SACHSEN-ANHALT

Landesverwaltungsamt

Vierter Tätigkeitsbericht

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

Berichtszeitraum 01.06.2007 – 31.05.2009

Inhaltsverzeichnis

1 Einführung 1

1.1 Das Recht auf informationelle Selbstbestimmung – mehr als nur ein Wort? 1

1.2 Aufgaben einer Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich 2

1.3 Der Beauftragte für den Datenschutz 3

1.4. Die Zielstellung eines Tätigkeitsberichtes 3

1.5. Zusammenarbeit mit anderen Aufsichtsbehörden 4

2 Das Bundesdatenschutzgesetz (BDSG) 5

2.1 Änderung des Bundesdatenschutzgesetzes 5

2.2 Die Rechte der Betroffenen nach dem Bundesdatenschutzgesetz 9

3 Datenschutz im nicht-öffentlichen Bereich des Landes Sachsen-Anhalt . 12

3.1 Allgemeines zur Aufsichtstätigkeit 12

3.1.1 Ansprechpartner und Internetpräsenz 12

3.1.2 Eingaben, Kontrollen 13

3.1.3 Beratung von Bürgern, Unternehmen und betrieblichen Datenschutzbeauftragten 13

3.1.4 Ordnungswidrigkeitenverfahren 14

3.2 Zahlenmäßiger Überblick über die Tätigkeit der Aufsichtsbehörde 15

4 Einzelne Punkte aus Anfragen und Beschwerden 18

4.1 Von Beratungsinteresse – ausgewählte Aspekte der Anfragen 18

4.1.1 Betriebs-/Dienstvereinbarungen 18

4.1.2 Mithören/Aufzeichnung von Telefongesprächen 20

4.1.3 Optisch-elektronische Einrichtungen (Videoüberwachung) 24

4.1.4 Übermittlung personenbezogener Daten im kleinen Rahmen - unternehmensinterne Zeitung 26

4.1.5 Übermittlung personenbezogener Daten im großen Rahmen - im Internet allgemein und im Rahmen von Bewertungsplattformen . 27

4.2 Was ist zulässig und was nicht – ausgewählte Beschwerdeverfahren 30

4.2.1 Überwachung von Beschäftigten 30

4.2.2 Videoüberwachung von Wohnanlagen 33

4.2.3 Erhebung personenbezogener Daten 35

4.2.4 Speicherung/Aufbewahrung personenbezogener Daten 36

4.2.5 Übermittlung personenbezogener Daten 37

4.2.6 Nutzung personenbezogener Daten für Zwecke der Werbung 38

4.2.7 Löschung personenbezogener Daten 43

4.2.8 Rechte der Betroffenen 45

4.2.9 Auskunfteien 47

5 Interessantes – Wissenswertes im Bereich des Datenschutzes 52

5.1 Google Street View 52

5.2 Soziale Netzwerke 55

5.3 Illegaler Datenhandel 57

6 Ausblick 60

1 Einführung

1.1 Das Recht auf informationelle Selbstbestimmung – mehr als nur ein Wort?

Wer nichts zu verbergen hat, hat nichts zu befürchten? Diese Aussage wird oft gehört, aber sollte man es sich so einfach machen und damit den Datenschutz ad akta legen? Nein, denn solche Aussagen ignorieren das Anliegen des Datenschutzes, die Bürger vor Beeinträchtigungen durch den **unbefugten** Umgang mit ihren Daten zu schützen.

Ausgangspunkt des Datenschutzes ist das sog. Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 (BVerfGE 65, 1). Darin wird aus dem in Art. 1 und 2 des Grundgesetzes (GG) verankerten allgemeinen Persönlichkeitsrecht das „Recht der informationellen Selbstbestimmung“ hergeleitet. Dieses gewährleistet die Befugnis:

- „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“ und
- „zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden“.
- Zudem müssen Betroffene „wissen können, wer was wann und bei welcher Gelegenheit über sie weiß“.

Das Grundrecht gilt nicht grenzenlos. Einschränkungen sind legitim, unterliegen jedoch strengen Anforderungen und sind nur im überwiegenden Allgemeininteresse zulässig. So ist eine gesetzliche Grundlage notwendig, aus der sich eindeutig die Voraussetzungen für die Einschränkungen und deren Umfang für die Betroffenen ergeben müssen. Der Umgang mit personenbezogenen Daten hat sich an einem präzise bestimmten Verwendungszweck zu orientieren und ist auf das für diese Zwecke erforderliche Mindestmaß zu beschränken.

Ein Umgang mit personenbezogenen Daten kann durch **öffentliche** oder **nicht-öffentliche** Stellen erfolgen. Die Unterscheidung, ob eine öffentliche oder nicht-öffentliche Stelle mit personenbezogenen Daten umgeht, ist maßgebend dafür, ob das Bundesdatenschutzgesetz (BDSG) oder eines der Landesdatenschutzgesetze zur Anwendung kommt.
Öffentliche Stellen sind zunächst sämtliche Behörden des Bundes oder der Länder, aber auch die Organe der Rechtspflege und andere öffentlich organisierte Einrichtungen ungeachtet ihrer Rechtsform. Darüber hinaus zählen auch nicht-öffentliche Stellen zu den **öffentlichen** Stellen, soweit sie hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen, z. B. die Kfz-Sachverständigen des TÜV und die öffentlich bestellten Vermessungsingenieure (§ 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. Beispielhaft zu nennen sind Banken, Versicherungen, Industrie- und Dienstleistungsunternehmen, aber auch freiberuflich Tätige, wie etwa Ärzte, Rechtsanwälte und Architekten. Für Stellen der Religionsgesellschaften gilt regelmäßig kirchliches Datenschutzrecht.

In Sachsen-Anhalt bestimmt diese Differenzierung darüber hinaus, welche Institution den Betroffenen beim Schutz seiner Daten zur Seite steht. Über die Einhaltung der datenschutzrechtlichen Bestimmungen durch die öffentlichen Stellen des Landes Sachsen-Anhalt wacht der Landesbeauftragte für den Datenschutz. Die Überwachung des Umgangs mit personenbezogenen Daten durch nicht-öffentliche Stellen obliegt demgegenüber dem Landesverwaltungsamt **als Aufsichtsbehörde** für den Datenschutz **im nicht-öffentlichen Bereich**.

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

Die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich hat die Aufgabe, die Ausführung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz zu überwachen. Dies geschieht im Wesentlichen über:

- die Bearbeitung von Anfragen, Eingaben und Beschwerden,
- die Beanstandung und ggf. Anordnung zur Beseitigung von Datenschutzverstößen und Sicherheitsmängeln inkl. der Durchführung von Bußgeldverfahren und
- die Führung des öffentlichen Registers der meldpflichtigen Unternehmen (vor allem Auskunfteien, Adressenhändler sowie Markt- und Meinungsforschungsinstitute).

Besonderen Wert legt die Aufsichtsbehörde auf die seit Mitte 2006 gesetzlich normierte Aufgabe, die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse zu beraten und zu unterstützen (§ 38 Abs. 1 Satz 2 BDSG). In einem konstruktiven Dialog wird auf die Belange potentieller Betroffener geachtet. Auf diesem Weg können die datenschutzrechtlichen Vorschriften sachgerecht ausgelegt und praktikable Lösungen entwickelt werden.

Das Tätigwerden der Aufsichtsbehörde liegt in deren pflichtgemäßem Ermessen. Für Prüfungshandlungen ist weder ein bestimmter Anlass noch ein Verdacht notwendig. Zulässig sind sowohl anlassbezogene wie anlassunabhängige Prüfungen. Anlässe können z. B. sein: Eingaben von Betroffenen, Anzeigen von Dritten (Interessenverband, Konkurrenzunternehmen, beteiligte Dritte), Informationen von Behörden oder die Berichterstattung in den Me-

dien. Die Bearbeitung von Anfragen und Eingaben von Bürgerinnen und Bürgern, die telefonisch und schriftlich (gern auch per E-Mail) an die Aufsichtsbehörde herangetragen werden, macht den Hauptteil der Arbeit aus. Viele Fragen lassen sich nicht immer sofort beantworten, sondern erfordern eine Aufklärung des Sachverhalts. Hierzu wendet sich die Aufsichtsbehörde unter Darstellung des bekannt gewordenen Sachverhalts und der Mitteilung der allgemeinen Rechtslage an die verantwortliche Stelle und bittet um eine Stellungnahme sowie ggf. um Ausführungen zu konkreten Einzelfragen. Die Mitarbeiter der Aufsichtsbehörde haben das Recht, die Geschäftsräume zu betreten und alle mit der Datenverarbeitung in Zusammenhang stehenden Unterlagen einzusehen. Die abschließende datenschutzrechtliche Bewertung wird dem Petenten mitgeteilt. Von Bedeutung für die Betroffenen ist, dass durch die Tätigkeit der Aufsichtsbehörde grundsätzlich keine Kosten entstehen.

1.3 Der Beauftragte für den Datenschutz (DSB)

Neben der Aufsichtsbehörde kümmern sich auch betriebliche Datenschutzbeauftragte (DSB) um Belange des Datenschutzes. Sie dienen der Selbstkontrolle der Stelle in der sie bestellt sind. Wann eine Pflicht zur Bestellung eines DSB besteht, ergibt sich aus § 4f Abs. 1 BDSG. Ein Datenschutzbeauftragter wirkt mit seinen spezifischen Fachkenntnissen auf die Einhaltung datenschutzrechtlicher Vorschriften hin. Wird der Beauftragte für den Datenschutz bereits frühzeitig in Verfahren einbezogen, kann er dafür sorgen, dass datenschutzrechtliche Vorgaben beachtet werden. Auch kann er notwendige technische und organisatorische Maßnahmen veranlassen, um Persönlichkeitsrechtsverletzungen zu verhindern.

Zu den Aufgaben eines Beauftragten für den Datenschutz gehört es weiterhin, die bei der Verarbeitung personenbezogener Daten tätigen Personen mit dem datenschutzgerechten Umgang personenbezogener Daten vertraut zu machen. Zur praktischen Anwendung datenschutzrechtlicher Vorschriften empfehlen sich Schulungsmaßnahmen der Mitarbeiter durch den betrieblichen Datenschutzbeauftragten.

1.4. Die Zielstellung des Tätigkeitsberichtes

Seit Mai 2001 sind die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich nach § 38 Abs. 1 Satz 7 BDSG verpflichtet, regelmäßig, spätestens alle zwei Jahre, über ihre Tätigkeit zu berichten. Mit dem Tätigkeitsbericht, der sich auf **den Berichtszeitraum vom 01.06.2007 bis 31.05.2009** bezieht, soll über die Aktivitäten der Aufsichtsbehörde für den Datenschutz Aufschluss gegeben werden.

Die Veröffentlichung des Tätigkeitsberichtes ist auch im Rahmen der Öffentlichkeitsarbeit wichtig. Die Bürger sollen mit Hilfe des Berichtes erkennen können, ob der Umgang mit personenbezogenen Daten gerechtfertigt ist bzw. wie man gegebenenfalls dagegen vorgehen kann. Der Tätigkeitsbericht soll daher nicht allein Rechenschaft über den Berichtszeitraum ablegen, sondern darüber hinaus Aufschluss über die Rechtmäßigkeit bestimmter Verfahren geben. Interessierte und betroffene Bürger sollen über aktuelle Themen unterrichtet und in die Lage versetzt werden, ihre Rechte wirkungsvoll wahrnehmen zu können.

1.5. Zusammenarbeit mit anderen Aufsichtsbehörden

Die Aufsichtsbehörde stellt immer wieder fest, dass es Betroffenen – insbesondere aufgrund gegebener Unternehmensstrukturen – im Einzelfall kaum möglich ist, die örtlich zuständige Aufsichtsbehörde (die Zuständigkeit richtet sich grundsätzlich nach dem Ort der in Rede stehenden Datenverarbeitung bzw. dem Sitz der verantwortlichen Stelle) zu informieren. Aus diesem Grund wenden sich Betroffene häufig an die Aufsichtsbehörde im eigenen Bundesland. Bei allgemeinen Anfragen ist es der Aufsichtsbehörde in solchen Fällen möglich, Auskünfte zu erteilen. Sind jedoch Sachverhaltsermittlungen notwendig, kann die Aufsichtsbehörde lediglich die Kontaktdaten der zuständigen Aufsichtsbehörde benennen oder gegebenenfalls mit Einverständnis des Betroffenen die Anfrage an die zuständige Aufsichtsbehörde weiterleiten. Niemand sollte bei Bedarf zögern, eine Aufsichtsbehörde – auch bei bestehenden Unsicherheiten über die örtliche Zuständigkeit – zu kontaktieren.

Die Aufsichtsbehörden stimmen sich auch in ihrer Vorgehensweise bei bundesweit auftretenden Problemstellungen, so z. B. in den Fällen der Mitarbeiterüberwachung bei einem Discounter, ab.

Die einheitliche Auslegung des Bundesdatenschutzgesetzes wird über den sog. „Düsseldorfer Kreis“ sichergestellt. Dies ist ein Gremium der Aufsichtsbehörden für den Datenschutz, in dem der Bund und die Länder vertreten sind. Es werden datenschutzrechtliche Grundsatzfragen erörtert. Die wichtigsten Ergebnisse werden in Arbeitspapieren oder Beschlüssen veröffentlicht. Die seit November 2006 gefassten Beschlüsse sind auf der Website des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (http://www.bfdi.bund.de, Pfad: „Datenschutz/Entschließungen/ Düsseldorfer Kreis“) eingestellt.

2 Das Bundesdatenschutzgesetz (BDSG)

Bei dem Bundesdatenschutzgesetz handelt es sich um ein Schutzgesetz, dass dem Schutz natürlicher Personen beim Umgang mit deren personenbezogenen Daten dient. Das BDSG hat auch eine verbraucherschützende Funktion. Zugleich dient es der Regulierung des Wettbewerbs, soweit personenbezogene Daten verarbeitet werden. Das BDSG ist anwendbar, soweit nicht bereichsspezifische Eingriffsbefugnisse mit Rechtsnormcharakter, wie z. B. die Sozialgesetzbücher, das Personenstandsgesetz oder die Grundbuchordnung vorliegen.

Das BDSG wurde in Teilen zum Abbau bürokratischer Hemmnisse bereits Mitte des Jahres 2006 novelliert. Eine grundsätzliche Modernisierung des Datenschutzrechts mit Blick auf die qualitativ und quantitativ veränderten Verhältnisse im Bereich der Informationstechnik und deren Nutzung erfolgte jedoch nicht.

Das Jahr 2008 war durch Datenschutzskandale wie z. B. „Spionage bei der Deutschen Telekom“, „Auftauchen einer CD mit Adressen und Kontodaten von Kunden der Süddeutschen Klassenlotterie“, „Kreditkartenabrechnung statt Christstollen“ geprägt. Dadurch stieg zum einen die öffentliche Wahrnehmung des Datenschutzes. Zum anderen wurde die weitergehende Notwendigkeit der Novellierungen des Datenschutzrechts deutlich. In einem so genannten „Datenschutzgipfel“ wurden im September 2008 Eckpunkte für legislative Maßnahmen festgelegt. Zu diesen zählten Neuregelungen im Bereich der Nutzung personenbezogener Daten für Werbung, im Bereich des Scoring und des Arbeitnehmerdatenschutzes sowie organisatorische und verfahrensmäßige Neuerungen, wie z. B. die Meldepflicht bei Sicherheitsverletzungen oder die Möglichkeit der erweiterten Gewinnabschöpfung bei Verstößen.

2.1 Änderung des Bundesdatenschutzgesetzes

Nach dem „Datenschutzgipfel“ wurde im weiteren Verlauf des Berichtszeitraumes der Novellierungsbedarf des Bundesdatenschutzgesetzes umfassend erörtert. Zwar erfolgte die Änderung des BDSG erst durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814) und somit nach Ende des Berichtszeitraums Ende Mai 2009. Wegen der Bedeutung der drei Novellen wird nachfolgend der Inhalt der bereits in Kraft getretenen Regelungen dargestellt.
Die **BDSG-Novelle II** trat mit ihren Übergangsregelungen (§ 47 BDSG) bereits am 1.9.2009 in Kraft und brachte vor allem Änderungen im Bereich der personalisierten Werbung, der Auftragsdatenverarbeitung und im Arbeitnehmerdatenschutz. Zudem wurde eine Informationspflicht bei Datenpannen eingeführt.

Zu den wichtigsten Regelungen im Einzelnen:

- **Datenverarbeitung zum Zwecke der Werbung**

Mit der Neuregelung des § 28 Abs. 3 BDSG erkennt der Gesetzgeber das Grundanliegen, den Betroffenen im Bereich der Werbung und des Adresshandels mehr Selbstbestimmung und Schutz zu geben, an. Hervorzuheben ist, dass der neue § 28 Abs. 3 BDSG als Grundsatz regelt, dass die Verwendung personenbezogener Daten für Zwecke des Adresshandels, der Werbung oder der Markt- oder Meinungsforschung nur zulässig ist, wenn der Betroffene eingewilligt hat. Die Bürger sollen eigenverantwortlich entscheiden können, ob sie einen entsprechenden Datenumgang wünschen. Trotzdem bleibt es ohne ausdrückliches Einverständnis erlaubt, listenmäßig zusammengefasste Daten über Angehörige einer bestimmten Personengruppe mit deren Berufs-, Branchen- oder Geschäftsbezeichnung, Namen, Titel (akademischer Grad), Anschrift und Geburtsjahr für Werbung mit eigenen Angeboten, für Zwecke der Werbung im Hinblick auf die berufliche Tätigkeit der Betroffenen sowie für Zwecke der Spendenwerbung zu verwenden. Künftig besteht bereits bei der Erhebung der Daten - und somit nicht erst bei der Ansprache zu Werbezwecken - eine Hinweispflicht, dass einer solchen Nutzung widersprochen werden kann. Zudem ist über die Herkunft der Daten zu informieren, wodurch die Identifizierung der verantwortlichen Stelle erleichtert wird. Die Regelungen greifen zwar zum Teil mit langfristigen Übergangsregelungen, z. B. für Zwecke der Markt- und Meinungsforschung erst ab dem 01.09.2010 und für Zwecke der Werbung erst ab dem 01.09.2012, dennoch müssen die Regelungen zu massiven Änderungen der Werbepraxis führen. Eine „Weiter-so-wie-bisher-Praxis“ führt unumgänglich zu Datenschutzverstößen.

- **Arbeitnehmerdatenschutz**

Ein eigenständiges Gesetz zum Datenschutz im Beschäftigungsverhältnis wurde nicht erlassen. Stattdessen wurde ein Paragraph in das Bundesdatenschutzgesetz eingefügt - § 32 BDSG Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses -. § 32 BDSG regelt den Umgang mit Beschäftigtendaten und stellt inhaltlich eine Reaktion auf die Datenschutzskandale insbesondere im Rahmen der „Korruptionsbekämpfung“ in Unternehmen dar. In der Norm werden die Ergebnisse der bisherigen Rechtsprechung zum Beschäftigtendatenschutz zusammengefasst. Hierdurch werden die bestehenden Regelungen der § 28 Abs. 1 Satz 1 Nr. 1 und § 28 Abs. 1 Satz 2 BDSG aufgegriffen und im Hinblick auf Beschäftigungsverhältnisse konkretisiert und teilweise verdrängt.
Nach § 32 Abs. 1 Satz 1 BDSG darf mit personenbezogenen Daten eines Beschäftigten nur umgegangen werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses, für dessen Durchführung oder Beendigung erforderlich ist. Die Regelung ist somit einschlägig beim Umgang mit Daten zur Bewerberauswahl, zu Leistungs- und Ver-

haltenskontrollen, zu Abmahnungen und Kündigungen, aber auch zur Verhinderung von Straftaten und sonstigen Verstößen.
Zur Aufdeckung von Straftaten beinhaltet § 32 Abs. 1 Satz 2 BDSG eine Spezialnorm, die enge Voraussetzungen zum Datenumgang mit Daten zu diesem Zweck vorgibt.

