
SACHSEN-ANHALT

Landesverwaltungsamt

# Zweiter Tätigkeitsbericht

## der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich des Landes Sachsen-Anhalt - Landesverwaltungsamt

**Berichtszeitraum: 01.06.2003 bis 31.05.2005**

# Das Landesverwaltungsamt im Überblick

## Abteilung 1 - Zentraler Service (0345) 514-1400

Fördermittelmanagement · Organisation, IT · Justiziariat · Haushalt · Innerer Dienst · Personaleinsatz, Personalbetreuung · Personalentwicklung, Aus- und Fortbildung

## Abteilung 2 - Bau und Ordnung (0345) 514-1201

Hoheitsangelegenheiten, Gefahrenabwehr · Brand- und Katastrophenschutz, militärische Angelegenheiten · Verbraucherschutz, Veterinärangelegenheiten · Bauwesen · Städte- und Wohnungsbauförderung, Wohnungswesen, Schulbauförderung · Denkmalschutz, UNESCO-Weltkulturerbe · Landesamt zur Regelung offener Vermögensfragen (Vermögensrecht, Singularentschädigung, Unternehmensentschädigung) · Integration Aussiedler, 2. SED-UnBerG

## Abteilung 3 - Wirtschaft und Kommunales (0345) 514-1361

Wirtschaft · Planfeststellungsverfahren · Beschäftigungs- und Arbeitsmarkt-förderung · Kommunalrecht, Kommunale Wirtschaft und Finanzen · Stiftungen · Kultur, Fachstelle für öffentliche Bibliotheken · Sport · Raumordnung, Landesentwicklung- und Verkehrswesen

## Abteilung 4 - Landwirtschaft und Umwelt (0345) 514-1377

Abfallwirtschaft, Bodenschutz · Immissionsschutz, Gentechnik, Umweltverträglichkeitsprüfung · Wasser · Abwasser · Naturschutz, Landschaftspflege · Großschutzgebiete · Forst- und Jagdhoheit · Agrarwirtschaft, Ländliche Räume, Fischerei

## Abteilung 5 - Schule (0345) 514-1830

Grundschulen · Sekundarschulen · Gymnasien, Gesamtschulen · Förderschulen · Berufsbildende Schulen · Fort- und Weiterbildung, Schulpsychologische Beratung · Evaluation, Schulinspektion · Personal, Haushalt, Schulrecht · Unterrichtsversorgung, Datenerhebung, Schulentwicklungsplanung · Staatliche Seminare für Lehrämter

## Abteilung 6 - Familie, Gesundheit, Jugend und Versorgung (0345) 6912-100

Landesjugendamt - Jugend, - Familie und Frauen, - Kindertageseinrichtungen · Gesundheit · Arzneimittel, Apothekenwesen · Heimaufsicht, Rettungsdienst · Landesprüfungsamt für Gesundheitsberufe · Integrationsamt · Landesversorgungsamt · Versorgungsamt - Hauptfürsorgestelle, Soziales Entschädigungsrecht · Versorgungsamt - Schwerbehindertenrecht · Bundeselterngeld

# Zweiter Tätigkeitsbericht

## der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich des Landes Sachsen-Anhalt – Landes-verwaltungsamt Sachsen-Anhalt

**Berichtszeitraum: 01.06.2003 bis 31.05.2005**

**Landesverwaltungsamt Sachsen-Anhalt**
- **Justiziariat –**
Willy-Lohmann-Straße 7

06114 Halle (Saale)

**Inhaltsverzeichnis**

# 1. Einführung

## 1.1 Datenschutz allgemein – Abgrenzung zwischen nicht-öffentlichem und öffentlichem Bereich

Datenschutz dient dem Zweck, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Eine solche Beeinträchtigung kann sowohl durch **öffentliche Stellen** als auch **nicht-öffentliche Stellen** erfolgen.

Zu den **öffentlichen Stellen** sind die

- öffentlichen Stellen des Bundes, also die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ungeachtet ihrer Rechtsform deren Vereinigungen, sowie
- öffentliche Stellen der Länder, d.h. die Behörden, die Organe der Rechtspflege und andere öffentlich-rechlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie ungeachtet ihrer Rechtsform deren Vereinigungen

zu zählen.
Alle übrigen natürlichen und juristischen Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts sind grundsätzlich **nicht-öffentliche** Stellen (für Stellen der Religionsgesellschaften gilt regelmäßiger kirchliches DS-Recht).

Diese Unterscheidung nach der Art der Personen oder Institutionen, die mit personenbezogenen Daten umgehen, ist maßgeblich dafür, welches bereichsübergreifendes Gesetz zum Schutz der Daten des Einzelnen zur Anwendung kommt, soweit der Datenschutz nicht in Fachgesetzen bereichsspezifisch geregelt ist.

Das **Bundesdatenschutzgesetz** **(BDSG)** gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch **öffentliche Stellen des Bundes**. Daneben regelt das BDSG aber auch die Rechte und Pflichten der **nicht-öffentlichen Stellen** beim Umgang mit personenbezogenen Daten.

In Sachsen-Anhalt gibt es des Weiteren das **Gesetz zum Schutz personenbezogener Daten (DSG-LSA)**, welches für die Erhebung, Verarbeitung und Nutzung personenbezogener

Daten durch Behörden, Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Landes, der Gemeinden, der Landkreise und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie - ungeachtet ihrer Rechtsform - deren Vereinigungen anzuwenden ist. Das DSG-LSA regelt demzufolge nur den Datenschutz im **öffentlichen Bereich**.

Werden also personenbezogene Daten durch **nicht-öffentliche Stellen** erhoben, verarbeitet und genutzt, gilt das BDSG. Allerdings nur, soweit die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben werden oder die Daten in oder aus nicht automatisierten Dateien verarbeitet, genutzt oder dafür erhoben werden. Zudem findet das BDSG nur Anwendung, wenn die Erhebung, Verarbeitung oder Nutzung der Daten nicht ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt.
Unbenommen hiervon bleibt jedoch die spezifische Regelung des § 6 b BDSG – Beobachtung öffentlich zugänglicher Räum mit optisch-elektronischen Einrichtungen.

Zusätzlich hat die Differenzierung zwischen dem Datenschutz im nicht-öffentlichen und dem Datenschutz im öffentlichen Bereich Einfluss darauf, welche Behörde dem Bürger beim Schutz seiner Daten zur Seite steht.
Über die Einhaltung der datenschutzrechtlichen Bestimmungen durch die öffentlichen Stellen des Landes Sachsen-Anhalt wacht der **Landesbeauftragte für den Datenschutz**. In jedem Bundesland existiert ein solcher Landesdatenschutzbeauftragter.

Die Überwachung des Umgangs in Sachsen-Anhalt tätiger nicht-öffentlicher Stellen mit personenbezogenen Daten obliegt demgegenüber der **Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich**. Diese Aufsichtsbehörden bestehen ebenfalls in allen Bundesländern.

## 1.2 Aufgaben einer Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich

Nach § 38 Abs. 1 Satz 1 BDSG kontrollieren die Aufsichtsbehörden die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln. Dies gestaltet sich im Wesentlichen über

- die Bearbeitung von Anfragen, Eingaben und Beschwerden,

- die Beanstandung von Datenschutzverstößen,
- die Überprüfung im Hinblick auf die Einhaltung des Datenschutzes,
- die Anordnung zur Beseitigung von Sicherheitsmängeln,
- die Führung des öffentlichen Registers der meldepflichtigen Unternehmen vor allem in Hinblick auf Auskunfteien, Adressenhandelsunternehmen sowie Markt- und Meinungsforschungsinstitute und
- die Durchführung von Bußgeldverfahren.

Die Aufsichtsbehörden können anlassbezogen, anlassfrei und aufgrund spezifischer gesetzlicher Aufgabenzuweisung tätig werden.

### 1.3 Zielstellung eines Tätigkeitsberichtes

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich sind seit der Novellierung des Bundesdatenschutzgesetzes im Mai 2001 durch § 38 Abs. 1 S. 6 BDSG verpflichtet, regelmäßig, spätestens alle zwei Jahre, über ihre Tätigkeit zu berichten. Mit dem Tätigkeitsbericht soll über die Aktivitäten und Prüfungen der Aufsichtsbehörde Aufschluss gegeben und damit die Öffentlichkeit über den Datenschutz informiert werden.

Die Zielstellung des Tätigkeitsberichtes erschöpft sich somit nicht darin, Rechenschaft über den zurückliegenden Zeitraum zu geben. Vielmehr soll der Bericht die interessierten und betroffenen Bürger informieren, wie sie ihr Recht auf informationelle Selbstbestimmung wirkungsvoll wahrnehmen können. Dieses Recht auf informationelle Selbstbestimmung ist Bestandteil des allgemeinen Persönlichkeitsrechts (Artikel 2 Absatz 1 i.V.m. Artikel 1 Absatz 1 Grundgesetz) und wird daher durch das Grundgesetz garantiert. Es schützt den Bürger gegen eine unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe von Daten aus seinem persönlichen Lebensbereich.

# 2. Das Landesverwaltungsamt Sachsen-Anhalt als Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich des Landes Sachsen-Anhalt

## 2.1 Allgemeines zum Landesverwaltungsamt Sachsen-Anhalt

Bereits der Beschluss der Landesregierung über die Bestimmung der zuständigen Aufsichtsbehörde des Landes Sachsen-Anhalt, welcher am 01. Oktober 2002 in Kraft trat, führte dazu, dass die Aufsicht über den Datenschutz im nicht-öffentlichen Bereich in Sachsen-Anhalt allein durch das Regierungspräsidium Halle wahrgenommen wurde. Zuvor waren die Regierungspräsidien Dessau, Magdeburg und Halle für ihr jeweiliges Territorium zuständig.

Zum 01.01.2004 entstand aus den Regierungspräsidien Halle, Dessau und Magdeburg sowie 22 weiteren Einzelbehörden das Landesverwaltungsamt Sachsen-Anhalt als zentrale Mittelbehörde des gesamten Landes. Mit Gründung des Landesverwaltungsamtes ging auch die Funktion der Aufsichtsbehörde auf dieses über. Intern obliegt die Wahrnehmung dieser Aufgabe dem Referat Justiziariat.

Sie erreichen die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich des Landes Sachsen-Anhalt unter folgender Anschrift:

*Landesverwaltungsamt Sachsen-Anhalt*
Referat Justiziariat (Referatsleiter Michael Wersdörfer)
An der Fliederwegkaserne 13
06130 Halle (Saale)

Telefonische oder schriftliche Anfragen können Sie an

Herrn Wersdörfer (Referatsleiter)
Email: Michael.Wersdörfer@lvwa.sachsen-anhalt.de
Telefon: 0345 514 3857

Frau Dönitz
Email: Anke.Doenitz@lvwa.sachsen-anhalt.de
Telefon: 0345 514 3925

Frau Damm
Email: Nicole.Damm@lvwa.sachsen-anhalt.de
Telefon: 0345 514 3775

richten.

Das Referat Justiziariat erreichen Sie auch unter der Fax-Nummer: 0345/514-3799.

## 2.2 Dieser Tätigkeitsbericht kurz und knapp

Dieser Tätigkeitsbericht ist bereits der 2. Tätigkeitsbericht der Aufsichtsbehörde des Landes Sachsen-Anhalt. Der 1. Tätigkeitsbericht wurde noch durch das ehemalige Regierungspräsidium Halle für den Berichtszeitraum vom 23.05.2001 bis 31.05.2003 erstellt. Er ist nach wie vor auf der Homepage des Landesverwaltungsamtes Sachsen-Anhalt (www.landesverwaltungsamt.sachsen-anhalt.de) einsehbar. Sie erreichen den Bericht, indem sie im Frame links oben unter *Organisation* den Bereich *Zentraler Service* aufrufen und dann im fließenden Text auf *Justiziariat, Referat 106* klicken. Im dann angezeigten Text stellt sich das Referat Justiziariat vor. Der Tätigkeitsbericht wird im Abschnitt Datenschutz erwähnt und ist entsprechend verlinkt.

In diesem 2. Tätigkeitsbericht wird die Arbeit der Aufsichtsbehörde während der vergangenen 2 Jahre im Zeitraum vom 01.06.2003 bis 31.05.2005 dargestellt. Damit ist auch das Wirken des Regierungspräsidiums Halle bis zum 31.12.2003 umfasst. Da sich zum 01.01.2004 die personelle Untersetzung der Aufsichtsbehörde des Landes Sachsen-Anhalt komplett veränderte, soll auf den Zeitraum bis zum 31.12.2003 jedoch nur bedingt eingegangen werden.
Mit diesem Tätigkeitsbericht soll nicht allein Aufschluss über unsere Tätigkeit gegeben werden. Anliegen ist vielmehr die Sensibilisierung der Bürger Sachsen-Anhalts für den Datenschutz und die Information über wichtige datenschutzrechtliche Fragen. Aus diesem Grund gibt der Bericht zunächst einen Überblick über die in den eingegangenen Anfragen und Beschwerden angesprochenen Themen. Nachfolgend werden dann zahlreiche im Berichtszeitraum behandelte Probleme vertiefend erörtert. Insgesamt will dieser Bericht über die Rechtslage im Allgemeinen aufklären und das Bewusstsein der verantwortlichen Stellen für den Datenschutz schärfen.

## 2.3 Überblick über die Tätigkeit als Aufsichtsbehörde

Seit dem 01.01.2004 nahm den größten Raum der täglichen Arbeit der Aufsichtsbehörde die Bearbeitung von Anfragen, Eingaben und Beschwerden von Bürgern, Unternehmen und anderen Personenvereinigungen ein.

Anfragen werden je nachdem, wie ausführlich der zugrundeliegende Sachverhalt vom Anfragenden mitgeteilt wird, möglichst konkret und fallbezogen beantwortet. Im Übrigen erstellt die

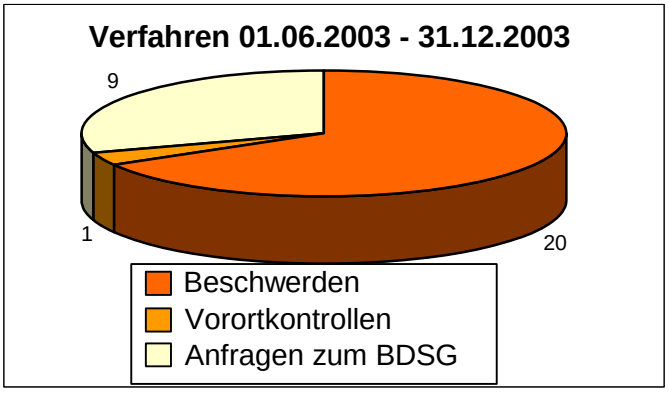
Aufsichtsbehörde anhand der vorgelegten Informationen unter Erläuterung der Rechtslage ein allgemeineres Antwortschreiben.
Bei Eingaben und Beschwerden wird der bekannt gewordene Sachverhalt der Partei, welcher der Verstoß gegen datenschutzrechtliche Bestimmungen vorgeworfen wird, schriftlich unter Mitteilung der Rechtslage dargelegt. Anschließend wird ihr zur korrekten Aufklärung des Sachverhaltes die Möglichkeit zur Stellungnahme eröffnet. Stellt sich bei der nachfolgenden Prüfung heraus, dass ein datenschutzrechtlicher Verstoß vorliegt, wirkt die Aufsichtsbehörde - sofern dies noch möglich ist - auf die Beseitigung hin und erteilt dem Beschwerdegegner zumindest entsprechende rechtliche Hinweise. Werden datenschutzrechtliche Bestimmungen nicht eingehalten, besteht für die Aufsichtsbehörde zudem die Möglichkeit Anordnungen zu treffen, Bußgeldverfahren durchzuführen oder gar Strafanzeige zu stellen. Nach Abschluss des Verfahrens teilt die Aufsichtsbehörde der beschwerdeführenden Partei das Ergebnis mit.

Sollten Sie also als Betroffener der Auffassung sein, dass Ihnen gegenüber datenschutzrechtliche Bestimmungen nicht eingehalten wurden, oder Zweifel daran haben, richten Sie eine entsprechende kurze Eingabe oder Beschwerde schriftlich ohne Beachtung von Formalitäten an das Landesverwaltungsamt. Sie können sich natürlich auch zunächst persönlich oder telefonisch beraten lassen oder sich anonym an die Aufsichtsbehörde wenden.
Darüber hinaus können Sie sich auch mit Anfragen zur Rechtslage im Bereich des Datenschutzes an die Aufsichtsbehörde des Landes Sachsen-Anhalt wenden.

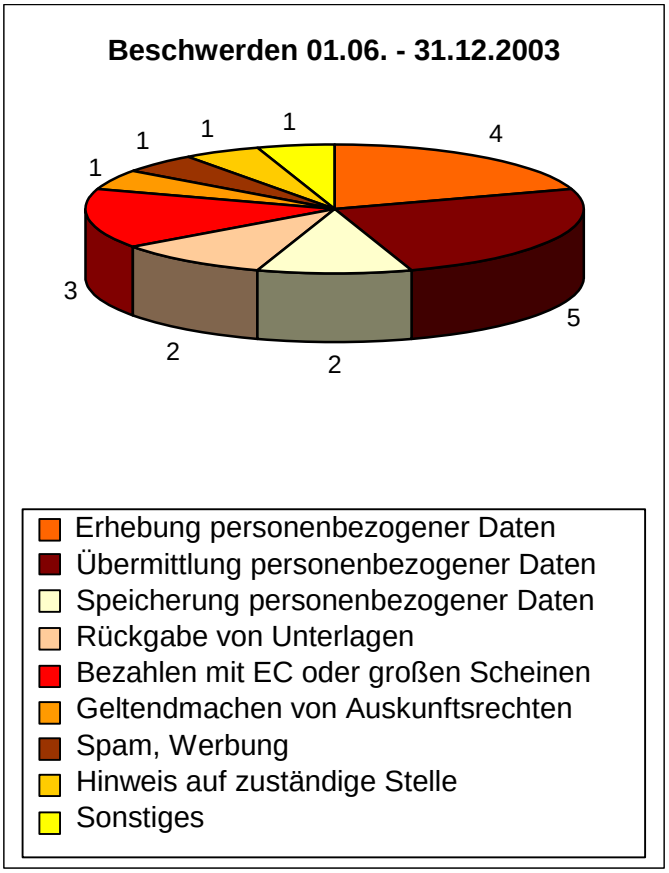
Die Anzahl und Art der in dem vom 2. Tätigkeitsbericht umfassten Zeitraum bearbeiteten Verfahren lässt sich den nachfolgenden Aufstellungen entnehmen.

