4. Tätigkeitsbericht

für den Datenschutz im nicht-öffentlichen Bereich

Berichtszeitraum: 2007-2008

Vorbemerkung zum Sprachgebrauch in diesem Bericht:

Logisch ist zu unterscheiden zwischen biologischem und grammatischem Geschlecht (sexus und genus). Es wäre ein Verlust, diese Unterscheidung aufzugeben; sie erleichtert das Verständnis von Texten und hilft, sich auf das Wesentliche zu konzentrieren. Frauen bitte ich, sich auch von scheinbar männlichen, in Wahrheit nur generellen Bezeichnungen gemeint zu wissen: Mitarbeiter, Datenschutzbeauftragter, Betroffener etc. (Übrigens gibt es auch den umgekehrten Fall: Der [männliche] Entbindungspfleger ist eine Hebamme i. S. v. § 53 Abs. 1 Nr. 3 StPO.)

Herausgeber: Der Sächsische Datenschutzbeauftragte
Andreas Schurig
Bernhard-von-Lindenau-Platz 1 Postfach 12 07 05
01067 Dresden 01008 Dresden
Telefon: 0351/493-5401
Fax: 0351/493-5490
E-Mail: saechsdsb@slt.sachsen.de
Internet: www.datenschutz.sachsen.de
Besucheranschrift: Devrientstraße 1
01067 Dresden

Gestaltung (Titelbild): agentur t.krüger kommunikation, Dresden
Herstellung: Reprogress GmbH
Bestellungen: Geschäftsstelle des Sächsischen Datenschutzbeauftragten

Inhaltsverzeichnis

Abkürzungsverzeichnis

AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
BA	Bundesagentur für Arbeit
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BewachV	Bewachungsverordnung
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BIOS	Basic Input Output System
BZRG	Bundeszentralregistergesetz
DEHOGA	Deutscher Hotel- und Gaststättenverband
DPWV	Deutscher Paritätischer Wohlfahrtsverband
DV	Datenverarbeitung
EC	Electronic Cash
EDV	Elektronische Datenverarbeitung
EnEV	Energieeinsparverordnung
Erfa-Kreis	Erfahrungsaustausch-Kreis
GDD	Gesellschaft für Datenschutz und Datensicherung e.V.
GewO	Gewerbeordnung
GmbH	Gesellschaft mit beschränkter Haftung
JVA	Justizvollzugsanstalt
LG	Landgericht
LKA	Landeskriminalamt
NADIS	Nachrichtendienstliches Informationssystem
NJW	Neue Juristische Wochenschrift
NZM	Neue Zeitschrift für Miet- und Wohnungsrecht
OLG	Oberlandesgericht
OWiZuVO	Ordnungswidrigkeiten-Zuständigkeitsverordnung
PersAuswG	Personalausweisgesetz
PIN	Persönliche Identifikationsnummer

SächsDSG	Sächsisches Datenschutzgesetz
SächsGVBl	Sächsisches Gesetz- und Verordnungsblatt
SächsKHG	Sächsisches Krankenhausgesetz
SächsVwVG	Sächsisches Verwaltungsvollstreckungsgesetz
SGB	Sozialgesetzbuch
SMI	Sächsisches Staatsministerium des Innern
StGB	Strafgesetzbuch
TB	Tätigkeitsbericht
TFG	Transfusionsgesetz
TMG	Telemediengesetz
VwVfG	Verwaltungsverfahrensgesetz
WpHG	Wertpapierhandelsgesetz

Vorwort

Der vorliegende vierte Tätigkeitsbericht der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich im Freistaat Sachsen ist zugleich der erste Bericht nach dem Wechsel der Kontrollzuständigkeit vom Sächsischen Staatsministerium des Innern bzw. den Regierungspräsidien auf den Sächsischen Datenschutzbeauftragten. An der inhaltlichen und äußerlichen Gestaltungsweise wurde dabei im Wesentlichen festgehalten, so dass dieser Bericht nicht nur zeitlich bruchlos an die Vorgängerberichte anschließt - was punktuelle Änderungen des bisher eingenommenen Rechtsstandpunktes der Behörde natürlich nicht ausschließt.

Bemerkenswert ist nichtsdestoweniger der gewachsene Umfang dieses Berichtes, der seine Ursache vor allem in einer erheblichen Zunahme der Anzahl der Beschwerden und damit der überprüften Sachverhalte im Berichtszeitraum hat. Zweifellos dürfte dafür neben der Zunahme der personenbezogene Daten verarbeitenden Aktivitäten in der Wirtschaft allgemein und der Steigerung der Wirtschaftstätigkeit in Sachsen insgesamt auch das gestiegene Datenschutzbewusstsein der Bevölkerung eine wesentliche Rolle gespielt haben. Die durch die Medien der Öffentlichkeit nahegebrachten Datenschutzskandale insbesondere des letzten Jahres haben die Sensibilität für Datenschutzbelange zumindest bei den Betroffenen wachsen lassen, die sich deswegen eben auch zunehmend an die Datenschutzaufsichtsbehörde gewandt haben.

Dabei haben sich die großen Datenschutzskandale der Privatwirtschaft insgesamt doch außerhalb Sachsens abgespielt, was den Ort der Vornahme der Verarbeitungshandlungen und damit verbunden die Kontrollzuständigkeit betrifft, natürlich aber nicht in jedem Fall auch hinsichtlich der Betroffenen. So haben auch mir Betroffene über den Missbrauch ihrer (Konto-)Daten durch Lotto-Gesellschaften oder von diesen eingeschaltete Call Center berichtet. Keines dieser Unternehmen hatte seinen Geschäftsbetrieb in Sachsen, so dass die Petenten an die jeweils örtlich zuständigen Aufsichtsbehörden verwiesen werden mussten. In der Lidl-Affäre sind in Sachsen keine Fälle der unzulässigen Mitarbeiterüberwachung festgestellt worden; in diesem Fall ist es daher bei einem Bußgeldverfahren wegen Nichtbestellung eines betrieblichen Datenschutzbeauftragten geblieben - die Medien haben seinerzeit berichtet, dass alle einzelnen Lidl-Vertriebsgesellschaften, und somit auch die im Freistaat Sachsen ansässige Gesellschaft, wegen dieses Verstoßes jeweils eine Geldbuße in Höhe von 10.000 € haben entrichten müssen. Auch hinsichtlich der Datenschutz-Vorfälle bei der Telekom oder der Deutschen Bahn ist davon auszugehen, dass zwar Sachsen als Arbeitnehmer davon betroffen gewesen sind, jedoch hat (auch) insoweit keine Kontrollzuständigkeit beim Sächsischen Datenschutzbeauftragten gelegen.

Negativschlagzeilen aus Sachsens Wirtschaft hat es allerdings dann im Herbst 2008 gegeben, als in einer Leipziger Messehalle Patientenakten mangelhaft gesichert gelagert gewesen sind, so dass im Interesse eines Konkurrenzunternehmens ein Unbefugter sich mit wenig Aufwand in strafbarer Weise Zugang zu den eben nur unzureichend gesicherten Unterlagen hat verschaffen und sogar Daten aus entwendeten Unterlagen für kurze Zeit hat im Internet verfügbar machen können.

Dieser Tätigkeitsbericht hat sich aber nicht mit den großen bundesweiten Datenschutzskandalen zu beschäftigen, sondern stattdessen einen Einblick in das auch in der inhaltlichen Breite der Sachverhalte und der Rechtsfragen erheblich gewachsene Tätigkeitsfeld der Sächsischen Datenschutzaufsichtsbehörde nach § 38 BDSG zu geben. Die Darstellung konkreter Einzelfälle soll Betroffenen wie auch den für die Einhaltung des Datenschutzes in den Unternehmen verantwortlichen Personen, insbesondere natürlich den betrieblichen Datenschutzbeauftragten, datenschutzrechtliche Fragestellungen und Lösungen aufzeigen und sie so bei ihrer Aufgabenwahrnehmung bzw. bei der Geltendmachung ihrer Rechte wirksam unterstützen.

1 Datenschutzaufsicht im nicht-öffentlichen Bereich

Der Sächsische Landtag hat am 13. Dezember 2006 das Gesetz zur Änderung des Sächsischen Datenschutzgesetzes beschlossen, welches zum 1. Januar 2007 in Kraft getreten ist (SächsGVBl 2006, 530 f.). Durch dieses Gesetz wurden die Kontrollzuständigkeit für den Datenschutz im nicht-öffentlichen Bereich (§ 30a SächsDSG) sowie (in Artikel 2 des Änderungsgesetzes) auch die Zuständigkeit zur Verfolgung von Ordnungswidrigkeiten nach dem Bundesdatenschutzgesetz auf den Sächsischen Datenschutzbeauftragten übertragen. Sachsen hat damit als letztes Bundesland seine dezentrale Kontrollstruktur aufgegeben und ist außerdem der verbreiteten Tendenz der Aufgabenübertragung auf den Landesdatenschutzbeauftragten gefolgt. Zum 1. Januar 2007 war damit in sieben Bundesländern (Berlin, Bremen, Hamburg, Mecklenburg-Vorpommern, Nordrhein-Westfalen, Sachsen sowie Schleswig-Holstein) der Landesbeauftragte für den Datenschutz zugleich auch Datenschutzaufsichtsbehörde für den nicht-öffentlichen Bereich. Nachdem im Berichtszeitraum zwei weitere Länder (Niedersachsen am 1. Februar 2007 und Rheinland-Pfalz am 1. Oktober 2008) diesem Vorbild gefolgt sind, sind nunmehr in neun Bundesländern die Landesdatenschutzbeauftragten zugleich auch Datenschutzaufsichtsbehörde nach § 38 BDSG. In den verbleibenden sechs Bundesländern sind entweder das Innenministerium (Baden-Württemberg, Brandenburg, Saarland) oder eine ausgewählte Mittelbehörde (Bayern, Hessen, Sachsen-Anhalt, Thüringen) für die Datenschutzaufsicht im nicht-öffentlichen Bereich zuständig.

Der Sächsische Datenschutzbeauftragte ist somit neben seiner Zuständigkeit nach Art. 57 SächsVerf, §§ 27 bis 31 SächsDSG zugleich auch oberste Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich. Ausschließlich in dieser letzteren Funktion (vgl. § 25 Abs. 4 Satz 1 und 2 SächsDSG) unterliegt er gemäß § 30a Satz 2 SächsDSG der Rechtsaufsicht der Sächsischen Staatsregierung.

Die Datenschutzaufsichtsbehörden überwachen die Durchführung des Datenschutzes bei nicht-öffentlichen Stellen und öffentlich-rechtlichen Wettbewerbsunternehmen und kontrollieren dabei die Einhaltung der Regelungen des Bundesdatenschutzgesetzes sowie anderer Datenschutzvorschriften, soweit sie die automatisierte Verarbeitung personenbezogener Daten oder aber die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht-automatisierten Dateien regeln. Die einzelnen Aufgaben der Datenschutzaufsichtsbehörden leiten sich wie folgt aus dem Bundesdatenschutzgesetz ab:

- **Registerführung** (§ 38 Abs. 2 Satz 1 BDSG)
  Die Aufsichtsbehörden führen das Register der nach § 4d BDSG meldepflichtigen automatisierten Verarbeitungen mit den Angaben nach § 4e Satz 1 BDSG.

- **Anlass- und Regelkontrollen** (§ 38 Abs. 1 Satz 1 BDSG)
  Die Datenschutzaufsichtsbehörden dürfen, soweit die grundsätzlichen Anwendungsvoraussetzungen des Bundesdatenschutzgesetzes erfüllt sind, alle nicht-öffentlichen Stellen kontrollieren. Es müssen weder hinreichende Anhaltspunkte für eine Datenschutzverletzung vorliegen, noch ist auf eine meldepflichtige Tätigkeit als Kontrollvoraussetzung abzustellen. Während sich **Anlasskontrollen** nichtsdestoweniger auf (vermutete) Verstöße gegen datenschutzrechtliche Vorschriften konzentrieren, decken (anlassfreie) **Regelkontrollen** ausgewählte branchenspezifische Schwerpunkte oder aber das gesamte Spektrum datenschutzrechtlicher Vorschriften ab.

- **Beratungstätigkeit** (§§ 4g, 4d, 38 Abs. 1 Satz 2 BDSG)
  Gesetzlich verankert ist die Beratungsfunktion in § 4g Abs. 1 Satz 2 BDSG (Aufgaben des Beauftragten für den Datenschutz) sowie in § 4d Abs. 6 Satz 3 BDSG (Meldepflicht / Vorabkontrolle), wonach sich der betriebliche Datenschutzbeauftragte jeweils in Zweifelsfällen an die Aufsichtsbehörde wenden kann. Darüber hinaus regelt § 38 Abs. 1 Satz 2 BDSG auch generell, dass die Aufsichtsbehörde die Datenschutzbeauftragten und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse berät.

- **Prüfung der Verhaltensregeln von Berufsverbänden** (§ 38a BDSG)
  Ferner können sich auch Berufs- und Unternehmensverbände an die Aufsichtsbehörde wenden, um von ihnen erarbeitete Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen auf die Vereinbarkeit mit geltendem Datenschutzrecht prüfen zu lassen.

- **Genehmigung von Datenübermittlungen in Drittstaaten** (§ 4c Abs. 2 BDSG)
  § 4b BDSG regelt die Übermittlung personenbezogener Daten ins Ausland. Für den konkreten Fall, dass personenbezogene Daten in Drittstaaten ohne angemessenes Datenschutzniveau übermittelt werden sollen, stellt § 4c BDSG einen Ausnahmekatalog bereit, der vermeiden soll, dass der Wirtschaftsverkehr mit diesen Staaten unangemessen beeinträchtigt wird. Über diesen Katalog hinausgehende Ausnahmen sind von der Aufsichtsbehörde zu genehmigen.

- **Öffentlichkeitsarbeit** (§ 38 Abs. 1 Satz 6 BDSG)
  Die Aufsichtsbehörden für den nicht-öffentlichen Bereich haben regelmäßig, spätestens jedoch alle zwei Jahre, einen Tätigkeitsbericht zu veröffentlichen.

Im Rahmen ihrer Tätigkeit können die Aufsichtsbehörden dabei nach pflichtgemäßem Ermessen von folgenden Durchsetzungs- bzw. Sanktionsbefugnissen Gebrauch machen:

- **Unterrichtung des Betroffenen** und **Anzeige** der für den Verstoß verantwortlichen Stelle **bei den zuständigen Ahndungs- und Verfolgungsbehörden** (§ 38 Abs. 1 Satz 6 BDSG)

- Verhängung von **Zwangsgeldern** zur Durchsetzung angeordneter Maßnahmen zur Mängelbeseitigung bzw. Verbot des Einsatzes einzelner Verfahren (§ 38 Abs. 5 Satz 1 und 2 BDSG)

- Aufforderung zur **Abberufung des betrieblichen Datenschutzbeauftragten** (§ 38 Abs. 5 Satz 3 BDSG)

- Erlass förmlicher und damit vollstreckbarer **Auskunftsheranziehungsbescheide**, gegebenenfalls auch verbunden mit der Verhängung von Zwangsgeldern, zur Durchsetzung der Erfüllung der gegenüber der Behörde bestehenden Auskunftspflichten (vgl. § 38 Abs. 3 BDSG) der verantwortlichen Stellen, vgl. hierzu auch unten 10

- Durchführung von **Ordnungswidrigkeitenverfahren**
  Die Zuständigkeit des Sächsischen Datenschutzbeauftragten zur Ahndung von Ordnungswidrigkeiten nach dem Bundesdatenschutzgesetz ergab sich zu Beginn des Berichtszeitraums zunächst aus § 3a OWiZuVO, ab 1. August 2008 dann aus § 13 OWiZuVO - vgl. hierzu auch unten 9.2

- Eigenständiges **Strafantragsrecht** bei BDSG-Straftatbeständen (§ 44 Abs. 2 BDSG)

Die örtliche Zuständigkeit des Sächsischen Datenschutzbeauftragten als Aufsichtsbehörde nach § 38 BDSG ist gemäß § 3 VwVfG auf den Freistaat Sachsen beschränkt. Für die Kontrollzuständigkeit maßgeblich ist, wo die Daten verarbeitet werden, d. h. wo die einzelnen Verarbeitungshandlungen jeweils stattfinden. In der Praxis ist der Sächsische Datenschutzbeauftragte also immer dann zuständig, wenn sich die tatsächliche in der Verarbeitung personenbezogener Daten bestehende Geschäftstätigkeit der verantwortlichen Stelle, deren Erhebung, Verarbeitung oder Nutzung personenbezogene Daten zu überprüfen ist, im Freistaat Sachsen abspielt oder wenn am Unternehmenssitz im Freistaat Entscheidungen darüber getroffen werden, in welcher Weise im Unternehmen personenbezogene Daten verarbeitet werden sollen. Ohne Bedeutung ist dabei, wo der von der Datenverarbeitung Betroffene seinen Wohnsitz hat.

2 Verfahrensregister

Die Aufsichtsbehörde führt ein Register der nach § 4d meldepflichtigen automatisierten Verarbeitungen mit den Angaben gemäß § 4e Satz 1 (§ 38 Abs. 2 Satz 1 BDSG).

§ 4d BDSG definiert eine Meldepflicht für automatisierte Verarbeitungen.

Diese Meldepflicht trifft zunächst alle Unternehmen, die personenbezogene Daten geschäftsmäßig zum Zweck der (gegebenenfalls auch anonymisierten) Übermittlung speichern (z. B. Wirtschaftsauskunfteien, Adresshändler, Markt- und Meinungsforschungsinstitute).

Darüber hinaus sind auch solche Unternehmen von der Meldepflicht betroffen, die höchstens neun Arbeitnehmer mit der automatisierten Datenverarbeitung für eigene Zwecke beschäftigen, diese Datenverarbeitung weder durch die Einwilligung der Betroffenen noch durch die Zweckbestimmung eines Vertragsverhältnisses gedeckt ist, und im Übrigen auch keine Vorabkontrolle erforderlich ist.

Von den Regierungspräsidien sind insgesamt 30 Registermeldungen an den Sächsischen Datenschutzbeauftragten übergeben worden. Im Rahmen der Unterrichtung der betroffenen Unternehmen sind diese Registereinträge überprüft und aktualisiert worden. Dabei erfolgten auch drei Löschungen; in einem Fall wurde die unterlassene Abmeldung mit einem Bußgeld geahndet (vgl. unten 9.1).

Nach weiteren An- und Abmeldungen lagen beim Sächsischen Datenschutzbeauftragten zum Stichtag 31. Dezember 2008 insgesamt 25 Registermeldungen von 24 Unternehmen vor, die

- in 10 Fällen Verfahren von Handels- und Wirtschaftsauskunfteien,

- in 11 Fällen Verfahren von Markt- und Meinungsforschungsinstituten sowie

- in je 1 Fall den Betrieb eines Verfügungszentralregisters, einer Warndatei, eines Adresshandels sowie eines Verfahrens zur Videoüberwachung

betrafen.

Eine Registereintragung bietet dabei weder die Gewähr, dass das betreffende Unternehmen datenschutzkonform arbeitet bzw. dass es bereits einer Kontrolle durch die Aufsichtsbehörde unterzogen worden ist, noch stellt sie eine Genehmigung oder Zustimmung zur Durchführung der gemeldeten Geschäftstätigkeit dar.

Die bei den Datenschutz-Aufsichtsbehörden geführten Verfahrensregister sind in dem in § 38 Abs. 2 BDSG beschriebenen Umfang öffentlich und können folglich von jedem eingesehen werden. Diesbezügliche Einsichtnahme- bzw. Auskunftsbegehren wurden innerhalb des Berichtszeitraums jedoch nicht an den Sächsischen Datenschutzbeauftragten herangetragen.

3 Regelaufsicht

3.1 Überblick

Die Aufsichtsbehörde kontrolliert die Ausführung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht-automatisierten Dateien regeln, einschließlich des Rechts der Mitgliedstaaten in den Fällen des § 1 Abs. 5 (§ 38 Abs. 1 Satz 1 BDSG).

Auch wenn im Bundesdatenschutzgesetz rechtlich nicht zwischen Regel- und Anlasskontrollen unterschieden wird, gibt diese Unterscheidung Aufschluss über die Tätigkeit der Aufsichtsbehörde. Hauptunterschied ist dabei der unterschiedliche Ausgangspunkt für die Kontrolltätigkeit. Während bei Anlasskontrollen (vgl. unten 4.1) regelmäßig ein konkreter Anhaltspunkt für eine mögliche Verletzung datenschutzrechtlicher Vorschriften besteht, handelt es sich bei einer Regelkontrolle (zunächst) um eine reine Routineüberprüfung. Diese unterschiedlichen Ausgangspunkte wirken sich dann natürlich auch auf den Kontrollumfang aus. Bei Anlasskontrollen steht der zu überprüfende Einzelfall im Vordergrund; Regelkontrollen betreffen entweder ausgewählte Teilaspekte oder aber die Verarbeitung personenbezogener Daten durch ein Unternehmen bzw. in einer Betriebsstätte insgesamt.

Im Vergleich zu den Vorjahren wurden im Berichtszeitraum vergleichsweise wenige Regelkontrollen durchgeführt. Dies hat seine Ursache zum wenigsten in der nach der Zuständigkeitsübernahme notwendig gewesenen Neuorganisation der nun beim Sächsischen Datenschutzbeauftragten eingerichteten landesweiten Aufsichtsbehörde, sondern vor allem darin, dass sich der Eingang von Beschwerden im Berichtszeitraum gegenüber dem vorhergehenden Berichtszeitraum weit mehr als verdoppelt (vgl. unten 4.1) und damit die ohnehin knappen personellen Ressourcen gebunden hat.

Die folgende Übersicht gliedert die Überprüfungen auf die Schwerpunktbranchen auf und verdeutlicht zugleich die Entwicklung im Vergleich zu den vorangegangenen Berichtszeiträumen:

Berichtszeitraum Branchen	2001/2002	2003/2004	2005/2006	**2007/2008**
Auskunfteien	0	0	4	**0**
Markt- / Meinungsforschung	1	0	4	**4**
Auftragsdatenverarbeiter	10	1	0	**1**
Wohnungsunternehmen	0	46	19	**15**
Sparkassen / Banken	30	0	0	**0**
Verkehrsunternehmen	57	3	0	**0**
Versorgungsunternehmen	4	7	1	**0**
Altenpflegeheime	0	48	0	**0**
Wohlfahrtsverbände	0	0	10	**7**
Ärzte	0	0	0	**25**
Sonstige	2	5	7	**3**
Gesamtanzahl	104	110	45	**55**

Tab. 1: Übersicht zu durchgeführten Regelüberprüfungen

Bei den in vorstehender Übersicht aufgelisteten Überprüfungen von Wohnungsunternehmen, Wohlfahrtsverbänden sowie Markt- und Meinungsforschungsinstituten handelt es sich überwiegend um durch die Regierungspräsidien noch im Jahr 2006 begonnene und durch den Sächsischen Datenschutzbeauftragten dann im Jahr 2007 fortgeführte bzw. im Hinblick auf die Anwendung einheitlicher Bewertungskriterien, beispielsweise die Gestaltung des öffentlichen Verfahrensverzeichnisses betreffend, neu wieder aufgenommene Regelkontrollen.

Bei den 25 bei Zahnärzten durchgeführten Kontrollen handelt es sich um Schwerpunktprüfungen zum Einsatz von Videoüberwachungsanlagen (vgl. hierzu unten 3.2).

Die verbleibenden, als örtliche Überprüfung ausgestalteten Kontrollen betrafen ein Aktenvernichtungsunternehmen, eine Weltanschauungsgemeinschaft, eine Videothek, ein weiteres Markt- und Meinungsforschungsinstitut sowie eine Schuldnerberatung.

Was die Reaktion der überprüften Unternehmen auf die Prüftätigkeit der Aufsichtsbehörde betrifft, so kann festgestellt werden, dass den Empfehlungen bzw. Beanstandungen der Aufsichtsbehörde im Wesentlichen durch entsprechende Maßnahmen Rechnung getragen worden ist. Anordnungen gemäß § 38 Abs. 5 BDSG waren demzufolge nicht erforderlich.

3.2 Videoüberwachung in Zahnarztpraxen

Im Rahmen einer Anlasskontrolle der Videoüberwachung in einer Hoyerswerdaer Zahnarztpraxis (vgl. Pkt. 4.2.1.7) hatte sich der Praxisinhaber darauf berufen, dass dies fast branchenüblich sei und viele weitere Hoyerswerdaer Zahnärzte in ihren Praxen, insbesondere in den jeweiligen Wartezimmern, Videoüberwachungstechnik im Einsatz hätten.

Um diesen Hinweis entsprechend zu verifizieren, ist im Herbst 2008 ein Großteil der Hoyerswerdaer Zahnarztpraxen einer diesbezüglichen örtlichen Überprüfung unterzogen worden. Die Überprüfung bestand aus einer Befragung des jeweiligen Inhabers sowie einer Sichtkontrolle des Anmelde- und des Wartebereiches.

In zwei der 25 insgesamt überprüften Praxen sind dabei Kameraattrappen festgestellt worden, in einer Praxis wurde eine Kamera tatsächlich zu Beobachtungszwecken eingesetzt.

In Bezug auf die festgestellten Kameraattrappen ist mangels Erhebung personenbezogener Daten ungeachtet der diesbezüglich gleichwohl bestehenden Bedenken keine Kontroll- bzw. Verfolgungszuständigkeit der Aufsichtsbehörde gegeben. Der in einem Einzelfall festgestellte Einsatz von Videokameras zu Beobachtungszwecken wurde als unzulässig bewertet (vgl. wiederum Pkt. 4.2.1.7).

Insgesamt kann festgestellt werden, dass sich die Vermutung eines verstärkten Einsatzes von Videoüberwachungstechnik in Zahnarztpraxen nicht bestätigt hat, insbesondere ist in keinem Fall eine Überwachung des Wartebereiches festgestellt worden. Es ist nicht zu erwarten, dass sich die vermuteten Videoüberwachungsfälle gerade auf die wegen Urlaubs oder anderweitig begründeter Schließzeiten zufällig nicht kontrollierten Praxen konzentrieren.

4 Anlassaufsicht

4.1 Überblick

Die Aufsichtsbehörde kontrolliert die Ausführung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht-automatisierten Dateien regeln, einschließlich des Rechts der Mitgliedstaaten in den Fällen des § 1 Abs. 5 (§ 38 Abs. 1 Satz 1 BDSG).

Von Anlasskontrollen wird im Gegensatz zu Regelkontrollen (vgl. Pkt. 3) immer dann gesprochen, wenn der Aufsichtsbehörde Anhaltspunkte für eine Datenschutzverletzung vorliegen. Zumeist geht ein solcher Anhaltspunkt aus einer Anfrage oder Beschwerde eines Betroffenen hervor. Darüber hinaus können aber beispielsweise auch Pressemeldungen, Hinweisgeber, Erkenntnisse aus Überprüfungen anderer Unternehmen oder eigene (Internet-)Recherchen der Aufsichtsbehörde Auslöser einer Kontrolle sein. Im Regelfall werden Anlasskontrollen im schriftlichen Verfahren durchgeführt, daneben - insbesondere wenn eine besondere Eilbedürftigkeit gegeben ist oder das Vorhandensein konkreter Daten bei der verantwortlichen Stelle zu prüfen ist - werden auch örtliche Überprüfungen durchgeführt. Im Übrigen gibt es aber auch kontinuierlich wiederkehrende Anfragen oder Beschwerden, deren Beantwortung ohne Anhörung der verantwortlichen Stelle möglich ist.

Auch wenn bei Anlasskontrollen der wesentliche Prüfungsschwerpunkt durch den Inhalt der Beschwerde regelmäßig bereits vorgegeben ist, schließt dies aber nicht aus, dass bei dieser Gelegenheit unabhängig davon auch noch andere Sachverhalte überprüft werden. In vielen Fällen werden so auch bei Anlasskontrollen allgemeine datenschutzrechtliche Anforderungen, insbesondere die Bestellung eines Datenschutzbeauftragten, die Verpflichtung auf das Datengeheimnis sowie das Vorhandensein einer internen Verfahrensübersicht, mit in die Kontrolle einbezogen.

Im Berichtszeitraum ist quer durch alle Branchen in insgesamt 425 Fällen derartigen Anhaltspunkten nachgegangen worden, was einer Steigerung um 146 % im Vergleich zum vorhergehenden Berichtszeitraum (173 Fälle) entspricht. Telefonische Eingaben, die auch sofort telefonisch beantwortet werden konnten, sind nicht erfasst worden und folglich in der nachfolgenden Übersicht nicht enthalten.