- **Informationspflichten bei Sicherheitslecks und Datenpannen**

Der neue § 42a BDSG begründet eine Informationspflicht der verantwortlichen Stellen gegenüber den Aufsichtsbehörden und Betroffenen. Diese kommt bei konkret bezeichneten Arten personenbezogener Daten zur Anwendung. Und zwar bei personenbezogenen Daten, die nach § 3 Abs. 9 BDSG besonders geschützt sind, die einem Berufsgeheimnis unterliegen, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht auf solche beziehen oder Bank- oder Kreditkartenkonten betreffen. Weiterhin müssen diese Daten Dritten unrechtmäßig zur Kenntnis gelangt sein und es müssen hierdurch schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Derartige Auswirkungen sind anzunehmen, wenn bei einzelnen Betroffenen finanzielle Schäden oder soziale Nachteile (z. B. Identitätsbetrug) möglich sind.

Die **BDSG-Novelle I** ist zum 1.4.2010 in Kraft getreten. Sie erfasst Neuregelungen, die sich auf die Tätigkeit von Auskunfteien und den Einsatz von Scoring-Systemen beziehen. Das Hauptziel dieser BDSG-Novelle war eine verbesserte Transparenz für die Betroffenen bei der Tätigkeit der Auskunfteien und den von diesen praktizierten Verfahren, insbesondere bei Scoring-Verfahren. Die Neuregelungen treffen hauptsächlich Auskunfteien und die Kreditwirtschaft. Von den Vorgaben zum Scoring und zur Bonitätsbewertung sind aber auch andere Bereiche wie etwa Telekommunikationsunternehmen und Versandhandel betroffen. Nachfolgend werden die wichtigsten Änderungen der BDSG-Novelle I im Überblick dargestellt:

- **Automatisierte Einzelentscheidung**

Um Menschen nicht rein maschinellen Entscheidungen, z. B. auf Basis eines durch Computer erstellten Persönlichkeitsprofils, auszuliefern, verbietet § 6a Abs. 1 BDSG bereits seit 2001 automatisierte Entscheidungen, denen die Bewertung einzelner Persönlichkeitsmerkmale zu Grunde liegen und die den Betroffenen erheblich beeinträchtigen. Nunmehr definiert der Gesetzgeber auch, wann eine ausschließlich auf eine automatisierte Verarbeitung gestützte Einzelentscheidung i. S. d. § 6a Abs. 1 Satz 1 BDSG vorliegt (§ 6a Abs. 1 S. 2 BDSG n. F.).
Zulässig war eine automatisierte Einzelentscheidung nach der alten Fassung des BDSG, wenn der Betroffene z. B. die Möglichkeit erhielt, seinen Standpunkt geltend zu machen, und die verantwortliche Stelle daraufhin die Entscheidung erneut geprüft hat. Die weitere Regu-

lierung solcher Entscheidungsverfahren erfolgt zum stärkeren Schutz der Betroffenen: Es soll verhindert werden, dass der Betroffene zum Objekt einer Bewertung wird, ohne auf einen voll automatisiert ablaufenden Prozess Einfluss nehmen zu können. Deswegen soll ein menschlicher Ansprechpartner existieren, der die Entscheidung gegenüber dem Betroffenen verantwortet und bei dem der Betroffene auch eine Gegendarstellung abgeben kann. Dem Betroffenen ist bei einer automatisierten Entscheidung mitzuteilen, „woran es gelegen hat" und hat zur Konsequenz, dass es in verantwortlichen Stellen sichergestellt werden muss, dass Entscheidungen unter Berücksichtigung etwaiger Gegendarstellungen durch den Betroffenen nochmals zu überprüfen sind.

- **Einmeldung von Daten bei einer Auskunftei**

Erstmalig hat der Gesetzgeber in § 28 a BDSG in einem konkreten Katalog festgelegt, unter welchen Voraussetzungen Daten über eine Forderung bei einer Auskunftei eingemeldet werden dürfen. Allerdings wird nunmehr auch die Einmeldung von sogenannten nicht titulierten Forderungen ausdrücklich gesetzlich legitimiert. Dabei handelt es sich um Forderungen, deren Bestehen weder durch einen Vollstreckungsbescheid noch durch einen Titel vor Gericht, d. h. von unabhängiger dritter Seite, festgestellt wurde. Diese Forderungen dürfen zukünftig unter bestimmten Verfahrensvoraussetzungen bei einer Auskunftei eingemeldet werden, wenn der Betroffene der Forderung nicht widersprochen hat. Der Betroffene ist rechtzeitig vor der Einmeldung zu unterrichten.
Eine weitere wichtige Änderung betrifft die Einmeldung von Informationen über die Begründung, ordnungsgemäße Durchführung und Beendigung des Vertragsverhältnisses bei Auskunfteien durch Kreditinstitute. Der Gesetzgeber hat grundsätzlich anerkannt, dass diese Informationen über die Auskunfteien anderen Banken und Kreditinstituten zur Verfügung stehen sollen. Damit soll das Einholen einer Einwilligung der Betroffenen als Grundlage für den Datenaustausch nicht mehr nötig sein. Der Betroffene hatte zuvor ohne Unterzeichnung der Erklärung ohnehin keine Chance, die gewünschte Leistung zu erhalten. Denn egal ob ein Girokonto eröffnet oder ein Kredit beantragt werden sollte, der Kunde musste einwilligen, dass die Bank die Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung des Vertragsverhältnisses an eine Auskunftei übermittelt (z. B. Schufa-Klausel). Nun darf die Datenübermittlung aufgrund der gesetzlichen Neuregelung stattfinden. Etwas anderes gilt für den Fall eines Kontos ohne Überziehungsmöglichkeit, hier ist die Einmeldung von Daten gesetzlich nicht erlaubt.

- **Scoring**

Der Gesetzgeber hat in § 28b BDSG erstmals das Scoring-Verfahren gesetzlich geregelt. Beim Scoring-Verfahren wird für bestimmte Merkmale ein Wert errechnet. Dieser Wert drückt

die statistische Wahrscheinlichkeit aus, mit welcher ein bestimmtes Ereignis eintritt oder ein bestimmtes Verhalten zukünftig erfolgt. Dem Betroffenen wird dieser Wert in einem Entscheidungsverfahren, z. B. im Rahmen einer Kreditvergabeentscheidung, mit entsprechenden Konsequenzen zugerechnet.
Welche Merkmale beim Scoring genutzt werden dürfen, normiert der Gesetzgeber nur bedingt. Festgelegt ist, dass die zum Einsatz kommenden Verfahren wissenschaftlich anerkannte mathematisch-statistische Verfahren sind und die genutzten Daten nachweisbar für die Berechnung der Wahrscheinlichkeit erheblich sein müssen. Dies ist der Aufsichtsbehörde bei entsprechender Kontrolle nachzuweisen und somit bereits im Vorfeld zu dokumentieren. Die ausschließliche Nutzung von Anschriftendaten ist unzulässig.

- **Auskunftsrecht der Betroffenen**

Um den Betroffenen Transparenz über den Umgang mit ihren Daten zu gewährleisten, wurde das Recht auf Auskunft (§ 34 BDSG) neu geregelt und ein diesbezüglicher Bußgeldtatbestand eingeführt. In § 34 Abs. 2 Satz 1 BDSG wird klargestellt, dass und wie Betroffene auf Verlangen Auskunft erhalten sollen, wenn ein Scoring-Verfahren eingesetzt wird.
Der Gesetzgeber hat auch für die Kosten der Auskunftserteilung eine Neuregelung getroffen. Grundsätzlich war die Auskunft bereits nach dem alten Recht unentgeltlich. Etwas anderes galt jedoch, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen konnte, so z. B. Auskünfte von Auskunfteien. Zwar war eine Auskunft auch hier bislang kostenfrei, wenn besondere Umstände die Annahme rechtfertigten, dass Daten unrichtig oder unzulässig gespeichert werden. Nunmehr sind solche Gründe nicht mehr notwendig, um **einmal pro Jahr** die bei einer Auskunftei gespeicherten Daten im Wege eines Auskunftsersuchens zu prüfen. Darüber hinaus sind in § 34 Abs. 8 Satz 5 BDSG die Fälle benannt, in denen ein Entgelt nicht verlangt werden darf.

2.2 Die Rechte der Betroffenen nach dem Bundesdatenschutzgesetz

Seit der Einführung der Personalcomputer und des Internets und der dadurch verursachten Explosion der Datenmengen, fällt es schwer, zu wissen, wer was bei welcher Gelegenheit über eine Person weiß und welcher Umgang mit den Daten beabsichtigt ist. Hinzu kommt, dass es auch bei persönlichem Kontakt in vielen Situationen an Transparenz mangelt.
Zur Wahrnehmung des Rechtes auf informationelle Selbstbestimmung normiert das Bundesdatenschutzgesetz in den §§ 33 – 35 BDSG Rechte für die Betroffenen. Sie versetzen Betroffene in die Lage, Korrektur-, Löschungs- oder ggf. Schadenersatzansprüche gegenüber der verantwortlichen Stelle geltend zu machen. Verantwortliche Stelle ist die Stelle, die per-

sonenbezogene Daten für sich erhebt, speichert, übermittelt, verarbeitet, nutzt oder dies durch andere im Auftrag vornehmen lässt.
Zu den grundlegenden Prinzipien des Datenschutzes gehört die Transparenz der Datenverarbeitung. Sie ist ein wesentlicher Akzeptanzfaktor für den Umgang mit personenbezogenen Daten und hat zum Ziel, den Betroffenen ausreichend über den Umfang des Umgangs mit seinen Daten zu informieren. Hierzu statuiert § 4 Abs. 2 Satz 1 BDSG den **Grundsatz der Direkterhebung** beim Betroffenen. Damit einher geht die Verpflichtung zur Information über Art und Verwendungszwecke der beabsichtigten Datenverarbeitung. 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.

Darüber hinaus normiert § 33 BDSG eine **Verpflichtung zur Benachrichtigung**, wenn eine verantwortliche Stelle Daten verarbeitet, die sie nicht direkt bei Betroffenen erhoben hat. Ohne eine Benachrichtigung wüsste der Betroffene nicht, gegenüber wem er beispielsweise seinen **Auskunftsanspruch** geltend machen kann. Mit einem an die verantwortliche Stelle gerichteten Auskunftsersuchen kann der Betroffene im Rahmen des § 34 Abs. 1 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.

Hat **ein Scoring stattgefunden**, kann der Betroffene gemäß § 34 Abs. 2 BDSG Auskunft erhalten über:

- die innerhalb der letzten sechs Monate vor dem Zugang des Auskunftsverlangens erhobenen oder erstmalig gespeicherten Wahrscheinlichkeitswerte,
- die zur Berechnung der Wahrscheinlichkeitswerte genutzten Datenarten und
- das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte, einzelfallbezogen und nachvollziehbar.

Die Auskunft ist, wie bereits ausgeführt, grundsätzlich unentgeltlich.

In diesem Zusammenhang soll nicht unerwähnt bleiben, dass jedermann ein **Recht auf Einsicht in das Verfahrensverzeichnis** einer verantwortlichen Stelle besitzt. Dabei handelt es sich um eine Übersicht über deren automatisierte Verarbeitungen. Darin sind die von dem

Unternehmen verwendeten Verfahren verzeichnet und ist festgehalten, zu welchem Zweck bzw. zur Erfüllung welcher Aufgabe die Verfahren angewendet werden. Außerdem kann man dem Verfahrensverzeichnis die verarbeiteten Datenarten entnehmen, die Personengruppen, über die Daten gespeichert werden sowie Kategorien von Empfängern, denen die Daten mitgeteilt wurden.

Stellt ein Betroffener fest, dass unrichtige Daten über ihn bei der verantwortlichen Stelle gespeichert werden, besitzt er ein **Berichtigungsrecht (**§ 35 Abs. 1 Satz 1 BDSG).
Personenbezogene Daten sind grundsätzlich zu **löschen**, wenn sie nicht mehr gebraucht werden oder die verantwortliche Stelle sie gar nicht hätte erheben dürfen. Gegebenenfalls tritt an die Stelle einer Löschung eine Sperrung, wenn

- besondere Gründe der 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. Die Tatsache der Sperrung darf ebenfalls nicht übermittelt werden.

Weiterhin besitzt jeder Betroffene ein **Recht auf Widerspruch**. Dieses Recht 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 **besonderes** Widerspruchsrecht steht den Betroffenen gegen die Verarbeitung oder Nutzung personenbezogener Daten zum Zwecke der Werbung und der Markt- oder Meinungsforschung zu (§ 28 Abs. 4 Satz 1 BDSG).
Hat ein Betroffener in den Umgang mit seinen personenbezogenen Daten eingewilligt, kann er die Einwilligung nach § 4a BDSG **jederzeit** widerrufen.

Schließlich 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

3.1 Allgemeines zur Aufsichtstätigkeit

3.1.1 Ansprechpartner und Internetpräsenz

Das Landesverwaltungsamt ist in Sachsen-Anhalt die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich. Die örtliche Zuständigkeit der Aufsichtsbehörde für den nicht-öffentlichen Bereich knüpft grundsätzlich an den Ort der Datenverarbeitung an, also der Betriebsstätte oder Zweigniederlassung, wo die Daten tatsächlich verarbeitet werden. Auf den Sitz der Unternehmensleitung kommt es daher 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)).

Die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich des Landes Sachsen-Anhalt ist unter folgender Anschrift erreichbar:

Landesverwaltungsamt - Referat Justitiariat
Ernst-Kamieth-Straße 2
06112 Halle (Saale)

Telefonische oder schriftliche Anfragen können auch an

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

Frau Westerkamp (Referentin)
E-Mail: Anke.Westerkamp@lvwa.sachsen-anhalt.de, Telefon: 0345/514-3925
und

Frau Damm
E-Mail: Nicole.Damm@lvwa.sachsen-anhalt.de, Telefon: 0345/514-3775
gerichtet werden.

Auch der Faxanschluss, Fax-Nummer: 0345/5143799 kann genutzt werden, um die Aufsichtsbehörde zu kontaktieren.

Der Internetauftritt des Landesverwaltungsamtes liefert Informationen zum Datenschutz im nicht-öffentlichen Bereich, die unter www.lvwa.sachsen-anhalt.de/datenschutz eingesehen werden können. Neben allgemeinen Hinweisen zum Datenschutz und Angaben zu Ansprechpartnern sind Merkblätter über ausgewählte datenschutzrechtliche Problemstellungen veröffentlicht.

3.1.2 Eingaben, Kontrollen

Schwerpunkt der Tätigkeit der Aufsichtsbehörde war auch in den Jahren 2007 bis 2009 die Bearbeitung von Beschwerden betroffener Bürger. Die Aufsichtsbehörde stellte im Jahr 2008 einen starken Anstieg der Beschwerden von Betroffenen fest. Dieser Trend setzte sich im Jahr 2009 fort. Dies ist dem unter 3.2 abgebildeten zahlenmäßigen Überblick über die Tätigkeit der Aufsichtsbehörde im Detail zu entnehmen.

Die meisten Verfahren konnten im schriftlichen Verfahren mit den verantwortlichen Stellen geklärt werden. Im Bereich der Videoüberwachung fanden zudem Vorortkontrollen statt.

Hinweise in der Presse führten zu einer umfassenden Prüfung aller Call-Center in Sachsen-Anhalt. Schwerwiegende Verstöße gegen das BDSG wurden dabei nicht festgestellt.

3.1.3 Beratung von Bürgern, Unternehmen und betrieblichen Datenschutzbeauftragten

Die Aufsichtsbehörde hatte vermehrt telefonische Anfragen und Beratungswünsche von Bürgern und Unternehmen zu verzeichnen. Telefonisch können regelmäßig nur die Bestimmungen des Datenschutzrechts allgemein erläutert und eine grobe Einschätzung der Rechtslage gegeben werden. Bei einem zu vertiefenden Beratungsbedarf bzw. der Bitte um Feststellung der Zulässigkeit einer Verfahrensweise, wird um schriftliche Sachverhaltschilderung (auch per E-Mail) gebeten. Von den telefonischen Anfragen wurden ca. 2/3 einer detaillierten Überprüfung im schriftlichen Verfahren unterzogen.

Im Rahmen ihrer personellen und zeitlichen Möglichkeiten nimmt die Aufsichtsbehörde an den von der Gesellschaft für Datenschutz und Datensicherung e. V. organisierten Sitzungen der Erfahrungsaustausch (ERFA)-Kreise der betrieblichen Datenschutzbeauftragten teil. Im sog. ERFA-Kreis werden aktuelle Datenschutz- und Datensicherheitsfragen erörtert.

Auch besteht die Möglichkeit, die Mitarbeiter der Aufsichtsbehörde um Vortragstätigkeiten im Bereich des Datenschutzes zu bitten. Im Berichtszeitraum wurde zu verschiedenen Themen, wie z. B. „Datenschutz im Mittelstand“, „Datenschutz in der Arztpraxis“ oder „Datenschutz für Betriebsräte“ bei anfragenden Institutionen wie der Ärztekammer oder der Industrie- und Handelskammer referiert.

Um das Bewusstsein für den Datenschutz bereits im jugendlichen Alter zu fördern, beteiligt sich die Aufsichtsbehörde mit eigenen Beiträgen an dem Schulprojekt „Sozialkunde-/Rechtskundeunterricht in Sekundarschulen und Gymnasien“ des Landesverwaltungsamtes. Unter dem Thema „Datenschutz und Internet“ wird in das Datenschutzrecht eingeführt, die Tätigkeit der Aufsichtsbehörde dargestellt und an Beispielen aufgezeigt, welche Gefahren bei einem zu freizügigen Umgang mit den eigenen Daten bestehen und welche Gegenmaßnahmen ergriffen werden können.

3.1.4 Ordnungswidrigkeitenverfahren

Nach § 43 des Bundesdatenschutzgesetzes sind zahlreiche Verstöße gegen datenschutzrechtliche Vorschriften bußgeldbewehrt. Die Aufsichtsbehörde macht nach pflichtgemäßem Ermessen von der Möglichkeit Gebrauch, ein Bußgeld zu verhängen.

Für die Aufsichtsbehörde stehen Bußgeldverfahren nicht im Vordergrund. Die Aufsichtsbehörde hat mehr Interesse daran, durch Aufklärung und Beratung das datenschutzgerechte Verhalten der verantwortlichen Stellen zukünftig sicherzustellen, als Verstöße im Nachhinein zu ahnden. Stets wurde geprüft, ob eine Verwarnung, ggf. mit Verwarngeld, ausreichend ist.

Im Berichtszeitraum hat die Aufsichtsbehörde gegen die Regionalgesellschaft eines Discounters ein Bußgeld in sechsstelliger Höhe verhängt, weil diese insbesondere unzulässig Mitarbeiterdaten durch Detektive erhoben hatte. Hierzu folgen unter Abschnitt 4, Punkt 2.1 gesonderte Ausführungen.

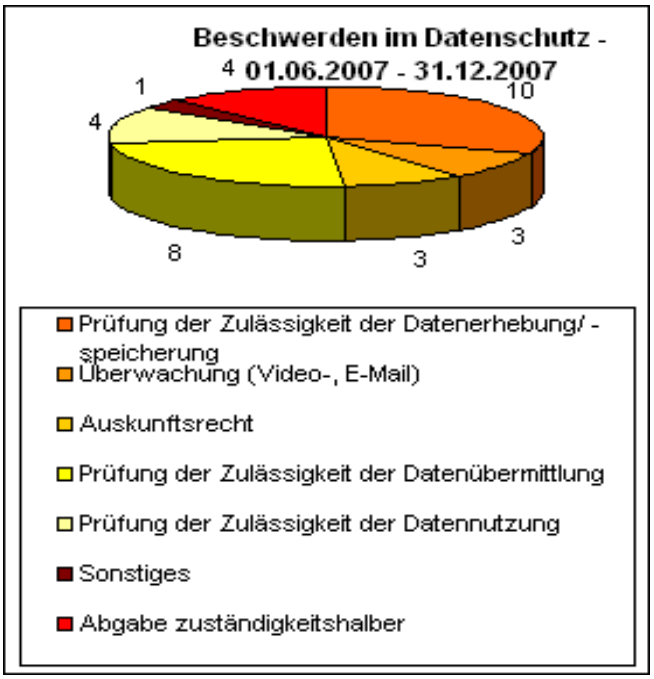
Insgesamt hat die Aufsichtsbehörde im Berichtszeitraum acht Bußgeldverfahren eingeleitet. In zwei Fällen wurde eine Verwarnung mit einem Verwarngeld ausgesprochen. In zwei anderen Fällen wurde die unzulässige Erhebung von Daten bei einer Auskunftei geahndet. Die Bußgeldbescheide wurden bestandskräftig. Die übrigen Verfahren befinden sich im Anhörungsverfahren. Drei dieser Verfahren beziehen sich auf die beharrliche Verweigerung, der Aufsichtsbehörde die erbetenen Auskünfte zu erteilen.