**Zeitraum vom 01.06.2003 bis 31.12.2003**

| Verfahren im Datenschutz - Überblick 01.06.2003 - 31.12.2003 | |
|---|---|
| Beschwerden | 20 |
| Vorortkontrollen | 1 |
| Anfragen zum BDSG (u.a. zum Beauftragten für Datenschutz, Zulässigkeit von Warndateien, Mitarbeiterdatenschutz) | 9 |

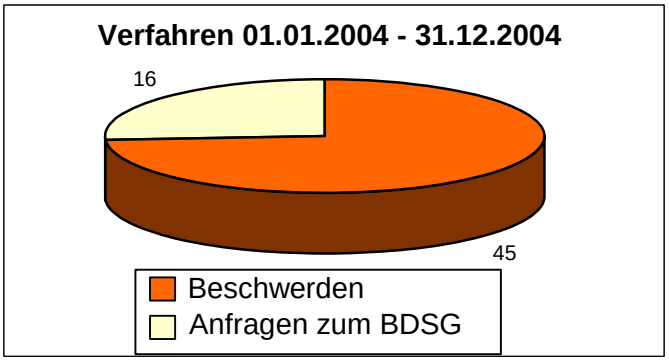


| Beschwerden im Datenschutz - Überblick 01.06.2003 - 31.12.2003 | |
|---|---|
| Erhebung personenbezogener Daten (auch biometrischer) | 4 |
| Prüfung der Zulässigkeit der Übermittlung personenbezogener Daten | 5 |
| Prüfung der Zulässigkeit der Speicherung personenbezogener Daten | 2 |
| Rückgabe von Unterlagen | 2 |
| Datenerhebung bei Bezahlung mit EC oder großen Scheinen | 3 |
| Geltendmachung von Auskunftsrechten | 1 |
| Spam, Werbung | 1 |
| Hinweis auf zuständige Stelle und Abgabe | 1 |
| Sonstiges | 1 |

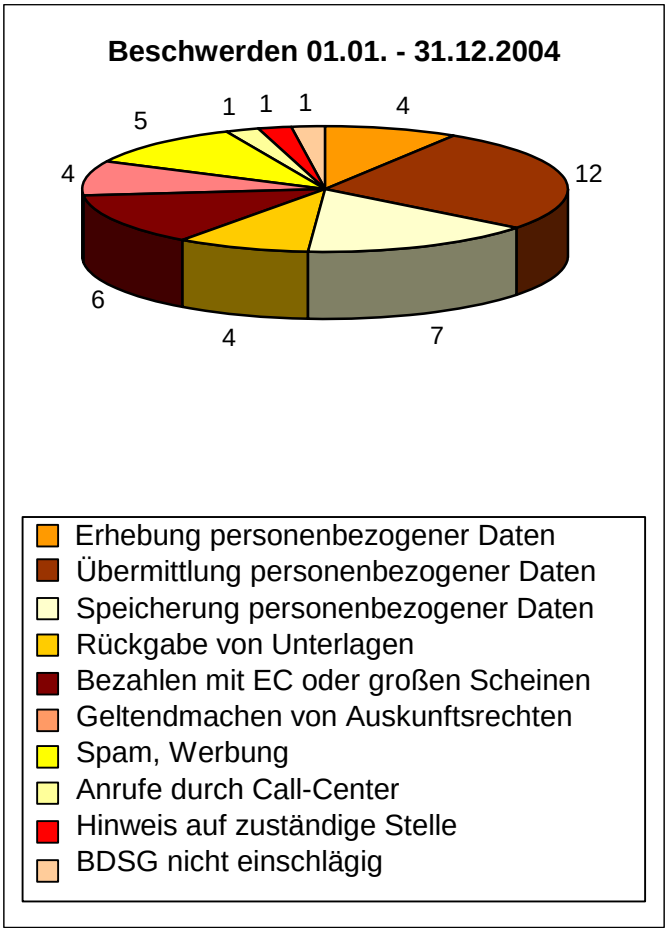



**Zeitraum 01.01.2004 bis 31.12.2004**

| Verfahren im Datenschutz - Überblick 01.01.2004 - 31.12.2004 | |
|---|---|
| Beschwerden | 45 |
| Anfragen zum BDSG (u.a. zum Beauftragten für Datenschutz, Zulässigkeit von Warndateien, Mitarbeiterdatenschutz) | 16 |

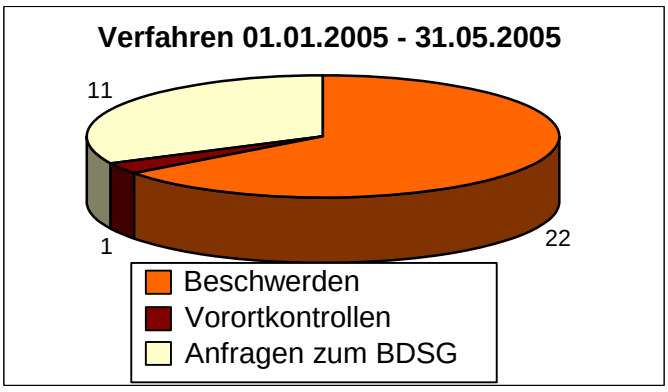


| Beschwerden im Datenschutz - Überblick 01.01.2004 - 31.12.2004 | |
|---|---|
| Erhebung personenbezogener Daten (auch biometrischer) | 4 |
| Prüfung der Zulässigkeit der Übermittlung personenbezogener Daten | 12 |
| Prüfung der Zulässigkeit der Speicherung personenbezogener Daten | 7 |
| Rückgabe von Unterlagen | 4 |
| Datenerhebung bei Bezahlung mit EC oder großen Scheinen | 6 |
| Geltendmachung von Auskunftsrechten | 4 |
| Spam, Werbung | 5 |
| Anrufe durch Call-Center | 1 |
| Hinweis auf zuständige Stelle und Abgabe | 1 |
| BDSG nicht einschlägig | 1 |

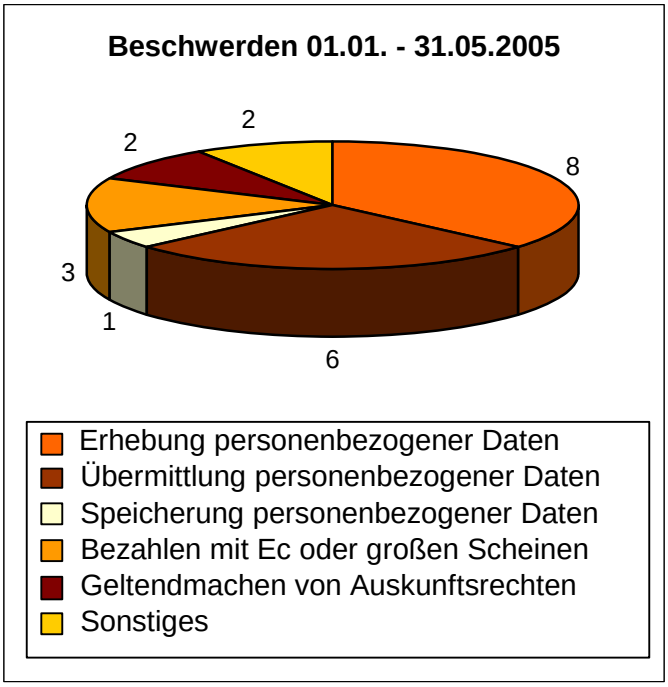



**Zeitraum 01.01.2005 bis 31.05.2005**

| Verfahren im Datenschutz - Überblick 01.01.2005 - 31.05.2005 | |
|---|---|
| Beschwerden | 22 |
| Vorortkontrollen | 1 |
| Anfragen zum BDSG (u.a. zum Beauftragten für Datenschutz, Zulässigkeit von Warndateien, Mitarbeiterdatenschutz) | 11 |



| Beschwerden im Datenschutz - Überblick 01.01.2005 - 31.5.2005 | |
|---|---|
| Erhebung personenbezogener Daten (auch biometrischer) | 8 |
| Prüfung der Zulässigkeit der Übermittlung personenbezogener Daten | 6 |
| Prüfung der Zulässigkeit der Speicherung personenbezogener Daten | 1 |
| Datenerhebung bei Bezahlung mit EC oder großen Scheinen | 3 |
| Geltendmachung von Auskunftsrechten | 2 |
| Sonstiges | 2 |



# 3. Das Bundesdatenschutzgesetz (BDSG) und seine wichtigsten Regelungen

## 3.1 Allgemeine Hinweise

Zweck des BDSG ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Das BDSG bindet die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch öffentliche und nicht öffentliche Stellen an feste Voraussetzungen. Es gilt in seiner aktuellen Fassung seit dem Inkrafttreten der BDSG-Novelle am 23. Mai 2001.
Die zum Verständnis des Gesetzes wichtigsten Begriffe werden in § 3 BDSG erläutert. Die allgemeinen für den Datenschutz im nicht-öffentlichen und öffentlichen Bereich gleichermaßen geltenden Bestimmungen sind in den §§ 1 bis 11 BDSG niedergelegt. So findet sich in § 4 die Rechtsgrundlage für die „Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung“, während in § 4d die „Meldepflicht“ und § 4f die Regelungen über den „Beauftragten für den Datenschutz“ normiert sind. Die §§ 12 – 26 BDSG betreffen die Datenverarbeitung der öffentlichen Stellen. Demgegenüber beinhalten die §§ 27 – 38a BDSG die für die Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen speziell anzuwendenden Vorschriften. Sondervorschriften sind im 4. Abschnitt (§§ 39 – 42 BDSG) enthalten und schließlich in den §§ 43 und 44 BDSG die Bußgeld- und Strafvorschriften.

## 3.2 Die Meldepflicht

Alle nicht-öffentlichen Stellen, die Verfahren automatisierter Verarbeitung durchführen, werden durch § 4d Abs. 1 BDSG verpflichtet, diese Verfahren vor deren Inbetriebnahme der zuständigen Aufsichtsbehörde zu melden. Automatisierte Verarbeitung in diesem Sinne ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen.

Diese Meldepflicht **entfällt**, wenn

1. die verantwortliche Stelle einen betrieblichen Datenschutzbeauftragten bestellt hat. (Bestimmte Stellen müssen immer einen Datenschutzbeauftragten bestellen (§ 4f Abs. 1

BDSG) und sind von der Meldepflicht befreit, sobald sie der Pflicht zur Bestellung eines Datenschutzbeauftragten nachgekommen sind ) *oder*

2. die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei höchstens vier Arbeitnehmer mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt (dann besteht auch keine Pflicht zur Bestellung eines Datenschutzbeauftragten) und entweder eine Einwilligung der Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.

Auch wenn ein Datenschutzbeauftragter bestellt ist, besteht die **Meldepflicht weiterhin**, wenn geschäftsmäßig personenbezogene Daten

- zum Zweck der Übermittlung (§ 29 BDSG, z.B. Auskunfteientätigkeit, Adresshandel) oder
- zum Zweck der anonymisierten Übermittlung (§ 30 BDSG, z.B. Markt- und Meinungsforschung)

gespeichert werden.

Welche Angaben gegenüber der zuständigen Aufsichtsbehörde zu machen sind, ist in § 4e BDSG geregelt. Die Aufsichtsbehörde führt ein Register der nach § 4 d BDSG meldepflichtigen automatisierten Verarbeitungen, in welchem die Angaben nach § 4e Satz 1 BDSG erfasst werden. Dieses Register kann von jedem eingesehen werden.

Nach § 43 Abs. 1 Nr. 1 BDSG handelt ordnungswidrig, wer vorsätzlich oder fahrlässig entgegen § 4d Abs. 1 BDSG, auch in Verbindung mit § 4e Satz 2 BDSG, eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht. Eine solche Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfundzwanzigtausend Euro geahndet werden.

### 3.3 Der Beauftragte für den Datenschutz

Die §§ 4f und 4g BDSG benennen die wichtigsten Regelungen in Bezug auf den Beauftragten für den Datenschutz, der häufig auch als betrieblicher Datenschutzbeauftragter bezeichnet wird. Sie definieren sowohl die Voraussetzungen, unter denen ein solcher Beauftragter bestellt werden muss, als auch die Rechte und Pflichten, die dem Beauftragten obliegen.

Eine Verpflichtung, einen Datenschutzbeauftragten zu bestellen, besteht in den verschiedensten Fällen.

So ist er *unabhängig* von der Zahl der Arbeitnehmer, die mit der Datenverarbeitung beschäftigt sind, zu bestellen in:

- Firmen, die personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung (z.B. Adresshandel, Auskunfteien etc.) erheben, verarbeiten oder nutzen,
- Firmen, die personenbezogene Daten geschäftsmäßig zum Zweck der anonymisierten Übermittlung (z.B. Markt- und Meinungsforschung) erheben, verarbeiten oder nutzen *und*
- Firmen, in denen automatisierte Verarbeitungen erfolgen, die nach § 4d Abs. 5 BDSG der Vorabkontrolle unterliegen.

Eine Verpflichtung zur Bestellung eines Datenschutzbeauftragten besteht *in Abhängigkeit* von der Zahl der Arbeitnehmer, die mit der Datenverarbeitung beschäftigt sind, wenn:

- mindestens fünf Arbeitnehmer mit der automatisierten Verarbeitung, Nutzung oder Erhebung personenbezogener Daten beschäftigt sind *oder*
- in der Regel mindestens zwanzig Personen mit der Verarbeitung, Nutzung oder Erhebung personenbezogener Daten auf andere Weise (manuelle Verarbeitung) beschäftigt sind.

Ausnahmen von der Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz gibt es nur dann, wenn der Anteil von Datenverarbeitung an der Aufgabenstellung eines Beschäftigten einen völlig untergeordneten Teil ausmacht. Die vereinzelte Erstellung von Schreiben mit personenbezogenen Daten genügt beispielsweise nicht, um die damit betraute Person der Zahl der mit Datenverarbeitung Beschäftigten hinzuzurechnen.

Vielfach wurde in der Presse publiziert, dass mit dem Ablaufen der Übergangsfrist zum 23. Mai 2004 (ausgewiesen in § 45 BDSG) zahlreiche Unternehmen nunmehr verpflichtet seien, einen Beauftragten für den Datenschutz zu bestellen, und nachfolgend verstärkte Kontrollen stattfinden würden. Nach § 45 Satz 1 BDSG waren Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten, „die am 23. Mai 2001 bereits begonnen haben“, innerhalb von drei Jahren nach diesem Zeitpunkt mit den Vorschriften des BDSG in Übereinstimmung zu bringen.
Da jedoch bereits vor der BDSG-Novelle die Notwendigkeit der Bestellung eines Datenschutzbeauftragten in Abhängigkeit von der Anzahl der beschäftigten Personen inhaltsgleich geregelt war, dürfte sich für viele Unternehmen nichts verändert haben. Sie unterlagen be-

reits vor dem 23. Mai 2001 der Verpflichtung, einen Beauftragten für den Datenschutz zu bestellen, so dass die Übergangsfrist insoweit nicht zum Tragen kam.
Neu geregelt wurde lediglich, dass nicht-öffentliche Stellen, die automatisierte Verarbeitungen vornehmen, welche einer Vorabkontrolle unterliegen oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung oder der anonymisierten Übermittlung erheben, verarbeiten oder nutzen *unabhängig von der Anzahl der Beschäftigten* einen Beauftragten für den Datenschutz bestellen müssen.

### 3.4 Rechte der Betroffenen

Die Rechte der Betroffenen sind insbesondere in den §§ 33 – 35 BDSG geregelt. § 33 BDSG legt fest, wann der Betroffene benachrichtigt werden muss, § 34 BDSG spricht ihm einen Anspruch auf Auskunft zu. § 35 BDSG regelt die Berichtigung, Löschung und Sperrung von Daten.

Die Transparenz der Datenverarbeitung ist zur Gewährleistung des Rechts auf informationelle Selbstbestimmung unverzichtbar. Jeder hat ein Recht auf Offenlegung seiner Daten, was ihn wiederum in die Lage versetzt, ggf. Korrektur-, Löschungs- oder Schadenersatzansprüche geltend zu machen.
Der Anspruch auf Auskunft ist als unabdingbares Recht in § 6 BDSG festgeschrieben. Dem Betroffenen ist Auskunft darüber zu erteilen, ob und welche Daten zu seiner Person gespeichert sind. Um dieses Recht ausüben zu können, muss der Betroffene zunächst einmal wissen, wer Daten über ihn speichert. Die Benachrichtigung soll sicherstellen, dass Betroffene von der über ihre Person erfolgten Datenerhebung und vom Verantwortlichen Kenntnis erhalten.
Die Benachrichtigungspflicht besteht für jede nicht-öffentliche Stelle und kommt vor allem dann zum Tragen, wenn Daten über die Betroffenen ohne deren Kenntnis verarbeitet werden. Inhalt sowie Art und Weise der Benachrichtigung sind ausdrücklich geregelt. § 33 Abs. 2 BDSG kennt jedoch auch einzelne Ausnahmen von der Benachrichtigungspflicht.

Die Auskunft versetzt den Betroffenen in die Lage, weitere Rechte bei unzulässiger Datenverarbeitung geltend zu machen. Die Erteilung der Auskunft setzt ein Auskunftsersuchen voraus. Für ein solches ist keine bestimmte Form vorgeschrieben, jedoch sollte der Auskunftsanspruch schriftlich geltend gemacht werden, da viele Stellen auf mündliche Auskunftsersuchen nicht reagieren werden. Das Auskunftsersuchen ist an die verantwortliche Stelle (d.h. jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, ver-

arbeitet oder nutzt oder dies durch andere im Auftrag übernehmen lässt) zu richten und sollte möglichst genau bezeichnen, worüber Auskunft erwünscht ist.
Nach § 34 Abs. 1 BDSG kann der Betroffene Auskunft verlangen über:

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft der Daten beziehen,
2. Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und
3. den Zweck der Speicherung.

In § 34 Abs. 4 BDSG sind die Fälle normiert, in denen keine Pflicht zur Auskunftserteilung besteht. Zudem können Stellen, die geschäftsmäßig personenbezogene Daten zum Zweck der Auskunftserteilung oder zum Zwecke der Übermittlung speichern, bei überwiegendem Interesse an der Wahrung des Geschäftsgeheimnisses die Auskunft über Herkunft und Empfänger der Daten verweigern.

Grundsätzlich ist eine Auskunft unentgeltlich. Bei schriftlichen Auskünften von Kreditauskunfteien und ähnlichen Einrichtungen, die gegenüber Dritten wirtschaftlich genutzt werden können, ist dies jedoch nicht der Fall. Allerdings darf das geforderte Entgelt nicht höher sein als die entstandenen direkt zurechenbaren Kosten. Wenn die Auskunft nötig ist, um zu ermitteln, ob Daten unrichtig oder unzulässig gespeichert sind, darf allerdings auch von diesen Unternehmen kein Entgelt verlangt werden.

Es besteht in der Regel ein Anspruch auf eine vollständige Auskunft, d.h. alle Angaben, bezüglich der nach dem Gesetz grundsätzlich eine Auskunftspflicht besteht, müssen mitgeteilt werden. Soweit die auskunftspflichtige Stelle aufgrund der gesetzlich vorgesehenen Ausnahmen nur teilweise Auskunft erteilt, muss sie auf die Unvollständigkeit der Auskunft ausdrücklich schriftlich hinweisen, damit für den Betroffenen die Möglichkeit besteht, eine Überprüfung zu verlangen. Im Allgemeinen ist die auskunftserteilende Stelle auch verpflichtet zu begründen, aufgrund welcher gesetzlichen Bestimmung und aufgrund welcher Tatsachen eine Auskunft über bestimmte Aspekte abgelehnt wird.

Bestehen Zweifel daran, ob die Auskunft korrekt erteilt worden ist oder wird die Auskunft nicht erteilt, überprüft die Aufsichtsbehörde des Landes Sachsen-Anhalt den Sachverhalt auf Ihren Wunsch. Dazu übersenden Sie dem Landesverwaltungsamt einfach den bisherigen Schriftwechsel in Kopie. Wir setzen uns mit der verantwortlichen Stelle in Verbindung. Sie erhalten nachfolgend in jedem Fall Bescheid, ob Ihre Rechte beachtet wurden. Es bleibt Ihnen unbenommen, Ihre Rechte zusätzlich auf gerichtlichem Wege geltend zu machen.

§ 35 BDSG stellt die Korrekturrechte der Betroffenen bei unrichtiger oder unzulässiger Datenverarbeitung dar. Er gibt dem Betroffenen die Möglichkeiten der Berichtigung, Löschung und Sperrung der Daten.

Jede Stelle ist verpflichtet, unrichtige Daten zu *berichtigen*. Dabei liegt es auch in der Hand des Betroffenen selbst, darauf hinzuweisen, dass Daten unrichtig oder überholt sind.
Eine *Löschung* der Daten kann jederzeit vorgenommen werden, außer es gibt Aufbewahrungsfristen oder es besteht Grund zu der Annahme, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Zusätzlich hat der Gesetzgeber in § 35 Abs. 2 Satz 2 BDSG bestimmte Fälle ausdrücklich aufgezählt, in denen die Daten zu löschen sind, also eine Verpflichtung zur Datenlöschung besteht.
Zu *sperren* sind personenbezogene Daten immer dann, wenn einer fälligen Löschung besondere Gründe entgegenstehen, etwa:

- gesetzlich, satzungsmäßig oder vertraglich festgelegte Aufbewahrungsfristen,
- schutzwürdige Interessen des Betroffenen oder
- ein unverhältnismäßig hoher Aufwand wegen der besonderen Art der Speicherung.

Ebenso sind personenbezogene Daten zu sperren, wenn der Betroffene ihre Richtigkeit bestreitet und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt. Gesperrte Daten dürfen sodann ohne Einwilligung des Betroffenen nur noch unter den sehr engen Voraussetzungen des § 35 Abs. 8 BDSG übermittelt oder genutzt werden.

Darüber hinaus ist in § 7 BDSG das Recht auf Schadenersatz normiert. Durch diese über die Haftung nach dem Bürgerlichen Gesetzbuch hinausgehende Verpflichtung zum Schadenersatz bei unrichtiger oder unzulässiger Erhebung, Verarbeitung oder Nutzung personenbezogener Daten verbessert das Gesetz den Schutz des Persönlichkeitsrechts – auch indem es auf diese Weise die datenverarbeitenden Stellen zu besonderer Sorgfalt beim Umgang mit personenbezogenen Daten anhält -. Schadenersatzansprüche sind jedoch auf dem Privatrechtsweg geltend zu machen, ihre Durchsetzung obliegt nicht der Aufsichtsbehörde.

# 4. Ausgewählte Themen aus Beschwerden und Anfragen

## 4.1 Erhebung und Speicherung personenbezogener Daten

Nach § 4 Abs. 1 BDSG sind die Erhebung, Verarbeitung (Speicherung, Veränderung, Übermittlung, Sperrung und Löschung) und Nutzung personenbezogener Daten nur zulässig, soweit das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Dabei ist eine Einwilligung nur unter Einhaltung der Voraussetzungen des § 4a BDSG wirksam.

Bei der Überprüfung der Zulässigkeit der Erhebung und Speicherung personenenbezogener Daten wird daher zunächst überprüft, ob dies aufgrund einer Einwilligung des Betroffenen zulässig erfolgte oder von einer anderen Rechtsvorschrift als dem Bundesdatenschutzgesetz erlaubt oder gar anordnet wurde. In den meisten der Aufsichtsbehörde zur Überprüfung übergebenen Sachverhalten, fehlt es sowohl an einer Einwilligung als auch an einer Rechtsgrundlage außerhalb des BDSG. Somit ist zu prüfen, ob sich die Zulässigkeit aus dem Bundesdatenschutzgesetz selbst ergibt. Normen, welche die Zulässigkeit der Datenerhebung und -speicherung regeln, sind § 28 BDSG „Datenerhebung, -verarbeitung und –nutzung für eigene Zwecke“ und § 29 BDSG „Geschäftsmäßige Datenerhebung und –speicherung zum Zweck der Übermittlung“.

### 4.1.1 Bezahlen mit ec-Karte im Lastschriftverfahren

Aus zahlreichen Beschwerden ergibt sich, dass beim täglichen Einkauf, der mit ec-Karte bezahlt wird, häufig zunächst ein Ausweisdokument vorzulegen ist und in vielen Fällen nachfolgend bestimmte Daten (darunter auch Personalausweisnummer und Geburtsdatum) durch die Kassierer/innen notiert werden.