Berichtszeitraum	2001/2002	2003/2004	2005/2006	**2007/2008**
Eingang	116	147	164	**410**
Übernahme Vorjahr	3	6	9	**15**
davon örtliche Kontrollen	18	24	17	**51**
davon begründet	50	65	62	**87**
keine Zuständigkeit	27	26	31	**57**
noch in Bearbeitung	6	9	15	**29**

Tab. 2: Anlasskontrollen

Die mit Abstand größte Anzahl der überprüften Sachverhalte ist dem Bereich der Videoüberwachung zuzuordnen. Weitere Eingabeschwerpunkte betrafen die (Nicht-)Gewährung der Rechte der Betroffenen, hier in erster Linie das Auskunftsrecht betreffend, sowie Sachverhalte im Zusammenhang mit der Internetnutzung, hier wiederum vor allem Fragen der Zulässigkeit der Veröffentlichung personenbezogener Daten oder der unverlangten Zusendung von Werbemails. Auch Eingaben zum Arbeitnehmerdatenschutz, insbesondere zu Kontrollmaßnahmen des Arbeitgebers, sowie zum Datenschutz im Rahmen des Gesundheitswesens (Arztpraxen, Apotheken, Krankenhäuser und sonstige Leistungserbringer) bildeten einen erheblichen Anteil der durch die Aufsichtsbehörde bearbeiteten Sachverhalte. Weiterhin in größerer Anzahl bei der Aufsichtsbehörde eingegangen sind Beschwerden über die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch Banken und Sparkassen, durch den Einzelhandel sowie branchenübergreifend zu Werbezwecken (Nichtbeachtung von Werbewidersprüchen). Auch Vereine und sonstige Vereinigungen verschiedenster Art, darunter auch eine Religionsgemeinschaft, sowie Vermieter, Hausverwaltungen und Immobilienmakler wurden nach entsprechenden Eingaben mehrfach durch die Aufsichtsbehörde kontrolliert. Im Einzelnen verteilten sich die Schwerpunkte der anlassbedingten Kontrolltätigkeit der Aufsichtsbehörde im Berichtszeitraum wie folgt:

1.	Videoüberwachung	61 Prüfungen
2.	Rechte des Betroffenen	42 Prüfungen
3.	Internet	41 Prüfungen
4.	Arbeitnehmerdatenschutz	22 Prüfungen
5.	Gesundheitswesen	21 Prüfungen
6.	Kreditinstitute	15 Prüfungen
7.	Werbung	15 Prüfungen
8.	Einzelhandel	14 Prüfungen
9.	Vereine, Verbände	12 Prüfungen
10.	Wohnungswesen	10 Prüfungen
11.	Freizeiteinrichtungen	9 Prüfungen
12.	Finanzdienstleister	8 Prüfungen
13.	Auftragsdatenverarbeitung	7 Prüfungen
14.	Auskunfteien / Warnsysteme	7 Prüfungen
15.	Gewinnspiele / Lotto	5 Prüfungen
16.	Verkehrsunternehmen	5 Prüfungen
17.	Rechtsanwälte	5 Prüfungen
18.	Markt- und Meinungsforschung	5 Prüfungen
19.	Gebäudebildaufnahmen	5 Prüfungen
20.	Personalausweisdaten	4 Prüfungen
21.	Versicherungen	4 Prüfungen
22.	Datensicherungsmaßnahmen	4 Prüfungen
23.	Internationaler Datenverkehr	3 Prüfungen
24.	Freie Träger im Sozialbereich	3 Prüfungen
25.	DV für Forschungszwecke	3 Prüfungen

Die festgestellten Datenschutzverstöße betrafen u. a. folgende Sachverhalte:
- unterlassene Bestellung eines betrieblichen Datenschutzbeauftragten (Pkt. 9.1),
- fehlende Verpflichtung auf das Datengeheimnis bzw. mangelhafte Verpflichtungserklärungen,
- fehlende bzw. unzureichende interne Verarbeitungsübersicht sowie Mängel im öffentlichen Verfahrensverzeichnis,

- Verstöße gegen die Meldepflichten (s. a. Pkt. 9.1),
- Nichtbeachtung von Auskunftsverlangen und Werbewidersprüchen,
- Videoüberwachung öffentlich zugänglicher Bereiche einschließlich deren Kennzeichnung, z. B. in einer Mensa (Essensausgabe), eines Wohngebietsparks, einer Ausstellungsfläche in einem Autohaus, in Gaststätten und Arztpraxen, eines Vereinsheimes oder im Einzelhandel (s. a. Pkt. 4.2.1),
- Videoüberwachung von Arbeitnehmern, z. B. in Produktionshallen, Arztpraxen, Küchen, Einzelhandelsgeschäften (s. a. Pkt. 4.2.1),
- Webcamaufnahmen im Internet, z. B. aus Einzelhandelsgeschäften und aus einer Werkhalle (Pkte. 4.2.1.10, 9.1),
- Veröffentlichung personenbezogener Daten im Internet, z. B. Hotelbuchungsdaten, Bewerberlebensläufe, Schiedsrichterlisten, Sportgerichtsurteile, Sportergebnisse, Veranstaltungsteilnehmer, schwarze Listen, Bestandsdaten (s. a. Pkt. 4.2.2),
- Weitergabe der Zugangsdaten für ein Webportal an ein Inkassobüro (Pkt. 4.2.2.6),
- Speicherung von IP-Adressen durch Webhoster (Pkt. 4.2.2.7),
- Newsletter-Versand, Werbemails (s. a. Pkt. 4.2.2.9),
- Kundenidentifikation im E-Commerce (Pkte. 4.2.2.10, 4.2.2.11),
- Datenerhebung durch den Arbeitgeber, z. B. in Form von bei Dritten einzuholenden Selbstauskünften (Pkt. 4.2.3.1) oder durch heimliches Kopieren der Festplatte eines Dienst-PC's (Pkt. 4.2.3.4),
- Übermittlung von Arbeitnehmerdaten, z. B. Aushang von Geburtstagslisten (Pkt. 4.2.3.2) oder zur Angebotserstellung für die Altersvorsorge (Pkt. 4.2.3.3),
- Weitergabe medizinischer Daten, z. B. im Rahmen des Outsourcings (Pkt. 4.2.4.1), bei der Beauftragung privatärztlicher Verrechnungsstellen oder auch bei der Praxisaufgabe (Pkt. 4.2.4.3),
- unzureichend bzw. nicht abgesicherte Lagerung von personenbezogenen Unterlagen (Pkte. 4.2.4.2, 9.1),
- Datenerhebung im Einzelhandel, z. B. beim Warenumtausch (Pkt. 4.2.5.2), bei Barkauf und Sofortmitnahme (Pkt. 4.2.5.3) oder beim EC-Kauf (Personalausweiskopien),
- fehlender Hinweis auf die Freiwilligkeit bei der Datenerhebung, z. B. bei Fragebögen nach dem Wertpapierhandelsgesetz (Pkt. 4.2.6.1) oder im Zusammenhang mit einem Messebesuch,
- Gestaltung und Verwendung von Einwilligungsklauseln zur Datenverarbeitung, z. B. bei Sportveranstaltungen (Pkt. 4.2.7.1),
- Weiternutzung der Mitgliederlisten ehemals verbandsangehöriger Vereine (s. a. Pkt. 4.2.7.2),
- Weitergabe von Versicherungsdaten an Dritte (s. a. Pkt. 9.1),
- Schufa-Abfragen durch Inkassounternehmen,
- Weitergabe von Steuerberatungsunterlagen durch einen Lohnsteuerhilfeverein.

4.2 Ausgewählte Sachverhalte

4.2.1 Videoüberwachung

4.2.1.1 Vielfältige Einsatzbereiche

Wie aus Pkt. 4.1 ersichtlich rangieren Videoüberwachungsfälle in diesem Berichtszeitraum an der Spitze der durch die Aufsichtsbehörde durchgeführten Anlasskontrollen. Bereits in den vorangegangenen drei Tätigkeitsberichten haben die diesbezüglichen Ausführungen einen immer breiteren Raum eingenommen. Die Ursachen dafür liegen einerseits im enormen Preisverfall der Videoüberwachungstechnik, die sie schon seit einiger Zeit in ihren einfacheren Formen praktisch für jedermann aus dem Fachhandel beziehbar und für private Zwecke einsetzbar macht. Andererseits ist der im Regelfall für Sicherheitszwecke erfolgende Einsatz von Videoüberwachungstechnik eben nicht nur mit einzelnen konkreten Geschäftsmodellen bzw. -zwecken verbunden, sondern durchzieht alle Branchen und ist somit für öffentliche wie nicht-öffentliche Stellen gleichermaßen und zunehmend eben auch für Privatpersonen interessant. Aber nicht nur das allseits gestiegene Sicherheitsbedürfnis ist eine wesentliche Ursache für die immer größere Durchdringung aller Bereiche des wirtschaftlichen und gesellschaftlichen Lebens mit Videoüberwachungstechnik; zunehmend werden damit - speziell mit Webcams - auch Marketinginteressen verfolgt. Ein aktuelles Beispiel hierzu ist in den nachfolgenden Ausführungen (Pkt. 4.2.1.10) zu finden.

Die im Anschluss nur beispielhaft vorgestellten Sachverhalte bringen die vielfältigen Einsatzbereiche der Videoüberwachung deutlich zum Ausdruck und ergänzen insoweit die diesbezüglich in den ersten drei Tätigkeitsberichten durch das seinerzeit zuständige Sächsische Staatsministerium des Innern vorgestellten Fälle:

- Tätigkeitsbericht 2001/2002:

  - Geldautomaten (Pkt. 4.2.2)
  - Erlebnisrestaurants (Pkt. 4.3.7)
  - Webcam an einem Supermarkt (Pkt. 4.3.8)

- 2. Tätigkeitsbericht 2003/2004:

  - Altenpflegeheime (Pkt. 4.2.2)
  - Werkhalle (Pkt. 4.3.2)
  - Wohn- und Gewerbegebiet (Pkt. 4.3.5)
  - Wohnanlage (Pkt 4.3.18)

- 3. Tätigkeitsbericht 2005/2006:

  - Freizeitbäder (Pkt. 4.2.1.1)
  - Webcams in Einzelhandelsgeschäften (Pkt. 4.2.1.2)
  - Hauseingangsbereiche (Pkt. 4.2.1.3)
  - Massage-Studio (Pkt. 4.2.1.4)
  - Imbissstand (Pkt. 4.2.1.5)

4.2.1.2 Anwendung des Bundesdatenschutzgesetzes

Bei der Überprüfung von Verfahren zur Videoüberwachung ist zunächst wesentlich, ob mit den eingesetzten Kameras öffentlich zugängliche Räume überwacht werden. Nur dann ist der Anwendungsbereich des § 6b BDSG eröffnet. Voraussetzung ist also, dass Bereiche (also nicht notwendigerweise Räume im engeren Sinn) videoüberwacht werden, die bestimmungsgemäß von jedermann ungehindert betretbar sind, d. h. der Allgemeinheit offenstehen, unabhängig davon, ob dies nur innerhalb bestimmter (Öffnungs- oder Sprech-)Zeiten oder auch nur gegen Entrichtung eines Eintrittsgeldes möglich ist. Bei nicht-öffentlichen Stellen kommen als Erlaubnistatbestände nur § 6b Abs. 1 Nr. 2 und 3 BDSG (Hausrecht oder berechtigte Interessen für konkret festgelegte Zwecke) in Betracht; in beiden Fällen dürfen keine Anhaltspunkte dafür bestehen, dass entgegenstehende schutzwürdige Interessen der Betroffenen überwiegen. Die Weiterverarbeitung der erhobenen Daten unterliegt nach § 6b Abs. 3 BDSG denselben Voraussetzungen.

Die Zulässigkeit der Videoüberwachung in nicht-öffentlich zugänglichen (Betriebs-) Räumen bestimmt sich im Regelfall nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG, ausnahmsweise auch nach Nr. 1 dieser Vorschrift. Auch in diesem Fall sind die berechtigten Interessen der verantwortlichen Stelle gegen die Betroffeneninteressen, hier die schutzwürdigen Arbeitnehmerinteressen, abzuwägen. Während dies im Anwendungsbereich des § 6b BDSG (öffentlich zugängliche Räume) nach vorherrschender Meinung ausnahmsweise anders sein soll, erfasst das Bundesdatenschutzgesetz in seinem Dritten Abschnitt (nicht-öffentlicher Bereich) weder die bloße Beobachtung noch die bloß analoge Bilddatenverarbeitung, da die Bilddaten dann jeweils nicht unter dem Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder *dafür* erhoben werden (§ 3 Abs. 2 Nr. 3, § 27 Abs. 1 Satz 1 Nr. 1 BDSG). Zeitlich beschränkt öffentlich zugängliche Bereiche sind außerhalb der jeweiligen (Öffnungs-)Zeiten wie nicht öffentlich zugängliche Bereiche einzuordnen.

Soweit Privatpersonen zu präventiven Zwecken ihr selbstgenutztes Wohneigentum, insbesondere ihren Hauseingang oder ihre Garageneinfahrt bzw. ihr Grundstück mit Videokameras überwachen und dabei auch angrenzende öffentlich zugängliche Be-

reiche (z. B. Gehweg, Straße) mit erfassen, erfolgt dies ausschließlich für *persönliche oder familiäre* Tätigkeiten, womit auch hier der Anwendungsbereich (vgl. § 1 Abs. 2 Nr. 3 BDSG) des Bundesdatenschutzgesetzes insgesamt, auch des § 6b, nicht eröffnet ist (vgl. Gola/Schomerus, BDSG 9. Aufl., Rdnr. 7a zu § 6b m. w. N., zum Teil abweichend Bizer in Simitis, BDSG, Rdnr. 31 bis 34). Dies gilt natürlich dann nicht mehr, wenn das betreffende Gebäude (auch) für gewerbliche Zwecke genutzt wird oder ganz

keine Daten erhoben, ja es werden nicht einmal Signale zu Beobachtungszwecken weitergeleitet. Fehlt es insoweit mangels Anwendbarkeit des Bundesdatenschutzgesetzes an der Zuständigkeit der Aufsichtbehörde, ist dessen ungeachtet aber darauf hinzuweisen, dass Kameraattrappen von der Rechtsprechung bei der Anwendung allgemeinen Zivilrechtes (z. B. LG Bonn, Urt. v. 16. November 2004 - 8 S 139/04 [RDV 2005, 122] oder LG Darmstadt, Urt. v. 17. März 1999 - 8 O 42/99 [NZM 2000, 360]) regelmäßig wie funktionstüchtige Kameras bewertet werden, denn für die Betroffenen, die den „scheinbar“ überwachten Bereich passieren müssen, stellt sich das äußere Bild beim bloßen Vorhandensein einer Attrappe nicht anders dar als bei Existenz einer funktionstüchtigen Kamera. Dies gilt insbesondere deshalb, weil die Abschreckung der einzige Zweck der Kameraattrappe ist. Allein in dem bei den Betroffenen entstehenden Eindruck des Anfertigens einer Filmaufnahme und dem daraus resultierenden und gerade bei Attrappen zielgerichtet und bewusst erzeugten Überwachungsdruck liegt aber schon ein erheblicher Eingriff in ihr allgemeines Persönlichkeitsrecht.

In der Praxis empfehle ich den Attrappenbetreibern, in der von § 6b Abs. 2 BDSG für den Anwendungsbereich dieser Vorschrift verlangten Weise Hinweise auf die - gar nicht, sondern nur scheinbar stattfindende - Videoüberwachung anzubringen, damit die Attrappe echter wirkt. Damit wird erreicht, dass, wenn die Attrappe zulässig ist, der scheinbar Betroffene sich auf den scheinbaren Eingriff in sein Recht auf informationelle Selbstbestimmung einstellen kann; auch wird die Zahl unbegründeter Beschwerden verringert.

4.2.1.3 Kleintierpraxis

Ohne mit seinen Mitarbeitern zunächst darüber gesprochen zu haben, hatte ein Tierarzt in seiner Praxis mehrere Videokameras installieren lassen. Nachdem er dann von einer Mitarbeiterin daraufhin angesprochen worden war, erklärte er, auch während seines Urlaubs sehen zu wollen, was in der Praxis vor sich geht. Der Aufsichtsbehörde gegenüber behauptete er, die Kameras zum Schutz seiner Angestellten vor Überfällen installiert zu haben. Darüber hinaus sollte dies eine präventive Maßnahme auch gegen Einbruch und Diebstahl sein.

Da die vier Kameras über alle wesentlichen Räume - mit Ausnahme des Warteraums - der Praxis (Rezeption, OP-Vorbereitungsraum, Behandlungsräume) verteilt und somit keine öffentlich zugänglichen Bereiche von der Videoüberwachung betroffen waren, konzentrierte sich die daher auf der Grundlage des § 28 BDSG vorzunehmende rechtliche Beurteilung hinsichtlich der von der Verarbeitung Betroffenen auf die Belange des Arbeitnehmerdatenschutzes. Die Kameras waren, soweit bekannt, so eingestellt, dass sie

insbesondere die vorhandenen Geldkassen sowie die Medikamentenschränke und damit regelmäßig auch die in diesen Bereichen tätigen Mitarbeiter erfassten.

Da nicht erkennbar war, dass die Videoüberwachung der Zweckbestimmung des Arbeitsverhältnisses gedient haben könnte, kam als Zulässigkeitstatbestand lediglich § 28 Abs. 1 Nr. 2 BDSG in Betracht.

Die nach dieser Vorschrift vorzunehmende Interessenabwägung zwischen dem Interesse des Praxisinhabers am Unterbleiben von Eigentumsverletzungen, unter Einschluss der ihn möglicherweise treffenden Berufspflicht, Betäubungsmittel sicher zu verwahren, und dem Interesse der Beschäftigten an Freiheit von ständigem Beobachtungsdruck fiel vorliegend zugunsten der Mitarbeiter aus. Dabei war insbesondere davon auszugehen, dass die betroffenen Mitarbeiter durch die ständige Überwachung und die mit der Aufzeichnung verbundene Möglichkeit der Nachvollziehbarkeit jeder ihrer Handlungen und Bewegungen über den Aufzeichnungszeitraum mit Sicherheit ganz erheblich belastet werden. Für Tierarztpraxen keinesfalls besonders häufige Einbrüche oder gar Überfälle sind demgegenüber eine geringfügige Gefahr, zumal sich dagegen auch mittels anderer Maßnahmen Schutzvorkehrungen treffen lassen.

Der Praxisinhaber hat die Videoüberwachung - jedenfalls innerhalb der Geschäfts zeiten - im Ergebnis eingestellt.

4.2.1.4 Kleingartensparte

In einer Kleingartensparte waren an dem dortigen Vereinsheim, welches auch eine Gaststätte beherbergte, drei Videokameras installiert worden, zwei davon am Giebel des Gebäudes, die dritte deutlich sichtbar am Schornstein. Die Kameras waren einerseits auf den Vereinsparkplatz, andererseits auf den vor dem Gebäude befindlichen Spielplatz, den vorderen Teil der unmittelbar daran anschließenden Parkanlage mit Voliere sowie auf den zum Vereinsheim führenden Fußweg gerichtet. Die genannten Bereiche waren für jedermann frei zugänglich und wurden dem Vernehmen nach auch rege durch vereinsfremde Personen im Rahmen ihres Arbeits- oder Schulweges genutzt. Angrenzende, durch mannshohe Hecken geschützte Gartenparzellen wurden nicht bzw. allenfalls marginal erfasst.

Von den Erlaubnistatbeständen des § 6b Abs. 1 BDSG kamen vorliegend die Wahrnehmung des Hausrechts (Nr. 2) und die Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (Nr. 3) in Betracht.

Mit der Videoüberwachung wurden zum einen Präventionszwecke verfolgt, zum anderen diente sie der Beweissicherung im Schadensfall. Der Verein hatte dargelegt, dass er

insbesondere in den Nachtstunden in nicht unerheblichem Maße von Vandalismusvorfällen betroffen ist, was wohl in erster Linie der Lage des Vereinshauses inmitten der Kleingartenanlage geschuldet ist. Spätabends und nachts halten sich hier im Allgemeinen keine oder nur sehr wenige Vereinsmitglieder auf.

Die genannten Zwecke waren als berechtigt anzuerkennen; im Übrigen befindet sich das gesamte Spartengelände im Eigentum des Vereins, so dass also zur Rechtfertigung der Überwachung alternativ auch das Hausrecht angeführt werden konnte. Die Videoüberwachung war wegen ihrer unstrittigen Präventionswirkung (deutlich sichtbare Kameras sowie entsprechende Hinweise) sowie der bestehenden Aufzeichnungsmöglichkeit auch geeignet, die genannten Zwecke zu erreichen, d. h. die Vandalismusschäden zu verringern und durch die Aufzeichnungen ggf. einen Aufklärungsbeitrag zu leisten. Als Alternativmaßnahme kam zwar die Beauftragung eines Wachdienstes in Betracht, was jedoch für den Verein nicht zu finanzieren und überdies wohl auch nicht gleichermaßen wirksam war (i. A. nur Kontrollgänge in größeren zeitlichen Abständen, eingeschränkte Beweissicherungsmöglichkeiten).

Schutzwürdige Interessen Betroffener (hier: Kleingärtner, Besucher sowie Passanten) standen der Videoüberwachung vor allem deswegen nicht entgegen, weil diese regelmäßig nur in den Nachtstunden in Betrieb war. Die Betriebszeiten begannen mit Schließung des Gartenlokals (22 Uhr) und endeten am frühen Morgen (4 Uhr) noch bevor der „Berufsverkehr“ einsetzte. Während dieses Zeitraums befinden sich üblicherweise kaum Vereinsmitglieder oder sonstige Personen in der Spartenanlage; Passanten werden die Anlage in dieser Zeit nur schnell passieren bzw. gleich umgehen.

Zudem wurde der Rekorder im „Black Box“-Prinzip betrieben, d. h. Auswertungen waren nur für den Schadensfall vorgesehen. Die Speicherdauer war mit drei Nächten als angemessen zu betrachten.

Im Ergebnis wurde die Videoüberwachungsmaßnahme des Kleingartenvereins als zulässig bewertet.

4.2.1.5 Ausstellungsgelände eines Autohauses

Ein Autohaus nutzte ein über zwei Zuwegungen vom öffentlichen Verkehrsraum zugängliches Gelände zur Präsentation von Fahrzeugen. In der Nachtzeit wurde das Gelände mit an den vorhandenen Beleuchtungsmasten montierter Videotechnik überwacht. Zum öffentlichen Verkehrsraum, einer Bundesstraße in Ortslage, wies das Gelände keinerlei Umfriedung oder sonstige bauliche Begrenzungen auf. Ebenso wenig war ersichtlich, dass die Besichtigungszeiten in irgendeiner Weise beschränkt sein sollten.

Hinweise auf diese Überwachungsmaßnahme, z. B. in Form von Schrifttafeln, waren nicht angebracht worden. Dies wurde durch die Aufsichtsbehörde im Hinblick auf § 6b Abs. 2 BDSG gerügt.

Das Ausstellungsgelände bildete einen öffentlich zugänglichen Raum i. S. v. § 6b BDSG. Zwar handelte es sich erkennbar um ein Betriebsgelände, jedoch erlaubte dessen Gestaltung ein unbeschränktes Betreten auch außerhalb der Betriebszeiten. Interessierte Kunden mussten daher davon ausgehen, dass eine Besichtigung auch außerhalb der Geschäftszeiten möglich und sogar gewünscht war.

Dem Grunde nach stand der vorgenommenen Überwachung kein Hindernis entgegen, weil ihr Zweck, insbesondere die Sicherung von Vermögensgegenständen gegen Beschädigung oder Entwendung, von § 6b Abs. 1 und 3 BDSG umfasst ist und keine Anhaltspunkte dafür bestanden, dass insbesondere bei einer auf die Nachtstunden beschränkten Überwachung schutzwürdige Interessen der Betroffenen überwiegen könnten.

An eine zulässige Überwachungsmaßnahme wird jedoch die Forderung geknüpft, dass sie durch geeignete Maßnahmen rechtzeitig erkennbar gemacht wird. Eine ausreichende Transparenz ist dabei nur gewährleistet, wenn bereits der nur potentiell Betroffene über die Überwachungsmaßnahme informiert wird, d. h. dieser somit noch ausweichen kann (vgl. Bizer in: Simitis, BDSG 6. Aufl., Rdnr. 70 zu § 6b). Eine Erkennbarkeit kann nicht schon daraus geschlossen werden, dass die verwendete Überwachungstechnik nach ihrer Bauweise und Installation für jedermann, der das Gelände betritt, (bei entsprechender Kenntnis) sichtbar ist.

Um den gesetzlichen Vorschriften zu entsprechen, kamen folgende alternativen Maßnahmen in Betracht:

a) Anbringen entsprechender Hinweise auf die Videoüberwachung; z. B. das Aufstellen je eines Schildes an beiden dafür vorgesehenen Zugängen, wobei die Schilder jeweils auch einen Hinweis auf das Autohaus als die für die Überwachung verantwortliche Stelle zu enthalten hat, oder

b) von der Straße aus deutlich erkennbare Beschränkung der Besichtigungszeiten auf die Öffnungszeiten oder auch darüber hinaus, z. B. durch Aufstellen je eines Schildes, das darlegt, in welchen Zeiten das Betreten des Betriebsgeländes erlaubt bzw. untersagt ist.

Die Beschränkung der Besichtigungszeiten hat dabei zur Folge, dass außerhalb dieser Zeiten kein öffentlich zugänglicher Raum mehr vorliegt und somit die - dessen unge-

achtet sicherlich wegen der damit verbundenen Präventionswirkung auch weiterhin sinnvolle - Kennzeichnungspflicht entfällt.

4.2.1.6 Außenüberwachung eines Juwelierladens

Ein Juwelier hatte die Installation einer Videokamera an der Außenfassade seines Ladengeschäftes geplant und sich zu seiner Absicherung im Vorfeld an die Aufsichtsbehörde gewandt.

Das Juweliergeschäft grenzte unmittelbar an einen öffentlichen Bürgersteig mit einer sich daran anschließenden Straße. Zudem befand sich direkt vor dem Geschäftseingang der Wartebereich einer Straßenbahnhaltestelle. Die in erster Linie zu Abschreckungszwecken zu installierende Kamera sollte damit diesen öffentlichen Verkehrsraum ganz oder teilweise erfassen; mithin war die datenschutzrechtliche Bewertung auf der Grundlage des § 6b BDSG vorzunehmen. Da der öffentliche Gehweg nicht mehr vom Hausrecht erfasst ist, kam als Rechtsgrundlage nur § 6b Abs. 1 Nr. 3 BDSG (Interessenabwägung) in Betracht.

Die in der Prävention von Raubüberfällen bzw. Anschlägen auf die Schaufensterscheibe bestehenden Interessen waren - insbesondere auch in Beachtung der Art des ausgeübten Gewerbes und des daraus resultierenden besonderen Schutzbedarfs - ohne Zweifel als berechtigt anzuerkennen. Eine Videoüberwachung war wegen ihrer unstrittigen Präventionswirkung sowie der grundsätzlich bestehenden Aufzeichnungsmöglichkeit nicht nur geeignet, die genannten Zwecke zu erreichen, d. h. Überfällen vorzubeugen, Vandalismusschäden zu verringern und durch die Aufzeichnungen gegebenenfalls einen Aufklärungsbeitrag zu leisten, sondern auch erforderlich. Es war kein zumutbares milderes Mittel erkennbar, mit dem die genannten Zwecke ebenso wirksam hätten erreicht werden können.

Dem standen jedoch schutzwürdige Interessen der Betroffenen, d. h. der den öffentlichen Verkehrsraum nutzenden Passanten entgegen. Diese sind - ohne dafür Anlass gegeben zu haben - möglicherweise (Überwachung der gesamten Gehwegbreite) generell von der Videoüberwachung betroffen, dies insbesondere auch dann, wenn sie das Geschäft gar nicht betreten wollen, sondern dieses nur auf ihrem möglicherweise sogar täglichen Weg zu einem anderen Ziel passieren müssen. Bei der angrenzenden Straße handelte es sich um eine belebte und stark befahrene Straße. Das zum Umgehen der Erfassung durch eine hier installierte Videoüberwachung erforderliche Wechseln der Straßenseite war den Passanten nicht zuzumuten. Dies galt umso mehr, als dass sich unmittelbar vor dem Eingang zu Ihrem Geschäft eine Straßenbahnhaltestelle befand. Wartende Fahrgäste halten sich regelmäßig auch direkt und vergleichsweise lange in

diesem Bereich auf. Die betroffenen Passanten konnten weder erkennen noch beeinflussen, wo genau sie in den Erfassungsbereich der Kamera gelangten, ob auch Aufzeichnungen angefertigt würden und wie lange diese ggf. gespeichert blieben. Der sich daraus ergebende Überwachungsdruck bewirkte eine beträchtliche Beeinträchtigung des allgemeinen Persönlichkeitsrechts. Diese Beeinträchtigung wurde auch nicht dadurch gemindert, dass die Videoaufzeichnungen ggf. nur bei Vorkommnissen ausgewertet und andernfalls zeitnah wieder gelöscht werden sollten. Denn dies kann durch die Betroffenen in keiner Weise überprüft werden.

Die erforderliche Abwägung ging daher zugunsten der Betroffenen aus. Dem dargestellten gewichtigen Eingriff in das allgemeine Persönlichkeitsrecht standen keine diesen aufwiegende Gründe entgegen, die sich aus rechtlich geschützten Belangen des Geschäftsinhabers ergeben. Dies galt nicht zuletzt unter der Annahme, dass im Innenbereich des Geschäftes in jedem Fall eine Videoüberwachung installiert werden sollte und dies auch außen am Geschäft entsprechend gekennzeichnet werden musste und somit bereits eine nicht unerhebliche Präventionswirkung erzielt werden konnte.

Damit war zumindest für die Überwachung des Gehweges in seiner gesamten Breite von ca. 3 m keine Zulässigkeit der Videoüberwachung zu erkennen. Anders ist der Fall zu sehen, dass die Videoüberwachung tatsächlich nur einen schmalen angrenzenden Streifen, ca. einen halben Meter, des Gehweges erfasst (vgl. hierzu AG Berlin, Urt. v. 18. Dezember 2003, Az.: 16 C 427/02, wonach die Überwachung eines schmalen an das vom Betreiber der Videoanlage genutzte Grundstück angrenzenden Streifens des Gehweges zu akzeptieren ist), so dass die Möglichkeit besteht, dass der Weg bzw. die Straßenbahnhaltestelle auch genutzt werden kann, ohne dabei gefilmt zu werden. Da der Zweck der Kamera vorrangig in der Prävention lag und für die Beweissicherung insbesondere bei Überfällen zusätzlich noch Innenkameras installiert werden sollten, sollte auf diese Weise dem berechtigten Schutzbedürfnis des Juweliers ausreichend Rechnung getragen worden sein.

