Sächsischer Landtag
5. Wahlperiode

DRUCKSACHE 5/7447

Schutz des Persönlichkeitsrechts im nicht-öffentlichen Bereich

5. Tätigkeitsbericht

des

Sächsischen Datenschutzbeauftragten

Berichtszeitraum: 1. Januar 2009 bis 31. Dezember 2010

Dem Sächsischen Landtag

vorgelegt zum 31. März 2011

gemäß § 30 des Sächsischen Datenschutzgesetzes

Eingegangen am: 16. Dezember 2011 Ausgegeben am: 16. Dezember 2011

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: Bauherr, Lehrer, Beamter, 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: 0351/4935-401
Fax : 0351/4935-490

Besucheranschrift: Devrientstraße 1
01067 Dresden

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

Vervielfältigung erwünscht.

Inhaltsverzeichnis

Abkürzungsverzeichnis

a. a. O.	am angegebenen Ort
AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
AGG	Allgemeines Gleichbehandlungsgesetz
AktG	Aktiengesetz
AO	Abgabenordnung
ArbG	Arbeitsgericht
AWG	Außenwirtschaftsgesetz
Az	Aktenzeichen
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAG	Bundesarbeitsgericht
BCC	Blind Carbon Copy (Blindkopie-Empfänger)
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BFDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGBl	Bundesgesetzblatt
BGH	Bundesgerichtshof
BIOS	Basic Input Output System
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
BMI	Bundesministerium des Innern
BO	Berufsordnung
BR-Drs	Bundesrats-Drucksache
BVerwG	Bundesverwaltungsgericht
CC	Carbon Copy (Kopie-Empfänger)
DDoS	Distributed Denial of Service (Verteilte Dienstblockade)
DFB	Deutscher Fußball-Bund e. V.
DOI	Double Opt In

DSG NRW	Datenschutzgesetz Nordrhein-Westfalen
DuD	Datenschutz und Datensicherheit
EC	Electronic Cash
EDV	Elektronische Datenverarbeitung
EEG	Erneuerbare-Energien-Gesetz
eID	elektronischer Idenitätsnachweis
EnWG	Energiewirtschaftsgesetz
Erfa-Kreis	Erfahrungsaustausch-Kreis
EuGH	Europäischer Gerichtshof
GasGVV	Gasgrundversorgungsverordnung
GBO	Grundbuchordnung
GDD	Gesellschaft für Datenschutz und Datensicherung e.V.
GG	Grundgesetz
GmbH	Gesellschaft mit beschränkter Haftung
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GPS	Global Positioning System
GwG	Geldwäschegesetz
HeimG	Heimgesetz
HeizkostenV	Verordnung über die verbrauchsabhängige Abrechnung der Heiz- und Warmwasserkosten
HGB	Handelsgesetzbuch
HmbDSG	Hamburgisches Datenschutzgesetz
KUG	Kunsturheberrechtsgesetz
KWG	Kreditwesengesetz
LG	Landgericht
MaRisk	Mindestanforderungen an das Risikomanagement
NDSG	Niedersächsisches Datenschutzgesetz
NGO	non-governmental organization
NJW	Neue Juristische Wochenschrift
NJW-RR	Neue Juristische Wochenschrift Rechtsprechungs-Report
OLG	Oberlandesgericht
OWiG	Ordnungswidrigkeitengesetz

OWiZuVO	Ordnungswidrigkeiten-Zuständigkeitsverordnung
PAuswG	Personalausweisgesetz
PIN	Persönliche Identifikationsnummer
PM	Pressemitteilung
PostG	Postgesetz
RDV	Recht der Datenverarbeitung
RiStBV	Richtlinien für das Strafverfahren und das Bußgeldverfahren
SächsArchivG	Archivgesetz für den Freistaat Sachsen
SächsDSG	Sächsisches Datenschutzgesetz
SächsGVBl	Sächsisches Gesetz- und Verordnungsblatt
SächsJOrgVO	Sächsische Justizorganisationsverordnung
SGB	Sozialgesetzbuch
SQL	Structured Query Language (Datenbanksprache)
SSL	Secure Sockets Layer (Netzwerksicherheitsprotokoll)
StGB	Strafgesetzbuch
StromGVV	Stromgrundversorgungsverordnung
StVG	Straßenverkehrsgesetz
TAN	Transaktionsnummer
TB	Tätigkeitsbericht
ThürDSG	Thüringer Datenschutzgesetz
TMG	Telemediengesetz
URL	Uniform Resource Locator (Webadresse)
UWG	Gesetz gegen den unlauteren Wettbewerb
VG	Verwaltungsgericht
VwVfG	Verwaltungsverfahrensgesetz

Vorwort

Der nunmehr bereits fünfte Tätigkeitsbericht der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich im Freistaat Sachsen ist wiederum erheblich umfangreicher als der Vorgängerbericht und verdeutlicht damit die gewachsene Bedeutung des Datenschutzes, die deutlich gestiegene Sensibilität der Bevölkerung und natürlich auch die gestiegene Arbeitsbelastung der Aufsichtsbehörde.

Im Vergleich zum vorangegangenen Berichtszeitraum sind fast 60 % mehr Beschwerden eingegangen; die Zahl der Beratungsanliegen ist sogar um fast 160 % gestiegen. Dieses erhebliche Arbeitspensum zu bewältigen war nur möglich, indem einerseits den doch recht zahlreichen Anfragen zu Vorträgen oder Schulungen bzw. zur aktiven Teilnahme an Tagungen, Diskussionspodien oder ähnlichen Veranstaltungen nur in wenigen Ausnahmefällen entsprochen und andererseits die Durchführung von anlassfreien Kontrollen auf ein Minimum zurückgefahren worden ist. Gerade Letzteres schmerzt dabei besonders, da die Erfahrungen anderer Aufsichtsbehörden, darunter auch des (bis Ende 2006 zuständigen) Sächsischen Staatsministeriums des Innern (vgl. 1. - 3. TB) zeigen, wie sinnvoll, d. h. wegen bestehender Datenschutzmängel notwendig und wegen der damit verbundenen öffentlichen Auswertung für andere Unternehmen auch äußerst hilfreich, derartige Kontrollen sind.

Leider steht zu befürchten, dass sich auch zukünftig daran nicht viel ändern wird. Die angesichts des nachweisbar ständig wachsenden Arbeitsanfalls ohnehin immer knapper bemessenen Personalressourcen der Aufsichtsbehörde werden zum Jahresende absehbar weiter reduziert, da der Sächsische Landtag beschlossen hat, eine dann aus Altersgründen bei der Aufsichtsbehörde frei werdende Stelle zu streichen, d. h. nicht wieder adäquat zu besetzen. Dies ist vor allem auch deshalb wenig nachvollziehbar, weil damit eine im Berichtszeitraum in Reaktion auf die bundesweit bekanntgewordenen Datenschutzskandale erfolgte Stellenzuweisung praktisch fast umgehend wieder rückgängig gemacht wird. Dass es auch anders geht, beweist beispielsweise der Freistaat Bayern, der im Zuge der Einrichtung seines Landesamtes für Datenschutzaufsicht die Anzahl der mit der Datenschutzkontrolle im nicht-öffentlichen Bereich befassten Mitarbeiter in etwa verdoppelt (vgl. 3. TB 2007/2008 [Pkt. 1.1] und 4. TB 2009/2010 [Pkt. 1.3] des Bayerischen Landesamtes für Datenschutzaufsicht) und weitere Personalverstärkungen bereits angekündigt hat (PM „Unabhängiges Landesamt für Datenschutzaufsicht erhält neuen Präsidenten“ vom 4. August 2011, http://www.lda.bayern.de).

Die Folgen sind ebenso absehbar wie fatal: Die Aufsichtsbehörde wird sich auch künftig in erster Linie mit der Bearbeitung von Eingaben befassen und daher überwiegend nur

reaktiv tätig sein können. Die Tätigkeit im präventiven Bereich, sei es in Form von anlassfreien Kontrollen, sei es durch eine verstärkte Öffentlichkeitsarbeit (Internet, sonstige Veröffentlichungen, Vorträge etc.) oder auch im Rahmen der (umfassenden) Beratung wird sich auch weiterhin im Wesentlichen nur auf die Erfüllung der gesetzlichen Pflichtaufgaben (z. B. Tätigkeitsbericht, strikte Beachtung der gesetzlichen Grenzen der Beratungspflicht, weitgehender Verzicht auf anlassfreie Kontrollen) beschränken müssen; die Mitarbeit in richtungsbestimmenden bundesweiten Gremien (Arbeitsgruppen des Düsseldorfer Kreises) nur eingeschränkt möglich sein.