3.2 Zahlenmäßiger Überblick über die Tätigkeit der Aufsichtsbehörde

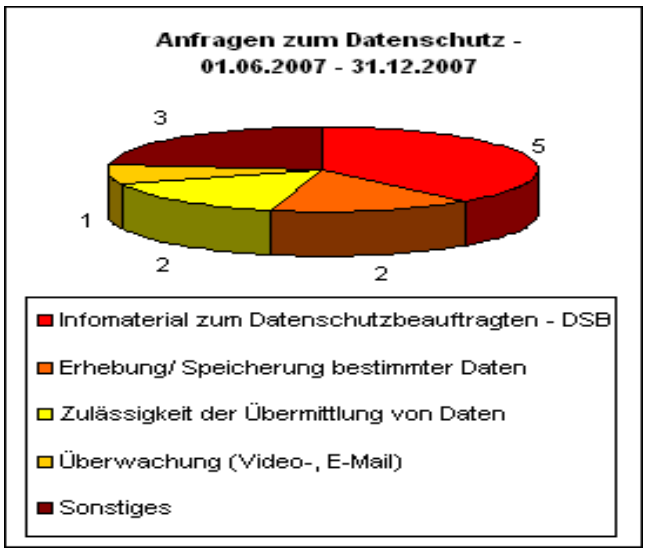
Zeitraum vom 01.06.2007 – 31.12.2007

Verfahren im Datenschutz **- Überblick -** 01.06.2007 - 31.12.2007	
Anfragen	13
Beschwerden	33

Beschwerden im Datenschutz - Überblick 01.06.-31.12.2007	
Prüfung der Zulässigkeit der Datenerhebung/ -speicherung	10
Überwachung (Video-, E-Mail)	3
Auskunftsrecht	3
Prüfung der Zulässigkeit der Datenübermittlung	8
Prüfung der Zulässigkeit der Datennutzung	4
Sonstiges	1
Abgabe zuständigkeits-halber	4

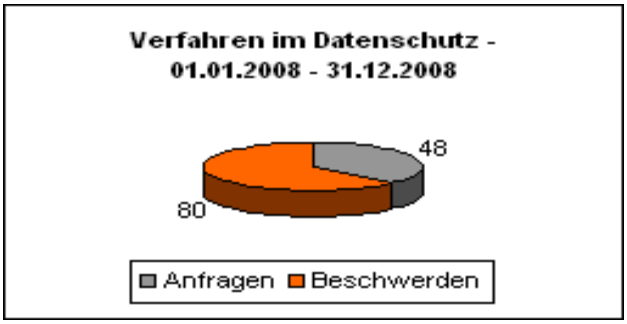


Anfragen im Datenschutz - Überblick 01.06.-31.12.2007	
Infomaterial zum Daten-schutzbeauftragten – DSB	5
Erhebung / Speicherung bestimmter Daten	2
Zulässigkeit der Über-mittlung von Daten	2
Überwachung (Video-, E-Mail)	1
Sonstiges	3

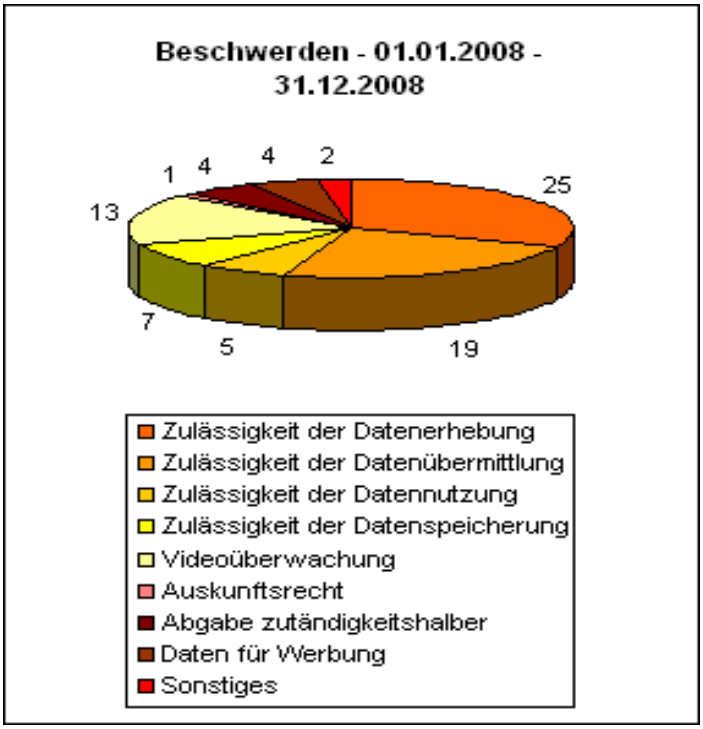


Zeitraum vom 01.01.2008 – 31.12.2008

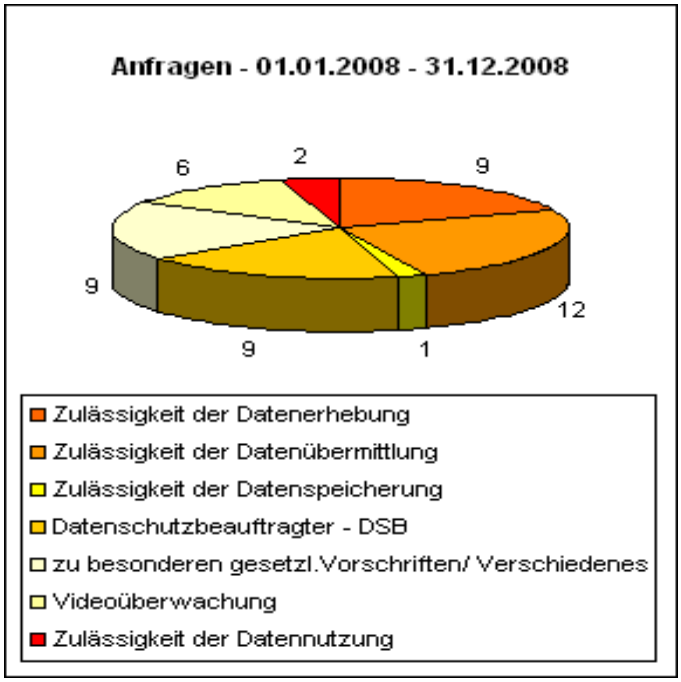
Verfahren im Datenschutz – **Überblick** – 01.01.2008 - 31.12.2008	
Anfragen	48
Beschwerden	80



Beschwerden im Datenschutz - Überblick 01.01.-31.12.2008	
Zulässigkeit der Daten-erhebung	25
Zulässigkeit der Daten-übermittlung	19
Zulässigkeit der Daten-nutzung	5
Zulässigkeit der Daten-speicherung	7
Videoüberwachung	13
Auskunftsrecht	1
Abgabe zuständigkeits-halber	4
Daten für Werbung	4
Sonstiges	2

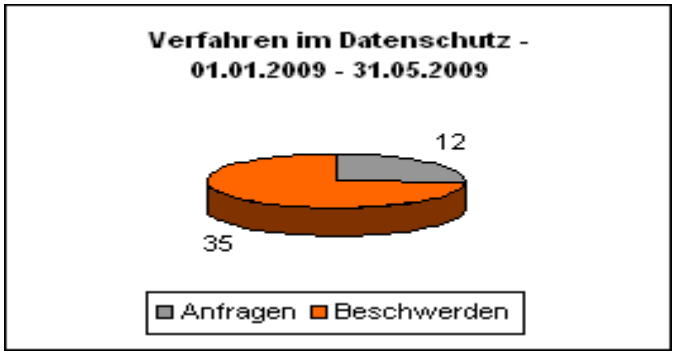


Anfragen im Datenschutz - Überblick 01.01.-31.12.2008	
Zulässigkeit der Daten-erhebung	9
Zulässigkeit der Daten-übermittlung	12
Zulässigkeit der Daten-speicherung	1
Datenschutzbeauftragter – DSB	9
zu besonderen gesetzl. Vorschriften / Verschie-denes	9
Videoüberwachung	6
Zulässigkeit der Daten-nutzung	2

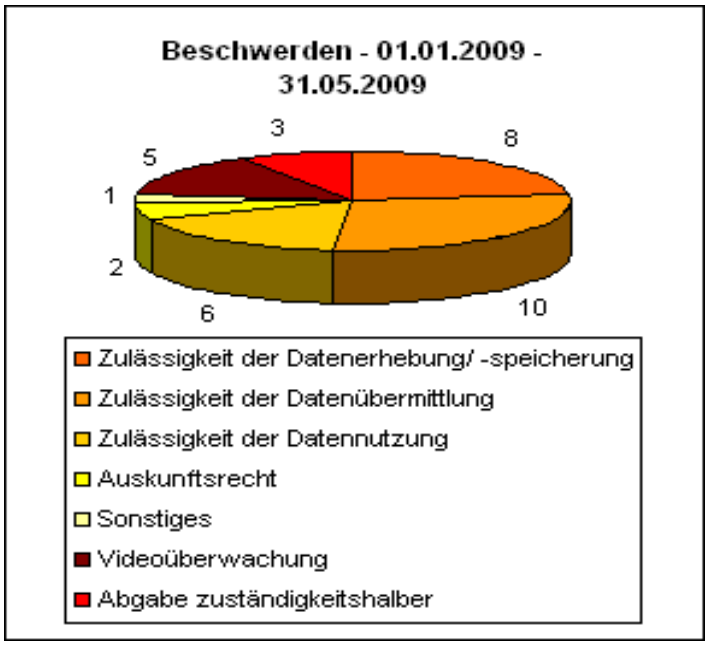


Zeitraum vom 01.01.2009 – 31.05.2009

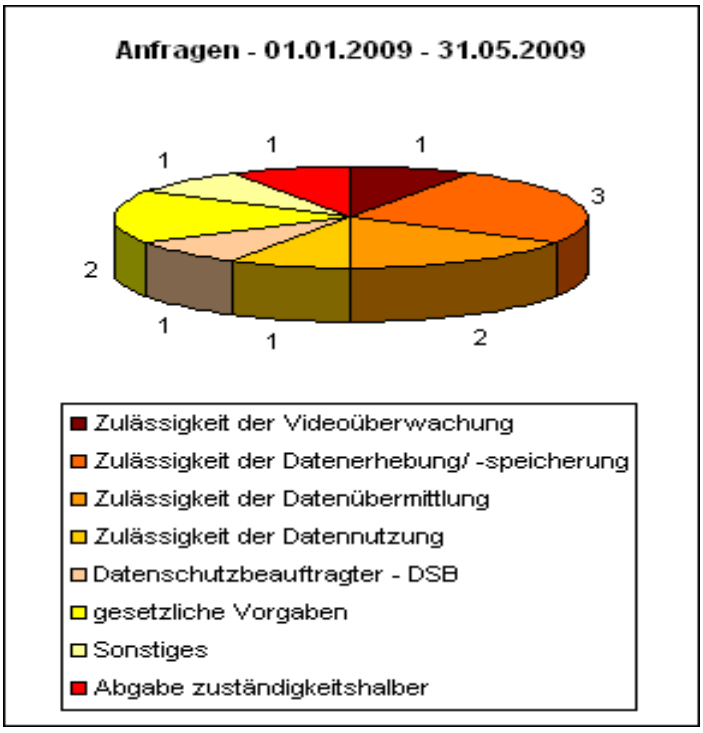
Verfahren im Datenschutz **- Überblick -** 01.01.2009 - 31.05.2009	
Anfragen	12
Beschwerden	35



Beschwerden im Datenschutz - Überblick 01.01.-31.05.2009	
Zulässigkeit der Daten-erhebung/ -speicherung	8
Zulässigkeit der Daten-übermittlung	10
Zulässigkeit der Daten-nutzung	6
Auskunftsrecht	2
Sonstiges	1
Videoüberwachung	5
Abgabe zuständigkeits-halber	3



Anfragen im Datenschutz - Überblick 01.01.-31.05.2009	
Zulässigkeit der Video-überwachung	1
Zulässigkeit der Daten-erhebung/ -speicherung	3
Zulässigkeit der Daten-übermittlung	2
Zulässigkeit der Daten-nutzung	1
Datenschutzbeauftragter – DSB	1
gesetzliche Vorgaben	2
Sonstiges	1
Abgabe zuständigkeits-halber	1



4 Einzelne Punkte aus Anfragen und Beschwerden

4.1 Von Beratungsinteresse – ausgewählte Aspekte der Anfragen

4.1.1 Betriebs-/Dienstvereinbarungen

Eine Betriebsvereinbarung ist ein Vertrag zwischen Arbeitgeber und Betriebsrat. Mit ihr werden alle Beteiligten betreffenden Rechte und Pflichten der Parteien begründet und verbindliche Normen für alle Arbeitnehmer eines Betriebes formuliert. Unterschiedliche Anlässe, so z. B. zur Einführung/Nutzung eines Zeiterfassungssystems, zum Voice-Recording oder zur Nutzung von Informations- und Kommunikationstechnik im Allgemeinen führen zu derartigen Verträgen.

Die Einführung verschiedenartiger technischer Systeme, mit denen regelmäßig ein Umgang mit personenbezogenen Daten verbunden ist, soll den Unternehmen Vorteile bringen. Bewegt sich der Umgang mit den Daten nicht im zulässigen Rahmen, werden allerdings die Schattenseiten technischer Systeme besonders deutlich. Daher sind die Betriebsräte in den entsprechenden Verhandlungen gefordert, wenn Betriebsvereinbarungen als Rechtsgrundlage für einen zulässigen Umgang mit Daten herangezogen werden sollen. Dies ist nur möglich, wenn die Betriebsvereinbarungen nicht gegen – höherrangige – Gesetze verstoßen.

Die Zulässigkeit von Personaldatenverarbeitung als Gegenstand einer Betriebs-/Dienstvereinbarung ist nach § 32 BDSG (bislang § 28 BDSG) zu prüfen.

In Besprechungen mit Betriebsratsmitgliedern unterschiedlicher Firmen konnte die Aufsichtsbehörde darauf hinweisen, welche Gefahren sich aus bestimmten Vereinbarungen ergeben können, welche Vereinbarungen missverständlich sind und in welchen Bereichen verstärkt Transparenz herbeigeführt werden muss. Es wurde deutlich, dass die Arbeitnehmervertreter ihre Aufgabe, für den Schutz der Beschäftigten vor Datenmissbrauch einzustehen, ernst nehmen. Der Einsatz immer komplexer werdender Technik am Arbeitsplatz soll nicht zur Überwachung der Mitarbeiter führen.

Betriebsräte haben bei der „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen“ (§ 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz

Ziel einer Betriebsvereinbarung muss sein, dass…

- für alle Beschäftigten Planungs-, Einführungs- und Anwendungsprozesse von Systemen transparent

(BetrVG)) mitzubestimmen. Für dieses Mitbestimmungsrecht ist nicht entscheidend, ob eine Überwachung auch tatsächlich stattfindet. Es genügt, dass sie möglich ist. Eine ohne Beachtung der Beteiligungsrechte durchgeführte Verarbeitung von Mitarbeiterdaten kann unzulässig sein.

Formell hat jede Betriebs- und Dienstvereinbarung einen räumlichen, persönlichen und sachlichen Geltungsbereich. Räumlich erfasst sie die Betriebe und Dienststellen, für die sie abgeschlossen ist. In persönlicher Hinsicht erstreckt sie sich auf die Beschäftigten bzw. auf bestimmte Beschäftigungsgruppen der betroffene Betriebe/Dienststellen. Der sachliche Geltungsbereich betrifft den eigentlichen Zweck oder Gegenstand der Verarbeitung.

und nachvollziehbar gestaltet sind;

- Systeme so eingesetzt werden, dass ein Beitrag zur Verbesserung der Arbeitsqualität geleistet wird;
- die Beschäftigten vor unzulässiger und vor allem unnötiger Nutzung der über sie erfassten und gespeicherten Daten geschützt werden.

-> Eine die Beschäftigten benachteiligende Verarbeitung personenbezogener Daten muss organisatorisch (und überall wo dies möglich ist auch technisch) ausgeschlossen werden.

-> Leistungs- und Verhaltenskontrolle ist demzufolge eigentlich immer ausgeschlossen.

Typische und wichtigste Regelungsgegenstände in der Praxis sind Vereinbarungen über:

- Arbeitszeitsysteme
- Betriebsdatenerfassung
- Datenschutz in Call-Centern
- E-Learning
- E-Mail- und Internetnutzung
- Handynutzung
- PC- bzw. Laptop-Einsatz
- personaldatenverarbeitende Systeme (Abrechnungs- und Informationssysteme)
- Telearbeit
- Telefondatenerfassung und
- Zugangskontrollen

Die Kernpunkte, die in Betriebs-/Dienstvereinbarungen behandelt werden, lassen sich wie folgt zusammenfassen:

- Ziele, Regelungsgegenstand und Geltungsbereich
- Systemanwendung, Datenkatalog
- Begriffsbestimmungen

- Zulässigkeit der Datenverarbeitung und -nutzung
- Leistungs- und Verhaltenskontrolle
- Auftragsdatenverarbeitung
- Rechte der betroffenen Beschäftigten
- Rechte des Betriebsrates (Informationen, Kontrollen, Sachverständige)
- Aufgaben des Datenschutzbeauftragten
- Datensicherung, Zugriffsberechtigungen
- Löschfristen
- Arbeitskreis/Verfahren bei Streitigkeiten
- Schlussbestimmungen, Kündigung und Nachwirkung.

Die Aufsichtsbehörde hat u. a. ein im Seniorenbereich tätiges Unternehmen bei der Einführung und Nutzung eines Zeiterfassungssystems beraten und konkrete Hinweise zu Regelungsinhalten und deren Umsetzung gegeben. Die Betriebsvereinbarung war insbesondere in folgenden Punkten zu ergänzen:

- konkrete Festlegungen zur Datenspeicherung und -nutzung,
- konkrete Regelungen zum Zugriff auf die Arbeitszeitdaten,
- die Nennung der zugriffsberechtigten Mitarbeiter,
- die Auskunftsrechte der Beschäftigten.

4.1.2 Mithören/Aufzeichnung von Telefongesprächen

Das Telefon ist ein gängiges und wichtiges Kommunikationsmittel. In Unternehmen wird es beim Kontakt mit Kunden und Lieferanten genutzt. Häufig darf der Arbeitnehmer das Firmentelefon auch für private Zwecke nutzen. Aus diesen vielfältigen Anwendungen resultieren verschiedene Anliegen der Arbeitgeber.

Hierzu hat die Aufsichtsbehörde den Betriebsrat eines Unternehmens aus dem Bereich der Telekommunikation beraten. Der Betriebsrat übersandte zwei Betriebsvereinbarungen, die diesem von der Geschäftsführung zu den Themen Business Coaching (Silent Monitoring) und Voice-Recording vorgelegt worden waren.

Konkret sollte der Mitarbeiter beim *Voice-Recording* unter Verwendung des vorgesehenen Programms seine eigenen Gespräche oder Gesprächsteile mitschneiden, sofern ein Abschluss zustande kommt, eine Dienstleistung beauftragt wird oder eine anderweitige Notwendigkeit für die Aufzeichnung besteht (One-way Recording). Bei einem Two-way Voice-Recording werden die Aussagen beider Gesprächspartner aufgezeichnet. Neben dem Ein-

satz der VoiceFiles (Sprachaufzeichnungen) als Beweismittel sollten die Projektverantwortlichen die Befugnis erhalten, eine Stichprobe von 10-15 % der Mitschnitte pro Tag anzuhören, um zu überprüfen, ob die Anforderungen der Auftraggeber eingehalten werden bzw. die geforderten Verbesserungen des Auftraggebers durch den Mitarbeiter umgesetzt wurden.

Im Rahmen des *„business-coachings“* sollte dem Arbeitgeber, einem Auftraggeber oder einem besonders beauftragten Dritten ein Zugriffsrecht auf einzelne Mitarbeiter-Plätze erteilt werden. Es sollte ein Zugriff auf dienstliche Gespräche und Applikationen (Bildschirminhalte) während eines Zugriffskorridors ohne vorheriges Signal ermöglicht werden. Das Mithören und Mitschneiden persönlicher Zwischengespräche wurde nicht gestattet. Auf Basis der erhaltenen Daten sollte die Bewertung einer Mitarbeitergruppe erlaubt werden. Die Bewertung eines einzelnen Mitarbeiters sollte einen Zeitraum von maximal einem Tag oder eine entsprechende Anzahl von Gesprächen – bezogen auf die durchschnittlichen Gesprächszeiten des Projektes pro Stunde - innerhalb eines Monats nicht überschreiten. Gesprächsmitschnitte einzelner Mitarbeiter sollten grundsätzlich nur zur Ermittlung von zusätzlichem Schulungsbedarf verwendet werden. In Ausnahmefällen jedoch auch, um Leistungsbeurteilungen und disziplinarische Maßnahmen zu verhängen.