Grundsätzlich sind Unternehmen, die den bargeldlosen Zahlungsverkehr akzeptieren, berechtigt, sich Ausweisdokumente vorlegen zu lassen. Einerseits dient ein solches Vorgehen dem Schutz des Kunden, da auf diese Weise geprüft werden kann, ob der berechtigte Karteninhaber die Karte zur Zahlung vorlegt.
Andererseits muss auch das Interesse des Unternehmens an einer reibungslosen Begleichung der eigenen Forderungen berücksichtigt werden, denn zwischen dem Erwerb der Ware durch den Kunden und dem Eingang des Geldes auf dem Unternehmenskonto gewährt der Unternehmer einen Warenkredit und trägt somit das Risiko eines Zahlungsausfalles.

Aus diesem Grunde ist es den Unternehmen auch erlaubt, Name und Anschrift des Kunden auf dem Lastschriftbeleg (nicht jedoch auf dem Duplikat des Kassenbons, um eine Verknüpfung der Adressdaten mit denen der erworbenen Ware zu verhindern) zu notieren. Diese Erhebung und Speicherung der Daten ist nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG im Rahmen der Zweckbestimmung des Kauf- und Warenkreditvertrages zulässig. So wird dem Unternehmen beim Scheitern der ec-Zahlung eine spätere Inanspruchnahme des Kunden ermöglicht.

Um jedoch den damit verbundenen Unannehmlichkeiten entgegen zu wirken, besteht für Kunden stets die Möglichkeit, die Preisgabe der Identität z.B. durch Barzahlung zu vermeiden. Zivilrechtlich ist die Barzahlung der gesetzlich vorgesehene Weg zur Begleichung einer Geldforderung und andere Zahlungsarten stellen nur Leistungen erfüllungshalber dar (§ 364 Abs. 2 BGB). Entsprechend wird der Kunde auch nicht unangemessen unter Druck gesetzt werden.

Um aber die Alternative der Bargeldzahlung nutzen zu können, müssen die Kunden zunächst wissen, dass im Falle einer Zahlung mit ec-Karte Adressdaten erhoben werden. Demzufolge sollte ein Unternehmen **darauf hinweisen**, dass im Lastschriftverfahren die Erfassung von Name und Anschrift ab einem bestimmten Warenwert erfolgt. Ohne entsprechendes Wissen der Kunden besteht sonst die Gefahr, dass diese nicht genügend Bargeld mit sich führen, um durch Barzahlung der Datenerhebung zu entgehen. Die Bestimmung des Warenwertes hat sorgfältig zu erfolgen, denn die geschilderte Vorgehensweise ist nicht in jedem Fall erforderlich. Bei einem unangemessen niedrig angesetzten Mindestzahlungswert wäre die Erhebung der Adressdaten damit ggf. nach dem Bundesdatenschutzgesetz unzulässig.
Insgesamt ist festzustellen, dass es erlaubt ist, ab einem gewissen Warenwert Name und Adresse des Kunden auf dem Transaktionsbeleg zu notieren. Das Notieren von personenbezogenen Daten, die über Name und Anschrift hinausgehen, so z.B die Erfassung der Personalausweisnummer und des Geburtsdatums ist demgegenüber nicht erforderlich. Eine solche Erhebung wäre ebenso wie die nachfolgende Speicherung der Daten unzulässig. Das hat aufgrund der Regelung des § 35 Abs. 2 S. 2 Nr. 1 BDSG zur Folge, dass diese personenbezogenen Daten zu löschen sind.

Des Weiteren ist der Zahlungsverkehr in der Regel nach sechs Wochen abgewickelt. Die beim ec-Kartenzahlungsverfahren erhobenen Daten sind also spätestens nach drei Monaten zu vernichten, sofern die Gutschrift eingelöst wurde. Eine darüber hinausgehende Speiche-

rung für die auf dem Zahlungsbeleg erhobenen Daten ist rechtswidrig, wenn der Zahlungsvorgang abgeschlossen ist (§ 35 Abs. 2 S. 2 Nr. 3 BDSG).

Die meisten der von der Aufsichtsbehörde angeschriebenen verantwortlichen Stellen passen ihre Verfahrensweise der erläuterten Rechtslage an, so dass die Vorgänge aus datenschutzrechtlicher Sicht nicht weiter betrachtet werden. Allerdings gibt es inzwischen auch Verfahren, in denen die Unternehmen zwar angeben, sich rechtskonform zu verhalten, nach Aussagen von Betroffenen jedoch weiterhin gegen datenschutzrechtliche Bestimmungen verstoßen. In diesen Fällen dauern die Ermittlungen derzeit noch an.

### 4.1.2 Herausgabe des Verkaufserlöses beim Verkauf von Schrott

Ein weiteres Verfahren betraf die Anfrage eines Bürgers, von dem, nachdem er Schrott aus eigenem Aufkommen bei einer Firma abgeliefert hatte, vor Auszahlung seiner Gutschrift eine Kopie seines Personalausweises verlangt wurde. Da er diese verweigerte, wurde ihm auch die Gutschrift nicht ausgezahlt.
Die Aufsichtsbehörde für den Datenschutz schrieb die Firma an und bat unter Erläuterung der Voraussetzungen des § 28 Abs. 1 BDSG um eine Stellungnahme zur Zulässigkeit der Erhebung und Speicherung der personenbezogenen Daten des Betroffenen.

Da die Firma sich nicht innerhalb der gesetzten Frist äußerte, wurde sie unter Hinweis auf die Bußgeldvorschrift des § 43 Abs. 1 Nr. 10 BDSG erneut um eine Auskunft gebeten.

In der nachfolgenden Stellungnahme führte das Unternehmen aus, aufgrund gesetzlicher Vorschriften (so der Abgabenordnung und des Geldwäschegesetzes) verpflichtet zu sein, bei der Bilanzierung von Geldauszahlungen die Zahlungsempfänger zu benennen, da andernfalls eine steuerliche Berücksichtigung dieser Geldabgänge nicht erfolge. Deshalb bestünde ein berechtigtes Interesse daran, bei Barauszahlungen Kopien von den Personalausweisen zu fertigen.

In einer neuerlichen Stellungnahme wurde der Firma mitgeteilt, dass ihr durchaus ein berechtigtes Interesse zuzuerkennen ist. Allerdings sei die Verfahrensweise des Kopierens des Personalausweises zur Wahrung dieses berechtigten Interesses nicht erforderlich.
Die Erforderlichkeit ist dann zu bejahen, wenn die berechtigten Interessen auf andere Weise nicht bzw. nicht angemessen gewahrt werden können. Zur Erfüllung der gesetzlich vorgesehenen Dokumentationspflichten über Zahlungsempfänger sind allein Name und Anschrift des Schrotteinlieferers erforderlich, nicht jedoch die übrigen aus einem Ausweisdokument er-

sichtlichen Daten (Passbild, Personalausweisnummer etc.). Entsprechend wurde die Firma informiert, dass die dargestellte Praxis nicht zulässig ist.

Daraufhin legte die Firma ausführlich dar, dass die Kopie des Personalausweises allein bei Einwilligung des Betroffenen erstellt werde. Der aktuelle Fall sei ein bedauerlicher Einzelfall, bei dem eine neue Mitarbeiterin die internen Kassenrichtlinien missverstanden und die Anweisung zur Ausweiskopie als in jedem Fall bindend interpretiert habe.
Die Auszahlung der Gutschrift an den Betroffenen wurde kurzfristig angewiesen.

Diese Verfahrensweise der Firma war nicht mehr zu beanstanden, da eine Kopie des Personalausweises nur bei Einwilligung des Betroffenen gefertigt wird und dies zur Zulässigkeit der Datenerhebung und -speicherung führt. Für die Fälle, in denen keine Einwilligung erteilt wird, dürfen jedoch lediglich Name und Anschrift des Schrotteinlieferers notiert werden. Diese Daten sind erforderlich, um das berechtigte Interesse, Auszahlungen als Betriebsausgaben gegenüber dem Finanzamt in Ansatz bringen zu können, zu wahren. Entsprechendes wurde dem Betroffenen mitgeteilt, der nachfolgend bestätigte, dass die Gutschrift ausbezahlt wurde.

### 4.1.3 Erhalt einer Einfahrtserlaubnis auf ein Betriebsgelände

Dieser Sachverhalt war bereits Gegenstand des 1. Tätigkeitsberichtes und wurde aufgrund einer erneuten Beschwerde nochmals überprüft. Ein Lastkraftwagenfahrer, der für seine Spedition vom Betriebsgelände eines Gewerbebetriebes Ladung aufnehmen sollte, durfte erst in das Gelände einfahren, nachdem er seinen Personalausweis vom Werkschutz ablichten ließ.

Der Firma wurde erläutert, dass sich eine Zulässigkeit der Datenerhebung und -speicherung allein aus § 28 Abs. 1 Nr. 2 BDSG ergeben könne, die Aufsichtsbehörde jedoch Zweifel an der Erforderlichkeit der Datenerhebung durch Kopieren des Personalausweises habe. Das Unternehmen erhielt Gelegenheit zur Stellungnahme mit der Bitte, zum berechtigten Interesse an der Datenerhebung und -speicherung und zur Erforderlichkeit vorzutragen.

Daraufhin teilte die Firma mit, dass es in der vergangenen Zeit zu zahlreichen Versuchen gekommen sei, die werthaltigen Produkte des Unternehmens zu entwenden. Daher sei es notwendig, die Identität des jeweils die Ware in Empfang nehmenden LKW-Fahrers zu kennen, um den unzulässigen Zugriffen auf die Produkte entgegenzuwirken. Entsprechendes habe das Unternehmen bereits mit dem Regierungspräsidium Halle erörtert und im Rahmen

einer Vorortbegehung am 28.06.2001 dokumentiert. Ergebnis dieses Treffens sei die Erarbeitung eines Informationsblattes gewesen, dass vor der Straßenwaage der Firma deutlich ausgehängt sei und von jedem LKW-Fahrer eingesehen werden könne. Es wurde schließlich mitgeteilt, dass jeder LKW-Fahrer das Recht habe, die Anfertigung von Kopien des Personalausweises zu untersagen. Dies sei jedoch mit der Konsequenz verbunden, dass dem Fahrer die Einfahrt auf das Betriebsgelände untersagt sei. Entsprechend habe man die Kopie des Personalausweises des Betroffenen vernichtet und veranlasst, dass er das Betriebsgelände nicht mehr betreten bzw. befahren kann.

Nach Prüfung des Protokolls der benannten Vor-Ort-Kontrolle ergab sich, dass auch dieses das Kopieren von Personalausweisdokumenten und das Speichern der entsprechenden personenbezogenen Daten gemäß § 4 Abs. 1 BDSG nur dann für zulässig erachtet, wenn der Betroffene wirksam eingewilligt hat. Zudem muss die Einwilligung auf der freien Entscheidung des Betroffenen beruhen.
Daher wurde die Firma informiert, dass sich die Erlaubnis zum Kopieren des Personalausweisdokuments weder aus einer speziellen Rechtsvorschrift noch aus dem BDSG selbst ergibt. Auch § 28 Abs. 1 Nr. 2 BDSG, wonach das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung für die Erfüllung eigener Geschäftszwecke zulässig ist, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, war nicht heranzuziehen. Zwar war der Firma ein berechtigtes Interesse, in dem Bemühen Straftaten zu verhindern bzw. die auf das Betriebsgelände eintretenden Personen zu kennen, anzuerkennen. Jedoch ist die Erhebung von Daten durch das Kopieren des Personalausweises nicht erforderlich, um das berechtigte Interesse zu wahren. Erforderlichkeit ist gegeben, wenn das berechtigte Interesse auf andere Weise nicht bzw. nicht angemessen gewahrt werden kann. Es wurde auf in der Praxis bewährte Verfahrensweisen hingewiesen, die weniger in das Persönlichkeitsrecht des Betroffenen eingreifen.

Auch die seitens der Kraftfahrer erteilten Einwilligungen konnten nicht zur Zulässigkeit der Datenerhebung durch Kopieren der Ausweise führen. Nach § 4a Abs. 1 BDSG ist die Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Aber gerade das Kriterium der Freiwilligkeit konnte bei der geschilderten Verfahrensweise nicht gewährleistet werden. Dem Betroffenen blieb nur die Wahl, entweder in das Kopieren des Personalausweises einzuwilligen oder keinen Zutritt zum Betriebsgelände zu erhalten und so den Arbeitsauftrag nicht erledigen zu können. Damit wurde die Einwilligung unter Ausnutzung einer wirtschaftlichen Machtposition abgenötigt.

Aufgrund dieser Ausführungen überprüfte die Firma ihre Verfahrensweise erneut und erkannte an, dass jeder Fahrer ohne nachteilige Folgen das Anfertigen von Kopien verweigern kann. Geschieht dies, muss er ein Dokument ausfüllen, in dem nur die erforderlichen Daten erhoben und gespeichert werden.
Gleichzeitig wurde um die Überprüfung eines erarbeiteten Informationsaushanges gebeten. Im Ergebnis wurde festgestellt, dass der Aushang auf den Zweck der Datenerhebung und den Umgang mit den Daten hinweist. Auch beleuchtet er die Folgen der Verweigerung einer entsprechenden Einwilligung. Die Aufsichtsbehörde empfahl lediglich, wichtige Textpassagen gut erkennbar hervorzuheben und nicht allein darauf zu vertrauen, dass die Fahrer den an der Straßenwaage angebrachten Aushang zur Kenntnis nehmen, sondern ggf. erstmals ankommende Fahrer darauf hinzuweisen.

Dem betroffenen Fahrer wurde das Ergebnis der Überprüfung mitgeteilt.

### 4.1.4 Biometrische Daten für eigene Zwecke

Eine Umschülerin teilte mit, dass in dem Bildungszentrum den Schülervertretern in einer Versammlung durch die Schulleitung/Geschäftsleitung mitgeteilt wurde, man werde einen Daumenabdruckscanner in der Schule installieren, um die Anwesenheit der Schüler und Lehrer im Objekt zu überprüfen. Die Einführung eines solchen Scanners wurde damit begründet, dass dies ein weniger aufwandsintensiver Anwesenheitsnachweis als das manuelle Erfassen der Anwesenheit gegenüber der Agentur für Arbeit sei.

Daraufhin informierte die Aufsichtsbehörde das Bildungszentrum, unter welchen Voraussetzungen personenbezogene Daten erhoben und gespeichert werden dürfen. Die schulische Einrichtung erhielt Gelegenheit, sich zu dem dargestellten Sachverhalt zu äußern und darzulegen, warum die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten zulässig sei.
Inzwischen anwaltlich vertreten teilte der Bildungsträger mit, dass er zu einer vollständigen und lückenlosen Anwesenheitskontrolle verpflichtet sei, da andernfalls die aus dem öffentlichen Haushalt zur Verfügung gestellten Mittel nicht ausgereicht oder erhaltene Mittel zurückgefordert würden. Aufgrund der steigenden Kosten im Verwaltungsbereich sei eine Rationalisierung notwendig. Die Anschaffung des geplanten Daumenabdruckerfassungssystems sei wirtschaftlich effizienter als die personalintensive mechanische Kontrolle von Anwesenheitslisten. Die Anwesenheitskontrolle über andere Erfassungssysteme (Chipcarten u.ä.) sei wegen der Missbrauchgefahr nicht zuverlässig genug. Im Ausbildungsbereich müsse jedoch ein

stabiles Niveau gewährleistet werden. Entsprechend seien die Voraussetzungen nach § 28 Abs. 1 Nr. 1 BDSG erfüllt, da die beabsichtigte Datenerhebung der Zweckbestimmung des mit dem jeweiligen Umschüler und der Bundesagentur für Arbeit geschlossenen Vertragsverhältnisses diene. Abschließend wurde gebeten, die Zulässigkeit der geplanten Maßnahme zu bescheinigen.

Der beabsichtigten Anwesenheitskontrolle durch Erfassung biometrischer Daten wurde seitens der Aufsichtsbehörde die Zulässigkeit versagt. Dem Bildungsträger wurde dargelegt, dass § 28 Abs. 1 Nr. 1 BDSG diese erstrebte Erfassung biometrischer Daten nicht deckt. Zwischen dem Bildungsträger und den Betroffenen besteht zwar ein Bildungsverhältnis, welches den Bildungsträger verpflichtet, die Umschüler auf angemessenem Bildungsniveau zu dem entsprechenden Beruf umzuschulen. Zweckbestimmung des Verhältnisses sei jedoch nicht, die Anwesenheit der Umschüler zu kontrollieren. Die Pflicht zur Anwesenheitskontrolle resultiert allein aus dem Verhältnis zwischen dem Bildungsträger und der Agentur für Arbeit und wirkt somit nicht auf die Betroffenen. Auch verdeutlichte die Aufsichtsbehörde, dass die vorgetragenen Wirtschaftlichkeitsaspekte keine berechtigten Interessen des Bildungsträgers bewirken können. Das Vorhaben der Erfassung biometrischer Daten wurde mit Blick auf den dahinterstehenden Zweck als nicht verhältnismäßig eingeschätzt, so dass sich die Zulässigkeit auch aus keiner anderen Regelung des Bundesdatenschutzgesetzes ergab. Aus diesen Gründen wurde die Zulässigkeit der beabsichtigten Maßnahme verneint und der Bildungsträger auf die Bußgeldvorschriften des § 43 BDSG hingewiesen.

Die betroffenen Umschüler wurden über die Versagung in Kenntnis gesetzt und gebeten, im Falle der verbotswidrigen Einführung des Daumenabdruckscanners die Aufsichtsbehörde zu informieren.

### 4.1.5 Bewerbungsunterlagen

Zahlreiche Personen wandten sich an die Aufsichtsbehörde des Landes Sachsen-Anhalt, da ihnen trotz mehrfacher Bitten ihre Bewerbungsunterlagen nicht zurückgegeben wurden.

Den säumigen Betrieben wurde dargetan, dass die Bewerbungsunterlagen Eigentum der Bewerber sind und bleiben, weshalb eine Firma verpflichtet ist, die Unterlagen sorgfältig aufzubewahren und vertraulich zu behandeln. Wenn die Unterlagen nicht mehr benötigt werden, müssen die Dokumente der nicht berücksichtigten Bewerber zurückgegeben und alle Kopien vernichtet werden. Zurückbehalten darf die Firma einzig die Unterlagen, die ihr gehören, wie

Bewerbungsschreiben, Personalfragebögen, graphologische Gutachten und Referenzauskünfte.
Sofern eine Rücksendung der Bewerbungsunterlagen aufgrund der hohen Bewerberzahlen nicht in Frage kommt, sollten die Bewerber schon im Zeitpunkt der Stellenausschreibung darauf hingewiesen werden, dass eine Rücksendung der Unterlagen nur im Falle der Beifügung von Rückporto erfolgt. Nicht zurück zu sendende Unterlagen sind, sobald sie nicht mehr benötigt werden, unverzüglich zu vernichten.

Nur mit der Zustimmung der Bewerber dürfen Unterlagen für eine bestimmte, im Voraus festgelegte Dauer aufbewahrt werden, wenn anzunehmen ist, dass sie demnächst wieder gebraucht werden.
Die im Rahmen des Bewerbungsverfahrens erhobenen personenbezogenen Daten sind somit nach § 35 Abs. 2 Nr. 3 BDSG zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Die Löschung kann über die Vernichtung der Unterlagen oder die Rückgabe dieser erfolgen.

Alle angeschriebenen Unternehmen haben die Bewerbungsunterlagen den Betroffenen ohne weitere Probleme übersandt. Lediglich in einem Verfahren sind die Unterlagen auf dem Postweg verloren gegangen. Die verantwortliche Stelle hatte hier jedoch nachgewiesen, die Unterlagen der Post übergeben zu haben.

## 4.2 Übermittlung personenbezogener Daten

### 4.2.1 Innerhalb eines Unternehmens

In diesem Fall meldete sich eine Bürgerin, die von einer Unternehmensgruppe unverlangt ein Reisemagazin erhalten hatte. Da sie die Zeitschrift nicht bestellt hatte, reagierte sie nicht auf deren Zusendung. Mit der Lieferung des 3. Exemplares erhielt sie jedoch eine Zahlungserinnerung, die sich auf ein angebliches Abonnement bezog. Ein solches hatte sie jedoch nach eigenen Ausführungen nicht abgeschlossen. Sie wandte sich daraufhin selbst an das Unternehmen. Gleichzeitig übergab sie den Vorgang dem Landesverwaltungsamt Sachsen-Anhalt zur Überprüfung aus datenschutzrechtlicher Sicht.

Die Aufsichtsbehörde verdeutlichte in ihrem an das Unternehmen gerichteten Anschreiben, dass infolge der Beschaffung der Adressdaten der Beschwerdeführerin Daten erhoben, gespeichert und nachfolgend auch verwendet wurden und somit in jedem Fall eine Verarbei-

tung personenbezogener Daten stattgefunden hat. Ohne Mitwirkung der Betroffenen dürfen diese nach § 4 Abs. 2 BDSG nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
2. a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder
   b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde

und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt sind.

Darüber hinaus wurde dargestellt, dass sich aufgrund der vermutlichen Erfüllung eigener Geschäftszwecke die Zulässigkeit der Datenerhebung, -speicherung und -nutzung aufgrund der fehlenden Einwilligung und der Unanwendbarkeit anderer Rechtsvorschriften allein aus § 28 BDSG ergeben könne. Da jedoch zum damaligen Zeitpunkt nicht ersichtlich war, woher die personenbezogenen Daten stammten, wurde das Unternehmen um eine entsprechende Stellungnahme gebeten.