Auch wenn bei der zeitnahen und sorgfältigen Bearbeitung eingegangener Anfragen und Beschwerden also auch weiterhin keine Abstriche gemacht werden (können), ist an dieser Stelle darauf hinzuweisen, dass die Bearbeitung entsprechender Anliegen sachverhaltsabhängig natürlich auch einmal etwas länger dauern kann. Petenten, die schon nach wenigen Tagen äußerst ungeduldig nachfragen, wann denn mit einer (abschließenden) Bearbeitung ihres Anliegens zu rechnen ist, verkennen, dass es der Aufsichtsbehörde nur in wenigen, von der Sachlage her klaren und bekannten Fällen möglich ist, eine kurzfristige Antwort zu geben. Im Regelfall ist zunächst der jeweils handelnden Stelle in tatsächlicher und rechtlicher Hinsicht (mit den entsprechenden Fristen) Gelegenheit zur Stellungnahme zu geben. Danach können weitere Nachfragen, ergänzende (örtliche) Kontrollen oder auch Abstimmungen mit anderen Aufsichtsbehörden notwendig werden. Ziel ist es insoweit nichtsdestoweniger, den Petenten spätestens nach drei bis sechs Monaten eine Abschlussnachricht zukommen zu lassen. Da jedoch nicht immer alle verantwortlichen Stellen in ausreichender Weise kooperativ sind, kann sich die Bearbeitung im Einzelfall durchaus auch länger hinziehen. Müssen Auskünfte etwa im Wege förmlicher Heranziehungsbescheide (Widerspruchsfrist: ein Monat) erzwungen werden (vgl. Pkt. 10.1) und kommt es dabei ggf. noch zum Widerspruchs- oder gar Klageverfahren - letzteres war bislang noch nicht der Fall - ist schnell ein Jahr vergangen. Ähnlich verhält es sich, wenn erhebliche technische und organisatorische Mängel festgestellt worden sind, deren Beseitigung umfangreiche Sicherungsmaßnahmen erfordern, die entsprechend konzipiert und umgesetzt (ggf. auch angeordnet) werden müssen, ganz abgesehen davon, dass es auch hier - nur mit entsprechendem Zeitaufwand zu klärende - Meinungsverschiedenheiten zwischen verantwortlicher Stelle und Aufsichtsbehörde geben kann.

Glücklicherweise stellen solche langwierigen Fälle eher die Ausnahme dar. Im überwiegenden Teil aller Eingaben kann die Bearbeitung innerhalb der o. g. Fristen abgeschlossen werden. Dass dabei zahlreiche Veränderungen zugunsten des Datenschutzes bewirkt werden konnten, können Sie dem vorliegenden Bericht ebenso entnehmen wie die Tatsache, dass es um den Datenschutz im nicht-öffentlichen Bereich letztendlich nicht so

schlecht bestellt ist, wie die gewachsenen Eingabenzahlen vermuten lassen - nur 22 % aller Eingaben lagen tatsächlich Datenschutzverstöße zugrunde. Zudem ist gerade auch der hohe Zuwachs bei den an die Aufsichtsbehörde gerichteten Beratungsanliegen ein deutliches Indiz für ein gewachsenes Datenschutzbewusstsein in den sächsischen Unternehmen.

1 Datenschutzaufsicht im nicht-öffentlichen Bereich

1.1 Organisatorische und rechtliche Stellung der Aufsichtsbehörden

Der Sächsische Datenschutzbeauftragte ist seit dem 1. Januar 2007 zuständige Aufsichtsbehörde nach § 38 BDSG über nicht-öffentliche Stellen im Anwendungsbereich des Dritten Abschnitts des BDSG (§ 30a Satz 1 SächsDSG) und außerdem - dies muss nicht zusammenfallen! - Verwaltungsbehörde nach § 36 Abs. 2 OWiG, § 13 SächsOWiZuVO, also die für die Verfolgung von Ordnungswidrigkeiten nach § 43 BDSG zuständige Behörde.

Der bereits länger anhaltenden bundesweiten Tendenz der Übertragung der Aufgaben der Datenschutzaufsichtsbehörden nach § 38 BDSG auf den Landesdatenschutzbeauftragten sind im Berichtszeitraum noch das Land Brandenburg, später dann - bis zum 1. Juli 2011 - auch Baden-Württemberg, das Saarland sowie Hessen gefolgt. Damit besteht nun lediglich in den Freistaaten Bayern und Thüringen sowie in Sachsen-Anhalt noch eine Trennung der Datenschutzaufsicht für den öffentlichen und den nicht-öffentlichen Bereich, wobei nur in Thüringen und Sachsen-Anhalt noch eine (weisungsgebundene) Mittelbehörde als Datenschutzaufsichtsbehörde bestimmt ist, während in Bayern das Anfang 2009 eingerichtete „Landesamt für Datenschutzaufsicht“ inzwischen den Status einer obersten und unabhängigen, mithin also weisungsfreien, Landesbehörde besitzt.

Die beschriebene Entwicklung der Neuorganisation und Zusammenfassung der Datenschutzaufsichtsbehörden ist maßgeblich durch das bereits 2005 wegen des Vorwurfs der fehlerhaften Umsetzung des Artikels 28 der Europäischen Datenschutzrichtlinie, wonach die Kontrollstellen ihre Tätigkeit in völliger Unabhängigkeit wahrzunehmen haben, durch die Europäische Kommission eingeleitete Vertragsverletzungsverfahren gefördert worden. In diesem Vertragsverletzungsverfahren hat der EuGH am 9. März 2010 (Az.: C-518/07) entschieden, dass die Organisation der Datenschutzaufsicht in Deutschland nicht mit dem Gemeinschaftsrecht vereinbar ist, weil die (d. h. alle) mit der Datenschutzaufsicht über nicht-öffentliche Stellen betrauten Institutionen, wenn auch in unterschiedlicher Weise, staatlicher Aufsicht unterstehen und daher ihre Tätigkeit entgegen den Anforderungen von Art. 28 Abs. 1 Satz 2 der Europäischen Datenschutzrichtlinie nicht in völliger Unabhängigkeit ausüben.

In Sachsen betraf dies die Regelung in § 30a Satz 2 SächsDSG, wonach der Sächsische Datenschutzbeauftragte als Aufsichtsbehörde nach § 38 BDSG der Rechtsaufsicht der Staatsregierung unterliegt. Spätestens mit dem Urteil des EuGH war also unzweifelhaft

davon auszugehen, dass eine Rechtsaufsicht durch die Staatsregierung wegen Unvereinbarkeit mit dem vorrangigen Europarecht unzulässig ist. An dieser Stelle erscheint erwähnenswert, dass es seit dem Zeitpunkt der Übertragung der Kontrollzuständigkeit an den Sächsischen Datenschutzbeauftragten lediglich einen einzigen Fall gegeben hat, in dem die Sächsische Staatsregierung diese Rechtsaufsicht tatsächlich ausgeübt hat.

Die Sächsische Staatsregierung hat auf das genannte Urteil reagiert, indem sie bekanntgegeben hatte, bis zu einer Änderung dieser gesetzlichen Regelung von der Ausübung staatlicher Aufsicht gegenüber dem Sächsischen Datenschutzbeauftragten abzusehen (vgl. Stellungnahme der Staatsregierung gegenüber dem Verfassungs-, Rechts- und Europaausschuss zum Antrag der Fraktion DIE LINKE, Drs. 5/2759, vom 29. Juni 2010 zum Thema „Urteil des EuGH umsetzen, Unabhängigkeit des Sächsischen Datenschutzbeauftragten sichern statt Stellen zu streichen“).

Am 29. Juni 2011 hat dann der Landtag in zweiter Lesung das „Zweite Gesetz zur Änderung des Sächsischen Datenschutzgesetzes“ beschlossen, welches auch die Streichung von § 30a Satz 2 SächsDSG beinhaltet (SächsGVBl. S. 270). Unverändert bestehen geblieben ist insoweit aber die Regelung zur Dienstaufsicht in § 25 Abs. 4 SächsDSG. Sowohl die Regierungskoalition (vgl. Beschlussempfehlung und Bericht des Innenausschusses zur Drs. 5/5296 - Drs. 5/6063) als auch die Staatsregierung (Drs. 5/2759 - s. o.) vertreten die Auffassung, dass allein durch den Wegfall der Rechtsaufsicht den Vorgaben des EuGH-Urteils in ausreichender Weise Rechnung getragen worden ist.

Dieser Auffassung kann nicht gefolgt werden. Die Aufgabenwahrnehmung in völliger Unabhängigkeit, wie sie Art. 28 Satz 2 der Europäischen Datenschutzrichtlinie vorschreibt, betrifft auch die Dienstaufsicht. Dies gilt nicht nur für die Tätigkeit als Datenschutzaufsichtsbehörde nach § 38 BDSG, sondern - auch wenn dies formell nicht Gegenstand des Klageverfahrens vor dem EuGH gewesen ist - für die Stellung des Sächsischen Datenschutzbeauftragten und seiner Mitarbeiter insgesamt. Man darf auf die weitere Entwicklung in dieser Streitfrage gespannt sein, insbesondere darauf, ob dieser - auch von anderen Landesparlamenten vertretene - Standpunkt durch die Europäische Kommission akzeptiert oder stattdessen zu den bereits angedrohten Zwangsgeldzahlungen führen wird.

Abschließend noch ein paar kurze Anmerkungen zu den Anfang März 2011 erschienenen Meldungen (PM 36/11 des Ministeriums des Innern des Landes Sachsen-Anhalt vom 2. März 2011), wonach die Innenminister von Sachsen, Sachsen-Anhalt und Thüringen an der Absicht festhielten, für den Datenschutz im nicht-öffentlichen Bereich eine gemeinsame mitteldeutsche Kontrollinstitution zu schaffen. Als Begründung wurde angegeben, dass damit die durch Urteil des Europäischen Gerichtshofs erforderlich ge-

wordene Trennung der entsprechenden Kontrollinstitutionen von der ministeriellen Verwaltung termingerecht erfolgen solle, um Strafzahlungen nach Brüssel zu vermeiden.

