SACHSEN-ANHALT

Landesverwaltungsamt

Dritter Tätigkeitsbericht

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

Berichtszeitraum: 01.06.2005 bis 31.05.2007

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 Arbeitsmarktförderung · Kommunaler Service · Kommunalaufsicht · 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

Inhaltsverzeichnis

1 Einführung 3

1.1 Datenschutz allgemein – Abgrenzung zwischen nicht-öffentlichem und öffentlichem Bereich 3

1.2 Aufgaben einer Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich 5

1.3 Zielstellung eines Tätigkeitsberichtes 5

2 Das Bundesdatenschutzgesetz 6

2.1 Änderung des Bundesdatenschutzgesetzes 6

2.1.1 Die Novelle im Überblick – Gegenüberstellung der Rechtslagen 6

2.1.2 Die Novelle im Detail 9

2.2 Die Rechte der Betroffenen nach dem Bundesdatenschutzgesetz 10

3 Datenschutz im nicht-öffentlichen Bereich des Landes Sachsen-Anhalt 13

3.1 Allgemeines zur Aufsichtstätigkeit 13

3.1.1 Ansprechpartner und Internetpräsenz 13

3.1.2 Eingaben, Anlasskontrollen 14

3.1.3 Beratung von Bürgern, Unternehmen und betrieblichen Datenschutzbeauftragten 14

3.1.4 Ordnungswidrigkeitenverfahren 15

3.2 Zahlenmäßiger Überblick über die Tätigkeit der Aufsichtsbehörde 15

4 Einzelne Tätigkeitsbereiche aus Anfragen und Beschwerden 19

4.1 Von Beratungsinteresse – ausgewählte Aspekte der Anfragen 19

4.1.1 Telefongespräche 19

4.1.2 Optisch-elektronische Einrichtungen ... 22

4.1.3 Kundenbindung ... 25

4.1.4 Unerwünschte E-Mail-Werbung (sogenannte SPAM-Mails) und Schutz vor Viren ... 27

4.1.5 Erhebung personenbezogener Daten mittels Fragebogen ... 29

4.1.6 Übermittlung personenbezogener Daten an einen Dritten ... 34

4.2 Was ist zulässig und was nicht – ausgewählte Beschwerdeverfahren ... 37

4.2.1 Erhebung von Arbeitnehmerdaten ... 37

4.2.2 Videoüberwachung in Geschäften ... 40

4.2.3 Auskunfteien ... 44

4.2.4 Übermittlung personenbezogener Daten ... 49

4.2.5 Nutzung personenbezogener Daten für Zwecke der Werbung ... 51

4.2.6 Löschung personenbezogener Daten ... 56

5 Interessantes – Wissenswertes im Bereich des Datenschutzes ... 59

5.1 Scoring ... 59

5.2 Telefonwerbung ... 61

5.3 Whistleblowing-Hotlines ... 63

6 Zusammenfassung und kurzer Ausblick ... 65

1 Einführung

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

In den Formulierungen des Bundesdatenschutzgesetzes (BDSG) wird der Begriff des Datenschutzes nicht explizit verwendet. Aus den Zweckbestimmungen des Gesetzes ergibt sich jedoch, dass „der Datenschutz“ den Einzelnen vor **Beeinträchtigungen** seines **Persönlichkeitsrechts**, die aus dem Umgang mit seinen personenbezogenen Daten herrühren können, bewahren soll. Dahinter verbirgt sich das Recht des Einzelnen, frei darüber zu entscheiden, wer seine Daten erhebt, verarbeitet oder nutzt (Recht auf informationelle Selbstbestimmung). Um dies zu können, benötigt jeder Einzelne Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen und die Möglichkeit, sich entsprechend seiner Entscheidung zu verhalten. Dazu ist es für jeden Einzelnen notwendig, darüber informiert zu sein, wer was wann wofür mit den eigenen Daten macht.
Allerdings ist diese Entscheidungsfreiheit dann eingeschränkt, wenn das Allgemeininteresse das Interesse des einzelnen Bürgers an der Verwendung seiner Daten überwiegt. Für derartige Einschränkungen ist jedoch eine gesetzliche Grundlage von Nöten, die sich im Bundesdatenschutzgesetz, aber auch in anderen Vorschriften, die Regelungen zum Datenschutz beinhalten, wie dem Telekommunikationsgesetz oder den Sozialgesetzbüchern, wiederfindet.

Einschränkungen des Persönlichkeitsrechts des Betroffenen können sowohl durch **öffentliche** als auch durch **nicht-öffentliche** Stellen erfolgen.

Öffentliche Stellen sind zunächst sämtliche Behörden des Bundes oder der Länder, aber auch die Organe der Rechtspflege und anderer öffentlich organisierter Einrichtungen ungeachtet ihrer Rechtsform. Darüber hinaus zählen auch nicht-öffentliche Stellen zu den **öffentlichen** Stellen, soweit sie hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen
(§ 2 Abs. 1 – 3 und Abs. 4 Satz 2 BDSG).

Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, sofern sie nicht als öffentliche Stelle anzusehen sind. Für Stellen der Religionsgesellschaften gilt regelmäßig kirchliches Datenschutzrecht.

Die Unterscheidung, ob eine öffentliche oder nicht-öffentliche Stelle personenbezogene Daten erhebt, verarbeitet oder nutzt, ist entscheidend dafür, ob das Bundesdatenschutzgesetz oder eines der Landesdatenschutzgesetze als bereichsübergreifende Gesetze zur Anwendung kommen, soweit es keine spezifische Regelung in einem Fachgesetz gibt.

Im nicht-öffentlichen Bereich kommt das Bundesdatenschutzgesetz zur Anwendung, wenn

- personenbezogene Daten
- von privaten Stellen
- unter Einsatz von Datenverarbeitungsanlagen oder in oder aus nicht automatisierten Dateien

verarbeitet, genutzt oder dafür erhoben werden, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Zwecke.

Unter **personenbezogenen Daten** versteht man nicht nur persönliche Angaben wie Namen, Anschrift, Telefonnummer, Alter oder Familienstand sondern alle Informationen, die über eine bestimmte Person etwas aussagen (z.B. Vermögen, Beruf, Hobby, Gesundheitszustand, Kauf- und Zahlungsverhalten).

Mit der Wortgruppe „für persönliche oder familiäre Tätigkeiten“ wird der Bereich persönlicher Lebensführung von der beruflichen und geschäftlichen Sphäre abgegrenzt. Es soll zum Ausdruck gebracht werden, dass der Umgang mit personenbezogenen Daten im persönlichen Freundes- und Bekanntenkreis nicht besonders geschützt wird. Darüber hinaus führt aber jegliche nach außen gerichtete, also über den persönlichen und familiären Kreis hinausreichende Tätigkeit, zur Anwendbarkeit des Bundesdatenschutzgesetzes.

Das Gesetz zum Schutz personenbezogener Daten (DSG-LSA) dagegen gilt 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 deren Vereinigungen, ungeachtet ihrer Rechtsform (öffentliche Stellen).

Die Einstufung als öffentliche oder nicht-öffentliche Stelle hat Einfluss darauf, welche Institution den Betroffenen beim Schutz des Rechts auf informationelle Selbstbestimmung zur Seite steht.
Über die Einhaltung der datenschutzrechtlichen Bestimmungen durch die öffentlichen Stellen des Landes Sachsen-Anhalt wacht der Landesbeauftragte für den Datenschutz. Soweit nicht-öffentliche Stellen mit personenbezogenen Daten umgehen, obliegt dem Landesverwaltungsamt Sachsen-Anhalt als Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich diese Aufgabe. Ein genauerer Überblick über die zuständigen Aufsichtsbehörden ist der im Anhang beigefügten Darstellung zu entnehmen.

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

Nach § 38 Abs. 1 Satz 1 BDSG kontrolliert die Aufsichtsbehörde im nicht-öffentlichen Bereich die Ausführung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz. Dies gestaltet sich im Wesentlichen über

- die Bearbeitung von Anfragen, Eingaben und Beschwerden,
- die Beanstandung von Datenschutzverstößen,
- die Anordnung zur Beseitigung von Sicherheitsmängeln,
- die Führung des öffentlichen Registers der meldpflichtigen Unternehmen vor allem in Hinblick auf Auskunfteien, Adressenhandelsunternehmen sowie Markt- und Meinungsforschungsinstitute und
- die Durchführung von Bußgeldverfahren.

Seit der Änderung des Bundesdatenschutzgesetzes am 22.08.2006 ist nunmehr gesetzlich normiert, dass die Aufsichtsbehörde die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse berät und unterstützt (§ 38 Abs. 1 Satz 2 BDSG).

Die Aufsichtsbehörde im nicht-öffentlichen Bereich kann sowohl anlassunabhängig als auch anlassbezogen tätig werden. Anlässe können beispielsweise sein: eine Eingabe eines Betroffenen, Anzeigen von Dritten (Interessenverband, Konkurrenzunternehmen, beteiligter Dritter), Informationen von Behörden. In Ausnahmenfällen wird die Aufsichtsbehörde auch auf der Grundlage anonymer Hinweise tätig.

1.3 Zielstellung eines Tätigkeitsberichtes

Mit dem Tätigkeitsbericht soll über die Aktivitäten und Prüfungen der Aufsichtsbehörde für den Datenschutz Aufschluss gegeben werden. Er stellt einen Teil der im Bereich des Datenschutzes notwendigen Öffentlichkeitsarbeit dar. Der Tätigkeitsbericht der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich soll nicht allein Rechenschaft über den Berichtszeitraum ablegen, sondern darüber hinaus auch Aufschluss über die Rechtmäßigkeit bestimmter Sachverhalte geben. Er soll interessierte und betroffene Bürger so informieren, dass diese ihr Recht auf informationelle Selbstbestimmung zukünftig wirkungsvoller wahrnehmen können. Dies ist gerade in Zeiten rasanter Entwicklungen der Technik von wachsender Bedeutung, da die Datenerfassung, Datenhaltung, Datenweitergabe und Datenanalyse immer einfacher wird.

2 Das Bundesdatenschutzgesetz

2.1 Änderung des Bundesdatenschutzgesetzes

Das Bundesdatenschutzgesetz ist zuletzt durch das Erste Gesetz zum Abbau bürokratischer Hemmnisse insbesondere in der mittelständischen Wirtschaft (BGBl. I, S. 1970) geändert worden. Die konkreten Änderungen des Bundesdatenschutzgesetzes sind nachfolgend dargestellt.

2.1.1 Die Novelle im Überblick – Gegenüberstellung der Rechtslagen

Alte Fassung	Neue Fassung
§ 4d Abs. 3 BDSG Die Meldepflicht entfällt ferner, wenn 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 und entweder eine Einwilligung der Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.	**§ 4d Abs. 3 BDSG** Die Meldepflicht entfällt ferner, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei höchstens *neun Personen* mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt und entweder eine Einwilligung der Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient.
§ 4f Abs. 1 Satz 1 BDSG Öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten automatisiert *erheben, verarbeiten oder nutzen*, haben einen Beauftragten für den Datenschutz schriftlich zu bestellen.	**§ 4f Abs. 1 Satz 1 BDSG** Öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten automatisiert *verarbeiten,* haben einen Beauftragten für den Datenschutz schriftlich zu bestellen.
§ 4f Abs. 1 Satz 4 BDSG Die Sätze 1 und 2 gelten nicht für nicht-öffentliche Stellen, die höchstens *vier Arbeitnehmer mit der Erhebung, Verarbeitung oder Nutzung* personenbezogener Daten beschäftigen.	**§ 4f Abs. 1 Satz 4 BDSG** Die Sätze 1 und 2 gelten nicht für die nichtöffentlichen Stellen, die *in der Regel* höchstens *neun Personen ständig mit der automatisierten Verarbeitung* personenbezogener Daten beschäftigen.

§ 4f Abs. 1 Satz 6 BDSG Soweit nicht-öffentliche Stellen automatisierte Verarbeitungen vornehmen, die einer Vorabkontrolle unterliegen oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung oder der anonymisierten Übermittlung *erheben, verarbeiten oder nutzen*, haben sie unabhängig von der Anzahl der *Arbeitnehmer* einen Beauftragten für den Datenschutz zu bestellen.	**§ 4f Abs. 1 Satz 6 BDSG** Soweit nicht-öffentliche Stellen automatisierte Verarbeitungen vornehmen, die einer Vorabkontrolle unterliegen*,* oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung oder der anonymisierten Übermittlung *automatisiert verarbeiten*, haben sie unabhängig von der Anzahl der *mit der automatisierten Verarbeitung beschäftigten Personen* einen Beauftragten für den Datenschutz zu bestellen.
	§ 4f Abs. 2 Satz 2 BDSG (eingefügt) *Das Maß der erforderlichen Fachkunde bestimmt sich insbesondere nach dem Umfang der Datenverarbeitung der verantwortlichen Stelle und dem Schutzbedarf der personenbezogenen Daten, die die verantwortliche Stelle erhebt oder verwendet.*
§ 4f Abs. 2 Satz 3 BDSG – ehemals Satz 2 Mit dieser Aufgabe kann auch eine Person außerhalb der verantwortlichen Stelle betraut werden.	**§ 4f Abs. 2 Satz 3 BDSG** *Zum Beauftragten für den Datenschutz* kann auch eine Person außerhalb der verantwortlichen Stelle bestellt werden; *die Kontrolle erstreckt sich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen.*

	§ 4f Abs. 4a BDSG (neu eingefügt nach Absatz 4) *Soweit der Beauftragte für den Datenschutz bei seiner Tätigkeit Kenntnis von Daten erhält, für die dem Leiter oder einer bei der öffentlichen oder nicht-öffentlichen Stelle beschäftigten Personen aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch dem Beauftragten für den Datenschutz und dessen Hilfspersonal zu. Über die Ausübung dieses Rechtes entscheidet die Person, der das Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann. Soweit das Zeugnisverweigerungsrecht des Beauftragten für den Datenschutz reicht, unterliegen seine Akten und andere Schriftstücke dem Beschlagnahmeverbot.*
	§ 4g Abs. 1 Satz 3 (neu eingefügt nach Satz 2) *Er kann die Beratung nach § 38 Abs. 1 Satz 2 in Anspruch nehmen.*
§ 4g Abs. 2 Satz 2 BDSG *Im Fall des § 4d Abs. 2 macht der Beauftragte für den Datenschutz* die Angaben nach § 4e Satz 1 Nr. 1 bis 8 auf Antrag jedermann in geeigneter Weise verfügbar.	**§ 4g Abs. 2 Satz 2 BDSG** *Der Beauftragte für den Datenschutz macht* die Angaben nach § 4e Satz 1 Nr. 1 bis 8 auf Antrag jedermann in geeigneter Weise verfügbar.
§ 4g Abs. 2 Satz 3 BDSG – gestrichen ~~Im Fall des § 4d Abs. 3 gilt Satz 2 entsprechend für die verantwortliche Stelle.~~	

	§ 4g Abs. 2a BDSG (neu eingefügt nach Abs. 2) *Soweit bei einer nicht-öffentlichen Stelle keine Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz besteht, hat der Leiter der nicht-öffentlichen Stelle die Erfüllung der Aufgaben nach den Absätzen 1 und 2 in anderer Weise sicherzustellen.*
	§ 38 Abs. 1 Satz 2 BDSG (neu eingefügt nach Satz 1) *Sie berät und unterstützt die Beauftragten für den Datenschutz und die verantwortliche Stellen mit Rücksicht auf deren typische Bedürfnisse.*

2.1.2 Die Novelle im Detail

Zentraler Gegenstand der Novellierung des Bundesdatenschutzgesetzes ist die Anhebung des Schwellenwertes für die Meldepflicht bzw. die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten. Konkret wird die Bezugsgröße von 4 auf 9 erhöht und es erfolgt eine Änderung des Begriffes „**Arbeitnehmer**“ in „ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigten **Personen**“. Dies stellt eine begriffliche Klarstellung dar, da die alte Fassung des Bundesdatenschutzgesetzes beide Begriffe verwendete. Es kommt somit nicht darauf an, welchen arbeitsrechtlichen Status die vorgenannten Personen haben, mithin ob sie einen regulären Arbeitsvertrag besitzen oder auf sonstige Weise, z.B. als Freier Mitarbeiter, Auszubildender oder Praktikant, mit der verantwortlichen Stelle verbunden sind. Allerdings wurden die Anwendungsbestimmungen des § 4f BDSG a. F. schon vor der Änderung dahingehend ausgelegt, dass maßgeblich sein sollte, ob die betroffenen Personen Aufgaben erfüllen, die mit der Verarbeitung personenbezogener Daten zusammenhängen, und nicht, ob sie unter formalen Gesichtspunkten als Arbeitnehmer gesehen werden konnten. Aus der Änderung resultiert, dass auch in Vereinen usw. ehrenamtlich Tätige zum Kreis der beschäftigten Personen gehören können. Ob im Rahmen einer Auftragsdatenverarbeitung i. S. v. § 11 BDSG tätige externe Mitarbeiter bei der Bestimmung des Bezugswertes einzubeziehen sind, ist einzelfallabhängig und dürfte grundsätzlich nicht der Fall sein, da Mitarbeiter eines externen Dienstleisters in der Regel nicht „ständig“ für den Auftraggeber tätig sind. Mit der Formulierung „ständig“ wird deutlich, dass Personen, die nur ab und an personenbezogene Daten verarbeiten, wie z.B. während einer Urlaubsvertretung oder auch freie Mitarbeiter, bei der Bestimmung der Bezugsgröße nicht mitzählen. Des Weiteren geht aus „in der Regel“ hervor, dass der Gesetzgeber von einem längeren Beurteilungszeitraum ausgeht und vorübergehende Schwankungen nicht zur Bestellungspflicht eines Beauftragten für den Datenschutz führen sollen.

Zwar könnte es sein, dass es durch die Anhebung der vorgenannten Beschäftigten-Schwellenwerte zu einem Wegfall der Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz führt, doch dies ändert nichts daran, dass die Unternehmen verpflichtet sind, die datenschutzrechtlichen Vorgaben zu beachten. Hierzu bestimmt der in § 4g BDSG neu eingefügte Absatz 2a, dass der Leiter der nicht-öffentlichen Stelle anstelle des betrieblichen Datenschutzbeauftragten für die Einhaltung datenschutzrechtlicher Bestimmungen verantwortlich ist. Dies bedeutet, dass er zum einen verpflichtet ist, für die Einhaltung datenschutzrechtlicher Vorschriften allgemein (§ 4g Abs. 1 BDSG) zu sorgen und zum anderen die Verfahrensbeschreibung (§ 4e BDSG) erstellen und diese den Betroffenen bzw. der Öffentlichkeit verfügbar machen muss. Vor dem Hintergrund zahlreicher Haftungszuweisungen in Spezialgesetzen stellt diese Norm eine klarstellende Mahnung an die Geschäftsleitung dar.

Darüber hinaus obliegt es dem Beauftragten für den Datenschutz nunmehr explizit, die Beratung der Aufsichtsbehörde in Anspruch zu nehmen. Entsprechendes ist auch zweckmäßig, da eine rechtzeitige Beratung spätere Eingaben und problematische Kontrollen verhindern kann. Allerdings ist die Beratung und Unterstützung i.S.d. § 38 Abs. 1 Satz 2 BDSG durch die Aufsichtsbehörde nicht in dem Sinne zu verstehen, dass die verantwortliche Stelle entgegen der Systematik des Datenschutzrechts ihre Verantwortlichkeit und damit die Haftung für datenschutzgerechtes Vorgehen auf die Aufsichtsbehörde abwälzen kann.

Letztlich wird im Rahmen der Novellierung durch § 4f Abs. 2 Satz 2 BDSG eindeutig festgelegt, dass sich die Tätigkeit des betrieblichen Datenschutzbeauftragten auch auf personenbezogene Daten bezieht, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Berufs- oder Amtsgeheimnisträger sind beispielsweise Steuerberater, Apotheker, Ärzte oder Rechtsanwälte. Dem betrieblichen Datenschutzbeauftragten steht allerdings nunmehr ein Zeugnisverweigerungsrecht zu, wenn er im Rahmen seiner Tätigkeit Kenntnis über Daten erhält, für die eine berufliche Geheimhaltungspflicht besteht (§ 4f Abs. 4a BDSG).

2.2 Die Rechte der Betroffenen nach dem Bundesdatenschutzgesetz

In Zeiten, in denen technisch sowohl der Datenerhebung als auch der Datenspeicherung und der Datenverwendung keine Grenzen gesetzt sind, fällt es nicht selten schwer, sein Recht auf informationelle Selbstbestimmung durchzusetzen. Oftmals liegt es bereits daran, dass ein Bürger nicht weiß, wer was bei welcher Gelegenheit über ihn weiß. Es mangelt an Transparenz, die ein wesentlicher Akzeptanzfaktor für den Umgang mit personenbezogenen Daten des Einzelnen ist.

Da ein solcher Zustand nicht mit der Gesellschafts- und Rechtsordnung in Einklang zu bringen ist, normiert das Bundesdatenschutzgesetz in den §§ 33 – 35 BDSG Rechte für die Betroffenen. Durch die Offenlegung seiner Daten soll ein Betroffener in die Lage versetzt werden, Korrektur-, Löschungs- oder ggf. Schadenersatzansprüche gegenüber der verantwortlichen Stelle geltend zu machen. Verantwortliche Stelle ist die Stelle, die personenbezogene Daten für sich erhebt, verarbeitet oder nutzt bzw. dies durch andere im Auftrag vornehmen lässt.

Damit jeder Einzelne bereits Kenntnis darüber erlangt, wer Daten über ihn erhebt, statuiert § 4 Abs. 2 Satz 1 BDSG zudem den **Grundsatz der Direkterhebung** von Daten beim Betroffenen. Damit einher geht auch die Verpflichtung, bei der Datenerhebung über Art und Verwendungszwecke der beabsichtigten Datenverarbeitung zu informieren. Werden personenbezogene Daten beim Betroffenen erhoben, dann hat ihn die verantwortliche Stelle über

- ihre Identität,
- die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und
- die Kategorien von Empfängern, soweit der Betroffene mit einer Übermittlung an diese nicht rechnen muss

zu unterrichten, soweit der Betroffene hiervon noch keine Kenntnis hat (§ 4 Abs. 3 BDSG).

Darüber hinaus normiert § 33 BDSG eine **Verpflichtung zur Benachrichtigung**, wenn eine Stelle Daten eines Betroffenen verarbeitet, die sie nicht direkt bei ihm erhoben hat. Ohne eine Benachrichtigung wüsste er nicht, gegenüber wem er beispielsweise seinen **Auskunftsanspruch** realisieren könnte. Mit einem an die verantwortliche Stelle gerichteten Auskunftsersuchen kann der Betroffene im Rahmen des § 34 BDSG in Erfahrung bringen,

- welche Daten zu seiner Person gespeichert sind
- die Herkunft dieser Daten
- Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden und
- den Zweck der Speicherung.

Die Auskunft ist grundsätzlich unentgeltlich. Kreditschutzorganisationen (SCHUFA) und Handels- und Wirtschaftsauskunfteien können jedoch unter bestimmten Voraussetzungen für die Auskunft ein Entgelt verlangen. Dies gilt jedoch nicht, wenn die Annahme gerechtfertigt ist, dass die zur Person des Betroffenen gespeicherten Daten unrichtig oder unzulässig gespeichert werden.
Auch hat jedermann ein **Recht auf Einsicht in das Verfahrensverzeichnis** der verantwortlichen Stelle. Dieses beinhaltet eine Übersicht über die automatisierten Verarbeitungen personenbezogener Daten der verantwortlichen Stelle. Auch finden sich darin insbesondere die Bezeichnungen der von dem Unternehmen verwendeten Verfahren und zu welchem Zweck diese Verfahren angewendet werden. Außerdem kann man dem Verfahrensverzeichnis die verarbeiteten Datenarten, die Personengruppen, über die Daten gespeichert werden sowie Kategorien von Empfängern von Datenübermittlungen entnehmen.

Stellt ein Betroffener fest, dass unrichtige oder unzulässig Daten über ihn bei der verantwortlichen Stelle gespeichert werden, besitzt er im Hinblick auf unrichtige Daten stets ein **Berichtigungsrecht** (§ 35 Abs. 1 BDSG). Daneben sind personenbezogene Daten zu **sperren**, wenn

- besondere Gründe einer fälligen Löschung entgegenstehen, z. B. gesetzliche, satzungsmäßige sowie vertragliche Aufbewahrungsfristen, schutzwürdige Interessen des Betroffenen oder
- wegen der Art der Speicherung eine Löschung nur mit unverhältnismäßigem Aufwand möglich ist, aber auch
- wenn der Betroffene ihre Richtigkeit bestreitet und sich weder deren Richtigkeit noch Unrichtigkeit feststellen lässt.

Gesperrte Daten dürfen grundsätzlich nicht mehr übermittelt oder genutzt werden. Dies ist nur zulässig zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründe.

Grundsätzlich sind personenbezogene Daten zu **löschen**, wenn sie nicht mehr gebraucht werden oder die verantwortliche Stelle sie gar nicht hätte erheben dürfen.

Weiterhin besitzt jeder Betroffene ein **Recht auf Widerspruch**. Ein solcher ist hinsichtlich der zur eigenen Person gespeicherten Daten begründet, wenn die schutzwürdigen Interessen des Betroffenen wegen einer besonderen persönlichen Situation das Interesse der privaten Stelle an der Datenverarbeitung überwiegen. Ein Widerspruchsrecht steht den Betroffenen auch gegen die Nutzung oder Übermittlung personenbezogener Daten zum Zwecke der Werbung und der Markt- oder Meinungsforschung zu. In diesen Rahmen fällt auch die **Berechtigung zum Widerruf** einer nach § 4a BDSG erteilten **Einwilligung**.

Letztlich haben die Betroffenen jederzeit das **Recht, sich an die Kontrollinstitutionen für den Datenschutz zu wenden**, wenn sie der Auffassung sind, bei der Erhebung, Verarbeitung oder Nutzung ihrer persönlichen Daten in ihren Rechten verletzt worden zu sein.

3 Datenschutz im nicht-öffentlichen Bereich des Landes Sachsen-Anhalt

3.1 Allgemeines zur Aufsichtstätigkeit

3.1.1 Ansprechpartner und Internetpräsenz

Das Landesverwaltungsamt Sachsen-Anhalt ist die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich des Landes Sachsen-Anhalt. Die örtliche Zuständigkeit der Aufsichtsbehörde für den nicht-öffentlichen Bereich knüpft stets an den Ort der Datenverarbeitung an. Dies ist der Ort, wo Daten physikalisch verarbeitet werden. Auf den Sitz der Unternehmensleitung kommt es nicht an.
Eine besondere Zuständigkeit gibt es für Telekommunikationsunternehmen. Bei Sachverhalten, in denen im Zusammenhang mit der Erbringung von Telekommunikationsdiensten Daten erhoben, verarbeitet und genutzt werden, obliegt die Kontrollzuständigkeit dem Bundesbeauftragten für den Datenschutz (§ 115 Abs. 4 des Telekommunikationsgesetzes (TKG)).

