mit Werbemaßnahmen, das Kopieren von Ausweispapieren sowie die Auslegungsprobleme bei sensitiven Daten i. S. v. § 3 Abs. 9 BDSG.