Allgemein sind in Bezug auf das Anliegen der „Qualitätssicherung“ in der Praxis folgende Varianten zum Mithören/Aufzeichnen von Telefongesprächen 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.

In diesem Zusammenhang ist es von Bedeutung, ob das heimliche Ab- bzw. Mithören von dienstlichen Telefongesprächen durch individuelle Einwilligungen oder kollektivrechtliche Vereinbarungen 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 nicht grundsätzlich unzulässig. Beim Abschluss eines Arbeitsvertrages wird durch den Arbeitnehmer eine gewisse Überwachung des Arbeitsverhaltens 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 oder etwaige Vereinbarungen zu stellen. Zudem muss der Grundsatz der Verhältnismäßigkeit beachtet werden. Ergibt die Abwägung der berechtigten Interessen des an der Überwachung Interessierten und den schutzwürdigen Interessen der Betroffenen, 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 „Überwachungs“sachverhalt von Fall zu Fall individuell zu beurteilen. Eine pauschale Aussage zur Zulässigkeit oder Unzulässigkeit beabsichtigter „Qualitätssicherungsmaßnahmen“ kann somit nicht getroffen werden. Werden die vorgenannten Rahmenbedingungen eingehalten, kann der Arbeitgeber eine Einwilligung von den betroffenen Arbeitnehmern verlangen oder diesbezügliche kollektivrechtliche Vereinbarungen treffen.

Nach Auffassung der Aufsichtsbehörde reicht die Möglichkeit des **offenen direkten Mithörens** grundsätzlich aus, die Qualitätssicherung in ausreichendem Maße durchführen zu können, ohne unverhältnismäßig in die Rechte der Betroffenen einzugreifen. Unbemerkte Abhörmaßnahmen sind nur in konkret begründeten Einzelfällen, wie z. B. zur Aufklärung schwerer Straftaten, der Verfolgung von Erpressern oder anonymen Anrufen im Einzelfall denkbar.

Diese Auffassung wurde auch gegenüber dem Betriebsrat des Unternehmens, der sich an die Aufsichtsbehörde wandte, vertreten. Es wurde ausgeführt, dass der beschriebene Umgang mit personenbezogenen Daten sowohl auf Basis eingeholter Einzeleinwilligungen der Mitarbeiter i. S. d. § 4a BDSG zulässig sein könnte als auch auf der Grundlage kollektivrechtlicher Regelungen in Form einer Betriebsvereinbarung. Eine gemischte Nutzung beider Alternativen wurde nicht empfohlen. Die Einholung von Einwilligungserklärungen verstärke im Vergleich zu Betriebsvereinbarungen zwar die Transparenz für die Betroffenen, die Einwilligungen seien jedoch jederzeit widerrufbar. Zudem stelle sich im Arbeitnehmerdatenschutzrecht stets die Frage, ob erteilte Einwilligungen freiwillig und damit wirksam sind.

Für die Betriebsvereinbarung zum Voice-Recording wurden zu den getroffenen Regelungen folgende Hinweise gegeben:

- Zur Verdeutlichung des Zwecks der von Auftraggebern geforderten Aufnahme ist darzulegen, welche Art der Aufzeichnung der Auftraggeber wozu benötigt.
- Eine Information der Mitarbeiter in mündlicher **und** schriftlicher Form ist notwendig (**ursprünglich vorgesehen**: mündlich **oder** schriftlich).
- One-way Voice-Recording widerspricht dem Zweck eine für den Auftraggeber nützliche Abschlusszusammenfassung zu erhalten.
- Zur Nutzung der Aufzeichnung auch zur Qualitäts- und Leistungsprüfung entsprechend der Vorgaben der Auftraggeber sind klare, transparente Regelungen vorzusehen.
- Es sind eindeutige Festlegungen zu treffen, in welchen berechtigten Fällen Anhörungen der VoiceFiles erfolgen.

Im Zusammenhang mit der Betriebsvereinbarung zum „Business-Coaching wurde der Betriebsrat allgemeingültig auf Folgendes hingewiesen:

- Die vorgeschlagenen Betriebsvereinbarungen waren bereits wegen unverhältnismäßiger Maßnahmen kritisch zu betrachten. Bei der Aufsichtsbehörde entstand zudem der Eindruck, dass das Monitoring (Mithören/Mitschneiden von Gesprächen) und Sceenrecording (Protokollieren/Aufzeichnungen von Bildschirmaktionen) der Leistungs- und Verhaltenskontrolle aller Arbeitnehmer dienen sollte und nicht allein eine „ungewollte Nebenwirkung“ dargestellt hätte. Zwischen den Maßnahmen Monitoring und Screenrecording sei zudem klar zu differenzieren.
- Werden Maßnahmen des Monitoring für notwendig erachtet, ist dem bloßen Mithören der Vorzug vor dem Aufzeichnen zu geben, wenn dies für die angestrebten Schulungszwecke ausreichend ist. Es muss in der Betriebsvereinbarung deutlich werden, dass das Monitoring-System ausschließlich eingesetzt wird, um die Ausbildungsprozesse zu verbessern und um die Qualifikation der Mitarbeiter und die Qualität der Kundenkontakte zu erhöhen. Der Einsatz des Monitoring zur Ermittlung von Basisdaten wie Zertifizierungen, Einzelplatz-Messungen, Bonus-Systemen oder ähnlichen Zwecken sei von vornherein auszuschließen.
- In der Betriebsvereinbarung ist zu regeln, dass die Mitarbeiter rechtzeitig durch das System mit Bildschirmanzeige darüber zu informieren sind, dass Telefongespräche mitgehört/aufgezeichnet werden. Aus Gründen der Verhältnismäßigkeit dürfen maximal zehn Telefongespräche je Monat und Person aufgezeichnet werden.
- Maßnahmen des Screenrecordings sollten durch eine Betriebsvereinbarung nur für die Probezeit und einmalig bei Aufnahme einer neuen Tätigkeit nach einer Versetzung ermöglicht werden.

- Der Betriebsrat wurde darauf hingewiesen, dass in der Betriebsvereinbarung Zugriffsberechtigungen hinsichtlich der Auswertung von Aufzeichnungen festgelegt werden sollten. Eine Auswertung entsprechend dem Zweck der Aufzeichnung sollte nur von zuständigen Trainern, nicht aber durch unmittelbare Vorgesetzte möglich sein.

4.1.3 Optisch-elektronische Einrichtungen (Videoüberwachung)

Das Thema „Videoüberwachung“ war auch im Berichtszeitraum ein „Dauerbrenner“. Durch eine Videoüberwachung kann in das Persönlichkeitsrecht von Personen eingegriffen werden. Die Aufsichtsbehörde setzt insbesondere auf Aufklärung und Beratung.

Zur Klärung der Zulässigkeit einer beabsichtigten Überwachung (§ 6b Abs. 1 BDSG) ist es sinnvoll, sich bereits vor der Installation der Videokamera an die Aufsichtsbehörde zu wenden. Dabei kann geklärt werden, wie dem Gebot der Datenvermeidung und -sparsamkeit (§ 3a BDSG) und dem Grundsatz der frühstmöglichen Datenlöschung (§ 35 Abs. 2 Satz 2 Nr. 3 BDSG) Folge geleistet werden kann.

***§ 6b BDSG – Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen* (Auszug)**

Abs. 1: *Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist zulässig, soweit sie*

1. *zur Aufgabenerfüllung öffentlicher Stellen,*
2. *zur Wahrnehmung des Hausrecht oder*
3. *zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke*

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

So wandte sich auch der Betreiber einer Sportanlage an die Aufsichtsbehörde. Er teilte mit, dass sich an bestimmten Stellen der Anlage „immer wieder mal“ Unfälle ereignen, die auf das Fehlverhalten einiger Benutzer zurückzuführen seien. Dies bedeute für das Unternehmen insbesondere Ärger mit dem Geschädigten, da die Schuldfrage nicht mehr zu klären sei. Man beabsichtige, eine Kamera mit Aufzeichnungsgerät zu installieren, da die Gefahr im Vorfeld nicht durch Hinweisschilder und die Belehrung der Fahrgäste durch das Personal zu minimieren gewesen sei.

Die Aufsichtsbehörde hat hier ein berechtigtes Interesse (siehe Begriffserläuterungen) des Unternehmens anerkannt und diesem mitgeteilt, dass dem Vorhaben, die beschriebene Kamera zu den dargelegten Zwecken zu installieren, grundsätzlich keine Bedenken entgegenstehen. Die konkrete Ausgestaltung der Kamera/s sollte jedoch vor Errichtung mit einem transparenten Videoüberwachungskonzept mit der Aufsichtsbehörde abgestimmt werden.

Ein Videoüberwachungskonzept soll mindestens folgende Angaben enthalten:

- die konkret festgelegten Zwecke der Beobachtung;
- Festlegung des erforderlichen Rahmens für die Beobachtung und für eine eventuell erforderliche Aufzeichnung;

  Aufgrund des Tatbestandsmerkmales der Erforderlichkeit (siehe Begriffserläuterungen) wurde im vorliegenden Fall aufgefordet, die Möglichkeit einer Kameraattrappe zu prüfen, da das Vorhandensein und die Kenntnis einer vermeintlichen Videobeobachtung genügen könnten, dass das Verhalten an Gefahrenstellen angepasst wird. Dabei wird eine Kameraattrappe wie eine funktionierende Kamera behandelt.
- Kenntlichmachung des Umstandes der Beobachtung und der verantwortlichen Stelle (§ 6b Abs. 2 BDSG);
- Löschfristen, verifiziert nach Vorgängen, in denen keine Unfälle auftreten und solchen, für die die Kamera installiert werden soll (§ 6b Abs. 5 BDSG);
- Hinweis für welche Zwecke die Daten verarbeitet und genutzt werden sollen (§ 6b Abs. 3 BDSG);
- Beschreibung der Betroffenenrechte (§ 6b Abs. 4, §§ 33 bis 35 BDSG).

Begriffserläuterungen:

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. Im Schutz des Eigentums ist regelmäßig ein berechtigtes Interesse zu sehen.

Der Zweck der Videoüberwachung ist vor Beginn der Überwachung konkret festzulegen. Dies soll zum einen die Nachprüfung des berechtigten Interesses erleichtern, aber auch Aufschluss darüber geben, dass die verantwortliche Stelle nicht leichtfertig optisch-elektronische Einrichtungen einsetzt.

Eine *Erforderlichkeit* ist dann nicht anzunehmen, wenn das berechtigte Interesse durch mildere, ebenfalls geeignete Mittel erreicht werden kann oder das angestrebte Ziel mit der Überwachung nicht erreicht werden kann. Dies ist z. B. der Fall, wenn die Videoüberwachung mangels ausreichender Beleuchtung im Dunkeln nicht funktionsfähig wäre. Zusätzlich zur Prüfung, ob der Einsatz einer Videoüberwachung gerechtfertigt ist, sind auch die techni-

schen Parameter der Kamera zu bewerten (Beweglichkeit der Kamera, Zoommöglichkeiten etc.).
Sind sowohl ein berechtigtes Interesse der verantwortlichen Stelle als auch die Erforderlichkeit der Überwachungseinrichtung zu bejahen, ist in einem letzten Schritt zu prüfen, ob Anhaltspunkte bestehen, dass *schutzwürdige Interessen der Betroffenen dem berechtigten Interesse der verantwortlichen Stelle überwiegen*. Dabei sind Betroffene nicht nur die Personen, deren Identität bestimmt werden kann oder bestimmbar ist. Schutzwürdige Interessen überwiegen, wenn die Intimsphäre Betroffener tangiert wird.

4.1.4 Übermittlung personenbezogener Daten im kleinen Rahmen - unternehmensinterne Zeitung

Ein Seniorenpflegeheim teilte der Aufsichtsbehörde mit, dass der Heimbeirat und viele Bewohner der Einrichtung wünschen, dass Geburtstage und Sterbetage der Bewohner in der Heimzeitung veröffentlicht werden. Hinsichtlich der Geburtstage sei das Geburtstagsdatum, der Name, die jeweilige Zimmernummer und das aktuelle Alter von Interesse.

Die Veröffentlichung von Daten in einer Heimzeitung stellt eine Übermittlung (siehe Begriffserläuterung) personenbezogener Daten dar.

Begriffserläuterungen:
Übermitteln ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener 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. Übermitteln stellt neben dem Speichern, Verändern, Sperren und Löschen personenbezogener Daten eine Form der Verarbeitung dar.

Als Zulässigkeitsalternativen für die Datenübermittlung kamen das Bundesdatenschutzgesetz (§§ 28ff BDSG) oder eingeholte Einwilligungen i. S. d. § 4a BDSG in Frage. Bezüglich der Zulässigkeit auf der Grundlage des § 28 BDSG a. F. bestanden aufgrund der Anfrage Zweifel an einem eigenen Interesse des Seniorenheimes an der Datenübermittlung. Darüber hinaus war für alle zu übermittelnden Daten (Name, Zimmernummer, Alter, Geburtstag) zu prüfen, ob die Interessen auf andere Weise nicht bzw. nicht angemessen gewahrt werden können (Grundsatz der Erforderlichkeit). Ein konkreter Umstand, der auf eine Beeinträchtigung schutzwürdiger Interessen der Heimbewohner hinwies, durfte ebenfalls nicht vorliegen. Die Aufsichtsbehörde führte hierzu beispielhaft aus, dass manche Heimbewohner daran inte-

ressiert sein könnten, ihr Alter zu verschweigen oder unerkannt in der Einrichtung untergebracht zu sein.

Es wurden folgende **Hinweise und Empfehlungen** zum Anliegen gegeben:

- Rechtssicher und transparenter ist, die Bewohner um eine Einwilligung (§ 4a BDSG) zur Übermittlung der Daten zu bitten.
- Im Hinblick auf die Einwilligung ist einführend zu erklären, wofür die Datenübermittlung erfolgen soll (Veröffentlichung in der Heimzeitung) und dass die Abgabe freiwillig ist. Dann sollten – jeweils mit Ankreuzkästchen versehen – die einzelnen zu veröffentlichenden Daten aufgeführt werden. So kann jeder Bewohner mittels Setzen eines Kreuzes entscheiden, welche Daten er preisgeben möchte. Sollte dies in der weiteren Bearbeitung der Veröffentlichung zuviel Arbeitsaufwand mit sich bringen, könnten auch nur die Daten benannt werden, die jeder preisgeben möchte.
- Nachfolgend sollte altersgerecht dargestellt werden, womit jeder einzelne Betroffene rechnen muss, wenn er seine Einwilligung nicht erteilt. Denkbar wäre z. B. dass sein Geburtstag nicht in der Zeitschrift veröffentlicht wird, aber auch dass sich keine Folgen für den Heimvertrag ergeben. Die Schriftlichkeit der Einwilligung sollte aus Gründen der Dokumentation bevorzugt werden. Auch empfiehlt es sich einen kurzen Hinweis darauf zu erteilen, dass die Einwilligung jederzeit widerrufbar ist.

4.1.5 Übermittlung personenbezogener Daten im großen Rahmen – im Internet allgemein und im Rahmen von Bewertungsplattformen

Gibt es noch Haushalte, in denen niemand das Internet nutzt? Fest steht jedenfalls, dass sich das Internet in fast jedem privaten Haushalt zu einem nicht mehr wegzudenkenden Medium entwickelt hat. Die Nutzungsmöglichkeiten sind vielseitig und kaum abschließend aufzuzählen, sie reichen von der reinen Beschaffung von Informationen bis zur Nutzung als Kommunikationsinstrument.

Verständlicherweise wollen auch Unternehmen oder Privatpersonen die Möglichkeiten des Mediums Internet nutzen, z. B. indem sie Informationen zugänglich machen oder eigene Dienste, wie Bewertungsplattformen, anbieten.

So wollte eine akademische Organisation das neue Mitgliederverzeichnis, welches Name incl. Foto, Forschungsinstitut, Universität und Informationen zum wissenschaftlichen Schwerpunkt enthielt, zusätzlich ins Internet einstellen. Die Informationen stammten z. T. von

den Personen selbst, aber zum Teil auch aus Angaben, die auf andere Weise bekannt geworden waren.

Ein Verein organisiert jährlich Sportveranstaltungen, für die auch – ganz zeitgemäß – eine Online-Anmeldung möglich ist. Die Meldelisten, die Name, Vorname, Geschlecht, Geburtsjahr, Wohnort und Verein beinhalten, sollten ebenfalls online gestellt werden.
In beiden Angelegenheiten wurde die Aufsichtsbehörde um Mitteilung gebeten, welche datenschutzrechtlichen Vorgaben zu beachten seien. In den beispielhaft genannten Fällen kommt es zu einer Übermittlung personenbezogener Daten, die nur erfolgen darf, wenn sie nach den Regeln des Datenschutzes zulässig ist.

Den anfragenden Stellen wurden daraufhin zunächst die möglichen Rechtsgrundlagen dargestellt. In beiden Sachverhalten könne die Zulässigkeit der beabsichtigten Datenübermittlung aus einer Einwilligung der Betroffenen i. S. d. § 4a BDSG resultieren, aber auch aus dem Bundesdatenschutzgesetz selbst (§ 28 Abs. 1 S. 1 Nr. 2 BDSG).

Der akademischen Organisation wurde weiterhin mitgeteilt, dass eine Befugnis oder Verpflichtung zur Veröffentlichung von Daten in Printmedien keineswegs pauschal zu einer Einstellung dieser Daten im Internet berechtige. Im Gegensatz zur Veröffentlichung der Daten in gedruckten Publikationen, die naturgemäß einem begrenzten, interessierten Kreis zugänglich sind, werden die Daten mit der Einstellung ins Internet global von jedermann abrufbar. Zudem könnten die Daten mit weiteren im WWW vorhandenen Daten zu Persönlichkeitsprofilen zusammengeführt werden.

Dem Sportverein wurden Bedenken hinsichtlich einzelner Daten, z. B. Angaben über den Wohnort einer für eine Sportveranstaltung angemeldete Person, mitgeteilt.

Die Aufsichtsbehörde konnte im Ergebnis allein richtungweisende Hinweise geben. Denn abschließende Zulässigkeitsprüfungen sind allein auf konkrete Einzelfälle bezogen durchzuführen und obliegen daher zunächst der verantwortlichen Stelle in Eigenverantwortung.

Dass bei der Thematik **Bewertungsportale** viele unterschiedliche Meinungen zusammentreffen, stellte die Aufsichtsbehörde nicht erst fest, als ihr Ende des Jahres 2007 mitgeteilt wurde, dass ein Unternehmen seit kurzem in Sachsen-Anhalt ein sog. Ärztebewertungsportal betreibt. Soweit die Aufsichtsbehörde dies aus dem Internetauftritt des Unternehmens beurteilen konnte, kommt es seitens der „Einmelder“ zu einer Erhebung und Speicherung personenbezogener Daten (siehe Begriffserläuterungen).

Begriffserläuterungen:
Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Zu ihnen gehören nicht nur „klassische“ Daten, wie Name, Vorname, Adresse, Geburtsdatum und Personenstand, sondern alle Informationen, die mit einer Bezugsperson in Verbindung zu bringen sind. Somit sind auch Meinungsäußerungen, Beurteilungen und Werturteile, die sich auf einen bestimmten oder bestimmbaren Betroffenen beziehen, die Wiedergabe von mündlichen und schriftlichen Aussagen eines Betroffenen u. v. m. erfasst.

Die Veröffentlichung der Meinung einer Privatperson zu einer anderen Person im Internet ist grundsätzlich nicht mehr als ausschließlich persönliche oder familiäre Tätigkeit anzusehen und eröffnet daher den Anwendungsbereich des Bundesdatenschutzgesetzes. Die Veröffentlichung der personenbezogenen Daten im Internet stellt auch im Rahmen eines Bewertungsportals eine Datenübermittlung dar, die nach § 4 Abs. 1 BDSG zulässig sein muss. Da die Bewerteten typischerweise keine Einwilligung in diese Datenübermittlung erteilt haben und keine andere Rechtsvorschrift die Datenübermittlung erlaubt oder gar anordnet, konnte sich die Zulässigkeit der Datenübermittlung im Rahmen eines Bewertungsportals allein aus den Erlaubnisnormen der §§ 28 ff. BDSG ergeben.