Mit Ihren Fragen, auch zur Zuständigkeit der Aufsichtsbehörde, können sich Bürgerinnen und Bürger an das Landesverwaltungsamt Sachsen-Anhalt unter folgender Anschrift wenden:

Landesverwaltungsamt Sachsen-Anhalt
Referat Justiziariat
Ernst-Kamieth-Straße 2 **(Hauptsitz)** bzw.
06112 Halle (Saale)

An der Fliederwegkaserne 13 **(Dienstgebäude)**
06130 Halle (Saale)

Persönliche telefonische oder schriftliche Anfragen können Sie an

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

Frau Anke Westerkamp
E-Mail: Anke.Westerkamp@lvwa.sachsen-anhalt.de
Telefon: 0345/5143925

Frau Damm
E-Mail: Nicole.Damm@lvwa.sachsen-anhalt.de
Telefon: 0345/514-3775
richten. Gern können Sie auch den Faxanschluss, Fax-Nummer: 0345/5143799, nutzen.

Darüber hinaus finden Sie im Internet bereitgestellte Informationen zum Datenschutz im nicht-öffentlichen Bereich des Landes Sachsen-Anhalt. Die Informationen können unter www.lvwa.sachsen-anhalt.de/datenschutz eingesehen werden.

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 Merkblätter über datenschutzrechtliche Fragen vorfinden, welche vermehrt an die Aufsichtsbehörde herangetragen wurden bzw. werden. Die bestehende Internetpräsenz wird weiter ausgebaut, beispielsweise sollen sich dort wichtige Neuigkeiten im Bereich des Datenschutzes wiederfinden und aktuelle Fragen aufgegriffen werden.

3.1.2 Eingaben, Anlasskontrollen

Schwerpunkt der Tätigkeit der Aufsichtsbehörde war auch 2005 und 2006 die Bearbeitung von Beschwerden betroffener Bürger. Im Berichtszeitraum war ein leichter Anstieg der Zahl der Beschwerden zu verzeichnen. Zudem ist festzustellen, dass die Beschwerden wesentlich komplexere Aspekte als in der vorangegangenen Berichtsperiode betrafen.

Die meisten Verfahren konnten im schriftlichen Verfahren mit den verantwortlichen Stellen geklärt werden. Allerdings fanden gerade im Bereich der Videoüberwachung auch zahlreiche Anlasskontrollen vor Ort statt, da sowohl die Ausrichtung der zu überprüfenden Videoüberwachungsanlagen als auch deren technische Details im schriftlichen Verfahren nur bedingt aufgeklärt werden können.

3.1.3 Beratung von Bürgern, Unternehmen und betrieblichen Datenschutzbeauftragten

Die Beratung ist ein wichtiger Aspekt des Datenschutzrechtes, denn nur unter Zuhilfenahme der Möglichkeit des vorlaufenden Datenschutzes ist es möglich, im Vorfeld aktiv zu wirken und zukünftige Verstöße gegen den Datenschutz zu verhindern. Dass der Bedarf an Beratung hoch ist, kommt auch darin zum Ausdruck, dass die Aufsichtsbehörde im Berichtszeitraum vermehrt telefonische Anfragen und Beratungswünsche von Bürgern und Unternehmen zu verzeichnen hatte. Da auf dem Gebiet des Datenschutzrechts nicht selten ein Abwägungsprozess zwischen den berechtigten Interessen der verantwortlichen Stelle und den schutzwürdigen Interessen der Betroffenen notwendig ist und damit keine ad hoc Aussage darüber getroffen werden konnte, ob die beanstandete Vorgehensweise zulässig oder unzulässig ist, konnten telefonisch lediglich die Bestimmungen des Datenschutzrechts allgemein erläutert und eine grobe Einschätzung der Rechtslage gegeben werden. Im Regelfall wurde sodann um eine schriftliche Sachverhaltschilderung (auch per E-Mail) gebeten.
Von solchen telefonischen Anfragen gelangen dann ca. 2/3 schriftlich an die Aufsichtbehörde und werden einer detaillierten Überprüfung unterzogen.

Im Rahmen ihrer personellen und zeitlichen Möglichkeiten nimmt die Aufsichtsbehörde zudem an den von der Gesellschaft für Datenschutz und Datensicherung e.V. viermal im Jahr an wechselnden Orten veranstalteten Sitzungen der Erfahrungsaustausch-Kreise der betrieblichen Datenschutzbeauftragten teil und stellt einmal jährlich ihre Räumlichkeiten für diesen Erfahrungsaustausch zur Verfügung. In den sogenannten ERFA-Kreisen werden aktuelle Datenschutz- und Datensicherheitsfragen erörtert. Zukünftig sollen neben den aktuellen Problemen auch seitens der Aufsichtsbehörde Vorträge zu Themen gehalten werden, die die Teilnehmer bei ihrer täglichen Arbeit interessieren.

3.1.4 Ordnungswidrigkeitenverfahren

Nach § 43 des Bundesdatenschutzgesetzes sind zahlreiche Verstöße gegen dieses Gesetz bußgeldbewehrt. Die Aufsichtsbehörde für den Datenschutz des Landes Sachsen-Anhalt macht in solchen Fällen nach pflichtgemäßem Ermessen von der Möglichkeit, ein Bußgeld zu verhängen, Gebrauch. Allerdings gestalten sich die notwendigen Sachverhaltsnachermittlungen in entsprechenden Vorgängen als äußerst kompliziert. Dies basiert darauf, dass Täter meist Beschäftigte eines komplexen Unternehmens sind und deren namentliche Ermittlung nur bedingt möglich ist. Vor Verhängung eines Bußgeldes wird allerdings stets auch geprüft, ob eine Verwarnung, ggf. mit Verwarngeld, welches maximal 30,00 EUR beträgt, genügt.

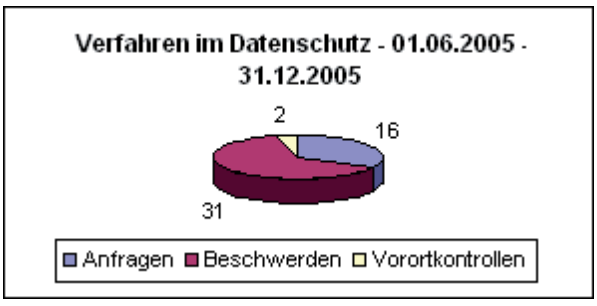
Die vorgenannten Ausführungen sollen allerdings keineswegs den Eindruck erwecken, dass die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich Bußgeldverfahren forciert. Vielmehr ist zu betonen, dass es für die Aufsichtsbehörde von größerer Bedeutung ist, für die Zukunft ein datenschutzgerechtes Verhalten eines Unternehmens sicherzustellen, als Verstöße in der Vergangenheit zu ahnden. Aus diesem Grund findet in derartigen Verfahren stets eine intensive Erörterung der Rechtmäßigkeit einer Vorgehensweise mit der verantwortlichen Stelle statt.

Im Berichtszeitraum hat die Aufsichtsbehörde acht Bußgeldverfahren eingeleitet. In zwei Sachverhalten wurde eine Verwarnung mit einem Verwarngeld i.H.v. 30,00 EUR ausgesprochen. Ein anderer Sachverhalt betraf das Gesetz zum Schutz personenbezogener Daten des Landes Sachsen-Anhalts. Hinsichtlich dieser Verfahren ist das Landesverwaltungsamt Sachsen-Anhalt für die Verfolgung und Ahndung von Ordnungswidrigkeiten zuständig. In zwei weiteren Fällen wurden Einsprüche gegen die Bußgeldbescheide wegen unzulässiger Datenerhebung, -speicherung und -nutzung, konkret in Form der heimlichen Videoüberwachung einer Arbeitnehmerin und der unbefugten Datenerhebung eines Anwaltes bei der Straßenverkehrsbehörde eines Landkreises, eingelegt. Ein weiterer Bußgeldbescheid ist bestandskräftig geworden. Die übrigen Verfahren befinden sich im Anhörungsverfahren. In vier Fällen musste die Aufsichtsbehörde wegen beharrlicher Verweigerung der Auskunft an die Aufsichtsbehörde Bußgeldverfahren einleiten.

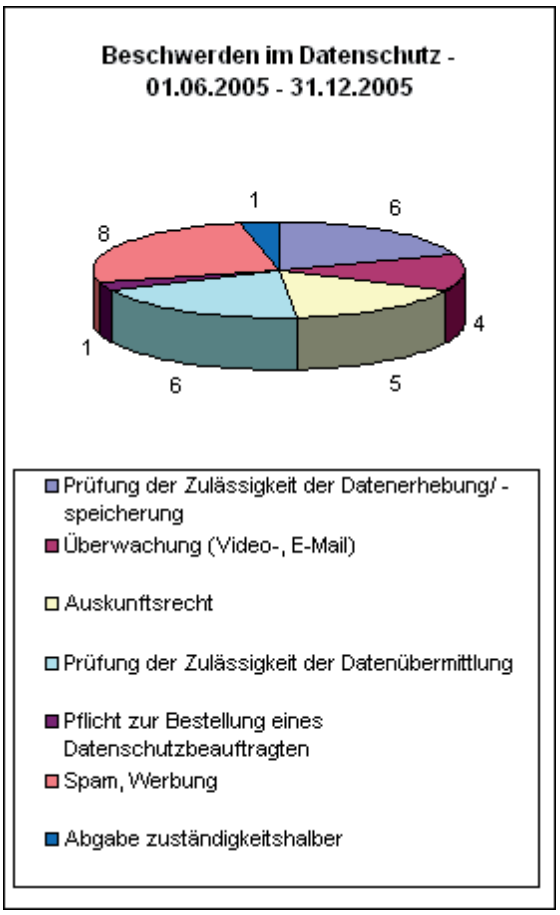
3.2 Zahlenmäßiger Überblick über die Tätigkeit der Aufsichtsbehörde

Zeitraum vom 01.06.2005 – 31.12.2005

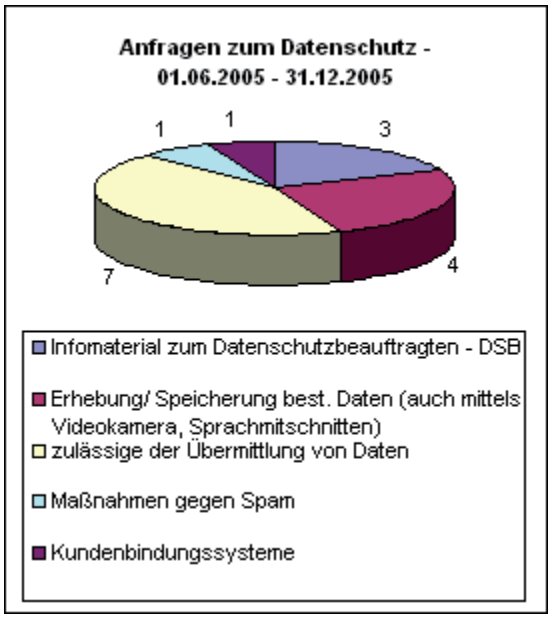
Verfahren im Datenschutz - Überblick 01.06. - 31.12.2005	
Anfragen	16
Beschwerden	31
Vorortkontrollen	2



Beschwerden im Datenschutz - Überblick 01.06. - 31.12.2005	
Prüfung der Zulässigkeit der Datenerhebung/ -speicherung	6
Überwachung (Video-, E-Mail)	4
Auskunftsrecht	5
Prüfung der Zulässigkeit der Datenübermittlung	6
Pflicht zur Bestellung eines Datenschutzbeauftragten	1
Spam, Werbung	8
Abgabe zuständigkeitshalber	1

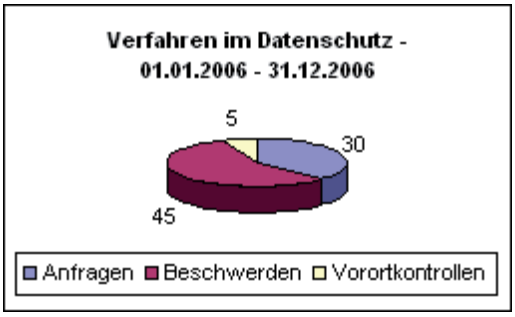


Anfragen im Datenschutz - Überblick 01.06. - 31.12.2005	
Infomaterial zum Datenschutzbeauftragten - DSB	3
Erhebung/ Speicherung best. Daten (auch mittels Videokamera, Sprachmitschnitten)	4
zulässige der Übermittlung von Daten	7
Maßnahmen gegen Spam	1
Kundenbindungssysteme	1

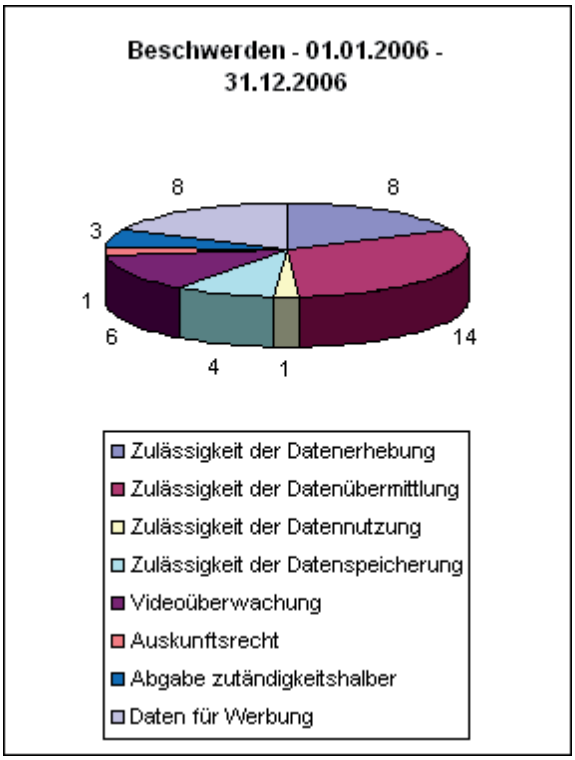


Zeitraum vom 01.10.2006 – 31.12.2006

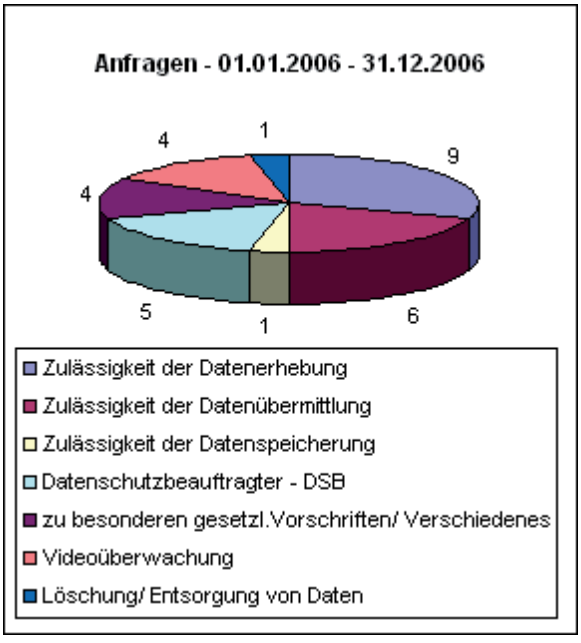
Verfahren im Datenschutz – Überblick 01.01. - 31.12.2006	
Anfragen	30
Beschwerden	45
Vorortkontrollen	5



Beschwerden im Datenschutz - Überblick 01.01. - 31.12.2006	
Zulässigkeit der Datenerhebung	8
Zulässigkeit der Datenübermittlung	14
Zulässigkeit der Datennutzung	1
Zulässigkeit der Datenspeicherung	4
Videoüberwachung	6
Auskunftsrecht	1
Abgabe zuständigkeitshalber	3
Daten für Werbung	8

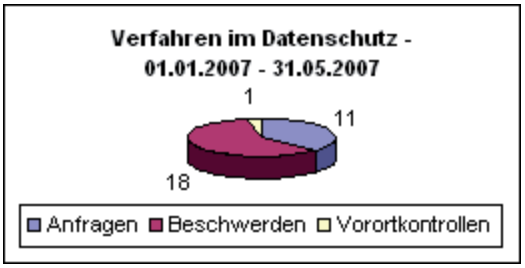


Anfragen im Datenschutz - Überblick 01.01.-31.12.2006	
Zulässigkeit der Datenerhebung	9
Zulässigkeit der Datenübermittlung	6
Zulässigkeit der Datenspeicherung	1
Datenschutzbeauftragter - DSB	5
zu besonderen gesetzl. Vorschriften/ Verschiedenes	4
Videoüberwachung	4
Löschung/ Entsorgung von Daten	1

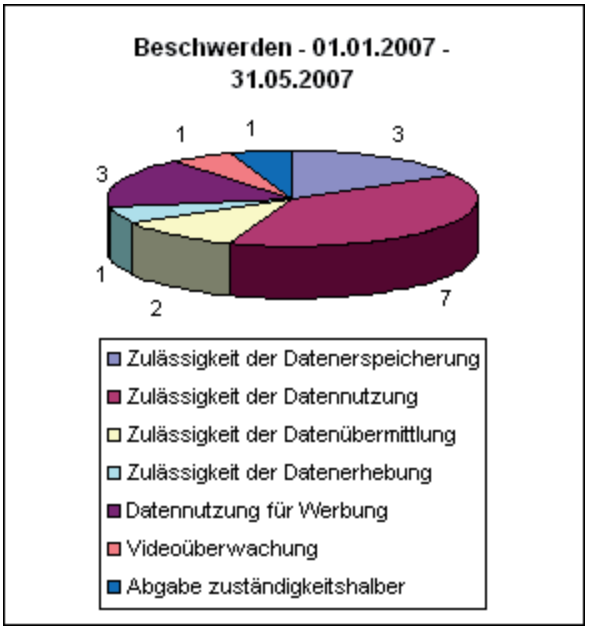


Zeitraum vom 01.01.2007 – 31.05.2007

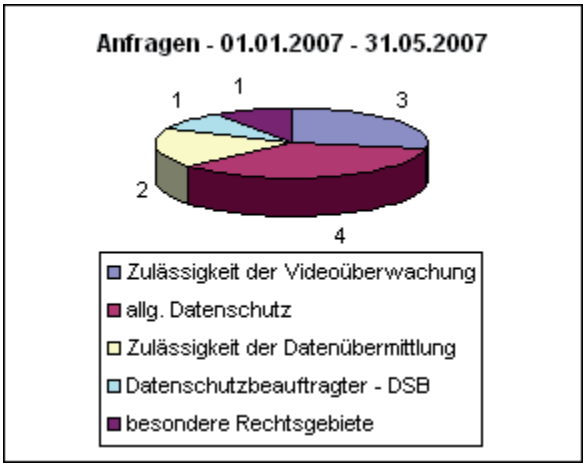
Verfahren im Datenschutz - Überblick 01.01. - 31.05.2007	
Anfragen	11
Beschwerden	18
Vorortkontrollen	1



Beschwerden im Datenschutz - Überblick 01.01. - 31.05.2007	
Zulässigkeit der Datenspeicherung	3
Zulässigkeit der Datennutzung	7
Zulässigkeit der Datenübermittlung	2
Zulässigkeit der Datenerhebung	1
Datennutzung für Werbung	3
Videoüberwachung	1
Abgabe zuständigkeitshalber	1



Anfragen im Datenschutz – Überblick 01.01. - 31.05.2007	
Zulässigkeit der Videoüberwachung	3
allg. Datenschutz	4
Zulässigkeit der Datenübermittlung	2
Datenschutzbeauftragter - DSB	1
besondere Rechtsgebiete	1



4 Einzelne Tätigkeitsbereiche aus Anfragen und Beschwerden

4.1 Von Beratungsinteresse – ausgewählte Aspekte der Anfragen

4.1.1 Telefongespräche

Das Telefon ist in allen Unternehmen ein gängiges und wichtiges Kommunikationsmittel. Insbesondere beim Kontakt mit Kunden und Lieferanten. Nicht selten ermöglicht der Arbeitgeber seinen Arbeitnehmern, das dienstliche Telefon auch für private Zwecke nutzen zu können. Aus dieser vielfältigen Verwendungsbreite resultieren verschiedene Anliegen der Arbeitgeber. So wurde beispielsweise bei der Aufsichtsbehörde angefragt, ob aus Gründen der Qualitätssicherung / zu Schulungszwecken alle Gespräche zwischen Mitarbeiter und Firmenkontakt, sei es Lieferant oder Kunde, aufgezeichnet werden könnten. Im Konkreten sollte dies derart gestaltet sein, dass ein Mitarbeiter selbst entscheiden könne, welches Gespräch er der Qualitätskontrolle unterwerfen möchte und der Firmenkontakt (Lieferant oder Kunde) entscheiden könne, ob er die Aufnahme und deren Auswertung wünsche.
Daneben gibt es bisweilen auch Bestrebungen von Arbeitgebern, Telefonate darauf zu kontrollieren, ob sie dienstlicher oder privater Natur waren. Entweder hat der Arbeitgeber die private Nutzung untersagt und will die Einhaltung dieses Verbotes kontrollieren oder er hat die private Nutzung in dem Maße gestattet, dass keine extensive Nutzung des Mediums unter Vernachlässigung der arbeitsvertraglichen Pflichten stattfindet.

Bei den „Qualitätssicherungsmaßnahmen“ sind in der Praxis folgende Realisationsvarianten denkbar:

- Offenes direktes Mithören des vom Arbeitnehmer gesprochenen Wortes am Arbeitsplatz durch eine Person ohne Nutzung elektronischer Hilfsmittel oder unter Nutzung von Kopfhörern etc.
- Offenes indirektes Mithören des vom Arbeitnehmer gesprochenen Wortes ohne unmittelbare Anwesenheit des Mithörers am Arbeitsplatz durch „elektronisches Aufschalten“; der Arbeitnehmer wird hierbei über das Mithören konkret vorab oder durch entsprechende akustische oder elektronische Signalisierung informiert
- Verdecktes Mithören des vom Arbeitnehmer gesprochenen Wortes oder des gesamten Telefongespräches durch „elektronisches Aufschalten“ Dritter ohne unmittelbare Anwesenheit des Mithörers am Arbeitsplatz und ohne direkte Kenntnis oder Einwilligung der Betroffenen („Silent Monitoring“)
- Testanrufe („Mystery Calls“), die beliebig oder gezielt an bestimmte Mitarbeiterplätze erfolgen und ausgewertet werden

Zu der Frage des unbemerkten Mithörens von Telefongesprächen hat sich das Bundesverfassungsgericht in seiner Entscheidung vom 19. Dezember 1991 grundlegend positioniert. In dieser Entscheidung ging es um die Frage der Beweisverwertungsmöglichkeit durch heimliches Abhören gewonnener Kenntnisse in einem arbeitsgerichtlichen Prozess.

In diesem Zusammenhang entschied das Gericht, dass die gerichtliche Verwertung der Kenntnisse, die aus einem heimlich mitgehörten Telefongespräch gewonnen werden, das Recht eines Bürgers am eigenen Wort verletzt. Dieses schütze die Befugnis des Sprechenden, den Kreis der Adressaten seiner Worte selbst zu bestimmen, und ist eine anerkannte Ausprägung des grundrechtlichen Persönlichkeitsschutzes. Weiterhin merkte es an, dass ein rein dienstlicher oder rein geschäftlicher Charakter des Telefongespräches die Bestimmungsbefugnis eines telefonierenden Bürgers nicht ohne weiteres beseitigen würde. Später führte das Bundesverfassungsgericht in Zusammenhang mit einem weiteren Verfahren ergänzend aus, dass der Kommunikationsinhalt in erster Linie den grundrechtlichen Schutz genießt. Dies bedeutet, dass es allein Sache der am Kommunikationsvorgang Beteiligten ist, darüber zu bestimmen, wer von dessen Inhalt Kenntnis erlangen soll. Das unbemerkte oder heimliche Ab- oder Mithören von Telefongesprächen durch Dritte ohne Kenntnis und **Einwilligung** der Telefonierenden ist aus dem Blickwinkel des Bundesverfassungsgerichtes im Regelfall unzulässig.
Dieser Rechtsauffassung folgt auch das Bundesarbeitsgericht, welches sich hauptsächlich infolge der Beweisverwertungsmöglichkeit von heimlichen Aufzeichnungen in arbeitsgerichtlichen Verfahren mit der Problematik auseinander gesetzt hat.

Der Bundesgerichtshof folgt dagegen für Zivilrechtsstreitigkeiten dieser Argumentation nicht vollständig. Insgesamt stellt jedoch auch er auf das Vorliegen einer wirksamen Einwilligung im konkreten Einzelfall ab. Liegt eine solche nicht vor, ist ein unbemerktes Mithören eines Telefongesprächs unzulässig.

Konsequenterweise stellte sich die Frage nach der rechtlichen Zulässigkeit und Wirksamkeit von individuellen Einwilligungen, durch die heimliches Ab- bzw. Mithören von dienstlichen Telefongesprächen ggf. legitimiert werden kann. Zwar sind bereits die Kontrolle der Arbeitsleistung und des Verhaltens der Arbeitnehmer mit einem Eingriff in Grundrechtspositionen des Betroffenen verbunden, doch derartige Eingriffe sind im Rahmen eines Arbeitsverhältnisses keineswegs grundsätzlich verboten. Vielmehr wird eine gewisse Überwachung des Arbeitsverhaltens bereits beim Abschluss eines Arbeitsvertrages billigend in Kauf genommen. Allerdings erteilt ein Betroffener auf diese Art und Weise kein Einverständnis zu einer lückenlosen Überwachung seines Arbeitsverhaltens. Vielmehr sind bei Maßnahmen von stärkerer Eingriffstiefe höhere Anforderungen an eine Einwilligung zu stellen. Zudem muss der Grundsatz der Verhältnismäßigkeit beachtet werden. Wenn die Abwägung der berechtigten Interessen des an der Überwachung Interessierten und den schutzwürdigen Interessen der Betroffenen ergibt, dass ein Eingriff in die Persönlichkeitsrechte der Betroffenen unumgänglich ist, muss die Einschränkung, denen die Betroffenen unterworfen sind, dennoch so gering und schonend erfolgen, wie dies zur Erreichung des rechtlich zulässigen Zwecks geboten ist. Dementsprechend ist jeder Sachverhalt unter Einbeziehung der Individualaspekte neu zu beurteilen und es kann keine pauschale Aussage zur Zulässigkeit oder Unzulässigkeit beabsichtigter „Qualitätssicherungsmaßnahmen“ getroffen werden. Nur wenn die vorgenannten Rahmenbedingungen eingehalten sind, kann der Arbeitgeber eine Einwilligung von den betroffenen Arbeitnehmern verlangen. Eine Einwilligung muss allerdings freiwillig sein. Freiwilligkeit ist nur gegeben, wenn eine Entscheidung nicht unter Druck oder in einer Zwangslage getroffen wird. Ob eine Einwilligung zu einer Zulässigkeit des Mithörens führt/e, ist folglich immer einzelfallbezogen zu ermitteln.

Aus hiesiger Sicht wird die Auffassung vertreten, dass es einem Arbeitgeber bereits mit der Möglichkeit des offenen direkten Mithörens hinreichend gewährleistet ist, die Qualitätssicherung in ausreichendem Maße durchführen zu können, ohne unverhältnismäßig in die Rechte der Betroffenen einzugreifen. Unbemerkte Abhörmaßnahmen sind nur in konkret begründeten Einzelfällen denkbar.