4.2.1.7 Zahnarztpraxen

Ein Zahnarzt hatte in seiner zahnärztlichen Gemeinschaftspraxis eine Videokamera im Einsatz, die den Eingangs- und Empfangsbereich, insbesondere auch die Arbeitsplätze der in der Anmeldung tätigen Mitarbeiterinnen, erfasste und deren Bilder bei Kenntnis der entsprechenden Zugangsdaten von jedem beliebigen Internet-PC abgerufen werden konnten. Der Zahnarzt gab an, diese Beobachtungsmöglichkeit zu nutzen, um sich sowohl von seinem Büro in der Praxis als auch von seiner Wohnung aus einen Überblick über das aktuelle Geschehen in der Praxis zu verschaffen. Darüber hinaus diente die Videoüberwachungsanlage Präventionszwecken insbesondere hinsichtlich Einbruch,

Diebstahl sowie Überfällen bzw. Übergriffen sowie Stalking. Eine Aufzeichnung erfolgte nicht.

Soweit die Kamera öffentlich zugängliche Räume, mithin den Eingangsbereich sowie den Bereich vor dem Anmeldetresen, erfasste, bestimmte sich die Zulässigkeit nach § 6b Abs. 1 Nr. 2 und 3 BDSG (Interessenabwägung). Die dort genannten Zulässigkeitsvoraussetzungen waren in dem konkreten Fall allerdings nicht erfüllt. Es fehlte einerseits (während der Sprechzeiten) entweder schon an einem berechtigten Beobachtungsinteresse des Arztes - das allgemeine Informationsinteresse am aktuellen Geschehen in der Praxis ist hierfür nicht ausreichend - oder aber an der Erforderlichkeit der Videoüberwachung, d. h. es standen mildere Mittel (z. B. die ständige Anwesenheit des Personals an der Rezeption, die Installation eines elektrischen Türöffners, ein sicherer Kassenstandort etc.) zum Erreichen des beabsichtigten Zweckes zur Verfügung.

Andererseits standen einer Videobeobachtung auch überwiegende schutzwürdige Interessen der betroffenen Patienten gegenüber. Die Patienten suchen eine Praxis auf, weil sie gesundheitliche Probleme haben. Dies spiegelt sich auch in ihrem Auftreten, gelegentlich sogar in ihrem Aussehen wider. Sie haben daher ein schutzwürdiges Interesse daran, dass ihr Verhalten während des Besuchs in Ihrer Praxis nicht auch noch per Videokamera beobachtet oder gar aufgezeichnet und nachfolgend für eine - für sie - unbestimmte Zeit vorgehalten wird, ohne dass sie die weitere Verwendung bzw. auch Löschung in irgendeiner Form kontrollieren oder beeinflussen können. Dies gilt weiterhin auch deshalb, weil sie für die rein präventiv erfolgende Überwachung überhaupt keinen Anlass gegeben haben. Für Zahnarztpraxen keinesfalls besonders häufige Einbrüche oder gar Überfälle sind demgegenüber eine geringfügige Gefahr, zumal sich dagegen auch mittels anderer Maßnahmen Schutzvorkehrungen treffen lassen. Im Regelfall sind Arztpraxen keine Orte mit einem tatsächlich erhöhten Gefährdungspotential (wie etwa Banken).

Auch die nach § 6b Abs. 1 BDSG vorzunehmende Abwägung ging daher zugunsten der Patienten aus. Aus den dargestellten Gründen war davon auszugehen, dass zweifelsfrei Anhaltspunkte für der Überwachung entgegenstehende überwiegende schutzwürdige Betroffeneninteressen bestanden; eine Videoüberwachung demnach also unzulässig war.

Soweit mit der Kamera nicht öffentlich zugängliche Räume, d. h. die Arbeitsplätze der Mitarbeiterinnen in der Anmeldung, erfasst worden waren, fiel diese bloße Beobachtung (ohne Aufzeichnung) nach der von mir vertretenen Rechtsmeinung nicht in den Anwendungsbereich des Bundesdatenschutzgesetzes (vgl. § 1 Abs. 2 Nr. 3 BDSG) und damit auch nicht in die Kontrollzuständigkeit der Aufsichtsbehörde.

In einem anderen Fall hatte ein Zahnarzt zur Überwachung des Anmelde- und Eingangsbereiches, insbesondere auch der dort befindlichen Geldkassette, ein funkgestütztes Kamera-Monitorsystem eingesetzt. Der nur in Pausenzeiten benutzte Monitor befand sich im Frühstücksraum auf der Eckablage der Sitzbank. Zweck der Videobeobachtung war die Kontrolle des Anmeldebereiches in den Pausen der dort tätigen Mitarbeiter. Zum einen sollte erkannt werden, wenn sich Unbefugte der unter dem Anmeldetresen befindlichen Geldkassette, in der sich zeitweise bis zu vierstellige Geldsummen befänden, näherten. Andererseits sollte auch erkannt werden, wenn neue Patienten eintreffen, um darauf entsprechend reagieren zu können.

Auch der Betrieb dieser Videobeobachtungsanlage wurde als unzulässig bewertet. Da bestimmungsgemäß keine Mitarbeiter von der Beobachtung betroffen gewesen sein dürften, bestimmte sich die Zulässigkeit ausschließlich nach § 6b BDSG. Wiederum fehlte es schon an der Erforderlichkeit der Beobachtungsmaßnahme, denn es gab eine Reihe milderer, nichtsdestoweniger aber gleichermaßen wirksamer Mittel (z. B. ständige Besetzung der Anmeldung, versetzte Pausen, Aufbewahrung der Geldkassette in verschließbarem Schrank oder Mitnahme in den Pausenraum, Klingel auf dem Anmeldetresen), mit denen der angestrebte Zweck gleichfalls verwirklicht werden kann. Im Übrigen wird auf die obigen Ausführungen verwiesen.

4.2.1.8 Wohngebietspark

Der Presse war zu entnehmen, dass eine Wohnungsgenossenschaft ihren Wohngebietspark mit einer Videokamera überwachen würde. Aus der daraufhin angeforderten Stellungnahme ergab sich, dass die Genossenschaft auf einem angrenzenden Hochhaus in ca. 33 m Höhe eine Kamera installiert hatte, die den zentralen Teil des Parks erfasste. Weiter wurde mitgeteilt, dass die Brennweite so eingestellt sei, dass keine Personenerkennung möglich sei. Aus einem beispielhaft beigefügten Überwachungsbild ergab sich in der Tat, dass eine Identifizierung von Personen in der großen Mehrzahl der Fälle ausgeschlossen war, jedenfalls waren keine Gesichter erkennbar. Immer dann, wenn der Betrachter über besondere, zusätzliche Informationen zu den sich im Überwachungsbereich aufhaltenden Personen (z. B. diesbezügliche Arbeitsaufträge an Mitarbeiter der Genossenschaft) verfügte, wäre eine Identifizierung aber zumeist möglich gewesen.

Für die Anwendbarkeit des Bundesdatenschutzgesetzes ist es bereits ausreichend, wenn nur eine Teilmenge der erhobenen Daten personenbeziehbar, d. h. die auf den Videoaufnahmen erfassten Personen bestimmbar (§§ 1 Abs. 2 Nr. 3, 3 Abs. 1 BDSG) sind, mithin war auch diese Überwachung nach den Vorgaben des Bundesdatenschutzgesetzes zu bewerten.

Zur datenschutzrechtlichen Beurteilung der Zulässigkeit der Videoüberwachung war zwischen den Öffnungs- und Schließzeiten der Parkanlage zu unterscheiden.

Soweit sich die Überwachung auf die Nachtstunden und damit auf den Zeitraum, in dem die umfriedete Parkanlage gerade nicht öffentlich zugänglich (Schließzeit) ist, erstreckte, war die datenschutzrechtliche Bewertung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG vorzunehmen. Mit der Videoüberwachung wurden zum einen Präventionszwecke verfolgt, zum anderen diente sie der Beweissicherung im Schadensfall sowie auch der zukünftigen Einsatzkoordinierung des Sicherheitsdienstes. Auslöser waren verschiedene von der Genossenschaft konkret benannte Vandalismusvorfälle. Die genannten Zwecke waren als berechtigt anzuerkennen. Die Videoüberwachung war wegen ihrer unstrittigen Präventionswirkung sowie der bestehenden Aufzeichnungsmöglichkeit auch geeignet, die genannten Zwecke zu erreichen, d. h. die Vandalismusschäden zu verringern und durch die Aufzeichnungen ggf. einen Aufklärungsbeitrag zu leisten. Mildere Mittel waren nicht erkennbar, insbesondere hatte sich der Einsatz eines Sicherheitsdienstes (Streifengänge) allein als nicht ausreichend erwiesen. Die Videoüberwachung war insoweit also auch erforderlich. Schutzwürdige Interessen Betroffener standen der Videoüberwachung vor allem deswegen nicht entgegen, weil davon nur Personen betroffen waren, die sich unberechtigterweise in der Parkanlage aufhielten.

Für die Zeit der Öffnung des Wohngebietsparks war die Zulässigkeitsprüfung nach § 6b Abs. 1 Nr. 3, Abs. 3 BDSG vorzunehmen. Auch hier kam es zunächst darauf an, dass die Videoüberwachung zum Erreichen der genannten Zwecke erforderlich war. Die Genossenschaft hatte dargelegt, dass sich die bekannten Vandalismusvorfälle in der Regel nach Einbruch der Dunkelheit ereignet hätten. Zur Begründung der Erforderlichkeit der Videoüberwachung auch tagsüber konnten diese Vorfälle daher nicht herangezogen werden. Auch der darüber hinaus angeführte Zweck des Schutzes von Kindern und Jugendlichen auf einem im Park befindlichen Spiel- und Matschplatz konnte eine Erforderlichkeit der Videoüberwachung nicht begründen. Denn einerseits war die Videoüberwachung in der realisierten Art und Weise zum Erreichen dieses Zweckes nicht geeignet, denn der Spiel- und Matschplatz befand sich im - vom Kamerastandort aus gesehen - hinteren, insoweit tatsächlich nur schemenhaft erfassten Teil der Parkanlage. Andererseits war es zweifelhaft, ob es als berechtigtes Interesse des Eigentümers überhaupt anzuerkennen war, wenn durch die Videoüberwachung erreicht werden soll, dass die Nutzer des Spielplatzes nicht durch Dritte bedroht oder verletzt oder gar entführt werden, mithin sich ungefährdet und sicher dort aufhalten können. Dies würde eine entsprechende Aufsichtspflicht des Spielplatzeigentümers voraussetzen. Die Aufsichtspflicht trifft stattdessen aber die jeweiligen Aufsichts- bzw. Betreuungspersonen, in erster Linie also die Eltern, im Weiteren auch die Erzieherinnen

dort spielender Gruppen aus Kindertagesstätten. Für die Wahrung der öffentlichen Ordnung und Sicherheit zuständig ist im Übrigen die Kreispolizeibehörde.

Mithin war die Videoüberwachung unter den dargestellten Randbedingungen also tagsüber unzulässig.

4.2.1.9 Gaststätten

Die im Berichtszeitraum zur Videoüberwachung in Gaststätten eingegangenen Eingaben verdeutlichen, dass sich der Einsatz von Videoüberwachungstechnik nicht mehr nur auf Einzelfälle beschränkt, sondern dass es sich insoweit wohl schon um eine in dieser Branche weit verbreitete Erscheinung handelt. Die in diesem Zusammenhang durchgeführten Überprüfungen haben ergeben, dass dies in vielen Fällen nicht im Einklang mit den datenschutzrechtlichen Vorschriften erfolgt. Dies war Anlass, in einem Merkblatt die diesbezüglichen Rechtsgrundlagen und die Voraussetzungen einer zulässigen Videoüberwachung zusammenzufassen und davon ausgehend Möglichkeiten einer rechtskonformen Videoüberwachung aufzuzeigen. Dieses Merkblatt steht auf der Website des Sächsischen Datenschutzbeauftragten zum Herunterladen bereit: *http://www.saechsdsb.de/informationen-noeb/kontrollpraxis-noeb* und ist auch der DEHOGA Sachsen mit der Bitte, es in geeigneter Weise allen ihren Mitgliedern zur Verfügung zu stellen, damit sich diese darauf einstellen können und Fehlinvestitionen vermieden werden, zur Kenntnis gegeben worden.

Die für den Betrieb einer Videoüberwachungsanlage in Gaststätten maßgeblichen Grundsätze lauten demnach wie folgt:

- Vor Einrichtung einer Videoüberwachung in Gaststätten sind die berechtigten Betreiberinteressen sorgfältig gegen die schutzwürdigen Interessen der betroffenen Gäste und Mitarbeiter abzuwägen. Im Ergebnis dieser Abwägung ist davon auszugehen, dass die Überwachung der Sitzbereiche einerseits sowie der ständigen Arbeitsplätze der Mitarbeiter (z. B. Bar, Küche) andererseits regelmäßig das Persönlichkeitsrecht der Betroffenen verletzt und damit unzulässig ist.
- In Bereichen, in denen sich die Betroffenen nur kurzfristig aufhalten, ist nicht von einem Überwiegen von deren schutzwürdigen Interessen auszugehen, so dass die Überwachung von Eingängen, Kassen- oder Garderobenbereichen als im Regelfall erlaubt angesehen werden kann.
- Keinen Bedenken begegnet die Videoüberwachung außerhalb der Geschäftszeiten.
- Eine Videoüberwachung ist für die Betroffenen deutlich sichtbar zu kennzeichnen.

- Eventuell angefertigte Aufzeichnungen sind - soweit kein Grund zu deren Auswertung besteht - kurzfristig wieder zu löschen; eine Speicherdauer von 24 Stunden ist hier im Allgemeinen als ausreichend zu betrachten.
- Das Aufzeichnungsgerät bzw. daran angeschlossene Peripheriegeräte sind wirksam vor unbefugtem Zugang zu schützen.

Bestätigt wurde die dargestellte Auffassung am 22. April 2008 durch eine Entscheidung des Amtsgerichts Hamburg (Az.: 4 C 134/08), welches einer Kaffeehaus-Kette die Videoüberwachung ihrer Kundenbereiche untersagt hat.

Das Geschäftsmodell dieser Kaffeehaus-Kette sieht vor, dass die Kunden ihre Waren selbst an einem Tresen holen, diese auch dort bezahlen und sich dann anschließend in die Kunden- bzw. Sitzbereiche begeben, um dort die Waren zu verzehren bzw. den Kaffee zu trinken. Auch das Amtsgericht hat die Erforderlichkeit der Videoüberwachung zur Prävention einer- wie auch zur Beweissicherung andererseits zunächst bejaht, anschließend dann jedoch festgestellt, dass die notwendige Abwägung mit den entgegenstehenden schutzwürdigen Kundeninteressen zu deren Gunsten ausgeht. Das Gericht hat dabei insbesondere festgestellt, dass - anders als in den Bereichen des Tresens, an dem sich die Kunden in der Regel nur kurzfristig zur Besorgung der gewünschten Produkte aufhalten - die Persönlichkeitsrechte der sich in den Sitzbereichen länger aufhaltenden Kunden durch eine Videoüberwachung erheblich beeinträchtigt werden und diese Rechtsverletzungen schwerer wiegen als die Interessen des Betreibers an einer effektiven Strafverfolgung.

4.2.1.10 Livetour durch eine Werkhalle mittels Webcam

Ein Internet-Druckunternehmen hatte seinen Internetauftritt mit einer so genannten Livetour versehen. Interessierte Kunden und natürlich auch alle sonstigen Surfer konnten eine von mehreren automatisch schwenkenden Webcams auswählen und sich aktuelle Livestreams aus dem Produktionsgeschehen an den heimischen PC übermitteln lassen. Das Unternehmen sah dies als vertrauensbildende Maßnahme gegenüber seinen (potentiellen) Kunden an und wollte damit insbesondere verdeutlichen, dass es sich bei diesem Werk um eine der - lt. Website - modernsten Printproduktionen Europas handelt. Bei Firmen, die ihre Kunden (fast) ausschließlich über das Internet akquirieren, sei es besonders wichtig, dass man potentiellen Interessenten verdeutliche, dass es sich um ein real existierendes, mit modernsten Methoden und Techniken arbeitendes Unternehmen handelt, mit dem man guten Gewissens eine Geschäftsbeziehung eingehen könne. Dies könne am besten mittels aktueller Livebilder aus dem Produktionsgeschehen erfolgen.

Da auf der Mehrzahl der durch Internetnutzer ansteuerbaren Webcams Mitarbeiter des Unternehmens erkennbar und soweit sie sich im Vordergrund des jeweiligen Bildausschnittes aufhielten (z. B. für den Arbeitgeber, für Bekannte oder Verwandte) auch zweifelsfrei identifizierbar waren, war zu klären, auf welcher Rechtsgrundlage die Datenweitergabe an einen insoweit unbestimmten Personenkreis erfolgte.

Das Unternehmen konnte hierzu einerseits eine Betriebsvereinbarung zum Einsatz der Webcams vorlegen, die insbesondere auch die Speicherung oder Nutzung der Bildaufnahmen zu Zwecken der Leistungs- und Verhaltenskontrolle ausschloss, andererseits wurde darauf verwiesen, dass zumindest in neueren Arbeitsverträgen auch diesbezügliche Regelungen enthalten waren. Ungeachtet der noch zu klärenden Detailfragen kann insoweit festgestellt werden, dass gerade eine Betriebsvereinbarung als Rechtsvorschrift im Sinne des § 4 Abs. 1 BDSG eine solche Datenverarbeitung durchaus rechtfertigen kann, dies selbst dann, wenn sie zuungunsten des Arbeitnehmers von dem durch das Bundesdatenschutzgesetz vorgegebenen Schutzniveau abweicht, d. h. wenn sich insbesondere aus den Vorschriften des § 28 BDSG keine Zulässigkeit ergibt und auch keine den Anforderungen des § 4a BDSG entsprechende Einwilligung vorliegt. Gleiches gilt dann, wenn der Einsatz von Webcams Bestandteil der arbeitsvertraglichen Vereinbarungen ist, d. h. somit der Zweckbestimmung des Arbeitsverhältnisses (vgl. § 28 Abs. 1 Satz 1 Nr. 1 BDSG) entspricht.

Neben den eigenen Mitarbeitern gab es aber in diesem Fall noch weitere von dieser Art der Videobeobachtung potenziell Betroffene. Das Druckunternehmen arbeitete, gewissermaßen als Referenzunternehmen, eng mit einem benachbarten Druckmaschinenhersteller zusammen, wodurch sich häufig auch Betriebsfremde in den Produktionshallen aufhielten. Dabei handelte es sich zum einen um das Service- und Wartungspersonal des Druckmaschinenherstellers, der den größten Teil der eingesetzten Technik geliefert hatte, zum anderen um Besucher (Kunden) beider Unternehmen, denen die Leistungsfähigkeit der modernen Drucktechnik im Rahmen einer Besichtigung demonstriert werden sollte.

Für diesen Personenkreis waren weder die Regelungen der eingangs genannten Betriebsvereinbarung noch die ggf. in den Arbeitsverträgen enthaltenen Zustimmungsklauseln von Relevanz.

Während dies bei den Teilnehmern an den Betriebsführungen eher unproblematisch erschien (Erkennbarkeit bzw. Identifizierbarkeit sollte hier im Allgemeinen nicht gegeben sein; auch handelt es sich hier nur um eine einmalige und sehr kurzzeitige Betroffenheit, die zudem voraussetzt, dass die Webcambilder zu diesem Zeitpunkt auch tatsächlich gerade abgerufen werden) und somit eine kurze mündliche Information zu

Beginn der Führung ausreichend sein sollte, stellte sich die Situation beim Servicepersonal doch wesentlich anders dar. Die betroffenen Mitarbeiter waren wiederholt und dann auch über einen vergleichsweise langen Zeitraum in den Hallen des Druckunternehmens tätig und damit wesentlich stärker von der Videoüberwachung betroffen.

Da zwischen dem Druckunternehmen und den Mitarbeitern des Druckmaschinenherstellers weder ein Vertrags- noch ein vertragsähnliches Vertrauensverhältnis i. S. v. § 28 Abs. 1 Satz 1 Nr. 1 BDSG vorlag, kam als Rechtsgrundlage nur § 28 Abs. 1 Satz 1 Nr. 2 BDSG (Interessenabwägung) oder eine Einwilligung nach § 4a BDSG in Betracht. In beiden Fällen ist eine ausreichende Transparenz für die Betroffenen von wesentlicher Bedeutung, dies impliziert sowohl Kennzeichnungen der überwachten Bereiche im Betriebsgelände als auch die Aushändigung eines entsprechenden Übersichtsplanes. Das Druckunternehmen hat sich diesbezüglich entschieden, zukünftig von jedem externen Servicemitarbeiter eine schriftliche Zustimmungserklärung zur Videopräsentation einzuholen.

4.2.2 Internet

4.2.2.1 Veröffentlichung von Sportgerichtsurteilen

In mindestens fünf Fällen hatten sächsische Fußballverbände Spielersperren und Sportgerichtsurteile in ihren Internetauftritt eingestellt. Diese Veröffentlichungen enthielten eine Reihe personenbezogener Daten der betroffenen Spieler, so u. a. Namen, Vornamen, Sportverein, Spieltag, Beschreibung des Regelverstoßes sowie auch das Strafmaß.

Datenschutzrechtlich stellt die Veröffentlichung eine Übermittlung personenbezogener Daten (§ 3 Abs. 4 Satz 2 Nr. 3 BDSG) dar, die einer entsprechenden Rechtsgrundlage bedarf. Gemäß § 4 Abs. 1 BDSG muss der Betroffene entweder in die Übermittlung (Veröffentlichung) einwilligen oder das Bundesdatenschutzgesetz bzw. eine andere Rechtsvorschrift muss dies ausdrücklich erlauben.

Aus den in erster Linie in Frage kommenden Vorschriften des § 28 BDSG - Datenerhebung, -verarbeitung und -nutzung für eigene Zwecke - ergab sich hierfür keine Zulässigkeit: Mitglied der Verbände sind nicht die in den Vereinen aktiven Sportler, sondern stattdessen die Vereine selbst. Insoweit scheidet § 28 Abs. 1 Nr. 1 BDSG (vertragsähnliches Vertrauensverhältnis - hier: Vereinsmitgliedschaft) als Rechtsgrundlage für die Veröffentlichung von Sportgerichtsurteilen aus. Damit verbleibt lediglich § 28 Abs. 1 Nr. 2 BDSG, d. h. die Datenübermittlung muss zur Wahrung berechtigter Interessen des Fußballverbandes erforderlich sein und es darf kein Grund zu der Annahme bestehen, dass entgegenstehende schutzwürdige Betroffeneninteressen überwiegen.

Diese Voraussetzungen waren in den mir bekannt gewordenen Fällen jedoch nicht erfüllt: Ein berechtigtes Interesse des Verbandes an der Bekanntgabe von Sportgerichtsurteilen war allenfalls bezogen auf einen eng begrenzten Adressatenkreis, nämlich die unmittelbar mit der Organisation und Überwachung des Spielbetriebs befassten Personen einschließlich der betroffenen Spieler und Vereine, zu erkennen. Diese Personen erhalten die für sie notwendigen Informationen zur Tätigkeit des Sportgerichts aber regelmäßig schon auf direktem Wege, sei es per Post, per Fax oder auch per E-Mail. Die zusätzliche Veröffentlichung im Internet bewirkt lediglich, dass der Inhalt der getroffenen Sportgerichtsentscheidungen darüber hinaus auch noch der (weltweiten!) Öffentlichkeit zur Verfügung gestellt wird. Dies ist aber für die Umsetzung und Beachtung der Sportgerichtsurteile im Spielbetrieb in keiner Weise erforderlich. Schon aus diesem Grund war die Veröffentlichung also unzulässig.

Darüber hinaus standen der Veröffentlichung aber auch überwiegende schutzwürdige Betroffeneninteressen gegenüber. Bei den Sportgerichtsurteilen handelt es sich um nachteilige Angaben über die Betroffenen, deren Veröffentlichung in jedem Fall mit einer gewissen Prangerwirkung verbunden ist. Diese Daten wurden durch die Internetveröffentlichung auch Personen außerhalb des Verbandes zugänglich gemacht und konnten damit auch in einem anderen Zusammenhang, z. B. bei der Bewerberauswahl für einen Arbeitsplatz, zum Nachteil des Betroffenen verwendet werden. Derartige Recherchen sind heutzutage mittels der verfügbaren Suchmaschinen bekanntermaßen schnell und einfach zu realisieren.

Da die gesetzlichen Verarbeitungserlaubnisse also, wie dargelegt, eine Veröffentlichung von Urteilsaussprüchen der Sportgerichte nicht gestatten und Einwilligung der betroffenen Sportler aus tatsächlichen Gründen als Grundlage für die Erlaubtheit der Veröffentlichung ausscheiden dürfte, fehlte es also an einer Rechtsgrundlage für die Veröffentlichung.

Nichtsdestoweniger müssen die Verbände in diesem Zusammenhang nicht gänzlich auf das Medium Internet verzichten, denn durch vergleichsweise einfache Maßnahmen, namentlich die Einrichtung eines geschützten Bereiches mit einem entsprechenden Zugangskontrollsystem (Benutzername und Passwort), ist eine sachgerechte Berücksichtigung der schutzwürdigen Interessen der betroffenen Spieler bzw. sonstiger Beteiligter möglich. In diesem Fall würden die Informationen über Spielersperren nur einem klar umgrenzten Personenkreis, nämlich den in den Vereinen des Verbandes unmittelbar mit der Organisation und Überwachung des Spielbetriebs befassten Personen, zugänglich gemacht.

Was die Befriedigung des öffentlichen Interesses an der Ahndung besonders schwerwiegender Vorfälle bei bzw. am Rande von Fußballspielen betrifft, so stehen einer Veröffentlichung entsprechender Urteile dann keine datenschutzrechtlichen Bedenken entgegen, wenn sich diese nicht auf einzelne Sportler, sondern auf Vereine insgesamt beziehen. Überdies sind anonyme, d. h. für Außenstehende auf keine konkrete Person beziehbare Mitteilungen im Internet oder sonst an die Öffentlichkeit zulässig, sodass erkennbar wird, welche konkreten Verhaltensweisen welche Folgen nach sich gezogen haben. Das Wichtigste, nämlich dass sich solche Entscheidungen in Spielerkreisen herumsprechen, geschieht wirkungsvoll ohnehin dort, wo es hingehört, nämlich im Vereinsleben und nicht beim individuellen häuslichen Internetsurfen.

In allen fünf mir bekannt gewordenen Fällen haben die jeweiligen Fußballverbände daraufhin die Veröffentlichung von Spielersperren und Sportgerichtsurteilen im Internet eingestellt. Der Sächsische Fußball-Verband e. V. hat mir dazu im Januar 2008 mitgeteilt, dass er die sächsischen Bezirks- und Kreisverbände davon in Kenntnis gesetzt hat, dass solche Veröffentlichungen ab sofort zu unterlassen sind.

Aktuelle Anmerkung:
Am 30. Januar 2009 hat das OLG Karlsruhe (14 U 131/08) entschieden, dass ein Sportverband Angaben zu Sportgerichtsurteilen in seinem Internetauftritt veröffentlichen darf. Zwar sei einzuräumen, dass eine Veröffentlichung von Sportgerichtsurteilen bzw. Spielerstrafen geeignet ist, das Ansehen der Betroffenen zu beeinträchtigen, und auch nachteilige Auswirkungen auf deren sonstige Tätigkeiten haben kann, jedoch würde dieses durchaus schutzwürdige Interesse hinter das Verbandsinteresse an einer umfassenden Information der am Sportgeschehen innerhalb des Verbandes Beteiligten zurücktreten müssen. Dass dies nicht in brieflicher Form an ausgewählte Adressaten geschehe, sondern der Verband hierfür die Vorteile des Internets nutze, entspreche der Bedeutung dieses Mediums und sei nicht zu beanstanden. Betroffene müssten es hinnehmen, dass damit auch die Allgemeinheit unbegrenzt Zugriff auf diese Informationen hat.

Diese Entscheidung übersieht nach meiner wie auch der Auffassung anderer Aufsichtsbehörden, dass die Veröffentlichung von Angaben über Sportgerichtsurteile regelmäßig nur der unverbindlichen Information der am Wettkampfbetrieb Beteiligten dienen soll und keinesfalls die verbindliche Bekanntgabe des Urteils, insbesondere der damit ausgesprochenen rechtlichen Folgen, beispielsweise Sperren, an die insoweit den Spielbetrieb kontrollierenden bzw. an ihm teilnehmenden sowie vor allem die betroffenen Spieler und deren Vereinsführung ersetzen kann und soll. Dies muss, schon wegen der Rechtsmittelmöglichkeit für die letzteren, ja auf normalem nachweisbarem Wege der Individualkommunikation geschehen können. Jeder, der heutzutage Vereins-

vorsitzender ist oder ein ähnliches Amt im Spielbetrieb hat, muss über eine entsprechende technische Erreichbarkeit verfügen. (Für die sächsischen Fußballverbände legt § 78 der Spielordnung des Sächsischen Fußball-Verbandes sogar die „amtlichen“ Kommunikationsformen zwischen Vereinen, Verbänden und Einzelpersonen fest - die Veröffentlichung im Internet gehört jedenfalls zu Recht nicht dazu.) Insoweit ist das Veröffentlichungsinteresse weit weniger bedeutsam einzuschätzen, als das entgegenstehende schutzwürdige Betroffeninteresse, zumal wie dargestellt auch im Internet problemlos entsprechende Zugangsbeschränkungen eingerichtet werden können.