Der betriebliche Datenschutzbeauftragte legte dar, dass das Unternehmen eine von zahlreichen Tochtergesellschaften sei. Als solche nutze es die personenbezogenen Daten der bei der Muttergesellschaft gemeldeten Mitglieder, um diesen eigene qualifizierte Angebote zu unterbreiten. Dies sei aufgrund der §§ 28 Abs. 1 Nr. 1 und 28 Abs. 3 Nr. 3 BDSG zulässig und daher nicht zu beanstanden. Ein Werbewiderspruch der betroffenen Bürgerin habe dem Unternehmen bislang nicht vorgelegen, sei jedoch nunmehr aufgrund ihrer Ausführungen vermerkt worden. Dies bedeute, dass künftig keine ihrer personenbezogenen Daten zum Zwecke der Werbung innerhalb der Unternehmensgruppe übermittelt werden.

Nachfolgend teilte die Betroffene mit, dass sich das Unternehmen vermutlich Dank des Eingreifens der Aufsichtsbehörde mit ihr in Verbindung gesetzt habe und nunmehr die Angelegenheit erledigt sei. Dennoch informierte die Aufsichtsbehörde sie darüber, dass das Unternehmen nicht gegen datenschutzrechtliche Bestimmungen verstoßen hat, nunmehr aber die aufgrund ihrer Mitgliedschaft gespeicherten Daten in Zukunft für Zwecke der Werbung, Markt- und Meinungsforschung gesperrt sind und zukünftig nur noch für die Abwicklung der Mitgliedschaft eingesetzt werden.

### 4.2.2 An einen Finanzberater

Von einem anderen Bürger wurde an die Aufsichtsbehörde folgender Fall herangetragen. Der Betroffene führte aus, dass er von einem Mann einen Anruf erhalten habe, der den Eindruck erweckte, er sei Mitarbeiter bei der Hausbank des Betroffenen. Im nachfolgenden Ge-

spräch habe ihn dieser Anrufer über seine Lebensumstände, Beruf, Hobbys etc. ausgefragt. Anschließend habe er ihn gebeten, in die Filiale zu kommen und seinen Freistellungsauftrag zu aktualisieren. In der Bank stellte sich später heraus, dass der Anrufer kein Mitarbeiter der Hausbank war, sondern ein selbständiger Finanzberater. Trotzdem hatte ihm die Bank eine schriftliche Aufstellung der Konten, Kontonummern, Umsätze und weiterer sensibler Daten des Betroffenen übermittelt.

Mit diesem Sachverhalt wurde die Bank konfrontiert und zudem darüber informiert, unter welchen Voraussetzungen die benannte Übermittlung von Daten zulässig ist. Da seitens der Aufsichtsbehörde nicht erkennbar war, aus welchen Gründen die Übermittlung der Daten zulässig gewesen sein sollte, erhielt die Bank zur Klärung des Sachverhaltes die Gelegenheit zur Stellungnahme.

Nachfolgend teilte die Bank mit, dass eine Vielzahl von Kunden Beratung auch außerhalb der Räumlichkeit und der Geschäftszeiten der Bank wünsche. Um diesem Kundenwunsch Rechnung zu tragen, würden Finanzberater auf selbständiger Basis beschäftigt. Diese Vorgehensweise werde mit den Kunden abgestimmt. Nur sofern die Bankkunden Interesse an einer solchen zusätzlichen Beratung wünschen und mit der notwendigen Übermittlung ihrer Daten einverstanden sind, erhalte der Finanzdienstleister die benötigten Angaben. Der vorliegende Verstoß gegen diese Verfahrensweise sei ein bedauerlicher Einzelfall.

Der betroffene Bankkunde erhielt daraufhin eine erste Einschätzung der Rechtslage. Da von der Bank bislang nicht mitgeteilt wurde, welche Daten der Finanzberater erhalten hat, wurde sie erneut angeschrieben. Sie legte schließlich dar, dass neben Name, Anschrift und Telefonnummer auch eine aktuelle Übersicht über die im Haus der Bank geführten Produkte und die Daten über die steuerliche Freistellung übermittelt wurden.

Nunmehr wurde ein Ordnungswidrigkeitenverfahren gegenüber der Bank eingeleitet. Dieses basiert auf der unzulässigen Übermittlung personenbezogener Daten. Der Bank wurde bereits eine Anhörung hinsichtlich der vorgeworfenen Ordnungswidrigkeit i.S.d. § 43 Abs. 2 Nr. 1, 2. Alt. BDSG übersandt. Danach handelt ordnungswidrig, wer vorsätzlich oder fahrlässig unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, verarbeitet. Nachfolgend plädierte die Bank für die Einstellung des Bußgeldverfahrens, da es sich um einen bedauerlichen Einzelfall handele und im Haus zu dieser Thematik klare Regelungen vorhanden seien. Das Verfahren wurde bislang nicht eingestellt.

### 4.2.3 Veröffentlichung personenbezogener Daten in Fehlzeitstatistik

Anonym wurde die Aufsichtsbehörde darauf aufmerksam gemacht, dass auf dem Gelände einer Firma an einer für jeden einsehbaren Infotafeln eine Statistik ausgehängt sei. Aus ihr gingen die Fehlzeiten aller Beschäftigten des Unternehmens hervor. Jeder Mitarbeiter sei in dieser Statistik mit Name und Vorname, dem Datum seines Firmeneintritts, einem Vermerk über die Kündigung bzw. Nichtkündigung, der Anzahl der geleisteten Arbeitstage, der Anzahl der Krankentage sowie der Zahl der Tage, in denen er arbeitsunfähig war, erfasst. Diese Liste sei nach den entstandenen Fehlzeiten sortiert und weise zudem die durch die Krankheits- und Arbeitsunfähigkeitstage verursachten Kosten aus.

Diese Firma wurde seitens der Aufsichtsbehörde darauf hingewiesen, unter welchen Voraussetzungen die Erhebung, Verarbeitung bzw. Nutzung personenbezogener Daten zulässig ist. Da die betroffenen Mitarbeiter nach Mitteilung des Beschwerdeführers weder eingewilligt hatten, noch eine andere Rechtsvorschrift die geschilderte Verfahrensweise erlaubte oder anordnete, konnte sich eine Zulässigkeit einer solchen öffentlichen Statistik unter Zugrundelegung eigener Geschäftszwecke allein aus § 28 Abs. 1 Nr. 2 BDSG ergeben.
Hierbei war zwar ein berechtigtes Interesse der Firma darin zu sehen, einen Überblick über die Fehlzeiten im Unternehmen zu haben, doch bestanden erhebliche Zweifel an der Erforderlichkeit der Übermittlung dieser Daten. Daher wurde die Firma um Stellungnahme gebeten.

Diese führte an, die Belegschaft über das Anfertigen der streitgegenständlichen Statistik im Rahmen einer Betriebsversammlung informiert zu haben. Auch der Betriebsrat sei in Kenntnis gesetzt worden. Da von keiner Seite Einspruch erhoben wurde, sei man davon ausgegangen, dass die beabsichtigte Vorgehensweise akzeptiert wird. Sinn und Zweck der Statistik sei es gewesen, den Beschäftigten die problematisch hohen Ausfallzeiten durch Krankheit und Arbeitsunfähigkeit bewusst zu machen und die Belegschaft zu einer Reduzierung zu motivieren. Hierzu sei auch ein Prämierungssystem eingeführt worden. Die Firma sagte zu, von einer weiteren Veröffentlichung der Daten abzusehen, es sei denn, die jeweiligen Personen willigen in die Veröffentlichung ein. Die Einwilligung sei jedoch Voraussetzung, um an dem Prämierungssystem teilzunehmen.

Die Firma wurde daher darauf hingewiesen, dass das fehlende Erheben eines Einspruchs im Hinblick auf eine vorgeschlagene Verfahrensweise keine wirksame Einwilligung i.S.d. § 4a BDSG darstellt. Um Wirksamkeit entfalten zu können, muss die Einwilligung regelmäßig schriftlich abgefasst werden und auf dem freien Willen des Erklärenden beruhen. An Letzte-

rem können im Hinblick auf die besondere Drucksituation innerhalb eines Arbeitsverhältnisses sowie aufgrund der Verknüpfung der Einwilligung mit der Teilnahme am Prämierungssystem schnell Zweifel entstehen.
Für eine Zulässigkeit der Datenverarbeitung nach § 28 Abs. 1 Nr. 2 BDSG konnte die Firma zwar ein berechtigtes Interesse dartun, doch war die gewählte Form der Übermittlung der Daten an sämtliche Beschäftigten nicht erforderlich. Eine Sensibilisierung der Unternehmensbelegschaft für das Problem der hohen krankheitsbedingten Kosten kann ebenso effektiv durch eine Veröffentlichung anonymisierter Daten erreicht werden. Für das Prämierungssystem und die dadurch erhoffte Motivation der Mitarbeiter genügt deren Wissen um diese Form der Anerkennung und die Kenntnis über die zugrundegelegten Kriterien. Die Auswertung der Abwesenheitsstatistik als Grundlage der Prämierung kann intern, z.B. in der Personalabteilung, erfolgen und bedarf zudem keiner Veröffentlichung von Daten der Nichtprämierten. Insgesamt stellte die Aufsichtsbehörde fest, dass eine unzulässige Übermittlung von Daten stattgefunden hat. Aus diesem Grund wurde die Einleitung eines Bußgeldverfahrens auf der Grundlage des § 43 Abs. 2 Nr. 1, 2. Alt. BDSG geprüft und zu diesem Zweck der betroffenen Firma erneut Gelegenheit zur Stellungnahme gegeben.

Nachfolgend erläuterte das Unternehmen, dass man mit Blick auf die finanziell schwierige Situation der neu gegründeten Firma versucht habe, vor allem moderne Anreizsysteme der Mitarbeiterbindung und -motivation einzusetzen, um aus der Verlustzone zu kommen. Es wies nochmals darauf hin, dass aus Sicht der Unternehmensleitung alle Mitarbeiter mit der Verfahrensweise einverstanden waren und denen, die nicht am Prämierungssystem teilnehmen, keine finanziellen Nachteile entstünden.

Da die Firma glaubhaft darlegte, davon ausgegangen zu sein, eine wirksame Einwilligung der Mitarbeiter zu haben, und die Veröffentlichung der Statistik zumindest in der Personalversammlung und gegenüber dem Betriebsrat zur Disposition gestellt wurde, hat die Aufsichtbehörde vom Erlass eines Bußgeldbescheides abgesehen. Für den Fall zukünftiger ähnlich gelagerter Verstöße wurden dem Unternehmen jedoch Bußgeldverfahren in Aussicht gestellt.

### 4.2.4 Erteilung von Mahnungen und Abmahnungen

In einem anderen Fall wandte sich eine Familie an die Aufsichtsbehörde, da dem Ehemann durch seinen Verein eine öffentliche Abmahnung wegen Missachtung gegenüber dem Vorstand ausgesprochen wurde. Die Abmahnung war zu diesem Zweck im öffentlichen Schau-

kasten auf dem Vereinsgelände ausgehängt worden und konnte so von jedermann eingesehen werden.

Dem Vorstand des Vereines schilderte die Aufsichtsbehörde den Sachverhalt und verdeutlichte die Rechtslage des § 28 BDSG. Es wurde erörtert, dass die Verfahrensweise nach § 28 Abs. 1 Nr. 2 BDSG zur Wahrung berechtigter Interessen erfolgt sein könnte. Bedenken bestanden allerdings, da aus Sicht der Aufsichtsbehörde bereits eine nicht öffentliche Abmahnung genügt hätte, um die berechtigten Interessen des Vereines zu wahren, so dass eine öffentliche Aushängung der Abmahnung nicht erforderlich gewesen wäre.

Der Verein hob hervor, dass die öffentliche Abmahnung als persönliche Daten lediglich den Namen des Betroffenen aber keine darüber hinaus gehenden Daten enthalten habe. Zudem sei diese Maßnahme nach vorheriger Absprache und Beratung des Vorstandes erforderlich gewesen, da der Betroffene in der Vergangenheit immer wieder vergeblich darauf hingewiesen wurde, dass er die Satzung des Rahmenvertrages und die Pachtordnung einhalten müsse. Nachdem diese zahlreichen mündlichen und schriftlichen Hinweise ohne Ergebnis blieben, sei er darüber in Kenntnis gesetzt worden, dass er eine öffentliche Abmahnung erhalten wird. Zuvor wurde ihm letztmalig Gelegenheit gegeben, sich bezüglich der entsprechenden Kritikpunkte mit dem Vorstand in Verbindung zu setzen. Dies habe er nicht getan. Die entsprechenden Schreiben sowie die Satzung und Pachtordnung wurden als Nachweis vorgelegt.

Die Überprüfung ergab, dass die öffentliche Abmahnung in der erfolgten Form zur Wahrung berechtigter Interessen erforderlich gewesen ist.
In dem Bemühen eines Vereines, den Betroffenen zur Anerkennung des Vorstandes und zur Beachtung seiner Verpflichtung als Gartenpächter anzuhalten, besteht für den Vorstand eines Vereines, dessen Aufgabe es u.a. ist, für die Einhaltung der Gartenordnung zu sorgen, ein berechtigtes Interesse. Da der Betroffene seitens des Vorstandes mehrfach persönlich angesprochen wurde und er mehrere Schreiben erhielt, auf welche er nie reagierte, bestand für den Vorstand als letztes Mittel vor der Kündigung des Pachtvertrages allein die Möglichkeit, eine öffentliche Abmahnung auszusprechen. Da diese nur den Namen und Vornamen enthielt, war das Kriterium der Erforderlichkeit erfüllt. Auch bestand kein Grund zu der Annahme, dass die schutzwürdigen Interessen des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung die berechtigten Interessen des Vereins überwiegen. Jedes Mitglied eines Vereines hat sich an die entsprechenden Regelungen zu halten und muss im Falle der Missachtung mit Maßnahmen zur Durchsetzung der Regelungen rechnen. Die öffentliche

Abmahnung war daher eine datenschutzrechtlich zulässige Sanktionsmaßnahme. Darüber wurde der Betroffene in Kenntnis gesetzt.

Der Verein wurde dennoch darauf hingewiesen, dass er zukünftig zunächst eine schriftliche Abmahnung mit eindeutiger Fristsetzung zur Ausräumung des gerügten Verhaltens erteilen und erst als weiteren Schritt eine öffentliche Abmahnung aussprechen sollte.

### 4.2.5 Mieterdaten an Betreiber des öffentlichen Stromnetzes

Es meldete sich ein Hauseigentümer, der sich von einem Stromversorger genötigt fühlte, die personenbezogenen Daten seiner Mieter zu übermitteln. Diese Forderung sei seines Erachtens ein Verstoß gegen geltendes Datenschutzrecht, zumal die geschlossenen Formular-Mietverträge keine Klausel enthielten, die den Vermieter zur Weiterleitung personenbezogener Daten berechtigt oder verpflichtet. Der Versorger versuche auf diesem Weg an die Mieterdaten ohne Einwilligung der Mieter zu gelangen, um eine bessere Ausgangsposition gegenüber anderen Wettbewerbern am Strommarkt zu erlangen.

Dem Versorgungsunternehmen wurde der Sachverhalt geschildert und die entsprechende Rechtslage erläutert. Da der Hausbesitzer bei Befolgen der Forderung, die Daten zu übermitteln, keinen eigenen Geschäftszwecken nachgehen würde, schied § 28 Abs. 1 BDSG als mögliche Zulässigkeitsnorm aus. Jedoch ist nach § 28 Abs. 3 BDSG die Übermittlung oder Nutzung für einen anderen Zweck zulässig:

1. soweit es zur Wahrung berechtigter Interessen eines Dritten oder
2. zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist, oder
3. für Zwecke der Werbung, der Markt- und Meinungsforschung, wenn es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf
   a) eine Angabe über die Zugehörigkeit des Betroffenen zu dieser Personengruppe,
   b) Berufs-, Branchen- oder Geschäftsbezeichnung,
   c) Namen,
   d) Titel,
   e) Akademische Grade,
   f) Anschrift und
   g) Geburtsjahr beschränken

und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat,oder

4. wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

Da sich eine Zulässigkeit somit nur aus § 28 Abs. 3 Nr. 1 BDSG ergeben konnte, wurde das Unternehmen zur Stellungnahme aufgefordert.

Der Stromversorger teilte mit, dass der Hauseigentümer keinesfalls bedrängt wurde, sämtliche in sein Haus einziehenden Mieter mitzuteilen, damit Stromlieferverträge geschlossen werden können. Es gehöre zur allgemeinen Versorgungspflicht des Unternehmens, jedermann zu zumutbaren Bedingungen an das Versorgungsnetz anzuschließen. Hierzu sei das Unternehmen als örtlicher Versorger verpflichtet, es sei denn, ein anderer Lieferant sei benannt und die Versorgung durch diesen sichergestellt. Bei der Inanspruchnahme eines anderen Lieferanten sei eine Durchleitungsvereinbarung mit dem örtlichen Versorger erforderlich und sofern eine solche nicht vorliege, käme durch die bloße Energieentnahme aus dem Stromnetz ein Vertrag mit dem örtlichen Versorger zu Stande. Die Verordnung über Allgemeine Bedingungen für die Elektrizitätsversorgung von Tarifkunden sehe ausdrücklich vor, dass ein Stromversorgungsvertrag bereits durch die bloße Entnahme von Elektrizität aus dem örtlichen Verteilungsnetz zu Stande kommt. Zur eindeutigen Identifizierung der Verbrauchsstellen sei die Mitteilung von Namen und Anschrift der Anschlussnehmer erforderlich. Weiterhin könnten freiwillige Daten wie Geburtsdatum, Telefonnummer und soweit vorhanden die vorherige Verbrauchsstelle des Kunden angegeben werden.

Es fand eine abschließende Überprüfung durch die Aufsichtsbehörde statt. Dem Hauseigentümer wurde dargelegt, dass der Stromversorger ein berechtigtes Interesse gemäß § 28 Abs. 3 Nr. 1 BDSG an der Übermittlung der Mieterdaten (Name und Anschrift) besitzt. Dies ergibt sich daraus, dass durch die Entnahme der Elektrizität aus dem Verteilungsnetz des örtlichen Elektrizitätsversorgungsunternehmens ein Vertrag zu Stande kommt und es dem Unternehmen möglich sein muss, seine sich daraus ergebenden Pflichten zu erfüllen und Rechte geltend zu machen. Nach der Verordnung über Allgemeine Bedingungen für die Elektrizitätsversorgung von Tarifkunden ist der Kunde sogar verpflichtet, die Entnahme anzuzeigen. Da allein Name und Anschrift zwingend anzugeben sind, wird auch nicht gegen den Erforderlichkeitsgrundsatz verstoßen, denn diese Angaben sind notwendig, um im Rahmen der Vertragsbeziehungen zu agieren. Auch besteht kein Grund zu der Annahme, dass Mieter ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung haben, da jemand, der eine Leistung bezieht, wissen muss, dass er für diese aufzukommen hat. Somit ist die Übermitt-

lung aufgrund des Bundesdatenschutzgesetzes zulässig (§ 28 Abs. 3 Nr. 1 BDSG). Da demzufolge die Bedingungen des § 4 Abs. 1 BDSG erfüllt sind, kann der Hauseigentümer der Bitte des Versorgungsunternehmens Folge leisten, ohne dass es einer entsprechenden Erklärung in den Mietverträgen bedarf.

## 4.3 Werbung und Marketing

Mit Werbung wird man im täglichen Leben oft konfrontiert, da sie ein wirtschaftlich bedeutender Teil der Marktwirtschaft ist. Ob im Kino, im Fernsehen, im Radio, an Plakatwänden, in der Zeitung oder aus Werbepost, man kann ihr nur schwer entgehen. Manch einem gefällt Werbung vielleicht sogar, mancher möchte nur bestimmte Werbung erhalten und wieder andere würden sich ihr am liebsten ganz entziehen.

Gegen Werbebriefe und Reklame im Briefkasten kann man sich mit einem geeigneten Aufkleber „Bitte keine Werbung einwerfen“ wehren, dies gilt jedoch leider nicht für adressiertes Werbematerial. Um die Werbeflut einzudämmen, eröffnen die Datenschutzgesetze dem Einzelnen die Möglichkeit, sich gegen die unerwünschte Verwendung seiner persönlichen Daten für Werbezwecke zu wehren. Die geeignetsten Möglichkeiten sind nachfolgend dargestellt.

### 4.3.1 Unerwünschte Werbung per Fax oder E-Mail (Spamming)

Ein besonders großes Problem für die Betroffenen stellt die unerwünschte Werbung bei Faxgeräten dar. Hier fallen nicht nur erhebliche zusätzliche Kosten für Strom, Papier und Toner an, es wird auch die bestimmungsgemäße Funktion des Faxgerätes stark beeinträchtigt. Für viele Menschen dient es dazu, wichtige Schreiben ohne die mit postalischer Beförderung oftmals verbundene Zeitverzögerung senden und empfangen zu können. Gerade das ist nicht möglich, wenn die entsprechende Leitung stetig besetzt ist. Oft werden Werbefaxe auch in der Nacht versandt, was zu Störungen der Nachtruhe, Papierstau etc. führen kann. In jedem Fall ist solche Faxwerbung ein Ärgernis für Personen, die mit dem Absender in keinerlei Vertragsbeziehungen stehen.

Darauf hat auch die Rechtsprechung reagiert und unverlangte Faxwerbung als unzulässig eingestuft. Sie verstößt gegen § 1 des Gesetzes gegen den unlauteren Wettbewerb, wenn zwischen Absender und Empfänger keine Geschäftsbeziehung besteht und auch sonst der Absender nicht annehmen darf, die Zusendung durch Telefax erfolge mit dem mutmaßlichen Einverständnis des Empfängers.