Bei der konkret zu beurteilenden Anfrage wurde durch die Aufsichtsbehörde eingeschätzt, dass es durch die Aufzeichnung eines Telefongespräches zwischen dem Mitarbeiter und dem Kunden zu einer Erhebung personenbezogener Daten sowohl bei dem Mitarbeiter als auch bei dem Kunden kam. Da es keine spezielle Rechtsvorschrift gibt, die eine solche Datenerhebung erlaubt oder gar anordnet, konnte sich die Zulässigkeit der Aufzeichnung eines kompletten Telefonates allein aus dem Bundesdatenschutzgesetz oder einer den Anforderungen des § 4a BDSG entsprechenden Einwilligung ergeben. Eine solche muss stets vor der Aufzeichnung eingeholt werden, da die Betroffenen sonst keine Möglichkeit haben, ihr Verhalten und ihre Ausführungen so zu steuern, dass der Eingriff in deren Persönlichkeitsrecht so gering wie möglich ist. Zudem wurde auf die Bestimmung des § 201 Abs. 1 Strafgesetzbuch verwiesen, wonach das Aufzeichnen von Telefongesprächen strafbar ist, soweit dies unbefugt erfolgt.
Ergänzend wurde nachfolgend bei der verantwortlichen Stelle nachgefragt, inwiefern aus kollektivrechtlichen Einwilligungstatbeständen bzw. Konzernbetriebsvereinbarungen, die Zulässigkeit von Eingriffen in das Persönlichkeitsrecht der Mitarbeiter resultieren könne. Es wurde darauf hingewiesen, dass die Befugnisse des Arbeitgebers und des Betriebsrates zum Abschluss einer Betriebsvereinbarung keiner unbegrenzten Gestaltungsfreiheit unterliegen. Bereits aus § 75 Abs. 2 Betriebsverfassungsgesetz resultiert, dass Arbeitgeber und Betriebsrat die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern haben. Demzufolge sei eine Einschränkung von Persönlichkeitsrechten auf diese Art und Weise nur zulässig, soweit dies aufgrund überwiegender betrieblicher Interessen und insbesondere im Interesse eines ungestörten Arbeitsablaufes erforderlich ist und hierbei die Einschränkung so gering und schonend erfolge, wie diese zur Erreichung des rechtlich zulässigen Zweckes erforderlich ist. Seitens der Aufsichtsbehörde wurde klargestellt, dass ein heimliches Mithören von dienstlichen Telefongesprächen nicht auf der Grundlage einer Betriebsvereinbarung zulässig sein kann. Ausnahmsweise kann es aufgrund einer Betriebsvereinbarung zulässig sein, wenn der Regelungsgehalt der Vereinbarung unter Beachtung der Erforderlichkeit und der Verhältnismäßigkeit der Maßnahme konkrete zeitmäßig begrenzte Mithörmöglichkeiten schafft, etwa durch unmittelbare Anwesenheit eines Mithörenden am Arbeitsplatz des betroffenen Beschäftigten während der Probezeit oder wenn das Mithören im Einzelfall zur Kenntnis gebracht wird.

Etwas anderes kann der einschlägigen Literatur folgend nur dann gelten, wenn sich aus einer Aufzeichnung weder die Identität des Getesteten noch des Gesprächpartners ergeben würden und auch sonst keine Personenidentifizierbarkeit hergestellt werden kann. Derartige Fallgestaltungen sind jedoch nicht praxisrelevant. Zudem können bei Privatgesprächen unter Umständen die Begleitumstände von Telefongesprächen wie Dauer und Kosten erfasst werden. In diesem Zusammenhang wiegt das Persönlichkeitsrecht nicht so schwer. Zu beachten ist allerdings, dass Telefonnummern allenfalls in verkürzter Form gespeichert werden dürfen. Mithin soll sich die Identität des Gesprächspartners nicht ermitteln lassen können.

4.1.2 Optisch-elektronische Einrichtungen

Schnell ist die Idee geboren, an einer bestimmten Stelle eine oder mehrere optisch-elektronische Einrichtungen (Videokameras) zur Verfolgung eines für die einrichtende Stelle vermeintlich sinnvollen Zweckes anzubringen. Doch nicht alles, was technisch möglich ist, muss rechtlich zulässig sein. Durch die erhobenen, aufgezeichneten, übertragenen und ausgewerteten Bilder der Videoüberwachung kann in das Persönlichkeitsrecht der Personen eingegriffen werden. Aus diesem Grund kann es sinnvoll sein, sich bereits vor der Installation der Videokamera an die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich des Landes Sachsen-Anhalt zu wenden, um mit dieser die Zulässigkeit der beabsichtigten Überwachung zu klären und abzustimmen, wie dem Gebot der Datenvermeidung und -sparsamkeit (§ 3a BDSG) und dem Grundsatz der frühestmöglichen Datenlöschung (§ 35 Abs. 2 Satz 2 Nr. 3 BDSG) Folge geleistet werden kann.

Entsprechende Anfragen erhielt die Aufsichtsbehörde Sachsen-Anhalt im Hinblick auf die geplante Installation einer Überwachungseinrichtung zur Unterrichtung der Öffentlichkeit via Internet über den Baufortschritt bei einer Müllverbrennungsanlage oder zur Abschreckung potentieller Zerstörer von abgestellten PkWs einer Hilfsorganisation auf gemieteten Stellflächen eines öffentlich zugänglichen Parkplatzes.

Bezüglich der Müllverbrennungsanlage wurden Bildmaterialien zur Verfügung gestellt, aus denen die Aufsichtsbehörde erkennen konnte, dass durch die Kamera keinerlei personenbezogene Daten erhoben werden. Da nicht einmal der Typ und das Kfz-Kennzeichen der abgestellten Fahrzeuge erkennbar waren, wurde festgestellt, dass keine Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person beschafft werden und daher das Bundesdatenschutzgesetz nicht zum Tragen kommt.

Der karitative Verein dagegen schilderte, dass deren zur Essensversorgung der Bevölkerung genutzten Fahrzeuge regelmäßig massiv beschädigt wurden. Das Beseitigen der Schäden, beispielsweise tiefer Kratzer, zertrümmerter Spiegel, zerstochener Reifen war jeweils mit hohen Kosten verbunden. Daher wolle man die Fahrzeuge durch Videoüberwachung schützen. Im Detail wurde geschildert, dass ein Festplattenrecorder und die Bildapparate in den Sommermonaten von 22.00 Uhr bis 06.00 Uhr und in den Wintermonaten zwischen 20.00 Uhr und 06.00 Uhr aktiv sein sollen.
Da mit den avisierten Überwachungseinrichtungen personenbezogene Daten erhoben, gespeichert und bei Vorfällen übermittelt oder genutzt werden sollten, galt es die Zulässigkeit der Beobachtung der öffentlich zugänglichen angemieteten Parkflächen mit optisch-elektronischen Einrichtungen nach § 6b Abs. 1 BDSG zu beurteilen. Danach ist die Beobachtung öffentlich zugänglicher Räume mit Videoüberwachung nur zulässig, soweit sie zur Aufgabenerfüllung öffentlicher Stellen, zur Wahrnehmung des Hausrechtes oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Konkret war zu beurteilen, ob die geplante Videoüberwachung zur Wahrnehmung eines berechtigten Interesses erforderlich ist und ob dieses im durchzuführenden Abwägungsprozess nicht von schutzwürdigen Interessen der Betroffenen,

also der Personen, von denen Daten auf einem „Videoband“ sein könnten, überwogen wird.
Berechtigte Interessen der verantwortlichen Stelle können sowohl wirtschaftlicher als auch ideeller Natur sein. Diese müssen allerdings objektiv begründbar sein, d.h. sie dürfen nicht allein aus subjektiven Interessen erwachsen. Der Schutz des Eigentums wird regelmäßig erfasst und ist vor Beginn der Überwachung konkret als Zweck festzulegen. Diese Festlegung soll zum einen die Nachprüfung des berechtigten Interesses erleichtern, aber auch Aufschluss darüber geben, dass die verantwortliche Stelle nicht leichtfertig mit der Thematik Überwachung mit optisch-elektronischen Einrichtungen umgegangen ist.
Trotz eines berechtigten Interesses, musste die Videoüberwachung weiterhin zum Schutz des Eigentums des Vereines erforderlich sein. Die Erforderlichkeit ist dann nicht anzunehmen, wenn das berechtigte Interesse durch mildere, ebenfalls geeignete Mittel erreicht werden kann oder der angestrebte Überwachungszweck gar nicht erreicht werden kann. Gegenstand der Erforderlichkeitsprüfung ist sowohl die Tatsache des Aufstellens der technischen Einrichtung als auch die konkrete Einstellung der Beobachtung und die technischen Möglichkeiten der optisch-elektronischen Einrichtung (z.B. Beweglichkeit der Kamera, Zoommöglichkeiten etc.). Da hinsichtlich der konkreten Gestaltung des Kameraeinsatzes keine Bedenken bestanden, wurde in einem letzten Schritt geprüft, ob Anhaltspunkte bestehen, inwieweit die schutzwürdigen Interessen der Betroffenen das berechtigte Interesse der verantwortlichen Stelle überwiegen. Schutzwürdige Interessen müssen sich auf belegbare Tatsachen beziehen und würden z.B. überwiegen, wenn die Intimsphäre eines Betroffenen beobachtet werden soll. Hinsichtlich der zu prüfenden Anfrage wurde festgestellt, dass sich etwaige Zerstörer nicht auf ein schutzwürdiges Interesse berufen könnten und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen zufällig erfasster Personen überwiegen, da diesen ausreichend Möglichkeiten geboten werden, der Videoüberwachung auszuweichen. Die beabsichtigte Überwachung wurde daher auf der Grundlage des § 6b Abs. 1 Nr. 3 BDSG für die angemieteten Plätze als zulässig erachtet. Bedenken wurden jedoch dahingehend geäußert, auch nicht angemietete Parkfläche, auf der Tag für Tag unterschiedliche Fahrzeuge abgestellt werden, in die Beobachtung einzubeziehen. In einem solchen Falle würden alle befugten Nutzer der Parkfläche erfasst werden. Dies ist unverhältnismäßig und die Beobachtung ohnehin technisch kaum realisierbar, da es dem Verein vor Abstellen der Fahrzeuge nicht möglich sein dürfte, eine adäquate Kameraausrichtung vorzunehmen. Abschließend wurde darauf hingewiesen, dass die Transparenz hinsichtlich der Datenerhebung und -nutzung entscheidend ist und demzufolge mit potentiell Betroffenen bereits im Vorfeld der Dialog gesucht werden sollte. In diesem Kontext hat auch der Verein gemäß § 6b Abs. 2 BDSG den Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen. Mit Hilfe der Kennzeichnung soll es den Betroffenen neben der Möglichkeit der Videoüberwachung ausweichen zu können, möglich sein, sich an die verantwortliche Stelle zu wenden, um herauszufinden, ob das ihnen zustehende Persönlichkeitsrecht gewahrt wird.

Neben den vorgenannten Anfragen hatte die Aufsichtsbehörde zu beurteilen, ob ein künstlerisches Projekt, mit dem die zunehmende Überwachung des öffentlichen Raums thematisiert werden sollte, nach den Bestimmungen des Datenschutzes möglich ist. So sollten beispielsweise auf Bahnhöfen mittels Monitor beobachtete Situationen mit entsprechenden Wort-/ Musikbeiträgen unterstrichen werden. Im Rahmen der Kunstaktion sollten somit durch eine andere verantwortliche Stelle die erhobenen personenbezogenen Daten genutzt werden. Alternativ wollte man selbst eine Überwachungseinrichtung installieren und die eigenhändig erhobenen Daten nutzen.
Hinsichtlich der Nutzung der Daten einer anderen verantwortlichen Stelle wurde darauf hingewiesen werden, dass sich allein aus § 6b Abs. 3 BDSG ergibt, unter welchen Voraussetzungen die Verarbeitung oder Nutzung von nach § 6b Abs. 1 BDSG erhobenen Daten zulässig ist. Nach § 6b Abs. 3 Satz 1 BDSG ist die Nutzung zulässig, wenn sie zum Erreichen des verfolgten Zweckes erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen des Betroffenen überwiegen. Damit ist die Verarbeitung oder Nutzung der aus der Videoüberwachung gewonnen Daten an den originären Beobachtungszweck geknüpft. Seitens der Aufsichtsbehörde wurde die Unzulässigkeit der geplanten Datennutzung auf dieser Grundlage beschieden.
Da die dargestellte Nutzung auch nicht zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich gewesen ist, konnte sich die Zulässigkeit auch nicht aus § 6b Abs. 3 Satz 2 BDSG ergeben. Lediglich eine Datennutzung nach Einholung von Einwilligungen, die den Anforderungen des Bundesdatenschutzgesetzes entsprechen, wäre möglich gewesen, allerdings nicht praktikabel.
Demgegenüber wurde beurteilt, dass die eigene Beobachtung mit optisch-elektronischen Einrichtungen im Rahmen des Kunstprojektes aufgrund des Art. 5 des Grundgesetzes ein berechtigtes Interesse i.S.d. § 6b Abs. 1 Nr. 3 BDSG darstelle. Bei Vorliegen der Erforderlichkeit und keinen im Abwägungsprozess dem berechtigten Interesse überwiegenden schutzwürdigen Belangen der Betroffenen, wäre die beabsichtigte Beobachtung zulässig gewesen. Erforderlichkeit und schutzwürdige Belange konnten allerdings mangels näherer Angaben nicht beurteilt werden. Es wurde lediglich weiterhin darauf hingewiesen, dass der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen sind. Wie dies konkret auszusehen hat, obliegt allerdings dem Ermessen der verantwortlichen Stelle. Eine abschließende Beurteilung nach ergänzenden Ausführungen wurde seitens der verantwortlichen Stelle nicht forciert.

4.1.3 Kundenbindung

Kundenbeziehungsmanagement oder Kundenpflege (engl. Customer Relationship Management, CRM) sind wichtige Bausteine des Beziehungsmanagement zu Kunden. Jedes Unternehmen ist daran interessiert, dass die Beziehungen zu seinen Kunden möglichst langfristig sind. Schließlich ist die Gewinnung von Neukunden bis zu fünf Mal teurer als die Kundenbindung. Kundenansprachen und Kundenbindungen nehmen demzufolge einen immer höheren Stellenwert ein.
Bei der Kundenbindung geht es um die Bestandskundenpflege. Kunden sollen z.B. fortlaufende Informationen über Waren und Dienstleistungen des Unternehmens erhalten, aber auch über Vergünstigungen und sonstige Vorteile. Die Vorteilsgewährung erfolgt häufig über Kundenkarten. Bei Kundenkarten ist zwischen einfachen, also solchen, die Unternehmen für ihre eigenen Kunden ausgeben, und solchen im Mehr-Parteienverhältnis, bei dem der Kunde seine Karte in allen angeschlossenen Unternehmen einsetzen kann, zu unterscheiden. Im Rahmen der Kundenkartensysteme werden unterschiedliche Daten erhoben. Je mehr Beteiligte es gibt, desto komplexer ist die datenschutzrechtliche Beurteilung der Systeme.
Die Teilnahme an einem solchen System beginnt üblicherweise mit dem Ausfüllen eines Antrages auf Erteilung einer Kundenkarte durch den Kunden. Ein solcher Antrag enthält Stammdaten und freiwillige Angaben. Stammdaten sind solche Daten, die im Rahmen des Kundenkartensystems notwendig sind. Diese sollten sich auf Name, Adresse und eventuell Alter beschränken, letzteres zum Schutz Minderjähriger. Freiwillige Angaben werden bei bestehenden Systemen in unterschiedlichem Umfang erhoben. Ist das Gebot der Transparenz gebührend gewahrt, kann jeder sein Recht auf informationelle Selbstbestimmung durch Angabe oder Nichtangabe seiner Daten frei umsetzen. Daneben werden oftmals auch Bewegungsdaten erfasst. Aus datenschutzrechtlicher Sicht unbedenklich ist die Erhebung von solchen Daten, die für die Abrechnung eines „Rabattkontos“ erforderlich sind. Dies ist im Allgemeinen das Datum und der Ort des Kaufs oder der Dienstleistung, Umsatz, Rabattgutschrift und Kennzeichen eines Partnerunternehmens. Darüber hinausgehende Daten, die Auskunft über das Konsumverhalten eines Einzelkunden geben können, wie z.B. gekaufte Artikel, gekaufte Menge, dürfen nur erhoben, verarbeitet oder genutzt werden, wenn der Kunde nach transparenter Information in diese Verarbeitungsschritte eingewilligt hat. Etwas anderes gilt nur, wenn eine anonyme Verarbeitung und Nutzung der Daten beispielsweise zur bedarfsgerechten Gestaltung des Angebotes von Waren und Dienstleistungen erfolgt. Im Hinblick auf die Verarbeitung gewonnener personenbezogener Daten muss zudem unterschieden werden nach der Kernverarbeitung, d.h. der Erfassung und Speicherung von Stammdaten, Bewegungsdaten, der Erstellung von Kontoauszügen zur ordnungsgemäßen Abwicklung der Bonusvereinbarung, der Verarbeitung zu sonstigen Zwecken, denen die Werbung zum Zweck der eigenen Kundenbindung oder Neukundengewinnung für eventuelle Partnerunternehmen unterfällt, aber auch nach der Information der Teilnehmer über Veränderungen des Programms. Bei der Verwendung der Daten für Zwecke der Werbung sind die Betroffenen bei jedem Kontakt auf das ihnen gemäß § 28 Abs. 4 Satz 1 BDSG zustehende Widerspruchsrecht hinzuweisen. Hierbei empfiehlt sich folgende Formulierung:

„Wenn Sie künftig unsere interessanten Angebote nicht mehr erhalten möchten, können Sie bei …(Nennung der verantwortlichen Stelle und deren Anschrift) der Verwendung Ihrer Daten für Werbezwecke widersprechen. Teilen Sie uns dies bitte schriftlich unter Beifügung des Werbemittels mittels Angabe Ihrer Adresse mit."

Bei einem der Aufsichtsbehörde zur Prüfung vorlegten Verfahren (Vorlage einer Projektbeschreibung, des entworfenen Antragsformulars und der Teilnahmebedingungen) wurde festgestellt, dass die eingereichten Unterlagen in weiten Teilen transparent und gut verständlich gewesen sind. Hinsichtlich des Antragsformulars wurde darauf hingewiesen, dass sich die zulässige Erhebung grundsätzlich auf die Daten zu beschränken hat, die zur Vertragsabwicklung erforderlich sind, d.h. Name und Anschrift des Kunden, nicht jedoch dessen Titel. Es wurde dem Unternehmen dargelegt, dass die Angabe des Titels allein eine freiwillige Angabe ist. Alle übrigen zu erhebenden Daten waren bereits als freiwillige Angaben gekennzeichnet. Darüber hinaus begrüßte die Aufsichtsbehörde, dass das Unternehmen hinsichtlich der Einwilligung der Nutzung der Daten für Werbezwecke eine Opt-In-Lösung bevorzugt hat. Dies bedeutet, dass der Beantragende ankreuzen muss, dass er bei Beantragung einer Kundenkarte auch Werbung wünscht. Opt-In-Verfahren sind aus Gründen der Transparenz zu bevorzugen. Lösungen, bei denen etwas vom Betroffenen wegzustreichen ist (Opt-Out-Verfahren), werden nämlich oftmals übersehen. Im Hinblick auf ein transparentes Verfahren wurde zudem darum gebeten, eine Information aus den Teilnahmebedingungen nochmals im Antragsformular zu wiederholen und im Übersendungsschreiben zur Kundenkarte ausführliche Erläuterungen zum Verfahren, den Teilnahmebedingungen etc. zu geben. Im Interesse der Verständlichkeit der Teilnahmebedingungen wurde zudem gebeten, bestimmte Begriffe näher zu erläutern und Verfahrenswege zu beschreiben.

Verbrauchertipp

Wenngleich Rabattkarten/ Kundenkarten im Alltag sehr geläufig sind, sind Kundenbindungsprogramme gerade unter dem Aspekt des Datenschutzes kritisch zu sehen, wenn die Antragsformulare keine klaren Informationen darüber enthalten, welche Daten über Sie gespeichert werden sollen und was mit den erhobenen Daten geschieht. Wenn es über den Namen, die Adresse und maximal das Alter hinausgehende Pflichtangaben gibt, ist die Offerte oft nicht datenschutzkonform.

Gerade unter dem Aspekt, dass mit solchen Karten häufig Ihr Kaufverhalten ausgewertet werden soll, um über Sie Nutzungsprofile und/ oder Persönlichkeitsprofile zu erstellen, sind die Gefahren einer Verletzung des Ihnen zustehenden Persönlichkeitsrechtes groß. Zumal die einmal gespeicherten Daten über längere Zeit gespeichert bleiben.

Daher prüfen Sie das Antragsformular und lesen Sie die Geschäftsbedingungen einer solchen Karte genau durch. Können Sie nicht erkennen, zu welchen Zwecken Ihre Daten durch wen verarbeitet werden, lassen Sie die Finger davon!

4.1.4 Unerwünschte E-Mail-Werbung (sogenannte SPAM-Mails) und Schutz vor Viren

Die mittels elektronischer Post übersandten Werbebotschaften, zum Teil auch in Form regelmäßig übersandter Newsletter, kennt jeder. Erhält man diese aufgrund eines geäußerten Wunsches, empfindet man die entsprechenden E-Mails nicht als belästigend. Anders verhält es sich allerdings bei solchen E-Mails, von denen man unverlangt quasi überrollt wird. Ständig ist das Postfach voll. Man muss aufpassen, keine relevanten E-Mails zu löschen, wenn man sich von SPAM durch Löschung der E-Mails befreien möchte. Das Interesse geht allerdings dahin, dass man SPAM-Mails gar nicht erst erhalten möchte.
Über die Regelungen im Gesetz gegen unlauteren Wettbewerb (UWG) hinaus, wonach unverlangte Werbesendungen wettbewerbswidrig sind, gibt es in Deutschland keine speziellen Gesetze, die Spamming verbieten oder unter Strafe stellen. Klagebefugt nach dem UWG sind allerdings nur direkte Mitbewerber, Verbraucherverbände sowie die Industrie- und Handelskammern.

Daher wandte sich ein Unternehmen an die Aufsichtsbehörde, um sich beraten zu lassen. Es wurde dem Unternehmen mitgeteilt, dass nicht alle hinlänglich bekannten Abwehrmethoden, die technisch möglich sind, auch rechtlich unbedenklich sind. Bei den Abwehrmaßnahmen ist zwischen der Durchsuchung von E-Mails auf Spam-Merkmale (Filterung) und dem Löschen, Blockieren oder Umleiten der E-Mails auf eine speziell zuständige Stelle zu differenzieren. Die detaillierten Ausführungen hierzu beziehen sich jedoch allein auf E-Mails, die an eine persönliche Adresse, z. B. peter.maier@firma.de, gerichtet sind und nicht an eine solche Adresse, die eindeutig als Adresse einer bestimmten Unterabteilung einer Firma zu qualifizieren ist, z.B. info@firma.de. Denn bei E-Mail-Adressen, die einem einzelnen Arbeitnehmer zugeordnet sind, kann die eingehende Post nicht ohne weiteres als betriebsbezogen gelten und zur Beurteilung der Zulässigkeit einzelner Maßnahmen sind daher die widerstreitenden Belange der verantwortlichen Stelle und der Betroffenen abzuwägen. Dabei kommen auf Seiten **der Nutzer**, zu denen auch die Arbeitnehmer zählen, vor allem das Telekommunikationsgeheimnis, das Persönlichkeitsrecht und gegebenenfalls die Wissenschaftsfreiheit zum Tragen.
Bei der *Blockierung* werden E-Mails bestimmter IP-Bereiche, ganzer Domänen oder Mails von Servern, die auf sogenannten Black Lists stehen, nicht zur Zustellung angenommen. Weiterhin werden sie zum Teil gelöscht, zum Teil aber auch mit einer entsprechenden Fehlermeldung zurückgesandt. Allerdings ist die zentrale Blockierung nur dann rechtlich zulässig, wenn der Nutzer dieser Vorgehensweise vorher zugestimmt hat, denn was für eine Stelle vermeintlich als SPAM identifiziert wird, kann für andere von Interesse sein. Das Zurückschicken von E-Mails ohne vorherige Zustimmung kann daher auch einen strafbaren Eingriff in das Fernmeldegeheimnis nach § 206 Abs. 2 Nr. 2 Strafgesetzbuch (StGB) bedeuten, insbesondere soweit in Unternehmen den Mitarbeitern die private Nutzung erlaubt ist. Das Unterdrücken von Nachrichten, die für den Nutzer bestimmt sind, kann schließlich auch als Datenunterdrückung gemäß § 303 a Abs. 1 2. Alt. StGB strafbar sein. Aus diesem Grund ist eher die Filterung von E-Mails anhand charakteristischer Merkmale, die eine Identifikation als SPAM ermöglichen, zulässig. Aber auch eine zentrale Filterung, der im nächsten Schritt regelmäßig eine Löschung der betroffenen E-Mails oder ein Verschieben der Mails in einen bestimmten Ordner folgt, sollte aus rechtlicher Sicht nicht ohne Einwilligung des Nutzers erfolgen. Insbesondere ist es

schwierig, brauchbare Filterkriterien festzulegen. Eine umfassende inhaltliche Filterung von E-Mails würde dem Persönlichkeitsrecht der Betroffenen zuwiderlaufen. Außerdem eignet sie sich kaum für die effektive Spam-Erkennung. So können bereits einfache Änderungen, wie z.B. das Ersetzen von „for you“ durch „4u“ oder „Access for all“ durch „xs4all“ zu einem Umgehen der Aussonderung aufgrund bestimmter Worte führen.
Vor dem Hintergrund des Fernmeldegeheimnisses, welches Inhalte und Verbindungsdaten von Telekommunikation vor unbefugter Kenntnisnahme schützt, ist daher eine Filterung nur zulässig, wenn sie automatisiert erfolgt und auch Administratoren von den gefilterten E-Mails keine Kenntnis erlangen können. Unbedenklich ist daher die Praxis im automatisierten Verfahren einer E-Mail, eine Bewertung ihrer Spam-Wahrscheinlichkeit vorzunehmen und diese Bewertung an den Mail-Header anzufügen. Daneben sind solche Maßnahmen möglich, die auf der Basis von Einwilligungen der Nutzer durchgeführt werden. Dem User können beispielsweise Programme angeboten werden, die ihm ein Filtern nach selbstdefinierten Stichwörtern und Kriterien ermöglichen. Auch können sie Nutzervorgaben treffen, welche E-Mails von welchen Absendern blockiert und gelöscht werden dürfen. Darüber hinaus sollte natürlich auch eine Aufklärung stattfinden, dass bei einer automatischen Filterung immer auch das Risiko einer Fehlbewertung besteht. Mithin müssen die Betroffenen wissen, dass unter Umständen auch seriöse E-Mails als SPAM gekennzeichnet werden und daher keine Zustellung erfolgt.

Was kann ich sonst noch beachten im Umgang mit SPAM-Mails?

Um sich wenigstens teilweise vor unerwünschter Werbung zu schützen, sollten Sie mit der Weitergabe Ihrer E-Mail-Adresse zurückhaltend sein. Sie sollten sich immer bewusst sein, dass das Versenden von massenhaften Werbe-E-Mails mit sehr geringfügigen Kosten verbunden ist.

Ist die Angabe Ihrer E-Mail-Adresse für die Teilnahme an Webforen und Newsgroups dennoch erforderlich, empfiehlt es sich, speziell für solche Zwecke eine gesonderte E-Mail-Adresse zu nutzen.