Für die Umsetzung des EuGH-Urteils ist die Schaffung einer solchen Dreiländereinrichtung nicht erforderlich; die dazu erforderlichen Gesetzesänderungen können - wie die laufenden Gesetzgebungsverfahren zeigen - wesentlich schneller und damit termingerecht durch die Länderparlamente erfolgen. Die Schaffung einer länderübergreifenden Kontrollstelle ist im Übrigen aber auch deswegen abzulehnen, weil sie zu einer institutionellen Schwächung des Datenschutzes führen würde. Statt wie in Sachsen auch in Thüringen und Sachsen-Anhalt die Datenschutzkontrolle im öffentlichen und nicht-öffentlichen Bereich beim Landesdatenschutzbeauftragten zusammenzuführen, müsste in diesem Fall die bewährte Form einer einheitlichen Kontrollstelle im Freistaat Sachsen wieder rückgängig gemacht werden. Anstelle von (zukünftig zu erwartenden) drei Kontrollstellen (Landesbeauftragte) würden dann vier solcher Kontrollstellen in sich teilweise überschneidenden Kontrollbereichen (öffentlicher / nicht-öffentlicher Bereich) und mit den bekannten (in Sachsen durch die Zusammenlegung im Wesentlichen überwundenen) Abgrenzungs-, Kompetenz- und Zuständigkeitsproblemen agieren, was zumindest in Teilbereichen auf eine Konkurrenzsituation hinauslaufen und insgesamt zu einer Schwächung des Datenschutzes führen würde. Ob in diesem Zusammenhang die sicherlich wieder als Argument angeführte Ressourceneinsparung tatsächlich erreicht werden kann, erscheint mehr als zweifelhaft. Immerhin entstünde eine komplette zusätzliche Behörde mit demzufolge in jeder Hinsicht zusätzlichen Kosten. Bei den Landesdatenschutzbeauftragten bestehende vielfältige Synergieeffekte würden damit aufgegeben; zusätzliches Personal müsste eingestellt werden. Örtliche Kontrollen in den entlegeneren Bereichen der drei Länder würden erheblich aufwändiger und damit kostenintensiver und damit sicher auch seltener. Im Interesse einer effektiven Datenschutzkontrolle kann dies sicher nicht sein.

1.2 Aufgaben der Aufsichtsbehörden

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 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 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)

- **Anordnung von Maßnahmen** zur Beseitigung festgestellter technischer oder organisatorischer Mängel und - seit dem 1. September 2009 - nun auch von Verstößen bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten (§ 38 Abs. 5 Satz 1 BDSG)

- Verhängung von **Zwangsgeldern** zur Durchsetzung angeordneter Maßnahmen zur Mängelbeseitigung (§ 38 Abs. 5 Satz 2 BDSG) bis hin zur **Untersagung** der Erhebung, Verarbeitung oder Nutzung bzw. einzelner Verarbeitungsverfahren

- 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

- Durchführung von **Ordnungswidrigkeitenverfahren** nach den Tatbeständen des Bundesdatenschutzgesetzes (§ 13 OWiZuVO)

- 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, und im Übrigen auch keine Vorabkontrolle erforderlich ist.

Zum Stichtag 31. Dezember 2010 lagen insgesamt 27 Registermeldungen von 25 Unternehmen vor, die

- in 9 Fällen Verfahren von Handels- und Wirtschaftsauskunfteien,
- in 14 Fällen Verfahren von Markt- und Meinungsforschungsinstituten sowie
- in je 1 Fall den Betrieb eines Verfügungszentralregisters, eines Widerspruchsregisters, 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. Innerhalb des Berichtszeitraumes wurden drei diesbezügliche Einsichtnahme- bzw. Auskunftsbegehren 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 Berichtszeitraum wurden lediglich zwei Regelkontrollen durchgeführt. Dies hat seine Ursache vor allem wiederum darin, dass der Eingang von Beschwerden gegenüber dem vorhergehenden Berichtszeitraum um mehr als die Hälfte höher war und sich die Anzahl der an die Aufsichtsbehörde herangetragenen Beratungsanliegen mehr als verdoppelt und damit die ohnehin knappen personellen Ressourcen weitgehend gebunden haben. Nachdem sich die Personalsituation zum Ende des Berichtszeitraums infolge einer Neueinstellung etwas gebessert hat, ist für die Zukunft zu erwarten, dass sich die Aufsichtsbehörde verstärkt auch wieder der anlassfreien Kontrolltätigkeit widmen kann. Voraussetzung dafür ist allerdings, dass die im Zuge des allgemeinen Stellenabbaus auch für den Sächsischen Datenschutzbeauftragten beschlossenen Stellenkürzungen ohne Auswirkung auf die Aufsichtsbehörde nach § 38 BDSG bleiben.

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	**2009** **2010**
Auskunfteien	0	0	4	0	**1**
Markt- / Meinungsforschung	1	0	4	4	**0**
Auftragsdatenverarbeiter	10	1	0	1	**0**
Wohnungsunternehmen	0	46	19	15	**0**
Sparkassen / Banken	30	0	0	0	**0**
Verkehrsunternehmen	57	3	0	0	**0**
Versorgungsunternehmen	4	7	1	0	**0**
Altenpflegeheime	0	48	0	0	**0**
Wohlfahrtsverbände	0	0	10	7	**0**
Ärzte	0	0	0	25	**0**
Sonstige	2	5	7	3	**1**
Gesamtanzahl	104	110	45	55	**2**

Tab. 1: Anlassfreie Überprüfungen

Die beiden in vorstehender Tabelle ausgewiesenen, als örtliche Überprüfung ausgestalteten Kontrollen betrafen ein als Wirtschaftsauskunftei tätiges Unternehmen sowie einen Anbieter bzw. Betreiber einer Vielzahl von Internetportalen.

3.2 Unterrichtung der Aufsichtsbehörde

3.2.1 Auftragsdatenverarbeitungsaufträge öffentlicher Stellen

Nach § 7 Abs. 3 SächsDSG haben öffentliche Stellen, wenn sie im Rahmen der Auftragsdatenverarbeitung auf private Unternehmen als Auftragnehmer zurückgreifen, die zuständigen Aufsichtsbehörden zu unterrichten. Analoge Vorschriften finden sich in den Datenschutzgesetzen Hamburgs (§ 3 Abs. 3 Satz 2 HmbDSG), Niedersachsens (§ 6 Abs. 4 Satz 2 NDSG), Nordrhein-Westfalens (§ 11 Abs. 3 Satz 2 DSG NRW) und Thüringens (§ 8 Abs. 6 ThürDSG).

Dies führt bei den Auftraggebern und den Aufsichtsbehörden zu einem - dem Grunde nach vermeidbaren - Verwaltungsaufwand. Ein Nutzeffekt ist nicht erkennbar; es kann an dieser Stelle nur vermutet werden, dass die Unterrichtungspflicht auf die bis Mai 2001 im Bundesdatenschutzgesetz enthaltene Meldepflicht der hier betrachteten Auftragsdatenverarbeiter zurückzuführen ist. Diese Meldepflicht, damals noch Voraussetzung einer anlassfreien Kontrolltätigkeit (Regelaufsicht), ist jedoch im Zuge der seinerzeitigen Novellierung des Bundesdatenschutzgesetzes abgeschafft worden. Seither können die Aufsichtsbehörden alle Unternehmen ihres Zuständigkeitsbereiches auch

ohne konkreten Anlass bzw. auch bei fehlender Meldepflicht einer datenschutzrechtlichen Kontrolle unterziehen, womit sich die Frage nach dem Sinn und Zweck dieser, für nicht-öffentliche Auftraggeber im Übrigen nicht bestehenden, Unterrichtungspflicht stellt.

Bis zum Ende des Berichtszeitraums sind beim Sächsischen Datenschutzbeauftragten (seit Übernahme der Kontrollzuständigkeit für den nicht-öffentlichen Bereich am 1. Januar 2007) 35 derartige, also sächsische Unternehmen betreffende, Meldungen - überwiegend aus Sachsen - eingegangen.

3.2.2 Abrufberechtigte für das maschinell geführte Grundbuch

Das OLG Dresden ist für die Zulassung nicht-öffentlicher Stellen zum automatisierten Abrufverfahren aus dem maschinell geführten Grundbuch im Freistaat Sachsen zuständig und unterrichtet den Sächsischen Datenschutzbeauftragten als Aufsichtsbehörde nach § 38 BDSG über jeweils neue Teilnehmer an diesem Verfahren.

Hintergrund dafür bildet die Regelung des § 133 Abs. 5 GBO, wonach dann, wenn der (Daten-)Empfänger eine nicht-öffentliche Stelle ist, § 38 BDSG mit der Maßgabe gilt, dass die Aufsichtsbehörde die Ausführung der Vorschriften über den Datenschutz auch dann überwacht, wenn keine hinreichenden Anhaltspunkte für eine Verletzung dieser Vorschriften vorliegen. Es ist unschwer erkennbar, dass auch diese Vorschrift noch auf die bis Mai 2001 geltende Fassung des Bundesdatenschutzgesetzes zurückgeht, da sie für den speziellen Fall der Abrufberechtigung für das maschinell geführte Grundbuch eine (heute bereits im Bundesdatenschutzgesetz verankerte) Regelaufsichtsbefugnis anstelle der seinerzeit für die Aufsichtsbehörden noch geltenden Beschränkung auf die Anlassaufsicht vorsieht.

Im Gegensatz zu den unter Pkt. 3.2.1 beschriebenen Fällen der Auftragsdatenverarbeitungsaufträge öffentlicher Stellen ergibt hier ungeachtet der fehlenden gesetzlichen Verpflichtung eine (nach § 14 Abs. 1 SächsDSG zulässige) Unterrichtung der Aufsichtsbehörde aber auch Sinn, denn bei den Abrufberechtigten handelt es sich - anders als bei den üblicherweise in typischen, der Aufsichtsbehörde bekannten Geschäftsfeldern und für eine Vielzahl von Auftraggebern tätigen Auftragsdatenverarbeitern - nicht um Stellen, bei denen sich für die Aufsichtsbehörde die besondere Art der Datenverarbeitung und der sich daraus ergebende Kontrollbedarf bereits aus der Branche bzw. den angegebenen Geschäftszwecken ergeben.