Die Aufsichtsbehörde teilte dem Unternehmen mit, dass bei Beurteilung einer Plattform im Internet, in die Daten von Betroffenen eingemeldet und daraus abgerufen werden können, sowohl beim geschäftsmäßigen Erheben und Speichern (§ 29 Abs. 1 BDSG) als auch bei der Übermittlung der Daten (§ 29 Abs. 2 BDSG) kein Grund zu der Annahme bestehen darf, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss dieser Vorgänge hat. Der Begriff des schutzwürdigen Interesses sei dabei sowohl im Lichte des Grundrechtes der Meinungsfreiheit als auch des Grundrechts der informationellen Selbstbestimmung auszulegen. Keines der in die Auslegung einzubeziehenden Grundrechte sei generell als nachrangig einzustufen. Der Abwägungsprozess könne jedoch nur einzelfallbezogen vorgenommen werden. Dem Plattformbetreiber wurde mitgeteilt:

- Bei Bewertungskriterien, die sich auf Wartezeit, Wartezimmer und Terminvergabe beziehen und die mit einer Punktevergabe verbunden sind, werden die Gefahren eines überwiegenden schutzwürdigen Interesses der Betroffenen für verhältnismäßig gering erachtet.
- Die Angaben zu „Freundlichkeit Arzt und Mitarbeiter“ und zur Ausstattung werden kaum objektiv zu beurteilen sein, erscheinen aber legitim.
- Kritisch ist die Möglichkeit von Freitexteingaben zu sehen, da hier die Gefahr des Missbrauchs besonders hoch ist. Hier müssen Schutzmechanismen maßgeblich ansetzen. In jedem Fall sind die Nutzer in den Nutzerbedingungen der Plattform über

die erlaubten Inhalte zu belehren, damit der Betreiber der Plattform die Möglichkeit hat, bestimmte Schmähkritik zu löschen, ohne sich des Vorwurfs der Zensur auszusetzen. Außerdem sollte eine Missbrauchsmeldemöglichkeit vorgesehen werden. Empfehlenswert ist auch der Einsatz einer Filtersoftware, die von vornherein bestimmte Begriffe mit beleidigenden Inhalten erkennt.

- Es muss gewährleistet sein, dem Beurteilten Kenntnis über die Veröffentlichung personenbezogener Daten zu ermöglichen und unrichtige Daten zu bestreiten.
- Es müssen Löschfristen definiert werden, damit die Aktualität der Daten gewährleistet werden kann.

Nachfolgend wurde umfassend zu den vorstehenden Belangen ausgeführt. Das Unternehmen hat sich weitgehend den Forderungen der Aufsichtsbehörde angeschlossen und deren Anregungen umgesetzt. Das Projekt befindet sich noch in der Markteinführungsphase und wird weiter datenschutzrechtlich begleitet.

4.2 Was ist zulässig und was nicht – ausgewählte Beschwerdeverfahren

4.2.1 Überwachung von Beschäftigten

„ Nicht nur Lidl spioniert Angestellte aus
– Ikea und Burger King ebenfalls im Verdacht“

Fernsehberichten zufolge sollen auch das Möbelhaus und die Fast-Food-Kette Mitarbeiter heimlich gefilmt haben…

Quelle: Spiegel Online

Bereits diese Berichterstattung verdeutlicht ein wesentliches Tätigkeitsfeld der Aufsichtsbehörde im Berichtsjahr 2008.

Die Daten von Arbeitnehmern sind regelmäßig nicht über spezielle Gesetze geschützt. Vielmehr unterfallen sie, wie auch andere personenbezogene Daten, den Regelungen des Bundesdatenschutzgesetzes. Dies bedeutet, dass ihre Erhebung, Verarbeitung und Nutzung nur zulässig ist, wenn der Arbeitnehmer in die einzelnen Verarbeitungsschritte einwilligt, eine andere Rechtsvorschrift als das Bundesdatenschutzgesetz diese erlaubt oder anordnet oder wenn sie aufgrund des Bundesdatenschutzgesetzes zulässig sind (§ 4 Abs. 1 BSDG). An vielen Stellen ist eine unzulässige Datenerhebung bereits ursächlich für eine unzulässige Nutzung der Daten. In den nachfolgenden Ausführungen steht daher die Zulässigkeit etwaiger Datenerhebungen im Vordergrund.

Die Überwachung von Arbeitnehmern führt zu einer Erhebung von Arbeitnehmerdaten. Arbeitgeber sind aus unterschiedlichsten Gründen geneigt, 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 Überwachung, die jede Regung und Bewegung der Mitarbeiter dokumentiert, nicht mit der Menschenwürde vereinbar ist. Allerdings kann es in Ausnahmefällen zulässig sein, Videoüberwachung vorzunehmen, insbesondere wenn ein hinreichend konkreter Verdacht auf heimlich begangene strafbare Handlungen besteht, der nicht oder nur schwer mit anderen, das Persönlichkeitsrecht des Überwachten wahrenden Mitteln, geklärt werden kann. Die **gezielte dauerhafte Überwachung** von Arbeitnehmern ist grundsätzlich nicht zulässig.

Daher wurden durch die Aufsichtsbehörde sämtliche Sachverhalte geprüft, in denen der Verdacht unzulässiger Überwachung von Arbeitnehmern bestand. Die Überprüfung erfolgt stets ähnlich, soll jedoch insbesondere am Beispiel eines Discounters dargestellt werden, der durch seine im März 2008 presseöffentlich bekannt gewordenen Methoden für einen Sturm der Entrüstung sorgte. Es wurde berichtet, dass ein Detektiv Berichte über seine Tätigkeit für einen deutschen Lebensmitteldiscounter an die Presse weitergegeben hat. Dabei wurde ersichtlich, dass die Mitarbeiter offensichtlich systematisch überwacht wurden.
Wie in allen ähnlichen Fällen wurde auch dieses der Arbeitnehmerüberwachung verdächtigte Unternehmen um Stellungnahme insbesondere zu folgenden Punkten gebeten:

- Darstellung von Verantwortungs- und Entscheidungsbereichen insbesondere hinsichtlich des Einsatzes von Überwachungsmaßnahmen unter Nennung der verantwortlichen Personen.
- Einsatzort der Videoüberwachungseinrichtungen (Beschreibung und Kennzeichnung in einem Grundriss).
- Vorliegen eines Videoüberwachungskonzepts.
- Mitwirkung des betrieblichen Datenschutzbeauftragten bei der Einrichtung der Videoüberwachung, Durchführung einer Vorabkontrolle und ggf. Einbeziehung des Betriebsrates.
- Benennung der Verantwortlichen, die die ggf. gefertigten Aufzeichnungen aus den Videoüberwachungseinrichtungen prüfen.
- Mitteilung, ob Dritte, z. B. Detektive, beauftragt wurden und ggf. zu welchem Zweck.
- Regelungen zur Löschung gespeicherter Daten.

Die umfassenden Ermittlungen der Aufsichtsbehörde ergaben, dass im Rahmen sogenannter Ladendiebstahlskontrollen Detektive jeweils für den Zeitraum von ca. einer Woche eingesetzt wurden. Den Mitarbeitern des Discounters ist der Einsatz der Detektive, ggf. unter Nut-

zung von Kameras bekannt gewesen. Was die Mitarbeiter jedoch nicht wussten, ist, dass der Einsatz der Detektive nicht allein dazu diente, Ladendiebe zu fassen, sondern auch die einzelnen Mitarbeiter beobachtet wurden, um Inventurdifferenzen aufzuklären. Die Detektive führten akribisch Protokoll darüber, was ihrer Ansicht nach „verdächtig“ war. Vorgaben hierfür gab es vom Unternehmen nicht. Es wurden Verhaltensweisen der einzelnen Mitarbeiter festgehalten, Informationen aufgezeichnet, die man aus eigenen Gesprächen mit den Mitarbeitern – auch über deren Privatleben – erhalten hatte, es wurden die Gespräche der Mitarbeiter untereinander belauscht und die Inhalte protokolliert.
Folgender Protokollinhalt – auszugsweise – wurde gerügt:

- „Frau H. hielt sich mit Sohn im Aufenthaltsraum auf“
- „Frau K. ist im 6. Monat schwanger“
- „Frau P. führt mit Mitarbeiter der Bausparkasse BHW im Aufenthaltsraum ein Gespräch, Vertrag über vermögenswirksame Leistungen geschlossen“
- „Frau P. und Herr H. scheinen sich gut zu verstehen und Frau P. wird etwas kindlich, wenn sie mit Herrn H. spricht“
- „Frau P. lästert im Pausenraum über Fr. P., deren stetigen Partybesuch, Alkoholkonsum und die Betreuung ihrer Kinder durch die Oma“
- „Frau H. raucht und murmelt „Wenn die nicht bald aufhört, haue ich dazwischen““
- „Frau G. tätigt während Pause Privateinkauf“
- „Frau G. tätigt vor Arbeitsbeginn Privateinkauf“
- „Herr O. im Markt und raucht nach Erkundigung noch eine mit Frau G.“
- „Frau H. geht in Feierabend und hat Rest der Woche frei“
- Frau M. S. fährt einen „Porsche Boxter“ (neues Modell)

Im Ergebnis ahndete die Aufsichtsbehörde, dass entgegen der gesetzlichen Bestimmungen kein Beauftragter für den Datenschutz bestellt war und es in 15 Fällen zu unzulässigen Datenerhebungen gekommen war. 11 der von einem Detektiv gefertigten Revisionsberichte wurden als erheblicher Verstoß kategorisiert, da die Berichte maßgeblich unbefugte subjektive Einschätzungen zu Mitarbeitern enthielten. In zwei Revisionsberichten wurden konkrete Verdachtsmomente oder dem Arbeitgeber unbekannte Angaben über den Gesundheitszustand von Mitarbeitern geschildert. In zwei weiteren Fällen wurden gravierende Verstöße festgestellt. Zum einen ging es um Äußerungen zum oder aus dem privaten Bereich, die das Persönlichkeitsrecht der Mitarbeiter verletzten. Wegen der festgestellten Verstöße wurde ein Bußgeld in sechsstelliger Höhe verhängt, und von dem Unternehmen auch gezahlt.

In anderen geprüften Bereichen konnte in Sachsen-Anhalt - entgegen der Berichterstattung in den Medien - nicht festgestellt werden, dass eine vorgenommene Videoüberwachung im Allgemeinen unzulässig erfolgte bzw. ein unverhältnismäßiger Überwachungsdruck

vorlag. Dieser entsteht insbesondere, wenn sich Mitarbeiter dem Erfassungsbereich einer Kamera nicht oder nicht ausreichend entziehen können. Es gab aber auch Einzelfälle, in denen die Aufsichtsbehörde zwar den Einsatz von Videoüberwachung grundsätzlich als notwendig anerkannte. Im Rahmen ihrer Untersuchungen zur Notwendigkeit der einzelnen angebrachten Einrichtungen wurden allerdings Änderungen angeordnet, beispielsweise hinsichtlich der Beobachtungszeit, des Erfassungsbereiches, der Zugriffsberechtigung auf aufgezeichnete Daten, der Dokumentation der Veränderung von Kameraausrichtungen etc..

Die Aufsichtsbehörde hat im 3. Tätigkeitsbericht eine **Checkliste für Verantwortliche und Datenschutzbeauftragte für den Einsatz optisch-elektronischer Einrichtungen (Videoüberwachung)** veröffentlicht. Dieser Tätigkeitsbericht ist vollständig abrufbar: @ http://www.sachsen-anhalt.de/LPSA/fileadmin/Elementbibliothek/LVwA-Bibliothek/Zentraler_Service/Referat_106_-_Justizariat/Dokumente/3_DS_Bericht_LVwA_08.pdf

4.2.2 Videoüberwachung von Wohnanlagen

Die Aufsichtsbehörde ermittelte auch in einem Fall, der die Videoüberwachung einer Wohnanlage betraf. Ein Mieter trug vor, dass er über Dritte erfahren habe, dass eine Videoüberwachungsanlage im Hausflur des Wohnobjektes, in dem auch ein Hostel angesiedelt ist, installiert werden soll. Dies sei ihm auch vom Vermieter bestätigt worden. Die Einwände des Mieters habe der Vermieter mit der Begründung zurückgewiesen, dass ein Mieter insoweit kein Mitspracherecht habe. Die Videoüberwachung sei notwendig, weil beim Betrieb eines Hostels häufiger Sachen „abhanden kommen“ würden.

Die Aufsichtsbehörde teilte dem Vermieter mit, dass bei einer Beobachtung eines Gebäudes, in dem sich ein Hostel befindet, von einer Beobachtung öffentlich zugänglicher Räume (siehe Begriffsbestimmungen) auszugehen ist, deren Zulässigkeit sich nach § 6b BDSG richte.

Begriffsbestimmungen:

Unter *öffentlich zugänglichen Räumen* sind Flächen zu verstehen, die ihrem Zweck nach dazu bestimmt sind, von einer unbestimmten Zahl oder nach nur allgemeinen Merkmalen bestimmten Personen betreten und genutzt zu werden. Öffentlich zugängliche Räume sind beispielhaft die Ausstellungsräume eines Museums, Schalterhallen, Tankstellen, Cafés, Parkhäuser u. v. m.. Maßgeblich für den Begriff des Raumes, wie er in § 6 b des Bundesdatenschutzgesetzes genutzt wird, ist, dass der Betroffene nur über begrenzte Möglichkeiten verfügt, der Videoüberwachung auszuweichen. Unter diesem Gesichtspunkt können „Räume“ auch außerhalb von Gebäuden liegen, wenn sie umgrenzt sind.

Bereits vor der Installation optisch elektronischer Einrichtungen muss festgestellt werden, dass die Beobachtung gemäß § 6b BDSG zulässig ist. Diese Vorschrift kommt auch bei reinen Kamera-Monitor-Systemen 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.

Zunächst gilt es den Zweck des Videoeinsatzes zu ermitteln und zu prüfen, ob die jeweilige beabsichtigte Videoüberwachung zur Erreichung des angegebenen Zieles erforderlich ist. Bedeutsam ist dabei, ob es andere, die Videoüberwachung vermeidende Mittel gibt, z. B. den Einsatz von Wachpersonal, der Einbau von Sicherheitssystemen etc. Es genügt nicht, von vornherein auf die Videoüberwachung zu setzen, ohne Alternativen geprüft zu haben. Von einer Erforderlichkeit der jeweiligen Videoüberwachung (dabei sind Anzahl der Kameras, Ausrichtung und technische Aspekte zu berücksichtigen) ist nur dann auszugehen, wenn ohne den Technikeinsatz das Ziel der Überwachung nicht mehr erreichbar wäre.

Konfrontiert mit den im Rahmen der Videoüberwachung zu beachtenden Vorgaben legte der Vermieter in seiner Stellungnahme dar, dass keinerlei konkrete Absicht bestehe, eine Videoüberwachung im Eingangsbereich durchzuführen. Sofern jedoch zu einem späteren Zeitpunkt eine Notwendigkeit bestehe, werde man die Hinweise der Aufsichtsbehörde berücksichtigen. Dem potentiell betroffenen Mieter konnte im Ergebnis allein angeboten werden, sich bei weiteren Erkenntnissen erneut an die Aufsichtsbehörde zu wenden.

BEACHTEN SIE:

Die Videoüberwachung berührt unmittelbar das allgemeine Persönlichkeitsrecht jedes Menschen, der sich in den Überwachungsbereich der Videokameras begibt. Stets ist eine Abwägung zwischen dem Persönlichkeitsrecht der von der Überwachung Betroffenen bzw. deren Recht am eigenen Bild und den Interessen der Stelle, die die Videoüberwachung nutzen möchte, zu treffen. Diese Abwägung fällt je nach Einzelfall unterschiedlich aus. In der Rechtsprechung gibt es Urteile, die dem Persönlichkeitsrecht der „Überwachten“ den Vorrang vor den Interessen des „Überwachenden“ geben (z. B. Landgericht Bonn, Urteil vom 16. November 2004 (NZM 2005, S. 399)). Andere Gerichte geben dem Schutzrecht des Überwachenden den Vorrang (z. B. Landgericht Koblenz, Urteil vom 22. März 2005 (NJW-RR 2006, S. 1200)).

Grundsätzlich sind Aufnahmen in Mietshäusern (z. B. im Treppenhaus) nur **im Ausnahmefall** erlaubt. Eine vom Mieter installierte Videoanlage darf in einem zulässigen Ausnahme-

fall nur den Bereich der eigenen Wohnungstür erfassen. Dies ist durch entsprechende Maßnahmen sicher zu stellen. Die Beobachtung von fremden Wohnungs- oder Haustüren ist unzulässig.

Vor dem Hintergrund bereits ergangener Rechtsprechung und der Regelung des § 6b BDSG sind beim Betrieb einer Videoüberwachungsanlage (mit Aufzeichnungsmöglichkeit) folgende Kriterien zu beachten:

- Hinweis auf die Videoüberwachungsanlage mit deutlichem Hinweis auf die verantwortliche Stelle,
- Beschreibung von Umfang und Zweck der Überwachung,
- Festlegung des zulässigen Gebrauchs,
- Maximale Speicherkapazität bzw. Aufbewahrungszeit von Aufzeichnungen (bis 52 Stunden),
- Automatisches Überschreiben der aufgezeichneten Bilddaten nach maximal 52 Stunden,
- Zulässigkeit und Verfahren der Anfertigung und Auswertung von Aufzeichnungen,
- Regelung der Löschung von Aufzeichnungen,
- Bestimmung eines Mitarbeiterkreises bei der verantwortlichen Stelle, der zur Kontrolle des Videosystems zugelassen ist,
- Festlegung eines Verfahrens im Falle einer Auswertung durch die Polizei.

4.2.3 Erhebung personenbezogener Daten

Ein Behindertenverein wandte sich an die Aufsichtsbehörde, nachdem er im Rahmen seiner Beratungstätigkeit von einem Bürger eine „Betriebliche Regelung für Arbeitnehmer“ eines Unternehmens erhalten hatte. Danach nehme das Unternehmen Lohnfortzahlungen nur vor, wenn

1. der Krankenschein abgegeben wird,
2. eine Kopie des Teils des Krankenscheins eingereicht wird, der für die Krankenkasse bestimmt ist und
3. ein vom Arzt auszufüllendes Formblatt vorgelegt wird.

Der Behindertenverein bat um Mitteilung, ob diese Vorgehensweise des Betriebes korrekt sei und um Hinweise zu Handlungsmöglichkeiten des Betroffenen.

Die Aufsichtsbehörde wies darauf hin, dass sich aus der „Betrieblichen Regelung für Arbeitnehmer“ ergebe, dass das Unternehmen mit den Forderungen nach Nummer 2 und 3 bestimmte Daten erheben möchte, ohne hierzu gesetzlich befugt zu sein.

Das Unternehmen setzte daraufhin die betrieblichen Regelungen sofort außer Kraft und erklärte, dass Unterlagen auf Grundlage der Regelung bislang nicht eingereicht worden seien. Der Behindertenverein wurde anschließend über das Ergebnis der Tätigkeit der Aufsichtsbehörde unterrichtet. Da die Verfahrensweise sofort geändert wurde und keine konkreten Einzelverstöße festgestellt wurden, war die Angelegenheit abgeschlossen.

Auch wandte sich ein Betroffener an die Aufsichtsbehörde und teilte mit, dass von seinem Konto Geld abgebucht wurde. Er ermittelte zunächst selbst, dass ein Behindertenverein die Lastschrift vorgenommen hatte. Der Betroffene ließ sich das Geld zurückbuchen, bat jedoch um Klärung, woher der Verein seinen Namen und seine Kontodaten hatte.

Die Aufsichtsbehörde bezog in die Ermittlungen neben dem Verein auch die am Lastschriftverfahren beteiligten Banken ein. Im Ergebnis konnte nicht festgestellt werden, dass der Behindertenverein die personenbezogenen Daten des Betroffenen unzulässig erhoben, gespeichert und genutzt hat. Es wurde festgestellt, dass ein Fördermitglied die Kontodaten des Betroffenen in das entsprechende Aufnahmeformular eingetragen und den Verein bis auf Widerruf ermächtigt hat, einen vereinbarten Betrag abzubuchen. Ein routinemäßiger Abgleich, ob der bekannte Kontoinhaber und die Bankverbindung übereinstimmen, erfolgt zwar grundsätzlich bei der kontoführenden Bank des Betroffenen. Bei Kleinbeträgen ist ein solcher Abgleich jedoch in der Regel bei Banken nicht vorgesehen, da die Möglichkeit der Rückbuchung besteht.