Haben Sie dennoch eine der unerwünschten Werbe-E-Mails erhalten, sollte Sie vorsichtig beim Beantworten solcher E-Mails sein. Einige Werbende verschicken nämlich sog. Test-Mails, um zu prüfen, ob E-Mail-Adressen existieren und genutzt werden. Dadurch erfährt das Unternehmen, dass Ihre E-Mail-Adresse kein „toter Briefkasten“ ist und die E-Mail-Adresse erfährt eine gewisse Wertsteigerung und wird zukünftig intensiver Adressat für E-Mails.

Der Verbraucherzentrale Bundesverband (vzbv) hat Ende des Jahres 2005 eine Beschwerdestelle für Spam-Mails eingerichtet. Wer unerwünschte E-Mails erhält, kann sie einfach an beschwerdestelle@spam.vzbv.de weiterleiten und der vzbv übernimmt dann die Verfolgung der Absender.

Unabhängig von Maßnahmen gegen SPAM wird regelmäßig zum Schutz vor Viren und anderen Schadprogrammen ein Virenscanning durchgeführt. Auch dabei kann es zu Auswirkungen auf das Persönlichkeitsrecht eines Betroffenen kommen. Demzufolge darf trotz des berechtigten Anliegens einer verantwortlichen Stelle, die Datensicherheit gewährleisten zu wollen, weder das Fernmeldegeheimnis noch das informationelle Selbstbestimmungsrecht der am Mailverkehr Beteiligten außer Acht gelassen werden.
Rechtlich unbedenklich ist ein Virenscanning von ein- und ausgehenden E-Mails dienstlicher oder privater Natur, solange es automatisiert abläuft und niemand von dem Kontrollvorgang und dessen Erkenntnissen Kenntnis nehmen kann. Wenngleich das Virenscanning eine notwendige Maßnahme der Datensicherheit darstellt, muss das Inhalts-Scanning auf fest definierte Virensignaturen begrenzt werden und darf nicht nach frei wählbaren Stichwörtern erfolgen. Mit der Identifikation virenverseuchter E-Mails (z. B. solche die einen gefährlichen oder verdächtigen ausführbaren Code enthalten, Dateien mit den Erweiterungen *.exe, *.bat, *.com oder gepackte Dateien wie *.zip, *.arj, *.lha) sind die Maßnahmen zur Abwehr von Viren jedoch noch nicht abgeschlossen. Vielmehr müssen die E-Mails oder deren Anhänge für eine abschließende Abwehr gelöscht werden. Allerdings liegt die alleinige Verfügungsbefugnis über E-Mails beim Nutzer. Beim Löschen der E-Mails ohne Einbeziehung des Nutzers besteht das Risiko des strafbewehrten Verstoßes gegen das Fernmeldegeheimnis sowie einer strafbaren Datenveränderung durch Unterdrückung bzw. Unbrauchbarmachung von Daten, die für den Mailempfänger bestimmt sind. Aus diesem Grund sollte stets eine Quarantänelösung vorgezogen werden. Dies bedeutet, dass vermeintlich virenverseuchte E-Mails zunächst nicht zugestellt, sondern in einen gesonderten Ordner umgeleitet werden sollten. Im Weiteren wird sodann der Adressat darüber informiert, dass eine an ihn adressierte E-Mail möglicherweise Viren enthält. Dann kann dieser entscheiden, ob er sich die Nachricht dennoch zustellen oder löschen lassen möchte. Eine ähnlich eigenverantwortliche Entscheidungsfreiheit besteht selbstverständlich auch dann, wenn der Nutzer im Voraus in einem benutzerspezifischen Profil festlegt, wie mit virenbehafteten E-Mails zu verfahren ist.

4.1.5 Erhebung personenbezogener Daten mittels Fragebogen

Die Datenerhebung mittels Fragebogen ist ein gängiges, nach Einschätzung der verantwortlichen Stellen, gut praktikables Mittel, um Daten zu gewinnen. Der Aufsichtsbehörde wurde u.a. ein Personalfragebogen und eine Selbstauskunft zum Abschluss einer Ratenzahlungsvereinbarung oder eines Zahlungsaufschubes für Forderungen vorgelegt und um Beurteilung der Zulässigkeit der darin zu erhebenden personenbezogenen Daten gebeten. Daneben wurden der Aufsichtsbehörde in der Berichtsperiode einige wissenschaftlich orientierte Projekte vorgestellt, bei denen eine Erhebung, Speicherung, Übermittlung und ggf. Nutzung personenbezogener Daten angedacht wurde. Da die Projektentwickler meist ihr Anliegen zweckmäßig umsetzen und dabei den Bestimmungen des Datenschutzes genüge tun wollten, wandten sie sich zur Beurteilung der Datenschutzkonformität vor der Umsetzung der Projekte an die Aufsichtsbehörde. Zum Teil verlangten auch öffentliche Institutionen eine Zustimmung der Datenschutzaufsichtsbehörden, dass das Modellprojekt den Anforderungen des Datenschutzes gebührend Rechnung trägt.

Hinsichtlich des Einstellungsfragebogens, mit dessen Hilfe oft eine Vorauswahl an Bewerbern hinsichtlich einer zu besetzenden Stelle getroffen wird, wurden bereits bei den „Angaben zur Person“ erfragte Daten als unzulässig erachtet. So steht es einem potentiellen Arbeitgeber nicht zu, den Familienstand eines Bewerbers und seit wann eine Veränderung eingetreten ist, zu erfassen. Lediglich die Tatsache, dass jemand verheiratet ist, kann z.B. bei der Lohnabrechnung von Relevanz sein. Hierzu genügen jedoch die aus der Lohnsteuerkarte entnehmbaren Daten. Aussagen über die Qualifikation eines Bewerbers lassen sich aus dem vorgenannten Datum ebenso wenig entnehmen wie aus der Angabe des Namens und des Berufes des Ehegatten, den Namen und dem Alter der Kinder. Derartige Daten sind für die Bewerberauswahl nicht erforderlich.

Des Weiteren wurden einige unter „Persönliche Verhältnisse“ gestellte Fragen, die letztlich alle Fragen nach dem Gesundheitszustand in sich bargen, für datenschutzrechtlich bedenklich eingeschätzt. Fragen nach dem Gesundheitszustand müssen nämlich durch spezifische, arbeitsplatzbedingte Anforderungen und Gefahren gerechtfertigt werden und dürfen daher nicht pauschal jedem Bewerber gestellt werden. Nach einer Schwangerschaft durfte nach einer ersten grundlegenden Änderung der Rechtsansicht des Bundesarbeitsgerichtes (BAG) infolge der Rechtsprechung des Europäischen Gerichtshofes (EuGH) ausnahmsweise nur dann gefragt werden, wenn für die Bewerberin ein Beschäftigungsverbot nach dem Mutterschutzgesetz gilt oder wenn eine Ersatzkraft für eine schwangere Mitarbeiterin befristet eingestellt werden soll. Inzwischen ist zu dieser Thematik weitere Rechtsprechung durch den EuGH ergangen, mit der diese Rechtsauffassung des BAG nicht mehr vereinbar gewesen ist. Es soll weder nach einer Schwangerschaft gefragt werden dürfen, wenn die Beschäftigung dem gesundheitlichen Schutz der Mutter oder des Kindes zuwiderläuft, noch wenn es sich nur um eine befristete Beschäftigung handelt, von der ggf. der überwiegende Teil nicht geleistet werden kann. Daher ist die Frage nach einer Schwangerschaft unzulässig. Auch braucht eine Frau auf eine Schwangerschaft nicht mehr hinzuweisen, außer sie kann die entsprechende Arbeit nicht mehr leisten. Nach dem Vorliegen einer Schwerbehinderteneigenschaft kann ein Bewerber dagegen uneingeschränkt gefragt werden und zwar unabhängig davon, welche Auswirkung die Schwerbehinderteneigenschaft oder die Gleichstellung sowie die zugrundeliegende Behinderung konkret für die in Aussicht stehende Tätigkeit hat. Dies resultiert daraus, dass der Arbeitgeber ein besonderes Interesse hat, den gesetzlichen Verpflichtungen zur Beschäftigung von Schwerbehinderten Folge leisten zu können. Auch wurden zahlreiche unter „Sonstiges“ formulierte Fragen für unzulässig erachtet.

So ist die Frage des Arbeitgebers nach den Gehältern oder Löhnen, die der Bewerber in seinem bisherigen oder früheren Arbeitsverhältnis bezieht oder bezogen hat, nur dann zulässig, wenn die Höhe der bisherigen Vergütung für die zu besetzende Stelle eine Aussagekraft hat oder wenn der Bewerber eine seiner bisherigen Bezahlung entsprechende Mindestvergütung fordert. Ebenso wie nach dem Gesundheitszustand darf ein Bewerber nicht allgemein befragt werden. Unter allgemeinen Fragen sind offene Fragen, z.B. „Wie geht es Ihnen heute?“, zu verstehen.

Die Frage nach Vorstrafen ist nur zulässig, wenn und soweit die Art des zu besetzenden Arbeitsplatzes und die vorgesehene Stellung des Arbeitnehmers dies erfordern. Auch darf nicht pauschal nach Ermittlungsverfahren gefragt werden. Zum einen gilt der Verdächtige bis zur rechtskräftigen Verurteilung als unschuldig, zum anderen besteht ein berechtigtes Interesse

an der Kenntnis von Ermittlungsverfahren allenfalls, wenn wegen der Umstände des Tatvorwurfes Zweifel an der persönlichen Eignung eines potentiellen Arbeitnehmers objektiv begründet sind.

Weiterhin sind Fragen nach den Vermögensverhältnissen nicht generell zulässig. Die Zulässigkeit der Frage richtet sich nach dem konkret zu besetzenden Arbeitsplatz. Sie kann regelmäßig an Personen gerichtet werden, die in Vertrauensstellungen (Leiter der Finanzbuchhaltung oder Personalstelle, Bankkassierer, Innenrevisor, Kassenpersonal usw.) beschäftigt werden sollen. Bei Mitarbeitern des unteren und mittleren Verantwortungsbereiches ist die Frage nach den Vermögensverhältnissen dagegen grundsätzlich unzulässig. Gleiches gilt für die Frage nach Lohnpfändungen, da diese regelmäßig nicht die Arbeitgeberinteressen gefährden, auch wenn das Interesse, die bei der Lohnberechnung und -auszahlung auftretenden Belastungen zu vermeiden, besteht. Die Frage nach geleisteten Wehr- oder Ersatzdienst wird bislang als zulässig anerkannt, da es um die uneingeschränkte oder noch beschränkte Verfügbarkeit des Einstellungsbewerbers geht und hierdurch die betrieblichen Interessen des Arbeitgebers berührt werden. Unter dem Aspekt der Gleichbehandlung von Männern und Frauen hinsichtlich des Zuganges zu einer Beschäftigung wird dies jedoch zunehmend kritisiert.

Während sich im Bereich der Bewerberdatenerhebung die Zulässigkeit der Erhebung von Personaldaten maßgeblich auch nach der Problematik „Fragerecht des Arbeitgebers bei Einstellungen“, zu welcher auch das Bundesarbeitsgericht bereits zahlreiche Entscheidungen getroffen hat, richtet, sind Fragebögen aus anderen Bereichen stets einzelfallbezogen zu beurteilen.
So auch der Fragebogen bezüglich des Abschlusses einer Ratenzahlungsvereinbarung. Anfragende Stelle ist in diesem Vorgang allerdings nicht die verantwortliche Stelle gewesen, sondern die betroffene Person, welche den Fragebogen ausfüllen sollte. Dem Betroffenen konnte nur erläutert werden, dass nach § 4 Abs. 1 BDSG die Erhebung personenbezogener Daten nur zulässig ist, soweit das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Festzustellen war, dass eine andere Rechtsvorschrift die in Rede stehende Datenerhebung weder ausdrücklich erlaubt noch anordnet. Zudem wurde eingeschätzt, dass aus der bloßen Angabe der erfragten Daten keine den Anforderungen des § 4a BDSG entsprechende Einwilligung resultiert und demnach die Zulässigkeit der Erhebung der einzelnen Daten allein nach dem Bundesdatenschutzgesetz, speziell § 28 BDSG, zu beurteilen ist. Der betroffenen Person wurde die Vorschrift des § 28 BDSG erläutert. Es wurde erklärt, dass regelmäßig ein Abwägungsprozess zwischen den berechtigten Interessen der verantwortlichen Stelle und den schutzwürdigen Interessen der Betroffenen vorzunehmen ist und daher keine pauschale Aussage über die Zulässigkeit bzw. Unzulässigkeit der besagten Daten getroffen werden kann, ohne die verantwortliche Stelle, auch in anonymisierter Form, einbezogen zu haben. Da die anfragende Person die Angabe der verantwortlichen Stelle ablehnte, fand keine weitere Überprüfung der zu erhebenden Daten statt. Für datenschutzrechtlich bedenklich wurden jedoch die im Fragebogen enthaltenen Frage nach dem Familienstand, dem Arbeitgeber inklusive Anschrift, der Höhe des Bankguthabens/ der Wertpapiere, dem Bausparguthaben, dem Rückkaufwert der Lebensversicherung und bei wem man diese Vermögenswerte hält, erachtet. Die Angaben bzgl. der Vermögensverhältnisse sollten sowohl für den Antragsteller als auch für den Bürgen getätigt werden. Insgesamt

bestehen daher Zweifel an der Erforderlichkeit der Daten zur Erfüllung eines berechtigten Interesses der verantwortlichen Stelle und daran, dass kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt (Zulässigkeitsnorm des § 28 Abs. 1 Satz 1 Nr. 2 BDSG).

Ein Unternehmen stellte ein Projekt vor, mit dem die Voraussetzungen und Möglichkeiten der Vernetzung hinsichtlich präventiver geriatrischer Gesundheitskompetenzen ermittelt werden sollten. Hierzu wollte man sich einer Situationsanalyse auf der Basis von amtlichen Statistiken und aus leitfadengestützten Interviews gewonnenen Erkenntnissen bedienen. Interviewpartner sollten Senioren sein, die von ihren Ärzten angesprochen werden, ob Interesse an der Projektteilnahme besteht. Wenn sich die Personen für eine Teilnahme entscheiden, würden sie einen Fragebogen erhalten, aus dem nach dem Ausfüllen allein Geschlecht und Alter des Befragten ersichtlich seien.
Das Projekt sollte durch die Nutzung der im Rahmen der üblichen Behandlung eines Patienten erhobenen Daten durch den Arzt eingeleitet werden. Der Arzt sollte aus seiner Patientenkartei mögliche Senioren zufällig ohne Verwendung etwaiger Gesundheitsdaten auswählen, die er hinsichtlich einer möglichen Teilnahme an dem Projekt befragt. Sobald ein Patient die Teilnahme an dem Projekt bestätigt, übermittelt der Arzt **die Adressdaten** des Patienten an das projektführende Unternehmen. Dieses verwendet die Adressdaten für die Übersendung des Fragebogens. Für die Überprüfung der datenschutzrechtlichen Zulässigkeit gab es verschiedene Verarbeitungsschritte bei zwei verantwortlichen Stellen, dem Arzt und dem projektführenden Unternehmen, zu untersuchen. Nach der Grundnorm des § 4 Abs. 1 BDSG sind die Erhebung, Verarbeitung (Speicherung, Veränderung, Übermittlung, Sperrung, Löschung) und Nutzung (alles was keine Verarbeitung darstellt) personenbezogener Daten nur zulässig, soweit das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Da die angesprochenen Patienten nicht die Möglichkeit haben, vorab ihre Einwilligung zur vom Arzt-Patientenverhältnis abweichenden Befragung zu erteilen und auch eine andere Rechtsvorschrift hierzu keine Regelung beinhaltet, konnte sich die Zulässigkeit dieser Datennutzung nur aus dem Bundesdatenschutzgesetz, speziell aus § 28 BDSG, ergeben.
Nach § 28 Abs. 3 Nr. 4 BDSG ist die Nutzung personenbezogener Daten für einen anderen Zweck auch zulässig, soweit es zur Wahrung berechtigter Interessen eines Dritten erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat.
In der Durchführung des Projektes und der Unterstützung durch die Ärzte ist ein berechtigtes Interesse des anfragenden Unternehmens zu sehen.
Die nachfolgende Interessenabwägung zwischen den berechtigten Interessen der Projektleitung und den schutzwürdigen Interessen der Patienten ergab, dass die Datennutzung zur Erreichung des berechtigten Interesses erforderlich ist und schutzwürdige Interessen der Betroffenen nicht überwiegen. Dementsprechend wurde durch die Aufsichtsbehörde bestätigt, dass die beabsichtigte Datennutzung nach dem Bundesdatenschutzgesetz zulässig wäre. Ein entsprechender Abwägungsprozess wurde auch für die Datenübermittlung an das projektführende Unternehmen vorgenommen und deren Zulässigkeit bejaht. Hinsichtlich der Datenübermittlung hätte man zudem Einwilligungen einholen können.

Weiterhin war zu klären, ob die Speicherung der übermittelten Daten (Name und Anschrift) bei der Projektgesellschaft und deren Nutzung für die Übersendung der Fragebögen zulässig ist. Die Zulässigkeit hätte in diesen Fällen aus den Anforderungen des § 4a BDSG entsprechenden Einwilligungen resultieren können. Diese hätten die Ärzte durch die Vorlage von Merkblättern, welche das Unternehmen ihnen zur Verfügung stellen könnte, einholen können.
Aber auch aus § 28 Abs. 1 Satz 1 Nr. 2 BDSG hätte sich die Zulässigkeit ergeben. Danach ist das Speichern personenbezogener Daten oder deren Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Da lediglich die Adressdaten gespeichert und genutzt wurden und keine Anhaltspunkte für überwiegende schutzwürdige Interessen der angesprochenen Patienten bestanden, wurde bestätigt, dass die notwendigen Verarbeitungsschritte datenschutzrechtlich zulässig sind. Weiterhin wurden Hinweise, insbesondere hinsichtlich der Rechte der Betroffenen (§§ 33 ff. BDSG), erteilt. Für die eigentliche Datenerhebung im Fragebogen ist das Bundesdatenschutzgesetz nicht einschlägig, da die Daten in anonymisierter Form erhoben wurden und folglich keine personenbezogenen Daten vorlagen. Dennoch wurde das Unternehmen gebeten, den Senioren das Projekt in dem Begleitschreiben verständlich in eigenen Worten vorzustellen und ihnen mitzuteilen, wie der Umgang mit den erhobenen Daten erfolgt und wofür diese genutzt werden.

In einem anderen Verfahren ging es um das Projekt „Gesellschaft und Demokratie in Europa – Bürger sagen ihre Meinung!“.
Auch bei diesem Projekt sollte eine stichprobenartige Bürgerbefragung stattfinden. Allerdings sollten hierbei die anzuschreibenden Personen durch das Einwohnermeldeamt zufällig ermittelt werden. Das projektführende Institut wollte hierzu eine Melderegistergruppenauskunft auf der Grundlage des Meldegesetzes des Landes Sachsen-Anhalts beantragen und hierbei lediglich vorgeben, dass nur Personen über 15 Jahre in Frage kommen. In derartigen Fällen müssen also die Einwohnermeldeämter prüfen, ob sie befugt zu einer Datenübermittlung, bestehend aus Name und Anschrift, sind. Das Institut wollte die Daten sodann für ihre Anfrage speichern und nutzen. In dem beabsichtigten Anschreiben wurde detailliert das Projekt vorgestellt, darauf hingewiesen, dass die Teilnahme an dem Projekt freiwillig ist und dass der Angesprochene zufällig für die Teilnahme ausgewählt worden sei. Des Weiteren wurde eine Erklärung zum Datenschutz und zur absoluten Vertraulichkeit etwaiger Angaben zur Verfügung gestellt. Insgesamt wurde das Schreiben als gut verständlich eingeschätzt. Aus Transparenzgründen wurde um nähere Erläuterungen den angesprochenen Personen gegenüber gebeten, wie die „zufällige Auswahl“ erfolge. In dem Verfahren sollte zudem keine schriftliche anonymisierte Befragung stattfinden, sondern ein Interviewer den Angesprochenen aufsuchen. Allerdings sollte der Interviewer auf dem Fragebogen nur die Antworten des Befragten, nicht jedoch dessen Name und Anschrift notieren. Mithin sollten auch in diesem Vorhaben anonymisierte Daten erhoben werden, so dass die gesamte aufgezeigte Vorgehensweise als datenschutzrechtlich unbedenklich beurteilt wurde. Eine spätere Anfrage, welche personenbezogenen Daten zu einer teilnehmenden Person gespeichert seien, ergab, dass lediglich Name und Anschrift, also die Daten, die für die Kontaktaufnahme genutzt wurden, gespeichert waren.

4.1.6 Übermittlung personenbezogener Daten an einen Dritten

Viele Anfragen an die Aufsichtsbehörde bezogen sich auf die Zurverfügungstellung von personenbezogenen Daten einem Dritten gegenüber „mal eben schnell".
Eine Datenübermittlung ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass die Daten an den Dritten weitergegeben werden oder der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft. Für eine Übermittlung gibt es Zulässigkeitsalternativen, nämlich die Einwilligung des Betroffenen, die Befugnis bzw. Verpflichtung aufgrund besonderer Rechtsvorschrift oder das Vorliegen von Übermittlungsvoraussetzungen des Bundesdatenschutzgesetzes. Ist die Übermittlung nicht aufgrund einer dieser Alternativen zulässig, muss die Übermittlung der personenbezogenen Daten verweigert werden, auch wenn das Anliegen der anfragenden Stelle nachvollzogen werden kann.

Da die Beurteilung der Zulässigkeit der Datenübermittlung nicht immer einfach ist, baten zahlreiche verantwortliche Stellen die Aufsichtsbehörde vorab um eine Einschätzung der Rechtslage.
Beispielsweise bat ein Krankenhaus um Beurteilung, unter welchen Voraussetzungen Befunddaten des Krankenhauses an den weiterbehandelnden Arzt übermittelt werden dürfen. Ein bislang für eine Einverständniserklärung genutztes Formular wurde vorgelegt. Zudem wurde gebeten, einzuschätzen, auf welchem Weg eine Datenübermittlung stattfinden könne (Fax, E-Mail oder Brief).
Zunächst wurde dem Krankenhaus mitgeteilt, dass es für einzelne Bereiche der ärztlichen Tätigkeit Spezialvorschriften für die Datenverarbeitung, der auch die Datenübermittlung unterfällt, gibt. Insbesondere gehen die Regelungen des Sozialgesetzbuches – Fünftes Buch – Krankenversicherung (SGB V) dem BDSG vor. So bestimmt § 73 Abs. 1b Satz 2 SGB V, dass die einen Versicherten behandelnden Leistungserbringer verpflichtet sind, den Versicherten nach dem von ihm gewählten Hausarzt zu fragen und diesem mit schriftlicher Einwilligung des Versicherten, die widerrufen werden kann, die den Versicherten betreffenden Behandlungsdaten und Befunde zum Zwecke der Dokumentation und der weiteren Behandlung zu übermitteln.
Die schriftliche Einwilligung bezieht sich dabei auf den jeweiligen Behandlungsfall und ist immer wieder neu beim Patienten einzuholen. Eine generelle Einwilligung, die sich auf alle laufenden und künftigen Behandlungsfälle bezieht, ist nicht zulässig. Da das SGB V keine weiteren spezifischen Anforderungen hinsichtlich der Einwilligung enthält, richtet sich diese nach § 4a BDSG bzw. § 67b Abs. 2 SGB X. Dementsprechend wurde dem Krankenhaus dargelegt, dass bei Einholung der den Anforderungen des § 4a BDSG entsprechenden Einwilligungen darauf zu achten ist, dass der Einwilligende eine im Wesentlichen zutreffende Vorstellung davon bekommt, worin er einwilligt. Er muss die Bedeutung und Tragweite seiner Entscheidung überblicken und wissen, aus welchem Anlass und mit welcher Zielsetzung er welche Personen von ihrer Schweigepflicht entbindet und so in die Preisgabe seiner Daten einwilligt.
Unter diesen Aspekten wurde sodann das zur Verfügung gestellte Formblatt „Datenübermittlung an den Hausarzt und/ oder weiterbehandelnden Arzt" überprüft. Nachfolgend wurde darauf hingewiesen, dass die Begrifflichkeiten „Facharzt" und „Hausarzt" in dem Formular teilweise vermischt wurden. Da die Regelungen des § 73 Abs. 1a SGB V allein für die **Haus-**

ärzte gelte, könne es zu Missverständnissen kommen. Zudem wurde empfohlen, dass in dem Formblatt zunächst erläutert wird, wofür die Übermittlung von Behandlungsdaten/ Befunden von Nöten ist und was zu den Behandlungs-/ Befunddaten zählt. Weiterhin wurde das Krankenhaus gebeten, seine Ausführungen um die Folgen der Verweigerung der Einwilligung zu ergänzen und darzustellen, wozu der die Daten erhaltende Arzt befugt ist. Letztlich wurde darauf hingewiesen, dass in Bezug auf das jederzeitige Widerrufsrecht der Einwilligung die Stelle, bei der dieses Recht ausgeübt werden kann, angegeben werden sollte. Ein Schriftformerfordernis bzgl. des Widerrufs ist vom Gesetz nicht vorgesehen. Das Formblatt entsprach insgesamt den Anforderungen des Datenschutzes. Es ist jedoch nach Ansicht der Aufsichtsbehörde mit Blick auf das Verständnis der Patienten verbesserungswürdig gewesen. Darüber hinaus wurde ausgeführt, dass für die Zulässigkeit der Datenübermittlung an einen **Facharzt** eine Schweigepflichtsentbindungserklärung vom Patienten einzuholen ist. Auch eine solche muss regelmäßig schriftlich erfolgen und ist nur wirksam, wenn die betroffene Person ausreichend über Form und Folgen der beabsichtigten Datenverarbeitung unterrichtet wurde und das Einverständnis freiwillig erklärt wird. Auch kann der Patient die Erklärung auf bestimmte Daten und Empfänger beschränken.
Zur Frage der Art der Datenübermittlung wurde ausgeführt, dass sich dies wegen mangelnder spezialgesetzlicher Regelungen an den allgemeinen Regelungen des Bundesdatenschutzgesetzes, insbesondere dem § 9 BDSG, orientiere. Danach haben die nicht-öffentlichen Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführungen des BDSG, darunter die in der Anlage zu § 9 Satz 1 genannten Anforderungen, zu gewährleisten. Daraus resultiert, dass bei der Datenübermittlung im Speziellen auf die Weitergabekontrolle zu achten ist. Im Besonderen sind Maßnahmen zu treffen, die den unbefugten Zugriff – lesen, kopieren, verändern oder entfernen – verhindern. Dies kann beispielsweise bei der Datenübermittlung per E-Mail dadurch geschehen, dass Daten vor der elektronischen Übermittlung verschlüsselt werden. Vor dem „Faxen“ personenbezogener Daten – insbesondere sensibler medizinischer Daten – sollte der Empfänger von der Übermittlung unterrichtet und darum gebeten werden, den datenschutzgerechten Zugang sicherzustellen.