Im Übrigen sah die im Rahmen des Verfahrens vor dem OLG Karlsruhe zu berücksichtigende Wettkampfordnung vor, dass sich alle Mitglieder der verbandsangehörigen Vereine damit einverstanden erklären, dass u. a. auch personenbezogene Strafübersichten auf der Verbands-Homepage veröffentlicht werden. Dies hat bei der Urteilsfindung des OLG Karlsruhe eine wesentliche Rolle gespielt - insoweit ist dieses Urteil also nicht ohne Weiteres auf andere Verbände übertragbar. Die für den Fußball im Freistaat Sachsen einschlägige Spielordnung des Sächsischen Fußball-Verbandes enthält jedenfalls keine derartige Regelung.

4.2.2.2 Veröffentlichung von Schiedsrichterlisten

Ein Fußballkreisverband hatte seine aktuelle Schiedsrichterliste auf seiner Homepage veröffentlicht. Die Liste enthielt Namen, Vornamen, Sportverein, Privatanschrift, private Festnetz- und Mobilfunknummer sowie E-Mail-Adresse. Begründet worden war dies damit, dass die diesbezüglichen Meldungen nicht rechtzeitig zur Drucklegung des Ansetzungsheftes beim Kreisverband eingegangen waren und daher den Vereinen auf andere Weise zur Kenntnis gegeben werden mussten.

Da eine wirksame Einwilligung der Betroffenen in diese Internetveröffentlichung nicht eingeholt worden war, war die Zulässigkeit der Veröffentlichung (Übermittlung) der privaten Kontaktdaten der Schiedsrichter nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG zu beurteilen, d. h. die Datenübermittlung musste zur Wahrung berechtigter Interessen des Fußballkreisverbandes erforderlich sein und es durfte kein Grund zu der Annahme bestehen, dass entgegenstehende schutzwürdige Betroffeneninteressen überwiegen. Diese Voraussetzungen waren vorliegend jedoch nicht erfüllt.

Ein berechtigtes Interesse des Fußballkreisverbandes an der Bekanntgabe der Kontaktdaten der Schiedsrichter war allenfalls bezogen auf einen eng begrenzten Adressatenkreis, nämlich der innerhalb der Vereine unmittelbar mit der Organisation und Überwachung des Spielbetriebs befassten Personen, zu erkennen. Auch hier beschränkten sich die (im Fall des Nichterscheinens des Schiedsrichters) notwendigen Daten aber im

Grunde genommen auf eine Telefonnummer und vielleicht noch den Wohnort. Die in den Vereinen für den Spielbetrieb verantwortlichen Personen erhalten diese Informationen regelmäßig über das Ansetzungsheft. Da im konkreten Fall eine Aufnahme der Schiedsrichterliste in das Ansetzungsheft aus drucktechnischen Gründen nicht möglich gewesen war, hätte diese Liste nachträglich auf die gleiche Weise (Postweg) wie das Ansetzungsheft an die verantwortlichen Personen in den Vereinen verteilt werden können und müssen. Mit einer Veröffentlichung wird dieser Zweck zwar auch erreicht, jedoch ist damit auch bewirkt worden, dass darüber hinaus auch noch die (weltweite) Öffentlichkeit über die privaten Kontaktdaten der (auch) als Schiedsrichter tätigen Personen informiert wird. Dies ist aber für die Durchführung des Spielbetriebes in keiner Weise erforderlich. Schon aus diesem Grund war die Veröffentlichung im Internet also unzulässig.

Darüber hinaus standen der Veröffentlichung aber auch überwiegende schutzwürdige Betroffeneninteressen gegenüber. Schiedsrichter stehen naturgemäß besonders im Blickpunkt der Öffentlichkeit. Sie müssen auch unpopuläre Entscheidungen treffen und sind auch nicht vor Fehlentscheidungen gefeit. Dies setzt sie insbesondere auch außerhalb des Spielbetriebs zweifellos besonderen Risiken, z. B. Belästigungen durch Spieler oder Zuschauer, aus. Sie haben daher ein schutzwürdiges Interesse daran, dass ihre privaten Kontaktdaten nicht jedermann bekannt werden.

Der betreffende Fußballkreisverband hat die Schiedsrichterliste daraufhin sofort von seiner Homepage entfernt.

4.2.2.3 Veröffentlichung von Sportergebnissen bei Beteiligung von Häftlingen

Werden auf Vereins- oder Verbandsebene Spielergebnisse, beispielsweise im Schachsport, mit den Namen der Aktiven im Internet veröffentlicht, so kann sich die Zulässigkeit derartiger Veröffentlichungen aus § 28 Abs. 1 Satz 1 Nr. 3 BDSG ergeben. Nach dieser Vorschrift ist eine Veröffentlichung allgemein zugänglicher Daten zulässig, wenn nicht das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Veröffentlichung das berechtigte Interesse der verarbeitenden Stelle offensichtlich überwiegt.

Die von einem Verein oder Verband ausgerichteten Wettkämpfe sind regelmäßig öffentlich. Die Namen und die Ergebnisse der Aktiven werden im Rahmen eines Turniers bzw. Spieltages regelmäßig öffentlich bekannt gegeben. Es handelt sich damit um allgemein zugängliche Daten. Auch sind keine Anhaltspunkte dafür ersichtlich, dass hier das schutzwürdige Interesse der Aktiven an einem Ausschluss der Veröffentlichung gegenüber dem berechtigten Interesse des Verbandes offensichtlich überwiegt. Zwar lassen sich die Daten im Internet für einen unbegrenzten Teilnehmerkreis erschließen

und stehen sie anders als bei anderen Medien zumeist über einen längeren Zeitraum zur Verfügung, jedoch ist nicht anzunehmen, dass eine Internetveröffentlichung der genannten Daten die Persönlichkeit eines Aktiven in besonderer Weise beeinträchtigt. Dies gilt insbesondere dann, wenn lediglich Namen, Vereinszugehörigkeit und Partie- bzw. Turnierergebnis veröffentlicht werden. Dem Wettkampfbetrieb ist öffentlicher Leistungsvergleich immanent. (Im Schach kommt das fachliche Interesse am Spielverlauf dazu. Der Übergang zur dem akademischen Wissenschaftsbetrieb eigenen Öffentlichkeit liegt da nicht mehr fern.)

Im Schachsport ist es allerdings mitunter Praxis, dass auch Mannschaften von Justizvollzugsanstalten (Mitarbeiter und Insassen) am Spielbetrieb teilnehmen, dies natürlich - aus nachvollziehbaren Gründen - nur mit „Heimspielen“ bzw. „Heimturnieren“.

Derartige Turniere weisen Besonderheiten auf: Dies ist zum einen der Ort des Turniers, zum anderen ist es die Tatsache, dass gerade auch Insassen der JVA an diesen Wettkämpfen teilnehmen. Vor diesem Hintergrund wird man zunächst wohl nicht mehr von einem in der Öffentlichkeit stattfindenden Wettkampf sprechen können. Daher kann die Zulässigkeit der Veröffentlichung nicht auf § 28 Abs. 1 Satz 1 Nr. 3 BDSG gestützt werden. Als Erlaubnisvorschrift kommt insoweit § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Frage. Diese Vorschrift verlangt neben dem berechtigten Interesse an der Veröffentlichung im Internet, dass diese zur Wahrung des berechtigten Interesses der verantwortlichen Stelle erforderlich ist, d. h. dass ohne diese Veröffentlichung die damit verfolgten Zwecke nicht mehr erreicht werden könnten. Weder für die Durchführung des Spielbetriebes noch für die Außendarstellung des jeweiligen Verbandes ist es aber zwingend notwendig, dass Einzelergebnisse der Wettkampfteilnehmer im Internet dargestellt werden. Für die Steuerung und Überwachung des Spielbetriebes genügt es, wenn die Spielergebnisse verbandsintern dokumentiert werden; für die Außendarstellung reichen insoweit vereins- bzw. mannschaftsbezogene Angaben aus. Darüber hinaus darf nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG auch kein Grund zu der Annahme bestehen, dass das schutzwürdige Interesse der Betroffenen am Ausschluss der Veröffentlichung überwiegt. Diese Voraussetzung ist vorliegend ganz sicher nicht erfüllt. Denn die Tatsache, dass man einer JVA-Mannschaft angehört, identifiziert den Betroffenen mit hoher Wahrscheinlichkeit als Straftäter. Dies liegt keinesfalls im Interesse des davon betroffenen Personenkreises.

Hinsichtlich derjenigen Teilnehmer, die nicht ausdrücklich einer JVA-Mannschaft zugeordnet sind, sollte durch einen allgemeinen Hinweis klargestellt werden, dass sie als von außen kommende Besucher am Wettkampf in der JVA teilgenommen haben. Andernfalls müsste wegen der in diesem Falle insoweit bestehenden Unklarheit auch

die Einwilligung der externen Teilnehmer in eine Veröffentlichung ihrer Teilnahme (und ihres Spielergebnisses) eingeholt werden.

Betreffend die JVA-Teilnehmer verbleibt nur die Möglichkeit der schriftlichen Einwilligung der - eben als JVA-zugehörig gekennzeichneten - Betroffenen (§ 4a BDSG). Im Falle einer fehlenden Einwilligung würde es genügen, wenn in der Ergebnisliste auf die Namensnennung verzichtet würde, d. h. sich dort bei der betreffenden Person auf die Nennung der Mannschaft, der Brett-Nummer und des Ergebnisses zu beschränken. Letzteres ist als Vorzugsvariante anzusehen, denn eine Einwilligung nach § 4a BDSG ist jederzeit widerrufbar, die veröffentlichten Ergebnislisten müssten mithin also im Falle eines Widerrufes auch nachträglich geändert werden. Alternativ wäre bei JVA-Insassen zu überlegen, ob diese unter einem festen Pseudonym spielen könnten; damit ließe sich vielleicht das schutzwürdige Interesse an Identitätsverschleierung gegenüber Dritten mit dem Interesse, als Spielerpersönlichkeit in seiner Identität innerhalb des Schachsportbetriebes wahrgenommen zu werden, verbinden. (Bekanntlich wird auf internationalen Schachspiel-Plattformen im Internet vielfach unter festem Pseudonym gespielt.)

4.2.2.4 Veröffentlichung einer Schwarzen Liste

Die Eingabe des eigenen Namens in eine Suchmaschine hat wohl ein jeder Internetnutzer schon einmal probiert. Mitunter stößt man dabei auch auf unerwartete Ergebnisse. So der Fall eines Petenten, der auf diese Weise erfahren hatte, dass er mit seiner vollständigen Adresse auf der Schwarzen Liste eines Unternehmens gelandet war. Bei dieser Liste handelte es sich offensichtlich um eine interne Liste, die mit „Lager A Mitarbeiterinfo - Kunden mit Außenständen / Liefersperre“ überschrieben war.

Solange eine derartige Liste lediglich für interne Zwecke verwendet wird, ist dagegen nichts einzuwenden (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG). Anders verhält es sich jedoch, wenn diese Liste veröffentlicht wird. Wegen der damit in der Öffentlichkeit verbundenen Prangerwirkung und weil es sich zudem um nicht von dritter Seite objektiv festgestellte Daten mit für den Betroffenen nachteiligen Angaben handelt, ist das schutzwürdige Interesse der Betroffenen am Ausschluss der Veröffentlichung höher zu bewerten als das diesbezüglich gegebenenfalls bestehende Interesse der verantwortlichen Stelle, Dritte vor diesen Personen zu warnen. Die Veröffentlichung der Schwarzen Liste war demnach unzulässig.

Angesichts der Tatsache, dass die betreffende Webseite nur noch über den Google-Cache erreichbar war, war davon auszugehen, dass die verantwortliche Stelle diese

Auffassung teilte bzw. dass es sich bei der vorangegangenen Veröffentlichung lediglich um ein technisches Versehen gehandelt hatte.

Um jedoch auch die aus der weiterhin bestehenden Abrufbarkeit der Schwarzen Liste resultierende Persönlichkeitsrechtsbeeinträchtigung der betroffenen Personen schnellstmöglich zu unterbinden, war es darüber hinaus notwendig, dass sich die verantwortliche Stelle als Domain-Inhaber umgehend mit Google in Verbindung setzte und dort die Löschung dieser Seite aus dem Cache veranlasste.

4.2.2.5 Offenlegung von Nutzerdaten

Infolge einer unzureichend abgesicherten Softwareumstellung (Programmierfehler in Verbindung mit unzureichenden Tests und einer zu frühen Freigabe der Software; fehlende Kontrolle der ordnungsgemäßen Funktion der Software nach deren Aktivierung) waren über ein Wochenende hinweg Bestandsdaten (Namen, Anschrift bzw. Geburtsdatum) von mehr als 10.000 Kunden eines Internetportals der Öffentlichkeit frei zugänglich.

Die Ursache der Veröffentlichung lag in letztendlich unzureichenden Tests und damit einer zu frühen Freigabe einer maßgeblich veränderten Software für das betreffende Internetportal. Zudem war es versäumt worden, zumindest für die ersten Tage nach der Softwareumstellung besondere Vorkehrungen für die Überwachung einer ordnungsgemäßen Funktionsweise dieser Software zu treffen und damit eine schnelle Reaktion auf etwaige Vorkommnisse sicherzustellen. Soweit eine neue Software also - wie geschehen - an einem Freitag in Betrieb genommen wird, gehört dazu auch, dass zumindest über das folgende Wochenende hinweg eine umgehende Reaktion auf eingehende Fehlermeldungen oder Beschwerden sichergestellt wird. Stattdessen war bei dem betreffenden Unternehmen das gesamte Wochenende über niemand erreichbar, der auf die diesbezüglichen zahlreichen Nutzerbeschwerden sofort hätte reagieren können.

Gemäß § 14 Abs. 1 TMG dürfen Diensteanbieter personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind. Eine - wenn auch unbeabsichtigte - Veröffentlichung der Bestandsdaten war für die in § 14 Abs. 1 TMG genannten Zwecke nicht erforderlich und stellte demnach einen - gemäß § 16 Abs. 2 Nr. 5 TMG bußgeldpflichtigen - Verstoß gegen diese Vorschrift dar. Der Verstoß ist durch das Unternehmen eingeräumt worden.

Für die Ahndung von Verstößen gegen das TMG sind in Sachsen gemäß § 2 OwiZuVO die Landkreise und kreisfreien Städte zuständig. Die diesbezügliche Abgabe an die zuständige Verwaltungsbehörde ist erfolgt.

4.2.2.6 Weitergabe von Zugangsdaten an ein Inkassobüro

Eine Internetnutzerin hatte sich bei einem ihrem Eindruck nach kostenlosen Internetportal angemeldet. Als dann der Portalbetreiber jedoch plötzlich doch Geld verlangte, hielt sie sich für nicht zur Zahlung verpflichtet und forderte die sofortige Löschung der sie betreffenden Eintragungen. Der Portalbetreiber war dazu natürlich nicht bereit und übergab die Angelegenheit einem Inkassounternehmen. Als die Betroffene auch dort ihre Anmeldung bei dem betreffenden Portal in Frage stellte, wurde ihr eine Kopie der vom Portalbetreiber erstellten und an sie versandten Anmeldebestätigung, die u. a. auch ihre Anmeldedaten, insbesondere das persönliche Kennwort, enthielt, vorgelegt.

Die Weitergabe dieser (vollständigen) Anmeldebestätigung an das beauftragte Inkassounternehmen war - jedenfalls was das darauf enthaltene Passwort betraf - unzulässig und damit rechtswidrig.

Sinn und Zweck eines Passwortes ist es, seinen Inhaber in Verbindung mit einem Benutzernamen eindeutig zu authentifizieren, so dass diesem Benutzer alle nachfolgenden Interaktionen (z. B. Bestellungen) eindeutig und nachweisbar zugeordnet werden können. Um dies dauerhaft zu gewährleisten, sind Passwörter nicht nur durch deren Inhaber, sondern natürlich auch durch die jeweils verantwortliche Stelle zwingend geheim zu halten und keinen Dritten zu offenbaren.

Die Weitergabe eines Passwortes an einen Dritten verstößt daher zunächst einmal gegen die Vorschriften des § 9 BDSG, wonach die verantwortliche Stelle technische und organisatorische Maßnahmen zur Verhinderung des unbefugten Datenzugriffs (vgl. insbesondere Nr. 3 der Anlage zu § 9) zu treffen hat. Denn mit der Weitergabe eines Passwortes erreicht man genau das Gegenteil, d. h. man ermöglicht gerade erst einen unbefugten Zugriff durch die Stellen, denen das Passwort weitergegeben worden ist.

Darüber hinaus stellte eine solche Datenübermittlung aber auch eine nach § 14 Abs. 1 TMG unzulässige Datenverwendung dar. Nach dieser Vorschrift dürfen Bestandsdaten (z. B. Passwort) nur verwendet werden, soweit dies für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer erforderlich ist.

Der Portalbetreiber hat diesen Verstoß eingeräumt und darauf zurückgeführt, dass von dem beauftragten Inkassounternehmen Informationen angefordert worden seien, aus

denen sich die Anmeldung der Betroffenen als Nutzerin der betreffenden Internetplattform ergäben. Dabei sei es dann in diesem Einzelfall insofern zu einem Fehlverhalten der damit befassten Mitarbeiterin gekommen, als diese dem Inkassobüro eine vollständige, nicht teilweise geschwärzte Kopie der Anmeldebestätigung zur Verfügung gestellt habe.

Im Übrigen hat der Portalbetreiber mitgeteilt, dass er personenbezogene Daten der auf seiner Internetplattform angemeldeten Nutzer nur für die Dauer des zugrunde liegenden Vertragsverhältnisses, darüber hinaus nur dann und so lange speichere, bis Forderungen aus dem Vertragsverhältnis beglichen worden sind.

Im Fall der - insoweit strittigen - Anmeldung der Petentin bedeutete dies demnach, dass deren Löschungsverlangen bis zur Klärung der - durch die Aufsichtsbehörde nicht zu entscheidenden - nicht-datenschutzrechtlichen zivilrechtlichen Frage (Vorfrage), ob tatsächlich noch eine Forderung aus einem Vertragsverhältnis zwischen dem Portalbetreiber und der Petentin offen war, nicht nachzukommen war. Diese Verfahrensweise stand im Einklang mit der Vorschrift des § 35 Abs. 2 Satz 2 Nr. 3 BDSG, wonach eine Löschungspflicht nur dann bestanden hätte, wenn die Kenntnis dieser Daten für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich gewesen wäre. Davon konnte aber seinerzeit nicht ausgegangen werden.

4.2.2.7 Speicherung von IP-Adressen durch Webhoster

Der Kunde eines sächsischen Web-Hosting-Unternehmens wollte die Protokollierung von IP-Adressen in den durch den Webhoster bezüglich seiner Internetseite erstellten Logfiles unterbinden, um das Siegel „Wir speichern nicht!“ des Arbeitskreises Vorratsdatenspeicherung zu erhalten. Nachdem ihm dies der Webhoster als technisch nicht realisierbar dargestellt hatte, wandte er sich an die Aufsichtsbehörde.

Bei Web-Hosting betreibenden Unternehmen handelt es sich regelmäßig im Rechtssinne um sogenannte Auftragsdatenverarbeiter. Dies bedeutet zunächst, dass grundsätzlich der Auftraggeber, hier also der Website-Inhaber, für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich ist (§ 11 Abs. 1 BDSG). Der Auftragnehmer, hier demnach der Webhoster, darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen (vgl. § 11 Abs. 3 BDSG). Wenn also ein Kunde bzw. Auftraggeber - etwa im Hinblick auf § 15 Abs. 4 TMG - verlangt, die Erhebung und Speicherung von IP-Adressen in einem seinen Internetauftritt betreffenden Logfile zu unterlassen, so ist der Webhoster aus folgenden Gründen verpflichtet, dem nachzukommen:

Richtigerweise ist der Begriff des Personenbezuges eines Datums *relativ*, nämlich bezogen auf denjenigen zu bestimmen, der Kenntnis des Datums erlangt. Das sehen viele Datenschutzrechtler anders, lässt sich aber an praktischen Beispielen leicht beweisen. Die Rechtsprechung ist zurzeit gespalten in der Frage, unter welchen Voraussetzungen bzw. für wen (insbesondere dynamische) IP-Anschriften personenbezogene Daten sind.

Da vom Webhoster nicht zu beeinflussen ist, was seine Kunden auf ihren Internetseiten anbieten, insbesondere welche Daten sie von ihren Nutzern erheben, verarbeiten und nutzen, muss er von der Möglichkeit ausgehen, dass IP-Adressen *für seine Kunden* personenbezogene Daten sind, weil sie eben mit gegebenenfalls darüber hinaus erhobenen personenbezogenen (die Person des IP-Anschriften-Inhabers bestimmbar machenden) Daten zusammengeführt werden können.

Der Webhoster ist dieser Argumentation gefolgt und hat umgehend eine technische Lösung erarbeitet, durch die jeder seiner Kunden nun selbst entscheiden kann, ob die IP-Adressen der Nutzer seines Internetauftritts im Logfile protokolliert werden oder nicht.

4.2.2.8 Veröffentlichung angemeldeter Veranstaltungsteilnehmer

Der Betreiber eines Unternehmer-Netzwerkes hatte seinen Mitgliedern bzw. auch anderen interessierten Personen die Möglichkeit geboten, sich auf seiner Internetseite zu verschiedenen Veranstaltungen anzumelden. Die der Anmeldung vorangestellten Veranstaltungsinformationen enthielten jeweils auch eine Übersicht über diejenigen, die sich bereits als Teilnehmer angemeldet hatten, mit folgenden Daten: Name, Vorname, Firma / Tätigkeit / Branche, Netzwerk-Mitgliedschaft und Personenzahl.

Für diese Veröffentlichung fehlte es an einer Rechtsgrundlage. Weder aus § 28 Abs. 1 Satz 1 Nr. 1 BDSG (Zweckbestimmung eines Vertragsverhältnisses) noch aus § 28 Abs. 1 Satz 1 Nr. 2 BDSG (Interessenabwägung) konnte sich die Zulässigkeit dieser Veröffentlichung ergeben. Für die Veröffentlichung bestand weder eine entsprechende Notwendigkeit noch konnte eine bestimmungsgemäße Verwendung beim Empfänger auch nur ansatzweise sichergestellt bzw. kontrolliert werden. Die Tatsache, dass es für potentielle Teilnehmer sicherlich interessant und u. U. vielleicht auch entscheidungserheblich ist, zu erfahren, wer noch an einer Veranstaltung teilnimmt, reicht zur datenschutzrechtlichen Begründung der Zulässigkeit einer Internetveröffentlichung keinesfalls aus. Schutzwürdige Betroffeneninteressen waren vor allem deswegen verletzt, weil potentielle Veranstaltungsteilnehmer nicht darüber informiert worden waren, dass sie bei Nutzung des Online-Anmeldeformulars automatisch in die darüber befindliche Teil-

nehmerliste aufgenommen werden und zudem kein diesbezüglicher alternativer Anmeldeweg (ohne Veröffentlichung) eröffnet worden war, und weil die Daten zu den Veranstaltungsteilnehmern - dazu gehört insbesondere auch die Tatsache der voraussichtlichen Anwesenheit am Veranstaltungsort bzw. der Abwesenheit von der Arbeitsstelle am jeweiligen Tag - einem unbestimmten weltweiten Empfängerkreis zugänglich gemacht worden sind.

Die daraufhin erfolgte Neuprogrammierung dieses Teils des Webauftrittes sieht seitdem vor, dass eine Veröffentlichung nur bei Markierung eines entsprechenden Feldes erfolgt, wobei als Grundeinstellung „keine Veröffentlichung“ vorgegeben ist, also nur auf Einwilligungsgrundlage.

4.2.2.9 Schreibfehler bei der Adressierung von Werbemails

Ein Hotel hatte E-Mails an ehemalige Übernachtungsgäste versandt und hierfür u. a. die zu diesem Zweck von den Gästen an der Rezeption hinterlassenen Visitenkarten genutzt. Eine solche Werbe-E-Mail erreichte auch eine Person, die glaubhaft machen konnte, dieses Hotel noch nie betreten und dort auch keine E-Mail-Adresse hinterlassen zu haben.

Das Hotel legte der Aufsichtsbehörde dann jedoch das Hotel-Anmeldeformular eines Kunden mit identischem Vor- und Nachnamen, jedoch abweichenden Wohnanschriftsdaten vor. Die Darstellung des Hotels, wonach höchstwahrscheinlich ein Fehler bei der Übertragung der tatsächlich außerhalb des Hotel-Meldezettels, angeblich mittels Visitenkarte, angegebenen E-Mail-Adresse ins elektronische Adressbuch des Hotels zu einem falschen Adressaten geführt habe, konnte - da die entsprechende Visitenkarte, wie es hieß, nach Übertragung der E-Mail-Adresse vernichtet worden war - weder bestätigt noch widerlegt werden, erschien jedoch angesichts der Tatsache, dass die E-Mail-Adresse des Petenten nach der Struktur: *Vorname.Nachname@Domainname* aufgebaut war, durchaus glaubwürdig.

An diesem Vorgang zeigt sich, dass im Umgang mit elektronischer Post besondere Sorgfalt geboten ist, weil sich E-Mail-Adressen - unvergleichlich leichter als herkömmliche postalische Adressen - durch einen geringfügigen Schreibfehler so verändern können, dass sie nicht unbedingt gegenstandslos sind, sondern einen tatsächlich existierenden und auf diese Weise ohne Weiteres zu erreichenden anderen Adressaten bezeichnen können. Das Hotel hat daraufhin seine internen Geschäftsabläufe überarbeitet und insbesondere vorgesehen, dass E-Mail-Adressen bei der manuellen Übernahme in den Adressverteiler zur Sicherheit noch ein zweites Mal abgefragt werden. Meiner Meinung nach ist darüber hinaus auch eine entsprechende Quellendokumentation erforderlich,

damit einem diesbezüglichen Auskunftsverlangen des Betroffenen (vgl. § 34 Abs. 1 Nr. 1 BDSG) entsprochen werden kann.

Allerdings hat sich dabei im Ergebnis die Unzuständigkeit der Aufsichtsbehörde für den Vorgang herausgestellt: Zumindest der lediglich *versehentliche* Versand von E-Mails an Unbekannt liegt außerhalb des Anwendungsbereiches des Bundesdatenschutzgesetzes und damit außerhalb der Zuständigkeit der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich, weil für den Verwender der Internet-Postanschrift nach seinem Wissensstand nicht einmal Erkenntnisse darüber vorliegen, dass es die Internet-Postanschrift gibt, und nach Ausbleiben einer Fehlermeldung noch nicht gesichert ist, dass ein Mensch gleichen bürgerlichen Namens Inhaber der betreffenden Internet-Postanschrift ist, geschweige denn, dass im anderen Falle der Name, von Fällen der Prominenz bzw. sehr seltener Namen abgesehen, für den Verwender mehr als „Schall und Rauch“ ist, also die betreffende Kenntnis des Verwenders (Namensinhabers) dessen reale Person tangiert.

Das ändert allerdings nichts daran, dass die Verwendung des bürgerlichen Namens (Klarnamens) als Bestandteils der Anschrift für elektronische Post die Zuordnung zu sonstigen (unmittelbaren) Identifikatoren (Anschriften in Telefonverzeichnissen o. ä.) im Vergleich zu stattdessen verwendeten pseudonymen Anschriften-Bestandteilen erheblich erleichtert. Dies sollten Nutzer von E-Post-Anschriften berücksichtigen, zumal Erwerb und Nutzung solcher Anschriften weder ein technisches noch ein wirtschaftliches Problem darstellen.

4.2.2.10 Identitätsmissbrauch bei Bestellungen

Eine Kontoinhaberin war mit einer Abbuchung belastet worden, für die sie keine Erklärung hatte. Da sie dies rechtzeitig bemerkt hatte, bereitete es ihr kein Problem, diese Lastschrift durch Widerspruch gegenüber der Bank wieder rückgängig zu machen. Um zu erfahren, wie es zu dieser Lastschrift gekommen war, richtete sie ein Auskunftsverlangen an den Einreicher der Lastschrift, ein im Internethandel tätiges Unternehmen. Da sie hierauf keine Antwort erhielt, schaltete sie die Aufsichtsbehörde ein. Die daraufhin durchgeführten Ermittlungen haben dann bestätigt, dass die Bestellung nicht von der Petentin aufgegeben war, sondern allem Anschein nach ein Dritter, der die Bestellung aufgegeben und die Ware geliefert bekommen hatte, deren Kontodaten missbraucht hatte.

Dies war nicht der einzige Fall, in dem die Aufsichtsbehörde mit einem Identitätsmissbrauch konfrontiert war. Ähnliche Vorfälle gibt es zwar auch in der Offline-Welt, etwa wenn bei einem Versandhaus unter einer kurzzeitigen Briefkastenadresse bestellt

wird, jedoch ist dies im Internet wesentlich einfacher zu realisieren, jedenfalls dann, wenn es zwischen Bestellung und Bezug der Ware oder Dienstleistung keinen Medienbruch gibt, d. h. wenn das gewünschte Produkt nicht per herkömmlicher Post an eine konkrete nachvollziehbare Wohn-Anschrift geliefert wird, sondern die Leistungserbringung gleichfalls direkt über das Internet erfolgt. Dies ist beispielsweise der Fall bei kostenpflichtigem Abruf von Inhalten von Datenbanken, deren Zugangsdaten gleich per E-Mail versandt werden. Soweit einem Dritten in einem solchen Fall Name, Anschrift, ggf. Geburtsdatum und natürlich Kontodaten einer real existierenden Person bekannt sind, kann er diese in Verbindung mit seiner eigenen, nur für diesen Zweck bei einem Freemailer zugelegten E-Mail-Adresse bei der Anmeldung zu einem Online-Dienst angeben. Bis dieser Missbrauch erkannt und der Zugang gesperrt wird, etwa als Reaktion auf eine Rücklastschrift, kann eine geraume Zeit vergehen, in der der Dritte de facto kostenlos das betreffende Internetangebot hat nutzen können. Da nicht jeder Kontoinhaber regelmäßig seine Kontobewegungen gründlich genug überprüft, kann es durchaus auch vorkommen, dass ein solcher Missbrauch unerkannt bleibt. Es sind auch Fallgestaltungen bekannt geworden, in denen bei sofortiger Gewährung der Zugangsberechtigung eine Zahlung auf - natürlich durch E-Mail übersandte - Rechnung und somit per Überweisung vorgesehen war. Wiederum lediglich per E-Post versandte Zahlungserinnerungen bzw. Mahnungen haben natürlich nur den tatsächlichen Nutzer der Zugangsberechtigung erreicht und durch diesen nicht weiter beachtet werden müssen. Erst als dann ein Inkassounternehmen beauftragt worden war, welches sich mit herkömmlicher Post an den vermeintlichen Schuldner wandte, ist in diesen Fällen der ganze Schwindel aufgeflogen.