Kontrollen bei den Abrufberechtigten konnten im Berichtszeitraum (anders als noch 2005/2006 - 3. TB, Pkt. 3.2) mangels ausreichender personeller Ressourcen (vgl. Pkt. 3.1) leider nicht durchgeführt werden.

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).

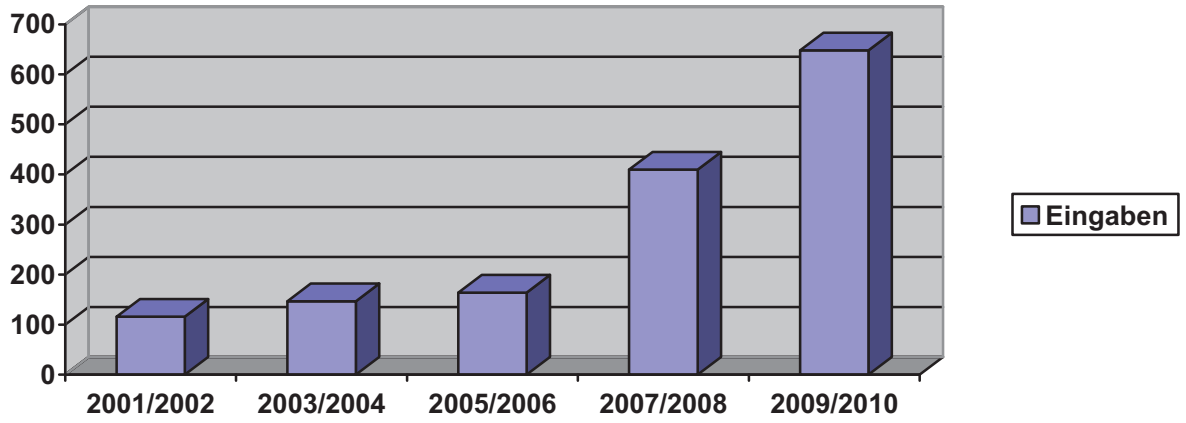
Von Anlasskontrollen wird im Gegensatz zu Regelkontrollen (vgl. Pkt. 3) immer dann gesprochen, wenn der Aufsichtsbehörde Anhaltspunkte für eine Datenschutzverletzung vorliegen. Zumeist geht ein solcher Anhaltspunkt aus einer Anfrage oder Beschwerde eines Betroffenen hervor. Darüber hinaus können aber 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 werden aber auch örtliche Überprüfungen (s. u.) 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 677 Fällen derartigen Anhaltspunkten nachgegangen worden. Was den Neueingang von Beschwerden (648 Fälle) betrifft, ist im Vergleich zum vorhergehenden Berichtszeitraum (410 Fälle) eine Steigerung um 58 % zu verzeichnen. 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	**2009 2010**
Neueingänge		116	147	164	410	**648**
zzgl. Übernahme Vorjahr		3	6	9	15	**29**
bearbeitete Eingaben gesamt		**119**	**153**	**173**	**425**	**677**
davon	örtliche Kontrollen	18	24	17	51	**68**
	begründet	50	65	62	87	**152**
	keine Zuständigkeit	27	26	31	57	**160**
	noch in Bearbeitung	6	9	15	29	**14**

Tab. 2: Bearbeitung von Eingaben



Die mit Abstand größte Anzahl der überprüften Sachverhalte (ca. 14 %) betraf den Umgang mit personenbezogenen Daten im Internet, wobei hier insbesondere die erhebliche Zahl der Beschwerden über unerwünschte Newsletter auffällig ist. Dabei handelte es sich jedoch keinesfalls immer um unzulässige Datennutzungen. Oftmals war den Betroffenen nicht mehr in Erinnerung, dass sie zuvor - etwa im Rahmen der Beteiligung an einem Gewinnspiel - ihr ausdrückliches Einverständnis - sogar im Double-Opt-In-Verfahren - zum Versand von Werbemails erteilt hatten. Möglicherweise war dies den jeweiligen E-Mail-Empfängern dabei auch deshalb nicht bewusst, weil diese Gewinnspiele durch einen Dritten veranstaltet worden waren. Die eingeholte Einwilligung war nichtsdestoweniger aber ausreichend und auch wirksam, da sie sich auch auf die Weitergabe der E-Mail-Adressen an konkret aufgeführte Sponsoren erstreckt hat.

Im Einzelnen verteilten sich die Schwerpunkte der anlassbedingten Kontrolltätigkeit der Aufsichtsbehörde im Berichtszeitraum wie folgt:

1.	Umgang mit Daten im Internet	96 Eingaben
	davon Werbemails (Newsletter)	*52 Eingaben*
2.	Videoüberwachung	52 Eingaben
3.	Rechte des Betroffenen	49 Eingaben
4.	Arbeitnehmerdatenschutz	41 Eingaben
5.	Gesundheitswesen	28 Eingaben
6.	Werbung	20 Eingaben
7.	Vermietung / Verpachtung	19 Eingaben
8.	Verkehrsbranche	12 Eingaben
	Tätigkeit von Auskunfteien	12 Eingaben
	Personalausweisdaten	12 Eingaben
9.	Umgang mit Daten durch Kreditinstitute	11 Eingaben
10.	Markt- und Meinungsforschung	10 Eingaben
	Zulässigkeitsfragen bei Bilddaten	10 Eingaben
11.	Datenverarbeitung durch Rechtsanwälte	9 Eingaben
	Datensicherungsmaßnahmen	9 Eingaben
12.	Energieversorgung	8 Eingaben
	Einzelhandel	8 Eingaben
13.	Finanzdienstleistungen	6 Eingaben
14.	Versicherungen	5 Eingaben
	Datenschutzbeauftragter	5 Eingaben
	bewusst illegale Datenverarbeitung	5 Eingaben
	Datenverarbeitung durch Vereine / Verbände	5 Eingaben

Nicht mehr auf dem ersten, aber wiederum auf einem Spitzenplatz zu finden sind demnach die Eingaben im Bereich der Videoüberwachung, welche immerhin noch einen Anteil von knapp 8 % am Gesamtumfang der bearbeiteten Eingaben haben. Mit einem Anteil von reichlich 7 % liegen dahinter die Beschwerden zur (Nicht-)Gewährung der Rechte der Betroffenen, hier wiederum in erster Linie das Auskunftsrecht betreffend, sowie Sachverhalte des Arbeitnehmerdatenschutzes (ca. 6 %). Markant ist dabei die deutliche Steigerung der Anzahl der Beschwerden (41) im Vergleich zum vorangegangenen Berichtszeitraum (22) bei Angelegenheiten des Arbeitnehmerdatenschutzes.

Bis Platz 5 (Gesundheitswesen - 4 %) sind die Eingabeschwerpunkte trotz veränderten Rankings gegenüber dem Berichtszeitraum 2007/2008 insgesamt praktisch unverändert geblieben. Absolut sind lediglich die Beschwerden zur Videoüberwachung etwas zurückgegangen, die anderen vier Bereiche haben aber auch insoweit deutlich zugelegt.

Deutlich zugenommen haben auch die Beschwerden im Bereich Vermietung / Verpachtung (von 10 auf 19), zur Datenverarbeitung durch Verkehrsunternehmen (von 5 auf 12) sowie betreffend die Erhebung, Verarbeitung und Nutzung von Personalausweisdaten (von 4 auf 12), hier insbesondere auch die Abforderung von Ausweiskopien bei Internetgeschäften.

Eine Steigerung um 33 % zu verzeichnen ist bei örtlichen Kontrollen: In den Jahren 2009 und 2010 wurden insgesamt 68 Überprüfungen bei 59 verantwortlichen Stellen durchgeführt. Die Gründe dieser naturgemäß vergleichsweise personalintensiven Variante der Kontrolltätigkeit lagen entweder in der besonderen Eilbedürftigkeit des Vorgangs, der Aussicht auf Vermeidung eines langwierigen Schriftwechsels, der Vermutung erheblicher Datenschutzverletzungen oder der Notwendigkeit, konkret das Vorhandensein bestimmter Daten im Unternehmen zu klären, beispielsweise auch die tatsächlichen Erfassungsbereiche von Videokameras zu ermitteln und die Speicherzeiten von Videoaufzeichnungen zu überprüfen.