In einem weiteren Vorgang wandte sich eine Kreisvolkshochschule, ein eingetragener Verein, an die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich. Der Verein wurde von einer Krankenkasse um das Ausfüllen eines Fragebogens für einen ihrer Versicherten auf der Grundlage des § 20 Abs. 1 SGB V gebeten. Nach § 20 Abs. 1 SGB V sei es Aufgabe der Krankenkassen im Bereich der Primärprävention tätig zu werden. Man bezuschusse daher die erfolgreiche Teilnahme eines Versicherten an bestimmten Programmen.
In dem von dem Verein auszufüllenden Fragebogen wurden als personenbezogene Daten nach dem Namen des Kursleiters und dessen beruflicher Grundqualifikation und seiner kursbezogenen Zusatzqualifikation gefragt. Zudem sollten Zeugnisse ggf. in Kopie übergeben werden. Der Volkshochschule wurde mitgeteilt, dass die Übermittlung der Daten des Kursleiters als eine Form der Verarbeitung personenbezogener Daten nur zulässig und damit datenschutzrechtlich unbedenklich ist, soweit das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat (§ 4 Abs. 1 BDSG). In diesem Zusammenhang wurde festgestellt, dass der von der Krankenkasse als Rechtsgrund-

lage für die Datenübermittlung angeführte § 20 SGB V keine andere Rechtsvorschrift darstellt, die die Übermittlung der Daten erlaubt oder anordnet. § 20 SGB V verpflichtet die Krankenkassen lediglich, Leistungen zur primären Prävention vorzusehen. Da von einer Einwilligung der Kursleiter zu der Datenübermittlung nicht auszugehen war, konnte sich die Zulässigkeit der angestrebten Datenverarbeitung demzufolge allein aus dem Bundesdatenschutzgesetz, speziell § 28 Abs. 3 Nr. 1 BDSG ergeben. Danach ist die Übermittlung personenbezogener Daten zulässig, soweit es zur Wahrung berechtigter Interessen eines Dritten erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Da jedoch nicht ersichtlich war, aus welchen Gründen der Name des Kursleiters und dessen Qualifikation im Rahmen der Bezuschussung eines Kurses von Belang ist, vermochte die Aufsichtsbehörde kein berechtigtes Interesse zu erkennen. Eine abschließende Stellungnahme konnte dies jedoch nicht darstellen, da dafür die Einbeziehung der Krankenkasse erforderlich gewesen wäre und die anfragende Stelle dies nicht wünschte.

Des Weiteren wurde eine Bank in einem Ermittlungsverfahren wegen des Vorwurfs des Betruges bzgl. eines bei ihr geführten Kontos nach Kontenbewegungen innerhalb eines bestimmten Zeitraumes, dem Verfügungsberechtigten und dessen Anschriften befragt. Die Bank bat die Aufsichtsbehörde um Beurteilung ihrer Auskunftspflicht. In diesem Zusammenhang konnte die Aufsichtsbehörde die Frage nach einer Auskunftspflicht nicht beantworten. Sie konnte der Bank lediglich darstellen, unter welchen Voraussetzungen diese befugt ist, Daten zu übermitteln. Da weder eine Einwilligung des Betroffenen vorlag, noch eine andere Rechtsvorschrift die geforderte Datenübermittlung erlaubte oder anordnete, konnte sich die Zulässigkeit allein aus dem Bundesdatenschutzgesetz ergeben. Es wurde eingeschätzt, dass die Zulässigkeit der Datenübermittlung aus § 28 Abs. 3 Nr. 2 BDSG resultieren könne. Danach ist die Übermittlung personenbezogener Daten für andere Zwecke zulässig, wenn sie zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung der Nutzung hat. Von daher wurde der Bank angeraten, eine Begründung von der Staatsanwaltschaft hinsichtlich der Erforderlichkeit einzuholen, da der im Anschreiben vorgenommene Verweis zu pauschal sei und auch die vorsorglichen Hinweise keinen weiteren Einblick in die Erforderlichkeit der Daten gewährleisten konnten. Es wurde der Bank angeboten, sich nach Vorliegen einer Begründung der Staatsanwaltschaft erneut an die Aufsichtsbehörde zu wenden. Dies erfolgte jedoch nicht.

Ein weiteres Unternehmen strebte eine Betriebsvereinbarung über Urlaubsgrundsätze an. In der Betriebsvereinbarung sollte festgelegt werden, dass einmal jährlich eine Liste ausgelegt werden sollte. Diese Liste sollte je Mitarbeiter Angaben über Name, Vorname, Familienstand, Anzahl der schulpflichtigen Kinder, Urlaubsanspruch im laufenden Kalenderjahr, etwaiger Restanspruch aus dem Vorjahr, gewünschter Urlaubszeitpunkt, besondere Gründe für die Wahl des beantragten Urlaubszeitraums enthalten. Zu der Frage, ob diese Liste frei ausliegen könnte, stellte die Aufsichtsbehörde folgendes fest: Durch das Ausliegen der Liste findet eine Datenübermittlung statt. Die Zulässigkeit dieser Datenübermittlung beurteilte sich nach § 4 Abs. 1 i. V. m. § 28 Abs. 1 Satz 1 Nr. BDSG, sofern keine Einwilligungen der Mitarbeiter i. S. d. § 4a BDSG vorliegen. Nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist die Erhebung und Speiche-

rung personenbezogener Daten zulässig, soweit dies 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. In der gerechten, effektiven Urlaubsplanung und der anschließenden Gewährung wurde ein berechtigtes Interesse des Unternehmens gesehen. Zur Beurteilung der Erforderlichkeit prüfte die Aufsichtsbehörde die einzelnen zur Erhebung beabsichtigten Daten. Sowohl die Angabe des Familienstandes als auch des Urlaubsanspruches im Urlaubsjahr wurden als nicht erforderlich eingeschätzt. Der Anspruch auf Resturlaub, der zu direkten Geldzahlungen führen kann, wurde dagegen als erforderlich angesehen. Auch die Angabe des Urlaubswunsches wurde als notwendig klassifiziert, da allein dieses Datum die Planung möglich macht. Hinsichtlich der besonderen Gründe für die Wahl des beantragten Zeitraumes wurde angegeben, diese als freiwilliges Datum zu kennzeichnen. Hinsichtlich der für erforderlich anerkannten Daten wurde letztlich auch beurteilt, dass kein Grund zur Annahme besteht, dass das schutzwürdige Interesse der Beschäftigten des Unternehmens an dem Ausschluss der Verarbeitung oder Nutzung das berechtigte Interesse des Unternehmens offensichtlich überwiegt. Die Erhebung und Speicherung der erforderlichen Daten ist somit zulässig. Die Übermittlung der Daten an alle Mitarbeiter wurde jedoch als unzulässig beurteilt.

4.2 Was ist zulässig und was nicht – ausgewählte Beschwerdeverfahren

4.2.1 Erhebung von Arbeitnehmerdaten

Arbeitnehmerdaten sind – von Ausnahmen abgesehen – keine über spezielle Gesetze geschützten Daten, sondern unterfallen, wie auch andere personenbezogene Daten, den Regelungen des Bundesdatenschutzgesetzes. Dies bedeutet, dass ihre Erhebung grundsätzlich nur zulässig ist, wenn der Arbeitnehmer in deren Erhebung einwilligt, eine andere Rechtsvorschrift als das Bundesdatenschutzgesetz dies erlaubt oder anordnet oder wenn die Erhebung aufgrund des Bundesdatenschutzgesetzes selbst zulässig ist. Die bloße Erhebung von sogenannten Arbeitnehmerdaten verursacht im Moment der Erhebung nicht das Gefühl, in seinem Persönlichkeitsrecht verletzt worden zu sein. Oftmals tritt die persönliche Betroffenheit erst bei der ggf. unzulässigen Nutzung der Daten zu Tage, der jedoch die erhobenen Daten zu Grunde liegen. Da aus einer unzulässigen Erhebung personenbezogener Daten grundsätzlich keine zulässige Verarbeitung oder Nutzung der Daten resultieren kann, wurde die Sachverhaltsdarstellung der in diesem Zusammenhang geprüften Verfahren allein auf die Beurteilung der Zulässigkeit der Datenerhebung beschränkt.

Personenbezogene Daten von Arbeitnehmern werden nicht selten erhoben, um diese überwachen zu können. Arbeitgeber sind aus unterschiedlichsten Gründen versucht, ihre Mitarbeiter zu „kontrollieren“. Dabei greifen sie auch zum Mittel der Videoaufzeichnung. Dass die Persönlichkeitsrechte der betroffenen Arbeitnehmer – die einem erheblichen Überwachungsdruck ausgesetzt werden – verletzt werden können, ist nicht von der Hand zu weisen. Fest steht, dass eine solche Überwachung, die jede Regung und Bewegung der Mitarbeiter zur Kenntnis nimmt und dokumentiert, nicht mit der Menschenwürde vereinbar ist. Allerdings kann es in Ausnahmefällen zulässig sein, Videoüberwachung vorzunehmen, insbesondere wenn ein hin-

reichend konkreter Verdacht auf heimlich begangene strafbare Handlungen besteht, der nicht oder nur schwer mit anderen, das Persönlichkeitsrecht des Überwachten wahrenden Mitteln, geklärt werden kann.

Einen solchen Sachverhalt schilderte eine Arbeitnehmerin, die drei Wochen heimlich mit einer Videokamera beobachtet wurde, weil der Verdacht bestand, dass sie als Verkäuferin in einem spezifischen Lebensmittelbereich Kaffee ohne Bezahlung an Dritte, darunter Familienangehörige, abgegeben habe. Derartige Umstände waren zunächst angezeigt und sodann von der Marktleiterin beobachtet worden. Da diese Beobachtung jedoch nach Aussagen der verantwortlichen Stelle nicht genügt habe, der Arbeitnehmerin zu kündigen, habe man sich in Zusammenarbeit mit dem Datenschutzbeauftragten und mit Einverständnis des Betriebsrates für eine heimliche Videoüberwachung entschieden. Nachdem die Aufzeichnungen offenbart hatten, dass auch später keine Verbuchung etwaiger Zahlbeträge für den ausgeschenkten Kaffee stattgefunden hat, kündigte man der Verkäuferin fristlos. In erster Linie war seitens der Aufsichtsbehörde zu klären, ob der Arbeitgeber die Verkäuferin zulässig mit Hilfe optisch-technischer Einrichtung beobachten und damit personenbezogene Daten erheben durfte. Da die Arbeitnehmerin in die Datenerhebung nicht eingewilligt hat und auch eine andere Rechtsvorschrift eine derartige Überwachung weder erlaubte noch anordnete, konnte sich die Zulässigkeit der dargestellten Datenerhebung allein aus dem Bundesdatenschutzgesetz ergeben. Im Speziellen konnte sich die Zulässigkeit aus § 6b BDSG – Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen – und § 28 BDSG – Datenerhebung, -verarbeitung und -nutzung für eigene Zwecke – ergeben. In diesem Zusammenhang galt es zunächst zu klären, ob ein Verkaufsraum auch dann als öffentlich zugänglicher Raum zu qualifizieren ist, wenn er auch einen nur den Mitarbeitern zugänglichen Bereich umfasst. Öffentlich zugängliche Räume sind immer solche Räume, die ihrem Zweck nach dazu dienen, von unbestimmt vielen oder nur nach allgemeinen Merkmalen bestimmten Personen betreten und genutzt zu werden. Nach vorherrschender Meinung in der Literatur lässt § 6b BDSG keine Differenzierung in öffentlich zugänglichen Verkaufsbereich und einen nur den Mitarbeitern zugänglichen Bereich zu. Zudem musste bei der in Rede stehenden Datenerhebung auch eine Verknüpfung zwischen der Verkäuferin und den Kunden, denen Kaffee geschenkt wurde, stattgefunden haben, um die Sachlage beurteilen zu können. Durch die Aufsichtsbehörde wurde festgestellt, dass die Zulässigkeit der Videoüberwachung und der damit verbundenen Datenerhebung allein auf der Grundlage des § 6b BDSG zu beurteilen ist. Dies bedeutet, dass die Zulässigkeit sich nach den Tatbestandsmerkmalen „berechtigte Interessen der verantwortlichen Stelle“, „schutzwürdige Interessen des Betroffenen“ und „Erforderlichkeit zur Wahrung der berechtigten Interessen“ i.S.d. § 6b Abs. 1 Nr. 3 BDSG richtet. Ein berechtigtes Interesse des Arbeitgebers an der Aufklärung des Verdachtes wurde anerkannt. Allerdings wurde beurteilt, dass eine Videokamera nur dann eingesetzt werden darf, wenn dies erforderlich ist, also dem Arbeitgeber keine weniger einschneidenden Mittel zur Aufklärung des Verdachtes zur Verfügung stehen. Solche alternativen Maßnahmen können Mitarbeiterkontrollen, Beobachtung der Arbeitnehmer durch andere Mitarbeiter oder Detektiveinsätze sein. Die bereits stattgefundene persönliche Inaugenscheinnahme der Vorkommnisse durch die Marktleitung hätte aber genügt, um eine Pflichtverletzung der Mitarbeiterin festzustellen, da diese verpflichtet ist, bereits mit der Abgabe von Ware eine Verbuchung des Vorganges zu tätigen. Unabhängig davon, ob

es Maßnahmen gibt, die gleichermaßen geeignet sind, ist eine berechtigte und erforderliche Videoüberwachung dennoch unzulässig, wenn die Betroffenen ein schutzwürdiges Interesse haben, das höher zu bewerten ist, als das Erreichen des mit der Beobachtung verfolgten Zwecks. Dies bedeutet, dass eine solche Maßnahme insgesamt nicht unverhältnismäßig sein darf (vgl. Bundesarbeitsgericht, 2. Senat, Urteil vom 27.03.2003, Az: 2 AZR 51/02). In diesem Zusammenhang wurde zwischen dem Gewicht des Rechtsverstoßes, seiner Bedeutung für die rechtlich geschützte Sphäre des Betroffenen und dem staatlichen Interesse an Strafverfolgung abgewogen. Die Interessenabwägung ergab, dass trotz fehlender abschließender arbeitsrechtlicher Beurteilung des Sachverhaltes, zunächst eine Abmahnung der Arbeitnehmerin ausgereicht hätte, damit diese keinen Kaffee mehr unentgeltlich ausschenkt. Insgesamt wurde die heimliche Videoüberwachung unter Würdigung der Gesamtumstände des Einzelfalles für unverhältnismäßig erachtet. Die Videoüberwachung und die daraus resultierende Datenerhebung wurden daher als unzulässig beurteilt.

In einem weiteren Sachverhalt, der unter die Thematik „Überwachung“ gezählt werden kann, wandte sich ein Betriebsrat an die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich des Landes Sachsen-Anhalt. Er schilderte, dass er in einem Prozess gegen „sein“ Unternehmen zugesprochen bekommen habe, dass ihm ein E-Mail-Anschluss als Sachmittel zur Verfügung gestellt werden müsse. Jedoch habe er nachfolgend festgestellt, dass sämtliche E-Mails, deren Adressen mit „*@unternehmensname*.de“ enden, nicht ankommen. Fehlermeldungen würde es jedoch nicht geben, so dass unklar sei, was mit den E-Mails passiere. Man gehe allerdings davon aus, dass die E-Mails auf dem Server des Unternehmens aussortiert werden. Dies habe der Betriebsrat auch gegenüber dem Unternehmen angesprochen. Nachdem keine Änderung erfolgte, wandte man sich an die Aufsichtsbehörde und bat gegenüber dem Unternehmen tätig zu werden. Nachdem dem Betriebsrat geschildert wurde, dass bei ankommenden E-Mails zwischen unerwünschten und infizierten E-Mails zu unterscheiden ist und die Befugnisse eines Unternehmens, entsprechende E-Mails zu identifizieren und Maßnahmen zu ergreifen, die eine Wahrung der IT-Sicherheit im Unternehmen zulassen, von der Zuordnung abhängen, wurde jedoch aufgrund der Sachverhaltsschilderung beurteilt, dass eher eine Filterung unerwünschter E-Mails in Rede steht. Im Hinblick auf dieses Vorgehen konnte jedoch allein auf § 206 Strafgesetzbuch verwiesen werden, dessen Schutzgut die Ungestörtheit des Telekommunikations-Verkehrs ist und der beim unbefugten Unterdrücken, Löschen, Verzögern und Blockieren von E-Mails Anwendung findet. Die Zuständigkeit hinsichtlich der Verfolgung entsprechender Tathandlungen obliegt jedoch der jeweiligen Staatsanwaltschaft. Über diese Verweisung hinaus gab die Aufsichtsbehörde zu bedenken, dass die Einführung von Maßnahmen zur E-Mail-Filterung stets die Zustimmung des Betriebsrates voraussetze. Bei der Einführung derartiger Programme handelt es sich nämlich um technische Überwachungsmaßnahmen nach § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG), weil die verwendeten technischen Einrichtungen regelmäßig geeignet sind, das Verhalten oder Leistung des Arbeitnehmers zu überwachen.

4.2.2 Videoüberwachung in Geschäften

Auch wenn die Kameras in Supermärkten und Geschäften zum Alltagsbild zählen, gibt es Betroffene, die sich zu Recht hinsichtlich dieser an die Aufsichtsbehörde für den Datenschutz wenden. Mal fehlt es an der Beschilderung bezüglich der stattfindenden Videoüberwachung, ein anderes Mal sind Kameras so verdeckt angebracht, dass man sie nur zufällig wahrnimmt. Werden optisch-elektronische Einrichtungen, mit denen in der Regel die Verkaufsfläche der Geschäfte beobachtet wird, bei der Aufsichtsbehörde angezeigt, findet nicht allein eine Überprüfung der aus dem Beschwerdeschreiben ersichtlichen kritischen Aspekte, sondern eine umfassende Prüfung der Zulässigkeit der Überwachungseinrichtungen statt. Entscheidend dabei ist die spezielle gesetzliche Regelung zur Videoüberwachung im privaten Bereich, § 6b BDSG – Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen.

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie
1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechtes oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke
erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.
(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.
(3) Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.
(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend den §§ 19a und 33 zu benachrichtigen.
(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

Da bereits die **reine Beobachtung** der Vorschrift des § 6b BDSG unterfällt, kommt er auch bei reinen Kamera-Monitor-Systemen, bei denen es zwar zu einer Datenerhebung, regelmäßig aber nicht zu einer Datenspeicherung kommt, zur Anwendung. Unerheblich ist zudem, ob die Videoüberwachung analog oder digital erfolgt oder ob es sich bei der Kamera um eine stationäre oder eine mobile Kamera handelt. Auch die eingesetzte Technik (Schwenkbarkeit, Zoom, Auswertungsmöglichkeit, Speicherungsform etc.) spielt hinsichtlich der Anwendbarkeit des § 6b BDSG keine Rolle. Lediglich das private Videografieren als Erinnerung für das persönliche Hauskino soll aufgrund der Zuordnung zum persönlichen oder familiären Bereich nicht erfasst werden. Die Geschäftsräume werden von der Vorschrift erfasst, da es für das Tatbestandsmerkmal **öffentlich**

zugängliche Räume lediglich relevant ist, dass die „Räume“ dem öffentlichen Verkehr gewidmet sind oder dazu dienen, von unbestimmten Personen genutzt bzw. betreten zu werden.
Als Zweck der Legitimierung des Videoeinsatzes beriefen sich die geprüften Unternehmen jeweils auf die Wahrnehmung ihres Hausrechtes i.S.d. § 6b Abs. 1 Nr. 2 BDSG. Wenngleich das Hausrecht den Einsatz von Videoüberwachung praktisch sehr weitgehend rechtfertigen kann, ist ein unzulässiger Eingriff in die Rechte Dritter, was z.B. bei verdeckten Aufnahmen oder bei Eingriffen in besonders geschützte persönliche Bereiche (Eingriff in die Intimsphäre, z. B. auf Toiletten, Umkleidekabinen) regelmäßig der Fall ist, nicht zulässig. Nachdem das Ziel der Videoüberwachung durch die Aufsichtsbehörde geklärt wurde, musste geprüft werden, ob die jeweilige Videoüberwachung zur Erreichung dieses Zieles erforderlich ist. Es war zu prüfen, ob es nicht die Videoüberwachung vermeidende Mittel gibt, um das Ziel zu erreichen. Denkbar ist der Einsatz von Wachpersonal, der Einbau von Sicherheitssystemen etc. Es genügt nicht, von vornherein auf die Videoüberwachung zu setzen, ohne Alternativen geprüft zu haben. Insgesamt ist von der notwendigen Erforderlichkeit der jeweiligen Videoüberwachung, wobei Anzahl der Kameras, Ausrichtung und technische Aspekte zu berücksichtigen sind, nur dann auszugehen, wenn ohne den Technikeinsatz die Überwachung nicht mehr zweckgemäß und wirtschaftlich gewährleistet wäre. Daraus folgt, dass nur dort ein Einsatz von Videoüberwachung in Frage kommt, wo eine Sicherheitsgefahr besteht, die mit der Kameraüberwachung gebannt oder zumindest reduziert werden kann. So muss der Mitteleinsatz in Verkaufsräumen immer in einem ausgewogenen Verhältnis zum Diebstahlsrisiko stehen. Soweit als Ergebnis der Prüfung nur die Videoüberwachung als bestgeeignete Maßnahme in Betracht kommt, wird durch die Aufsichtsbehörde beurteilt, ob die schutzwürdigen Interessen der potentiell videoüberwachten Personen höher als die berechtigten Interessen der verantwortlichen Stelle zu bewerten sind.
So überwiegen schutzwürdige Interessen regelmäßig, wenn sensitive Daten erhoben werden (politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualität) oder die Intimsphäre verletzt wird. Also dort, wo die freie Entfaltung der Persönlichkeit oder die Wahrnehmung von Freiheitsrechten im Vordergrund steht. In der Berichtsperiode ist es durch die Aufsichtsbehörde lediglich in einem Fall zu Beanstandungen hinsichtlich der Zulässigkeit der Beobachtung mit optisch-elektronischen Einrichtungen gekommen (näher siehe Seite 45f.).

Defizite stellte die Aufsichtsbehörde bei der Kenntlichmachung des Umstandes der Beobachtung fest. Beispielsweise fehlte in einem Supermarkt jegliche Kennzeichnung. In einem anderen erfolgte sie erst, nachdem man von der ersten Kamera bereits erfasst wurde. Dabei soll die Kenntlichmachung ermöglichen, dass der Einzelne sich je nach seinen Bedürfnissen dem Erfassungsbereich entziehen kann und die Abschreckungswirkung der optisch-elektronischen Einrichtung verstärkt wird. Zwar schreibt § 6b Abs. 2 BDSG nicht vor, wie der Umstand der Videoüberwachung erkennbar zu machen ist, das am besten geeignete Mittel der Kenntlichmachung dürften aber Hinweisschilder sein. Der Betroffene muss erkennen können, wohin er sich im Fall einer Beschwerde oder zur Geltendmachung seiner Rechte wenden kann. Dies lässt sich ohne großen Aufwand durch Ergänzung des Hinweisschildes um die Benennung der verantwortlichen Stelle und die Angabe von Erreichbarkeitsdaten (Adresse, Telefonnummer) erreichen. Verstößt eine verantwortliche Stelle gegen die Kennzeichnungspflicht, wie in den geprüften Vorgängen regelmäßig festgestellt, kann die Aufsichtsbehörde Beanstandungen aussprechen. Die Zuläs-

sigkeit der weiteren Verarbeitungsschritte richtet sich nach den Absätzen 3 bis 5 des § 6b BDSG. Hervorzuheben ist nochmals, dass mit Videoüberwachungsmaßnahmen zweifellos Risiken für die Persönlichkeitsrechte der erfassten Personen verbunden sind, insbesondere da überwiegend Personen betroffen sein werden, von denen keine die Überwachung rechtfertigende Gefahr ausgeht. Daher ist nach § 4d Abs. 5 BDSG eine Vorabkontrolle regelmäßig dann erforderlich, wenn Überwachungskameras nicht punktuell, sondern in großer Zahl und zentral kontrolliert oder schwenkbar und mit hoher Auflösung angebracht werden. Eine mögliche Verpflichtung zur Durchführung einer Vorabkontrolle zwingt den Betreiber vor Einrichtung eines Überwachungssystems zu einer rationalen Begründung der konkreten Erforderlichkeit und der Erstellung eines Sicherheitskonzeptes.

Checkliste für Verantwortliche und Datenschutzbeauftragte

Aspekte, die die Überwachung mit und ohne Aufzeichnung anbelangen:

- Welche Zwecke sollen mit der Videoüberwachung erreicht werden?
- Ist ein betrieblicher Datenschutzbeauftragter bestellt worden und wird er in das Verfahren einbezogen?
- Soll eine Attrappe oder eine Kamera eingesetzt werden?
- Muss eine Bildaufzeichnung erfolgen oder genügt eine bloße Beobachtung (Monitoring) um die verfolgten Zwecke erreichen zu können?
- Welche Personen bzw. -gruppen werden dabei erfasst?
- Kann der Zweck mit anderen Maßnahmen erreicht werden?
- Welche Bereiche sollen/ dürfen überwacht bzw. nicht einbezogen werden?
- Müssen Schablonen angebracht und der Schwenkbereich der Kameras festgelegt werden?
- Können bestimmte Bereiche der Überwachung elektronisch ausgeblendet werden, z.B. Fenster von Wohnungen innerhalb des Überwachungsbereichs? (Anmerkung: AG Hamburg fordert mechanische Sperre)
- Werden die Hinweisschilder mit einem Text oder Piktogramm einschließlich Namen und Anschrift der verantwortlichen Stelle versehen?
- An welchen Stellen des überwachten Bereichs sind Hinweisschilder anzubringen?
- Ist bei einer Webcam gewährleistet, dass in den Aufnahmen keine Personen erkennbar sind bzw. die Betroffenen in die Datenübermittlung eingewilligt haben mit dem Hinweis, dass die Einwilligung jederzeit widerrufbar ist?
- Wie werden Änderungen der Kameraeinstellung dokumentiert?

Aspekte, die speziell bei der Überwachung mit Aufzeichnung von Belang sind:

- Wird jede Person benachrichtigt, soweit Aufnahmen bzw. Daten dieser zuzuordnen sind oder liegt eine Ausnahme von der Benachrichtigungspflicht i.S.d. § 33 BDSG vor?
- Wie lange werden die Aufzeichnungen aufbewahrt?
- Werden die Bilddaten analog oder digital aufgenommen?
- Wie erfolgt der Transport der Aufnahmen an den Monitor, z.B. über das Internet, per Funk oder über ein Kabel?
- Werden die bei Anlässen festgestellten Ausschnitte von Aufnahmen von den übrigen zu löschenden Aufzeichnungen getrennt?
- Unter welchen Voraussetzungen wird Einsicht in die Aufnahmen genommen?
- Wer hat unter welchen Voraussetzungen Zugriff auf gespeicherte Bilddaten?
- Wie werden die Zugriffsrechte und deren Veränderung dokumentiert?