Abmahnungen oder gar Klagen versprechen jedoch wenig Erfolg, da häufig der Absender der Faxwerbung nicht erkennbar ist. Sofern es sich um 0180er Nummern handelt oder Sie sich wenig Erfolg von einem eigenen Widerspruch hinsichtlich der Nutzung Ihrer Faxnummer versprechen, können Sie sich gern an das Landesverwaltungsamt Sachsen-Anhalt wenden.

Darüber hinaus gibt es für Sie folgende andere Möglichkeiten um Faxpapier, Toner und Nerven zu schonen:

- Auch für die Faxwerbung gibt es eine sogenannte Robinson-Liste, die im Auftrag der BITKOM (Bundesverband Informationswirtschaft, Kommunikation und neue Medien e.V) geführt wird. Sie gilt jedoch nur gegenüber Mitgliedern des Bundesverbandes, die sich verpflichtet haben, sie zu beachten, als durchsetzbar. Das Antragsformular für die Aufnahme in diese Robinsonliste können Sie per Fax-Abruf unter der Fax-Nr. 01805 000 761 (0,12 EUR/Min.) anfordern oder sich im Internet (http://www.retarus.de/upload/058_1_2005Bitkom.pdf) ausdrucken**.**
- Bei der Bestellung von Waren kann man schriftlich der Nutzung der eigenen Daten für Werbung und Marktforschung widersprechen, indem man der Bestellung einfach einen entsprechenden Satz hinzufügt (auf die Form dieses Widerspruchs kommt es nicht an).
- ISDN-Nummern können Faxe ohne erkennbare Anrufnummer abweisen.
- Bei schwerwiegenden Belästigungen oder bei Bedrohung kann man bei seinem Telekommunikationsunternehmen eine sogenannte Fangschaltung beantragen.
- Wenn man auf eine Bekanntgabe (z.B. aus beruflichen Gründen) der Faxnummer nicht angewiesen ist, kann man auf deren Veröffentlichung verzichten.

Auch SPAM-Mails stellen eine sehr lästige Art von Werbung dar. An die Aufsichtsbehörde wurden bereits mehrere Beschwerden herangetragen. Diese können jedoch nur weiterverfolgt werden, sofern die dafür verantwortliche Stelle bekannt ist. Oft kommt SPAM jedoch aus Asien oder Amerika, dann sind leider auch der Aufsichtsbehörde die Hände gebunden.

In einem der Aufsichtsbehörde vorgetragenen Fall war der Betreiber der Website bekannt, durch die ein Betroffener mit SPAM belästigt wurde. Diesen Betreiber schrieb die Aufsichtsbehörde an. Ihm wurde erläutert, dass SPAM-Mails eine Ansprache zum Zwecke der Werbung i.S.d. § 28 Abs. 4 BDSG darstellen.
Zwar wurde durch das Bundesdatenschutzgesetz die Erhebung, Speicherung, Nutzung und Übermittlung von personenbezogenen Daten zum Zwecke der Werbung und zur Markt- und Meinungsforschung in gewissem Maße erleichtert, die Verarbeitung und Nutzung der Daten muss jedoch bei Widerspruch des Betroffenen unterbleiben. Damit wird der Annahme Rech-

nung getragen, dass der Wille des Bürgers, frei von der Suggestivwirkung der Werbung zu bleiben und seinen Lebensbereich von jedem Zwang der Auseinandersetzung nach Möglichkeit freizuhalten, als schutzwürdig anerkannt ist.
Die Zusendung von unverlangten E-Mails verstößt zudem grundsätzlich gegen die guten Sitten im Wettbewerb. Eine solche Werbung ist nur dann ausnahmsweise zulässig, wenn der Empfänger ausdrücklich oder konkludent erklärt hat, E-Mail-Werbung erhalten zu wollen, oder wenn bei der Werbung gegenüber Gewerbetreibenden aufgrund konkreter tatsächlicher Umstände ein sachliches Interesse des Empfängers vermutet werden kann. Der Betreiber der Website wurde über den Werbewiderspruch des Betroffenen in Kenntnis gesetzt und um Stellungnahme gebeten.

Der Betreiber erklärte, dass auch er an seine eigene Email-Adresse versandte SPAM-Mails von seiner Website erhalten habe. Er nahm an, dass Dritte den Absender der Werbemails verfälscht und dadurch mit der von ihm angemeldete Adresse SPAM versandt haben. Um weiterem Missbrauch entgegenzuwirken, habe er inzwischen alle Emailaccounts auf der Website gelöscht.

Somit konnte ihm kein Verstoß gegen das Bundesdatenschutzgesetz nachgewiesen werden.

### 4.3.2 Telefon-Marketing

Ein weiteres lästiges Werbemittel sind Anrufe. Aus diesem Grund wandte sich eine betroffene Bürgerin an die Aufsichtsbehörde. Sie schilderte, dass sie in letzter Zeit unter ihrer privaten Telefonnummer diverse sogenannte cold calls erreicht hätten. So sei sie von einem Callcenter angerufen worden, welches ihr einen kostenlosen Check für Wintergärten angeboten habe. Der genaue Name des anrufenden Call-Centers war der Betroffenen ebensowenig bekannt, wie der Name der Firma, in deren Auftrag der Anruf erfolgte. Da die Betroffene mit keinerlei in Frage kommenden Firmen in Kontakt stand, bat sie um eine Überprüfung aus datenschutzrechtlicher Sicht.

Ihr wurde erläutert, dass der Anruf eine Ansprache zum Zwecke der Werbung darstellt und das Bundesdatenschutzgesetz hierfür in § 28 Regelungen zum Schutz der Bürger enthalte. Von der Rechtsprechung wird eine Telefonwerbung gegenüber Privatpersonen nur dann als zulässig angesehen, wenn der Angerufene zuvor stillschweigend oder ausdrücklich sein Einverständnis erklärt hat, zu Werbezwecken angerufen zu werden.

Da auf der Basis der Ausführungen der Betroffenen keine Einschätzung zur Zulässigkeit des Anrufes abgegeben werden konnte, wurde ihr die Möglichkeit des Werbewiderspruches erläutert (siehe Punkt 6.1 dieses Berichtes).

Zusammenfassend ist festzustellen, dass Telefonwerbung im Rahmen der unerwünschten Werbung die wohl schwerwiegendste Beeinträchtigung der Privatsphäre des einzelnen darstellt. Man kann sich ihr kaum entziehen, zudem trifft sie den Angerufenen völlig unvorbereitet. Aus diesem Grund hat der Bundesgerichtshof in ständiger Rechtsprechung entschieden, dass diese massive Einflussnahme, der sich der Angerufene häufig nur unter Verletzung der Regeln der Höflichkeit entziehen kann, nicht zulässig ist, sofern sich der Betroffene nicht ausdrücklich mit ihr einverstanden erklärt hat. Scheuen Sie sich also nicht, klare Aussagen zu treffen, wenn sie mal wieder angerufen werden.

### 4.3.3 Herkunft der genutzten Daten

In zahlreichen Verfahren wenden sich Bürger an die Aufsichtsbehörde, da sie per Post Werbung von einer bestimmten Stelle erhalten haben und sich fragen, woher das entsprechende Unternehmen die genutzten Daten hat. Da der Betroffene nach § 34 Abs. 1 Nr. 1 BDSG Auskunft über die zu seiner Person gespeicherten Daten verlangen kann, auch soweit sie sich auf die Herkunft der Daten bezieht, werden die Unternehmen (zu ihnen zählen der Versandhandel, Banken, aber auch Veranstalter von Verkaufsveranstaltungen) durch die Aufsichtsbehörde angeschrieben und um eine entsprechende Auskunft gebeten.

In einem Fall erhielt die verstorbene Ehefrau des Bürgers auch noch 3 Jahre nach ihrem Tod Werbepost an eine Anschrift, unter der sie zu Lebzeiten weder gewohnt hat, noch gemeldet gewesen ist. Entsprechende Anschreiben an die werbenden Firmen ergaben, dass die Adresse von einer bestimmten Firma zum Zwecke der Werbung angemietet wurde. Diese Firma gab auf Nachfrage an, die Anschrift von anderer Stelle angemietet zu haben. Der letzte angeschriebene Adresshändler erklärte, die neue Anschrift der Frau aufgrund einer Postretouresendung durch den Briefträger erhalten zu haben.
Aus diesem Grund richtete die Aufsichtsbehörde eine Anfrage direkt an die Deutsche Post AG. Diese teilte mit, dass vermutlich der Mann der Verstorbenen bei seinem Nachsendeauftrag die Möglichkeit eines Widerspruchs gegen die Weitergabe der Daten nicht genutzt hat. Somit besaß die Deutschen Post die Berechtigung, die Adressdaten auch an andere Postdienstleister weiterzuleiten, damit auch diese Sendungen nachsenden können. Diesen Postdienstleistern wurde damit wiederum die Möglichkeit gegeben, die Anschriftenänderung an die Absender weiterzuleiten, welche noch die alte Anschrift verwandt haben.

Darüber wurde der Betroffene informiert. Alle angeschriebenen Unternehmen haben unverzüglich den Datensatz seiner verstorbenen Frau vor weiterer Verwendung gesperrt.

**Tipp:** Durch einen Nachsendeauftrag bei der Deutschen Post kann man sich gewünschte Post weiterleiten lassen. Beim umsichtigen Ausfüllen des Antrages kann man durch Streichen der Formulierung im Punkt 5:

*Einwilligung in die Weitergabe von Adressdaten an Wettbewerber, andere Postdienstleister und Dritte,*

den Eingang zahlreicher Werbeschreiben nach einem Umzug verhindern, da zunächst nur wenige Unternehmen Ihre neue Anschrift kennen.

## 4.4 Mieterbereich

### 4.4.1 Mieterselbstauskunft

Nach telefonischer Rücksprache übergab ein Mieter der Aufsichtsbehörde eine Mieterselbstauskunft und bat um deren Überprüfung, da ihn die Art und die Tiefe der erfragten Angaben erstaunte. Das vorgelegte Dokument sah wie folgt aus:

Der/die Mietinteressent(en) .....
Erteilt (en) hiermit folgende freiwillige und wahrheitsgemäße Selbstauskunft.

| | Mietinteressent | Ehegatte/Mitmieter |
|---|---|---|
| Name/Vorname | ..... | ..... |
| Geburtsdatum | ..... | ..... |
| Staatsangehörigkeit | ..... | ..... |
| Familienstand (ledig, verheiratet, Partnerschaft) | ..... | ..... |
| Anschrift | ..... | ..... |
| Telefon privat | ..... | ..... |
| Telefon geschäftlich | ..... | ..... |
| Bisheriger Vermieter (Anschrift/Telefon) | ..... | ..... |

| | | |
|---|---|---|
| Beschäftigt in ungekündigter Stellung | ..... | ..... |
| Derzeit ausgeübter Beruf | ..... | ..... |
| Aktuelles monatl. Gesamteinkommen (Nachweis beifügen) | ..... | ..... |
| Konto-Nr./BLZ | ..... | ..... |

Zum Haushalt gehörende Kinder, Verwandte, Hausangestellte oder sonstige Mitbewohner unter Angabe von Name, Vorname, Verwandtschaftsgrad, Alter und Einkommen der jeweiligen Personen.

Ich/wir erkläre(n) hiermit der Wahrheit entsprechend folgendes:

Die Wohnung wird für ..... Personen benötigt.
Es bestehen keinerlei Absichten oder Gründe, weitere Personen in die Wohnung aufzunehmen oder eine Wohngemeinschaft zu gründen.
Ich/wir habe(n) folgende Haustiere:
Die Wohnung wird nicht gewerblich genutzt.
Ich/wir spiele(n) folgende Musikinstrumente:
Mein/unser derzeitiges Mietverhältnis besteht seit: .....
Mein/unser derzeitiges Mietverhältnis wurde gekündigt durch:
Vermieter, wegen .....
Mieter
Über die Räumung meiner/unserer Wohnung war/ist ein Räumungsrechtsstreit anhängig.
Es bestehen Zahlungsverpflichtungen aus:

| | |
|---|---|
| Teilzahlungsgeschäften | ..... € je Monat |
| Darlehensverpflichtungen | ..... € je Monat |
| Bürgschaften | ..... € je Monat |
| Sonstige Verpflichtungen | ..... € je Monat |

Ich/wir habe(n) weder die eidesstattliche Versicherung abgegeben, noch erging ein Haftbefehl hierzu, noch ist ein solches Verfahren anhängig.
Über mein/unser Vermögen wurde in den letzten 5 Jahren kein Konkurs- oder Vergleichsverfahren bzw. Insolvenzverfahren eröffnet bzw. die Eröffnung mangels Masse abgewiesen und solche Verfahren sind derzeit auch nicht anhängig.

Ich/wir sind in der Lage, eine Mietsicherheit von 3 Monatsmieten zu leisten und die geforderte Miete zu zahlen.
Ich/wir gestatten Referenzfragen bei: .....
Ich/wir sind mit einer Verwendung der angegebenen Daten für eigene Zwecke des Vermieters einverstanden (§ 22 Bundesdatenschutzgesetz)

Achtung: Wichtiger Hinweis!
Die Angaben dieser Selbstauskunft dienen der Beurteilung des/der Mietinteressenten und werden der Entscheidung über den Abschluss des Mietvertrages zu Grunde gelegt. Ein etwaiger Mietvertrag kommt deshalb unter der Bedingung zu Stande, dass die Angaben der Wahrheit entsprechen.

Sollte sich deshalb nach Abschluss des Mietvertrages herausstellen, dass einzelne Angaben falsch sind, ist/sind die Mieter zur sofortigen Räumung und Herausgabe des Mietobjektes verpflichtet und haben dem Vermieter jeden mittelbaren und unmittelbaren Schaden zu ersetzen.

Dem Betroffenen wurde mitgeteilt, dass grundsätzlich das Speichern und Nutzen personenbezogener Daten von Mietbewerbern von § 28 Abs. 1 Nr. 1 BDSG gedeckt ist, da die Datenspeicherung und Nutzung für eigene Zwecke im Rahmen des Mietvertrages bzw. seiner Anbahnung erfolgt. Hinsichtlich der Art und des Umfanges der gespeicherten personenbezogenen Daten gilt jedoch, dass nur solche Daten erfragt werden dürfen, die für den Abschluss oder die Erfüllung des Mietvertrages von Bedeutung sind. Es wird dabei anerkannt, dass der Vermieter ein berechtigtes Interesse an Daten hat, die die Zahlungsfähigkeit des Mieters betreffen (z.B. Art des Einkommens), ebenso Angaben zur Zahl der in der Wohnung lebenden Personen und deren Stellung zum Mieter. Unrichtige Angaben zu unzulässigen Fragen berechtigen den Vermieter nicht zur Anfechtung oder Kündigung des Mietvertrages, wie es in der dargestellten Selbstauskunft angedroht wird.
Gleichzeitig war festzustellen, dass in der Selbstauskunft zahlreiche personenbezogene Daten abverlangt werden, die keineswegs dem berechtigten Interesse des Vermieters zuzuordnen sind. Dazu zählen beim Mietinteressenten Angaben über Personalausweis- oder Passnummer, Geburtsdaten, Staatsangehörigkeit, geschäftliche Telefonnummer, bisheriger Vermieter mit Anschrift und Telefon, die Angaben über die Dauer der Beschäftigung in ungekündigter Stellung, Kontonummer und Bankleitzahl. Zudem sind derartige Angaben hinsichtlich des Ehegatten gar nicht zulässig, wenn er nicht mietvertraglich eingebunden wird. Bezüglich der weiteren im Haushalt lebenden Personen ist lediglich deren Anzahl und Ver-

wandtschaftsgrad für den Vermieter von Interesse. Nutzungen als Wohngemeinschaft oder für gewerbliche Zwecke sollten im Mietvertrag ausgeschlossen werden.
Die übrigen unzulässigen Fragen wurden in der Selbstauskunft für den Betroffenen markiert.

Trotz der Feststellung, dass zahlreiche Fragen in der Selbstauskunft nicht durch ein berechtigtes Interesse des Vermieters gedeckt sind, ist absehbar, dass es für den einzelnen Mietbewerber unter Umständen oft schwierig sein kann, Fragen des Vermieters ohne Risiko für seine Bewerbungschancen unbeantwortet zu lassen. Seitens der Aufsichtsbehörde kann hier zumindest gegenüber den Vermietern auf die Rechtslage hingewiesen und auf die korrekte Ausgestaltung des Fragebogens hingewirkt werden.

Zusammenfassend sollten nachfolgende Hinweise beachtet werden, da nicht jeder Fragebogen so strukturiert ist, wie der vorstehend abgedruckte.
Zulässig sind Fragen, an deren Beantwortung für das Mietverhältnis ein „berechtigtes billigenswertes und schutzwürdiges Interesse“ besteht. Unzulässig sind Fragen, die diskriminierend sind und für die kein sachlicher Grund besteht. Gefragt werden darf nur nach Umständen, „die für den Vermieter bei objektiver Wertung unter Berücksichtigung schutzwürdiger Belange des Mieters“ wesentlich sind, d.h. deren „Offenbarung dem Mieter zuzumuten ist“. Dabei ist das Informationsinteresse des Vermieters gegen das Interesse der Mietinteressenten/innen, ihre Privatsphäre zu schützen, abzuwägen.
Im Detail sind regelmäßig Fragen nach Rasse, der Hautfarbe oder der Nationalität unzulässig. Grundsätzlich unzulässig sind auch Fragen nach Vorstrafen oder nach einem anhängigen staatsanwaltschaftlichen Ermittlungsverfahren, dem Grund für den Wohnungswechsel, nach der Bankverbindung, nach der Mitgliedschaft in einem Mietverein, einer Rechtsschutzversicherung oder in einer politischen Partei, oder (bei weiblichen Mietinteressentinnen) nach dem Bestehen einer Schwangerschaft. Den Vermieter hat es nicht zu interessieren, ob eine Bewerberin bzw. ein Bewerber getrennt lebt, verlobt oder geschieden ist. Für ihn ist auch nicht von Belang, ob Kinder geplant sind, ob Krankheiten oder Behinderungen vorliegen oder welche Hobbys und Vorlieben bestehen. Werden Vereinbarungen über entsprechende höchstpersönliche Entscheidungen und Fragen getroffen, so sind diese sittenwidrig und nichtig. Rechtlich bedenklich sind auch solche Fragen, die den Zweck verfolgen, bei dritten Personen oder Stellen (z.B. dem Arbeitgeber, dem früheren Vermieter) Auskünfte einzuholen. Etwas anderes gilt, wenn die Bewerberin oder der Bewerber ausdrücklich darin eingewilligt hat, dass der Vermieter bei diesen Dritten Auskünfte einholt. Hinsichtlich der Wirksamkeit dieser Einwilligung ist § 4a BDSG zu beachten.
Als zulässig werden Fragen nach den Einkommensverhältnissen angesehen, z.B. ob eine eidesstattliche Versicherung abgegeben wurde. Auch die Frage nach dem Beruf ist in der

Regel nicht zu beanstanden, da über die berufliche Tätigkeit zumeist die Miete finanziert wird. Gibt ein Arbeitsloser fälschlicherweise einen früheren Arbeitgeber an oder täuscht er anderweitig ein bestehendes Arbeitsverhältnis vor, so wird darin teilweise ein Anfechtungsgrund gesehen. Dies ist aber insofern problematisch, als nicht grundsätzlich davon ausgegangen werden kann, dass Arbeitslose ihre Wohnung nicht bezahlen können. Zumindest besteht die Verpflichtung, den Vermieter darüber aufzuklären, dass die Miete nur mit Hilfe entsprechender Lohnersatz- oder Sozialleistungen aufgebracht werden kann. Keine Rolle können falsche Angaben über den Arbeitgeber oder das Einkommen einer Bewerberin oder eines Bewerbers spielen, wenn die Person eingezogen ist und die Mietzahlungen pünktlich erfolgen.
Aber auch hinsichtlich der Fragen nach der Zahlungsfähigkeit sind dem Vermieter enge Grenzen gesetzt. Soweit diese keine Einstandspflichten haben, ist die Frage nach dem Einkommen von Angehörigen unzulässig. Die Interessentin oder der Interessent müssen auch nicht ihre eigenen gesamten finanziellen Verhältnisse offenbaren. Unzulässig sind detaillierte Fragen zur persönlichen Finanzsituation, z.B. nach der Inanspruchnahme von Teilzahlungskrediten. Auskünfte, mit denen die Zahlungsfähigkeit in Höhe des Mietzinses bestätigt wird, sind ausreichend. Unzumutbar ist z.B. auch die Aufforderung, eine vom Vorvermieter unterschriebene Erklärung vorzulegen, in der dieser bescheinigt, dass es sich bei der Person um einen ordentlichen und pünktlichen Menschen handelt.

### 4.4.2 Mietwarndateien

In der Vergangenheit hat die Aufsichtsbehörde des Landes Sachsen-Anhalt vermehrt Anfragen hinsichtlich der datenschutzrechtlichen Zulässigkeit von Mieterwarndateien erhalten. In einer entsprechenden Datenbank sollen Daten auffällig gewordener Mieter erfasst werden. Solche Überlegungen resultieren nach den Aussagen der Anfragenden aus dem Umstand, dass eine ständig wachsende Zahl von Wohnungsmietern nicht gewillt sei, ihre Miete zu zahlen.