Derartige Missbräuche können nur dann weitgehend ausgeschlossen werden, wenn die Vertragsbestätigung einschließlich der Zugangsdaten in solchen Fällen per herkömmlicher Post an die jeweiligen Kunden versandt oder andere Zahlungsverfahren eingesetzt werden. In erster Linie sind hier also Aktivitäten der entsprechenden Inhaltsanbieter gefragt. Unabhängig davon sollten diese Fälle jedem die Notwendigkeit einer regelmäßigen und sorgfältigen Überprüfung seiner Kontobewegungen sowie eines sorgsamen und zurückhaltenden Umgangs mit den eigenen Daten verdeutlichen.

Ein *spezifisch* datenschutzrechtliches Fehlverhalten des Internethandelsunternehmens hat danach nicht vorgelegen: Der in gutem Glauben vorgenommene Zugriff auf das vom Käufer angegebene Konto eines unbeteiligten Dritten geht zwar mit objektiv unzulässiger Verarbeitung personenbezogener Daten einher. Soweit der Verkäufer jedoch aufgrund der ihm gemachten Angaben davon ausgehen darf, dass Käufer und Kontoinhaber identisch sind, darf er aber subjektiv von einer Erlaubtheit der mit der vertragsgemäßen Abwicklung (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG) und der dazu gehörenden

Einzugsermächtigung verbundenen Verarbeitungshandlungen ausgehen. Das ist dann zwar objektiv datenschutzrechtlich rechtswidrig, aber es fehlt in Fällen wie diesem am Verschulden und es besteht wohl auch keine Wiederholungsgefahr.

Allerdings hatte das Unternehmen seine datenschutzrechtliche Auskunftspflicht nach § 34 Abs. 1 BDSG erst nach Einschalten der Aufsichtsbehörde erfüllt. Dass im Lastschriftverfahren schon die Angabe einer Kontonummer ausreicht, ohne dass zusätzlich der Name des Kontoinhabers zutreffend benannt sein muss, erscheint bankrechtlich befremdlich.

4.2.2.11 Authentifizierung im E-Commerce

Mehrfach erreichten die Aufsichtsbehörde Fragen und Beschwerden von Internetnutzern, die von Inhaltsanbietern zwecks Authentifizierung zur Übersendung von Ausweiskopien aufgefordert wurden. An deren Einreichung war beispielsweise die Auszahlung von Vergütungen oder Gewinnen geknüpft. Die Firmen begründeten dies u. a. mit Vorgaben des Jugendschutzes sowie der Betrugsbekämpfung.

Ein Authentifizierungsverlangen im Geschäftsverkehr ist mit datenschutzrechtlichen Vorschriften in der Regel vereinbar. Gemäß § 4 Abs. 1 PersAuswG kann das Personaldokument sehr wohl auch im nicht-öffentlichen Bereich zu Ausweis- und Legitimationszwecken benutzt werden. Allerdings ist die Vorlage eines Personaldokuments grundlegend verschieden von der Überlassung einer Ausweiskopie. Ein bloßes Vorzeigen beinhaltet nicht den datenschutzrechtlich relevanten Vorgang der Speicherung aller manuell auslesbaren Merkmale. Die Aushändigung einer Kopie hingegen ist wegen der damit verbundenen Datenspeicherung auf der Grundlage der Vorschriften des Bundesdatenschutzgesetzes zu beurteilen.

Eine insoweit im Regelfall nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG zulässige Erhebung, Verarbeitung und Nutzung personenbezogener Daten setzt dabei voraus, dass sie der Zweckbestimmung des Vertragsverhältnisses, mithin also auch der Authentifizierung, dient. Dies trifft zweifelsfrei nur für einen Teil der in einem Personalausweis enthaltenen Daten zu. E-Commerce-Kunden können daher geltend machen, diejenigen Daten schwärzen zu dürfen, deren Erhebung für den angegebenen Zweck nicht erforderlich sind. Den Nachweis der Erforderlichkeit hat der E-Commerce-Betreiber zu führen. Ohne dass ein etwaiges Erfordernis weiterer Merkmale begründet wird oder offenkundig ist, sollten die folgenden Merkmale zur Authentifizierung ausreichen:

- Name, Vornamen
- Geburtsdatum und -ort
- Gültigkeitsdauer des Dokuments

- Unterschrift
- Anschrift

Dies bedeutet, dass insbesondere die Ausweisnummer, die Körpermerkmale sowie der maschinenlesbare Teil geschwärzt werden können. AGB, die pauschal eine vollständig lesbare Ausweiskopie verlangen, sind daher mit dem Bundesdatenschutzgesetz nicht vereinbar.

Ein weiteres, in diesem Zusammenhang von mir festgestelltes Problem ist die Übermittlung der Ausweiskopie als Bilddatei an den jeweiligen Anbieter. Soweit diesbezüglich eine unverschlüsselte Eingabemöglichkeit im Internetauftritt angeboten oder die Zusendung per E-Mail vorgeschlagen wird, widerspricht dies den Vorgaben der Nr. 4 der Anlage zu § 9 BDSG, wonach zu gewährleisten ist, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Ungeachtet dessen bestehen aber auch generelle Zweifel an der Eignung einer - auch teilgeschwärzten - Ausweiskopie für eine sichere und zweifelsfreie Authentifizierung des Nutzers, denn abgesehen von den bei einer elektronischen Übertragung oder dem Versand einer Papier- oder Faxkopie bestehenden Fälschungsmöglichkeiten erlaubt es dieses Verfahren nicht, auch den tatsächlichen Bezug auf die Person zu prüfen, die eine solche Kopie vorlegt. Inhaltsanbietern ist daher stattdessen die Nutzung des PostIdent-Verfahrens oder des IdentitätsChecks der SCHUFA zu empfehlen, zukünftig möglicherweise De-Mail.

4.2.3 Arbeitnehmerdatenschutz

4.2.3.1 Fremdbestimmte Selbstauskünfte bei Sicherheitsunternehmen

Ein bereits seit mehreren Jahren bei einem privaten Sicherheitsunternehmen beschäftigter Mitarbeiter war von seinem Arbeitgeber aufgefordert worden, zum Zwecke der Zuverlässigkeitsüberprüfung eine Selbstauskunft beim LKA Sachsen einzuholen und ihm diese unverzüglich nach Erhalt auszuhändigen. Die datenschutzrechtliche Überprüfung dieses Sachverhaltes ergab, dass der Arbeitgeber hierzu nicht berechtigt war:

§ 28 Abs. 1 Satz 1 Nr. 1 BDSG erlaubt das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel zur Erfüllung eigener Geschäftszwecke, wenn es der Zweckbestimmung des Arbeitsverhältnisses mit dem Betroffenen dient. Bei Arbeitsverträgen dienen nur die Daten der Zweckbestimmung des Vertragsverhältnisses, die einen Bezug zur konkreten Tätigkeit aufweisen. Deren Erhebung, Verarbeitung und Nutzung ist zulässig, wenn die Erforderlichkeit gegeben ist

und sie nicht aufgrund arbeitsrechtlicher Besonderheiten, insbesondere der von der Rechtsprechung entwickelten Grundsätze verboten ist. Der Persönlichkeitsschutz ist dabei auch im Arbeitsverhältnis zu wahren, weshalb Eingriffe jeweils im Einzelfall einer Güter- und Interessenabwägung bedürfen. Im konkreten Fall definiert die Bewachungsverordnung die für die Zuverlässigkeitsüberprüfung anzuwendenden Grundsätze und präzisiert insoweit die allgemeinen Regelungen des § 28 BDSG.

Demnach hat ein Unternehmer zum Zwecke der Zuverlässigkeitsprüfung neu einzustellendes Wachpersonal der Gewerbebehörde nach Maßgabe des § 9 BewachV zu melden. Ohne eine derartige Überprüfung darf die Tätigkeit nicht ausgeübt werden. § 9 BewachV regelt diesbezüglich zum einen, dass die Überprüfung der Zuverlässigkeit grundsätzlich anhand einer unbeschränkten Auskunft nach § 41 Abs. 1 Nr. 9 BZRG zu beurteilen ist. Daneben können die Gewerbeämter aber auch andere Erkenntnisquellen nutzen, beispielsweise zusätzliche Auskünfte aus dem Gewerbezentralregister oder von der Industrie- und Handelskammer.

In § 9 Abs. 2 Satz 2 BewachV wird für bestimmte Wachleute außerdem die Möglichkeit einer vertieften Zuverlässigkeitsüberprüfung geschaffen: So kann die zuständige Behörde bei Wachpersonen, die mit Schutzaufgaben von Objekten beauftragt werden sollen, von denen im Falle eines kriminellen Eingriffs eine besondere Gefahr für die Allgemeinheit ausgehen kann, zusätzlich bei der Verfassungsschutzbehörde die Abfrage im NADIS veranlassen.

Dem Arbeitgeber darf gemäß § 34a Abs. 3 GewO das Ergebnis der Überprüfung einschließlich der für die Beurteilung der Zuverlässigkeit erforderlichen Daten mitgeteilt werden. Diese Vorschrift bildet die datenschutzrechtliche Grundlage für die Übermittlung des Ergebnisses der Zuverlässigkeitsüberprüfung durch die Gewerbebehörde an den Bewachungsgewerbetreibenden. Die Übermittlungsbefugnis wird dabei auf solche Daten beschränkt, die der Beurteilung der Zuverlässigkeit zugrunde zu legen sind.

Aus dem dargestellten Sachverhalt ergibt sich also, dass nicht der Arbeitgeber für die Zuverlässigkeitsüberprüfung zuständig ist, sondern die jeweilige Gewerbebehörde. Eine Befugnis zur Erhebung von Daten aus beim LKA eingeholten Selbstauskünften zum Zweck der Zuverlässigkeitsprüfung ergibt sich daher weder aus § 28 BDSG noch aus § 9 BewachV.

Werden demnach also Arbeitnehmer aufgefordert, in eine Auskunftsbitte des Arbeitgebers bei der Polizei oder dem Verfassungsschutz einzuwilligen oder die dort selbst eingeholte Auskunft („fremdbestimmte Selbstauskunft“) dem Arbeitgeber vorzulegen, so wird dadurch das mit den genannten Vorschriften verfolgte Ziel, dem Arbeitgeber

nicht alle, sondern nur die nach dem Bundeszentralregistergesetz zulässigen polizeilichen Informationen zu einer Person („Führungszeugnis“) verfügbar zu machen, ersichtlich unterlaufen. Eine über die Abfrage beim Bundeszentralregister hinausgehende Datenerhebung wird insbesondere auch nicht dadurch zulässig, dass hierzu die Einwilligung des Mitarbeiters eingeholt wird. Es ist offensichtlich, dass in Arbeitsverhältnissen von der für eine Einwilligung erforderlichen Freiwilligkeit des Betroffenen nicht ausgegangen werden kann. Der betroffene Arbeitnehmer steht im Arbeitsverhältnis stets unter dem faktischen Druck des Wohlverhaltens zum Zwecke der Sicherung seines Arbeitsplatzes.

Die Gewerbeämter werden im Übrigen auch im laufenden Arbeitsverhältnis von der Staatsanwaltschaft bzw. dem Gericht über Strafsachen unterrichtet, deren Tatvorwurf Zweifel an der Zuverlässigkeit begründet. Diese in § 15 BewachV enthaltene Regelung soll sicherstellen, dass die Angehörigen des Bewachungsgewerbes über die für diese Branche in besonderem Maße notwendige Zuverlässigkeit nicht nur anfänglich, sondern auch während der gesamten Dauer ihrer Tätigkeit verfügen.

4.2.3.2 Aushängen von Geburtstagslisten in Betriebsräumen

Einem anonymen Hinweis zufolge sollten in einem mittelständischen Unternehmen an mehreren Stellen Geburtstagslisten (Name, Vorname, vollständiges Geburtsdatum) aushängen. Die Eingabe als solche war zwar anonym gehalten, jedoch war der dargestellte Sachverhalt hinreichend glaubhaft dargelegt, insbesondere lag dem Schreiben auch eine Kopie der ausgehängten Liste bei.

Wenn in einem Unternehmen in dieser Weise Geburtstagslisten ausgehängt werden, handelt es sich um ein „Nutzen“ personenbezogener Daten (§ 3 Abs. 5 BDSG); und weil auch Personen, die nicht mit der notwendigen Verwaltung der Geburtstagsdaten betraut sind oder zur Geschäftsführung gehören, von diesen Daten Kenntnis nehmen können, handelt es sich auch um eine Übermittlung (§ 3 Abs. 4 Satz 2 Nr. 3 BDSG).

Die Zulässigkeit dieser Datenverwendungen ergibt sich weder aus dem Bundesdatenschutzgesetz noch aus einer sonstigen Rechtsvorschrift. Sie dienen insbesondere nicht der Zweckbestimmung des Arbeitsvertrages gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG. Auch bei der alternativ nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG durchzuführenden Interessenabwägung ergibt sich keine Zulässigkeit für das Aushängen der Geburtstagsdaten. Diesbezüglich ist einerseits kein berechtigtes Interesse des Arbeitgebers zu erkennen, andererseits wird man annehmen müssen, dass schutzwürdige Interessen zahlreicher Arbeitnehmer am Ausschluss dieser Datenverwendungen bestehen.

Gemäß § 4 Abs. 1 BDSG bleibt damit als Alternative nur die individuelle Einwilligung aller Mitarbeiter. § 4a BDSG schreibt diesbezüglich die Schriftform vor; darüber hinaus sind die Mitarbeiter in diesem Zusammenhang vorab auf den vorgesehenen Zweck der Erhebung, Verarbeitung und Nutzung hinzuweisen. Die Einwilligung ist dabei nur wirksam, wenn sie auf der freiwilligen Entscheidung des Betroffenen beruht.

Obwohl das betreffende Unternehmen (daraufhin) eine diesbezügliche Unterschriftsliste anfertigen ließ und der Aufsichtsbehörde vorlegte, konnte dies den Aushang der Geburtstagslisten nicht rechtfertigen. Auch wenn die Einwilligung in die Erstellung interner Geburtstagslisten in kleineren Unternehmen vielleicht noch hinreichend freiwillig sein mag, war dies für den konkreten Fall, d. h. für ein Unternehmen mit einer Belegschaft von mehr als 50 Personen, auszuschließen. Das Abhängigkeitsverhältnis eines Arbeitnehmers sowie ein gewisser Gruppendruck innerhalb der Belegschaft sprechen gegen eine freie und damit rechtswirksame Einwilligung. Im vorliegenden Fall war es offenkundig, dass diejenigen, die sich (anonym) an die Aufsichtsbehörde gewandt hatten, sich nicht getraut haben, die Unterschrift auf der Einwilligungsliste zu verweigern.

Soweit derartige Initiativen ungeachtet dessen von den Mitarbeitern selbst ausgehen, sich dabei auf die jeweilige Organisationseinheit und entsprechende Vermerke (zweckmäßigerweise ohne Geburtsjahr) in einem Kalender beschränken, wird sich - auch ohne schriftliche Einwilligung - sicher kein Mitarbeiter daran stoßen.

4.2.3.3 Weitergabe der Telefonnummern von Arbeitnehmern zur Angebotserstellung für die betriebliche Altersvorsorge

Der Betriebsratsvorsitzende eines mittelständischen Betriebes berichtete, dass in seiner Firma eine Betriebsvereinbarung zur betrieblichen Altersvorsorge getroffen und ein Versicherungsmakler mit der Durchführung dieser Vereinbarung beauftragt worden war. Dieser hatte Kontakt mit einzelnen Arbeitnehmern unter deren privaten Telefonnummern aufgenommen, um die Möglichkeiten eines Vertragsabschlusses zu erkunden und zu einer Informationsveranstaltung einzuladen.

Im Laufe meiner Ermittlungen hat sich dann herausgestellt, dass der Arbeitgeber dem Versicherungsmakler eine Liste der privaten Telefonnummern seiner Arbeitnehmer ausgehändigt hatte, die die Arbeitnehmer für betriebliche Notfälle angegeben hatten.

Diese Übermittlung der personenbezogenen Daten ist datenschutzrechtlich unzulässig gewesen: Gemäß § 28 Abs. 1 Nr. 1 BDSG ist die Übermittlung personenbezogener Daten für die Erfüllung eigener Geschäftszwecke nur zulässig, wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses

mit dem Betroffenen dient. Ein solches Vertrags- oder Vertrauensverhältnis besteht in dem Arbeitsverhältnis der Mitarbeiter. Diesem Arbeitsverhältnis wird man jedoch auch im Hinblick auf die Betriebsvereinbarung zur Altersvorsorge nicht entnehmen können, dass personenbezogene Daten der Mitarbeiter an Versicherungsmakler weiterzugeben sind. Denn die Weitergabe der Telefonnummern ist dafür nicht erforderlich gewesen. Die Firmenleitung hätte den Versicherungsmakler auch ohne Nennung der privaten Telefonnummern beauftragen und das Ergebnis bzw. weitere Informationen zur Altersvorsorge in einer Informationsveranstaltung bekannt geben können.

Der Arbeitgeber hat im Ergebnis die Telefonliste von dem Versicherungsmakler zurückverlangt und seine Angestellten darüber informiert, dass die privaten Telefonnummern nicht mehr bei dem Versicherungsmakler gespeichert oder aufbewahrt werden.

4.2.3.4 Heimliche Anfertigung einer Festplattenkopie eines Dienst-PC's

Während der urlaubsbedingten Abwesenheit des betroffenen Institutsleiters hatte der Geschäftsführer einer Klinik seinem DV-Leiter die dienstliche Weisung erteilt, umgehend die mutmaßlich im PC des Betroffenen gespeicherte aktuelle Fassung der Hygieneordnung des Krankenhauses zu beschaffen. Dazu hatte der DV-Leiter die durch den Institutsleiter mit einen Boot-Passwort geschützte Festplatte ausgebaut, sie kopiert und sodann wieder in den Rechner eingesetzt. Nur durch Zufall hat der Institutsleiter dies anschließend erfahren und sich daraufhin an die Aufsichtsbehörde gewandt.

Die datenschutzrechtliche Überprüfung hat ergeben, dass die ohne Wissen und Beteiligung des Betroffenen erfolgte Erstellung einer Festplattenkopie eines dienstlichen PC's rechtswidrig gewesen war:

Die Festplatte enthielt eine Vielzahl personenbezogener Daten, einerseits Dritter, insbesondere Patienten, andererseits des Betroffenen selbst. Letztere betrafen zunächst auf die eigene Person bezogene Aufzeichnungen unabhängig davon, ob diese mit dienstlichem oder privatem Hintergrund erfolgt waren, darüber hinaus aber auch Dateien, die - wie beispielsweise auch die gesuchte Krankenhaushygieneordnung - inhaltlich zwar keine personenbezogenen Daten aufwiesen, über die dazugehörigen Metainformationen sowie unter der Annahme einer wirksamen Zugriffskontrolle, d. h. der Beschränkung des Schreib-Zugriffs auf den Institutsleiter, jedoch in vielfältiger Weise mit der Person des Bearbeiters verknüpft waren.

Das Kopieren der Festplatte eines dienstlichen PC's impliziert somit zweifelsfrei eine Erhebung und Speicherung personenbezogener Daten des Arbeitnehmers und wäre nur zulässig gewesen, wenn es der Zweckbestimmung des Arbeitsverhältnisses gedient hätte (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Diesbezüglich ist festzuhalten, dass es dem Arbeit-

geber zwar grundsätzlich zusteht, die Einhaltung der arbeitsvertraglichen Pflichten zu kontrollieren und sich dabei auch die notwendigen Unterlagen oder Arbeitsergebnisse vorlegen zu lassen, jedoch darf der Betroffene dabei, sieht man von Fällen konkreten Verdachtes schwerer, in der Regel strafbarer Verletzungen des Arbeitsvertrages ab, nicht bewusst darüber im Unklaren gelassen werden, dass und wie eine Kontrollmaßnahme stattfindet. Insoweit verletzt jede heimliche, d. h. ohne Wissen des Betroffenen erfolgende Überwachung oder Kontrolle Persönlichkeitsrechte des Arbeitnehmers. Dies gilt bereits für jeden Einzelzugriff auf die persönlichen Speicherbereiche eines Arbeitnehmers, erst recht natürlich für das Abziehen einer kompletten Festplatte. Das Arbeitsverhalten des Institutsleiters wurde dadurch weitgehend erfasst und konnte entsprechend ausgewertet werden.

Nur ausnahmsweise kann in solchen Fällen ein gegenläufiges Arbeitgeberinteresse überwiegen, etwa, wie schon erwähnt, wenn es um die Verhinderung von Straftaten geht oder aber Daten bzw. Dateien dringend und unaufschiebbar benötigt werden und der zugriffsberechtigte Mitarbeiter - aus welchen Gründen auch immer - tatsächlich unerreichbar ist, mithin eine notstandsähnliche Lage vorliegt, in der der Schutz des allgemeinen Persönlichkeitsrechts zurücktritt. Ein solcher Eingriff ist jedoch am Grundsatz der Verhältnismäßigkeit auszurichten, daran hat es in dem betreffenden Fall jedoch gefehlt. Der Betroffene war - obwohl die Möglichkeit dazu im Rahmen eines Telefonats bestanden hatte - nicht über die beabsichtigte Maßnahme informiert worden, zudem hätte das Kopieren der betreffenden Datei ausgereicht. Das Kopieren der gesamten Festplatte ist nicht erforderlich gewesen.

Aus § 87 Abs. 1 Nr. 6 BetrVG ergibt sich zudem in solchen Fällen die Notwendigkeit der Einbeziehung des Betriebsrates, denn die erzeugte Festplattenkopie war, wie dargestellt, zur Verhaltens- und Leistungskontrolle geeignet. Auch die unterlassene Beteiligung des Betriebsrates hat daher dazu beigetragen, die schutzwürdigen Betroffeneninteressen überwiegen zu lassen.

Abschließend festzustellen blieb, dass der Eingriff in das Persönlichkeitsrecht des Betroffenen auch durch geeignete technische und organisatorische Maßnahmen der Klinik hätte verhindert werden können, d. h. gar nicht hätte notwendig werden müssen. Es hatte sowohl an verbindlichen Regelungen darüber, wo (in Netz- bzw. Gruppenlaufwerken) welche Dateien abzuspeichern waren, gefehlt, als auch bezüglich der Privatnutzung dienstlicher Arbeitsmittel. Zudem ist es nicht akzeptabel gewesen, dass einem Mitarbeiter auch der Zugriff auf das BIOS des durch ihn genutzten Rechners erlaubt und somit in Kauf genommen worden war, dass dieser Rechner durch Vergabe eines BIOS- und eines Boot-Passwortes selbst für den Zugriff durch den Administrator gesperrt war.

4.2.4 Gesundheitswesen

4.2.4.1 Zulässigkeit des Outsourcings durch Krankenhäuser

Eine ehemalige Mitarbeiterin und zugleich Patientin einer Klinik hat der Aufsichtsbehörde berichtet, dass die Klinik zunehmend Funktionsbereiche in eine „Management- und Beteiligungsgesellschaft“ auslagere, womit sie nicht einverstanden sei. Dies betreffe u. a. das Archiv, die Systemadministration sowie auch den betrieblichen Datenschutzbeauftragten.

Auch wenn es für die Auslagerung dieser Funktionsbereiche nicht des Einverständnisses der Betroffenen bedurft hat, war die Eingabe der Petentin allerdings insofern begründet, als die vertraglichen Vereinbarungen zwischen der Klinik und ihrem Auftragnehmer in mehreren Punkten nicht den gesetzlichen Anforderungen entsprachen:

Krankenhäuser können sich nach § 33 Abs. 10 SächsKHG zur Verarbeitung von Patientendaten anderer Stellen bedienen, wenn sichergestellt ist, dass diese die Datenschutzbestimmungen dieses Gesetzes und die in § 203 StGB sanktionierte Schweigepflicht einhalten. Die Krankenhäuser sind dabei verpflichtet, erforderlichenfalls den Auftragnehmer anzuweisen, Technik und Organisation der Datensicherung zu ergänzen. Die Auftragserteilung bedarf der vorherigen Zustimmung durch die zuständige Behörde der Krankenhausaufsicht. Der Zustimmung der Patienten bedarf es demnach (wie auch nach Bundesdatenschutzgesetz) nicht.

Von besonderer Bedeutung ist dabei zunächst die Forderung, dass die für Ärzte und ärztliches Hilfspersonal geltende Schweigepflicht auch beim Auftragnehmer, d. h. hier bei der Management- und Beteiligungsgesellschaft, entsprechend einzuhalten ist. Da dessen Mitarbeiter nicht zum ärztlichen Hilfspersonal gehören, findet § 203 StGB keine unmittelbare Anwendung. Für die Praxis bedeutet dies, dass die mit der Verarbeitung von Patientendaten beauftragten Personen nach § 2 Abs. 2 Nr. 2 Verpflichtungsgesetz zur Verschwiegenheit verpflichtet werden müssen. Nur in diesem Fall gehören sie als für den öffentlichen Dienst besonders Verpflichtete zu den in § 203 StGB genannten Personen und können wie Ärzte und ärztliches Hilfspersonal bei einem Bruch des Patientengeheimnisses bestraft werden. Für die förmliche Verpflichtung im konkreten Fall zuständig war der Landkreis.

Der Vertrag zwischen der Klinik und der Management- und Beteiligungsgesellschaft benannte als Vertragsgegenstand nur allgemein die Übertragung von Verwaltungs- und Einkaufstätigkeiten. Bei den unter diesen Vertragsgegenstand fallenden Verarbeitungen (Archivierung, EDV-Administration und -Wartung) handelte es sich um eine Datenverarbeitung im Auftrag. Die diesbezüglichen, nach § 33 Abs. 1 Satz 1 SächsKHG zu

beachtenden Vorgaben des Bundesdatenschutzgesetzes waren dabei allerdings weitgehend unberücksichtigt geblieben. So waren weder die Datenerhebung, -verarbeitung oder -nutzung ausreichend detailliert benannt noch die beim Auftragnehmer zu treffenden technischen und organisatorischen Maßnahmen festgelegt (§ 11 Abs. 2 Satz 2 BDSG). Die (festgestellte) bloße Wiederholung der gesetzlichen Vorgaben (Anlage zu § 9 BDSG) genügt den gesetzlichen Anforderungen zweifelsfrei nicht.

§ 33 Abs. 10 SächsKHG fordert ausdrücklich die vorherige Zustimmung der Krankenhausaufsicht. Ziel der gesetzlichen Regelung ist, dass das Outsourcing von Datenverarbeitungen vor Auftragserteilung noch einmal durch die Aufsichtsbehörde dahingehend geprüft wird, ob diese im Einzelfall zulässig ist und ob hierfür ausreichende vertragliche Vereinbarungen getroffen worden sind. Auch diese Zustimmung lag nicht vor.

Dass die Datenschutzbeauftragte der Klinik gleichfalls bei der Management- und Beteiligungsgesellschaft beschäftigt war, begegnete keinen datenschutzrechtlichen Bedenken. Das Sächsische Krankenhausgesetz verweist insoweit auf die Regelungen des Bundesdatenschutzgesetzes, welches in § 4f Abs. 2 Satz 3 festlegt, dass auch eine Person außerhalb der verantwortlichen Stelle zum Datenschutzbeauftragten bestellt werden kann und das sich deren Kontrollbefugnis auch auf personenbezogene Daten erstreckt, die einem Berufsgeheimnis unterliegen.

4.2.4.2 Unbefugte Einsichtnahme in Patientenakten

Den Medien (Rundfunk, Internet) musste ich entnehmen, dass in einer Messehalle, in der gleichzeitig ein Werksverkauf stattgefunden hatte, Patientenakten gelagert worden waren, was dazu geführt habe, dass ein Mitarbeiter einer Firma für Aktenvernichtung dies habe entdecken sowie eine Trennwand ohne Mühe überwinden und den Lagerbereich sowie einige Dokumente habe fotografieren können. Die Fotos waren anschließend für kurze Zeit im Internet veröffentlicht worden.

Bei der umgehend von mir vorgenommenen örtlichen Überprüfung konnte zunächst festgestellt werden, dass die von dem verantwortlichen Unternehmen in der Zwischenzeit getroffenen Sofortmaßnahmen ausreichend waren, um weiteren unbefugten Zugriff auf die in der Messehalle gelagerten Patientenunterlagen hinreichend wirksam auszuschließen. Insbesondere war der in der Halle durchgeführte Werksverkauf sofort abgebrochen worden, die Halle seitdem nicht mehr für die Öffentlichkeit zugänglich und ein Wachdienst ständig an Ort und Stelle im Einsatz.

Die Überprüfung ergab ferner, dass die betreffende Messehalle zum Teil durch ein in der Archivierung von Schriftgut tätiges Unternehmen gemietet und zur Zwischenlagerung von zur Digitalisierung und anschließenden Vernichtung bestimmten Patienten-

unterlagen genutzt worden war. Die Medienveröffentlichungen waren dabei insoweit unzutreffend gewesen, als die kurzzeitig im Internet veröffentlichten Patientenunterlagen nicht mehr oder weniger zufällig gefunden, sondern zielgerichtet durch den Mitarbeiter eines konkurrierenden Unternehmens durch Überwindung bestehender Sicherungen gegen unbefugten Zutritt beschafft worden waren.