4.2.4 Speicherung/Aufbewahrung personenbezogener Daten

Jeder Arzt und jedes Krankenhaus hat als zivilrechtliche Nebenpflicht zum Behandlungs-/Krankenhausaufnahmevertrag Dokumentationspflichten. Auch die standesrechtlichen Regelungen - Berufsordnungen - geben Dokumentations- und Aufbewahrungspflichten auf. Über die in Ausübung des Berufes gemachten Feststellungen und getroffenen Maßnahmen sind die erforderlichen Aufzeichnungen zu fertigen. Sie dienen als Gedächtnisstütze für den Arzt und dem Interesse des Patienten an einer ordnungsgemäßen Dokumentation. Ärztliche Aufzeichnungen sind nach der Berufsordnung für die Dauer von 10 Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach gesetzlichen Vorschriften eine längere Aufbewahrungsfrist besteht (z. B. lt. Röntgenvorordnung: 30 Jahre nach der letzten Behandlung bei Aufzeichnungen über Röntgenbehandlung). Mit der Aufbewahrung von Patientenunterlagen geht die **Speicherung** personenbezogener Daten einher. Dabei stehen der zur Aufbewahrung verantwortlichen Stelle verschiedene Möglichkeiten zur Aufbewahrung von Unterlagen zur Verfügung, darunter ggf. auch die Aufbewahrung in angemieteten Räumen.

Die Ärztekammer Sachsen-Anhalt gab der Aufsichtsbehörde den Hinweis, dass die Aufbewahrung von Patientenunterlagen einer ehemaligen Arztpraxis in den Räumlichkeiten eines Umzugsunternehmens nicht den datenschutzrechtlichen Bestimmungen entspreche.

Die Aufsichtsbehörde ermittelte, dass u. a. sechs Kartons mit Patientenakten in den Büroräumen des Umzugsunternehmens aufbewahrt wurden. Zugang zu den Unterlagen hatten dabei der Geschäftsführer und seine kaufmännische Angestellte.

Das Umzugsunternehmen hatte die Patientendaten weder auf Basis von Einwilligungen aller Patienten noch einer spezialgesetzlichen Ermächtigungsgrundlage oder dem Bundesdatenschutzgesetz selbst – § 28 Abs. 6 BDSG – zulässig gespeichert. Daher wurde das Unternehmen gebeten, die Unterlagen an die Aufsichtsbehörde zur Weiterleitung an die Ärztekammer oder dieser direkt zu übergeben. Dies erfolgte nachfolgend ordnungsgemäß.

4.2.5 Übermittlung personenbezogener Daten

„Dokumente liegen auf der Straße“ Ermittlungen wegen Verletzung des Datenschutzes eingeleitet Quelle: MZ	Die Aufsichtsbehörde ermittelte hinsichtlich des Vorfalles. Das Unternehmen legte dar, dass personenbezogene Daten streng vertraulich behandelt und die ordnungsgemäße Entsorgung von Unterlagen grundsätzlich fachgerecht organisiert sei. Der bekannt gewordene Sachverhalt sei darauf zurückzuführen, dass innerhalb des Unternehmens Müllsäcke mit personenbezogenen Unterlagen für die Entsorgung durch einen Aktenvernichterdienst bereit gestellt worden seien. Die Säcke seien jedoch versehentlich zu den „normalen“ Mülltonnen gestellt worden. Die unruhige Wetterlage habe sodann die Öffnung der Müllsäcke bewirkt, so dass einige Dokumente auf die Straße geweht wurden. Der Vorfall wurde bedauert. Die Aufsichtsbehörde führte hinsichtlich des Einzelfalles ein Ordnungswidrigkeitenverfahren wegen unzulässiger Datenübermittlung durch. Dies wurde abgeschlossen.

Weiterhin ist ein Sachverhalt aufzuzeigen, in dem die Mitarbeiter eines Unternehmens einen mit Name, Anschrift, Geschlecht, Geburtsdaten, Arbeitgeber vorausgefüllten Antrag „Aufnahme zur Krankenversicherung“ einer Krankenversicherung und ein vorgefertigtes Schreiben zur Kündigung der Mitgliedschaft in der bisherigen Krankenversicherung durch ein Schreiben vom eigenen Arbeitgeber erhielten.

Die Ermittlungen der Aufsichtsbehörde bestätigten den Verdacht der Betroffenen, dass es zu einer Übermittlung der Daten an die „neue“ Krankenversicherung gekommen ist. Das Unternehmen sorgte eigenständig dafür, dass die übermittelten Daten bei der Krankenversicherung gelöscht werden und entschuldigte sich bei den Mitarbeitern für „den möglichen Datenschutzverstoß“ von dem man im Vorfeld jedoch nicht ausgegangen sei. Die Aufsichtsbehörde stellt im Ergebnis der Ermittlungen eine unzulässige Datenübermittlung fest und ahndete dies im Rahmen eines Ordnungswidrigkeitenverfahrens. Der Bescheid ist bestandskräftig.

Schließlich ist ein Fall darzustellen, bei dem sich ein Mitglied eines Vereines an die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich wandte, da ein anderes Vereinsmitglied in einer Vorstandssitzung Informationen über seine Person, u. a. über eine Betreuung bzw. ein Verbraucherinsolvenzverfahren vorgelesen habe.
Die Aufsichtsbehörde ermittelte, dass die Daten nicht von dem benannten Verein erhoben wurden. Das andere Vereinsmitglied wies nach, dass es die in Rede stehenden Daten mittels eines anonymen Schreibens erhalten hat.
Im Ergebnis wurde daher keine Datenerhebung im Sinne des Bundesdatenschutzgesetzes festgestellt. Das Vorlesen des anonymisiert an das Vereinsmitglied gerichteten Schreibens in der Vorstandssitzung stellt auch kein Übermitteln i. S. d. BDSG dar, da das Bundesdatenschutzgesetz nur dann anzuwenden ist, wenn Daten unter Einsatz von Datenverarbeitungsanlagen oder aus nicht automatisierten Dateien verarbeitet wurden (§ 1 Abs. 2 Nr. 3 BDSG). Der Zweck des Vorlesens, d. h. ob dies erfolgte, um das betroffene Vereinsmitglied zu diskreditieren oder ob im Vorstand erörtert werden sollte, ob aus den Angaben Konsequenzen zu ziehen sind, war daher datenschutzrechtlich nicht von Belang.

4.2.6 Nutzung personenbezogener Daten für Zwecke der Werbung

Ein mit kostenlosen Zeitungen und Prospekten gefüllter Briefkasten ist vielen Haushalten bekannt. Flyer, Prospekte, „an alle Haushalte“ adressierte Schreiben sind schnell entsorgt, auch deren Einwurf kann in der Regel durch einen Aufkleber am Briefkasten mit der Aufschrift „Bitte keine Werbung“ verhindert werden. Gleiches gilt allerdings nicht für adressierte Schreiben, hinter denen zunächst etwas Wichtiges, Persönliches vermutet wird. Umso größer ist die Verärgerung, wenn man die Briefe öffnet und Werbung für Kredite, Arzneimittel oder sonstige Dinge offenbar wird. Daneben stellt sich der Empfänger eines adressierten Werbeschreibens häufig die Frage, woher die Absender die genutzte Anschrift bezogen haben, wenn man noch nie Kontakt mit dem werbenden Unternehmen hatte.

Die Wege für den Bezug von Adressdaten sind verschieden. 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 auf Adressbestände von 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. Manche Unternehmen erhalten die Werbebotschaft vom werbenden Unternehmen und versenden die Schreiben selbst indem sie jeweils die Anschriften ergänzen (sog. Lettershop-Verfahren). In derartigen Fällen ist es möglich, dass das werbende Unternehmen noch gar keine personenbezogenen Daten von dem von der Werbung Betroffenen erhält. Diese erhält das Unternehmen erst, wenn jemand auf die Werbung regiert.

Die Zulässigkeit der Übermittlung und Nutzung der typischerweise im Werbebereich genutzten personenbezogenen Daten (Zugehörigkeit zu einer Personengruppe, Berufs-, Branchen- oder Geschäftsbezeichnung, **Name**, Titel, akademischer Grad, **Anschrift** und Geburtsjahr) richtete sich bis zur Novellierung des Bundesdatenschutzgesetzes typischerweise nach § 28 Abs. 3 Nr. 3 BDSG.

Sollte die werbende Stelle Zweifel haben, dass schutzwürdige Interessen der Betroffenen ihren Belangen überwiegen könnten, hat sie die Nutzung der Daten zu unterlassen. Da die beworbenen Personen im Vorfeld allerdings nicht bekannt sind, besteht zunächst kein Grund zu einer entsprechenden Annahme. Ein pauschales Überwiegen der Betroffeneninteressen wollte der Gesetzgeber somit nicht. Er erleichterte die Nutzung der aufgeliste-

***§ 28 BDSG – Datenerhebung, -verarbeitung und –nutzung für eigene Zwecke* (Auszug)**

Abs. 3: *Die Übermittlung oder Nutzung für einen anderen Zweck ist auch zulässig:*

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

ten Daten in gewissem Maß, legte den verantwortlichen Stellen allerdings Folgepflichten auf. Über § 28 Abs. 4 BDSG wurde dem Betroffenen die Möglichkeit eingeräumt, jederzeit der Nutzung u. a. für Werbezwecke zu widersprechen. Die verantwortlichen Stellen haben hierüber zu unterrichten. 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 das Widerspruchsrecht zur Kenntnis zu nehmen.

f) Anschrift und

g) Geburtsjahr

beschränken

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

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

Nach erfolgtem Widerspruch dürfen die Daten nicht mehr zu den genannten Zwecken verwendet werden. Allerdings ist das speichernde Unternehmen nicht verpflichtet, den Datensatz zu löschen. Häufig führen die werbenden Unternehmen eine interne Sperrliste, in der sie die Datensätze incl. Widerspruch aufnehmen, um die Beachtung des Widerspruches gewährleisten zu können.

Formulierung Ihres Werbewiderspruchs

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

Sie können auch 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 Verbraucherband gegen das Verteiler- bzw. Werbeunternehmen rechtlich vorgehen.

Um sich vor adressierten Werbezuschriften zu schützen, bietet der private Deutsche Direkt-Marketing-Verband (DDV) Verbraucher/Innen an, sich in die sogenannte Robinsonliste eintragen zu lassen. Ein Formular für die Aufnahme in die Robinsonliste erhalten Sie bei DVV Robinsonliste, Postfach 1401, 71243 Ditzingen oder online auf der Verbraucherwebsite www.ichhabediewahl.de. 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 Robinsonliste.

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 den Brief unfrankiert in die Post. Gewissenhafte Unternehmen werden nachfolgend Ihre Anschrift auf ihre interne „Sperrliste“ setzen.

Die Aufsichtsbehörde hat auch im vergangenen Berichtszeitraum zahlreiche Sachverhalte im Zusammenhang mit unerwünschter Werbung überprüft.

In einem Fall erhielt ein Einzelunternehmer immer wieder per Telefax Werbung von einem Personalserviceunternehmen.

Neben der Belästigung durch die Werbesendung wird ein Faxbesitzer damit konfrontiert, dass er zu jeder Tages- und Nachzeit gestört wird, weil das Faxgerät anspringt, aber auch, dass er für „unnütze“ Informationen sein eigenes Papier und den Toner einsetzen muss.

Im konkreten Fall bat der Unternehmer das werbende Untenehmen zunächst selbst um Auskunft zur Herkunft der genutzten Daten und widersprach der weiteren Nutzung seiner Daten für Zwecke der Werbung. Dennoch erhielt er ca. ein halbes Jahr später erneut Werbung per Telefax. Dies veranlasste ihn zur Eingabe bei der Aufsichtsbehörde.

Diese forderte das Personalserviceunternehmen unter Mitteilung der Sach- und Rechtslage auf, ausführlich zur Zulässigkeit der Datenerhebung und -speicherung, zur Datennutzung – insbesondere unter dem Aspekt des geäußerten Werbewiderspruchsrecht – und zur Erfüllung der Unterrichtungspflichten gem. § 28 Abs. 4 S. 2 BDSG Stellung zu nehmen.

Das werbende Unternehmen entschuldigte sich für die erneute Nutzung des Datensatzes. Dies sei dem Umstand geschuldet, dass die genutzten Adressdatensätze nicht gespeichert

seien, sondern stets aktuell aus dem Internet abgerufen würden. Zukünftig werde man jedoch interne Maßnahmen ergreifen, dass Personen, die der Nutzung ihrer Daten für Zwecke der Werbung widersprochen haben, keine mehr erhalten.

Der Petent wurde nach Auswertung des Sachverhaltes informiert, dass die spätere Datennutzung aufgrund der Äußerung des Widerspruchs unzulässig gewesen ist, zukünftig jedoch Maßnahmen ergriffen werden, um Verstöße gegen das BDSG im Zusammenhang mit Werbung zu verhindern.

Weiterführende Tipps zum Verhalten bei Werbefaxen:

- Beantworten Sie ein Werbefax niemals per Fax, denn die angegebenen Nummern sind in der Regel kostenpflichtig!
- Prüfen Sie, ob Sie Telefaxe von Mehrwertdienstenummern (0180, 0190, 0900 usw.) wirklich benötigen. Über Ihren Telefonanbieter besteht die Möglichkeit der Sperrung des Empfangs von Absendern, die diese Nummern verwenden. Der kostenpflichtige Dienst ist zu empfehlen, wenn die Zusendung von Werbefaxen überhand nimmt.
- Gehen Sie sparsam mit der Veröffentlichung Ihrer Faxnummer um.
- Sollten Sie Werbefaxe erhalten, schalten Sie nachts das Faxgerät ab.

In einem weiteren Fall informierte ein Arzt seine Patienten, dass die Praxis auch bestehen bleibe, wenn er sich erfolgreich um ein politisches Amt beworben habe. Hierfür bat er um Verständnis, aber auch um Unterstützung bei der Wahl.

Die Aufsichtsbehörde bat den Arzt um Stellungnahme. Dabei wurde erläutert, warum aus dem in Rede stehenden Schreiben eine Ansprache zum Zwecke der Werbung resultiert.

Der Arzt räumte Fehler bei der Behandlung seiner Patientendaten – insbesondere da eine Einwilligung zur Verwendung der Daten für die Wahlwerbung nicht vorlag – ein. Dennoch sei vordringliches Anliegen gewesen, die Patienten hinsichtlich der Gerüchte, dass die Praxis im Falle eines Wahlsieges schließe, über die weitere Sicherung der Versorgung zu informieren.

Dem Beschwerdeführer wurde mitgeteilt, dass die Nutzung der Patientendaten zum Zwecke der Werbung weder nach dem BDSG noch nach anderen Rechtsvorschriften erlaubt gewesen ist. Denn Patientendaten dürfen nur in dem Umfang genutzt werden, wie dies dem Behandlungsvertrag zwischen Arzt und Patient dient.

4.2.7 Löschung personenbezogener Daten

Neben der Berichtigung und Sperrung personenbezogener Daten zählt auch die Löschung (siehe Begriffserläuterung) zu den Rechten des Betroffenen. Diese Rechte ermöglichen dem Betroffenen, ggf. rechtswidrige Verarbeitungen personenbezogener Daten zu unterbinden und damit sein Recht auf informationelle Selbstbestimmung durchzusetzen.
Die Bedeutung dieser Rechte wird dadurch unterstrichen, dass diese nach § 6 Abs. 1 BDSG nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden können. Auch verursacht die Ausübung der Rechte für den Betroffenen keine Kosten.

Begriffserläuterungen:
Die *Löschung* personenbezogener Daten bedeutet die Unkenntlichmachung der bei einer verantwortlichen Stelle gespeicherten Daten.

Ein Betroffener erhielt im Oktober 2007 eine Werbesendung von einem Unternehmen, dessen Dienstleistungen er vor längerer Zeit (er gab an vor über vier Jahren) in Anspruch genommen hatte. Er habe daraufhin um die Löschung seiner Daten gebeten. Ihm sei jedoch folgendes mitgeteilt worden: „… Insofern ist aus steuerlichen Gründen eine vollständige Entfernung Ihrer Daten aus unserer Datenbank gesetzlich nicht möglich“. Der Petent bat um Überprüfung dieser Ablehnung bzw. darum, ggf. eine Löschung der Daten zu erwirken.

Prüfungsgegenstand war die Frage, ob das Unternehmen verpflichtet ist, die Daten zu löschen (§ 35 Abs. 2 und 3 BDSG).

***§ 35 BDSG – Berichtigung, Löschung und Sperrung von Daten* (Auszug)**

Abs. 2: *Personenbezogene Daten* ***können*** *außer in den Fällen des Absatzes 3 Nr. 1 und 2 jederzeit gelöscht werden. Sie* ***sind*** *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.

Abs. 3: *An die Stelle einer Löschung tritt eine Sperrung, soweit*

1. *im Fall des Absatzes 2 Nr. 3 einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,*
2. *Grund zu der Annahme besteht, das durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder*
3. *eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.*

Eine andauernde Datenspeicherung ist nämlich nur zulässig, wenn aus den genannten Vorschriften keine Verpflichtung zur Datenlöschung resultiert. Nach einer entsprechenden umfassenden Überprüfung teilte die Aufsichtsbehörde dem Petenten mit, dass kein Verstoß des Unternehmens gegen die Bestimmungen des Bundesdatenschutzgesetzes festgestellt werden konnte. Dies ist damit zu begründen, dass das Unternehmen seine Daten auch vier Jahre nach Abwicklung eines Auftrages nicht vollständig löschen kann. Dies folgt aus den Aufbewahrungspflichten des Handelsgesetzbuches (§ 257 HGB) und der Abgabenordnung (§ 147 AO) für die Daten: Kundenadresse, Auftragsdatum, bestellte Artikel, Lieferdatum und Datum des Ausgleichs des Kundenkontos. Es wurde erläutert, dass kein Verbot bestand, die Anschrift Jahre nach dem Auftrag für Zwecke der Werbung zu nutzen. Denn § 28 Abs. 3 Nr. 3 BDSG erlaubt die Nutzung von bestimmten Daten für Zwecke der Werbung so lange der Betroffene der Nutzung nicht widerspricht. Das Unternehmen wertete das geäußerte Löschungsbegehren - dem Sachverhalt angemessen - als Widerspruch gegen die Nutzung der Daten für Zwecke der Werbung und teilte mit, diesen zukünftig zu beachten.

Im Zusammenhang mit Verpflichtungen zur Löschung personenbezogener Daten ist auch auf den **Umgang mit Bewerbungen** nach Abschluss eines Bewerbungsverfahrens einzugehen. Auch im Berichtszeitraum hat die Aufsichtsbehörde Beschwerden bezüglich der Herausgabe von Bewerbungsunterlagen bzw. der Löschung der Daten erhalten.

Die Aufsichtsbehörde informierte die jeweils verantwortliche Stelle darüber, dass die im Rahmen eines Bewerbungsverfahrens erhobenen personenbezogenen Daten nach § 35 Abs. 2 Nr. 3 BDSG zu löschen sind, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Nur mit der Zustimmung der Bewerber dürfen Unterlagen für eine bestimmte, im Voraus festgelegte Dauer aufbewahrt werden, wenn anzunehmen ist, dass sie wieder gebraucht werden, z. B. für eine später zu besetzende Stelle. Grundsätzlich

wurden die Bewerbungsunterlagen nachfolgend zurückgeschickt oder im Unternehmen gelöscht und ein entsprechender Nachweis gegenüber der Aufsichtsbehörde erbracht.

In einem Fall teilte das Unternehmen mit, dass die Daten bereits von der verantwortlichen Person, die jedoch nicht mehr im Unternehmen sei, entsprechend der üblichen Regeln gelöscht worden seien. Ein anderweitiger Löschnachweis könne allerdings nicht erbracht werden. Zukünftig werde man allerdings die Bewerbungsanschreiben aufbewahren und die Löschung auf diesem Schreiben handschriftlich notieren und per Unterschrift bestätigen. Dies erachtet die Aufsichtsbehörde als adäquaten Löschnachweis.