Mehr und mehr Wohnungsunternehmen und einzelne Vermieter schließen sich zu Gläubigergemeinschaften zusammen und errichten Warndateien. Andere Unternehmen und Existenzgründer sehen Mieterwarndateien als lukrative Geschäftsidee an. Daher folgen zu diesem Problemkreis einige allgemeine Ausführungen.
In Mieterwarndateien sollen ausweislich der an die Aufsichtsbehörde herangetragenen Anfragen detaillierte Angaben zu den Vermögensverhältnissen sowie bestehenden Ratenzahlungen, zur Höhe von Unterhaltszahlungen etc. ebenso erfasst werden, wie Fragen nach der Staatsangehörigkeit oder nach Personalausweis- oder Passnummern. Vermieter möchten in

diese Warndateien auch verspätete oder unregelmäßige Mietzahlungen melden, obwohl die Rückstände im Einzelfall z.B. durch Mietminderungen wegen eines Mangels der Mietsache etc. begründet sein können und nicht unbedingt auf eine generelle Zahlungsunfähigkeit oder –unwilligkeit des Mieters hinweisen. Gleichermaßen sollen Verstöße gegen die Hausordnung oder sonstiges vertragswidriges Verhalten Eingang in die Warndatei finden.

Zunächst einmal ist das Interesse der Vermieter, schwarze Schafe unter den Mietinteressenten zu erkennen und dadurch das betriebswirtschaftliche Risiko zu minimieren, nachvollziehbar und verständlich.
Dennoch müssen auch die Belange der Wohnungssuchenden beachtet werden. Die Wohnung ist der Mittelpunkt des privaten Lebensbereiches. Durch ungeprüfte Eingaben von Mieterdaten in Warndateien kann jedermann zum „Negativmieter“ werden. Es lässt sich nicht ausschließen, dass Personen unverschuldet und ohne berechtigten Anlass in diesen Ruf geraten. Mit Blick auf die zentrale Bedeutung von Wohnraum im Leben jedes einzelnen Bürgers muss daher die Gefahr unberechtigter Einschränkungen bei der Wohnungssuche vermieden werden.
Entsprechend sind bei der Überprüfung der Zulässigkeit derartiger Datenerhebungen und -speicherungen strenge Maßstäbe anzulegen. Die Errichtung und der Betrieb einer Warndatei sind aus Sicht des Datenschutzes äußerst kritisch zu sehen.

Da die in einer solchen Datenbank erfassten Personen dazu in der Regel keine Einwilligung gegeben haben (auch keine wirksame Einwilligung aufgrund der Voraussetzungen des § 4a BDSG möglich sein dürfte) und andere Rechtsvorschriften diese Verfahrensweise weder erlauben noch anordnen, kann sich die Zulässigkeit von Mieterwarndateien allein aus dem Bundesdatenschutzgesetz ergeben. Weil die Daten geschäftsmäßig zum Zweck der Übermittlung erhoben und gespeichert werden, findet § 29 BDSG Anwendung.

Nach § 29 Abs. 1 Satz 1 BDSG ist das geschäftsmäßige Erheben, Speichern oder Verändern personenbezogener Daten zum Zweck der Übermittlung zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat, oder
2. 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 Erhebung, Speicherung oder Veränderung offensichtlich überwiegt.

Geplante Warndateien können nur dann hinsichtlich ihrer Zulässigkeit beurteilt werden, wenn die Aufsichtsbehörde über die Art der einzelnen zur Erhebung und Speicherung beabsichtigten Daten informiert wird.

§ 29 Abs. 1 Satz 1 Nr. 2 BDSG scheidet als Zulässigkeitsalternative für die Speicherung von Daten zur Zahlungsmoral von Mietern aus, wenn entsprechende Daten nicht allgemein zugänglichen Quellen, wie dem Schuldnerverzeichnis oder dem Insolvenzregister entnommen werden können.

Die Zulässigkeitsalternative des § 29 Abs. 1 Nr. 1 BDSG erfordert eine Vorabprüfung möglicher der Erhebung, Speicherung oder Veränderung der Daten entgegenstehender schutzwürdiger Interessen des Betroffenen. In keinem Fall kann von vornherein ein schutzwürdiges Interesse des Betroffenen, hier also der Mieter, ausgeschlossen werden. Besteht auch nur Grund zu der Annahme, dass die Interessen des Betroffenen an der Verarbeitung entgegenstehen, so ist die Verarbeitung unzulässig. Ein solcher Grund kann sich bereits mit Blick auf die Sensibilität der Daten und eventuelle Auswirkungen ihrer Übermittlung für den Betroffenen ergeben. Da bei Warndateien die Auswirkungen auf den einzelnen Mieter sehr weit reichen können, ist eine Abwägung zwischen den verschiedenen Interessen sehr sorgfältig vorzunehmen.

Zudem werden Art und Umfang der für eine Mieterwarndatei erhebbaren und speicherbaren Daten auch danach bestimmt, welche Daten im Fall einer Anfrage eines Vermieters zulässiger Weise an diesen übermittelt werden dürfen.
Gemäß § 29 Abs. 2 BDSG ist die Übermittlung personenbezogener Daten im Rahmen der Zwecke nach Absatz 1 zulässig, wenn

1. a) der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat oder
   b) … *[für eine Übermittlung an Vermieter nicht einschlägig]*… und
2. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Vermieter, welche sich an die Warndatei wenden, müssen demzufolge ein berechtigtes Interesse an den begehrten personenbezogenen Daten nachweisen. Anerkannt wird hier das berechtigte Interesse der Vermieter an einer Minimierung des Mietausfallrisikos durch Übermittlung von Daten zum Zahlverhalten der Mieter.
Im Falle einer Mietübernahmegarantie durch Sozialleistungsträger besteht daher keine Notwendigkeit zu einer entsprechenden Datenerhebung.

Zudem dürfen schutzwürdige Interessen des betroffenen Mieters der Übermittlung nicht entgegenstehen.
Ein vollständiger Katalog von personenbezogenen Daten, welche an Vermieter übermittelt werden dürfen, existiert nicht. Von allen Aufsichtsbehörden für den Datenschutz werden übereinstimmend derzeit die Daten des nachfolgenden Kataloges als ohne jeden Zweifel an den Vermieter übermittelbar angesehen:

- Daten aus öffentlichen Schuldverzeichnissen
- Rechtskräftige Titel zum Zahlungsverzug im Mietbereich
- Rechtskräftige Urteile zur fristlosen Kündigung wegen
    - Zahlungsverzug
    - sonstiger Vertragsverletzung
- Rechtskräftiges Räumungsurteil wegen fristloser Kündigung
- bei „Mietnomaden“, wenn innerhalb der ersten 3 Monate zwei Monatsmieten nicht gezahlt wurden und Strafantrag/ -anzeige gestellt wurde.

Diese Daten können auch zum Zwecke der Errichtung einer Warndatei erhoben und gespeichert werden. Sie dürfen ohne Einwilligung des Mieters durch den Vermieter abgefragt bzw. eingemeldet werden, jedoch nur, wenn der betroffene Mieter darüber angemessen informiert wird.
Insgesamt ist festzustellen, dass ein datenschutzrechtlich nicht zu beanstandender Betrieb einer Mieterauskunftei häufig nicht den erhofften Effekt bringt, da bei Beachtung der datenschutzrechtlichen Vorschriften, insbesondere der §§ 4d – 4g, 28 bzw. 29 sowie 33 – 35 BDSG, ein nicht zu unterschätzender Aufwand bei der Pflege und dem Betrieb einer solchen Datenbank entsteht und auch hinsichtlich der Übermittlung der gespeicherten Daten enge Voraussetzungen erfüllt sein müssen.

Weiter klärungsbedürftig ist auch die Frage, in welchem Umfang bei branchenübergreifenden Auskunfteien gespeicherte Daten an Vermieter übermittelt werden dürfen. Diese Auskunfteien (u.a. SCHUFA, Creditreform, Infoscore und Bürgel) speichern nicht nur personenbezogene Daten aus Mietverhältnissen, sondern führen weit umfangreichere Datenmengen.
Einigkeit der Aufsichtsbehörden besteht dahingehend, dass eine uneingeschränkte Übermittlung sämtlicher über einen Betroffenen bei einer brachenübergreifenden Auskunftei gespeicherter Daten an potentielle Vermieter unzulässig ist. Ob und wie weit eine über den oben stehenden seitens der Aufsichtsbehörden anerkannten Katalog hinausgehende Datenübermittlung und -einmeldung als zulässig erachtet werden kann, wird derzeit noch geprüft. E-

benfalls haben die Aufsichtsbehörden ihre Meinungsbildung noch nicht abgeschlossen, inwieweit Mieterinformationen geschlossenen Nutzergruppen vorbehalten sein sollten.

Aus Sicht der Aufsichtsbehörden verdienen die auf branchenspezifische Daten beschränkten Auskunftssysteme, bei denen die Daten sichere Rückschlüsse auf Mietausfallrisiken zulassen, den Vorzug, da sie datenschutzrechtlichen Belangen am Besten Rechnung tragen.

### 4.4.3 Erteilung von Hausverboten

Ein Polizeirevier übersandte der Aufsichtsbehörde mehrere Schriftstücke, welche Hausverbote zum Inhalt hatten und im Hausflur eines Wohngebäudes vorgefunden wurden. Diese Hausverbote enthielten personenbezogene Daten (Name, Geburtsdatum, Wohnanschrift) der betroffenen Personen. Die Hausverbote waren an einer uneingeschränkt einsehbaren Hinweistafel im Eingangsbereich des Gebäudes angebracht. Auf diese Weise konnte die Daten jeder, der das Haus betritt, einsehen. Da das Polizeirevier Bedenken hinsichtlich der Einhaltung datenschutzrechtlicher Bestimmungen hatte, entfernte ein Beamter die Hausverbote und übersandte diese der Aufsichtsbehörde zur weiteren Überprüfung.

Die Immobilienverwaltungsfirma wurde daraufhin seitens der Aufsichtsbehörde informiert, dass insbesondere die erfolgte Übermittlung von Daten nur zulässig sei, wenn dies zur Wahrung berechtigter Interessen erforderlich gewesen ist, § 28 Abs. 1 Nr. 2 BDSG. Berechtigte Interessen der Hausverwaltung hätten aber beispielsweise auch bei teilweiser Anonymisierung der personenbezogenen Daten gewahrt werden können, weshalb starke Bedenken gegen die Erforderlichkeit der Datenverarbeitung beständen. Zudem muss bei Vorliegen „berechtigten Interesses“ und der „Erforderlichkeit“ weiterhin geprüft werden, ob kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Die Immobilienverwaltungsfirma ging davon aus, sich datenschutzkonform verhalten zu haben. Dies wurde damit begründet, dass die erteilten Hausverbote nur ihre Wirkung erzielen, sofern die Hausbewohner deren Einhaltung anhand der Aushänge kontrollieren können. Ein milderes ebenso geeignetes Mittel gäbe es nicht.

Der Firma gegenüber wurde bestätigt, dass ihr die Ausübung des Hausrechts nach dem Strafgesetzbuch zusteht und dieses somit ein Mittel für die Erfüllung eigener Geschäftszwecke darstellt. Die Zulässigkeit des Erhebens, Speichern oder des Übermitteln insofern notwendiger Daten ergibt sich jedoch allein aus §§ 28 Abs. 1 bis 3 BDSG.

Die Erhebung und Speicherung der personenbezogenen Daten der vom Hausverbot betroffenen Personen ist von den Bestimmungen des Bundesdatenschutzgesetzes aufgrund des Zweckes „Ausübung des Hausrechtes“ auch gedeckt.
Der Übermittlung der Daten fehlt allerdings die Rechtsgrundlage. Übermitteln ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass

a) die Daten an den Dritten weitergegeben werden oder
b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft.

Das Übermitteln stellt eine Verarbeitung dar. In der Kontrolle des Hausrechtes ist das hierfür nötige berechtigte Interesse zu sehen. Jedoch waren die Aushänge zur Wahrung dieses Interesses nicht erforderlich.
Zur Verwirklichung einer Kontrolle des Hausverbotes durch die Hausbewohner müssten diese die Daten der Aushänge mit den Daten der im Haus befindlichen Personen abgleichen. Dafür müssten die Hausbewohner Daten erheben, wozu sie jedoch nicht berechtigt sind. Bereits an dieser Stelle wird deutlich, dass das berechtigte Interesse der Hausverwaltung durch das streitgegenständliche Aushängen der Hausverbote gar nicht ohne Verstoß gegen datenschutzrechtliche Bestimmungen gewahrt werden konnte. Schon daran scheiterte die Erforderlichkeit dieser Datenübermittlung. Auch konnte durch die Firma nicht dargelegt werden, dass kein weniger stark in die Rechte der Betroffenen eingreifendes Mittel existiert. Vor dem Aushängen der Verbote war kein Versuch unternommen worden, die Adressaten der Verbote auf schriftlichem Weg über ihr Zugangsverbot zu informieren und dessen Einhaltung abzuwarten.
Zudem besteht Grund zu der Annahme, dass die Betroffenen ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung ihrer Daten haben. Im Zweifelsfall ist davon auszugehen, dass die Betroffenen sich an das ihnen erteilte Hausverbot halten und folglich unnötig ihre personenbezogenen Daten bekannt werden.

Insgesamt war festzustellen, dass aufgrund der in Rede stehenden Aushänge gegen das Bundesdatenschutzgesetz verstoßen wurde. Nach § 43 Abs. 2 Nr. 1 BDSG handelt ordnungswidrig, wer vorsätzlich oder fahrlässig unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet. Aus diesem Grund wurde nach erneuter Anhörung ein Bußgeldverfahren eingeleitet. Eine seitens der inzwischen anwaltlich vertretenen Firma angekündigte weitere Stellungnahme ist bisher ausgeblieben, so dass nunmehr der Erlass des beabsichtigten Bußgeldbescheides aussteht.

## 4.5 Auskunfteien

### 4.5.1 Allgemeines

Handels- und Wirtschaftsauskunfteien sammeln Informationen über die wirtschaftliche Betätigung, Kreditwürdigkeit und Zahlungsfähigkeit von Unternehmen und Privatpersonen. Zu den Bekanntesten zählen die SCHUFA, die Creditreform und Bürgel. Daneben gibt es eine Vielzahl kleinerer Auskunfteien und Brancheninformationsdienste. Auch diesen Auskunfteien gegenüber besitzt der Betroffene ein Auskunftsrecht. Grundsätzlich ist die Auskunft über die zur eigenen Person gespeicherten Daten unentgeltlich, es sei denn der Betroffene kann die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen.

Auskunfteien erheben und speichern Daten geschäftsmäßig zum Zweck der Übermittlung, weshalb § 29 BDSG eine der wichtigsten Rechtsgrundlagen für die Tätigkeit dieser Unternehmen darstellt.
Üblicherweise werden durch die Unternehmen, wobei dies im Detail verschieden ist, neben Namen, Anschrift und Geburtsdatum Daten zum Einkommen und Vermögen (z.B. zu Tätigkeit, Arbeitgeber, Umsatz, Grundbesitz, Bankverbindung und Schulden) erfasst. Festgehalten wird auch, ob eine eidesstattliche Versicherung abgegeben, ein Zwangsversteigerungsverfahren betrieben, gegen den Betroffenen wegen Säumigkeit ein Haftbefehl angeordnet wurde oder ob vollstreckbare Schuldtitel vorliegen.
Bei einigen Auskunfteien werden, wenn konkrete Daten des Betroffenen nicht vorliegen, statistische Daten (Schätzdaten) zu Grunde gelegt. Dies ist nur rechtmäßig, wenn die Daten als solche gekennzeichnet werden. Teilweise enthalten die Auskünfte auch Bonitätsbewertungen aufgrund mathematisch-statistischer Verfahren (credit-scoring).
Die Daten stammen zum großen Teil aus allgemein zugänglichen Quellen, wie Telefon- und Adressbüchern sowie Branchenverzeichnissen, oder öffentlichen Registern, wie dem Handelsregister oder dem Schuldnerverzeichnis. Ebenso geben die anfragenden Kunden der Auskunfteien Daten über die Geschäftsbeziehungen weiter. Auch werden an Betroffene Selbstauskünfte versandt, aus welchen anschließend Daten erhoben werden. Solche Selbstauskünfte sind jedoch stets freiwillig. In Ausnahmefällen kommt es auch vor, dass Informationen durch eine Befragung des Umfeldes des Betroffenen beschafft werden. Gegen diese Verfahrensweise bestehen jedoch datenschutzrechtliche Bedenken.

Nach § 29 Abs. 2 BDSG dürfen nur solche Stellen eine Auskunft erhalten, die ein berechtigtes Interesse haben (z.B. vor einem konkreten Vertragsabschluss) und die die Informationen benötigen, um das finanzielle Risiko besser abschätzen zu können. Vor allem der Versand-

handel, Hypothekenbanken und auch Autovermieter sowie Kaufhäuser interessieren sich für die Auskünfte über Privatpersonen. Personen, die aus bloßer Neugier Informationen, z.B. über Nachbarn, haben wollen, gehören nicht zum Kreis der Auskunftsberechtigten.
In jedem Fall sind die Persönlichkeitsrechte des Betroffenen gegen die Interessen des Anfragenden abzuwägen. Schutzwürdige Interessen der Betroffenen stehen immer dann der Verwendung der Daten entgegen, wenn die Angaben nicht der Beurteilung der Kreditwürdigkeit und Zahlungsfähigkeit der Betroffenen dienen. Dies ist etwa der Fall bei unrichtigen Daten oder bei Vermögensangaben über Ehepartner und Verwandte etc..

### 4.5.2 Unrichtigkeit gespeicherter personenbezogener Daten

Der Aufsichtsbehörde sind hinsichtlich unrichtiger bei Auskunfteien gespeicherter Daten zahlreiche Beschwerden zugegangen. Diese reichen vom Bestreiten verzeichneter Forderungen über die irrtümliche Speicherung der Daten aufgrund von Namensgleichheit oder -verwechslung bis hin zur unbegründeten Erfassung von Daten einer Person, der ihre inzwischen von Kriminellen zu Straftaten missbrauchten Dokumente diebstahlsbedingt abhanden gekommen sind.

Ein Betroffener erfuhr während der Verhandlungen um die Finanzierung eines neuen Pkws, dass er eine negative Eintragung hat. Die Hausbank lehnte daher die Finanzierung aufgrund der eingeholten Auskunft ab. Daraufhin forderte der Betroffene auf Anraten der Aufsichtsbehörde eine Selbstauskunft an, in der er die nicht korrekten Eintragungen markierte. Im Anschluss übergab er den Vorgang der Aufsichtsbehörde und führte ergänzend aus, dass die negativen Eintragungen allein mit dem Diebstahl seiner Dokumente vor 2 Jahre zu erklären seien.

Die Auskunftei wurde über die Sach- und Rechtslage in Kenntnis gesetzt und um Stellungnahme sowie um Mitteilung der Anschriften der „Einmelder“ der Daten gebeten.

Die Auskunftei teilte mit, nichts von dem Verlust der Dokumente gewusst zu haben. Bis zur Übersendung der Verlustanzeige sei jedoch ein vorläufiger Hinweis über den Verlust der Dokumente in den Datenbestand aufgenommen worden. Zudem habe sie eine Überprüfung des Datenbestandes bei den entsprechenden Vertragspartnern eingeleitet. Entsprechend hätten hinsichtlich zweier Datensätze die informierten Firmen bereits gemeldet, dass Betrug vorgelegen hat. Daher wurden diese Daten gelöscht. Die Rückfragen bei den übrigen Vertragspartnern dauere noch an.

Nachfolgend wurde ergänzend mitgeteilt, dass auch die anderen Firmen bestätigt haben, dass Betrug vorlag. Somit wurden auch die entsprechenden Eintragungen aus dem Datensatz des Betroffenen gelöscht.

Die Aufsichtsbehörde setzte daraufhin den Betroffenen über die Berichtigung seiner Daten in Kenntnis.

## 4.6 Schutz besonderer personenbezogener Daten

Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

### 4.6.1 Betriebsarztdaten

Ein Bürger wandte sich an die Aufsichtsbehörde, da in seinem Fall ein als „betriebliches Ergebnis einer Eignungsuntersuchung“ bezeichnetes Dokument verschiedenen Personen ohne seine Einwilligung zugänglich gemacht wurde. Dieses Dokument umfasste nach seinen Angaben neben der Eignung (positives Leistungsbild) Aussagen zur körperlichen Belastbarkeit, geistig-seelischen Belastbarkeit, zum negativen Leistungsbild sowie ein frei formuliertes ergänzendes Leistungsbild. Er bat um Überprüfung, ob der Datenschutz in irgendeiner Form verletzt wurde.

Es wurde ihm mitgeteilt, dass personenbezogene Daten übermittelt werden, wenn seitens (des Betriebsarztes) des ihn beschäftigenden Unternehmens die Ergebnisse seiner Eignungsuntersuchung an andere Personen weitergegeben werden. Das Übermitteln fällt in den Bereich der Verarbeitung personenbezogener Daten und ist unter den Voraussetzungen des § 4 BDSG zulässig. Da keine Einwilligung des Betroffenen zur Weitergabe der Daten vorlag und auch keine andere Rechtsvorschrift die Übermittlung der Daten der betrieblichen Eignungsuntersuchung ausdrücklich erlaubte oder gar anordnete, wurde geprüft, ob die Übermittlung der Daten durch Vorschriften des Bundesdatenschutzgesetzes zugelassen ist.