4.2.3 Auskunfteien

Häufig ist auch die Tätigkeit von Auskunfteien Gegenstand von Beschwerden im Datenschutz. Das Spektrum der in den Beschwerden aufgezeigten Probleme ist umfangreich, angefangen bei der Frage, woher die Auskunftei die Daten hat, ob sie die Daten speichern darf, über die Aussage, dass die Daten vollkommen falsch sind, bis hin zu der Aussage, dass die Daten zweckwidrig genutzt wurden. Obwohl in den Medien nicht selten über Auskunfteien berichtet wird, sind die Beschwerden vielfach gerechtfertigt. Auskunfteien sind solche Unternehmen, die Daten über Privatpersonen oder Unternehmen, insbesondere deren wirtschaftliche Betätigung, Kreditwürdigkeit und Zahlungsfähigkeit „sammeln“ und auf dieser Datenbasis Auskünfte über die wirtschaftlichen Verhältnisse dieser erteilen. Derartige Auskünfte werden i. d. R. eingeholt, um wirtschaftliche Risiken zu senken. Die wohl bekannteste Auskunftei ist die SCHUFA (Schutzgemeinschaft für allgemeine Kreditsicherung). Sie ist eine Gemeinschaftseinrichtung der kreditgebenden Wirtschaft, d.h. solcher Unternehmen, die mit ihren Kunden ein Kreditrisiko eingehen, z. B. die Kreditinstitute, Kreditkartengeber, Leasinggesellschaften und Handels- und Telekommunikationsunternehmen. Weitere große Auskunfteien sind beispielsweise die Creditreform oder Bürgel.

Die Tätigkeit von Auskunfteien vollzieht sich typischerweise in verschiedenen Phasen. Zunächst erfolgt eine Erhebung von Daten bzw. Datenübermittlung von den Geschäftspartnern der Auskunftei zum Zweck der Speicherung und Beauskunftung der Daten durch die Auskunfteien (Einmeldung). In der Phase der Datenverarbeitung ist vor allem die Übermittlung von Daten der Auskunfteien an Dritte von Relevanz. Erheben und verwenden die Auskunfteien personenbezogene Daten, unterliegen sie den Datenerhebungs- und Verwendungsvorschriften des BDSG. Die Zulässigkeit der einzelnen Verarbeitungsschritte richtet sich, sofern keine entsprechende Einwilligung gem. § 4a BDSG der Betroffenen vorliegt, nach § 29 BDSG – Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung.

(1) Das geschäftsmäßige Erheben, Speichern oder Verändern personenbezogener Daten zum Zweck der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunfteien, dem Adresshandel oder der Markt- und Meinungsforschung dient, ist 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.*

§ 28 Abs. 1 Satz 2 ist anzuwenden.

(Dies bedeutet, dass bei der Erhebung personenbezogener Daten die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen sind.)

(2) Die Übermittlung im Rahmen der Zwecke nach Absatz 1 ist zulässig, wenn

1. *a) der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat oder*

b) es sich um listenmäßig oder sonst zusammengefasste Daten nach § 28 Abs. 3 Nr. 3 handelt, die für Zwecke der Werbung oder der Markt- oder Meinungsforschung übermittelt werden sollen, und

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

§ 28 Abs. 3 Satz 2 gilt entsprechend. Bei der Übermittlung nach Nummer 1 Buchstabe a sind die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung von der übermittelnden Stelle aufzuzeichnen. Bei der Übermittlung im automatisierten Abrufverfahren obliegt die Aufzeichnungspflicht dem Dritten, dem die Daten übermittelt werden.

(3) Die Aufnahme personenbezogener Daten in elektronische oder gedruckte Adress-, Telefon-, Branchen- oder vergleichbare Verzeichnisse hat zu unterbleiben, wenn der entgegenstehende Wille des Betroffenen aus dem zugrunde liegenden elektronischen oder gedruckten Verzeichnis oder Register ersichtlich ist. Der Empfänger der Daten hat sicherzustellen, dass Kennzeichnungen aus elektronischen oder gedruckten Verzeichnissen oder Registern bei der Übernahme in Verzeichnisse oder Register übernommen werden.

(4) Für die Verarbeitung oder Nutzung der übermittelten Daten gilt § 28 Abs. 4 und 5.

(5) § 28 Abs. 6 bis 9 gilt entsprechend.

Zur Beurteilung der Zulässigkeit der Erhebung und Speicherung von personenbezogenen Daten hat sich in der Praxis die Einteilung der Daten in verschiedene Kategorien durchgesetzt. Unterschieden wird zwischen den sog. Negativdaten, welche weiche und harte Negativdaten umfassen, und den sog. Positivdaten. Letztere werden nicht von allen Auskunfteien in ihren Datenbestand aufgenommen.
Unter Positivdaten versteht man in der Regel alle Daten, die sich nicht auf vertragswidriges Verhalten des Betroffenen beziehen (z. B. Daten über die Beantragung, Aufnahme, ordnungsgemäße Abwicklung und Beendigung einer Vertragsbeziehung), mit Ausnahme der sog. Identifizierungs- oder Personenstammdaten, zu denen Namen, Anschrift und Geburtsdatum/-ort gehören. Die Positivdaten dürfen den Auskunfteien von ihren Geschäftspartnern grundsätzlich nur aufgrund einer ausdrücklichen vorhergehenden Einwilligung i. S. d. § 4a BDSG übermittelt werden. Als Beispiel einer Einwilligung ist die Unterzeichnung der SCHUFA-Klausel anzuführen. Damit willigt ein Betroffener ein, dass die Vertragspartner der SCHUFA die vorgenannt beschriebenen sog. Positivdaten an die SCHUFA übermitteln dürfen. Wie jede Einwilligung kann der Kunde seine Einwilligung zur Übermittlung von Positivdaten an die SCHUFA zurückziehen. Und obgleich es sich sowohl bei der Unterzeichnung als auch dem Widerruf der SCHUFA-Klausel um eine freiwillige Entscheidung des Kunden handelt, kann es dazu führen, dass dem Kunden bei fehlender Unterzeichnung der Klausel unter Umständen die Eröffnung eines Kontos bzw. der Kredit verwehrt wird. Da weit über 90 % aller deutschen Kreditinstitute Vertragspartner der SCHUFA sind, besteht oft faktisch keine andere Wahl, als der Klausel

zuzustimmen. Sie wird allerdings unzulässigerweise verlangt, wenn ein Vertragsverhältnis mit dem Kreditinstitut begründet werden soll, bei dem das Kreditinstitut nicht in Vorleistungen tritt, z.B. beim Sparbuch oder einem Girokonto auf Guthabenbasis. In derartigen Fällen empfiehlt es sich, den Einzelfall von der Aufsichtsbehörde prüfen zu lassen.
Negativdaten sind dagegen solche, die Auskunft über die nicht vertragsgemäße Abwicklung eines Vertrages geben und lassen Rückschlüsse auf die Zahlungsunfähigkeit oder -unwilligkeit des Betroffenen zu. Dabei sind harte Negativmerkmale solche, die aufgrund objektiver Tatsachen den Rückschluss auf die Zahlungsunfähigkeit oder -willigkeit erlauben (beispielsweise Daten, denen eine gerichtliche Entscheidung zugrunde liegt, wie Angaben über die Durchführung eines Zwangsvollstreckungsverfahrens oder die Eröffnung eines Insolvenzverfahrens). Weiche Negativmerkmale lassen dagegen einen solchen Rückschluss nicht ohne Weiteres zu. Es handelt sich dabei um Angaben, die auf einer einseitigen Rechtsausübung des Geschäftspartners der Auskunftei beruhen, also etwa um Angaben über Mahnungen, Kreditkündigungen, den Lohnabzug im Pfändungsverfahren oder Mahnbescheide. Die Erhebung und Speicherung der Negativmerkmale ist grundsätzlich nach § 29 Abs. 1 BDSG zulässig. Allerdings müssten in beiden Fällen die „Einmelder“ prüfen, ob die Übermittlung der Daten eines Kunden an die Auskunftei zulässig ist. Dies richtet sich nach § 28 Abs. 1 Satz 1 Nr. 2 oder § 28 Abs. 3 Nr. 1 BDSG und ist dann zulässig, wenn sie zur Wahrung berechtigter Interessen der Verwender erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Übermittlung überwiegt. In diesem Kontext ist die Übermittlung eines weichen Negativmerkmals nur möglich, wenn aus dem Verhalten des Betroffenen, das dem Merkmal zugrunde liegt, mit hinreichender Eindeutigkeit auf seine Zahlungsunfähigkeit oder -unwilligkeit geschlossen werden kann.
Die bei Auskunfteien gespeicherten Daten stammen jedoch nicht nur aus übermittelten Daten, sondern auch aus allgemein zugänglichen Quellen wie Telefon- und Adressbüchern, Branchenverzeichnissen oder öffentlichen Registern wie dem Handelsregister oder dem Schuldnerverzeichnis. Nach § 915e Abs. 1 der Zivilprozessordnung (ZPO) können Handels- und Wirtschaftsauskunfteien Abdrucke des Schuldnerverzeichnisses erhalten. Die Aufsichtsbehörde wird in diesen Fällen entsprechend informiert. Bei der Herkunft der Daten aus allgemein zugänglichen Quellen, zu denen jedoch nicht solche zählen, bei denen die Möglichkeit der Einsichtnahme vom Vorliegen eines „berechtigten Interesses“ oder sonstiger materieller Anforderungen abhängig ist, richtet sich die Zulässigkeit des geschäftsmäßigen Erhebens, Speicherns oder Veränderns der personenbezogenen Daten nach § 29 Abs. 1 Satz 1 Nr. 2 BDSG.

Darüber hinaus „informieren“ Auskunfteien teilweise die Betroffenen mit Anschreiben, in denen sie mitteilen, welche Daten sie über die Betroffenen gespeichert haben. Gleichzeitig werden die Betroffenen jedoch aufgefordert, Selbstauskünfte über ihre Wirtschafts- und Vermögensverhältnisse zu erteilen, um von vornherein eine Speicherung unrichtiger Daten zu vermeiden oder überhaupt Datenmaterial zu erhalten. Es wird darauf hingewiesen, dass eine solche Selbstauskunft **stets freiwillig** ist.

Von besonderer Relevanz für die Betroffenen ist die Frage, wem die Auskunftei welche Daten übermittelt. Die an die Geschäftspartner (Kunden) der Auskunftei übermittelte Auskunft zu einem Betroffenen variiert nach Inhalt und Umfang von Auskunftei zu Auskunftei und ggf.

auch nach den jeweils angebotenen Dienstleistungen. In der Regel enthält eine Auskunft die Stammdaten zu der Person. Daneben werden Angaben über den Beruf des Betroffenen und die allgemeine Vermögenslage (z.B. regelmäßiges Einkommen, Immobilienbesitz), über Bankkonten, Kreditanträge und Kreditvergaben, ausgegebene Kreditkarten, offene Forderungen, eingeleitete Inkasso-, Mahn-, Vollstreckungs- oder Insolvenzverfahren, Haftandrohungen und unausgeglichene Forderungen beauskunftet. Die Zulässigkeit der Datenübermittlung richtet sich insbesondere nach § 29 Abs. 2 Satz 1 Nr.1a und 2 BDSG, wonach die Übermittlung nur zulässig ist, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der personenbezogenen Daten glaubhaft dargelegt hat und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Berechtigte Interessen können vorliegen, wenn die Anfrage vor einem konkreten Vertragsabschluss getätigt wird und die Informationen benötigt werden, um das mit dem Geschäft verbundene finanzielle Risiko besser abschätzen zu können. Allerdings kann nicht jedes wirtschaftliche Interesse eine Abfrage bei einer Auskunftei rechtfertigen.

In zwei der Aufsichtsbehörde vorliegenden Verfahren erhielten die Betroffenen ein Anschreiben mit dem Betreff „Aktualisierung der Auskunftsunterlagen über Ihre Firma“. Bei den Firmen handelte es sich jeweils um Einzelfirmen, so dass die von der Auskunftei bereits gespeicherten und den Betroffenen mit dem Schreiben zur Verfügung gestellten Daten personenbezogene Daten darstellen und unter den Schutzbereich des Bundesdatenschutzgesetzes fallen. Es wurde darum gebeten, die Rechtmäßigkeit der Auskunftei und deren Geschäftsidee zu prüfen bzw. zu prüfen, inwieweit die Auskunftei Daten speichern und an Dritte weitergeben darf.
In einem Verfahren wurden die von der Auskunftei übermittelten Daten von der Betroffenen als falsch gekennzeichnet. Bei derartigen Beschwerden wird die Auskunftei um Stellungnahme gebeten, auf welcher Rechtsgrundlage sie die in Rede stehenden Daten speichern und übermitteln darf und aus welchen Quellen die Daten resultieren. Dies wird sodann bei der Aufsichtsbehörde einer Prüfung unterzogen und, sofern es keinen Grund zu Beanstandungen gibt, den Betroffenen mitgeteilt. In den vorgenannten Verfahren wurden die Daten zulässig auf der Grundlage des § 29 Abs. 1 Satz 1 Nr. 2 BDSG gespeichert. Konkrete Datenübermittlungen, die unzulässig erfolgt sein könnten, konnte die Aufsichtsbehörde wegen fehlender Kenntnis etwaiger Zweifel nicht feststellen. Ebenso keiner detaillierten Überprüfung unterzogen wurde der Vortrag der Betroffenen, dass bereits bei der Auskunftei gespeicherte Daten unrichtig seien. Hierzu wurde um weitere Ausführungen der Betroffenen gebeten, um ggf. einen Löschungsanspruch nach § 35 Abs. 1 BDSG durchsetzen zu können. Ergänzende Ausführungen wurden jedoch nicht getätigt.

In einem anderen Verfahren wandte sich der Betroffene an die Aufsichtsbehörde, weil er von einer Kanzlei für Wirtschaftsauskünfte ein Schreiben mit dem Betreff „Information gemäß der Bestimmung des BDSG § 33“ erhielt. In diesem wurde er von dem Unternehmen darauf hingewiesen, dass über seine Person erstmalig personenbezogene Adressdaten gespeichert wurden. Dem Betroffenen war unerklärlich, wie das Unternehmen zu seinen Adressdaten gekommen ist und bat darum, die Herkunft der Daten zu klären und eine Löschung der Daten zu veranlassen. Unter Mitteilung der Sach- und allgemeinen Rechtslage wurde die vermeintliche Auskunftei um Mitteilung gebeten, warum die Erhebung und Speicherung der Daten des Be-

troffenen ihrer Ansicht nach zulässig gewesen ist. Hierzu wurde auch um Ausführungen gebeten, welche Daten zu seiner Person gespeichert sind, woher diese resultieren, an wen die Daten weitergegeben werden, und über den Zweck der Speicherung.
In der Stellungnahme wurde ausgeführt, dass die Daten von einem Großversandhaus zur Überprüfung der Gültigkeit der Adresse übermittelt und lediglich zu diesem Zweck gespeichert wurden. Es wurde betont, dass die Daten nicht zur Übermittlung zum Zwecke des Adresshandels, der Werbung und/oder der Markt- und Meinungsforschung gespeichert wurden. Insgesamt wurde festgestellt, dass es sich trotz der Bezeichnung des Unternehmens als Kanzlei für Wirtschaftsauskünfte bei der konkreten Tätigkeit nicht um eine solche handelt, die als geschäftsmäßige Datenerhebung und -speicherung zum Zwecke der Übermittlung einzustufen ist. Daher wurde dem Betroffenen mitgeteilt, dass das Unternehmen mit dem an ihn gerichteten Schreiben seiner aus § 33 Abs. 1 Satz 1 BDSG resultierenden Verpflichtung nachkommen wollte. Danach ist der Betroffene von der verantwortlichen Stelle zu benachrichtigen, wenn erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert werden. Die Benachrichtigung umfasst die Nachricht über die Tatsache der Speicherung, die Art der gespeicherten Daten, die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Identität der verantwortlichen Stelle. Wären dagegen personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung ohne Kenntnis des Betroffenen gespeichert worden, wäre der Betroffene nach § 33 Abs. 1 Satz 2 BDSG erst von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen gewesen. Der Betroffene wurde jedoch lediglich über die Speicherung an sich benachrichtigt. Die Aufsichtsbehörde geht jedoch davon aus, dass es bei korrekter Erfüllung der Verpflichtung durch die verantwortliche Stelle, auf die diese hingewiesen wurde, nicht zu einer Beschwerde gekommen wäre. Insgesamt wurde festgestellt, dass die Vorgehensweise des Unternehmens grundsätzlich datenschutzkonform war. Dementsprechend bestand kein Anspruch auf sofortige Löschung der Daten wegen unzulässiger Speicherung nach § 35 Abs. 2 Satz 2 Nr. 1 BDSG.

Weiterhin kam es zu einer Beschwerde wegen unzulässiger Datenerhebung von einer Auskunftei und anschließender Nutzung der Daten.
Konkret kaufte ein Betroffener bei einer Privatperson, die in gehobener Position bei einer Bank tätig ist, einen im Internet angebotenen Pkw. Als er zufällig auf www.meineschufa.de prüfte, welche Daten die SCHUFA über ihn gespeichert hat, stellte er fest, dass vorgenannte Bank im Zeitpunkt der privaten Vertragsverhandlungen eine Anfrage über seine Person bei der SCHUFA getätigt hat. Am gleichen Tag wurde der Kaufvertrag geschlossen. Da der Betroffene sich in seinem Persönlichkeitsrecht verletzt fühlte und keinerlei Kontakte zu der Bank unterhielt, fragte er selbst bei der Bank nach dem Grund der SCHUFA-Auskunft nach. Die Bank teilte ihm daraufhin mit, dass eine Kontrollanfrage stattgefunden habe, aber eine Dokumentation über den Grund der Anfrage und ein Geschäftsverhältnis jedoch nicht vorhanden seien. Man entschuldigte sich für die fehlende Nachvollziehbarkeit der Anfrage und versprach, die Anfrage aus den Daten der SCHUFA löschen zu lassen. Wenngleich die Bank einräumte, dass die Datenerhebung unzulässig erfolgt war, fanden seitens der Aufsichtsbehörde weitere Sachverhaltsermittlungen hinsichtlich der Frage, wer die Anfrage getätigt hat und wie im Rahmen der organisatorischen Maßnahmen dafür Sorge getragen wird, dass nur Berechtigte das Datenverarbeitungssystem nutzen können, statt. Da die Datenerhebung unzulässig erfolgte, wird ein Ordnungswidrigkeitenverfahren eingeleitet.

4.2.4 Übermittlung personenbezogener Daten

Es kommt nicht nur vor, dass Auskunfteien oder Adresshändler geschäftsmäßig personenbezogene Daten übermitteln, die bei ihnen gespeichert werden. Auch Stellen, die Daten für eigene Zwecke erheben, verarbeiten oder nutzen, übermitteln personenbezogene Daten. Eine Datenübermittlung i.S.d. Bundesdatenschutzgesetzes kann durch Weitergabe, Einsehen oder Abruf personenbezogener Daten erfolgen. Nach § 3 Abs. 4 Nr. 3 BDSG ist das *Übermitteln 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.

Es wird also nicht nur die bloße Übergabe von Daten als Datenübermittlung erfasst, sondern auch das Bekanntgeben personenbezogener Daten im Rahmen von geschaffenen Einsichts- oder Abrufmöglichkeiten.

Liegt keine den Anforderungen des § 4a BDSG entsprechend wirksame Einwilligung vor und erlaubt auch eine andere Rechtsvorschrift eine Übermittlung der Daten nicht, kann sich die Zulässigkeit der Datenübermittlung für eigene Zwecke allein aus § 28 BDSG ergeben.

In einem von der Aufsichtsbehörde zu prüfenden Sachverhalt nahm eine Wohnungsgenossenschaft in einem ihrer Mietshäuser einen Aushang mit einer Abfrage zur Heizperiode vor. Aus diesem waren die Mieternamen und die von ihnen gemieteten Wohneinheiten ersichtlich. Darin sollten die Mieter ankreuzen, ob sie gegen oder für eine Heizperiode im Sommer seien. Zusätzlich zu den bereits notierten Daten wurde noch die Meinung der Mieter als weiteres personenbezogenes Datum erhoben und nachfolgend durch den Aushang an alle die Liste einsehenden Mieter und ggf. andere im Gebäude aufhaltenden und einsehenden Personen übermittelt. Nach einer Schilderung der Sach- und allgemeinen Rechtslage wurde das Unternehmen gebeten, anzugeben, woraus die Zulässigkeit der Datenübermittlung resultiert. Hierbei sollte nicht lediglich die Zulässigkeitsnorm angegeben werden, sondern es sollten gegebenenfalls vorgenommene Abwägungen klar zu erkennen sein. Das Unternehmen erklärte in seiner Stellungnahme, dass die Befragung ein wichtiges Instrument der Mitbestimmung in einer Genossenschaft sei und die Mieter, die nicht mittels des Aushanges abstimmen wollen, genügend andere Möglichkeiten der Meinungsäußerung hätten. Darüber hinaus sei die Befragung ohnehin freiwillig. Es wurde um eine abschließend Entscheidung über die Zulässigkeit der Verfahrensweise der Abstimmung gebeten.
Die Wohnungsgenossenschaft wurde darauf hingewiesen, dass sie bei zukünftigen Aushängen auf die verschiedenen Möglichkeiten der Meinungsabgabe, z. B. direkt bei den Mitarbeitern der Wohnungsgenossenschaft, hinweisen solle. Gäbe es nur die Möglichkeit, seine Meinung in dem Aushang kundzutun, würde der Erhebung der Daten möglicherweise eine unzulässige Datenübermittlung nachfolgen, da weder eine andere Rechtsvorschrift noch das Bundesdatenschutzgesetz dies erlaube oder anordne. Insbesondere greift nicht § 28 BDSG, da es sich bei einer Meinung stets um ein sensitives Datum handelt und es nicht erforderlich ist, dieses an andere Mietparteien zu übermitteln. Zudem stellt das bloße Eintragen der Daten in den Aushang keine wirksame Einwilligung i. S. d. § 4a BDSG in die Datenübermittlung dar.

Zwar konnte sich prinzipiell die Zulässigkeit der in Rede stehenden Datenübermittlung auf der Basis von Einwilligungen ergeben, doch dazu hätten die Mieter erkennen können müssen, dass sie in eine Datenübermittlung eingewilligt haben. Gibt es keine andere Möglichkeit zur Meinungsabgabe und verweigert ein Mieter eine Einwilligung zur Datenübermittlung, z.B. indem er seine Meinung aus diesem Grund nicht kundgibt, sollte er vorab die Folgen der Verweigerung der Einwilligung kennen.

Im Bereich des Mietverhältnisses ist der Aufsichtsbehörde zudem ein Sachverhalt aufgezeigt worden, in dem sich ein Mieter wegen Lärmbelästigung durch seinen Nachbarn bei dem für die Vermietung verantwortlichen Unternehmen beschwert hat. Dieser hat das Beschwerdeschreiben zur Aufklärung der Lärmbelästigung fotokopiert und weiteren Nachbarn zur Verfügung gestellt. Dem Beschwerdeschreiben waren Name, Anschrift, Telefonnummer, Faxnummer und die Auffassung des sich beschwerenden Mieters bezüglich der Lärmzustände zu entnehmen. In seiner Stellungnahme zur Zulässigkeit der erfolgten Datenübermittlung machte das Unternehmen geltend, dass diese aus § 28 Abs. 1 Satz 1 Nr. 1 BDSG resultiere. Danach ist die Übermittlung personenbezogener Daten für die Erfüllung eigener Geschäftszwecke zulässig, wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient. Es wurde zwar durch die Aufsichtsbehörde anerkannt, dass aus einem Mietvertrag die Verpflichtung des Vermieters resultiere, die Mietsache im vertragsgemäßen Zustand zur Verfügung zu stellen. Demzufolge müsse der Vermieter auch etwaigen Beschwerden nachgehen. Allerdings muss sich die Übermittlung der Daten im Rahmen der Ermittlungen auf die Verwendung der für den konkreten Vertragszweck objektiv erforderlichen Daten beschränken. Dabei ist insbesondere bei Werturteilen Zurückhaltung angebracht, da sich der Zusammenhang mit dem Vertragszweck gerade bei solchen Aussagen leicht verwischt und die Verarbeitung von Werturteilen die Betroffenen besonders gefährdet. Insgesamt wurde daher entschieden, dass im Rahmen der reinen Sachverhaltsfeststellungen kein Bezug zu den Betroffenen hätte hergestellt werden müssen. Beispielsweise hätten die einbezogenen Mieter ohne weitere Namensnennung zu den Lärmimmissionen befragt werden können. Weiterhin hätten sie gebeten werden können, das Belästigungspotential zu beschreiben. Da die Datenübermittlung nicht für erforderlich gehalten wurde, konnte sich die Zulässigkeit auch nicht aus anderen Alternativen des § 28 BDSG ergeben. Die Datenübermittlung war unzulässig.

Weiterhin wurde der Aufsichtsbehörde ein Sachverhalt geschildert, in dem eine Person ein Bautagebuch über den Fortschritt des Baus seines Einfamilienhauses führte und dieses via Internet allen potentiellen Usern zugänglich machte. In diesem Bautagebuch wurden insbesondere auch kritische Bemerkungen zu namentlich benannten Einzelfirmen getätigt. Mithin kam es zu einer Datenübermittlung, deren Zulässigkeit es zu beurteilen galt. Im Rahmen der Ermittlungen stellte sich heraus, dass die Person, die mittels des Bautagebuches über den Fortschritt des Baus berichtete, einen Generalübernehmer mit dem Bau seines Einfamilienhauses beauftragt hat. Seitens der Aufsichtsbehörde wurde beurteilt, dass die Datenübermittlung mangels Einwilligung der Betroffenen und anderer Rechtsvorschrift allein auf der Grundlage des § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig sein könnte. Danach ist die Übermittlung personenbezogener Daten für eigene Zwecke nur zulässig, 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. In diesem Zusammenhang wurde beurteilt, dass die Privatperson kein berechtigtes Interesse an der Datenübermittlung hat. Aufgrund seiner Entscheidung, einen Generalübernehmer mit dem Bau seines Hauses zu beauftragen, welcher ein fertiges Haus schuldet, jedoch Subunternehmer nach eigener Auffassung in seinen Auftrag integrieren kann und folglich auch beurteilen muss, ist es nicht Aufgabe der Privatperson, die Subunternehmer zu beurteilen. Auch unter der hypothetischen Annahme eines berechtigten Interesses wurde beurteilt, dass Grund zu der Annahme überwiegender schutzwürdiger Interessen des Betroffenen bestanden, da die Ausführungen im Bautagebuch allein ein subjektives Urteil des Schreibenden beinhalteten, jedoch zu vermuten ist, dass dieses von durchschnittlichen Lesern als korrekt angenommen wird.

4.2.5 Nutzung personenbezogener Daten für Zwecke der Werbung

Ein jeder kennt die Situation des täglichen Leerens seines Briefkastens. An bestimmten Tagen, insbesondere mittwochs und an den Wochenenden, droht er nahezu überzuquellen. Flyer, Prospekte, „an alle Haushalte“ adressierte Schreiben sind schnell entsorgt, auch wenn man bei der Flut an Werbematerialien aufpassen muss, nichts Wichtiges auszusortieren. Schwieriger ist es allerdings bei adressierten Schreiben, hinter denen regelmäßig etwas Wichtiges, Persönliches vermutet wird. Umso größer ist die Verärgerung, wenn man seine Briefe öffnet und sich Werbung für Kredite, Arzneimittel oder sonstige Dinge offenbaren. Unverlangte Werbung wird meist als störend empfunden.