Wie genau sich der Täter Zugang zu dem betreffenden Mietbereich verschafft hat, ist ungeklärt geblieben. Dessen ungeachtet hat dieser Vorfall aber verdeutlicht, dass die getroffenen Sicherungsmaßnahmen unzureichend gewesen sind. Räumliche Sicherungsmaßnahmen müssen wirksam verhindern, dass Unbefugte, insbesondere auch solche, die nicht dem Unternehmen angehören, mit zu erwartendem Aufwand Zugriff auf Unterlagen mit personenbezogenen Daten erhalten können. Dies gilt natürlich auch und gerade dann, wenn die Unbefugten zielgerichtet und mit entsprechend krimineller Energie vorgehen.

Datenschutzrechtlich handelte es sich um einen Fall von Auftragsdatenverarbeitung (vgl. § 11 BDSG). Unbeschadet der diesbezüglichen Pflichten des Auftraggebers hat der Auftragnehmer in eigener Verantwortung zu gewährleisten, dass die ihm überlassenen Datenbestände nur im Rahmen der Weisungen des Auftraggebers (§ 11 Abs. 3 BDSG) verarbeitet werden können. § 11 Abs. 4 BDSG stellt diesbezüglich klar, dass sich die Pflicht, ausreichende Datensicherungsmaßnahmen zu treffen, unmittelbar an den Auftragnehmer richtet. Der Vorfall war daher zumindest in erster Linie unmittelbar dem (im Unterschied zu vielen seiner Auftraggeber meiner örtlichen Zuständigkeit unterliegenden) Auftragnehmer anzulasten.

Die von dem Auftragnehmer getroffenen Sofortmaßnahmen wie auch die in Aussicht gestellten längerfristigen Maßnahmen sind von der Aufsichtsbehörde als ausreichend betrachtet worden, um den Anforderungen des § 9 BDSG zu genügen und weitere diesbezügliche Gefährdungen für die Zukunft auszuschließen.

4.2.4.3 Kundenvermittlung bei Betriebsaufgabe

Der Inhaber eines ‚Instituts für medizinische Ästhetik' hatte im Zuge der Verlagerung seiner Praxis ins Ausland Daten über seinen Kundenstamm in Gestalt der ihm vorliegenden Einverständniserklärungen (Einwilligung in eine konkrete kosmetische Behandlung) an ein Kosmetikstudio übergeben und mit dem Empfänger eine Provisionsregelung für alle auf diese Weise erfolgreich vermittelten Kunden vereinbart. Eine Kundin, die daraufhin ein Werbeschreiben des Kosmetikstudios erhalten hatte, hat sich anschließend bei mir beschwert.

Die Übergabe dieser Einverständniserklärungen durch den ehemaligen Inhaber des Instituts für medizinische Ästhetik war unzulässig gewesen.

Die hierfür in Frage kommenden Erlaubnisnormen des § 28 Abs. 1 Satz 1 Nr. 2 (berechtigtes Interesse des Instituts an der Datenweitergabe) bzw. des § 28 Abs. 3 Satz 1 Nr. 1 BDSG (berechtigtes Interesse des Kosmetikstudios am Erhalt der Kundendaten) setzen jeweils voraus, dass die zu übermittelnden Daten zum Erreichen des beabsichtigten Zweckes erforderlich sind.

Dies war vorliegend nicht zu erkennen. Soweit man nur die Vermittlung der Kunden als Zweck der zur Kundenübernahme abgeschlossenen Vereinbarung ansieht, wäre eine Übermittlung personenbezogener Daten gar nicht erforderlich gewesen, da der bisherige Praxisinhaber hierzu den Kunden auch Empfehlungsschreiben seines vor der Beendigung stehenden Betriebes oder auch Werbeschreiben des Kosmetikstudios selbst hätte übersenden können, auf deren Grundlage sie sich dann beim Kosmetikstudio hätten melden und weiterbehandeln lassen können (Adressmittlungsverfahren). Abgesehen davon hätte es, um darüber hinaus dem Kosmetikstudio als Datenempfänger auch eigene Werbeaktionen zu ermöglichen, im Übrigen ausgereicht, lediglich die Adressdaten der Kunden des Instituts für medizinische Ästhetik zu übermitteln.

Es hat also an der Erforderlichkeit der Weitergabe der (vollständigen) Einverständniserklärungen gefehlt. Der legitime Zweck des Verkaufes der Kundenkontaktdaten hätte ebenso ohne diese oder aber zumindest mit der Übermittlung eines wesentlich kleineren Datensatzes (Beschränkung auf Adressdaten) erreicht werden können.

Die Zulässigkeit der weiteren Speicherung (Aufbewahrung) der Einverständniserklärungen sowie deren Nutzung für eigene Geschäftszwecke durch das Kosmetikstudio war differenziert zu betrachten:

Bei Kunden, die inzwischen bereits wegen einer Weiter- oder Nachbehandlung im Kosmetikstudio vorstellig geworden waren, ergab sich die Zulässigkeit der Verarbeitung und Nutzung aller auf den Einverständniserklärungen enthaltenen Daten nunmehr aus § 28 Abs. 1 Satz 1 Nr. 1 BDSG (Zweckbestimmung des Behandlungsvertrages). Von den Kunden, die sich bis dahin noch nicht im Kosmetikstudio gemeldet hatten, durften für die wohl allenfalls in Frage kommenden Zwecke der Werbung bzw. Kundenakquise im Weiteren nur die hierfür erforderlichen und insoweit auch zulässigerweise übermittelten Adressdaten verarbeitet und genutzt werden. Dies galt wiederum aber auch nur so lange, wie die Betroffenen nicht von ihrem diesbezüglichen Widerspruchsrecht nach § 28 Abs. 4 BDSG Gebrauch gemacht haben.

Das Kosmetikstudio hat daraufhin mitgeteilt, dass die Einverständniserklärungen aller ehemaligen Kunden, die bislang noch nicht zwecks einer Weiterbehandlung vorstellig geworden waren, vernichtet worden seien. Weiterhin (zulässigerweise) für Werbezwecke gespeichert wären lediglich noch deren Adressdaten.

4.2.4.4 Verarbeitung von Daten abgewiesener Blutspender

Ein Blutspendedienst hatte einen Spendewilligen zurückgewiesen, nachdem sich bei der Überprüfung der gesundheitlichen Voraussetzungen eine aktuell bestehende Nichteignung herausgestellt hatte. Seine Einwilligung in die Blutabnahme hatte er abgegeben. Als Beschwerdeführer kritisierte er nun, dass sich der Blutspendedienst nach Feststellen der Ausschlussgründe geweigert habe, die bis dato in die Datenbank eingestellten Angaben zu löschen sowie die auf Papier festgehaltenen Aufzeichnungen auszuhändigen.

Die Beschwerde war nicht begründet. Das Handeln des Blutspendedienstes hat im Wesentlichen der geltenden Rechtslage entsprochen.

Der Blutspendedienst berief sich mir gegenüber auf § 11 Abs. 1 Satz 1 TFG, wonach „jede Spendeentnahme und die damit verbundenen Maßnahmen“ - nach Satz 2 für eine Mindestdauer von 15 Jahren - zu protokollieren sind. Daraus meinte er folgern zu können, dass dies auch die Dokumentation von Vorbereitungshandlungen betreffe, soweit diese zur Nichtzulassung zur Blutspende führen. Zur Begründung der Erforderlichkeit wurde ausgeführt, der Fall der Zurückweisung eines Spendeangebotes sei für den Blutspendedienst dokumentationspflichtig, damit dieser im Falle einer erneuten Anmeldung desselben Spenders auch dann den seinerzeitigen Nichtzulassungsgrund erkennen könne, wenn der Blutspendewillige beim nächsten Mal den betreffenden Umstand nicht mehr erwähne.

Dem Gesetzeswortlaut (*jede Spendeentnahme und die damit verbundenen Maßnahmen*) lässt sich allerdings nicht unmissverständlich entnehmen, dass der Begriff der Spendeentnahme auch den der Zurückweisung eines Spendeangebotes umfasst. Aber auch wenn der Vorgang einer Zurückweisung eines Blutspendeangebotes nicht die in § 11 Abs. 1 TFG vorgesehene Dokumentationspflicht auslöst, ist die Speicherung der Personalien (Namen, Geburtsdatum, Geburtsort) und des Zurückweisungsgrundes gemäß § 28 Abs. 7 Satz 2 i. V. m. Satz 1 BDSG zulässig, weil es für die im Gesetz genannten Zwecke der Gesundheitsvorsorge sowie der medizinischen Behandlung erforderlich ist, die nötige Sicherheit bei der Gewinnung von Blutspenden zu gewährleisten. Zu dieser Sicherheit ist es nach den insoweit überzeugenden Ausführungen des Blutspendedienstes erforderlich, dass gesichert wird, dass Blutspendewillige, die vorsätzlich oder aus Nachlässigkeit bei einem erneuten Blutspendeangebot bei demselben Spendedienst

einen vorher schon einmal als Zurückweisungsgrund eingeschätzten Umstand nicht mehr erwähnen, von der Blutspende ausgeschlossen werden.

Von der nach dieser Rechtsauffassung bestehenden Speicherungsbefugnis des Blutspendedienstes sind allerdings nur die eingangs genannten Daten umfasst, also die jeweiligen Personalien sowie der Zurückweisungsgrund. Weitere Daten sind für den genannten Zweck nicht erforderlich und müssten gelöscht werden.

4.2.4.5 Keine Anwendbarkeit des Bundesdatenschutzgesetzes bei Unterlassung ärztlicher Aufzeichnungen

Bei der Aufsichtsbehörde hatte eine Patientin vorgesprochen und dargelegt, dass sie vor etwa drei Jahren Geschädigte eines Körperverletzungsdelikts gewesen und ihr das diesbezüglich von ihrer Ärztin formlos ausgestellte Attest abhanden gekommen sei. Als sie ihre Ärztin um die erneute Ausstellung eines solches Attestes ersucht habe, habe sich herausgestellt, dass diese über keine Aufzeichnungen zu der diesbezüglichen ärztlichen Konsultation durch die Patientin verfügte. Die Patientin fühlte sich durch diese Tatsache in ihrem informationellen Selbstbestimmungsrecht beeinträchtigt, da es nach ihrer Auffassung eine lückenlose Dokumentation zu ihren Behandlungsfällen bei der sie versorgenden Ärztin geben müsste.

Die Überprüfung der Rechtslage hat ergeben, dass das Bundesdatenschutzgesetz vorliegend nicht einschlägig und somit die Zuständigkeit der Aufsichtsbehörde nicht gegeben war:

Die Anwendbarkeit des Bundesdatenschutzgesetzes ist bei nicht-öffentlichen Stellen wie beispielsweise niedergelassenen Ärzten gemäß § 1 Abs. 2 Nr. 3 dahingehend beschränkt, dass diese die Daten unter Einsatz von Datenverarbeitungsanlagen oder in bzw. aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben. Da es bei dem geschilderten Sachverhalt aber abgesehen von dem seinerzeit ausgestellten Attest entweder von vornherein nicht zu einer Datenverarbeitung (Speicherung) gekommen ist oder aber zumindest zum Beschwerdezeitpunkt keine solche festzustellen war, war das Bundesdatenschutzgesetz vorliegend nicht anwendbar. Das Bundesdatenschutzgesetz erfasst nicht die Unterlassung einer Verarbeitung, also z. B. auch nicht das Nicht-Anfertigen von Aufzeichnungen. Dies ergibt sich ferner aus dem Zweck des Gesetzes, den § 1 Abs. 1 BDSG mit dem Schutz des Einzelnen vor aus dem Umgang mit seinen personenbezogenen Daten resultierenden Persönlichkeitsrechtsbeeinträchtigungen definiert. Der Ausdruck *Umgang mit Daten* setzt aber voraus, dass diese Daten - eben Aufzeichnungen über einen Sachverhalt - existieren.

Ein Datenschutzrechtsverstoß war damit vorliegend nicht zu erkennen. Ob davon unabhängig ein Verstoß gegen die in § 10 der Berufsordnung der Sächsischen Landesärztekammer geregelten Dokumentationspflichten gegeben war, war durch die Aufsichtsbehörde nicht zu beurteilen. Zuständig war insoweit die Landesärztekammer.

4.2.4.6 Keine Anwendung des Bundesdatenschutzgesetzes bei Auskünften aus dem Kopf

Ein Patient gab an, seine Tochter sei von seinem Arzt vom Inhalt eines ihn betreffenden Arztbriefes in Kenntnis gesetzt worden, und sah darin einen Datenschutzverstoß.

Mangels genauer zusätzlicher Informationen konnte hier die Anwendbarkeit des Bundesdatenschutzgesetzes und somit die Zuständigkeit der Aufsichtsbehörde nicht abschließend geklärt werden:

Gemäß §§ 27, 38 Abs. 1 Satz 1 BDSG beschränkt sich die Anwendung des Bundesdatenschutzgesetzes auf Verarbeitungsvorgänge, soweit diese unter Einsatz von Datenverarbeitungsanlagen oder mittels nicht automatisierter Dateien erfolgen. Diese Anwendungs- und Zuständigkeitsvoraussetzungen wären nur dann erfüllt gewesen, wenn sich der Arzt für seine Äußerung gegenüber der Tochter die (möglicherweise elektronisch geführte) Patientenakte gezogen hätte. Ob dies der Fall war, konnte den vom Petenten zugesandten Unterlagen nicht entnommen werden. Falls der Arzt die Auskünfte aus dem Kopf erteilt hatte, fiel das also nicht unter das Bundesdatenschutzgesetz.

Aber auch in diesem Fall konnte die Informationsweitergabe als Bruch des Arztgeheimnisses rechtswidrig gewesen sein. In jedem Fall, sowohl bei der Überprüfung der Einhaltung des Bundesdatenschutzgesetzes wie bei einer strafrechtlichen Überprüfung, stellt sich allerdings die Frage, ob nicht eine mutmaßliche Einwilligung oder zumindest eine den Vorsatz ausschließende (vgl. § 16 StGB) irrtümliche Annahme einer Einwilligung vorliegt. Die dies bejahenden Feststellungen der vom Petenten gleichfalls mit dieser Angelegenheit befassten Ärztekammer sind insoweit zwar weder für die Aufsichtsbehörde noch für die strafrichterliche Beurteilung maßgeblich, aber sie sind doch von erheblichem Gewicht, weil es sich um die Beurteilung durch mit der ärztlichen Praxis vertraute und überdies mit berufsrechtlichen Fragen besonders befasste Personen handelt.

4.2.5 Einzelhandel

4.2.5.1 Vorlage des Personalausweises beim bargeldlosen Bezahlen

Fast schon regelmäßig wenden sich Bürger mit der Bitte an die Aufsichtsbehörde, die allgemeine Praxis der Einsichtnahme in den Personalausweis oder gar des Notierens

von Personalausweisdaten beim bargeldlosen Bezahlen einer Überprüfung zu unterziehen.

Soweit es sich dabei lediglich um eine reine Sichtkontrolle (Name, Vorname, Lichtbild und ggf. noch Unterschrift) zur Erkennung bzw. Vermeidung des Einsatzes gestohlener EC-Karten handelt, ist nicht zu erkennen, dass schutzwürdige Interessen der Kunden verletzt wären. Gleiches gilt, wenn ausgewählte Personalausweisdaten (Namen, Anschrift, Geburtsdatum) auf dem Transaktionsbeleg oder auch auf separaten Formularen erhoben werden. Zum Schutz vor Kartenmissbrauch und Zahlungsausfall darf ein Händler diese Daten erheben und bis zum erfolgreichen und unwiderruflichen Lastschrifteinzug speichern. Für Einzelheiten wird auf die Ausführungen im 2. Tätigkeitsbericht der Aufsichtsbehörde unter Pkt. 4.3.10 verwiesen.

Auch das Personalausweisgesetz steht den genannten Verfahrensweisen nicht entgegen, insbesondere regelt § 4 Abs. 1 PersAuswG, dass der Personalausweis auch im nichtöffentlichen Bereich, d. h. also auch gegenüber einem Einzelhandelsunternehmen und nicht wie teilweise angenommen nur gegenüber Behörden, als Ausweis- und Legitimationspapier benutzt werden darf.

Nicht notwendig ist die Sichtkontrolle allerdings beim Einsatz von Kreditkarten - hier hat der Einzelhändler die Zahlungsgarantie der jeweiligen Kreditkartengesellschaft - sowie immer dann, wenn das so genannte EC-Cash-Verfahren zur Anwendung kommt: Diese Zahlungsausfälle von vornherein vermeidende und damit auch bedeutend sichere Variante der Zahlung per EC-Karte unter Eingabe der PIN ist allerdings für den Handel mit höheren Kosten verbunden und daher weit weniger verbreitet.

4.2.5.2 Datenerhebung beim Warenumtausch

Die Kundin eines Supermarktes wunderte sich über das Verlangen, beim Umtausch einer - beanstandungsfreien - Ware personenbezogene Daten (hier: Name, Anschrift, Geburtsdatum, Telefonnummer) auf ein Formular einzutragen.

Das Verlangen des Handelsmarktes, dass sich der Kunde identifiziert und dies auch entsprechend dokumentiert wird, ist in der Sache nicht zu beanstanden. Dies gilt allerdings nicht für Daten, die zur Identifikation bei solchen Geschäften nicht erforderlich sind (Telefonnummer, Geburtsdatum).

Ein Umtausch oder auch die Rückgabe erworbener Waren hängt, soweit dem Käufer nicht - insbesondere durch Sachmängel begründet - ein Recht zum Rücktritt vom Kaufvertrag zusteht (vgl. § 437 Nr. 2 BGB), letztlich von der Kulanz des Händlers ab. Geht er darauf ein, so ist er zur Sicherung seiner rechtlichen Interessen, etwa um sich gegen

Umtauschbetrug, sei es durch Kunden oder aber auch das eigene Personal, zu schützen, berechtigt, Namen und Anschrift des Kunden erfassen (vgl. § 28 Abs. 1 Satz 1 Nr. 2 BDSG) und diese Angaben auch anhand eines vorzulegenden Personaldokumentes überprüfen zu lassen. Letzteres ergibt sich insbesondere auch aus § 4 Abs. 1 PersAuswG, wonach der Personalausweis auch im nicht-öffentlichen Bereich als Ausweis- und Legitimationspapier benutzt werden darf. Entgegenstehende überwiegende schutzwürdige Betroffeneninteressen sind dann nicht erkennbar, wenn sich die Datenerfassung auf Name und Anschrift beschränkt.

Händler sollten sich in diesem Zusammenhang allerdings auch von Opportunitätserwägungen leiten lassen und sich die Frage stellen, ob der Erfassungsaufwand und damit verbunden der Aufwand zur (eventuellen) Geltendmachung von Schadensersatzforderungen in einem angemessenen Verhältnis zu dem dabei erreichbaren Nutzen (Warenwert) steht. Gerade bei kleineren Beträgen dürfte dies regelmäßig nicht der Fall sein. Überdies gilt: Datensparsamkeit ist hier auch ein Indiz für Kundenfreundlichkeit.

4.2.5.3 Erhebung von Käuferdaten bei Barkauf und Sofortmitnahme (Handgeschäft)

Die Kundin eines Möbelmarktes berichtete, dass sie beim Kauf eines Möbelstückes, das sie sogleich ab Lager mitzunehmen gedacht und auch sofort habe bezahlen wollen, von der Kundenbetreuerin alternativlos aufgefordert worden sei, für die Erstellung des Abholscheines Namen und Anschrift anzugeben. Das zur Stellungnahme aufgeforderte Unternehmen stellte dies als Dienst am Kunden dar - so könne der Kunde namentlich aufgerufen werden, wenn die Ware vom Lagerpersonal zur Abholung bereitgestellt sei - und sich im Übrigen darauf berufen, dass diese Angaben dessen ungeachtet natürlich freiwillig seien. Auf Kundenwunsch könne der Auslieferungsauftrag für das Lager auch anonym ausgestellt werden.

Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es der Zweckbestimmung eines Vertragsverhältnisses (hier: Kaufvertrag) mit dem Betroffenen dient. Zur Direktabholung bezahlter Ware genügt die Vorlage des Abholscheines, zumal dieser regelmäßig ein Doppel enthält, welches beim Lagerpersonal verbleibt. Weder der Name noch die Wohnanschrift des Kunden sind für die Abwicklung der Warenausgabe erforderlich. Im Zweifelsfall, kann sich der abholberechtigte Kunde immer noch mit seiner Ausfertigung des Abholscheines ausweisen.

Die Stellungnahme des Unternehmens ließ ein Fehlverhalten der betreffenden Kundenberaterin vermuten; die Einlassungen der Kundin schienen jedoch auch ein Organisationsverschulden des Unternehmens nicht auszuschließen. Der Möbelmarkt wurde daher

aufgefordert, sowohl die betreffende Verfahrensweise beim Möbelkauf zukünftig datenschutzrechtlich korrekt zu gestalten, insbesondere die Freiwilligkeit der Angabe der Adressdaten hervorzuheben und dabei auch die diesbezüglichen Zwecke (etwa auch Werbepost) korrekt zu benennen, als auch die Mitarbeiter entsprechend zu schulen.

4.2.6 Sparkassen / Banken

4.2.6.1 Fragebögen nach dem Wertpapierhandelsgesetz

Einem Sparkassenkunden war von seiner Sparkasse ein mit „Kundenangaben für Geschäfte in Finanzinstrumenten“ überschriebenes Formular des Deutschen Sparkassenverlages zugesandt worden. Mit diesem Vordruck sollten in Übereinstimmung mit § 31 WpHG u. a. Kundenangaben über Kenntnisse und Erfahrungen und Anlageziele in Bezug auf Wertpapiergeschäfte erhoben werden. Während das Formular einen Hinweis auf die Freiwilligkeit des Fragebogens enthielt, schloss das dazugehörige Anschreiben jedoch mit der Formulierung „*Bitte beachten Sie, dass wir ab 1. November 2007 keine Wertpapierorder für Sie entgegennehmen dürfen, wenn uns kein gültiger Wertpapierinformationsbogen vorliegt*“ ab.

Diese Formulierung widersprach sowohl der Gesetzeslage als auch den Formulierungen im beigelegten Formular und suggerierte dem Kunden fälschlicherweise, dass er keine Wertpapiergeschäfte mehr tätigen könne, ohne den Wertpapierinformationsbogen vollständig ausgefüllt zu haben. Tatsächlich regelt das Wertpapierhandelsgesetz für den Fall der Nichterlangbarkeit der erforderlichen Kundeninformationen aber, dass dann der Kunde darüber zu informieren ist, dass das jeweilige Kreditinstitut die ihm obliegende Beurteilung der Angemessenheit nicht vornehmen kann (§ 31 Abs. 5 Satz 4 WpHG).

Die Sparkasse ist dieser Auffassung gefolgt und hat die betreffende Formulierung fortan nicht mehr verwendet. Sie hat insbesondere auch klargestellt, dass Kunden, die den Wertpapierinformationsbogen nicht ausgefüllt haben, auch nicht von Wertpapiergeschäften ausgeschlossen werden.

4.2.7 Vereine / Verbände

4.2.7.1 Datenverarbeitungsbefugnis bei Sportveranstaltungen

Einem Sportfreund waren die offenbar viel zu weit formulierten Teilnahmebedingungen einer Marathon-Großveranstaltung aufgefallen. Laut diesen Teilnahmebedingungen sollten die Interessenten für eine Teilnahme am Marathon zwingend ihr Einverständnis erklären, dass die in der Anmeldung abgefragten Daten in Rundfunk, Fernsehen, Werbung, Büchern, fotomechanischen Vervielfältigungen genutzt und weitergegeben werden dürfen. Auf dem Anmeldebogen erhoben wurden insbesondere Namen, Anschrift,

Vereinszugehörigkeit, Geburtsjahr, Nationalität, Geschlecht und Kontodaten. Auch wenn davon auszugehen war, dass sich diese wohl in erster Linie auf die Verwertungsrechte zielende Einverständniserklärung keinesfalls auf alle im Anmeldeformular abgefragten Daten erstreckt und die Verwendung und Weitergabe auch nur zweckgebunden erfolgt, ergab sich aus dem Wortlaut der Erklärung doch etwas anderes. Diese erweckte den Eindruck, dass jegliche Nutzung durch jeden erlaubt werden sollte.

Die Zulässigkeit der Erhebung, Verarbeitung und Nutzung von Teilnehmerdaten bei derartigen Sportveranstaltungen ergibt sich vom Grundsatz her aus § 28 Abs. 1 Satz 1 Nr. 1 BDSG, wonach das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig ist, wenn es der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen (hier: Marathonlauf-Teilnahmevertrag) dient. Eine diesbezügliche Einwilligung der Teilnehmer ist daher an dieser Stelle entbehrlich. Dies wird oftmals - auch in anderen Zusammenhängen - übersehen. Die Teilnehmer müssen lediglich gemäß den Vorgaben des § 4 Abs. 3 BDSG über die verantwortliche Stelle, die Zweckbestimmung der Erhebung, Verarbeitung und Nutzung sowie über die Kategorien von Empfängern unterrichtet werden. Dabei ist auch der - gleichfalls noch oft zu findende, tatsächlich aber überflüssige - „Hinweis lt. Datenschutzgesetz: Ihre Daten werden maschinell gespeichert.“ entbehrlich, da die Daten mit Kenntnis des Betroffenen gespeichert werden (§ 33 Abs. 1 Satz 1 BDSG).

Von der datenschutzrechtlichen Unterrichtung deutlich abzusetzen sind die davon unabhängige Einwilligungserklärung betreffend nicht vom Teilnahmevertrag gedeckte Nutzungszwecke (Werbung, sonstige Veröffentlichungen) und die Zustimmungsklausel hinsichtlich der Verwertungsrechte. Letztere darf sich keinesfalls pauschal auch auf die in der Anmeldung gemachten Daten beziehen, sondern muss deutlich machen, dass diese nur die direkt während der Veranstaltung angefertigten Fotos, Filmaufnahmen und Interviews betrifft.

Der Veranstalter hat sich mit dieser Problematik mit der notwendigen Ernsthaftigkeit erst auseinandergesetzt, nachdem ich mit einer diesbezüglichen Pressemitteilung an die Öffentlichkeit gegangen war. Für die Folgeveranstaltungen dieses - jährlich durchgeführten - Marathonlaufes ist nunmehr jedoch für datenschutzkonforme Teilnahmebedingungen gesorgt.

4.2.7.2 Nutzung der Mitgliederliste eines Vereins nach Verbandsaustritt

Ein Verein beschwerte sich, dass der Verband, dem er lange angehört hatte, mehr als ein Vierteljahr nach Ausschluss des Vereins aus dem Verband die aktuelle Ausgabe der

Verbandszeitschrift an die Vereinsmitglieder versandt hatte. Zu diesem Zeitpunkt war der (monatliche) Versand der Verbandzeitschrift an die Vereinsmitglieder bereits seit einem Jahr eingestellt gewesen. Dem aktuellen Versand zu Grunde gelegt worden war eine Mitgliederliste des Vereins, die dem Verband ursprünglich monatlich, zuletzt jedoch vor Jahresfrist in aktualisierter Form zweckgebunden zur Verfügung gestellt worden war. Ausgelöst worden war die Beschwerde offensichtlich durch den Inhalt der aktuellen Ausgabe. In einem darin abgedruckten Beitrag wurden die Mitglieder des aus dem Verband ausgeschlossenen Vereins zum Vereinsaustritt und Beitritt zu einem anderen, einem verbandstreuen Verein aufgerufen.

Diese Nutzung der dem Verband zweckgebunden für die Auslieferung einer konkreten Vorjahresausgabe der Verbandszeitschrift übersandten Adressdatei war rechtswidrig.

Gemäß § 35 Abs. 2 Satz 2 Nr. 3 BDSG sind personenbezogene Daten, die für eigene Zwecke verarbeitet werden, zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Mit der Auslieferung der jeweiligen Ausgabe der Verbandszeitschrift zuzüglich einer gewissen Frist (ungefähr einen Monat) zur Bearbeitung eventueller Reklamationen in Bezug auf den Nichterhalt der Zeitschrift war der Zweck der Speicherung der monatlich in aktualisierter Form neu übermittelten Mitgliederliste erfüllt. Die Adressdateien wären somit jeweils etwa spätestens einen Monat nach Versand der jeweiligen Ausgabe zu löschen gewesen.

Der Verband argumentierte zunächst, dass die ein Jahr später erfolgte Nutzung der noch vorhandenen Mitgliederliste zulässig gewesen sei, da diese Zweckänderung über die Verweisung in § 28 Abs. 5 Satz 2 BDSG entweder durch Abs. 1 Nr. 2 (Interessenabwägung) oder nach Abs. 3 Satz 1 Nr. 3 (Listenprivileg) rechtmäßig gewesen sei. Darauf kam es aber überhaupt nicht an, denn die genutzten Daten hätten zu diesem Zeitpunkt schon längst gelöscht sein müssen.

Der Verband hat die noch vorhandene Adressdatei des ehemalig verbandsangehörigen Vereins schließlich gelöscht.

4.2.8 Energieversorgungsunternehmen

4.2.8.1 Ausstellung von Energieausweisen

Mit dem Inkrafttreten der Energieeinsparverordnung im Jahr 2007 benötigen Hauseigentümer unter bestimmten Voraussetzungen einen sogenannten Energieausweis, auch Energiepass genannt. Dies ist unter anderem dann der Fall, wenn Häuser oder Wohnungen verkauft oder vermietet werden sollen. Energieausweise können entweder auf der Grundlage des tatsächlichen Energieverbrauchs oder auf der Grundlage des auf-

grund der baulichen Gegebenheiten gewissermaßen objektiv anzusetzenden Energiebedarfs ausgestellt werden. Soweit dafür nach der Energieeinsparverordnung eine Wahlmöglichkeit besteht bzw. bestand, haben sich Vermieter aus Kostengründen häufig für das auf den Energieverbrauch abstellende Verfahren entschieden.