Fast jeder vierten Eingabe (ca. 22 %) lag dabei im Ergebnis ein Verstoß gegen datenschutzrechtliche Vorschriften zu Grunde. Die festgestellten Datenschutzverstöße betrafen u. a. folgende Sachverhalte:

Nichtgewährung von Betroffenenrechten

- unvollständige, falsche oder unterlassene Auskunftserteilung (Pkt. 4.3.9.3)
- Verweigerung der Löschung
- Nichtbeachtung von Werbewidersprüchen (Pkt. 4.3.2.3)
- unvollständige Akteneinsicht bzw. Auskunftserteilung durch Ärzte (Pkt. 4.3.4.2)
- unzulässige Datennutzung infolge unzureichender Sperrung

Auftragsdatenverarbeitung

- Beauftragung von Subauftragnehmern ohne Kenntnis des Auftraggebers (Pkt. 4.3.13.1)
- kein schriftlicher Auftragsdatenverarbeitungsvertrag
- inhaltliche Mängel bei Auftragsdatenverarbeitungsverträgen

Betrieblicher Datenschutzbeauftragter

- Geschäftsführer als Datenschutzbeauftragter
- Personalleiter als Datenschutzbeauftragter
- kein Datenschutzbeauftragter bestellt
- fehlende Annahme der Bestellung durch den Datenschutzbeauftragten
- keine schriftliche Bestellung
- Widerruf der Bestellung mit dem Ziel der externen Vergabe (Pkt. 4.3.16.2)
- fehlende bzw. unzureichende interne Verarbeitungsübersicht sowie Mängel im öffentlichen Verfahrensverzeichnis

Meldepflicht

- unterlassene oder unvollständige Meldungen

Verarbeitung und Nutzung für Werbezwecke bzw. Vertragsangebote

- fehlende Unterrichtung über das Widerspruchsrecht
- Nutzung von Gesundheitsdaten ohne Einwilligung (Pkt. 4.3.4.6)
- Nichtbeachtung von Werbewidersprüchen
- Telefonanrufe ohne ausdrückliche Einwilligung
- Auswertung einer SCHUFA-Auskunft für Werbezwecke
- Vertragsangebot durch ein Kreditinstitut nach Auswertung von Kontobewegungen (Pkt. 4.3.6.2)
- Nutzung von Bewerberdaten für Werbezwecke (Pkt. 4.3.3.2)

Videoüberwachung

- fehlende Kennzeichnung
- Blutspendezentrum (Pkt. 4.3.1.4)
- Eingänge eines Pflegeheimes
- Mitarbeiter an den Kassen eines Fachmarktes
- Gaststätten (Sitzbereiche, Küche, Theken)
- Arbeitsbereiche in Bierwägen
- Treppenhaus eines Mehrfamilienhauses
- öffentliche Verkehrsflächen (Gehwege, Straßen, Schrankenanlagen, Parkplätze) (Pkt. 4.3.1.3)
- Fitnessstudios, Freizeitbäder (Pkt. 4.3.1.2)

Erhebung, Verarbeitung und Nutzung im Arbeitsverhältnis

- Rückgabe/Vernichtung von Bewerbungsunterlagen (Pkt. 4.3.3.1)

- offene Verteilung von Lohnzetteln
- Dokumentation der Krankheit bei Krankenrückkehrgesprächen (Pkt. 4.3.3.3)
- Aushang der Anzahl individueller Krankheitstage am Schwarzen Brett (Pkt. 4.3.3.4)
- Aushang personenbezogener Reklamationsstatistiken (Pkt. 4.3.3.5)
- Weitergabe von Personaldaten an die Konzernmutter in einem Drittstaat
- Aufbewahrungszeiten für Protokolle von Personalkontrollen (Supermarkt) (Pkt. 4.3.3.6)
- Abgleich von Arbeitnehmerdaten mit Antiterrorlisten (Pkt. 4.3.3.9)
- Weitergabe von Mitarbeiterdaten für Zwecke einer freiwilligen Zusatzversicherung (Pkt. 4.3.3.10)
- GPS-Geräte in Außendienstfahrzeugen (Pkt. 4.3.3.8)
- s. a. oben unter Videoüberwachung

Zulässigkeit der Erhebung und Speicherung bei Kaufverträgen

- Erfassung der Personalausweisnummer beim bargeldlosen Bezahlen
- Erhebung von Kundendaten bei Barzahlung und Sofortmitnahme
- unzureichende Einwilligungserklärungen bei Kundenkarten (Apotheken) (Pkt. 4.3.4.4)
- Inhalt von Schuldanerkenntnissen bei fehlendem Bargeld und/oder defekter EC-Karte einschließlich deren späterer Rückgabe bzw. Löschung (Pkt. 4.3.5.1)
- personenbezogene Erfassung verkaufter Eintrittskarten bei beschränktem Kartenkontingent im Fußball (Pkt. 4.3.7.1)
- Personalausweiskopien bei Bezahlung per Kreditkarte im Internet (Pkt. 4.3.15.2)

Zulässigkeit der Datenerhebung

- Telefonnummer als Pflichtfeld in einem Online-Shop
- Personalausweisnummer bei Kabelanschlussverträgen
- Personalausweiskopien bei Kontaktanzeigen (Pkt. 4.3.15.4)
- Privatanschrift von LKW-Fahrern bei Ladungsaufnahme (Pkt. 4.3.15.6)
- halbmonatliche Verbrauchswerte (Heizung, Warmwasser)
- Fernabfrage von Verbrauchswerten zur Klärung von Mietrechtsfragen (Pkt. 4.3.12.1)
- s. a. oben unter Zulässigkeit der Erhebung und Speicherung bei Kaufverträgen

Übermittlung / Veröffentlichung

- Weitergabe von Mieterdaten bei Auftrag zur Anfertigung eines Ersatzschlüssels
- Weitergabe von Kontodaten an Geschäftspartner zum selbstständigen Einzug ihm zustehender Serviceentgelte (Pkt. 4.3.13.2)
- Verkauf von Kundendaten (Telefonnummer) bei Geschäftsaufgabe
- (unverlinkte) Schuldnerlisten im Internet (Pkt. 4.3.2.10)

- Veröffentlichung von Babyfotos und -daten ohne Einwilligung im Internet
- Weitergabe der Daten von Versicherungsmaklern an Vertriebspartner zwecks Erschließung neuer Absatzmärkte

Markt- und Meinungsforschung

- Nichtbeachtung von Widersprüchen gegen die weitere Ansprache für Marktforschungszwecke (Pkt. 4.3.10.1)
- Abfrage von Gesundheitsdaten zum Aufbau eines Probandenstammes (Pkt. 4.3.10.2)

Technische und organisatorische Maßnahmen

- funktionsunfähige automatische Abmeldeschnittstellen bei Newsletterversand (Pkt. 4.3.2.3)
- unzureichende Schulung und Einweisung von Mitarbeitern in Datenschutzangelegenheiten (Pkt. 4.3.2.3)
- Versand von Massenmails mit offener Empfängerliste (Pkt. 4.3.2.4)
- Fehladressierung von Faxsendungen und E-Mails (Pkt. 4.3.2.8)
- Fehlleitung von Kontoauszügen und Rechnungen
- unterlassene Kontrolle von Patientenschließfächern nach Entlassung
- mangelhafte Sicherheitsmaßnahmen beim Betrieb eines Online-Shops (unzureichende Absicherung gegen unbefugte Zugriffe, fehlende Verschlüsselung bei der Datenübertragung)
- Versand von Zugangsdaten per unverschlüsselter E-Mail (Pkt. 4.3.2.8, 4.3.3.11, 4.3.8.4)
- ungenehmigte Weiterbearbeitung personenbezogener Daten auf Privat-PC's einschließlich der ungesicherten Übertragung per E-Mail
- Administratorrechte für Aufsichtsratsmitglieder (Pkt. 4.3.4.7)
- Personenverwechslungen durch mangelnde Sorgfalt bei der Datenerfassung
- Sichtbarkeit des Geburtsdatums im Klarsichtfeld eines Briefumschlages
- Möglichkeit des Mithörens von Patientenaufnahmegesprächen über unzureichend schallisolierte Lüftungsschächte
- allgemeine Einsehbarkeit eines Kontrollmonitors bei der Passagierabfertigung (Pkt. 4.3.14.1)
- offene Führung von Unterschriftslisten (Pkt. 4.3.7.4, 4.3.12.4)

- fehlende Verpflichtung auf das Datengeheimnis bzw. mangelhafte Verpflichtungserklärungen

4.2 Grenzen der aufsichtsbehördlichen Befugnisse

4.2.1 Zivilrechtliche Vorfragen

Bei der Aufsichtsbehörde gehen immer wieder Eingaben ein, die sich gegen Geldforderungen von Inhaltsanbietern im Internet (i. d. R. so genannte Abofallen) richten. Die betreffenden Petenten wollen dabei mit datenschutzrechtlichen Mitteln - etwa über die Bewertung als unzulässige Datenspeicherung einschließlich eines sich darauf stützenden Löschungsverlangens - einen Ausstieg aus den jeweils abgeschlossenen Ein- oder Zweijahresverträgen erreichen.

Nach den der Aufsichtsbehörde geschilderten Sachverhalten musste dabei in den meisten Fällen davon ausgegangen werden, dass sich die Petenten - um die auf diesen Websites jeweils angebotene Software downloaden oder die versprochenen Informationen abrufen zu können - auch tatsächlich dort registriert hatten, es sich also nicht um Identitätsmissbrauch (vgl. 4. TB, Pkt. 4.2.2.10) gehandelt hat. Wenn sowohl die Zugangsdaten als auch die Rechnung per E-Mail an den jeweiligen Nutzer versandt worden sind, ist insoweit nicht davon auszugehen, dass das Registrierungsformular missbräuchlich durch Dritte, die sich dadurch die Zugangsdaten erschleichen wollten, ausgefüllt worden ist, denn dann hätte die E-Mail mit der Rechnung die Petenten gar nicht erreichen können. Auch dafür, dass die Registrierungen durch die verantwortliche Stelle komplett gefälscht worden sein könnten, etwa durch Verwendung anderweitig (rechtswidrig) bezogener Kontaktdaten (Name, Anschrift, Geburtsdatum, E-Mail-Adresse), sind keine belastbaren Anhaltspunkte vorhanden gewesen.

Die Problematik der Abofallen ist ausreichend bekannt. Regelmäßig kommt es dabei darauf an, ob die Nutzer vor der Registrierung ausreichend und deutlich über die anfallenden Kosten informiert worden sind. Ob dies im Einzelfall jeweils der Fall gewesen ist, hat die Aufsichtsbehörde aber nicht zu beurteilen. Dies ist eine verbraucherrechtliche Problemstellung.

Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Darunter fällt auch die Geltendmachung und Durchsetzung etwaiger sich aus dem Vertragsverhältnis ergebender finanzieller Ansprüche.