4.2.8 Rechte der Betroffenen

Die Betroffenenrechte sind unter anderem in den §§ 34 und 35 BDSG geregelt. Während das Auskunftsrecht des § 34 BDSG die Betroffenen in die Lage versetzt, zu wissen, wer was aus welcher Gelegenheit über sie gespeichert hat, gibt die Vorschrift des § 35 BDSG – Berichtigung, Löschung und Sperrung von Daten – dem Betroffenen verschiedene Befugnisse, um „seine“ Daten in Einklang mit seinen berechtigten Interessen bringen zu können.

Ein Fall begann damit, dass ein Betroffener von einer ARGE SGB II die Nachricht erhielt, dass er bei einer Bank in einem Jahr Kapitalerträge in einer bestimmten Höhe hatte. Da dem Betroffenen nicht bekannt war, woraus diese Kapitalerträge resultieren, wandte er sich zunächst selbst an die Bank. Eine hinreichende Aufklärung ergab sich dabei jedoch nicht, so dass die Aufsichtsbehörde eingeschaltet wurde.

Die Ermittlungen der Aufsichtsbehörde ergaben, dass die zuständige Bank dem Betroffenen die Kapitalerträge fehlerhaft zugeordnet hatte. Diese teilte mit, dass der Datensatz nicht habe korrigiert werden können, da eine rückwirkende Änderung des zuordnungsrelevanten Freistellungsauftrages trotz späterer Kenntnis der Information nicht möglich gewesen sei.

Die Aufsichtsbehörde vertrat die Auffassung, dass ein Freistellungsauftrag die Anweisung eines Steuerpflichtigen an sein Kreditinstitut darstellt, anfallende Zinseinnahmen vom automatischen Steuerabzug freizustellen. Folglich sei nicht ersichtlich, warum dies eine nicht korrigierbare Zuordnung der vom Steuerabzug freigestellten Zinseinnahmen bzw. des zu Grunde liegenden Vermögens zu einer bestimmten Person, auslöst. Der Datensatz, der dem Betroffenen Kapitalerträge zuweist, sei unrichtig (siehe Begriffserläuterungen) gewesen.

Begriffsbestimmungen:
Unrichtig sind Daten, wenn die Information, welche einzelne Angaben über die persönlichen oder sachlichen Verhältnisse des Betroffenen vermittelt, nicht mit der Realität übereinstimmen. Unrichtig sind Daten auch, wenn die durch sie vermittelte Information unvollständig ist oder wenn durch Verwendung – für sich genommen richtiger – Daten durch Verwendung in einem anderen Zusammenhang ein falsches Gesamtbild entsteht.

Dem Betroffenen steht ein Berichtigungsanspruch nach § 35 Abs. 1 BDSG zu. Das Bundesdatenschutzgesetz gibt nicht vor, wie Daten zu berichtigen sind. Da es stets auf den Einzelfall ankommt, kann die gesetzliche Vorschrift insoweit keine Vorgaben treffen. Im vorliegenden Fall waren daher geeignete Maßnahmen zu treffen, um die beschriebene unrichtige Information über den Betroffenen zu korrigieren. Aus Sicht der Aufsichtsbehörde war hierzu keine Änderung des Freistellungsauftrages erforderlich. Auch eine Speicherung von Zusatzinformationen (d. h. zusätzlicher klärender Hinweise, wie z. B. Scheidung der Eheleute zum…, Kenntnis hiervon erst…, Zugriffsberechtigung für zu Grunde liegendes Vermögen obliegt …) kann zur Berichtigung der gespeicherten Daten führen. Die Aufsichtsbehörde forderte die Bank auf, die erforderlichen Berichtigungsmaßnahmen vorzunehmen und dies zu bestätigen. Es wurde darauf hingewiesen, dass an eine Berichtigung unrichtiger Daten weitere gesetzliche Verpflichtungen geknüpft sind. Nach § 35 Abs. 7 BDSG ist die verantwortliche Stelle dazu verpflichtet, die Stelle von der Berichtigung unrichtiger Daten zu verständigen, der im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben wurden, wenn dies keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen. Da ein einfaches Schreiben der Bank genügt, um der ARGE mitzuteilen, dass die mittels Datenabruf erhaltenen Daten unrichtige Informationen über den Betroffenen lieferten, war nicht ersichtlich, warum die Interessen der Bank höher zu bewerten waren als die des Betroffenen. Folglich wurde die Bank aufgefordert, die Benachrichtigung nach der Berichtigung der Daten umgehend nachzuholen.

Ein Petent wandte sich an die Aufsichtsbehörde, da er wissen wollte, woher ein Adresshändler seine Daten bezogen hat, die er nachweislich einem anderen Unternehmen zur Verfügung gestellt hatte. Ein gegenüber dem Unternehmen direkt geäußertes Auskunftsersuchen brachte keine Erkenntnisse zur Herkunft der Daten. Das Unternehmen benannte der Aufsichtsbehörde die Bezugsquelle des Datensatzes bestehend aus Name, Anschrift und Telefonnummer und teilte mit, dass man zukünftig im Rahmen von Auskunftsersuchen entsprechend § 34 Abs. 1 Nr. 1 BDSG auch die Herkunft der Daten bezeichnen werde. Die Herkunft der Daten bei dem angegebenen Unternehmen, das im Internet ein Telefonverzeichnis

anbietet, wurden überprüft. Es wurde bestätigt, dass der Datensatz des Betroffenen von diesem Unternehmen bezogen wurde.

In einem anderen Fall wunderte sich ein Betroffener, woher ein Anrufer seine Mobilfunknummer bezogen hatte. Er wandte sich zunächst an den Mobilfunkanbieter, da der Anrufer sich mit Nachname, Name vom „… Kundenservice“ gemeldet hatte und beschwerte sich über den unerbetenen Werbeanruf. Das Unternehmen belegte, dass der Anruf nicht vom Unternehmen erfolgte bzw. von diesem in Auftrag gegeben worden war. Die weiteren Ermittlungen des Betroffenen ergaben, dass ein Call-Center in Sachsen-Anhalt ihn angerufen hatte. Er machte diesem gegenüber seinen Auskunftsanspruch nach § 34 BDSG geltend. Das Call-Center informierte ihn jedoch lediglich darüber, dass der in Rede stehende Anruf versehentlich erfolgt sei, man habe keine Daten über ihn gespeichert, die Rufnummer sei aus dem System gelöscht, so dass weitere Auskünfte nicht möglich seien.

Die Aufsichtsbehörde bat das Unternehmen um Stellungnahme. Nach einem Erörterungstermin der Aufsichtsbehörde mit Vertretern des Unternehmens war festzustellen, dass das Call-Center von einem Distributor (Großhändler) beauftragt wurde, den Betroffenen als sog. Vertragsverlängerungskunden anzurufen. Das Call-Center speicherte im Zusammenhang mit der Telefonnummer (der Name des Kunden war nicht gespeichert) lediglich, wann Anrufversuche unternommen wurden, wann der Betroffene von wem erreicht wurde und dass kein Interesse an telefonischen Vertragsabschlüssen besteht. Die Aufsichtsbehörde beriet das Unternehmen in Bezug auf organisatorische Maßnahmen. Im Hinblick auf die Datenerhebung durch den Distributor wurde die Angelegenheit auf Bitte des Betroffenen an die zuständige Aufsichtsbehörde weitergeleitet.

4.2.9 Auskunfteien

Auch in der Berichtsperiode erhielt die Aufsichtsbehörde zahlreiche Anfragen und Eingaben, die die Verarbeitung personenbezogener Daten durch Handels- und Wirtschaftsauskunfteien betrafen. Thematisch bezogen sich die Eingaben darauf, ob es Dritten überhaupt erlaubt ist, private Daten geschäftsmäßig zu vermarkten sowie auf die Unrichtigkeit der gespeicherten Daten und die Erteilung von Auskünften.

Auskunfteien sind solche Unternehmen, die Daten über Privatpersonen oder Unternehmen, insbesondere deren wirtschaftliche Betätigung, Kreditwürdigkeit und Zahlungsfähigkeit „sammeln“ und auf dieser Datenbasis Auskünfte über wirtschaftlichen Verhältnisse 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. Kreditinstitute, Kreditkartengeber, Leasinggesellschaften sowie 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. eine Datenübermittlung von dem Geschäftspartner der Auskunftei zum Zweck der Speicherung und Beauskunftung der Daten durch die Auskunftei (Einmeldung). Die Daten stammen jedoch nicht nur aus übermittelten Daten, sondern auch aus allgemein zugänglichen Quellen wie Telefon- und Adressbücher, Branchenverzeichnissen oder öffentlichen Registern wie dem Handelsregister oder dem Schuldnerverzeichnis (§ 915e Abs. 1 ZPO).

In der Phase der Datenverarbeitung ist vor allem die Übermittlung von Daten der Auskunfteien an Dritte von Relevanz. Erheben, verarbeiten und nutzen Auskunfteien personenbezogene Daten, unterliegen sie den Datenerhebungs- und Verwendungsvorschriften des BDSG. Die Zulässigkeit der einzelnen Verarbeitungsschritte richtet sich, sofern keine entsprechende Einwilligung nach § 4a BDSG der Betroffenen vorliegt, nach § 29 BDSG – geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung.

Neben Namen, Anschrift und Geburtsdatum werden gegebenenfalls auch Daten zum Einkommen und Vermögen, z. B. Tätigkeit, Arbeitgeber, Umsatz, Grundbesitz, Bankverbindung und Schulden gespeichert. Gespeichert wird auch, ob eine eidesstattliche Ver-

***§ 29 BDSG – Geschäftsmäßige Datenerhebung und –speicherung zum Zweck der Übermittlung* (Auszug)**

Abs. 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.

sicherung abgegeben, ein Zwangsversteigerungsverfahren betrieben, gegen den Betroffenen wegen Säumigkeit ein Haftbefehl angeordnet wurde oder ob vollstreckbare Schuldtitel vorliegen.
Bei Unternehmen und gewerblich tätigen Einzelpersonen werden bei einigen Auskunfteien bei fehlenden Informationen auch „Schätzdaten“ gespeichert.

Abs. 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.

Durch die Einführung des § 28a BDSG wird nunmehr seit dem 01.04.2010 gesetzlich definiert, unter welchen Voraussetzungen eine Datenübermittlung an Auskunfteien zulässig ist.

Festzustellen ist, dass die Auskunfteien die Betroffenen häufig mit Anschreiben „informieren“, 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. Eine solche **Selbstauskunft** ist **stets freiwillig**.

Neben der Zulässigkeit der Datenerhebung und -speicherung ist für die Betroffenen von besonderer Relevanz, 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 einer 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 nach § 29 Abs. 2 BDSG. Danach ist die Übermittlung nur zulässig, 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 abschätzen zu können.

In einem Fall wandte sich der Betroffene zunächst selbst an die Auskunftei, die im Rahmen einer Veröffentlichung zu bestimmten Firmen (juristischen Personen), an denen der Betroffene beteiligt ist, auch dessen persönliche Telefon- und Faxnummer und E-Mail-Adresse veröffentlichte. Zwar wurde der Forderung des Betroffenen auf Löschung der Daten nachgekommen, diesem wurde allerdings dargelegt, dass die Angelegenheit keinen datenschutzrechtlichen Bezug hatte. Dies wurde damit begründet, dass es sich bei den Daten allein um Firmendaten gehandelt habe.

Die Aufsichtbehörde teilte der Auskunftei mit, dass sich die in Rede stehenden Daten zumindest auf eine bestimmbare Person beziehen. Datenschutzrechtlich sind auch Unternehmensdaten relevant, die sich auf eine natürliche Person beziehen lassen, was bei einer Einzelfirma der Fall ist. Die Verknüpfung von personenbezogenen Daten mit Unternehmensdaten stellt eine Nutzung personenbezogener Daten dar.

Die Auskunftei führte aus, dass erst im Zuge der Korrespondenz mit dem Betroffenen deutlich geworden sei, dass es sich bei der angegebenen Telefonnummer um eine persönliche Nummer handelt und nicht um eine zentrale Einwahlnummer des Unternehmens. Nach entsprechender Kenntnis habe man die Daten aus dem Firmenprofil herausgenommen und den Datensatz gelöscht. Diese Vorgehensweise der Auskunftei war korrekt. Weitere datenschutzrechtliche Mängel konnten nicht festgestellt werden. Dies wurde dem Betroffenen mitgeteilt und die Angelegenheit damit abgeschlossen.

In einem anderen Verfahren wandte sich der Betroffene an die Aufsichtsbehörde, weil von einer Stadtverwaltung bei einer Auskunftei zu seiner Person angefragt wurde und

die Auskunftei Daten übermittelte. Der Betroffene hält sowohl die Datenerhebung als auch die Datenübermittlung für unzulässig, da er die Stadtverwaltung lediglich bezüglich eines Spendenkontos, auf das er keinen Zugriff haben wollte, um Unterstützung gebeten habe. Auch habe ein Unternehmen, mit dem Barzahlung vereinbart worden ist, ebenfalls bei einer Auskunftei zu seiner Person angefragt. In beiden Angelegenheiten sei nicht zu erkennen, welches Interesse an der Einholung einer entsprechenden Auskunft bestanden habe.

Die Aufsichtsbehörde prüfte die Datenerhebung durch das private Unternehmen und die jeweiligen Datenübermittlungen durch die Auskunftei an die anfragenden Stellen. Die Beurteilung der Zulässigkeit der Datenerhebung seitens der Stadtverwaltung als öffentliche Stelle oblag nicht der Aufsichtsbehörde.

Das private Unternehmen begründete das Interesse an der Datenerhebung damit, dass der Betroffene Neukunde sei und vorab stets geprüft werden müsse, ob ein Kunde erbrachte Leistungen bezahlen kann. Grundsätzlich kann hierin ein berechtigtes Interesse zu sehen sein. Es ist allerdings zweifelhaft, ob dies auch gilt, wenn Barzahlung bei Anlieferung vereinbart wird. Erfolgt eine Bezahlung in solchen Fällen nicht, kann die Leistung vom Unternehmen nicht erbracht werden. Die Auskunftei selbst erkannte jeweils ein berechtigtes Interesse an der Datenübermittlung an. Dass eine Abwägung entsprechend § 29 Abs. 2 Nr. 1a und 2 BDSG stattgefunden hat, ließ sich den jeweiligen Stellungnahmen nur bedingt entnehmen. Die Prüfung ist noch nicht abgeschlossen.

Begriffsbestimmungen:
Tatsachen sind **glaubhaft** dargelegt, wenn eine überwiegende Wahrscheinlichkeit für ihr Vorliegen spricht. Glaubhaft darzulegen sind alle Tatsachen, die von der übermittelnden Stelle bei der Prüfung des „berechtigten Interesses“ zu berücksichtigen sind. Werden Daten im Hinblick auf beabsichtigte oder bevorstehende vertragliche Beziehungen mit dem Betroffen angefordert, so ist die Art des Vertrages mitzuteilen. Andernfalls kann nicht geprüft werden, ob ein berechtigtes Interesse vorliegt. Zwar wird durch § 29 BDSG als **berechtigtes Interesse** nicht allein ein kreditorisches Risiko normiert, es muss jedoch ein anderes wirtschaftliches Risiko vorliegen.

5 Interessantes – Wissenswertes im Bereich des Datenschutzes

5.1 Google Street View

Google Street View ist ein Geodienst des US-Unternehmens Google Inc. und seit 2008 auch in Deutschland in aller Munde. Dieser Dienst ermöglicht es am Computerbildschirm bei einem virtuellen Spaziergang einen Straßenzug aus der Perspektive des Fußgängers zu betrachten. Nach Aussagen der Diensteanbieter bietet Street View vielfältige Nutzungsmöglichkeiten, man könne sich über Parkmöglichkeiten oder barrierefreie Zugänge informieren, seiner Familie zeigen, wo man lebt etc..

Bisher sind über Google Street View noch keine Bilder aus Deutschland abrufbar, da Google zuvor Forderungen der Datenschutzbehörden nachkommen will. Google gab zwar zunächst an, dass der Nutzen des Dienstes nicht zu Lasten der Privatsphäre der auf dem Bildmaterial zufällig ersichtlich werdenden Passanten geht, da durch modernste Technologie verhindert werden soll, dass Passanten und Kfz-Kennzeichen auf dem ins Internet eingestellten Bildmaterial erkennbar werden. Zweifelsfrei ist aber bei der Aufnahme eine Erhebung personenbezogener Daten möglich. Dieser Datenschutzbezug wurde im November 2008 vom Düsseldorfer Kreis bestätigt. Es wurde zum Thema „Datenschutzrechtliche Bewertung von digitalen Straßenansichten insbesondere im Internet“ folgender Beschluss gefasst:

„Bei digital erfassten Fotos von Gebäude- und Gebäudeansichten, die über Geokoordinaten eindeutig lokalisiert und damit einer Gebäudeadresse und dem Gebäudeeigentümer sowie den Bewohnern zugeordnet werden können, handelt es sich in der Regel um personenbezogene Daten, deren Erhebung und Verarbeitung nach dem Bundesdatenschutzgesetz zu beurteilen ist. Die Erhebung, Speicherung und Bereitstellung zum Abruf ist nur zulässig, wenn nicht schutzwürdige Interessen der Betroffenen überwiegen. Bei der Beurteilung schutzwürdiger Interessen ist von Bedeutung, für welche Zwecke die Bilddaten verwendet werden können und an wen diese übermittelt bzw. wie diese veröffentlicht werden. Die obersten Aufsichtsbehörden sind sich einig, dass die Veröffentlichungen von georeferenziert (Zuweisung raumbezogener Referenzinformationen, der Georeferenz, zu einem Datensatz) und systematisch bereit gestellten Bilddaten **unzulässig** ist, wenn hierauf Gesichter, Kraftfahrzeugkennzeichen oder Hausnummern erkennbar sind. Den betroffenen Bewohnern und Grundstückseigentümern ist zudem die Möglichkeit einzuräumen, der Veröffentlichung der sie betreffenden Bilder zu widersprechen und dadurch die Bereitstellung der Klarbilder zu unterbinden.

Keine schutzwürdigen Interessen bestehen, wenn die Darstellung der Gebäude und Grundstücke so verschleiert bzw. abstrakt erfolgt, dass keine individuellen Eigenschaften mehr erkennbar sind. Um die Möglichkeiten zum Widerspruch schon vor der Erhebung zu eröffnen, sollte die geplante Datenerhebung mit einem Hinweis auf die Widerspruchsmöglichkeit rechtzeitig vorher bekannt gegeben werden. Die Widerspruchsmöglichkeit muss selbstverständlich auch noch nach der Veröffentlichung bestehen."

Google Fahrzeug abgebildet in Wikipedia
© Axel Mauruszat

Seit Juli 2008 nimmt Google bereits hierzulande Straßenansichten in vielen Städten und Landkreisen mit Fahrzeugen auf, die mit speziellen Kameras ausgestattetet sind, und veröffentlicht, an welchen Orten weitere Aufnahmen geplant sind.
Die Veröffentlichung der aufgenommenen Bilder war ursprünglich für 2010 vorgesehen, soll aber nunmehr erst nach Abarbeitung aller Widersprüche gegen die Erfassung der Bilder und Daten erfolgen. Dies gab die Bundesverbraucherministerin Ilse Aigner am 30.04.2010 in Berlin bekannt.

Aktueller Stand (31.05.2010) ist, dass vor der Inbetriebnahme des Dienstes die von Google Germany GmbH im Juni 2009 gegenüber dem zuständigen Hamburger Datenschutzbeauftragten gemachten Zusagen praktisch umgesetzt werden. Dabei handelt es sich um einen 13-Punkte-Katalog. Google hat u. a. zugesichert,

- die geplanten Befahrungen mit einem Hinweis auf die Widerspruchsmöglichkeiten im Internet rechtzeitig vorher bekanntzugeben,
- eine Technologie zur Verschleierung von Gesichtern und Kfz-Kennzeichen vor der Veröffentlichung derartiger Aufnahmen einzusetzen,
- Widerspruchsmöglichkeiten zur Entfernung bzw. Unkenntlichmachung eines Gebäudes durch einen Bewohner oder Eigentümer vorzuhalten,
- Widersprüche zu Personen, Kennzeichen und Gebäuden bzw. Grundstücken vor Veröffentlichung zu berücksichtigen und entsprechenden Bilder bereits vor der Veröffentlichung unkenntlich zu machen,
- die Widerspruchsmöglichkeit auch nach der Veröffentlichung vorzuhalten,

- die Löschung oder Unkenntlichmachung der Rohdaten von Personen, Kfz und Gebäudeansichten vorzunehmen, die aufgrund eines Widerspruchs zu entfernen sind.