Ein Vermieter hatte zu diesem Zweck von seinem Energieversorgungsunternehmen die Verbrauchsdaten aller einzelnen Wohn- und Gewerbeeinheiten seines Gebäudes aus den letzten drei Abrechnungsjahren wissen wollen. Als ihm diese unter Berufung auf den Datenschutz verweigert worden waren, hat er sich an mich gewandt.

Der Energieversorger hatte sich korrekt verhalten:

Nach § 28 Abs. 3 Nr. 1 BDSG ist die Übermittlung personenbezogener Daten, wozu natürlich die hier gewünschten Energieverbrauchsdaten für den Vermieter als Übermittlungsempfänger gehörten, zulässig, soweit es zur Wahrung berechtigter Interessen eines Dritten - in diesem Fall also des Vermieters - erforderlich ist und kein Grund zu der Annahme besteht, dass die Betroffenen ein schutzwürdiges Interesse am Ausschluss der Übermittlung haben.

Die berechtigten Interessen des Vermieters ergeben sich aus dessen gesetzlicher Pflicht, sich einen Energieausweis zu besorgen, und sind somit datenschutzrechtlich grundsätzlich anzuerkennen. Wenn diese gesetzliche Verpflichtung nicht nur auf der Grundlage des berechneten Energiebedarfes des Hauses (§ 17 Abs. 1, 2 EnEV), sondern stattdessen auch auf derjenigen des erfassten Energieverbrauches erfüllt werden kann, wird man denjenigen Gebäudeeigentümer, der Vermieter ist, nicht unter dem Gesichtspunkt der Erforderlichkeit der Datenbeschaffung auf die - aufwendigere - Möglichkeit der Ermittlung des berechtigten Energiebedarfes verweisen dürfen (weil nämlich der Gesetzgeber der Energieeinsparverordnung die andere Möglichkeit implizit gerade auch für Hauseigentümer eröffnet, die Vermieter sind). Dies gilt, obwohl, wie dem Verordnungsgeber klar gewesen sein muss, die Energieverbrauchsdaten sehr stark von der Anzahl der im Gebäude wohnenden Personen und deren Verbrauchsgewohnheiten abhängig, die energetischen Eigenschaften eines Gebäudes hingegen von jeweiligen Bewohnern unabhängig und somit eigentlich wesentlich besser für die Ausstellung eines Energieausweises geeignet sind. Ein objektiv richtiges Bild des gebäudetypischen Energiebedarfes kann eigentlich nur auf der Basis des ingenieurmäßig berechneten Energiebedarfs erstellt werden. Aber wenn der (materielle) Gesetzgeber die Einstufung des Gebäudes auch auf der eigentlich weniger geeigneten Grundlage als gleichwertig für die Erfüllung der von ihm aufgestellten Pflicht anerkennt, ist das eine für die datenschutzrechtliche Beurteilung hinzunehmende, für sie maßgebliche Vorgabe.

Aber aus einem anderen Grund hatte das Energieversorgungsunternehmen recht gehabt: Für die Zwecke des Petenten hätte (und hat) die Übermittlung der zusammengefassten Verbrauchsdaten aller Zähler ausgereicht, denn Energieausweise werden nicht für einzelne Wohnungen, sondern nur für ganze Gebäude ausgestellt (§ 17 Abs. 3 EnEV). Zumindest datenschutzrechtliche Gründe waren einer solchen Übermittlung in dem konkreten Fall dann nicht mehr entgegenzuhalten, da bei insgesamt acht Stromzählern ein Personenbezug bei den zusammengefassten Verbrauchswerten vom Vermieter sicher nicht mehr hergestellt werden konnte.

Daraus folgt übrigens, dass im Falle der Vermietung eines Gebäudes an eine einzelne Person die Übermittlung deren persönlicher Verbrauchsdaten an den Vermieter im Hinblick auf die Energieeinsparverordnung zulässig sein muss.

4.2.9 Handels- und Wirtschaftsauskunfteien

4.2.9.1 Versand einer Selbstauskunft betreffend eine juristische Person per Telefax

Der Geschäftsführer einer GmbH (zugleich einer der Gesellschafter) führte Beschwerde über eine Auskunftei. Diese hatte entgegen einem die Art des Postversandes betreffend von ihm geäußerten Verlangen die bei der Auskunftei gespeicherten Daten der Gesellschaft bzw. des Unternehmens, dessen Rechtsträger die GmbH war, darunter nicht nur z. B. die Höhe des Stammkapitals und die Geschäftszahlen, sondern auch Namen, Geburtsdaten, Anschriften und Gesellschaftsanteile des Geschäftsführers und der anderen Gesellschafter, ohne weitere Vorankündigung *per Telefax* an die GmbH übermittelt. Infolgedessen konnte auch ein nicht näher bestimmbarer Kreis von Arbeitnehmern der GmbH von diesen Daten Kenntnis erlangen.

Diese Verfahrensweise stellte sowohl einen Verstoß gegen § 9 BDSG dar, wonach personenbezogene Daten bei der Übertragung so zu sichern sind, dass sie Unbefugten nicht zur Kenntnis gelangen können, als auch gegen das Schriftformerfordernis des § 34 Abs. 3 BDSG.

Auch wenn die Daten juristischer Personen als solcher dem klaren Wortlaut des Gesetzes (§ 3 Abs. 1) nach nicht in den Anwendungsbereich des Bundesdatenschutzgesetzes fallen (obwohl immer stärker anerkannt wird, dass auch juristische Personen, wenn auch vielleicht nur in Teilbereichen, Träger des Grundrechts auf informationelle Selbstbestimmung sind, vgl. zuletzt OVG Lüneburg, Beschl. v. 15. Mai 2009 - 10 ME 385/08, NJW 2009, 2697), fiel der Sachverhalt insoweit unter das Bundesdatenschutzgesetz, als die erteilte Firmenauskunft auch unmittelbare und mittelbare personenbezogene Daten des Geschäftsführers und der anderen Geschäftsführer enthielt. (Zudem

hatte der Geschäftsführer seinen Auskunftsanspruch als Person gegenüber der Auskunftei geltend gemacht. Die Auskunft hätte also schon aus diesem Grund auch nur ihm erteilt werden dürfen.)

Übrigens ist zweifelhaft, ob dem gesetzlichen Schriftformerfordernis durch eine Telefaxmitteilung genügt werden kann (anders die wohl herrschende Kommentarmeinung, vgl. Simitis/Dix Rdnr. 47 zu § 34 BDSG). Etwas anderes gilt natürlich dann, wenn sich beide Seiten auf diese Art des Versands geeinigt haben. In diesem Fall verlangt die Literatur (Simitis/Mallmann, Rdnr. 58 zu § 19 BDSG; Däubler/Klebe/Wedde/Weichert, Rdnr. 32 zu § 34 BDSG) allerdings aus den am hier zu beurteilenden Fall anschaulich werdenden Gründen überzeugend, dass dem Fax eine telefonische Vorankündigung vorausgeht, so dass es zuverlässig ausschließlich von befugter Seite entgegengenommen werden kann. Keine dieser Voraussetzungen war in dem dargestellten Fall erfüllt.

5 Beratungstätigkeit

5.1 Überblick

Seit 2006 gilt: *Die Aufsichtsbehörde berät und unterstützt die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse (§ 38 Abs. 1 Satz 2 BDSG).*

Diese Vorschrift erweitert die Beratungspflicht der Aufsichtsbehörde gegenüber den betrieblichen Datenschutzbeauftragten aus §§ 4g Abs. 1 Satz 2, 4d Abs. 6 Satz 3 BDSG und bezieht die verantwortlichen Stellen selbst ein. Damit wird insbesondere auch dem Umstand Rechnung getragen, dass für eine Vielzahl von insbesondere Klein- und mittelständischen Unternehmen keine Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten besteht.

Im Berichtszeitraum sind in 34 Fällen derartige Beratungen durchgeführt worden. Telefonische Anfragen, die auch sofort durch telefonische Beratung erledigt werden konnten, sind in dieser Zahl ebenso wenig - hierüber wurde keine Statistik geführt - enthalten wie Anfragen von Betroffenen, denen es lediglich darum ging, das eigene Misstrauen von kompetenter Seite her bestätigt oder widerlegt zu bekommen, um dann mit den notwendigen Argumenten und Rechtsgrundlagen versehen die Lösung des jeweiligen Problems in eigener Regie anzugehen bzw. gegebenenfalls auch zu unterlassen; diese Beratungsfälle sind in die Statistik oben unter 4.1 eingegangen.

In diesen 34 unter § 38 Abs. 1 Satz 2 BDSG fallenden Beratungsfällen ist es um

- konkrete Fragen der Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten (13 Fälle),
- den betrieblichen Datenschutzbeauftragten selbst (7 Fälle) - hier insbesondere um Bestellungsvoraussetzungen und -formalitäten, um die erforderliche Fachkunde sowie um die Wahrnehmung der gesetzlichen Aufgaben, so etwa auch Fragen des Verfahrensverzeichnisses, sowie
- Datensicherheitsfragen (3 Fälle)

gegangen.

Die verbleibenden elf Anfragen hatten ihren Ausgangspunkt in dem Ansinnen, von der Aufsichtsbehörde eine sogenannte Unbedenklichkeitsbescheinigung zu erhalten - mehr dazu im folgenden Abschnitt:

5.2 Unbedenklichkeitsbescheinigungen

5.2.1 Begutachtung neuer Geschäftsmodelle

Gelegentlich wenden sich Unternehmen an die Aufsichtsbehörde, um eine neue Geschäftsidee bzw. ein daraus sich ergebendes Datenverarbeitungsvorhaben vorzustellen und um anschließend eine diesbezügliche Unbedenklichkeitsbescheinigung zu erhalten. Damit soll dann die Vermarktung des jeweiligen Angebots unterstützt werden, teilweise fordern potentielle Auftraggeber dem Vernehmen nach wohl auch eine derartige Bescheinigung.

Eine Rechtsgrundlage für die Erteilung von Unbedenklichkeitsbescheinigungen gibt es allerdings nicht. Es gibt insbesondere keine Rechtsvorschriften, die die Voraussetzungen einer solchen Unbedenklichkeitsbescheinigung regeln. Derartigen Anliegen kann durch die Aufsichtsbehörde daher nicht entsprochen werden. Überhaupt gehört die datenschutzrechtliche Zertifizierung von Datenverarbeitungssystemen nicht zu den Aufgaben der Aufsichtsbehörde. Für solche Zertifizierungen ist daher auf die am Markt tätigen Anbieter zu verweisen.

Unbeschadet dessen nutzt die Aufsichtsbehörde natürlich im Rahmen der ihr nach § 38 Abs. 1 Satz 2 BDSG obliegenden Beratungspflicht die sich auf diese Weise bietende Möglichkeit, die jeweiligen Unternehmen auf besondere datenschutzrechtliche Aspekte des jeweiligen Vorhabens und auch aus den vorgelegten Unterlagen bereits erkennbare Mängel hinzuweisen.

5.2.2 „Elektronische Maßnahmeabwicklung“ zwischen der Bundesagentur für Arbeit und den von ihr beauftragten Bildungsträgern

Mitte 2007 hat die Bundesagentur für Arbeit von ihr mit der Durchführung berufsvorbereitender Bildungsmaßnahmen nach § 61 SGB III oder behindertenspezifischer berufsvorbereitender Bildungsmaßnahmen nach § 102 i. V. m. § 61 SGB III beauftragte, im Fortbildungsbereich tätige Unternehmen aufgefordert, für den diesbezüglichen Datenaustausch zwischen ihnen und der BA einen bestimmten technischen Anforderungen genügenden elektronischen Informationsaustausch zu organisieren und für die dafür von ihnen zu beschaffenden und einzusetzenden Rechner und Programme der zuständigen regionalen Organisationseinheit der BA *eine datenschutzrechtliche Unbedenklichkeitsbescheinigung des Landesbeauftragten für Datenschutz vorzulegen*.

Etliche in Sachsen tätige Bildungsträger-Unternehmen dieser Art haben sich daraufhin, wegen der ihnen gesetzten Frist einigermaßen beunruhigt, an mich gewandt und um eine solche *datenschutzrechtliche Unbedenklichkeitsbescheinigung* gebeten. Dass sie

dabei keinerlei Anstalten gemacht haben, mir irgendwelche Unterlagen vorzulegen, war unschädlich. Denn die BA war mit dem betreffenden Verlagen auf dem rechtlichen Holzweg: Eine Rechtsgrundlage für die Erteilung einer derartigen Unbedenklichkeitsbescheinigung, einschließlich der dazu etwa erforderlichen Erhebung personenbezogener Daten der verarbeitenden (verantwortlichen) Stelle, gab es nicht. Es gab - und gibt - insbesondere keine Rechtsvorschriften, die Voraussetzungen einer solchen Unbedenklichkeitsbescheinigung regeln.

Dass die BA mit dem betreffenden Verlangen von falschen rechtlichen Voraussetzungen ausging, war auch schon daran zu ersehen, dass zuständig für diejenigen Daten verarbeitenden Stellen, denen die Unbedenklichkeitsbescheinigung hätte erteilt werden sollen, die Aufsichtsbehörden nach § 38 Abs. 1 Satz 1, Abs. 6 BDSG hätten sein müssen; diese sind jedoch nicht regelhaft mit den im Schreiben der BA genannten „Landesbeauftragten für den Datenschutz“ identisch (vgl. oben Abschnitt 1).

Erkennbar war: Hier hatten Bedienstete der BA diese von der Verpflichtung entlasten wollen, die betreffenden Unternehmer (Funktionsübernehmer, nicht bloße Auftragsdatenverarbeiter) auch in dieser Hinsicht sorgfältig auszuwählen (was nicht nur gemäß § 11 Abs. 2 Satz 1 BDSG für die Datenverarbeitung im Auftrag gilt).

6 Prüfung den Datenschutz betreffender Verhaltensregeln von Berufsverbänden

Gemäß § 38a BDSG überprüft die Aufsichtsbehörde ihr von Berufsverbänden und anderen, bestimmte Gruppen verantwortlicher Stellen vertretenden Vereinigungen unterbreiteten Entwürfe für interne datenschutzrechtliche Verhaltensregeln auf ihre Vereinbarkeit mit dem geltenden Datenschutzrecht.

Im Berichtszeitraum sind an die Aufsichtsbehörde keine derartigen Anliegen herangetragen worden.

7 Genehmigung von Datenübermittlungen in Drittstaaten

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

Als Garantien für den Schutz des Rechts auf informationelle Selbstbestimmung als Teil des zivilrechtlichen Persönlichkeitsrechtes sind entsprechende Vertragsklauseln oder verbindliche Unternehmensregelungen vorzulegen. Werden allerdings die von der Europäischen Kommission festgelegten Standardvertragsklauseln verwendet, ist die Genehmigung der Datenübermittlungen durch die Aufsichtsbehörde nicht mehr erforderlich.

Im Berichtszeitraum sind beim Sächsischen Datenschutzbeauftragten keine derartigen Anträge gestellt worden.

8 Öffentlichkeitsarbeit

Die Aufsichtsbehörden für den nicht-öffentlichen Bereich haben regelmäßig, spätestens jedoch alle zwei Jahre, einen Tätigkeitsbericht zu veröffentlichen (§ 38 Abs. 1 Satz 7 BDSG).

Mit dem vorliegenden Bericht erfüllt der Sächsische Datenschutzbeauftragte erstmals seit Übernahme der Kontrollzuständigkeit seine Verpflichtung, die Öffentlichkeit alle zwei Jahre über die Tätigkeit der Aufsichtsbehörde zu informieren, und schließt an die drei bereits vorliegenden Tätigkeitsberichte des SMI an.

Hinzu kommt die Behandlung von die Tätigkeit als Aufsichtsbehörde nach dem Bundesdatenschutzgesetz betreffenden Themen zum Datenschutz im nicht-öffentlichen Bereich im Internetauftritt des Sächsischen Datenschutzbeauftragten: *http://www.datenschutz.sachsen.de*.

Meine Zusammenarbeit mit der Gesellschaft für Datenschutz und Datensicherung e.V., insbesondere mit dem GDD-Erfa-Kreis Sachsen, war ein weiterer wesentlicher Schwerpunkt der Öffentlichkeitsarbeit im Berichtszeitraum. Die viermal jährlich stattfindenden Erfa-Kreis-Tagungen bieten sehr gute Möglichkeiten für den Meinungsaustausch mit den betrieblichen Datenschutzbeauftragten und fördert den fachlichen Austausch zwischen diesen. Dies geschieht durch die regelmäßige und aktive Teilnahme von Behördenvertretern oder durch die organisatorische Unterstützung der Ausrichtung einzelner Tagungsveranstaltungen wie etwa im Juni 2007.

Darüber hinaus hat sich der Sächsische Datenschutzbeauftragte auch noch an anderen Tagungen oder Fachveranstaltungen mit Fachvorträgen beteiligt, so etwa am 4. Sächsischen Fundraisingtag im September 2007 in Dresden mit einem Vortrag zum Thema „Mit Spenderdaten korrekt umgehen - Datenschutz als Transparenzkriterium“ oder am Branchentag Sicherheitsgewerbe im November 2007 in Chemnitz mit Ausführungen zum Thema „Datenschutz - Chancen und Risiken für das Bewachungsgewerbe“. Gleichfalls im November 2007 wurde auf der DPWV-Fachgruppentagung in Dresden zur Thematik des „Datenschutzes in sozialtherapeutischen Wohnstätten für chronisch psychisch kranke sowie für abhängigkeitskranke Menschen“ referiert.

Leider konnte - in Ermangelung ausreichender personeller Ressourcen - bei weitem nicht allen derartigen Anfragen entsprochen werden. Vorrangig ist in jedem Fall die Erfüllung der gesetzlich vorgegebenen Kontroll- und Beratungsaufgaben (vgl. § 38 Abs. 1 BDSG) - nur wenn diese Aufgabenwahrnehmung nicht gefährdet ist, kann - ein entsprechendes öffentliches Interesse vorausgesetzt - darüber hinaus auch Wünschen

nach Vorträgen bzw. Tagungsteilnahmen entsprochen werden. In jedem Fall von einer Teilnahme abgesehen wurde bei Veranstaltungen mit kommerziellem Hintergrund. Auch Anfragen zur Übernahme interner Schulungsveranstaltungen in Unternehmen oder Vereinen sind regelmäßig ablehnend beantwortet worden. Derartige Schulungen, so nützlich sie auch wären, übersteigen die Grenzen der in § 38 Abs. 1 Satz 2 BDSG verankerten Beratungs- und Unterstützungspflicht (für betriebliche Datenschutzbeauftragte und die verantwortlichen Stellen selbst). Es gibt genügend freiberuflich tätige Datenschutzfachleute bzw. gewerbliche Anbieter von Schulungsveranstaltungen, auf die insoweit zurückgegriffen werden kann.

9 Ordnungswidrigkeitenverfahren

9.1 Überblick

Der Sächsische Datenschutzbeauftragte ist zuständig für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 43 BDSG (§ 13 OWiZuVO).

Im Berichtszeitraum sind durch den Sächsischen Datenschutzbeauftragten 16 Bußgeldverfahren eingeleitet worden; fünf weitere Verfahren waren von den bis zum 31. Dezember 2006 zuständigen Regierungspräsidien übernommen worden, drei davon in der Anhörungsphase, zwei jeweils als Einspruch gegen bereits erlassene Bußgeldbescheide in Höhe von 200 € bzw. 500 € (vgl. hierzu 3. TB 2005/2006 des SMI, Pkt. 9).

Der eine unbefugte Datenübermittlung betreffende Bußgeldbescheid über 200 € war dem zuständigen AG bereits 2006 durch das betreffende Regierungspräsidium zur Entscheidung vorgelegt worden - das AG hat dieses Verfahren dann 2007 allerdings eingestellt. Der zweite Bußgeldbescheid über 500 € betraf einen Verstoß gegen die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten, der dem AG erst durch den Sächsischen Datenschutzbeauftragten übergeben worden ist. Hier hat der Betroffene seinen Einspruch kurz vor dem angesetzten Verhandlungstermin zurückgenommen.

Von den somit verbleibenden 19 Verfahren sind zehn eingestellt worden, zwei befanden sich zum Ende des Berichtszeitraumes noch in der Anhörungsphase.

Damit sind im Berichtszeitraum schließlich sieben Verfahren mit einem Bußgeldbescheid abgeschlossen worden; die Bußgeldsumme belief sich insgesamt auf 13.450 €:

- Mit drei Bußgeldbescheiden (750 €, 1.000 € und 10.000 €) wurden Verstöße gegen die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten (§ 43 Abs. 1 Nr. 10 BDSG) geahndet. In einem Fall (750 €) ist dagegen Einspruch eingelegt worden; die diesbezügliche Entscheidung des zuständigen AG stand zum Ende des Berichtszeitraumes noch aus.
- Wegen Verletzung der Meldepflichten wurde gegen ein Kleinunternehmen ein Bußgeldbescheid über 50 € erlassen (§ 43 Abs. 1 Nr. 1 BDSG). Zwar war das Unternehmen zum bei der Aufsichtsbehörde geführten Verfahrensregister gemeldet gewesen, jedoch hatte sein Geschäftsführer es über einen Zeitraum von drei Jahren bereits damals versäumt, dem seinerzeit noch zuständigen Regierungspräsidium eine Änderung des Firmensitzes mitzuteilen. Im Rahmen der routinemäßigen Überprüfung der Registereinträge ist dies dann nach Zuständigkeits-

übergang durch den Sächsischen Datenschutzbeauftragten festgestellt und - nach Ermittlung des neuen Firmensitzes - auch geahndet worden.

- Drei Bußgeldverfahren betrafen materielle Rechtsverletzungen (§ 43 Abs. 2 Nr. 1 BDSG); die nachfolgend kurz aufgeführten Sachverhalte wurden mit Bußgeldern in Höhe von 250 €, 400 € sowie 1.000 € geahndet:

  - Übermittlung einer auf einzelne Gebäudeteile aufgeschlüsselten Wertermittlung einer Immobilie an den (zugleich mit Sanierungsarbeiten beauftragten) Lebensgefährten der Stieftochter der Eigentümerin durch einen Versicherungsmitarbeiter,
  - Offene Lagerung von zur Entsorgung bestimmten Unterlagen mit personenbezogenen Daten in einer frei zugänglichen Tiefgarage durch einen Finanzvermittler,
  - Internetveröffentlichung von Webcamaufnahmen (Mitarbeiter, Kunden) aus Einzelhandelsgeschäften eines Unternehmens der Telekommunikationsbranche.

9.2 Zeitweilige Entziehung der Zuständigkeit

Im Zuge der Übertragung der Kontrollzuständigkeit für den Datenschutz im nicht-öffentlichen Bereich zum 1. Januar 2007 auf den Sächsischen Datenschutzbeauftragten war durch Artikel 2 des Gesetzes zur Änderung des Sächsischen Datenschutzgesetzes vom 14. Dezember 2006 (SächsGVBl. S. 530) auch ein neuer § 3a in die OWiZuVO eingefügt worden, wonach der Sächsische Datenschutzbeauftragte zugleich auch die Zuständigkeit für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach dem Bundesdatenschutzgesetz erhalten hatte.

Mit Wirkung vom 5. Februar 2008 hat die Sächsische Staatsregierung dann aber eine überarbeitete Fassung der Ordnungswidrigkeiten-Zuständigkeitsverordnung bekannt gemacht (SächsGVBl. S. 67), die überraschenderweise keine Zuständigkeit des Sächsischen Datenschutzbeauftragten für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach dem Bundesdatenschutzgesetz mehr vorsah; weder der § 3a noch eine dem § 3a entsprechende Regelung waren in dieser Verordnung enthalten.

Vermutlich hatte der Verordnungsgeber diese letzte, nicht von ihm, sondern vom Parlament in einem Parlamentsgesetz vorgenommene Änderung schlicht übersehen und ist diese durch die Neuregelung bewirkte wenig zweckmäßige Übertragung der Zuständigkeit für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach dem Bundesdatenschutzgesetz auf die Landkreise und kreisfreien Städte (Auffangzuständigkeit gemäß § 2 OWiZuVO) nicht beabsichtigt gewesen. Nichtsdestoweniger war dem Sächsischen Datenschutzbeauftragten damit aber dennoch die diesbezügliche Zuständigkeit

entzogen. Auch wenn die Sächsische Staatsregierung, der dies zunächst noch gar nicht aufgefallen war, dann die Auffassung vertreten hat, dass sich an der Zuständigkeit des Sächsischen Datenschutzbeauftragten nichts geändert habe, denn der Verordnungsgeber könne keine durch Gesetz in eine Verordnung eingefügte Regelung ändern, sind durch den Sächsischen Datenschutzbeauftragten bis zur Bekanntmachung der diesen Fehler korrigierenden Verordnung vom 16. Juli 2008 alle Bußgeldverfahren ausgesetzt bzw. keine neuen Verfahren eingeleitet worden. Maßgeblich dafür war der Beschluss des Bundesverfassungsgerichts vom 13. September 2005 - 2 BvF 2/03 -, wonach auch die im Verfahren förmlicher Gesetzgebung in eine Verordnung eingefügten Teile lediglich Verordnungsrang haben und damit einer abermaligen Änderung durch die Exekutive offen stehen (Entscheidung einer alten verfassungsrechtlichen Streitfrage dahingehend, dass die sogenannten Entsteinerungsklauseln nur deklaratorische Wirkung haben).

Der Verordnungsgeber hat, wie schon erwähnt, schnell reagiert: Seit dem 1. August 2008 regelt nunmehr § 13 der neuen (SächsGVBl. 2008, 481) OwiZuVO (wieder), dass der Sächsische Datenschutzbeauftragte für die Verfolgung von Ordnungswidrigkeiten nach § 43 BDSG zuständig ist.

10 Durchsetzung des Auskunftsrechts der Aufsichtsbehörde

Die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen (§ 38 Abs. 3 Satz 1 BDSG).

Verstöße gegen die Auskunftspflichten sind - jedenfalls solange sich der Auskunftspflichtige nicht berechtigterweise auf sein Auskunftsverweigerungsrecht (§ 38 Abs. 3 Satz 2 BDSG) beruft - bußgeldbewehrt. Von der Möglichkeit, in solchen Fällen ein Bußgeld zu verhängen, war in der Vergangenheit durch die seinerzeit zuständigen Regierungspräsidien vergleichsweise rege Gebrauch gemacht worden (vgl. z. B. 3. TB 2005/2006 des SMI, Pkt. 9: Neun Verfahren wegen Verstoßes gegen die Auskunftspflichten). Auch wenn die Einleitung eines Bußgeldverfahrens oftmals bewirkt, dass sich die auskunftspflichtige Stelle besinnt und dann zumindest noch nachträglich die geforderten Auskünfte erteilt, ist das Bußgeldverfahren kein geeignetes Mittel zur Durchsetzung der Auskunftsansprüche der Aufsichtsbehörde. Denn der erfolgreiche Abschluss eines Bußgeldverfahrens bedeutet nicht notwendigerweise, dass die Aufsichtsbehörde die benötigten Auskünfte auch tatsächlich erhält. Der Auskunftspflichtige kann das Bußgeld auch bezahlen, ohne die von ihm geforderten Auskünfte zu erteilen.

Der Sächsische Datenschutzbeauftragte ist daher dazu übergegangen, immer dann, wenn eine verantwortliche Stelle nach entsprechender Aufforderung und Mahnung ihren Auskunftspflichten nicht nachkommt, ein förmliches Auskunftsheranziehungsverfahren durchzuführen. Gegen die verantwortliche Stelle wird ein (kostenpflichtiger) Verwaltungsakt erlassen, mittels dessen sie konkret zur Erteilung bestimmter Auskünfte verpflichtet wird. Um diesem Auskunftsverlangen entsprechend Nachdruck zu verleihen, wird zur Erfüllung der Auskunftserteilungspflicht gleichzeitig ein Zwangsgeld angedroht. Wird die Auskunft dennoch nicht erteilt, wird - nach Rechtskraft des Heranziehungsbescheides - dieses Zwangsgeld festgesetzt und gleichzeitig - für den Fall der weiteren Auskunftsverweigerung - ein erhöhtes Zwangsgeld angedroht.

Im Berichtszeitraum sind in vier Fällen solche förmlichen Auskunftsverfahren eröffnet bzw. durchgeführt worden. In einem Fall sind die erbetenen Auskünfte nach Festsetzung des angedrohten Zwangsgeldes schließlich erteilt worden, ein Heranziehungsbescheid konnte nicht zugestellt werden, weil sich der Empfänger in der Zwischenzeit ins Ausland abgesetzt hatte, und in einem weiteren Verfahren stand die Zwangsgeldfestsetzung zum Ende des Berichtszeitraumes noch aus. Das vierte Verfahren war insoweit besonders spektakulär, weil dort bereits zwei Zwangsgelder in Höhe von 300 € und 600 € bezahlt worden waren, ohne dass die auskunftspflichtige Stelle in irgendeiner Weise reagiert hatte. Erst nach Festsetzung eines weiteren Zwangsgeldes in Höhe von

1.500 € gab es eine Rückfrage durch das Unternehmen, bei dem sich dann herausstellte, dass der Geschäftsführung der durch die Aufsichtsbehörde überprüfte Fall noch gar nicht bekannt war und offensichtlich eine Mitarbeiterin, die die ersten Schreiben der Aufsichtsbehörde, möglicherweise auch die des Petenten, nicht ordnungsgemäß bearbeitet und weitergeleitet hatte, die bisher fällig gewordenen Verwaltungsgebühren und Zwangsgelder aus eigener Tasche bezahlt hatte. Die Reaktion des Unternehmens war insoweit also nur dem Umstand zu verdanken, dass sich die betreffende Mitarbeiterin zum Zeitpunkt der Zustellung des letzten Zwangsgeldbescheides im Mutterschaftsurlaub befunden und diesen daher nicht hatte „abfangen“ können.