Nicht selten stellt sich für die von adressierten Werbeschreiben betroffenen Bürger die Frage, wie die werbenden Unternehmen an die genutzte Anschrift kommen, wenn man noch nie mit dem Unternehmen in Kontakt gestanden hat. Die Wege dafür sind unterschiedlich. Einige Unternehmen führen Preisausschreiben, Verlosungen oder Informationsveranstaltungen durch, um an Anschriften und werberelevante Informationen zu gelangen. Auch Kundenbindungs- und Rabattsysteme dienen häufig diesem Zweck. Viele Werbende greifen darüber hinaus auch auf Adressbestände von sogenannten Adresshändlern zurück. Diese vermieten oder verkaufen speziell nach den Wünschen ihres Kunden, den werbenden Unternehmen, zugeschnittene Adressdaten, die sie meist aus der Auswertung öffentlich zugänglicher Quellen (Adress- und Telefonbücher, Branchenverzeichnisse, Handels- und Vereinsregister etc.) ermittelt haben. Bei den sog. Adresshändlern können die werbenden Unternehmen die Adressdatenbestände erwerben und selbst den Versand ihrer Werbeschreiben vornehmen, zahlreiche Unternehmen übergeben jedoch ein erstelltes Werbeschreiben und übertragen dem Unternehmen den Versand, welches die Daten tatsächlich gespeichert hat. Der Versand erfolgt dann unter dem Namen des werbenden Unternehmens, ohne das dieses Kenntnis von personenbezogenen Daten hat. Diese erhält das werbende Unternehmen erst, wenn jemand auf die Werbeofferte reagiert.

Die Übermittlung und Nutzung einiger personenbezogener Daten (Zugehörigkeit zu einer Personengruppe, Berufs-, Branchen- oder Geschäftsbezeichnung, Name, Titel, akademischer Grad, Anschrift und Geburtsjahr) zu Werbezwecken ist infolge der Regelung des § 28 Abs. 3 Nr. 3 BDSG möglich, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat. Sobald die verantwortliche Stelle also Zweifel hätte, dass schutzwürdige Interessen der Betroffenen ihre Belange überwiegen, hat sie die Nutzung und Übermittlung der Daten zu unterlassen. Daraus resultiert, dass die Nutzung und Übermittlung der von § 28 Abs. 3 Nr. 3 BDSG erfassten Daten zwar in gewissem Maß erleichtert wird. Zum Ausgleich räumt § 28 Abs. 4 BDSG den Belangen der Betroffenen aber ein Widerspruchsrecht ein. Der Betroffene kann der Nutzung oder Übermittlung der eigenen Daten für Werbezwecke oder Markt- und Meinungsforschung widersprechen. Damit wird dem Willen des Bürgers, frei von der Suggestivwirkung der Werbung zu bleiben und seinen Lebensbereich von jedem Zwang der Auseinandersetzung mit Werbung nach Möglichkeit freizuhalten, Rechnung getragen. Bei Ansprachen zum Zwecke der Werbung, aber auch der Markt- oder Meinungsforschung, hat eine Unterrichtung über die verantwortliche Stelle sowie das Widerspruchsrecht zu erfolgen. Die Unterrichtung muss spätestens zum Zeitpunkt der Ansprache erfolgen. Sie muss in einer Weise geschehen, die es dem Betroffenen erlaubt, nicht nur den Verwendungszweck klar zu erkennen, sondern auch und gerade zur Kenntnis zu nehmen, dass ihm ein Widerspruchsrecht zusteht.
Nach erfolgtem Widerspruch dürfen die Daten nicht mehr zu den genannten Zwecken verwendet werden. Sofern die verantwortliche Stelle die Daten nicht nur für Werbezwecke gespeichert hatte, ist das speichernde Unternehmen nicht verpflichtet, den Datensatz zu löschen. Oftmals bleibt der Adressdatensatz im Unternehmen in einer separaten Datei mit dem Vermerk gespeichert, dass vom Werbewiderspruchsrecht Gebrauch gemacht wurde. Mittels dieser Datenspeicherung ist es möglich, neu erworbene Adressdaten mit den „ausgesonderten“ Daten zu vergleichen.

Formulierung Ihres Werbewiderspruches

„Ich widerspreche der Nutzung oder Übermittlung meiner Daten für Zwecke der Werbung und/ oder für die Markt- oder Meinungsforschung."

Auch können Sie bereits bei Vertragsabschlüssen auf Vertragsformularen folgenden handschriftlichen Vermerk anbringen: „Bitte keine Übermittlung oder Nutzung meiner Daten zu Werbezwecken!". Seriöse Vertragspartner respektieren diesen Vermerk.

Weitere praktische Tipps

Der Briefkastenaufkleber „Keine Werbung bitte" schützt vor Werbematerial, das **nicht persönlich** an Sie adressiert ist. Die Zusteller von Werbematerial müssen sich an Ihren auf diesem Weg geäußerten Wunsch halten. Tun sie es nicht, können Sie selbst oder ein Verbraucherverband gegen das Verteiler- bzw. Werbeunternehmen rechtlich vorgehen.

Um sich vor persönlich an Sie adressierten Werbezuschriften zu schützen, bietet der private Deutsche Direkt-Marketing-Verband (DDV) Verbraucherinnen und Verbrauchern an, sich in die sogenannte Robinson-Liste eintragen zu lassen. Ein Formular für die Aufnahme in die Robinsonliste erhalten Sie bei DDV, Robinson-Liste, Postfach 1401, 71243 Ditzingen. Die dem DDV angeschlossenen Unternehmen erhalten dann die Nachricht, dass Sie keine Werbung wünschen. In der Regel überprüfen die angeschlossenen Unternehmen auch ihre Adresslisten anhand der Robinson-Liste. Darüber hinaus können Sie auch die Annahme an Sie adressierter Werbebriefe verweigern. Dazu streichen Sie Ihre Adresse durch, vermerken Sie „Zurück an Absender" und stecken Sie den Brief unfrankiert in die Post. Gewissenhafte Unternehmen werden nachfolgend Ihre Anschrift auf ihre interne „Sperrliste" setzen.

In einem der Aufsichtsbehörde geschilderten Sachverhalt erhielt die Betroffene immer wieder Newsletter eines Unternehmens, obwohl sie dem Unternehmen ihre E-Mail-Adresse zu keiner Zeit zur Verfügung gestellt hatte. Daraufhin wurde das Unternehmen seitens der Aufsichtsbehörde angeschrieben. Es wurde diesem gegenüber festgestellt, dass die Zusendung der in Rede stehenden E-Mails als Ansprachen zum Zwecke der Werbung zu qualifizieren seien. Demzufolge wurde um eine Stellungnahme gebeten, die Ausführungen hinsichtlich des Widerspruchsrechts, der Zulässigkeit der Datenerhebung, -speicherung und -nutzung und des Auskunftsrechts nach § 34 Abs. 1 BDSG, insbesondere hinsichtlich der Herkunft der genutzten Daten beinhalten sollte. Nachfolgend stellte sich heraus, dass die Betroffene an einem Bewerbungsverfahren des Unternehmens teilgenommen hatte. Ihre Daten gab sie im Rahmen der Registrierung preis und erklärte im Wege des Opt-In-Verfahrens, d.h. durch Ankreuzen, ausdrücklich ihr Einverständnis, zukünftig Werbung von dem Unternehmen zu erhalten. Das Unternehmen teilte mit, dass das Schreiben der Aufsichtsbehörde zum Anlass genommen wurde, die E-Mail-Adresse der Betroffenen zu löschen, so dass sie zukünftig keine Werbung mehr erhalten wird.

In einer weiteren Angelegenheit tätigte ein Betroffener bei einem kreditvermittelnden Unternehmen eine unverbindliche Anfrage per E-Mail. Ein Vertragsverhältnis ist nicht zustande gekommen. Dennoch erhielt er einige Zeit später E-Mails mit Werbeinhalt. Da er dem Unternehmen nie seine Zustimmung zur Nutzung seiner Daten für Werbung gegeben hatte, verlangte er von dem Unternehmen die Löschung seiner Daten und eine Bestätigung, dass die Daten gelöscht wurden. Nachdem das Unternehmen auf seine entsprechende E-Mail nicht reagierte, wandte er sich an die Aufsichtsbehörde. Diese schilderte dem verantwortlichen Unternehmen die Sach- und allgemeine Rechtslage und bat um eine Stellungnahme, die insbesondere Ausführungen hinsichtlich des Widerspruchsrechtes, des Auskunftsrechtes und der Zulässigkeit von Datenerhebung, -speicherung und -nutzung umfassen sollte. Gleichzeitig wurde um Mitteilung gebeten, ob in dem Unternehmen ein Beauftragter für den Datenschutz bestellt ist, ggf. warum keine Verpflichtung zur Bestellung eines solchen besteht. Sofern ein Beauftragter bestellt sei, sollte der Aufsichtsbehörde gegenüber ausgeführt werden, woraus dessen zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit resultiert und wie er in den konkreten Sachverhalt einbezogen wurde.
Nach einigen Mahnungen wegen ausgebliebener Stellungnahme teilte das Unternehmen mit, dass die Daten des Betroffenen gelöscht wurden und eine Reaktion auf die E-Mail des Betroffenen nicht erfolgte, da die Anfrage des Betroffenen vom betreuenden IT-Unternehmen falsch kategorisiert worden sei.
Da mit diesen Ausführungen der Bitte um Stellungnahme nur bedingt nachgekommen wurde, bat die Aufsichtsbehörde um ergänzenden Vortrag. Daraufhin führte die anwaltliche Vertretung des Unternehmens aus, dass die Daten bei Besuch der Homepage des Unternehmens auf der Grundlage von Einwilligungen erhoben würden. Die Einwilligung resultiere daraus, dass man den Allgemeinen Geschäftsbedingungen zustimmt. In diesen werde auch darauf hingewiesen, dass die Daten neben dem Zweck der Angebotserstellung auch zu Marketing-, Kundenbetreuungs-, Marktforschungs- und Werbezwecken verarbeitet werden.
Dieser Rechtsauffassung folgte die Aufsichtsbehörde jedoch nicht. Zwar kann eine Einwilligung des Betroffenen auch in elektronischer Form abgegeben werden, doch auch elektronische Einwilligungen sind nur unter bestimmten Bedingungen wirksam. Zu den Bedingungen zählt, dass eine Einwilligung nachweisbar durch den Betroffenen vorgenommen wurde und ihm zugeordnet werden können muss. Des Weiteren kommt es darauf an, die Authentizität der Erklärung zu gewährleisten und mögliche Modifikationen und Verfälschungen durch nicht erkennbare Eingriffe auszuschließen. Zudem kann eine Einwilligung nur wirksam abgegeben werden, wenn man den Umstand einer Einwilligung auch wahrnehmen kann. Dies ist bei einer Passage in den Allgemeinen Geschäftsbedingungen nicht der Fall. Demnach lag in dem geprüften Sachverhalt keine wirksame Einwilligung vor und die Zulässigkeit der Datenerhebung, -speicherung und -nutzung konnte sich allein aus dem Bundesdatenschutzgesetz ergeben. Diese lag mangels anderer Anhaltspunkte nach § 28 Abs. 1 Satz 1 Nr. 2 und § 28 Abs. 3 Nr. 3 BDSG vor. Allerdings wurde festgestellt, dass der Betroffene nicht über die verantwortliche Stelle und das ihm zustehende Widerspruchsrecht unterrichtet wurde.

In einem weiteren beispielhaft aufzuzeigenden Vorgang wurde der Betroffene von seinem ehemaligen Verein telefonisch kontaktiert. In dem Telefonat wurde er gefragt, ob er bereit wäre, eine erneute Mitgliedschaft einzugehen oder einen einmaligen Beitrag zu leisten. Dies habe er verneint, jedoch hinsichtlich etwaiger Einzelspenden zu einem späteren Zeitpunkt seine Bereitschaft

signalisiert. Er erhielt ein Schreiben des Vereins, in diesem ihm für seine Entscheidung, den Verein wieder zu unterstützen, gedankt wurde. Gleichzeitig wurde ihm mitgeteilt, dass ein bestimmter Geldbetrag von seinem Konto abgebucht werde.
Aus dem geschilderten Sachvortrag wurde ersichtlich, dass der Verein personenbezogene Daten des Betroffenen gespeichert und genutzt hat. Es galt zu klären, ob beide Verfahrensschritte zulässig erfolgten. Der Verein wurde gebeten, in einer Stellungnahme mitzuteilen, woraus sich die Zulässigkeit der andauernden Speicherung und Nutzung der Daten (wobei Anschreiben und Abbuchung separiert erörtert werden sollten) resultiert. Da die Datennutzung zum Zwecke der Werbung erfolgte, sollten zudem Ausführungen zum Widerspruchsrecht getätigt werden. In seiner Stellungnahme führte der Verein aus, dass die Daten nur versehentlich im Rahmen des Direktmarketings genutzt worden seien. Die Daten des Petenten seien bereits gelöscht worden. Darüber hinaus vertrat die verantwortliche Stelle die Auffassung, dass das Schreiben lediglich die Bereitschaft zur Fördermitgliedschaft bestätigen und zur technischen Abwicklung von Spenden und Beiträgen dienen sollte. Demzufolge würde § 28 Abs. 4 BDSG keine Anwendung finden. Seitens der Aufsichtsbehörde wurde der Betroffene über die Löschung seiner Daten informiert. Der Verein wurde darauf hingewiesen, dass grundsätzlich allein die Löschung der Daten nicht genügt. Es wurde aufgegeben, zukünftig die Zulässigkeit einzelner Verfahrensschritte anhand der rechtlichen Bestimmungen zu prüfen und darauf zu achten, dass § 28 Abs. 4 BDSG jede Form der Übermittlung oder Nutzung von Daten für Zwecke der Werbung erfasst. Es wurde zudem mitgeteilt, dass es gleichgültig sei, ob für rein wirtschaftliche oder für politische, soziale oder religiöse Zwecke geworben wird.

In einem anderen Beschwerdeverfahren erhielt ein Betroffener Werbepost von einem Fitnessstudio. Da er Mitglied in einem anderen Fitnessstudio ist und weder an einem Preisausschreiben, Gewinnspiel oder Ähnlichem des werbenden Clubs teilgenommen hatte, konnte er sich nicht erklären, woher dieser seine Anschrift hat.
Seitens der Aufsichtsbehörde wurde der Sachverhalt der verantwortlichen Stelle geschildert und nach einer allgemeinen Darstellung der rechtlichen Situation wurde um eine Beurteilung gebeten, woher sich die Zulässigkeit der Datenerhebung, -speicherung und -nutzung ergibt. Des Weiteren sollte der Aufsichtsbehörde eine Kopie der versandten Schreiben in anonymisierter Form vorgelegt und mitgeteilt werden, woher die Daten des Betroffenen resultieren. Der Fitnessclub konnte zu dem konkreten Betroffenen keine Ausführungen tätigen, da er keine Daten über diesen gespeichert hatte. Es wurden daher Ausführungen getätigt, auf welchen Wegen man personenbezogene Daten erhebt. Meist erfolge dies freiwillig durch das Ausfüllen von Aktionskarten. Der verantwortlichen Stelle wurden nochmals die Voraussetzungen einer wirksamen Einwilligung und die aus § 28 Abs. 4 BDSG resultierende Verpflichtung erläutert. Des Weiteren sollte der Aufsichtsbehörde vorgetragen werden, wie gewährleistet werden soll, dass man die Herkunft der gespeicherten personenbezogenen Daten entsprechend § 34 Abs. 1 Nr. 1 BDSG nachweisen kann, wenn die Aktionskarten nach der elektronischen Erfassung der Adressdaten vernichtet werden. Da es zahlreiche allgemeine Aspekte zu klären gab, bat die verantwortliche Stelle nachfolgend um ein Gespräch. In diesem wurden datenschutzrechtliche Probleme der einzelnen Werbemaßnahmen erörtert und damit das datenschutzrechtliche Bewusstsein geschärft. Der Betreiber des Fitnessstudios gab an, zukünftig seine Verfahrensweise zu verbessern und zeigte in einer abschließenden Stellungnahme die zukünftige Verfahrensweise unter Beachtung der angesprochenen Problemfelder auf.

4.2.6 Löschung personenbezogener Daten

Neben der Berichtigung und Sperrung personenbezogener Daten zählt auch die Löschung zu den Rechten des Betroffenen. Durch die genannten Rechte soll der Betroffene in die Lage versetzt werden, aufgrund der durch die Auskunft oder in anderer Weise gewonnenen Erkenntnisse ggf. eine rechtswidrige Verarbeitung seiner personenbezogenen Daten zu unterbinden. Nur so ist es ihm möglich, sein Recht auf informationelle Selbstbestimmung durchzusetzen. Die Rechte auf Berichtigung, Löschung und Sperrung können nach § 6 Abs. 1 BDSG ausdrücklich nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden. Es können dem Betroffenen keine Kosten der daraus resultierenden Handlungen auferlegt werden.
Die Löschung personenbezogener Daten bedeutet die Unkenntlichmachung der bei einer verantwortlichen Stelle gespeicherten Daten und wird von den Betroffenen in der Regel dann geltend gemacht, wenn sie der Auffassung sind, dass ein Unternehmen ihre Daten nicht mehr benötigt, beispielsweise weil ein Rechtsgeschäft gescheitert ist oder weil sie nicht wissen, wofür ihre Daten nachfolgend genutzt werden. Nach § 35 Abs. 2 Satz 1 BDSG können personenbezogene Daten außer in den Fällen, in denen die Daten zu sperren sind (genannt in § 35 Abs. 3 Nr. 1 und 2 BDSG) jederzeit gelöscht werden. Sie sind nach Satz 2 des § 35 Abs. 2 BDSG zu löschen, wenn

1. ihre Speicherung unzulässig ist,
2. es sich um Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit, über Gesundheit oder das Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann,
3. sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist, oder
4. sie geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine Prüfung jeweils am Ende des vierten Kalenderjahres beginnend mit ihrer erstmaligen Speicherung ergibt, dass eine längerwährende Speicherung nicht erforderlich ist.

Da der Aufsichtsbehörde für den Datenschutz noch keine Sachverhalte geschildert wurden, in denen es zu einer unbefugten Datenlöschung gekommen ist, ist Satz 1 des § 35 Abs. 2 BDSG, welcher die Voraussetzungen für die Berechtigung zur Löschung normiert, bis dato nicht prüfungsrelevant gewesen. Vielmehr galt es zu prüfen, ob eine Pflicht zur Löschung gespeicherter Daten besteht.

In einem Fall forderte eine Betroffene einen sozialen Verein zur Herausgabe aller über sie und ihren verstorbenen Ehemann angefertigten Klientenunterlagen auf. Diese sollten alle schriftlichen Aufzeichnungen über geführte Gespräche, Dokumentationen in Form von Bildern und ggf. Tonaufzeichnungen umfassen. Da seitens des Vereines keinerlei Reaktion erfolgte, bzw. er der blinden Frau anbot, in ihrem Beisein die Unterlagen zu vernichten, wandte sie sich an die Aufsichtsbehörde. Diese stellte fest, dass es der Petentin allein um die Klärung der Zulässigkeit der andauernden Datenspeicherung und der Löschung der Daten geht. In diesem Kontext wurde sodann dem Verein gegenüber dargestellt, woraus sich die Zulässigkeit der in Rede stehenden Verarbeitungsschritte ergeben könnte und um Stellungnahme hinsichtlich der

Zulässigkeit gebeten. Seitens des Vereins wurde dargestellt, dass dieser dateimäßig Stammdaten der Petentin gespeichert habe. Alle übrigen Unterlagen befänden sich in einer Akte. Es wurde erklärt, dass die Stammdaten weiterhin benötigt würden. Die Handakte würde aber mit einem persönlich an die Frau gerichteten Schreiben zur Abholung bereit liegen. Die übrige Handakte, die allein der internen Dokumentation diene, könne allerdings nur unter Aufsicht gelöscht bzw. geschreddert werden. Weiterhin teilte der Verein mit, dass die Akte des verstorbenen Ehemannes nicht ausgehändigt werden kann, da dies aufgrund der gegenüber dem verstorbenen Ehemann bestehenden Schweigepflicht nicht zulässig sei.
Seitens der Aufsichtsbehörde wurde festgestellt, dass aufgrund der Tatsache, dass die Petentin seit einigen Jahren keine Hilfe seitens des Vereines mehr in Anspruch nahm und ihr Ehemann verstorben ist, aus § 35 Abs. 2 Satz 2 Nr. 3 BDSG eine Pflicht zur Löschung der Daten besteht. Die Daten sind für den Verein nicht mehr erforderlich. Allerdings wurde ausgeführt, dass eine Löschungspflicht nur bedeutet, dass gespeicherte Daten irreversibel unkenntlich gemacht werden. Demzufolge müsse eine verantwortliche Stelle zur Erfüllung eines Löschungsgebotes stets einen Zustand herstellen, in dem sie die betreffenden Informationen nicht mehr aus von ihr gespeicherten Daten gewinnen kann. Mit welchen Verfahren und Mitteln dies erfolgt, obliegt jedoch allein der verantwortlichen Stelle. Es könnte daher auch durch das ordnungsgemäße Schreddern von Unterlagen erfolgen. Somit bestand seitens der blinden Petentin kein Anspruch auf Herausgabe der Unterlagen.
Darüber hinaus wurde der Petentin erläutert, dass der Herausgabe der Daten des verstorbenen Ehemannes die ärztliche Schweigepflicht entgegensteht. Diese ist in § 203 Abs. 1 des Strafgesetzbuches normiert und stellt unter Strafe, wenn durch einen Berufsgeheimnisträger wie z. B. einen Arzt, Rechtsanwalt, Steuerberater, Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Suchtberater unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis unbefugt offenbart wird. Von der Schweigepflicht sind Tatsachen und Umstände umfasst, die nur einem beschränkten Personenkreis bekannt sind und an deren Geheimhaltung der Betroffene ein bei Berücksichtigung seiner Situation sachlich begründetes Interesse hat. Eine solche Geheimhaltungspflicht besteht auch gegenüber Familienangehörigen des Betroffenen und besteht über dessen Tod hinaus.
Kein Verstoß gegen die Schweigepflicht liegt vor, wenn eine Offenbarungsbefugnis besteht. Eine solche bestand nicht. Eine Entbindung von der Schweigepflicht durch Angehörige nach dem Tode des Betroffenen gibt es nicht. Etwas anderes kann sich nur dann ergeben, wenn der zur Geheimhaltung Verpflichtete zu dem Ergebnis kommen würde, dass es das mutmaßliche Interesse des Verstorbenen gewesen ist, dass die Offenbarung seiner Geheimnisse erfolgt.
Bezüglich der Herausgabe der eigenen vollständigen Handakte, d.h. auch inklusive der internen Aufzeichnungen, ist die verantwortliche Stelle nicht verpflichtet, den Teil der Aufzeichnungen zu offenbaren, der persönliche Eindrücke über den Betroffenen oder dessen Angehörige umfasst. Dies gilt insbesondere für psychologische Behandlungen, weil in den Aufzeichnungen die Persönlichkeit des Patienten ebenso wie dritter Personen umfassender einfließt und spezifische therapeutische Risiken aus einer Rekonstruktion verarbeiteter Problemfelder für den Betroffenen entstehen können. Insgesamt wurde der Petentin gegenüber beurteilt, dass ihrem Anliegen wie folgt sachgerecht und rechtmäßig Rechnung getragen wird:

- Herausgabe der persönlichen Schriftstücke
- Vernichtung der übrigen Dokumente in der eigenen Handakte und der des verstorbenen Ehemannes unter ihrem Beisein und beliebiger Zeugen und
- Anonymisierung der dateimäßig erfassten Stammdaten.

Aufgrund der in dem Vorgang bestehenden „Vertrauensfrage“ wurde angeboten, die vorgenannten Maßnahmen im Beisein der Aufsichtsbehörde durchzuführen. Dies wurde genutzt.

In einem weiteren Sachverhalt begehrte eine Person von einer Bank einen Kredit zu bestimmten Konditionen. In einem dazu stattgefundenen Beratungsgespräch wurden folgende persönliche Daten schriftlich und elektronisch aufgenommen:

- Sparguthaben aller Familienmitglieder,
- Schulden aller Familienmitglieder,
- finanzielle Verbindlichkeiten (Raten, Unterhalt, Beiträge zu Parteien, Vereinen und Kindergärten) aller Familienmitglieder,
- Versicherungen aller Familienmitglieder (Lebens-, Unfall-, Hausrat-, Gebäude-, Kranken- und Rentenversicherung) und
- Bausparverträge aller Familienmitglieder.

Da der begehrte Kreditbetrag lediglich zu anderen Konditionen hätte zur Auszahlung gelangen können, lehnte die beantragende Person einen Kreditvertrag ab und beantragte die Löschung der Daten. Es wurde lediglich der Papierausdruck der elektronisch aufgenommenen Daten vernichtet, nicht jedoch die anderweitig gespeicherten Daten gelöscht. Daraufhin wurde die Bank unter Mitteilung der Sach- und allgemeinen Rechtslage angeschrieben und um eine Stellungnahme gebeten, warum ihrer Ansicht nach keine Pflicht zur Löschung der Daten nach § 35 Abs. 2 Satz 2 Nr. 3 BDSG bestehe. In der mit einiger Verspätung erfolgten Stellungnahme wurde ausgeführt, dass der komplette Datensatz des Betroffenen gesperrt ist, eine Löschung jedoch wegen gesetzlichen, satzungsmäßigen oder vertraglichen Aufbewahrungsfristen (§ 35 Abs. 3 Nr. 2 BDSG) nicht in Frage komme. Insbesondere sei im Laufe des Beratungsgespräches eine SCHUFA-Abfrage erfolgt. Zum Nachweis des berechtigten Interesses gegenüber der Kreditauskunftei i.S.d. § 29 Abs. 2 BDSG sei eine andauernde Datenspeicherung nötig. Daraufhin wurde der Bank mitgeteilt, dass man deren Auffassung teile, dass aus § 29 Abs. 2 Satz 4 BDSG eine gesetzliche Aufbewahrungspflicht resultiert und daher an die Stelle der Löschung eine Sperrung trete. Allerdings wurde um weitere Ausführungen gebeten, ob hierfür alle streitgegenständlichen Daten allein zu sperren und nicht zu löschen sind und in welchem Zeitraum mit Kontrollen des berechtigten Interesses zu rechnen ist, da sich daraus die Aufbewahrungsfrist ergebe.

Für den Nachweis eines berechtigten Interesses genügen nämlich allgemein personenbezogene Daten wie Name, Anschrift, Geburtsdatum, Art des beabsichtigten Geschäftsverhältnisses, nicht jedoch die sehr weitreichenden Angaben zu allen Familienmitgliedern.
Bei der Prüfung dieses Sachverhaltes dauerte es längere Zeit an, bis sich die verantwortliche Stelle detailliert mit den zu beachtenden datenschutzrechtlichen Aspekten auseinandergesetzt hatte und die Daten nicht allein aus „Kulanz“ löschte. Es bleibt nachfolgend zu hoffen, dass die Bank ihre Verfahrensweise anhand der Hinweise der Aufsichtsbehörde auch für zukünftige Löschungsbegehren überdenkt.

5 Interessantes – Wissenswertes im Bereich des Datenschutzes

5.1 Scoring

Scoring stellt typischerweise bei Massengeschäften ein Instrumentarium dar, mit dessen Hilfe man das vermutliche Verhalten potentieller Kunden sowie das mit einem Vertragsabschluss einhergehende Risiko einschätzen kann. Scoring findet in unterschiedlichen Konsumbereichen statt, darunter bei Kredit-, Versicherungs-, Telekommunikations-, Kfz- oder Wohnungsmietverträgen. Für den potentiellen Kunden beinhaltet das Scoring jedoch Gefahren, die dieser selten vorhersehen kann. Diese resultieren aus meist fehlender Transparenz hinsichtlich der Ermittlung des Score-Wertes und fehlenden Möglichkeiten zur Korrektur von durch Score-Werten ausgelösten Fehleinschätzungen.