Die vollständige Liste der Zusagen von Google ist auf den Webseiten des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit zu finden.

@ http://www.hamburg.de/datenschutz/aktuelles/1569338/google-street-view-zusage.html

Deutlich wird, dass dem Widerspruchsrecht entscheidende Bedeutung zukommt. Widersprüche können eingelegt werden im Internet unter http://maps.google.de/intl/de/help/maps/streetview/faq.html#q7 oder schriftlich bei der Google Germany GmbH, betr.: Street View, ABC-Straße 19, 20354 Hamburg.

Um die Einreichung eines Widerspruchs zu erleichtern, hat das Landesverwaltungsamt als erste Datenschutzaufsichtsbehörde im vergangenen Jahr auf seiner Internetseite ein Formular zur Verfügung gestellt, mit dem das Widerspruchsrecht geltend werden kann.

Absender (Name, Anschrift)

Google Germany GmbH
ABC-Straße 19
20354 Hamburg

per Fax: +49 40-4921-9194
per E-Mail: streetview-deutschland@google.com

Erhebung und Veröffentlichung von Aufnahmen durch den Dienst "Google Street View"
Widerspruch gegenüber Google Inc./USA bzw. Google Germany GmbH

Sehr geehrte Damen und Herren,

hiermit nutze ich die mir zustehende Möglichkeit, der Erhebung und Veröffentlichung von Aufnahmen in jedweder Form der eigenen Person, von eigenen Kraftfahrzeugen und selbst bewohnten oder genutzten Gebäuden bzw. Grundstückseigentum zu widersprechen.

Konkret widerspreche ich der Erhebung und Veröffentlichung von Aufnahmen:

Widerspruchsobjekt	Beschreibung des Widerspruchsobjektes [1]
Bitte auswählen	

[1] Erläuterungen zur Beschreibung der Widerspruchsobjekte finden Sie in unserem Hinweisblatt

Den Grund für meinen Widerspruch lege ich dar, soweit es im Einzelfall für Sie, z.B. zur Vermeidung von Missbrauch, notwendig ist.

Ich bitte um Bestätigung meines Widerspruchs.

Sollten Sie Rückfragen zum Widerspruchsobjekt haben, stehe ich zur Verfügung.

Mit freundlichen Grüßen

Vollständig abrufbar: @:
http://www.sachsen-anhalt.de/LPSA/fileadmin/Elementbibliothek/LVwA-Bibliothek/Aktuelles/Presse/Google-Street-View.pdf

5.2 Soziale Netzwerke

StudiVZ ***SchülerCC*** ***Facebook*** **Wer-Kennt-Wen (WKW)** **Myspace** **XinG**	Soziale Netzwerke boomen. In solchen Online-Kontaktnetzwerken haben Internetnutzer die Möglichkeit, sich kennenzulernen, sich zu „treffen“, zu chatten, sich online auszutauschen und hierfür auch eigene Inhalte bis zum ausführlichen Persönlichkeitsprofil samt Interessen und Aktivitäten einzustellen.

Nutzer der Plattformen für Soziale Netzwerke sind Schüler, Studenten, Senioren, Fachexperten usw.. So vielfältig die Nutzungsmöglichkeiten sind, so komplex können auch die datenschutzrechtlichen Probleme der jeweiligen Angebote sein. Denn oftmals werden der virtuellen und scheinbar anonymen (Online-)Welt Informationen anvertraut, die der Nutzer im realen Leben sogar gegenüber besten Freunden verschweigen würde. Welche Risiken und Gefahren für die Persönlichkeitsrechte damit verbunden sein können, ist den Betroffenen zumeist nicht bekannt oder wird von ihnen ignoriert.

Natürlich möchte die Aufsichtsbehörde den Trend zur Nutzung sozialer Netzwerke nicht pauschal verteufeln, vielmehr will sie nachfolgend die Risiken aufzeigen und Hinweise geben, wie man seine Privatsphäre auch in sozialen Netzwerken schützen kann.

Welche Risiken sich für Nutzer ergeben können, belegen die nachfolgenden der Presse entnommenen Beispiele:

- Personalberater setzen Personensuchmaschinen ein bzw. recherchieren in Sozialen Netzwerken, um sich Informationen über Bewerber zu verschaffen. Lassen sich Einträge oder Fotos finden, die entweder nicht zur Einstellung eines Unternehmens passen oder scheinbar auf mangelnde Arbeitsmoral schließen lassen, wird ein Bewerber abgelehnt.
- Negative Aussagen über das eigene Unternehmen führten bereits zu Kündigungen.
- Angaben über den Beziehungsstatus wurden vom Ex-Partner zum Stalking genutzt.
- Es kam zu Schulverweisen nach beleidigenden Äußerungen über Lehrer.

Bisher ist nicht bekannt geworden, dass die Plattformen genutzt werden, um spezielle Risiken abzuprüfen, z. B.

- von Versicherungen vor Abschluss von Lebens-, Berufsunfähigkeits-, Kranken- oder Kfz-Versicherungen,
- von Auskunfteien zur Ermittlung der Kreditwürdigkeit, Kaufkraft oder des umsatzrelevante Verhaltens (bspw. Viel-/Wenigtelefonierer) oder
- von Vermietern, die Rückschlüsse auf das Verhalten von Mietbewerbern (häufige Partys, laute Musik, Haustiere etc.) ermitteln wollen.

Die Möglichkeit einer solchen Nutzung ist jedoch nicht von der Hand zu weisen.

Die folgenden Tipps sollen aufzeigen, wie soziale Netzwerke genutzt und dabei gleichzeitig mögliche negative (Spät-)Folgen mit geringen Einschränkungen vermieden werden können. Denn das Internet vergisst bekanntlich nichts.

Tipps zur Nutzung von sozialen Netzwerken:

- Das Auftreten im sozialen Netzwerk sollte grundsätzlich unter Verwendung von Pseudonymen (Spitznamen) – ggf. vollständiger Vorname, abgekürzter Nachname - erfolgen! Der „echte“ Name sollte nur zur ersten Kontaktaufnahme genutzt werden.
- Fotos, auf denen die Person deutlich erkennbar ist, sollten vermieden werden.
- Der Grundsatz der Datensparsamkeit ist zu beachten. Die Daten, die man offenbaren möchte, sollten dem Zweck des Profiles angepasst sein.
- Kontaktdaten sollten grundsätzlich nicht angegeben werden!
- Die Standardeinstellungen des Netzwerkbetreibers sollten auf „Privatsphäre hoch“ gesetzt werden, so dass der Zugriff auf die Profildaten nicht für die allgemeine Öffentlichkeit möglich ist.
- Die Daten des sozialen Netzwerkes sollten nicht in Suchmaschinen auffindbar sein. Einige Netzwerke ermöglichen den Zugriff auf Profildaten grundsätzlich nur anderen Mitgliedern, andere ermöglichen den Ausschluss der Recherche über Suchmaschinen oder die Beschränkung des Zugriffs zumindest als Option.
- Anwendungen von Drittanbietern sollte kein Zugriff auf die Profildaten ermöglicht werden.
- Vorsicht bei netzwerkübergreifenden Verknüpfungen! Soziale Netzwerke oder andere Dienstleister ermöglichen die gemeinsame Pflege oder Nutzung der Profildaten in mehreren Netzwerken.
- Die Rechte Dritter müssen beachtetet werden. So sollten z. B. Fotos anderer Personen nur mit deren Zustimmung eingestellt werden.

5.3 Illegaler Datenhandel

Wie bereits dargestellt, erhalten Datenschutzbehörden eine Vielzahl von Beschwerden von Verbraucher/Innen über unerwünschte Telefonanrufe. Im Berichtszeitraum verschärfte sich die Problematik dadurch, dass sich während des ungebetenen Anrufes teilweise herausstellte, dass die Kontodaten des Verbrauchers beim Anruf bereits bekannt waren. Bei den Anrufen sollen typischerweise die persönlichen Daten abgeglichen werden und/oder Gewinnspielabonnements, die Teilnahme an Lotterien oder sonstige Dienstleistungsverträge aufgeschwatzt oder **untergeschoben** werden. Obwohl die Betroffenen telefonische Angebote meist ablehnten, kam es vor, dass kurze Zeit später Abbuchungen von dem „abgeglichenen" Bankkonto stattfanden. Kontrolliert ein Betroffener seine Abbuchungen nicht regelmäßig und macht unerlaubte Abbuchungen rückgängig, hat er neben dem unzulässigen Umgang mit seinen personenbezogenen Daten auch materiellen Schaden zu befürchten.

Um an die Daten der Betroffenen zu gelangen, gibt es verschiedene „Geschäftsmodelle". Stets werden die Betroffenen in Gespräche verwickelt, bei denen versucht wird, ihnen so viele Informationen wie möglich zu entlocken. So wird z. B. häufig eine falsche Kontoverbindung genannt, die der überrumpelte Verbraucher ohne nachzudenken korrigiert. Sofern den Betroffenen bereits die korrekte Kontoverbindung mitgeteilt wird, stellt sich die Frage, woher diese Daten resultieren. Eine allgemeingültige Antwort auf diese Frage gibt es kaum, denn die Wege der illegalen Datenbeschaffung sind vielfältig. Die meisten Datensätze stammten offensichtlich aus Beständen von Glücksspielunternehmen. Entweder haben unzuverlässige Mitarbeiter Firmendatenbestände kopiert und weiterverkauft oder zwischengeschaltete Call-Center haben die Daten nach Abschluss ihrer Aufträge nicht gelöscht, sondern gesammelt und weiter verwendet. Die Datenbestände können allerdings auch aus der Inanspruchnahme von Internetdiensten, aus dem Zeitschriftenvertrieb, aus Spendensammlungen, von Preisausschreiben oder aus Kundenbeständen anderer Unternehmen resultieren.
Verständlicherweise stellt sich der ein oder andere Leser die Frage, wie es möglich sein kann, mit illegal erworbenen Kontodaten Abbuchungen zu erwirken. Denn grundsätzlich dürfen Dritte ohne eine zuvor erfolgte Einzugsermächtigung des Kontoinhabers keine Beträge vom fremden Konto abbuchen. Im sog. Lastschriftverfahren ist dies dennoch möglich, da es wie folgt abläuft:
Der Einzugsberechtigte übergibt seinem Geldinstitut ein als Lastschrift ausgewiesenes Formular mit dem Namen und der Bankverbindung des Zahlungspflichtigen sowie dem abzubuchenden Betrag. Das Geldinstitut wendet sich daraufhin an die Bank des Zahlungspflichtigen, die aufgrund der erklärten Einzugsermächtigung das Konto des Zahlungspflichtigen

belastet. Im Massenverfahren der Lastschrifteinlösung werden Abbuchungen im Rahmen einer sog. Inkassovereinbarung zugelassen. Die Ermächtigung des Kontoinhabers zum Einzug der Lastschrift wird nur stichprobenartig überprüft. Der Zahlungsempfänger muss sich somit nur vorab verpflichten, die Einzugsermächtigung auf Verlangen vorzulegen.
Wie Sie sich dennoch gegen derartige Geschäfte mit Ihren Bankdaten zur Wehr setzen können, zeigt die nachfolgende Übersicht:

Illegaler Datenhandel – Was kann ich tun?

- **Was kann ich tun, wenn bereits Geld von meinem Konto abgebucht wurde?**

Nachdem Sie von einer rechtswidrigen Lastschriftabbuchung Kenntnis erlangt haben, können Sie diese bei Ihrem Geldinstitut innerhalb von einer Frist von 6 Wochen ohne Begründung widerrufen. Der abgebuchte Betrag wird Ihrem Konto problemlos wieder gutgeschrieben. Dies setzt voraus, dass Sie Ihre Kontobewegungen regelmäßig kontrollieren.

- **Wie kann ich zukünftige unerlaubte Abbuchungen verhindern?**

Im Fall des Missbrauchs Ihrer Kontodaten kann es ggf. empfehlenswert sein, von Ihrer Bank den Wechsel Ihrer Kontonummer zu verlangen. Denn sind Ihre Daten einmal im Umlauf und kann weder von der Quelle, noch von weiteren Empfängern eine effektive Datenlöschung verlangt werden, kann es erneut zu unberechtigten Abbuchungen kommen.

- **Sollte ich einen Strafantrag stellen?**

Sollte von Ihrem Konto unberechtigerweise Geld abgebucht worden sein, kann dies sowohl den Tatbestand des Betruges erfüllen, als auch eine strafbewehrte unbefugte Datenverarbeitung (§ 44 BDSG) darstellen. Daher ist **unbedingt** zu empfehlen, nach dem Zurückholen des Geldes (**1. Priorität**) Strafantrag zu stellen.

- **Wie kann ich zukünftig vermeiden, dass meine Adresse, Telefon- und Kontonummer in Umlauf gelangen?**

Zum präventiven Schutz ist immer wieder zu empfehlen, mit dem Angeben persönlicher Daten sparsam umzugehen.
Vermeiden Sie die Weitergabe Ihrer Daten am Telefon und im Internet (Achtung: sog. Phishing-Mails erwecken den Eindruck, dass Sie Ihre Zugangsdaten (z. B. der Bank) bestätigen sollen. Derartiges würden seriöse Anbieter jedoch nicht per Internet vornehmen.
Geben Sie insbesondere Konto- und Telefonverbindungsdaten nur an, wenn dies zwingend notwendig ist und Ihnen Ihr Vertragspartner zuverlässig erscheint.

Weiterhin wird dringend empfohlen, bei Vertragsabschlüssen nicht in eine Weitergabe Ihrer Daten an Dritte einzuwilligen, auch nicht im „Kleingedruckten“. Sofern Ihnen etwas nicht plausibel erscheint, sollten Sie nachfragen. Wenn Sie auf Ihre Fragen keine befriedigende, sondern eine ausweichende oder sogar abweisende Antwort erhalten, sollten Sie Ihrem „Bauchgefühl des Misstrauens“ folgen und keine näheren Angaben machen. Unternehmen sind nämlich gesetzlich verpflichtet, Sie zu informieren, zu welchem Zweck Ihre Daten verwendet werden.

- **An wen kann ich mich bei einem Missbrauch meiner Daten wenden?**

Wenn es um Verbraucherschutzfragen im Allgemeinen geht, können Sie sich an die örtlichen Verbraucherzentralen wenden. Für konkrete Fragen im Zusammenhang mit der Verarbeitung Ihrer personenbezogenen Daten sind die Aufsichtsbehörden für den Datenschutz die richtigen Ansprechpartner. Diese nehmen die Kontrolle über diejenigen Stellen wahr, die Ihre personenbezogenen Daten verarbeiten.

6 Ausblick

In Anbetracht der immer wieder bekannt werdenden Datenskandale ist aktiver Selbstdatenschutz wichtiger denn je. Denn gerade die bekannt gewordenen Fälle des illegalen Datenhandels haben gezeigt, dass auch die besten realitätsnahen und wirksamen materiellrechtlichen Regelungen (z. B. datenschutzrechtliche Gesetzlichkeiten) zum Schutz des Persönlichkeitsrechts, die Gefahr betrügerischen und unzulässigen Umgangs mit personenbezogenen Daten nur reduzieren kann.
Daher ist zunächst darauf zu achten, dass die persönlichen Daten sparsam preisgeben werden und klar ist, wozu die verantwortliche Stelle welche Daten benötigen. Daneben sollten gerade im technischen Bereich Maßnahmen ergriffen werden, um versteckten Gefahren bereits im Vorfeld zu begegnen. In diesem Zusammenhang wird auf die Veröffentlichung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) *„Schützen – Aber wie?“* (veröffentlicht - @: https://www.bsi-fuer-buerger.de). Sobald weiterführender Rat notwendig wird, sollte das Beratungs- und Prüfungsangebot der Aufsichtsbehörde genutzt werden.

Durch die Aufsichtsbehörde kann zwar selten kategorisierend festgestellt werden, ob diese oder jene Datenerhebung, -speicherung oder -nutzung zulässig ist oder nicht, die Aufsichtsbehörde wird allerdings weiterhin jeden ihr bekannt werdenden Sachverhalt einzelfallbezogen untersuchen. Zudem gibt sie auch zukünftig Tipps und Anregungen zur datenschutzkonformen Vorgehensweise der verantwortlichen Stellen geben und wird den schutzwürdigen Interessen der Betroffenen zur Geltung verhelfen. Möglicherweise von datenschutzrechtlichen Verstößen betroffenen Bürgern wird geraten, nicht jede Vorgehensweise von verantwortlichen Stellen ohne Weiteres zu akzeptieren, sondern bei Zweifeln die Aufsichtsbehörde zu informieren. Dies kann ausnahmsweise auch anonym geschehen, wenn der zu überprüfende Sachverhalt hinreichend konkretisiert dargestellt wird und die Daten verarbeitende Stelle benannt wird.

Die Aufsichtsbehörde setzt weiterhin auf vorbeugenden Datenschutz. So kann schon im Vorfeld verhindert werden, dass es zu Verstößen gegen den Datenschutz kommt. Dabei hat die Stärkung des Datenschutzbewusstseins jedes Einzelnen hohe Bedeutung. Dieser Aufgabe stellt sich die Aufsichtsbehörde durch vermehrte Öffentlichkeitsarbeit, insbesondere auch durch Vorträge zum Datenschutz in Schulen.

Hier sind wir erreichbar

▶ Hauptsitz
Ernst-Kamieth-Straße 2, 06112 Halle [Saale]
Telefon [0345] 514 –0

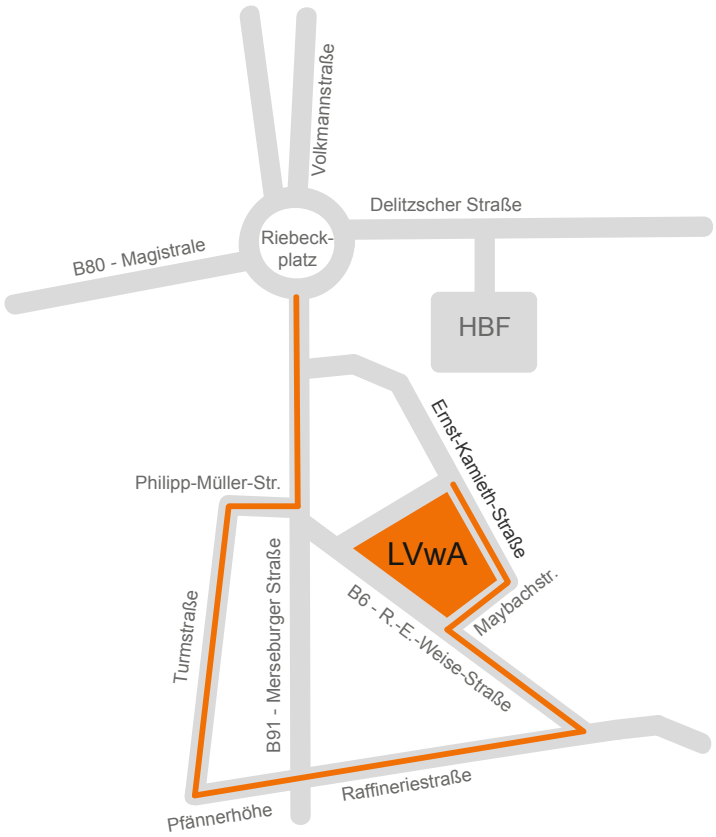
Dienstgebäude Halle
Dessauer Straße 70, 06118 Halle [Saale]
Telefon [0345] 514 –0

Dienstgebäude Halle
Maxim-Gorki-Straße 7, 06114 Halle [Saale]
Telefon [0345] 514 –0

Dienstgebäude Dessau - Roßlau
Kühnauer Straße 161, 06846 Dessau - Roßlau
Telefon [0340] 6506 –0

Dienstgebäude Magdeburg
Olvenstedter Straße 1-2, 39108 Magdeburg
Telefon [0391] 567 –02

Anfahrtsskizze Hauptsitz



Impressum: Landesverwaltungsamt
Ernst-Kamieth-Straße 2
06112 Halle [Saale]
Tel.: [0345] 514 0
Fax: [0345] 514 1477
E-Mail: poststelle@lvwa.sachsen-anhalt.de
Internet: www.lvwa.sachsen-anhalt.de