Für die datenschutzrechtliche Beurteilung der Zulässigkeit einer Verarbeitung oder Nutzung personenbezogener Daten kommt es somit entscheidend auf die - in diesen Fällen regelmäßig strittigen - rechtlichen Voraussetzungen des Bestehens eines Schuldver-

hältnisses an. Zur Klärung dieser außerhalb des Datenschutzrechtes stehenden zivilrechtlichen Vorfragen ist die Datenschutzaufsichtsbehörde aber nicht berufen. Erst wenn diese Vorfragen geklärt sind, können die Betroffenen dann in einem nächsten Schritt ggf. die Löschung ihrer Daten durchsetzen und sich hierzu natürlich auch an die Aufsichtsbehörde wenden.

4.2.2 Umfang der Prüfungspflicht

Nicht jeder Petent ist mit dem durch die Aufsichtsbehörde erzielten Ergebnis auch zufrieden, insbesondere dann, wenn dieses nicht seinen Erwartungen entspricht, sei es, dass sich ein vermuteter Datenschutzverstoß nicht bestätigt hat, sei es, dass der Sachverhalt nicht bis ins Letzte hat aufgeklärt und damit auch nicht abschließend bewertet werden können. Mitunter wird dann versucht, über Kritik gegenüber den Vorgesetzten des jeweiligen Bearbeiters die Wiederaufnahme des Prüfverfahrens zu erreichen und dabei auch am besten der Aufsichtsbehörde gleich noch vorzugeben, wie der betreffende Sachverhalt weiter zu prüfen und zu bearbeiten ist.

Was das Ausmaß der Bemühungen der Datenschutzaufsichtsbehörde um Klärung des Anliegens eines Petenten in tatsächlicher und rechtlicher Hinsicht betrifft, ist zu beachten, dass das sog. Anrufungsrecht nach § 38 Abs. 1 Satz 8 BDSG i. V. m. § 21 Satz 1 BDSG die Behörde zu sachlicher Prüfung und Bescheidung, wohl eher nicht zur Begründung einer zurückweisenden Bescheidung (dies ist jedoch strittig), und nicht zu mehr verpflichtet und dem Petenten diesbezüglich auch keine weitergehenden Ansprüche gibt. Nach der Rechtsprechung besteht kein Anspruch auf bestimmte tatsächliche oder rechtliche Feststellungen, kein Anspruch auf umfassende Sachverhaltsprüfung und auch kein Anspruch auf umfassende Rechtmäßigkeitskontrolle hinsichtlich des zur Überprüfung gestellten Sachverhaltes. Mit anderen Worten: Der Beschwerde ist nachzugehen und über die Ergebnisse ist zu unterrichten, mehr nicht.

Zur Erläuterung: Es handelt sich bei der Anrufung der Datenschutzkontrolle nicht um die Auslösung einer Sachverhaltsklärung von derjenigen Intensität, wie sie die Rechtsordnung zur Durchsetzung des staatlichen Strafanspruches, also in Gestalt der Tätigkeit der Strafverfolgungsbehörden, vorsieht.

Natürlich bleibt es einem Petenten unbenommen, auf die Mitteilung des Prüfungsergebnisses neue Tatsachen vorzubringen, die zu einer geänderten Einschätzung der Angelegenheit führen könnten. Die Aufsichtsbehörde prüft dann, ob die angegebenen neuen Gesichtspunkte Anlass zu zusätzlichen Ermittlungen geben, ohne sich dabei aber vorschreiben lassen zu müssen, in welcher Weise diese dann ggf. durchgeführt werden.

4.2.3 Befragung Dritter

Gegenüber der Aufsichtsbehörde nach § 38 Abs. 3 BDSG auskunftspflichtig ist die der Kontrolle unterliegende (verantwortliche) Stelle, mithin also deren gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter. Liegt der zu überprüfende Sachverhalt schon eine Weile zurück und hat inzwischen beispielsweise die Geschäftsführung gewechselt, kann dies unter Umständen - weil man dazu eben auf Aussagen des früheren Geschäftsführers angewiesen ist - dazu führen, dass der Sachverhalt nicht mehr (vollumfänglich) aufgeklärt werden kann.

Die Sachverhaltsaufklärungsmöglichkeiten und -pflichten der Aufsichtsbehörde gehen nicht so weit, dass sie auch die Befragung Dritter, hier also eines früheren Geschäftsführers, umfassen. Denn gemäß § 38 Abs. 3 Satz 1 BDSG besteht eine Auskunftspflicht gegenüber der Datenschutzaufsichtsbehörde und dementsprechend deren Erhebungsbefugnis nur im Hinblick auf die sog. verantwortliche Stelle sowie die mit deren Leitung beauftragten Personen, d. h. die aktuell mit deren Leitung beauftragten Personen, nicht aber im Hinblick auf Dritte, die das einmal gewesen sind, jetzt aber nicht mehr befugt sind, für die verantwortliche Stelle zu sprechen.

Ein Petent hat in so einem Fall aber die Möglichkeit, entsprechende Feststellungen durch die Zivilgerichtsbarkeit - vor der dann auch ein ehemaliger Geschäftsführer als Zeuge aussagen müsste - anzustreben.

4.2.4 Unterrichtung Betroffener über Inanspruchnahme des Auskunftsverweigerungsrechts

Im Rahmen einer datenschutzrechtlichen Kontrolle war die Herkunft einer größeren Anzahl von Adressdaten nachzuweisen. Als Datenquelle kam dabei ein ganz konkretes Unternehmen in Frage, da nach Kenntnis des Petenten dort viele Betroffene als Kunden registriert waren. Bei der Kontrolle selbst konnten dafür allerdings keine Anzeichen gefunden werden, wobei der dazu auch konkret befragte Geschäftsinhaber diesbezüglich von seinem Auskunftsverweigerungsrecht Gebrauch gemacht hat.

Das hat zu der Frage geführt, in welchem Umfang die Petenten über das negative Ermittlungsergebnis zu unterrichten waren. Aus der Mitteilung, dass die von den Petenten als verdächtig genannte Stelle sich auf ihr Auskunftsverweigerungsrecht berufen habe, würden die Petenten wohl (nachvollziehbarerweise) abgeleitet haben, dass sie mit ihrer Vermutung Recht gehabt hatten. Im konkreten Falle ist daher die Mitteilung an den Petenten (Verarbeitungsbetroffenen) darauf beschränkt worden, dass

- nach § 38 Abs. 1 Satz 6 BDSG eine Befugnis zur Unterrichtung des Betroffenen nur dann besteht, wenn der Verantwortliche eines zu seinen Lasten gehenden Verstoßes gegen Vorschriften des Datenschutzes festgestellt werden konnte,
- im Hinblick auf die Erfolg versprechenden Ermittlungsansätze von den Befugnissen nach § 38 Abs. 4 BDSG Gebrauch gemacht worden ist, diese jedoch kein Ergebnis erbracht haben, das gemäß § 38 Abs. 1 Satz 6 BDSG, nämlich als Angabe einer hinreichend sicher festgestellten bestimmten Verletzungshandlung einer bestimmten verantwortlichen (nicht-öffentlichen) Stelle, mitgeteilt werden könnte,
- angesichts dessen der Vorgang unter dem ausdrücklichen Vorbehalt abgeschlossen wird, in dem Falle, dass neue Erkenntnisse zu erfolgversprechenden Ermittlungsansätzen eingehen, natürlich diesbezüglich erneut entsprechende Aufsichtsmaßnahmen getroffen werden könnten bzw. würden.

In dem Fall, dass ein Verarbeitungsablauf nicht hat aufgeklärt werden und insbesondere ein bestimmter Verarbeitungsverantwortlicher nicht hat feststellt werden können, umfasst die Übermittlungsbefugnis des § 38 Abs. 1 Satz 6 BDSG also nicht die Angabe, dass und aus welchen Gründen (insbesondere etwa Auskunftsverweigerung seitens einer verdächtigen Stelle!) eine Kontrolle bei einem vom Betroffenen angegebenen Verdächtigen, also einer möglicherweise als verantwortliche Stelle infrage kommenden Stelle, nicht zu einer hinreichenden Gewissheit geführt hat, dass diese angegebene und kontrollierte Stelle für die Verarbeitung verantwortlich gewesen ist.

Dies gilt nicht nur für § 38 Abs. 1 Satz 6 BDSG, sondern auch für § 23 Abs. 5 Satz 7 i. V. m. § 38 Abs. 1 Satz 8 BDSG (ebenfalls als Übermittlungsbefugnis ausgestaltet).

Davon zu unterscheiden ist der Fall, dass einem Petenten erläutert wird, warum ein Verarbeitungshandeln, das ihn betroffen hat, rechtmäßig gewesen ist. In diesem Fall hat die Aufsichtsbehörde aus allgemeinen rechtsstaatlichen Gründen eine Begründung dafür zu geben, warum sie eine Mitteilung nach § 38 Abs. 1 Satz 6 bzw. nach § 23 Abs. 5 Satz 7 i. V. m. § 38 Abs. 1 Satz 8 BDSG vollständig unterlässt.

4.3 Ausgewählte Sachverhalte

4.3.1 Videoüberwachung

4.3.1.1 Die Kamera im Vogelhäuschen

Es ist beileibe kein Einzelfall, dass sich Petenten wegen in Vogelhäuschen oder andernorts versteckter Videokameras an die Aufsichtsbehörde wenden. Fast immer verbergen sich dabei Nachbarschaftsstreitigkeiten hinter solchen Eingaben.