Da der Aufsichtsbehörde keine detaillierten Informationen über die Art der vom Betroffenen ausgeübten Beschäftigung sowie Einzelheiten der übermittelten Daten vorlagen, wurde dem Betroffenen dargelegt, unter welchen Voraussetzung die Übermittlung seiner Gesundheitsdaten zulässig ist.

Bei den in dem Dokument über die betriebliche Eignungsuntersuchung enthaltenen Gesundheitsdaten handelt es sich um vom Bundesdatenschutzgesetz speziell geschützte besondere personenbezogene Daten. Die maßgebliche Vorschrift des § 28 Abs. 6 BDSG erklärt u.a. das Verarbeiten von besonderen Arten personenbezogener Daten für eigene Geschäftszwecke für zulässig, wenn dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt (§ 28 Abs. 6 Nr. 3 BDSG).
Die geschilderte Übermittlung könnte zur Erfüllung der Geschäftszwecke des Arbeitgebers zulässig gewesen sein, sofern dies zur Durchsetzung seiner rechtlichen Ansprüche erforderlich war und die schutzwürdigen Interessen des Mitarbeiters dem nicht entgegenstanden.

Der Arbeitgeber darf zudem nur solche Gesundheitsinformationen erfragen, die sich aus den spezifischen Anforderungen des Arbeitsplatzes und den sich daraus ergebenden Gefahren rechtfertigen. Dies ist nur dann der Fall, wenn die Kenntnis der Gesundheitsdaten unmittelbar bedeutsam für die konkret ausgeübte Tätigkeit ist. Sofern eine solche Tätigkeit ausgeübt wird, dürfen trotzdem nicht genaue Diagnosen oder gar die Krankengeschichte eingesehen werden. Der Arbeitgeber hat lediglich ein Recht auf Übermittlung der für den Arbeitsplatz relevanten Untersuchungsergebnisse, d.h. der Eignung oder Nichteignung für bestimmte Tätigkeiten.

Die Aufsichtsbehörde bot dem Betroffenen an, beim Vorliegen weiterer Informationen über die Art seiner Tätigkeit, die Funktion der Personen, an welche die Daten weitergegeben wurden, den Umfang der übermittelten Daten und seine der Datenübermittlung entgegenstehenden Interessen eine abschließende Zulässigkeitsprüfung vorzunehmen.

Nachfolgend übersandte der Betroffene die erbetenen Auskünfte. Infolgedessen konnte abschließend festgestellt werden, dass Gegenstand der übermittelten Daten lediglich das Ergebnis der Eignungsuntersuchung war, welches sich auf die dem Betroffenen angetragene Tätigkeit beschränkte. Es wurden weder einzelne Krankheiten, noch Ablauf und Inhalt möglicher medizinischer Behandlungen erwähnt, weshalb es sich bei den darin enthaltenen personenbezogenen Daten nicht um klassische Angaben über die Gesundheit und mithin nicht um besondere Arten personenbezogener Daten handelte. Die erhobenen Daten waren zudem für das jeweilige Arbeitsverhältnis erforderlich. Entsprechend wurde die Zulässigkeit der Datenverarbeitung anhand der Regelungen des § 28 Abs. 1 bis 3 BDSG überprüft und festgestellt, dass die Datenübermittlung danach zulässig gewesen ist.

### 4.6.2 Medizinische Gutachten

In einem weiteren Verfahren wandte sich eine Betroffene an die Aufsichtsbehörde und trug vor, dass eine Versicherung die Kausalität zwischen einem Unfall, den sie erlitten hatte, und ihrem Gesundheitszustand in Frage stelle und aus diesem Grund ein Gutachten über ihre Person angefertigt habe. Dieses nervenärztliche Gutachten sei, ohne dass sie den Gutachter von seiner ärztlichen Schweigepflicht entbunden hat, an ihren Arbeitgeber übersandt worden, welcher das Gutachten jedoch nicht angefordert habe.

Zur Sachverhaltsermittlung wurde die Versicherung angeschrieben. Hier lag eine Verarbeitung durch die Übermittlung des Gutachtens vor. Da die Betroffene nicht eingewilligt hat und auch keine andere Rechtsvorschrift die Verfahrensweise anordnete oder erlaubte, war die Zulässigkeit der Verarbeitung allein anhand des Bundesdatenschutzgesetzes zu prüfen. Bei den übermittelten Daten handelt es sich um besondere Arten personenbezogener Daten, weshalb allein § 28 Abs. 6 BDSG einschlägig ist. Die streitgegenständliche Verfahrensweise könnte zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich gewesen sein. Daher wurde die Versicherung nach dem Grund der Datenübermittlung befragt.

Der Datenschutzbeauftragte der Versicherung teilte nachfolgend mit, dass der Arbeitgeber der Betroffenen Ansprüche gegen einen ihrer Versicherten geltend gemacht habe, die abgelehnt wurden. Da die Anspruchsablehnung auf den Ausführungen des Gutachters basiere, habe man das Gutachten dem diesbezüglichen Schreiben beigefügt. Die Übermittlung des Gutachtens sei aus Gründen der Nachvollziehbarkeit der Forderungsablehnung erfolgt und somit i.S.d. § 28 Abs. 6 Nr. 3 BDSG zulässig gewesen.

Nunmehr hat sich die Aufsichtsbehörde zur Aufklärung des Sachverhaltes mit dem Arbeitgeber der Betroffenen in Verbindung gesetzt. Dessen Reaktion steht noch aus. Erst nach ihrem Eingang kann eine abschließende Überprüfung der Zulässigkeit der Übermittlung des Gutachtens erfolgen.

### 4.6.3 Outsourcing – externe Archivierung und Löschung von Patientenakten aus Krankenhäusern und Arztpraxen

Die Aufsichtsbehörde erhielt von einem Krankenhaus die Anfrage, was bei der Vernichtung von Patientenakten zu beachten sei. Unter der Vernichtung von Akten ist im datenschutz-

rechtlichen Sinn eine Löschung von Daten zu verstehen. Löschen bedeutet das Unkenntlichmachen gespeicherter personenbezogener Daten und stellt einen Unterfall der Verarbeitung personenbezogener Daten dar.

Bei der Verarbeitung von personenbezogenen Daten im Krankenhaus ist neben dem ärztlichen Berufsrecht das Datenschutzrecht anzuwenden. Die Entscheidung, welches Datenschutzrecht anzuwenden ist, hängt von der Rechtsform des Trägers des jeweiligen Krankenhausbetriebes ab. Auf Krankenhäuser in privater Trägerschaft ist das Bundesdatenschutzgesetz (BDSG) anzuwenden. Krankenhäuser mit öffentlich-rechtlicher Trägerschaft auf Landesebene (hierzu gehören die Krankenhäuser der Gemeinden und Landkreise sowie die Universitätskliniken) unterliegen demgegenüber dem jeweiligen Landesdatenschutzrecht.

Da die Vernichtung von Patientenakten keine originäre ärztliche Arbeit darstellt und die Vernichtung outgesourct, d.h. ausgelagert, erfolgen soll, werden dabei Patientendaten weitergegeben oder auf andere Weise zugänglich gemacht, so dass eine Offenbarung von Patientendaten erfolgt. Schon das Einräumen der Möglichkeit der Kenntnisnahme durch einen Dritten genügt für eine Offenbarung. Dies ist selbst dann der Fall, wenn dem Dritten nur zeitweilig die Verfügungsmöglichkeit über die Daten eingeräumt wird. Eine Offenbarung von Patientendaten ist nach § 203 Strafgesetzbuch (StGB) jedoch nur zulässig, wenn hierfür eine besondere Befugnis besteht. Diese Befugnis kann sich ausdrücklich aus gesetzlichen Ermächtigungen und Verpflichtungen zur Datenweitergabe oder aus einer Einwilligung des Patienten ergeben. Ohne gesetzliche Befugnis oder Einwilligung kann der jeweils zuständige Arzt (in Krankenhäusern die jeweiligen Ärzte) eine strafbare Offenbarung nur vermeiden, wenn er ausschließt, dass die am Outsourcing Beteiligten Kenntnis von Patientendaten nehmen können.

Die Verletzung der ärztlichen Schweigepflicht ist durch § 203 Abs. 1 sowie 3 bis 5 StGB strafbewehrt. Der hohe Stellenwert der ärztlichen Schweigepflicht kommt auch darin zum Ausdruck, dass dem Arzt in Straf- oder Zivilprozessen ein Zeugnisverweigerungsrecht zusteht, er also auch vor Gericht in diesen Fällen die Verschwiegenheit wahren kann, § 53 Abs. 1 Nr. 3 StPO und § 383 Abs. 1 Nr. 6 ZPO. Dem Zeugnisverweigerungsrecht des Arztes steht zusätzlich auch ein ausdrückliches Beschlagnahmeverbot zur Seite, § 97 StPO. Damit ist es den Strafverfolgungsbehörden verwehrt, die im Besitz eines Arztes befindlichen Krankengeschichten, Untersuchungsbefunde und anderen Unterlagen mit Angaben über Patienten zu beschlagnahmen. Für Gegenstände in Krankenhäusern besteht eine Spezialregelung in § 97 Abs. 2 StPO, da sich die Unterlagen regelmäßig nicht im Gewahrsam eines einzelnen Arztes befinden.

Für Patientendaten/-unterlagen außerhalb eines Krankenhauses, an denen das Krankenhaus keinen Gewahrsam mehr hat, besteht kein Schutz vor Beschlagnahme. Beim Outsourcing der Patientenaktenvernichtung wird der jeweilige Patient, also der Betroffene, somit schlechter gestellt, als beim Vernichten der Unterlagen im Krankenhaus.
Innerhalb des Krankenhauses könnten die Mitarbeiter des Krankenhausarchives die Tätigkeit der Aktenvernichtung unproblematisch vornehmen. Sie sind in ihrem jeweiligen Bereich selbst und strafrechtlich gebunden für die Wahrung der Schweigepflicht verantwortlich (§ 203 Abs. 3 S. 2 StGB), weshalb es ihnen gegenüber zu keiner Verletzung der Offenbarungspflicht kommen kann. Voraussetzung für eine solche Gehilfentätigkeit ist, dass diese Mitarbeiter rechtlich direkt im Rahmen der Krankenhausorganisation gegenüber der ärztlichen Leitung weisungsgebunden sind. Angehörige von Fremdfirmen können grundsätzlich keine Gehilfen sein.

Es wird beim Outsourcing des Bereiches Patientenaktenvernichtung eine unterstützende Hilfstätigkeit im Bereich der Datenverarbeitung ausgelagert, für die die Regelungen der Auftragsdatenverarbeitung (§ 11 BDSG oder § 8 DSG-LSA) geschaffen wurden. Dabei stellt der Datenfluss zwischen Auftragnehmer und Auftraggeber rechtlich zwar keine Datenübermittlung, sondern eine sonstigen Art der Datenweitergabe dar, die als Datennutzung anzusehen ist. Dennoch findet mit dieser Datenweitergabe eine Offenbarung im Sinne des Strafgesetzbuches statt, die einer besonderen Befugnis bedarf. Die Regeln zur Auftragsdatenverarbeitung sind keine ausreichende Befugnisnorm, weil darin der besondere Schutz des Patientengeheimnisses keine genügende Berücksichtigung findet (s.o.).

Da die gesetzlich geregelten Offenbarungspflichten nur soweit reichen, wie der Gesetzeszweck es jeweils erfordert und die zu offenbarenden Daten im Gesetz benannt sind, dürfen keine darüber hinausgehenden Daten offenbart werden. Patientenakten unterliegen gerade keiner Offenbarungspflicht. Daher gibt es keine gesetzliche Befugnis, die deren Weitergabe zum outgesourcten Bereich ermöglicht, ohne dass die Ärzte gegen die ärztliche Schweigepflicht verstoßen.

Aus diesem Grund besteht zunächst allein die Möglichkeit, die ausgelagerte Vernichtung der Patientenakten durch Einholung von Einwilligungserklärungen der Patienten zu erreichen. Werden die Anforderungen an eine wirksame Einwilligung beachtet, so kann eine Auslagerung, mit der eine Offenbarung von Patientendaten verbunden ist, erfolgen. Grundsätzlich setzt eine wirksame Einwilligung voraus, dass der Patient weiß, wem erlaubt wird, welche Daten zu welchem Zweck zu verarbeiten. Die Erklärung muss freiwillig erfolgen, über etwaige Folgen der Nichteinwilligung ist der Patient zu informieren. Ferner ist zu beachten, dass

die Einwilligung grundsätzlich mit Wirkung für die Zukunft widerrufbar ist. Regelungen zur Einwilligung sind in § 4a BDSG und § 4 Abs. 2 und 3 DSG-LSA normiert. Gewöhnlich ist die Einholung einer Einwilligung von jedem Patienten jedoch nicht praktikabel, zumal mutmaßliche oder konkludente Einwilligungen keine Wirksamkeit entfalten.

Da somit im Regelfall sowohl eine gesetzliche Offenbarungsbefugnis als auch eine Einwilligung des Patienten fehlt, kann sich der Arzt durch eine Weitergabe von Patientendaten strafbar machen. Das gilt allerdings nur, wenn bei der Beauftragung Dritter tatsächlich eine Offenbarung von Patientendaten erfolgt. Dies kann vermieden werden, wenn die im Auftrag verarbeiteten Daten anonymisiert bzw. pseudonymisiert übertragen werden, also der Bezug auf einen Patienten fehlt und nicht ohne besonderen Aufwand wieder herzustellen ist. Anonymisierung und Pseudonymisierung sind in den §§ 3 Abs. 6 und 6a BDSG und 2 Abs. 7 und 7a DSG-LSA ausdrücklich geregelt.
Erfolgt also eine wirksame Verschleierung der Identität der Betroffenen, so können die damit verbundenen Patientendaten weitergegeben und folglich die Aufgabe der Aktenvernichtung an Dritte übertragen werden.
Natürlich kann auch durch sonstige technische und organisatorische Maßnahmen bei einer Aufgabenauslagerung eine unbefugte Kenntnisnahme ausgeschlossen werden. An solche Maßnahmen werden allerdings hohe Anforderungen gestellt. Zudem ist dann auch weiterhin eine staatsanwaltliche Beschlagnahmung der Unterlagen möglich, nach der eine Zuordnung der personenbezogenen Daten erfolgen kann.

Die Auslagerung der Aktenvernichtung ist also nur dann möglich, wenn eine unbefugte Kenntnisnahme durch Dritte, also insbesondere durch die Mitarbeiter der Entsorgungsfirma, nicht stattfinden kann. Erst wenn das gewährleistet ist, kommt die Ausgestaltung eines entsprechenden Vertrages zur Auftragsdatenverarbeitung zum Tragen.

## 4.7 Videoüberwachung

### 4.7.1 Allgemeine Rechtslage

Aus der Praxis ist bekannt, dass die unterschiedlichsten Fälle von Videoüberwachung aus den verschiedensten Beweggründen existieren. Das Bundesdatenschutzgesetz enthält für nicht-öffentliche Stellen in § 6 b BDSG eine gesetzliche Regelung hinsichtlich der Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen. Der Begriff „öffentlich zugänglicher Raum“ umfasst nach allgemeinem Verständnis alle Bereiche, in de-

nen sich jedermann berechtigterweise ohne jede Zugangsschranke aufhalten und bewegen darf. § 6 b BDSG ist daher immer anwendbar, wenn von den Kameras der Straßenraum, Gehwege oder andere für jedermann frei zugängliche Flächen erfasst werden, unabhängig davon, ob es sich um eine reine Beobachtung handelt oder ob zusätzlich eine Aufzeichnung stattfindet.
Kein Fall des § 6 b BDSG sind alle Videobeobachtungen und –aufzeichnungen, die innerhalb geschlossener Räumlichkeiten in privaten Wohnanlagen oder Mietobjekten durchgeführt werden, also etwa in Hausfluren, privaten Tiefgaragen, Fahrstühlen etc.. Allerdings gilt das nur dann, wenn für den Betroffenen erkennbar ist, dass er sich im besonders geschützten (privaten) Bereich einer anderen Person und nicht auf öffentlichen zugänglichen Flächen befindet.

Kommt § 6 b BDSG zur Anwendung, ist eine Videoüberwachung nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Der Umstand der Beobachtung und die hierfür verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen. Auch die Verarbeitung und Nutzung so gewonnener Daten, hierzu zählt auch die Aufzeichnung, sowie die zweckveränderte Verwendung und die Löschung der Daten werden durch § 6 b BDSG an enge Voraussetzungen geknüpft.

Aber auch wenn § 6 b BDSG nicht zur Anwendung kommt, ist nicht etwa alles erlaubt oder möglich. Es gelten dann die zivilrechtlichen Regelungen zum Schutz des allgemeinen Persönlichkeitsrechts, die durch zahlreiche Gerichtsentscheidungen ausgestaltet worden sind und dem Betroffenen auch Unterlassungsansprüche einräumen. Niemand muss es hinnehmen, dass sein Kommen und Gehen ebenso wie das seiner Besucher vom Nachbarn oder der Hausverwaltung mittels Videoanlage permanent beobachtet oder aufgezeichnet wird. So hat das Kammergericht Berlin in einem Beschluss vom 26. Juni 2002 einen unzulässigen Eingriff in das Persönlichkeitsrecht der Mitbewohner darin gesehen, dass über ein „Videoauge“ im Klingeltableau jeder Bewohner jederzeit den Hausflur über sein Fernsehgerät beobachten und Videoaufzeichnungen herstellen und auswerten kann, auch wenn bei ihm selbst nicht geklingelt worden ist.
Da es sich bei den ergangenen Urteilen aber um Einzelfallentscheidungen handelt und außerhalb des BDSG konkrete Schutznormen fehlen, kann an dieser Stelle nicht auf einen Katalog allgemeingültiger Regeln im Hinblick auf eine Zulässigkeit der Videoüberwachung verwiesen werden. Dennoch sind folgende Hinweise zu beachten:

Sehr wichtig ist die Transparenz der Videoüberwachung für die von ihr Betroffenen, d.h. es muss für jedermann ersichtlich sein, dass der von ihm betretene Bereich videoüberwacht wird. Verdeckte Videoüberwachung ist in jedem Fall ein nicht hinnehmbarer Eingriff in die Persönlichkeitsrechte des Betroffenen. Auch die Zwecke der Videobeobachtung müssen klar definiert sein, ebenso wie die Personen, die gegebenenfalls Zugang zu Bildschirmen oder Aufzeichnungen haben. Im Vorfeld einer beabsichtigten Videoüberwachung sollte in jedem Fall der Konsens mit allen Betroffenen hergestellt werden. Hinsichtlich der Zwecke, Nutzungen und Löschung der Aufzeichnungen sollten eindeutige schriftliche Regelungen getroffen werden.

### 4.7.2 Videoüberwachung im Kaufhaus

Zur Videoüberwachung ist der Aufsichtsbehörde für den Datenschutz im aktuellen Tätigkeitszeitraum nur eine Beschwerde zugegangen. Der Betroffene gab an, in einem Geschäft beim Bezahlen mit ec-Karte während der PIN-Eingabe gefilmt worden zu sein. Gespräche mit der Geschäftsführung hinsichtlich der Zulässigkeit dieser Verfahrensweise hätten keinen Erfolg erzielt, so dass er eine Überprüfung aus datenschutzrechtlicher Sicht wünsche.

Das entsprechende Unternehmen verneinte einen Verstoß gegen datenschutzrechtliche Bestimmungen und bat die Aufsichtsbehörde, die verfahrensgegenständliche Videoüberwachung vor Ort in Augenschein zu nehmen.

Im Verlauf dieser Vor-Ort-Besichtigung wurden folgende Aspekte überprüft:
- Zulässigkeit der Beobachtung mit optisch-elektronischen Einrichtungen
- Art der Beobachtung
- weitergehende technische Gestaltung der eingesetzten technischen Einrichtungen
- Feststellung der die Beobachtung durchführenden Stelle
- Kenntlichmachung der Beobachtung
- Feststellung, unter welchen Umständen die Aufzeichnung erfolgt
- Regelungen hinsichtlich der Löschung der personenbezogenen Daten

Insgesamt zeigte die Überprüfung, dass die Beobachtung in den Geschäftsräumen des Unternehmens den Rahmen der gesetzlichen Vorschriften einhält. Alleiniger Grund einer Beanstandung war der beim Betreten des Geschäfts nur bedingt ersichtliche Hinweis auf die Videobeobachtung. Die Geschäftsleitung sicherte unverzügliche Nachbesserung durch Anbringen eines deutlich größeren Hinweisschildes zu.

Bei einer neuerlichen Inaugenscheinnahme der Geschäftsräume musste leider festgestellt werden, dass die zugesagte verbesserte Ausschilderung nicht vorgenommen wurde.

Gleichzeitig erhielt die Aufsichtsbehörde Kenntnis davon, dass ein ebenfalls im Gebäude ansässiges Geschäft, seine in der Vergangenheit mustergültige Kennzeichnung der Videoüberwachung inzwischen ersatzlos entfernt hat. Aus diesem Grund wurden beide Unternehmen durch die Aufsichtsbehörde angeschrieben. Die Verfahren dauern über das Ende des Berichtszeitraumes an.

# 5. Technische Aspekte des Datenschutzes

## 5.1 Radio Frequency Identification (RFID) – Funktionschip für jede Gelegenheit?

Die Radio Frequency Identification bezeichnet eine Mikrochiptechnologie zur kontaktlosen Speicherung von Daten. Diese werden mittels einer Funkübertragungstechnik abgefragt und mit Energie versorgt. Die im Sprachgebrach oft nur mit „Tags“ bezeichneten Chips gelten bisher als attraktive Ergänzung zur Strichcodetechnologie, bekannt durch Etiketten oder Aufdrucke auf Lebensmitteln und Konsumgütern. Zudem finden sie z.B. bei der Zugangs- und Diebstahlsicherung, bei der Kennzeichnung von Tieren oder in der Automobilindustrie bei Wegfahrsperren Anwendung. Gegenüber den noch im Handel verbreiteten Barcodes können mit RFID-Chips deutlich mehr Informationen über Produkte gespeichert und zusätzlich vollautomatisch und ohne Sichtkontakt ausgelesen werden.