11 Zusammenarbeit mit anderen Aufsichtsbehörden

Die obersten Datenschutzaufsichtsbehörden der Bundesländer treffen sich zweimal jährlich im sogenannten *Düsseldorfer Kreis*, um ihre Rechtsauffassungen in grundsätzlichen oder sonst besonders wichtigen datenschutzrechtlichen Fragen sowie länderübergreifenden Sachverhalten untereinander abzustimmen; teilweise geschieht dies zusätzlich auch im schriftlichen Verfahren. Die im Berichtszeitraum gefassten Beschlüsse, die auch dann veröffentlicht werden, wenn einzelne Aufsichtsbehörden durch Enthaltung zum Ausdruck bringen, dass sie sich der Rechtsauffassung nicht anschließen, sind unter Pkt. 12 dieses Berichts abgedruckt. Der Freistaat Sachsen wird im Düsseldorfer Kreis durch den Sächsischen Datenschutzbeauftragten vertreten, insbesondere ist er darüber hinaus auch ständiges Mitglied in dessen - gleichfalls zweimal jährlich tagenden - Arbeitsgruppe „Telekommunikation / Tele- und Mediendienste“. Weitere Arbeitsgruppen beschäftigen sich intensiv mit den Themenbereichen „Versicherungen“, „Internationaler Datenverkehr“, „Kreditwesen“ und „Auskunfteien“; daran kann sich meine Behörde aufgrund ihrer personellen Ausstattung bisher leider nur in recht beschränktem Ausmaß beteiligen, obwohl hier vielfach Vorentscheidungen für den Düsseldorfer Kreis fallen.

Eher praktischer Natur sind die Fragen, die auf den jährlich durchgeführten Workshops der Datenschutzaufsichtsbehörden diskutiert werden. Diese Treffen dienen dem Erfahrungsaustausch sowie der Sicherstellung einer zumindest in wesentlichen Punkten einheitlichen Kontrollpraxis. 2007 fand der Workshop im Landesverwaltungsamt Sachsen-Anhalt in Halle, 2008 bei der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen in Düsseldorf statt. An beiden Veranstaltungen hat meine Behörde mit eigenen Beiträgen teilgenommen.

12 Beschlüsse des Düsseldorfer Kreises

12.1 Sitzung vom 19./20. April 2007 in Hamburg

12.1.1 Kreditscoring / Basel II

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich beurteilen die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten beim Einsatz von Scoring-Verfahren im Bereich der Kreditwirtschaft wie folgt:

I. Welche personenbezogenen Merkmale dürfen für die Berechnung des Scores genutzt werden?

1. Es dürfen nur Parameter genutzt werden, deren Bonitätsrelevanz mittels eines den wissenschaftlichen Standards entsprechenden mathematisch-statistischen Verfahrens nachgewiesen wurde. Die statistische Relevanz eines Parameters ist für die Einstellung in das Scoring-Verfahren eine notwendige, aber noch keine hinreichende Bedingung.

2. Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG dürfen nur Daten erhoben und gespeichert werden, soweit dies zur Zweckbestimmung eines Vertragsverhältnisses erforderlich ist. Die Tatsache, dass ein Scoring-Verfahren durchgeführt wird, ändert daran nichts und erweitert nicht den Berechtigungsrahmen der Banken. Es dürfen daher nur Daten in ein Scoring-Verfahren eingestellt werden, die das Institut im Rahmen eines Kreditvertrages erheben darf (Erforderlichkeitsprinzip). Soweit Daten für andere Zwecke, etwa aufgrund von Vorgaben des KWG oder des WpHG erhoben und gespeichert wurden, dürfen diese Daten nur für diese Zwecke, nicht jedoch für Scoring-Verfahren verwendet werden. (Da sensitive Daten im Sinne des § 3 Abs. 9 BDSG nicht nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG erhoben und verarbeitet werden, dürfen diese auch nicht in die Score-Berechnung einfließen.)

3. Das Scoring-Verfahren selbst stellt eine Datennutzung dar. Für diese gilt § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Danach ist die Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Ein berechtigtes Interesse der Banken an der Nutzung der für das Scoring-Verfahren verwendeten Parameter kann in der Regel angenommen werden. Wenn das Kreditinstitut die Möglichkeit hat, konkrete, unmittelbar bonitätsrelevante Daten zu erheben, darf es nicht auf Daten zurückgreifen, die nur Indizcharakter haben.

Soweit ein berechtigtes Interesse der Banken vorliegt, ist bei jedem einzelnen Parameter zu überprüfen, ob der Betroffene überwiegende schutzwürdige Interessen am Ausschluss der Datennutzung geltend machen kann. Die hier vorzunehmende Abwägung stellt einen normativen Prozess dar; die bloße statistische Relevanz eines Kriteriums führt noch nicht dazu, dass nicht von überwiegenden schutzwürdigen Interessen des Betroffenen auszugehen ist.

Bei der Abwägung können die gesetzgeberischen Wertungen aus § 10 Abs. 1 Satz 3 ff. KWG herangezogen werden. § 10 Abs. 1 KWG gilt zwar als bankenaufsichtsrechtliche Norm nur für die Erhebung und Verarbeitung personenbezogener Daten zur internen Risikobemessung (Eigenkapitalausstattung), nicht jedoch für das Scoring im Außenverhältnis zu den (potentiellen) Kundinnen und Kunden. Die Wertungen aus § 10 Abs. 1 Satz 3 ff. KWG können allerdings als gesetzgeberisches Leitbild in die Auslegung des BDSG einfließen. Das gilt insbesondere für die Anforderungen an Scoring-Merkmale. Die Merkmale müssen daher nicht nur mathematisch-statistisch erheblich sein, sondern eine ebenso hohe Stringenz aufweisen wie die im Merkmalskatalog des § 10 Abs. 1 Satz 6 KWG aufgeführten Regelbeispiele. So sind Angaben zur Staatsangehörigkeit bereits aufgrund des ausdrücklichen Verbots in § 10 Abs. 1 Satz 3 KWG als Score-Merkmale ausgeschlossen.

Bei der Abwägung sind darüber hinaus Wertungen des Grundgesetzes wie auch des einfachen Rechts daraufhin zu überprüfen, ob eine Benachteiligung der (potentiellen) Kundinnen und Kunden aufgrund eines bestimmten Kriteriums unzumutbar ist.

4. Auch wenn sich Basel II vornehmlich mit der Eigenkapitalhinterlegung der Institute befasst, wird der Einsatz von Scoring-Verfahren zunehmend dazu führen, jeden Kredit entsprechend dem individuellen Risiko zu bezinsen. Nur wenn in einer Gesamtschau der Kriterien sichergestellt ist, dass diesem Anliegen Rechnung getragen wurde, erfolgt die Datennutzung zur Wahrung berechtigter Interessen und sind keine überwiegenden schutzwürdigen Interessen der Betroffenen tangiert.

II. Wie transparent müssen die Bewertungen für die Betroffenen sein?

Für die Betroffenen (wie auch für die Aufsichtsbehörden) muss nachvollziehbar sein,

1. welche personenbezogenen Merkmale in die Berechnung des Score-Wertes einfließen;

2. welche konkreten personenbezogenen Daten der kreditsuchenden Person dafür genutzt wurden;

3. welches die maßgeblichen Merkmale sind, die den konkreten Score-Wert der betroffenen Person negativ beeinflusst haben. Diese maßgeblichen Merkmale sollen nach ihrer Bedeutung bzw. den Grad ihres Einflusses auf den konkreten Score-Wert aufgelistet werden, wobei sich die Auflistung auf die vier bedeutsamsten Merkmale beschränken soll.

Darüber hinaus ist bei der Anwendung von Scoring-Verfahren der § 6a BDSG zu beachten.

12.1.2 Internationaler Datenverkehr

1. Der Düsseldorfer Kreis beschließt das anliegende **Positionspapier**[1] zum internationalen Datenverkehr. Der BlnBDI wird gebeten, das Papier als Vorsitzender der AG „Internationaler Datenverkehr“ an die damals beteiligten Wirtschaftsvertreter zu versenden, die zugleich darauf hingewiesen werden sollen, dass weitere Fallkonstellationen in einer allgemein zugänglichen Handreichung näher dargestellt werden.

   Die im Positionspapier genannten Auffassungen können von den Aufsichtsbehörden bei der Beratung auch anderer Wirtschaftsvertreter genutzt werden.

2. Der Düsseldorfer Kreis beschließt ferner die anliegende **Handreichung**[1] zur rechtlichen Bewertung von Fallgruppen zur internationalen Auftragsdatenverarbeitung. Sie beinhaltet die häufigsten Fallkonstellationen und soll den Unternehmen die rechtliche Bewertung erleichtern. Im Einzelfall kann eine abweichende Bewertung erforderlich sein. Deshalb verbieten sich schematische Lösungen. Den Aufsichtsbehörden wird anheim gestellt, die Handreichung im Internet zu veröffentlichen oder auf andere Weise interessierten Unternehmen zugänglich zu machen.

12.1.3 Erhebung von Positivdaten zu Privatpersonen bei Auskunfteien

Nicht nur sog. Verbraucherauskunfteien wie beispielsweise die SCHUFA, sondern auch Handels- und Wirtschaftauskunfteien erheben und verarbeiten zunehmend Bonitätsdaten zu Privatpersonen, die nicht gewerblich tätig sind. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen in diesem Zusammenhang darauf hin, dass die Handels- und Wirtschaftsauskunfteien insoweit dieselben datenschutzrechtlichen Vorgaben zu beachten haben wie die „Verbraucherauskunfteien“.

[1] Das Positionspapier und die Handreichung finden Sie auf der Webseite des BfDI: http://www.bfdi.bund.de/cln_118/DE/Entschließungen/DuesseldorferKreis/DKreis_node.html.

Handels- und Wirtschaftsauskunfteien können daher sog. Positivdaten zu Privatpersonen grundsätzlich nicht auf Grundlage des § 29 Abs. 1 BDSG erheben. Denn bei Positivdaten - das sind Informationen, die keine negativen Zahlungserfahrungen oder sonstiges nicht vertragsgemäßes Verhalten zum Inhalt haben - überwiegt das schutzwürdige Interesse der betroffenen Personen, selbst über die Verwendung ihrer Daten zu bestimmen. Werden die Daten übermittelt, ist insoweit bereits die Übermittlung nach § 28 BDSG regelmäßig unzulässig.

Will eine Auskunftei Positivdaten zu Privatpersonen erheben, bedarf es dafür einer wirksamen Einwilligung der Betroffenen im Sinne des § 4a BDSG. Sofern die Auskunftei oder ihre Vertragspartner zu diesem Zweck eine für eine Vielzahl von Fällen vorformulierte Einwilligungsklausel verwenden, die als Allgemeine Geschäftsbedingung im Sinne des § 305 BGB zu werten ist, muss eine entsprechende Einwilligung darüber hinaus den Anforderungen des § 307 BGB genügen.

12.1.4 Weitergabe von Kundendaten durch Versandhandelsunternehmen an Auskunfteien

Die Übermittlung von personenbezogenen Daten über das vertragsgemäße Zahlungs- und Geschäftsabwicklungsverhalten ihrer Kunden sowie die Übermittlung von Scorewerten, die auf der Grundlage dieses Verhaltens berechnet wurden, durch Versandhandelsunternehmen an Auskunfteien zur Nutzung für deren eigene Geschäftszwecke ist unzulässig, es sei denn, die Kunden haben ausdrücklich in die Weitergabe dieser Daten eingewilligt.

Ein Datenschutzhinweis in den Allgemeinen Geschäftsbedingungen eines Versandhandelsunternehmens entspricht weder der Form noch dem Inhalt nach den Anforderungen an eine wirksame Einwilligung im Sinne von § 4a BDSG. Eine Einwilligung der Kunden setzt voraus, dass diese ausdrücklich darauf hingewiesen werden, welche Daten zu welchem Zweck an wen weitergegeben werden sollen.

Die Zulässigkeit einer Weitergabe von Kundendaten in dem genannten Umfang kann nicht auf § 28 BDSG gestützt werden, da sie nicht der Zweckbestimmung des Vertragsverhältnisses des Versandhandelsunternehmens mit dem Kunden dient (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG) und die schutzwürdigen Interessen der Kunden an dem Ausschluss der Weitergabe ihrer Daten an Auskunfteien überwiegen (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG). Die Kunden, die im Versandhandel bestellen, müssen nicht damit rechnen, dass ihr bisheriges Kundenverhalten gegenüber einem Versandhaus entscheidend dafür sein kann, ob sie Lieferungen von anderen Unternehmen erhalten, die bei einer Auskunftei Bonitätsauskünfte einholen. Die Kunden dürfen nicht zum Objekt wirtschaftlichen

Handelns dadurch gemacht werden, dass der Handel selbst definiert, was für die Kunden bzw. ihre Daten gut ist. Sie haben daher ein überwiegendes schutzwürdiges Interesse an dem Ausschluss der Vermarktung ihrer positiven Bonitätsdaten.

12.1.5 Weitergabe von umzugsbedingten Adressänderungen durch Versandhandelsunternehmen

(In der Fassung vom 26. Juni 2007)

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich stellen dazu fest: Übermittelt ein Unternehmen Umzugsadressen seiner Kunden an andere Unternehmen zur weiteren Übermittlung dieser Adressänderungen an angeschlossene Unternehmen zum Zwecke des Adressabgleichs, so ist dies nur mit einer ausdrücklichen Einwilligung der Betroffenen gemäß § 4a BDSG zulässig.

Ein Datenschutzhinweis in den Allgemeinen Geschäftsbedingungen eines Versandhandelsunternehmens entspricht weder der Form noch dem Inhalt nach den Anforderungen an eine wirksame Einwilligung im Sinne von § 4a BDSG. Eine Einwilligung der Kunden setzt voraus, dass diese ausdrücklich darauf hingewiesen werden, welche Daten zu welchem Zweck an wen weitergegeben werden sollen.

12.1.6 Mahnung durch Computeranruf

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich stellen dazu fest:

Eine telefonische Mahnung durch Computeranruf ist wegen der hohen Gefahr, dass ein anderer als der vorgesehene Empfänger die Nachricht erhält und so personenbezogene Daten einem Dritten unbefugt offenbart werden, unzulässig.

12.2 Sitzung vom 8./9. November 2007 in Hamburg

12.2.1 Gesetzesinitiative der Bundesregierung zu Auskunfteien und Scoring

Im modernen Wirtschaftsleben kommt Auskunfteien eine ständig wachsende Bedeutung zu. Diese sammeln eine Vielzahl von persönlichen Daten auch über Privatpersonen, um sie Dritten insbesondere für die Beurteilung der Kreditwürdigkeit ihrer Geschäftspartner gegen Entgelt zur Verfügung zu stellen.

Während in der Vergangenheit vor allem Kreditinstitute, der Versandhandel und Telekommunikationsunternehmen Auskünfte abgefragt haben, werden Informationen zur Beurteilung der Kreditwürdigkeit zunehmend auch von Vermietern, Versicherungen und sonstigen Unternehmen eingeholt. Von den Auskunfteien wird dabei vielfach ein so

genannter Scorewert übermittelt. Hierbei handelt es sich um einen Wert, der auf der Grundlage eines mathematisch-statistischen Verfahrens aus den bei der Auskunftei vorhandenen Angaben errechnet wird und eine Aussage über die Wahrscheinlichkeit des künftigen Zahlungsverhaltens der Betroffenen und damit über ihre Kreditwürdigkeit enthält.

Der Aufbau und die Erweiterung der zentralen Datenbestände über Betroffene bei Auskunfteien und die branchenübergreifende Bereitstellung dieser Informationen für eine Vielzahl von Unternehmen sowie der zunehmende Einsatz von Scoring-Verfahren gefährden nachhaltig das Recht auf informationelle Selbstbestimmung der Betroffenen.

Vor diesem Hintergrund begrüßt der Düsseldorfer Kreis im Grundsatz den vom Bundesministerium des Innern vorgelegten Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes, mit dem die Rechte der Betroffenen gestärkt und insbesondere auch die Transparenz beim Einsatz von Scoring-Verfahren verbessert werden sollen.

Nach Auffassung des Düsseldorfer Kreises bedarf der vorliegende Gesetzentwurf allerdings einer grundlegenden Überarbeitung, um das Ziel der Stärkung der Rechte der Betroffenen auch tatsächlich zu erreichen.

Dabei muss insbesondere sichergestellt werden, dass die bei Auskunfteien gesammelten Daten die Erstellung umfassender Persönlichkeitsprofile von Betroffenen nicht zulassen. Darüber hinaus ist gesetzlich eindeutig zu regeln, dass die Einholung einer Bonitätsauskunft auch in Zukunft an das Vorliegen eines finanziellen Ausfallrisikos geknüpft bleibt. Die im Entwurf derzeit vorgesehene Regelung, wonach jedes rechtliche oder wirtschaftliche Interesse einschließlich der Vermeidung allgemeiner Vertragsrisiken ein berechtigtes Interesse darstellen kann, würde die Rechte der Betroffenen unverhältnismäßig beeinträchtigen.

Des Weiteren muss eindeutig klargestellt werden, dass nur vertragsrelevante Daten in die Berechnung eines Scorewerts einbezogen werden dürfen. Im Übrigen dürfen die Auskunftsrechte der Betroffenen nicht durch die pauschale Berufung auf ein Geschäftsgeheimnis vereitelt werden.

12.2.2 Anwendbarkeit des Bundesdatenschutzgesetzes auf Rechtsanwälte

Der Düsseldorfer Kreis begrüßt, dass die Bundesregierung in ihrer Stellungnahme zum 21. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erklärt hat, dass die Erhebung und Verwendung personenbezogener - auch mandatsbezogener - Daten durch Rechtsanwälte den Vorschriften des Bundesdaten-

schutzgesetzes unterliegt und dass die Aufsichtsbehörden der Länder zuständig sind, die Datenschutzkontrolle durchzuführen.

Der Düsseldorfer Kreis sieht darin die Bestätigung seiner Auffassung, dass das Bundesdatenschutzgesetz (BDSG) - auch hinsichtlich mandatsbezogener Daten - auf Rechtsanwälte anwendbar ist. In der Bundesrechtsanwaltsordnung (BRAO) befinden sich aus datenschutzrechtlicher Hinsicht nur punktuelle Regelungen (§ 43a Abs. 2 BRAO Schweigepflicht, § 50 BRAO Handakten). Die Vorschriften des BDSG treten gemäß § 1 Abs. 3 BDSG lediglich insoweit zurück, als bereichsspezifische Datenschutzvorschriften bestehen. Durch das anwaltliche Berufsgeheimnis werden die Informationsrechte der Aufsichtsbehörden nach § 38 BDSG in Verbindung mit § 24 Abs. 6 und 2 BDSG nicht eingeschränkt.

12.3 Sitzung vom 17./18. April 2008 in Wiesbaden

12.3.1 Datenschutzkonforme Gestaltung sozialer Netzwerke

Der datenschutzgerechten Gestaltung sozialer Netzwerke im Internet kommt eine zentrale Bedeutung zu. Die Aufsichtsbehörden rufen in diesem Zusammenhang in Erinnerung, dass Anbieter in Deutschland zur Einhaltung des Regulierungsrahmens zum Datenschutz verpflichtet sind.

Insbesondere sind folgende rechtliche Rahmenbedingungen einzuhalten:

- Anbieter sozialer Netzwerke müssen ihre Nutzer umfassend gemäß den gesetzlichen Vorschriften über die Verarbeitung ihrer personenbezogenen Daten und ihre Wahl- und Gestaltungsmöglichkeiten unterrichten. Das betrifft auch Risiken für die Privatsphäre, die mit der Veröffentlichung von Daten in Nutzerprofilen verbunden sind. Darüber hinaus haben die Anbieter ihre Nutzer aufzuklären, wie diese mit personenbezogenen Daten Dritter zu verfahren haben.

- Die Aufsichtsbehörden weisen darauf hin, dass nach den Bestimmungen des Telemediengesetzes (TMG) eine Verwendung von personenbezogenen Nutzungsdaten für Werbezwecke nur zulässig ist, soweit die Betroffenen wirksam darin eingewilligt haben. Bei Werbemaßnahmen aufgrund von Profildaten müssen die Betroffenen nach den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) mindestens eine Widerspruchsmöglichkeit haben. Die Aufsichtsbehörden empfehlen, dass die Anbieter die Nutzer selbst darüber entscheiden lassen, ob - und wenn ja, welche - Profil- oder Nutzungsdaten zur zielgerichteten Werbung durch den Anbieter genutzt werden.

- Die Aufsichtsbehörden erinnern weiterhin daran, dass eine Speicherung von personenbezogenen Nutzungsdaten über das Ende der Verbindung hinaus ohne Einwilligung

der Nutzer nur gestattet ist, soweit die Daten zu Abrechnungszwecken gegenüber dem Nutzer erforderlich sind.

- Für eine vorauseilende Speicherung von Daten über die Nutzung sozialer Netzwerke (wie auch anderer Internet-Dienste) für eventuelle zukünftige Strafverfolgung besteht keine Rechtsgrundlage. Sie wird insbesondere auch nicht durch die Regelungen zur Vorratsdatenspeicherung vorgeschrieben.

- Schließlich weisen die Aufsichtsbehörden darauf hin, dass das TMG die Anbieter dazu verpflichtet, das Handeln in sozialen Netzwerken anonym oder unter Pseudonym zu ermöglichen. Dies gilt unabhängig von der Frage, ob ein Nutzer sich gegenüber dem Anbieter des sozialen Netzwerks mit seinen Echtdaten identifizieren muss.

- Die Anbieter sind verpflichtet, die erforderlichen technisch-organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Sie müssen insbesondere einen systematischen oder massenhaften Export oder Download von Profildaten aus dem sozialen Netzwerk verhindern.

- Bei der datenschutzfreundlichen Gestaltung von sozialen Netzwerken kommt den Standardeinstellungen - z. B. für die Verfügbarkeit von Profildaten für Dritte - eine zentrale Bedeutung zu. Die Aufsichtsbehörden fordern die Anbieter sozialer Netzwerke auf, datenschutzfreundliche Standardeinstellungen für ihre Dienste zu wählen, durch die die Privatsphäre der Nutzer möglichst umfassend geschützt wird. Diese Standardeinstellungen müssen besonders restriktiv gefasst werden, wenn sich das Portal an Kinder richtet. Der Zugriff durch Suchmaschinen darf jedenfalls nur vorgesehen werden, soweit der Nutzer ausdrücklich eingewilligt hat.

- Der Nutzer muss die Möglichkeit erhalten, sein Profil auf einfache Weise selbst zu löschen. Schließlich sollten die Anbieter sozialer Netzwerkdienste die Einführung von Verfallsdaten oder zumindest automatische Sperrungen erwägen, die von den Nutzern selbst festgelegt werden können.

12.3.2 Internet-Portale zur Bewertung von Einzelpersonen

1. Die Datenschutzaufsichtsbehörden weisen darauf hin, dass es sich bei Beurteilungen und Bewertungen von Lehrerinnen und Lehrern sowie von vergleichbaren Einzelpersonen in Internet-Portalen vielfach um sensible Informationen und subjektive Werturteile über Betroffene handelt, die in das Portal eingestellt werden, ohne dass die Urheber erkennbar sind und die jederzeit von jedermann abgerufen werden können.

2. Anbieter entsprechender Portale haben die Vorschriften des Bundesdatenschutzgesetzes über die geschäftsmäßige Verarbeitung personenbezogener Daten einzuhalten.

3. Bei der danach gesetzlich vorgeschriebenen Abwägung ist den schutzwürdigen Interessen der bewerteten Personen Rechnung zu tragen. Das Recht auf freie Meinungsäußerung rechtfertigt es nicht, das Recht der Bewerteten auf informationelle Selbstbestimmung generell als nachrangig einzustufen.

12.3.3 Keine fortlaufenden Bonitätsauskünfte an den Versandhandel

Auskunfteien dürfen Bonitätsauskünfte gemäß § 29 Absatz 2 Nr. 1a BDSG grundsätzlich nur erteilen, wenn der Dritte, dem die Daten übermittelt werden sollen, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat.

Besteht zwischen diesem Dritten (also dem anfragenden Unternehmen) und dem Betroffenen ein Dauerschuldverhältnis, aufgrund dessen das anfragende Unternehmen während der gesamten Dauer des Bestehens ein finanzielles Ausfallrisiko trägt (z.B. Ratenzahlungskredit, Girokonto, Energielieferungs-, Telekommunikationsvertrag), so dürfen Bonitätsauskünfte nicht nur zu dem Zeitpunkt erteilt werden, zu dem der Betroffene ein solches Vertragsverhältnis beantragt hat, sondern während der gesamten Laufzeit des Vertragsverhältnisses und bis zur Erfüllung sämtlicher Pflichten des Betroffenen.

Ein Versandhandelsgeschäft stellt als solches kein Dauerschuldverhältnis dar. Die aufgrund der bisherigen Erfahrungen mit den Kunden möglicherweise bestehende Wahrscheinlichkeit und darauf gegründete Erwartung, dass der Kunde nach der ersten Bestellung wiederholt bestellen wird, und die zur Erleichterung der Bestellvorgänge möglicherweise erfolgte Einrichtung eines „Kundenkontos“ rechtfertigten es nicht, ein Versandhandelsgeschäft mit einem Dauerschuldverhältnis gleichzusetzen.

Ein berechtigtes Interesse seitens des Versandhandels gem. § 29 BDSG ist demnach nur gegeben, wenn aufgrund eines konkreten Bestellvorgangs ein finanzielles Ausfallrisiko vorliegt.

Nach Vertragsschluss sind Bonitätsauskünfte an Versandhändler dann nicht zu beanstanden, wenn ein Ratenzahlungskredit vereinbart wurde oder noch ein offener Saldo besteht. In allen anderen Fällen ist das Rechtsgeschäft nach Abwicklung des einzelnen Kaufgeschäftes für den Versandhandel abgeschlossen, ein berechtigtes Interesse an Bonitätsauskünften ist dann nicht mehr zu belegen. Damit sind Nachmeldungen oder sonstige Beauskunftungen in dieser Konstellation rechtlich unzulässig.

Hinweis:
Die Vertreter des Versandhandels und der Auskunfteien haben sich bereit erklärt, ihre Verfahren entsprechend den vorgenannten gesetzlichen Anforderungen bis spätestens Ende September 2008 umzustellen.

12.4 Sitzung vom 13./14. November 2008 in Wiesbaden

12.4.1 Datenschutzrechtliche Bewertung von digitalen Straßenansichten insbesondere im Internet

Bei digital erfassten Fotos von Gebäude- und Grundstücksansichten, 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 Veröffentlichung von georeferenziert und systematisch bereit gestellten Bilddaten unzulässig ist, wenn hierauf Gesichter, Kraftfahrzeugkennzeichen oder Hausnummern erkennbar sind. Den betroffenen Bewohnern und Grundstückeigentümern 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 Möglichkeit 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.

12.4.2 Novellierung des Bundesdatenschutzgesetzes in den Bereichen Adressenhandel, Werbung und Datenschutzaudit

Der Düsseldorfer Kreis begrüßt, dass die Bundesregierung durch eine Novellierung des Bundesdatenschutzgesetzes aus den jüngst bekannt gewordenen Datenschutzverstößen im Bereich der Privatwirtschaft Konsequenzen ziehen möchte. Die uneingeschränkte Streichung des Listenprivilegs und die Pflicht zur Einholung einer Einwilligung des Betroffenen bei der Übermittlung an Dritte oder bei der Nutzung für Werbezwecke für Dritte sind erforderlich, um das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger zu stärken. Hiervon wird künftig auch die Wirtschaft profitieren.

Die geplanten Änderungen ermöglichen es, Werbung zielgerichteter und ohne Streuverluste vorzunehmen und unerwünschte Belästigungen zu vermeiden, so dass das Verbrauchervertrauen in die Datenverarbeitung der Wirtschaft gestärkt wird. Die vorgesehenen Regelungen zur Klarstellung, wann eine wirksame Einwilligung in die Werbenutzung vorliegt, und dass diese nicht mit wichtigen vertraglichen Gegenleistungen gekoppelt werden darf, verbessern die Transparenz und die Freiwilligkeit für den Betroffenen.

Darüber hinaus hat die beim Datenschutzgipfel am 4. September 2008 eingesetzte Länderarbeitsgruppe weitere Vorschläge zur Verbesserung des Bundesdatenschutzgesetzes unterbreitet, die jedoch bisher nicht berücksichtigt wurden.

Die derzeit geplanten Vorschriften genügen nicht, um künftig im Bereich der privaten Wirtschaft ein ausreichendes Datenschutzniveau zu verwirklichen. Hierzu bedarf es zum einen einer angemessenen Ausstattung der Datenschutzaufsichtsbehörden. Es bedarf zum anderen gemäß den europarechtlichen Vorgaben wirksamer Einwirkungsbefugnisse. Hierzu gehört neben adäquaten Kontroll- und Sanktionsmitteln die Möglichkeit, bei schwerwiegenden Datenschutzverstößen die Erhebung und Verwendung personenbezogener Daten zu untersagen. Auch die Stellung der betrieblichen Datenschutzbeauftragten sollte gestärkt werden.

Die bisherigen Vorschläge des Bundesministeriums des Innern zur Einführung eines Datenschutzaudits sind nicht geeignet, den Datenschutz in der Wirtschaft zu verbessern.