Ein Fall war aber in besonderer Weise kurios. Bemerkenswert war dabei nicht nur, dass in diesem Fall wieder einmal eine Videokamera in einem unmittelbar hinter dem Gartenzaun an einer Straße auf einer Stange montierten Vogelhäuschen versteckt war, sondern auch, dass sich dieses Vogelhäuschen immer wieder einmal bewegte. Der aufmerksame Beobachter - und davon gab es genug, weil sich direkt gegenüber ein Polizeirevier befand - konnte immer wieder Schwenkbewegungen über einen Winkel von knapp 180° feststellen, so als ob mit dieser Kamera die Straße bzw. das gegenüberliegende Gebäude überstrichen würde.

In dem betreffenden Vogelhäuschen befand sich auch tatsächlich eine Videokamera, dessen Drehbewegungen durch den betreffenden Grundstückseigentümer nach dessen Angaben über Angelsehnen gesteuert und die Bilder auf seinem Fernseher angezeigt würden; eine Aufzeichnung erfolge nicht. Zweck der Kamera sei einerseits die Beobachtung des links vom Vogelhäuschen befindlichen Eingangsbereiches seines Hauses sowie der rechts davon befindlichen Garageneinfahrten. Der Wechsel zwischen beiden Überwachungsbereichen führe dabei zu der festgestellten Schwenkbewegung. Die Kamera diene der Überwachung der Eingangstür, insbesondere der Feststellung, wer davor stehe und geklingelt habe, sowie der Überwachung der Garageneinfahrt, die häufig durch Falschparker - selbst durch Fahrzeuge der Polizei - zugestellt sei.

Auch wenn nachvollziehbar war, dass sich die im Polizeirevier tätigen Beamten durch diese Kamera permanent beobachtet fühlten, so war dies doch kein Fall, bei dem die Aufsichtsbehörde einschreiten konnte.

Der Anwendungsbereich des Bundesdatenschutzgesetzes in Bezug auf die Datenverarbeitung durch Privatpersonen ist nur dann eröffnet, wenn die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nicht nur ausschließlich für persönliche oder familiäre Tätigkeiten - wozu auch der Schutz des privaten Wohneigentums zählt - erfolgt, sondern darüber hinaus auch nur dann, wenn die (mittels Videokamera) erhobenen Daten auch tatsächlich gespeichert werden (vgl. § 1 Abs. 2 Nr. 3 BDSG). Diese Voraussetzungen lagen in dem geschilderten Fall nach den getroffenen Feststellungen nicht vor, d. h. die Kamera im Vogelhäuschen lag außerhalb der sich auf § 38 BDSG gründenden Kontrollzuständigkeit der Aufsichtsbehörde.

4.3.1.2 Freizeitbäder, Fitnessräume, Saunen

Über die Anforderungen an die Zulässigkeit von Videokameras in Freizeitbädern ist schon ausführlich im 3. TB (Pkt. 4.2.1.1) berichtet worden.

Eine sowohl Badeanlagen, einen Fitnessraum sowie zahlreiche Saunabereiche umfassende Freizeiteinrichtung hatte dabei besonders extensiv auf den Einsatz von Video-

überwachungstechnik gesetzt. Insgesamt waren 44 Kameras im Einsatz, davon allein 27 Kameras im Bereich der für die Besucher bestimmten Schrankanlagen.

Ursächlich für die eingegangene Beschwerde war dabei wohl insbesondere, dass die Umkleideschränke in Gruppen rechteckförmig angeordnet und diese Gruppen mit einer Eingangstür versehen waren und daher durchaus als eine Art Massenumkleide missverstanden werden konnten, zumal sich vor den Schränken in Kniehöhe ein umlaufendes Ablage- bzw. Sitzbrett befand. Jedenfalls waren insbesondere auch diese Bereiche annähernd lückenlos überwacht - über jeder Schrankgruppe waren an den beiden Stirnseiten jeweils gegenüberliegend zwei Kameras deutlich sichtbar an der Decke montiert.

Gegen die Videokameras im Bereich der Schrankanlagen bestanden allerdings keine Einwände. Dem Petenten war zwar zuzustimmen, dass die Vielzahl der (auch in den Gängen davor installierten) Kameras einen doch erheblichen Überwachungsdruck erzeugten, entscheidend für die datenschutzrechtliche Bewertung war jedoch, dass die eigentlichen Umkleidekabinen von der Überwachung ausgenommen waren und im Übrigen deutlich auf die Überwachung hingewiesen worden ist.

Nicht den datenschutzrechtlichen Anforderungen entsprachen jedoch die in den unmittelbaren Saunabereichen festgestellten Kameras:

Dies betraf zum einen eine Kamera direkt in einem thematisch gestalteten Saunaraum, in dem in der Vergangenheit (inzwischen durch Befestigung gesicherte) kleinere Dekorationsteile entwendet worden sein sollen. Derartige Vorkommnisse reichen weder aus, um die Erforderlichkeit der Videoüberwachung zu begründen, noch um die mit der Überwachung verbundene Beeinträchtigung schutzwürdiger Betroffeneninteressen zu rechtfertigen. Gerade in einer Sauna, in der sich die Gäste in der Regel unbekleidet und unter entsprechenden physischen Belastungen stehend aufhalten, ist deren Interesse, sich dabei nicht dem permanenten Überwachungsdruck einer Videoüberwachung auszusetzen, besonders schutzwürdig. Die - im Übrigen überall in einer solchen Einrichtung bestehende - Gefahr, dass Dekorations- oder sonstige Gegenstände geringen Wertes im täglichen Betrieb beschädigt werden oder abhanden kommen können, gehört zum normalen Betriebsrisiko und ist nicht geeignet, einen derart tiefgreifenden Eingriff in die Persönlichkeitsrechte der Saunagäste zu rechtfertigen, zumal dieser Gefahr vorliegend bereits durch eine entsprechende Befestigung dieser Teile begegnet worden war.

Weitere Kameras waren im Sauna-Ruhebereich, einer attraktiven, mit gepolsterten Sitz- und Liegemöbeln ausgestatteten Räumlichkeit, installiert. Auch hier war zur Begründung angeführt worden, dass es in der Vergangenheit vereinzelt zu Diebstählen von Ausstattungsgegenständen, wie beispielsweise Kissen, gekommen sei. Tatsächlich ist

dieser Sachverhalt aber nicht anders zu bewerten als die Überwachung der Saunaräume. Die schutzwürdigen Betroffeneninteressen betreffend ist dabei zu beachten, dass diese in öffentlichen Räumen, in denen sich Menschen typischerweise länger aufhalten, wo sie sich entspannen und miteinander kommunizieren, regelmäßig besonders hoch zu bewerten sind.

Wie eingangs bereits erwähnt, gehörte zu der betreffenden Freizeiteinrichtung auch ein - in Teilen gleichfalls videoüberwachter - Fitnessraum. Die vom Betreiber diesbezüglich zur Rechtfertigung angeführten, auf die Vermeidung und (ggf. rechtzeitige) Erkennung von Unfällen (Monitore an der Rezeption) gerichteten Gründe:

- (räumlich ungünstige) Lage des gering genutzten Fitnessraumes
- keine ständige Aufsichtsperson anwesend
- gelegentliche zweckfremde Nutzung durch Hotelgäste (Kinder)
- laufende Überprüfung von Ordnung und Sicherheit
- Überwachung der Einhaltung der Benutzerordnung

waren vom Grundsatz her anzuerkennen. Den Betreiber eines Fitnessraumes treffen entsprechende ständige Aufsichtspflichten (vgl. OLG Hamm, NJW-RR 1992, 243 f.). Er muss für den Fall von Verletzungen zur Verfügung stehen und steht in der Pflicht, die Fitnessgeräte und Räumlichkeiten so in Ordnung und gefahrlos zu halten sowie ständig zu kontrollieren, dass die Nutzer keine Gefährdung und Verletzung ihrer Gesundheit und ihres Lebens erleiden (vgl. OLG Stuttgart, NJW-RR 1988, 1082 f.).

Eine Aufzeichnung ist für diese Zwecke allerdings nicht erforderlich; eine Beobachtung - auch angesichts der Präventionswirkung der Videoüberwachung - vollkommen ausreichend. Eine Aufzeichnung dient weder der Unfallverhütung, noch verhindert sie einen falschen Gebrauch der Geräte, zweckfremde Nutzungen oder anderweitige Verstöße gegen die Benutzerordnung. Sie wirkt lediglich im Nachhinein, d. h. mit ihr könnten - soweit die Kameras den jeweiligen Sachverhalt überhaupt ausreichend detailliert erfassen - entsprechende Vorgänge allenfalls nachvollzogen werden. Ein rechtliches Erfordernis dafür ist nicht erkennbar, zumal dann im Grunde genommen alle Fitnessstudios mit Videoaufzeichnungstechnik ausgerüstet werden müssten. Auch dem Arbeitgeberverband deutscher Fitness- und Gesundheits-Anlagen liegen diesbezüglich keine Erkenntnisse vor, insbesondere hat dieser mitgeteilt, dass dort nicht bekannt sei, dass etwa Versicherungen Kameraaufzeichnungen verlangen würden.

4.3.1.3 Außenkameras an einem Nachtklub

In der Öffentlichkeit große Aufregung verursachte die Eröffnung eines Nachtklubs nicht zuletzt auch deswegen, weil sein an einer stark frequentierten Kreuzung gelegener Eingang mit immerhin sechs in den öffentlichen Verkehrsraum gerichteten Videokameras ausgerüstet war. Diese Kameras waren ständig, d. h. auch tagsüber, in Betrieb und erfassten annähernd komplett den öffentlichen Gehweg vor dem über Eck befindlichen Haupteingang des Klubs sowie entlang der beiden angrenzenden Gebäudefronten.