Um einer Person einen Score-Wert zuordnen zu können, erfolgt zunächst eine automatisierte Verarbeitung deren persönlicher Merkmale wie z. B. Alter, Geschlecht, Beruf. Dies ist notwendig, um diese Person mittels eines mathematisch-statistischen Verfahrens einer Vergleichsgruppe zuzuordnen. Anhand der ermittelten Vergleichsgruppe und deren in anonymisierter Form dokumentierten Verhalten in bestimmten Situationen, z. B. hinsichtlich der Rückzahlung von Krediten, wird für den potentiellen Kunden prognostiziert, wie wahrscheinlich es ist, dass er seinen aus einem Vertrag resultierenden Pflichten ordnungsgemäß nachkommt. Auf diesem Weg werden persönliche Merkmale eines potentiellen Kunden (z. B. 37 Jahre alt, Deutscher, wohnhaft in Halle (Saale)) mit den Erfahrungen abgeglichen, die das den Score-Wert ermittelnde Unternehmen mit allen anderen Menschen gemacht hat, die gleiche Merkmale erfüllen. So führt beispielsweise die Erfahrung, dass 2,4 % aller in Halle (Saale) lebenden 37jährigen ihre Rechnungen unzuverlässig zahlen, zu einem bestimmten Score-Wert. Ein solcher wird entweder im internen Verfahren (auch Unternehmens-Scoring), d.h. innerhalb der verantwortlichen Stelle, die auch die Entscheidung über die Vertragsbindung trifft, getroffen oder es wird ein Score-Wert zu dem Betroffenen von externen Stellen (Büro-Scoring), wie beispielsweise der SCHUFA, eingekauft.

Wird beim **internen Scoring** auf die der Zweckbestimmung eines Vertrages dienenden Daten zurückgegriffen, handelt es sich um eine zweckändernde Nutzung der Daten. In derartigen Fällen kann die Zulässigkeit der Datennutzung allein aus § 28 Abs. 1 Satz 1 Nr. 2 BDSG resultieren und es muss eine Interessenabwägung zwischen den berechtigten Interessen der verantwortlichen Stelle und den schutzwürdigen Interessen des Betroffenen vorgenommen werden. Auch muss in diesem Zusammenhang geprüft werden, ob die genutzten Daten tatsächlich erforderlich sind, um das berechtigte Interesse der verantwortlichen Stelle gewährleisten zu können. Zur Beurteilung der Kreditwürdigkeit eines Betroffenen erscheinen folgende Daten erforderlich: Vermögen, Einkommen, Beruf, Dauer der Beschäftigung, Sicherheiten, Verbindlichkeiten, regelmäßige Ausgaben, Zahl und Höhe der bestehenden Kredite oder andere harte Negativdaten. Nicht erforderlich wäre dagegen die Nutzung von Daten wie Adresse, Wohnumfeld, Haushaltstyp, Wohndauer, Geschlecht, Familienstand, Alter, Zahl der Kinder, Kfz-Besitz, Religionszugehörigkeit. Mithin ist bei der Erforderlichkeitsprüfung auf die Art des konkreten

Vertragsverhältnisses und des zu bewertenden Risikos Bezug zu nehmen. Demzufolge wird bei einer Überprüfung stets eine detaillierte Untersuchung des Einzelfalles stattfinden müssen. Basiert das Scoring nicht auf einer speziellen sich aus dem Bundesdatenschutzgesetz ergebenden rechtlichen Grundlage (§ 6a BDSG), kann sich die Zulässigkeit allein aus einer den Anforderungen des § 4a BDSG entsprechenden Einwilligung ergeben. Diese hat beim Scoring in jedem Fall schriftlich zu erfolgen. Wegen der Komplexität des Scoring wäre jede andere Form nicht angemessen. Die Einwilligung muss zeitlich vor der Scoreberechnung liegen und hinreichend bestimmt sein bezüglich des Zwecks, der verantwortlichen Stelle und der verwendeten Daten.

Beim externen Scoring erfolgt die Auswertung von Konsumentendaten durch ein darauf spezialisiertes Unternehmen. Dabei kann die Auswertung auf der Basis der dort bereits gespeicherten Daten erfolgen oder es kann vorab eine Datenübermittlung der Vertragsdaten an das auswertende Unternehmen erfolgen. Bei der ersten Alternative handelt es sich bei der Auswertung um eine Zweckänderung der üblicherweise für Auskunftszwecke gespeicherten Daten. Sie werden vom vorgenannten Zweck abweichend zum Zweck der Erkennung von prognoserelevanten Gesetzmäßigkeiten genutzt. Dies ist nur zulässig, wenn ein berechtigtes Interesse der verantwortlichen Stelle an der Veränderung der personenbezogenen Daten besteht (vgl. § 29 Abs. 1 Satz 1 Nr. 1 BDSG). Erfolgt jedoch zunächst eine Datenübermittlung (zweite Alternative), muss bereits diese zulässig sein. Die Zulässigkeit kann aus einer Einwilligung nach § 4a BDSG oder wegen berechtigter Interessen aus § 28 Abs. 1 Satz 1 Nr. 2 oder § 28 Abs. 3 Satz 1 Nr. 1 BDSG resultieren, wenn das übermittelnde Unternehmen zugleich von der Übermittlung dadurch profitiert, dass anonymisierte Bewertungsgrundlagen für künftige Vertrags-Prognosen zur Verfügung gestellt werden. Direkt beim Kredit-Scoring kann sich die Zulässigkeit der Datenübermittlung aus § 28 Abs. 1 Satz 1 Nr. 1 BDSG ergeben. Die Dienlichkeit für den Vertrag und darauf basierend die Zulässigkeit der Übermittlung ist üblicherweise dann gegeben, wenn das Kreditunternehmen selbst nicht zur Durchführung des Scoring in der Lage ist.
Bei der nachfolgenden Berechnung des Score-Wertes durch das externe Unternehmen richtet sich die Zulässigkeit der weiteren Datenverarbeitung nach § 29 BDSG. Die Datenverarbeitung ist zulässig, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges entgegenstehendes Interesse hat (§ 29 Abs. 1 Satz 1 Nr. 1 BDSG). Schutzwürdige Interessen der Betroffenen ergeben sich daraus, dass von ihnen kein solvenzbezogener Persönlichkeitswert berechnet wird, aber auch, dass nur die Stelle, bei der ein bestimmter Antrag gestellt wurde, von diesem erfährt und nicht auch ein Scoring-Unternehmen. Es besteht jedoch dann kein Grund zur Annahme entgegenstehender schutzwürdiger Interessen, wenn z. B. ein Kreditnehmer bei der Antragstellung über die Einschaltung eines Scoring-Unternehmens informiert wurde und er sich mit der Verfahrensweise einverstanden erklärt hat. Eine abschließende Beurteilung lässt sich jedoch allein anhand eines konkreten Einzelfalles abgeben.

Im Anschluss an die Erstellung eines Score-Wertes erfolgt dessen Nutzung für eine bestimmte unternehmerische Entscheidung. Dabei darf das Scoringverfahren nicht zu einer automatisierten Einzelentscheidung im Sinne des § 6a BDSG führen. Der Score-Wert darf nicht zur ausschließlichen Grundlage der Entscheidung über den Abschluss des Geschäftes gemacht werden, es sei denn, einem Antrag des Betroffenen wird in vollem Umfang entsprochen. An-

dernfalls muss durch geeignete Maßnahmen gewährleistet werden, dass der Betroffene seine berechtigten Interessen wahren kann. Dies erfolgt z.B. dadurch, dass dem Betroffenen die Möglichkeit gegeben wird, sich beispielsweise zu seiner Kreditwürdigkeit zu äußern. Auf dieser Äußerung des Betroffenen hat die verantwortliche Stelle ihre Entscheidung nochmals zu prüfen. Trotz der Ausführungen zur Zulässigkeit der Erstellung und Nutzung von Scoring-Werten gilt es zu beachten, dass mit Scoring-Verfahren häufig datenschutzrechtliche Bedenken einhergehen.

5.2 Telefonwerbung

Telefonwerbung ist eine Form der elektronischen Kommunikation. Die entsprechenden Werbeanrufe erfolgen zumeist durch Call-Center, z.B. mit persönlichem Ansprechpartner oder auch mit Bandansagen.

Zunächst wurde die Telefonwerbung durch die Rechtsprechung reglementiert. Inzwischen werden jedoch im Rahmen des § 7 Abs. 2 des Gesetzes gegen den unlauteren Wettbewerb (UWG) konkrete Grenzen gezogen. Darin sind beispielhaft unzumutbare Belästigungen angeführt, die zur wettbewerbsrechtlich unlauteren Handlung i.S.d. § 3 UWG führen. Danach handelt beispielsweise unlauter, wer Werbung mit Telefonanrufen gegenüber Verbrauchern ohne deren Einwilligung bzw. gegenüber sonstigen Marktteilnehmern ohne deren zumindest mutmaßliche Einwilligung betreibt. Der „Verbraucher“ darf also ohne seine Einwilligung nicht telefonisch beworben werden. Zwar ist § 7 Abs. 2 UWG keine datenschutzrechtliche Vorschrift, sondern bezweckt allein den Verbraucherschutz, doch unlautere Werbemaßnahmen stellen mangels fehlender legitimer Zweckbestimmung keine zulässige Datennutzung nach dem Bundesdatenschutzgesetz, insbesondere nach § 28 BDSG, dar.

Demzufolge können Anrufe, die nicht der Klärung von unmittelbar mit einem Vertragsverhältnis zusammenhängenden Fragen dienen, allein auf der Basis von Einwilligungen der Betroffenen datenschutzrechtlich zulässig sein. Die Einwilligung in die Nutzung der Telefonnummer muss jedoch unter Beachtung des § 4a BDSG erfolgen. Die Einwilligung bedarf daher u.a. der Schriftform, sofern nicht „wegen besonderer Umstände eine andere Form angemessen ist“. Eine „andere Form“ ist eine ausdrücklich mündliche, nicht jedoch eine stillschweigende oder konkludente Einwilligung. Eine den Anforderungen des § 4a BDSG entsprechende Einwilligung kann dabei allerdings nicht darin gesehen werden, dass der Kunde beim Ausfüllen eines Coupons oder Antrages ohne nähere Erläuterung seine Telefonnummer preisgibt. Der Betroffene müsste entweder einen Passus, der seine Werbeabsicht ausdrückt, nicht streichen (opt-out Verfahren) oder ein Kreuz setzen, dass er der Nutzung der Daten für Zwecke der Werbung zustimmt (wesentlich transparenteres und von der Rechtsprechung anerkannteres opt-in Verfahren).

Erfahrungen, insbesondere der anderen Aufsichtsbehörden, zeigen, dass oft für die Nutzung von Telefonnummern für Zwecke der Werbung keine wirksame Einwilligung vorliegt. Häufig wird eine den Anforderungen des § 4a BDSG entsprechende Einwilligung bereits dann angenommen, wenn der Betroffene seine Telefonnummer in einem Formular angibt, auch wenn er nicht einmal ansatzweise über die beabsichtigte Nutzung für Zwecke der Werbung informiert

wird. Immer wieder kommt es auch vor, dass man die Vorschriften dadurch umgehen möchte, dass man im Rahmen des Telefonats die Einwilligung in die Telefonwerbung einholt. Darüber hinaus haben die Aufsichtsbehörden festgestellt, dass datennutzende Stellen sich meist darauf verlassen, dass ihnen ein Adresshändler zugesichert habe, dass es sich um Telefondaten handelt, bei denen die Betroffenen im Opt-In Verfahren der Werbung zugestimmt hätten. Nachgeprüft oder um die Vorlage des entsprechenden Beleges gebeten, wird jedoch in den seltensten Fällen.

Angesichts der Vielzahl von festgestellten Verfehlungen und der Häufigkeit von Werbeanrufen werden folgende Hinweise erteilt:

Die einzuholende Einwilligung muss so gestaltet sein, dass Sie als potentieller Betroffener eine eigene Erklärung abgeben („Ich willige ein, dass…“). Ein bloßer Hinweis auf eine bestimmte Nutzung Ihrer Daten („mir ist bekannt, dass…“) genügt nicht. Zudem muss die Einwilligungserklärung, wenn sie zusammen mit anderen Erklärungen abgegeben wird, graphisch besonders hervorgehobenen und gut sichtbar platziert sein. Sie darf nicht versteckt in den Allgemeinen Geschäftsbedingungen enthalten sein oder in der Kopfzeile genannt werden. Die Einwilligungserklärung muss eigenständig unterschrieben sein.

Die Einwilligung muss ausdrücklich erteilt werden. In diesem Zusammenhang entschied die Rechtsprechung bereits mehrfach, dass das Nichtankreuzen des Satzes „hier ankreuzen, falls die Einwilligung nicht erteilt wird“, als Schweigen des Betroffenen und nicht als Einwilligung zu werten ist.

Die Einwilligung muss bereits vor dem ersten Anruf vorliegen.

Einwilligungserklärungen sind solange aufzubewahren, wie von ihnen Gebrauch gemacht wird. Verantwortliche Stellen, die die zu nutzenden Daten von Dritten beziehen, müssen sich zumindest immer wieder stichprobenartig davon überzeugen, dass dem § 4a BDSG entsprechende Erklärungen vorliegen.

5.3 Whistleblowing-Hotlines

Die Qualität der Arbeit eines Unternehmens ist ein wichtiges Aushängeschild und notwendige Voraussetzung um sich mit seiner Leistung am Markt behaupten zu können. Darüber hinaus ist es für ein Unternehmen wichtig zu wissen, dass man sich auf seine Mitarbeiter verlassen kann und aus deren Wirken keine Gefahren resultieren, die dem Ansehen oder der Leistung des Unternehmens Schaden zufügen können. In diesem Kontext finden sich Whistleblowing-Hotlines wieder, denn regelmäßig ist es der Unternehmensleitung oder den Unternehmensinhabern nicht möglich, alle Verhaltensweisen ihrer Mitarbeiter auf Regelkonformität bzw. mögliche Schädlichkeit zu prüfen. Mit Hilfe der Whistleblowing-Hotlines sollen die Mitarbeiter eines Unternehmens die Möglichkeit erhalten, ein nicht regelkonformes Verhalten anderer Mitarbeiter dem Unternehmen aufzuzeigen. Mögliche Verstöße können sein:

- Verhaltensweisen, die einen sich gegen das Unternehmensinteresse richtenden Straftatbestand erfüllen (insbesondere Betrug und Fehlverhalten in Bezug auf die Rechnungslegung sowie interne Rechnungslegungskontrollen, Wirtschaftsprüfungsdelikte, Korruption, verbotene Insidergeschäfte etc.)
- Verhaltensweisen, die gegen Menschenrechte (z.B. Ausnutzung günstiger Produktionsbedingungen im Ausland durch in Kauf genommene Kinderarbeit) oder Umweltschutzbelange verstoßen
- Verhaltensweisen, die unternehmensinterne Ethikregeln beeinträchtigen.

In jedem Fall kann es zu einer Erhebung, Verarbeitung oder Nutzung personenbezogener Daten kommen. Betroffene Personengruppen sind vor allem die Hinweisgeber sowie die beschuldigten Personen. Die Datenerhebung umfasst in jedem Fall Angaben über die beschuldigte Person, die (angeblichen) Verhaltensverstöße sowie die entsprechenden Sachverhalte. Von dem Hinweisgeber werden personenbezogene Daten nur dann erhoben, wenn er sich nicht in anonymisierter Form äußern kann oder seine Angaben zum Sachverhalt zu seiner Identifikation führen können.
Die Zulässigkeit der einzelnen Verarbeitungsschritte kann aus Einwilligungen i.S.d. § 4a BDSG resultieren, aus anderen Rechtsvorschriften oder dem Bundesdatenschutzgesetz, insbesondere § 28 Abs. 1 Satz 1 Nr. 2 BDSG selbst. Bezüglich der Zulässigkeit auf Basis wirksamer Einwilligung ist es jedoch fraglich, ob im Arbeitsverhältnis eine Einwilligung freiwillig erklärt werden kann. Eine gesetzlich andere Rechtsvorschrift, die die Erhebung, Verarbeitung und Nutzung im Zusammenhang mit Whistleblowing-Hotlines erlaubt oder gar anordnet, gibt es nicht. In Frage käme allein eine Betriebsvereinbarung. In dieser müsste die Datenerhebung-, -verarbeitung und -nutzung ausreichend und präzise – innerhalb des Erlaubnisumfangs des BDSG – geregelt sein und es dürfte durch sie nicht das durch das Bundesdatenschutzgesetz gesetzte Schutzniveau unterschritten werden. Hinsichtlich der Zulässigkeit nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist zunächst anzuerkennen, dass es sich bei dem Ziel der Verhütung von strafbewehrten Handlungen um ein berechtigtes Interesse des eine Whistleblowing-Hotline nutzen wollenden Unternehmens handelt. Auch kann die Einrichtung von Verfahren zur Meldung von Missständen zur Verwirklichung des berechtigten Interesses in Abhängigkeit von den konkret zu erhebenden Daten für erforderlich gehalten werden. Eine Datenverarbeitung zur Wahrung des berechtigten Interesses wäre dennoch nur zulässig, wenn die schutzwürdi-

gen Interessen der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung nicht überwiegen. Dass das Persönlichkeitsrecht der von einer Meldung Betroffenen stark berührt ist, ist unstreitig. Insbesondere besteht die Gefahr, dass Personen angeschwärzt werden, um sie zu ärgern oder sich an ihnen zu rächen. Aus diesem Grund muss stets eine einzelfallabhängige Interessenabwägung vorgenommen werden, wobei diese im Hinblick auf die belasteten Personen besonders sorgfältig vorgenommen werden muss. Dabei ist auch einzubeziehen, ob es sich um sogenannte harte Verstöße (Spiegelstriche 1 und 2 der Aufzählung) oder sogenannte weiche Verstöße (Spiegelstrich 3) handelt. Letztere Verhaltensregeln sind meist nicht klar umrissen, so dass sich ein Verstoß selten einwandfrei identifizieren lässt.
Es wird ersichtlich, dass auch bei Whistleblowing-Hotlines stets ein Abwägungsprozess durchzuführen ist. In keinem Fall sind derartige Angebote pauschal als datenschutzrechtlich unzulässig einzustufen. Was bei ihrer datenschutzgerechten Gestaltung und dem nachfolgenden Betrieb zu beachten ist, lässt sich insbesondere dem Arbeitsbericht der Ad-hoc-Arbeitsgruppe „Beschäftigtendatenschutz“ des Düsseldorfer Kreises unter dem Titel „Whistleblowing-Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz“ im Abschnitt E: Datenschutzgerechte Gestaltung eines Meldeverfahrens mittels Hotlines entnehmen. Der Bericht ist abrufbar unter http://www.datenschutz-hamburg.de (Pfad: Datenschutzbeauftragter/Informationsmaterial/Wirtschaft).

6 Zusammenfassung und kurzer Ausblick

Aus den Ausführungen dieses Tätigkeitsberichtes wird deutlich, dass es sich beim Datenschutz um ein Rechtsgebiet handelt, bei dem nicht kategorisierend festgestellt werden kann, dass diese oder jene Datenerhebung, -speicherung oder -nutzung zulässig ist oder nicht. Aus diesem Grund wird die Aufsichtsbehörde für den Datenschutz des Landes Sachsen-Anhalt weiterhin jeden der ihr bekannt gewordenen Sachverhalte einzelfallbezogen untersuchen, Tipps und Anregung zur datenschutzkonformen Vorgehensweise der verantwortlichen Stellen geben und gleichzeitig den schutzwürdigen Interessen der Betroffenen zur Geltung verhelfen. Beispielsweise indem die Auskunft über gespeicherte Daten erreicht wird, unzulässig erhobene Daten der Betroffenen gelöscht oder Verstöße gegen die Bestimmungen des Datenschutzes geahndet werden. Möglicherweise von datenschutzrechtlichen Verstößen betroffenen Bürgern ist anzuraten, bestimmte Vorgehensweisen von verantwortlichen Stellen nicht ohne Weiteres zu akzeptieren, sondern die Aufsichtsbehörde zu informieren. Dies kann in Ausnahmefällen auch in anonymisierter Form erfolgen, wenn der zu überprüfende Sachverhalt hinreichend konkretisiert dargestellt wird und die datenverarbeitende Stelle benannt wird.

Darüber hinaus soll mittels verstärkter Präventivarbeit verhindert werden, dass es zu Verstößen gegen das Bundesdatenschutzgesetz kommt. Hierzu können sich die verantwortlichen Stellen mit ihrem Anliegen an die Aufsichtsbehörde wenden. Gleichzeitig sollen verstärkt Informationen zum Datenschutz zur Verfügung gestellt werden. Auch anlassunabhängigen Vorortkontrollen wird in der Präventivarbeit eine wichtige Bedeutung zugemessen. Weiterhin werden – wie im Berichtszeitraum – die Gelegenheiten genutzt, mittels Fachvorträgen zu einzelnen Themen den Datenschutz transparenter zu machen. Insgesamt sollen die Belange des Datenschutzes noch stärker ins Problembewusstsein der verantwortlichen Stellen, aber auch der Betroffenen rücken.

Das Landesverwaltungsamt Sachsen-Anhalt wird seine Tätigkeit als Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich noch stärker als bisher in der Öffentlichkeit darstellen und sich auch so als Ansprechpartner anbieten.

Anlage: Anschriften der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich

Baden-Württemberg

Innenministerium Baden-Württemberg
Dorotheenstraße 6, 70173 Stuttgart
Tel.: +49 711 231-3250 / Fax: +49 711 231-3299 oder -5000
www.bwl.de
E-Mail: Datenschutz@im.bwl.de

Bayern

Regierung von Mittelfranken
Bayerische Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich
Promenade 27, 91522 Ansbach
Tel.: +49 981 53-1300 / Fax: +49 981 53-5301
www.regierung.mittelfranken.bayern.de
E-Mail: datenschutz@reg-mfr.bayern.de

Berlin

Berliner Beauftragter für Datenschutz und Informationsfreiheit
An der Urania 4 – 10, 10787 Berlin
Tel.: +49 30 13889-0 / Fax: +49 30 21550-50
www.datenschutz-berlin.de
E-Mail: mailbox@datenschutz-berlin.de

Brandenburg

Ministerium des Innern des Landes Brandenburg
Hennig-von-Tresckow-Straße 9-13, 14467 Potsdam
Tel.: +49 331 866-2230 / Fax: +49 331 866-2202
www.mi.brandenburg.de
E-Mail: poststelle@mi.brandenburg.de

Bremen

Landesbeauftragter für den Datenschutz und Informationsfreiheit
der Freien Hansestadt Bremen
Arndtstr. 1, 27570 Bremerhaven
Tel: +49 421 361-2010/ Fax: +49 421 496-18495
www.datenschutz.bremen.de
E-Mail: office@datenschutz.bremen.de

Bund

Der Bundesbeauftragte für Datenschutz und Informationsfreiheit
Husarenstr. 30, 53117 Bonn
Tel.: +49 228 81995-0 / Fax: +49 228 81995-550
www.bfdi.bund.de
E-Mail: poststelle@bfdi.bund.de

Hamburg

Hamburgischer Datenschutzbeauftragter
Klosterwall 6, Block C, 20095 Hamburg
Tel.: +49 40 42854-4040 / Fax: +49 40 42854-4000
www.datenschutz.hamburg.de
E-Mail: mailbox@datenschutz.hamburg.de

Hessen

Regierungspräsidium
Luisenplatz 2, 64283 Darmstadt
Tel.: +49 6151 12–5792 / +49 6151 12-5794
http://www.rp-darmstadt.hessen.de
E-Mail: Datenschutz @rpda.hessen.de

Mecklenburg-Vorpommern

Landesbeauftragter für Datenschutz und Informationsfreiheit
Johannes – Stelling - Str. 21m, 19053 Schwerin
Tel.: +49 385 59494-0 / Fax: +49 385 59494-58
E-Mail: datenschutz@mvnet.de

Niedersachsen

Niedersächsisches Ministerium für Inneres und Sport
Lavesallee 6, 30169 Hannover
Tel.: +49 511 120-4756 / Fax: +49 511 120-99+Hausruf (PC-Fax)
E-Mail: poststelle@mi.niedersachsen.de

Landesbeauftragter für den Datenschutz Niedersachsen
Brühlstr. 9, 30159 Hannover
Tel.: +49 511 120-4500 / Fax: +49 511 120-4599
E-Mail: poststelle@lfd.niedersachsen.de

Nordrhein-Westfalen

Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
Kavalleriestraße 2- 4, 40213 Düsseldorf
Tel.: +49 211 38424-15 / Fax: +49 211 38424-10
www.ldi.nrw.de
E-Mail: poststelle@ldi.nrw.de

Rheinland-Pfalz

Ministerium des Innern und für Sport des Landes Rheinland-Pfalz
Wallstraße 3, 55122 Mainz
Tel.: +49 6131 16-3259 / Fax: +49 6131 16-3369
www.ism.rlp.de
E-Mail: poststelle@ism.rlp.de

Saarland

Ministerium für Inneres, Familie, Frauen und Sport
Franz-Josef-Röder-Str. 21, 66119 Saarbrücken
Tel.: +49 681 962-1640 / Fax: +49 681 962-1605
www.innen.saarland.de
E-Mail: Datenschutz@innen.saarland.de

Sachsen

Sächsischer Datenschutzbeauftragter
Bernhard-von-Lindenau-Platz 1, 01067 Dresden
Tel.: +49 351 4935-401 / Fax: +49 351 4935-490
www.datenschutz.sachsen.de
E-Mail: saechsdsb@slt.sachsen.de

Sachsen-Anhalt

Landesverwaltungsamt Sachsen-Anhalt
Referat 106 (Justitiariat)
Ernst-Kamieth-Str. 2, 06112 Halle (Saale)
Tel.: +49 345 514-3857 / Fax: +49 345 514-3799
www.sachsen-anhalt.de/LPSA/index.php?id=13572
E-Mail: poststelle@lvwa.sachsen-anhalt.de

Schleswig-Holstein

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Holstenstr. 98, 24103 Kiel
Tel.: +49 431 988-1200 / Fax: +49 431 988-12 23
www.datenschutzzentrum.de
E-Mail: mail@datenschutzzentrum.de

Thüringen

Thüringer Landesverwaltungsamt
Weimarplatz 4, 99423 Weimar
Tel.: +49 361 377-37299 / Fax: +49 361 377-3746
http://www.thueringen.de/de/tlvwa/inneres/hoheit/datenschutz/content.html
E-Mail: poststelle@tlvwa.thuerungen.de

Hier sind wir erreichbar

1 Hauptsitz
Ernst-Kamieth-Straße 2, 06112 Halle (Saale)
Telefon (0345) 514-0

2 Dienstgebäude Halle
Ahornweg 30b, 06132 Halle (Saale)
Telefon (0345) 7779730

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
Willy-Lohmann-Straße 7, 06114 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
Ernst-Kamieth-Straße 2, 06112 Halle (Saale)
06114 Halle (Saale)
Telefon: (0345) 514-0

www.landesverwaltungsamt.sachsen-anhalt.de