Schon in naher Zukunft sollen RFID den heutigen Strichcode verdrängen und in vielen Bereichen des täglichen Lebens Einzug halten. Aktuell ist z.B. geplant, RFID u.a. auch zur Speicherung biometrischer Merkmale in Reisepässen oder zur Fälschungssicherung einzusetzen. Die Befürchtungen sind deshalb groß, dass z.B. das Einkaufsverhalten von Kunden durch die an mitgeführten Gegenständen angebrachten RFID mit einer eindeutigen Seriennummer ausgeforscht und auf diese Weise unbemerkt detaillierte Kauf- und Bewegungsprofile erstellt werden.

Daraus ergibt sich, dass bei der großflächigen Einführung von RFID-Chips im Handel Aufklärungs- und Schutzmaßnahmen für Bürger/innen notwendig sind, da die Gefahr besteht, mit dem entsprechenden System personenbezogene Daten zu speichern, ohne die Verarbeitungsvorgänge ausreichend transparent zu gestalten. Zudem könnten sogar Dritte die Daten auslesen oder verändern, ohne dass der Nutzer dies bemerkt oder unterbinden kann. Aus

Sicht des Datenschutzes muss der Einsatz von RFID also für die Betroffenen eindeutig nachvollziehbar erfolgen. Nur durch einen transparenten Umgang mit dieser Technologie kann zukünftig die in den Datenschutzgesetzen geforderte Zweckbindung, Datensparsamkeit und Vertraulichkeit bei der Verarbeitung personenbezogener Daten sichergestellt werden. Unzulässig wäre es, wenn RFID-Tags versteckt angebracht und verdeckt ausgelesen werden und Daten der RFID-Chips aus verschiedenen Produkten mit personenbezogenen Daten zusammengeführt oder Verhaltens-, Nutzungs- und Bewegungsprofile erzeugt und gespeichert werden.
Die Verwendung von RFID-Chips im Handel ist also dann datenschutzrechtlich relevant, wenn eine Verknüpfung mit personenbezogenen Daten hergestellt wird.

*Quelle: 20. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz für 2003-2004*

Weiterführende Informationen zu RFID finden Sie auf der nachfolgenden Internetseite der Art.29-Datenschutzgruppe der Europäischen Union:
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_de.pdf

### 5.2 Funknetze (WLAN) im täglichen Einsatz

Die mobile Nutzung elektronischer Dienste (E-Mail, Internet, Personal Digital Assistents) ist heute gängige Praxis. Dabei gehen die Möglichkeiten weit über das einfache Telefonieren hinaus. So können Handys E-Mails senden und empfangen, über Notebooks ist vielerorts der Zugang ins Internet eröffnet oder Personal Digital Assistents leiten Autofahrer und Fußgänger durch Straßennetze.
Notwendige Basis für die meisten der mobil nutzbaren Dienste ist eine Vernetzung der Telekommunikationsgeräte. Dafür existieren neben den Mobilfunknetzen für die Telefonie (GSM, GPRS) zunehmend andere Technologien für die lokal begrenzte Kommunikation, darunter Wireless Local Area Network (WLAN), auf welches hier näher eingegangen wird.

Der Vorteil der drahtlosen Kommunikationsinfrastruktur, also die Erhöhung von Komfort, Effizienz und die Flexibilität bei der Nutzung, ist unbestritten. Leider ist die Verbesserung von Mobilität und Flexibilität oft mit einem Sicherheitsverlust für die via Funk übertragenen Daten sowie die drahtgebundenen Netze, an die die Funkkomponenten angeschlossen sind, verbunden. Zudem besteht die Gefahr von Verlust oder Diebstahl mobiler Endgeräte und somit der darauf gespeicherten Daten.

Für den Datenschutz und die Datensicherheit ist der Vorteil der drahtlosen Kommunikation also gleichzeitig eine Gefahr: Es besteht keine direkte physikalische Verbindung der Geräte untereinander; sie sind Teilnehmer an einem offenen Medium. Offen bedeutet dabei, dass eine räumliche Begrenzung auf bestimmte Bereiche, z.B. nur die Geschäftsräume eines Unternehmens, nahezu unmöglich ist, da sich Funkwellen unkontrolliert und unbegrenzt ausbreiten. So ist bei einem Gebäude, dass mit der Funkinfrastruktur komplett „ausgeleuchtet" ist, mit an Sicherheit grenzender Wahrscheinlichkeit auch immer außerhalb des Gebäudes ein Empfang von Funkwellen möglich.
Ist das der Fall, sind zahlreiche Angriffsszenarien denkbar. So sind Denial-of-Service-Attacken (DoS-Attacken) in ungeschützten Funknetzen relativ einfach durchführbar, ebenso wie Man-in-the-middle-Attacken, bei denen durch geschickte Positionierung von Funkkomponenten echte Gegenstellen vorgegaukelt werden und dadurch z.B. die Datenübertragung zu bestimmten Netz-Segmenten protokolliert oder blockiert werden kann. Große Sicherheitsrisiken bestehen bereits, wenn Geräte „Out-Of-The-Box" eingesetzt werden, also ohne Anpassung der Konfiguration und mit „Default"-Passwörtern. Entsprechende Angriffswerkzeuge und Informationen darüber, wie diese einzusetzen sind, können sogar leicht aus dem Internet heruntergeladen werden.

Insgesamt ist festzustellen, dass sich Nutzer entsprechender Funknetze nicht auf die im jeweiligen Standart definierten Sicherheitsmechanismen verlassen sollten. Die voreingestellten Sicherheitseinstellungen der Geräte reichen in der Regel nicht aus, um sich wirksam gegen Angreifer zu sichern.
Nachfolgend werden einige Hinweise gegeben, wie Sie sich und damit Ihre Daten vor Angriffen schützen können und im Hinblick auf den Datenschutz auch sollten:

- Standard-Netzwerknamen ändern
- Standard-Passwort an allen Komponenten ändern
- MAC-Adress-Filterung einschalten
- WEP Verschlüsselung mit maximaler Schlüssellänge einschalten und Schlüssel periodisch wechseln
- Sendeleistung an Access-Point optimieren
- DHCP-Server am Access-Point abschalten
- Funk-LAN-Komponenten nur bei Gebrauch einschalten
- Konfiguration des Access-Point nur über sichere Kanäle (SSL benutzen)
- Zusätzliche Verschlüsselung (VPN-Tunnel) verwenden
- Einsatz eines Authentifikations-Servers (Radius-Server)
- Alle Clients vor Computerviren schützen

*Quelle: 20. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz für 2003-2004*

Weiterführende Informationen erhalten Sie auf der Internetseite des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ des Bundes und der Länder.

### 5.3 USB–Sticks und ihre Gefahren

Praktisch ist jeder derzeit verkauft PC ausschließlich mit Universal Serial Bus (USB)-Schnittstellen ausgestattet, über die externe Geräte wie Tastatur, Maus und Arbeitsplatzdrucker angeschlossen werden. Mit dem USB-Anschluss steht dem Benutzer also in der Regel ein universeller Anschluss für eine Vielzahl von Hardwarekomponenten zur Verfügung. Die Betriebssystemunterstützung ist grundsätzlich so ausgelegt, dass USB-Geräte vom PC selbständig erkannt werden und sofort betriebsbereit sind.

Eine Sicherheitsrelevanz ergibt sich insbesondere für Netzwerkadapter, Modems oder ISDN-Adapter, da mit ihnen unerlaubte „Seiteneingänge“ in das betriebliche Netz geschaffen werden können, die die zentralen Sicherheitseinrichtungen unterlaufen. Auch die über USB anschließbaren Speichermedien – memory sticks – bergen Sicherheitsrisiken in sich.

Kritisch im Falle der memory sticks ist das unzulässige Speichern schutzwürdiger Daten auf ihnen, die mit ihrer Hilfe mögliche Einschleusung nicht freigegebener Programme in das dienstliche System oder ihre Nutzung zum Start von Betriebssystemen, mit denen Sicherheitsmechanismen unterlaufen werden können. Auch mobile Festplatten, mit einer Speicherkapazität von bis zu 200 GB, sind auf dem Markt erhältlich und über solche Geräte lassen sich sogar ganze Datenbanken aus dem System kopieren.

Neben den Risiken eröffnet diese Technik aber auch Möglichkeiten für die Datensicherheit. So kann es sinnvoll sein, besonders vertrauliche Datenbestände auf memory sticks oder USB-Festplatten zu speichern und diese dann entsprechend zu verwahren.
Als Sicherungsmaßnahmen kommen viele Mittel in Betracht. So kann der physische Zugriff auf derartige Medien auf einfache Weise eingeschränkt werden, um so die Chancen eines potentiellen Angreifers zu vermindern. Auch die Authentifizierung und damit der Zugang zum Rechner kann über den USB-Anschluss technisch abgesichert werden. Grundsätzlich sollte beim Einsatz von USB-Sticks oder USB-Festplatten die Speicherung immer verschlüsselt erfolgen, um bei Verlust des Mediums unbefugte Zugriffe zu verhindern.

*Quelle: 20. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz für 2003-2004*

Weiterführende Informationen erhalten Sie auf der Internetseite des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ des Bundes und der Länder in der Orientierungshilfe „Datensicherheit bei USB-Geräten“:
http://www.bfd.bund.de/technik/usb.pdf

# 6 Wissenswertes für den Alltag

## 6.1 Werbewiderspruch

Hat die verantwortliche Stelle für eigene Belange Daten für einen bestimmten Zweck erhoben und gespeichert, ist deren Übermittlung oder Nutzung für Zwecke der Werbung, der Markt- und Meinungsforschung sind, zulässig, wenn es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf:

- eine Angabe über die Zugehörigkeit des Betroffenen zu dieser Personengruppe,
- Berufs-, Branchen- oder Geschäftsbezeichnung,
- Namen,
- Titel,
- akademischer Grad,
- Anschrift und
- Geburtsjahr beschränken

und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat.

Diese Erleichterung im Umgang mit personenbezogenen Daten wird durch das Widerspruchsrecht des Betroffenen kompensiert.
Um sich vor unerwünschter zielgerichteter Werbung schützen zu können, wurde den Betroffenen nämlich ein uneingeschränktes Widerspruchsrecht gegenüber der verantwortlichen Stelle bezüglich der Nutzung oder Übermittlung ihrer Daten zu Zwecken der Werbung oder Markt- und Meinungsforschung, d.h. der unmittelbaren diesbezüglichen Ansprache, eingeräumt. Von diesem Widerspruchsrecht ist jedoch nur die Werbung zum Zwecke des Direktmarketings erfasst.

Da das Bundesdatenschutzgesetz keine Ausführungen hinsichtlich der Form des Widerspruches macht, genügt bereits ein Telefonanruf, damit ein entsprechender Widerspruch wirksam

wird. Auch konkludente Äußerungen kommen zum Tragen, z.B. durch den Vermerk „Annahme verweigert“ auf einem Werbeschreiben. Eine kurze schriftliche Mitteilung (als Fax oder E-Mail) ist dem Betroffenen jedoch zu empfehlen, bietet sie doch die größte Gewähr, dass der Widerspruch sein Ziel erreicht. Der Widerspruch muss der verantwortlichen Stelle gegenüber geäußert werden. Dies ist, wenn für den Betroffenen der Werbende nicht ersichtlich ist, auch der Versender der Werbung.
Darüber hinaus besteht für die Betroffenen, die keine adressierte Werbung wünschen, die Möglichkeit, sich in die sog. Robinsonliste, eine vom Deutschen Direktmarketing Verband für die Mitgliedsfirmen geführte Sperrliste, eintragen zu lassen.

Das entsprechende Antragsformular kann unter folgender Anschrift angefordert werden:

Deutscher Direkt-Marketing-Verband
- Robinson-Liste –
Postfach 14 01
71243 Ditzingen
Telefon: 07156 / 95 10 10

Allerdings besteht nicht für jede verantwortliche Stelle die Pflicht, vor einer Nutzung oder Übermittlung personenbezogener Daten diese anhand der Listeneinträge zu überprüfen. Lediglich bei der Vermarktung von Adressen dürfen nur solche Datensätze von Adresshändlern eingesetzt werden, die nicht in der Robinsonliste erfasst sind.

Darüber hinaus besteht für die verantwortliche Stelle bzw. die Stelle, welche die werbende Ansprache durchführt, eine Belehrungs- und Informationspflicht gegenüber dem Betroffenen. Der Betroffene ist bei der werbenden Ansprache über sein Widerspruchsrecht und über die Stelle, gegenüber der das Widerspruchsrecht ausübt werden kann, zu informieren. Diese Belehrung muss zwar nicht den Gesetzestext wiederholen, jedoch eindeutig zum Ausdruck bringen, dass dem Wunsch, nicht mehr beworben zu werden, Rechnung getragen wird. Der Hinweis hat vor oder zumindest gleichzeitig mit der werbenden Ansprache zu erfolgen und sollte zumindest so sichtbar gemacht werden, dass er nicht erfahrungsgemäß überlesen wird.
Der Verstoß gegen diese Unterrichtungspflicht ist nach § 43 Abs. 1 Nr. 3 eine Ordnungswidrigkeit, wenn er vorsätzlich oder fahrlässig begangen wurde. Derartige Fälle ahndet die Aufsichtsbehörde.

## 6.2 Eintrag im Telefonbuch

Telefonbücher sind in der Praxis ein gutes Instrument, um eine Person ausfindig zu machen. Häufig schaut man im gedruckten oder elektronischen Telefonbuch nach oder ruft die Auskunft an. Nicht selten findet man auf diesem Weg sogar die Anschrift der gesuchten Person. *Im Telefonbuch zu stehen, kann aber auch unangenehm sein,* da man von jedem angerufen werden kann, unter Umständen ein großer Personenkreis die eigene Anschrift aus diesem Verzeichnis erfährt.

Daher sollte man folgende Dinge beachten:

- Im Telefonbuch steht man freiwillig, d.h. jeder Teilnehmer bestimmt durch seinen Antrag beim Netzbetreiber, ob und mit welchen Angaben er im Telefonbuch eingetragen werden möchte.
- Eine Auskunft über seine Rufnummer kann der Teilnehmer unterbinden, indem er bei seinem Netzbetreiber gegen die Veröffentlichung Widerspruch einlegt. Ohne ausdrückliche Einwilligung eines Teilnehmers darf keine Auskunft über die Daten erteilt werden.
- Seit Ende Juni 2004 ist es der Auskunft erlaubt, bei Nennung einer Rufnummer den Namen und die Anschrift des gesuchten Anschlussinhabers mitzuteilen (sogenannte Inverssuche). Voraussetzung hierfür ist, dass sich der Teilnehmer mit diesen Angaben in das Telefonbuch hat eintragen lassen. Dieser Inverssuche kann man ebenfalls bei seinem Netzbetreiber widersprechen.

Für die Datenschutzkontrolle des Netzbetreibers ist der Bundesbeauftragte für den Datenschutz zuständig. Die Aufsicht über die Netzbetreiber liegt bei der Regulierungsbehörde für Telekommunikation und Post.

# 7 Ausblick

## 7.1 Überprüfungen vor Ort

Im Berichtszeitraum beschränkte sich die Prüftätigkeit vor Ort vornehmlich auf Beschwerdefälle, in denen die Sachverhaltsaufklärung anderweitig nicht möglich war.

Das Landesverwaltungsamt beabsichtigt jedoch im folgenden Berichtszeitraum, die Vorortkontrollen auszuweiten. Dann werden verstärkt anlassbezogene Vorortprüfungen stattfinden, aber auch anlasslose Überprüfungen vorgenommen werden.

## 7.2 Bußgeldverfahren

Bereits mit der Änderung des Bundesdatenschutzgesetzes wurde der Katalog der Ordnungswidrigkeiten verändert. Verstöße gegen formale Vorschriften sind mit einem Bußgeld von bis zu 25.000,- € bewehrt. Auch Verstöße gegen materielles Datenschutzrecht werden geahndet, so ist eine unzulässige Datenverarbeitung mit einem Bußgeld von bis zu 250.000,- € bedroht.

In der Aufsichtsbehörde des Landes Sachsen-Anhalt wurden im Berichtszeitraum keine Bußgeldbescheide erlassen. Allerdings wurden aufgrund von drei Verstößen gegen materielles Datenschutzrecht Bußgeldverfahren eingeleitet. In mindestens zwei weiteren Verfahren liegt eine zu ahndende Ordnungswidrigkeit wegen unterlassener Auskunft gegenüber der Aufsichtsbehörde vor.

In den Fällen, in denen gegen materielles Datenschutzrecht verstoßen wurde, wurde die Aufsichtsbehörde aufgrund von Beschwerden tätig. Diese betrafen die Übermittlung von Bankdaten durch eine Bank an einen Finanzdienstleister und die Veröffentlichung von Daten (Name, Anschrift, Geburtsdatum) durch öffentliches Aushängen von Hausverboten. Nachdem die betroffenen Unternehmen unter Mitteilung der Sach- und Rechtslage um eine Stellungnahme gebeten wurden und die Aufsichtsbehörde dargelegt hat, worin der datenschutzrechtlich relevante Verstoß lag, sind inzwischen auch die Anhörungen im Hinblick auf die festgestellten Ordnungswidrigkeiten nahezu abgeschlossen. Der Erlass entsprechender Bußgeldbescheide steht nunmehr aus.

### 7.3 Internetpräsenz

Die von der Aufsichtsbehörde im Internet bereitgestellten Informationen erhalten Sie über die Internetseite des Landesverwaltungsamtes Sachsen-Anhalt (www.landesverwaltungsamt.sachsen-anhalt.de).
In der oberen rechten Ecke auf der Startseite des Landesverwaltungsamtes befindet sich das Schnellsprungmenü. Sobald Sie den Mauszeiger auf dieses Menü bewegen, öffnet sich eine Liste. Der dort eingestellte Link „Datenschutz“ führt Sie zur Seite der Aufsichtsbehörde.

Alternativ gelangen Sie über die Internetadresse www.lvwa.sachsen-anhalt.de/datenschutz direkt zum Internetauftritt der Aufsichtsbehörde.

Auch durch Eingabe des Suchbegriffes „Datenschutz“ auf der Internetseite des Landesverwaltungsamtes finden Sie zu uns.

Eine verbesserte Internetpräsenz wird derzeit erarbeitet. Dann wird sich die im Landesverwaltungsamt Sachsen-Anhalt ansässige Aufsichtsbehörde im Netz noch schneller ausmachen lassen. So soll zukünftig das Landesverwaltungsamt mit den Suchbegriffen „Datenschutz“ und „Sachsen-Anhalt“ über Suchmaschinen auffindbar sein.

Auch inhaltlich wird sich das Angebot für die Besucher der Seite erweitern. Neben allgemeinen Hinweisen zum Datenschutz, z.B. der Unterscheidung zwischen dem nicht-öffentlichen und dem öffentlichen Bereich und der Mitteilung der Ansprechpartner für Anfragen und Beschwerden, werden Sie dort auch wichtige Neuigkeiten im Bereich Datenschutz sowie Merkblätter über solche datenschutzrechtlichen Fragen vorfinden, welche vermehrt an die Aufsichtsbehörde herangetragen wurden. Unser Anliegen ist es hierbei, den bestehenden Beratungsbedarf auf möglichst einfachem und schnellem Wege zu decken.

## Hier sind wir erreichbar

**1 Hauptsitz**
Willy-Lohmann-Straße 7, 06114 Halle (Saale)
Telefon (0345) 514-0

**2 Dienstgebäude Halle**
Ahornweg 30b, 06132 Halle (Saale)
Telefon (0345) 777-9730

**3 Dienstgebäude Halle**
Am Kirchtor 8, 06108 Halle (Saale)
Telefon (0345) 514-0

**4 Dienstgebäude Halle**
An der Fliederwegkaserne 13, 06130 Halle (Saale)
Telefon (0345) 514- 0

**5 Dienstgebäude Halle**
Dessauer Straße 70, 06118 Halle (Saale)
Telefon (0345) 514-0

**6 Dienstgebäude Halle**
Ernst-Kamieth-Straße 2, 06112 Halle (Saale)
Telefon (0345) 514-0

**7 Dienstgebäude Halle**
Maxim-Gorki-Straße 7, 06114 Halle (Saale)
Telefon (0345) 5276-0

**8 Dienstgebäude Halle**
Maxim-Gorki-Straße 13, 06114 Halle (Saale)
Telefon (0345) 514-0

**9 Dienstgebäude Halle**
Neustädter Passage 15, 06122 Halle (Saale)
Telefon (0345) 6912-0

**10 Dienstgebäude Dessau**
Kühnauer Straße 161, 06846 Dessau
Telefon (0340) 6506-0

**11 Dienstgebäude Magdeburg**
Halberstädter Straße 39 a, 39112 Magdeburg
Telefon (0391) 627-3000

**12 Dienstgebäude Magdeburg**
Olvenstedter Straße 1-2, 39108 Magdeburg
Telefon (0391) 567- 02

Landesverwaltungsamt
Willy-Lohmann-Straße 7
06114 Halle (Saale)
Telefon: (0345) 514-0

www.landesverwaltungsamt.sachsen-anhalt.de