Im vorliegenden Fall der Videoüberwachung in der Umgebung eines Wohn- und Geschäftshauses kommt als Erlaubnistatbestand nur § 6b Abs. 1 Nr. 3 BDSG in Frage, d. h. die Videoüberwachung muss zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich sein und es dürfen keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen (hier: Passanten) überwiegen.

Seine Interessen hatte der Betreiber mit Sicherheitserwägungen für seinen Klub beschrieben. Dieser werde vorwiegend in den Nachtstunden betrieben und unterliege daher einem erhöhten Gefährdungsrisiko. Der Klub sei nur nach vorherigem Klingeln betretbar; geöffnet werde nur, wenn die Einlass begehrende(n) Person(en) auf dem Monitor vertrauenswürdig erscheine(n). Mit den rückwärts entlang der Gebäudefronten gerichteten Kameras solle zudem ausgeschlossen werden, dass sich hinter der Hausecke weitere „ggf. für einen Überfall bereite“ Personen versteckten.

Grundsätzlich sind generelle Sicherheitserwägungen - zumal unter den gegebenen Umständen eines Nachtbetriebs - als berechtigte Interessen anzuerkennen.

Berechtigte Interessen allein sind jedoch nicht ausreichend; § 6b BDSG fordert darüber hinaus auch, dass die Videoüberwachung zu dem angestrebten Zweck erforderlich sein muss, d. h. der Zweck muss mit der Videoaufzeichnung auch tatsächlich erreicht werden können und es darf keine milderen Mittel geben, mit denen der angestrebte Zweck gleichfalls erreicht werden kann.

Unbestritten sind Videokameras ein geeignetes Mittel, um sich vorab über einen Monitor einen Eindruck über die Einlass begehrenden Personen zu verschaffen (und diesen ggf. den Zutritt zu verwehren) sowie auch eine präventive Wirkung auf potentielle Randalierer zu erzielen. Für diesen Zweck ist jedoch weder die Überwachung des gesamten Gehweges noch eine Aufzeichnung notwendig, zumal sich die befürchteten Vorkommnisse dann wohl im Innern des Klubs abspielen würden.

Nicht geeignet waren die installierten Kameras zum Erkennen weiterer Personen, die sich mit Überfallabsichten hinter den Hausecken verstecken. Die beiden für diesen

Zweck installierten Kameras konnten dies gar nicht erkennbar machen, da sie den unmittelbaren Bereich an der Hauswand hinter den Hausecken gerade nicht erfassten (toter Winkel). Zudem stellte sich die Frage, wie relevant eine solche Annahme in der Praxis tatsächlich ist. Derartige Absichten hegende Personen können sich genauso gut in der näheren Umgebung, etwa hinter einem parkenden Auto, verstecken und würden dann ebenso wenig über die Videokameras entdeckt.

Für die Einlasskontrolle boten sich als Alternativlösung eine weit weniger in die Rechte Unbeteiligter eingreifende Klingelkamera oder einfach nur ein Türspion an. Klingelkameras bieten heute Bilder von guter Qualität und weisen einen weiten Erfassungsbereich auf, so dass sie für Zwecke der Einlasskontrolle durchaus ausreichend sein sollten. Eine weitere Möglichkeit bestand in der Verpflichtung eines Wachmannes bzw. Türstehers. Dies ist in der Branche durchaus üblich und ein bewährtes und wesentlich wirksameres Mittel, um Übergriffe oder Überfälle zu verhindern (bzw. unattraktiv zu machen), ein Sicherheitsgefühl bei Kunden und Personal zu erzeugen und insbesondere (was eine Videokamera nicht leisten kann) bei entsprechenden Vorkommnissen auch schnell und effektiv zu reagieren.

Im konkreten Fall war also schon nicht ersichtlich, dass die installierte Videoüberwachungsanlage nachts (tagsüber fehlt es wohl unstreitig schon an einem berechtigten Betreiberinteresse) tatsächlich zum Erreichen der angegebenen Zwecke erforderlich gewesen ist.

Für die Zulässigkeit einer Überwachungsmaßnahme dürfen darüber hinaus aber auch keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen (hier: Passanten) überwiegen. Da insbesondere der öffentliche Gehweg vor dem Klub (Kreuzungsbereich) sowie entlang der angrenzenden Straße in vollem Umfang überwacht worden war und für Passanten an diesen Stellen keine ihnen zuzumutende Ausweichmöglichkeit bestanden hat, war zweifelsfrei von solchen überwiegenden schutzwürdigen Betroffeneninteressen auszugehen. Angesichts der Lage in einem Gebiet mit starker Wohnbebauung und an der Kreuzung mit einer Hauptverkehrsstraße konnte auch nicht damit argumentiert werden, dass nachts (außer den Klubbesuchern) keine weiteren Passanten den öffentlichen Gehweg in diesem Bereich nutzen würden. Diese haben aber ein schützenswertes Interesse, während ihrer Bewegung im öffentlichen Raum nicht durch private Stellen mit Videokameras beobachtet zu werden und Aufnahmen von ihnen - für sie selbst weder beeinfluss- noch kontrollierbar - aufgezeichnet und für eine aus ihrer Sicht unbestimmte Zeit gespeichert werden, zumal sie selbst überhaupt keinen Anlass für eine solche Überwachung gegeben haben.

Der Betreiber hat schließlich drei der sechs Kameras abgebaut sowie die verbleibenden Kameras so ausgerichtet, dass sie nur noch den unmittelbar vor dem Eingang liegenden Bereich sowie die an einer der beiden Gebäudefronten befindliche Terrasse erfassten. Die bis zu diesem Zeitpunkt erfolgte Videoüberwachung ist zudem als Ordnungswidrigkeit verfolgt worden (vgl. Pkt. 11.1).

4.3.1.4 Blutspendezentrum

In einem Blutspendezentrum sollten an den Anmeldetresen installierte Videokameras die Sicherheit für die dort tätigen, die Aufwandsentschädigung an die Spender auszahlenden Mitarbeiter erhöhen, insbesondere das diesbezügliche Überfallrisiko minimieren und ggf. entsprechende Beweismittel sichern.

Ein besonderes Sicherheits- bzw. Schadensrisiko war in dem konkreten Fall nicht zu erkennen, denn die wesentlichen Geldmittel lagerten im Tresor des Spendezentrums. Es war somit nicht nötig, größere, d. h. etwa den ganzen Tagesbedarf abdeckende Geldmengen an den Anmeldetresen vorzuhalten. Zudem befand sich das Spendezentrum im dritten und vierten Obergeschoss eines Bürogebäudes - dies bedingte entsprechend lange Fluchtwege. Das Spendezentrum war immer sehr gut besucht - auch der damit gut besetzte Wartebereich unmittelbar vor dem Anmeldetresen verringerte die Erfolgsaussichten eines Überfalls. Insgesamt betrachtet sollte das Spendezentrum daher keine besondere Attraktivität für Überfälle aufweisen. Derartige Fälle sind während der Kontrolle auch nicht berichtet worden. Gleichwohl musste - wenn auch in begrenztem Ausmaß - von einem berechtigten Überwachungsinteresse des Betreibers ausgegangen werden.

Die jeweils zwei Kameras an den Anmeldetresen waren allerdings so eingestellt, dass sie auch größere Teile der Wartebereiche mit erfassten. Dies war zum Erreichen des oben dargestellten Zweckes nicht erforderlich. Eventuelle Täter werden ihre Forderung nicht aus dem Wartebereich heraus erheben, sondern an den Tresen herantreten. Der Erfassungsbereich war daher durch eine veränderte Kameraanordnung bzw. -einstellung entsprechend einzuschränken, so dass wartende Spender nicht mehr davon erfasst worden sind. Die in Berücksichtigung der oben vorgenommenen Risikobetrachtung nach § 6b Abs. 1 Nr. 2, Abs. 3 BDSG vorzunehmende Abwägung führte insoweit zum Überwiegen der einer Überwachung entgegenstehenden Spenderinteressen und daher zur Unzulässigkeit der vorgefundenen Kameraeinstellung.

Die beiden Kameras waren darüber hinaus auch so eingestellt, dass sie die hinter dem Anmeldetresen befindlichen Arbeitsplätze komplett erfassten. Die dort tätigen Mitarbeiter waren dadurch einem ständigen Überwachungsdruck ausgesetzt, dem sie sich prak-

tisch nicht entziehen konnten. Für den beabsichtigten Zweck (Sicherung der Geldauszahlung) wäre es ausreichend gewesen, wenn nur diejenige Hälfte des Anmeldetresens überwacht worden wäre, in der die Geldmittel aufbewahrt und die Aufwandsentschädigungen ausgezahlt werden, einschließlich desjenigen Bereiches, in dem ein etwaiger Täter sich das Geld geben lassen müsste. Nur insoweit war die Erforderlichkeit (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG) dieser Überwachung gegeben. Die an der Anmeldung tätigen Mitarbeiterinnen hätten dann einen Rückzugsbereich zur Verfügung, in dem sie ihren Aufgaben nachgehen könnten, ohne sich dabei ständig im Blickfeld der Kamera zu bewegen - ihren schutzwürdigen Interessen konnte damit in ausreichender Weise Rechnung getragen werden.

Weitere Kameras befanden sich in den Spendesälen. Über die diesen Kameras zugeordneten Monitore konnten die Spendesäle von den Mitarbeitern wechselseitig beobachtet werden und Spender gezielt auf freie Abnahmebereiche verwiesen werden.

Bei den Spendesälen handelte es sich nicht um öffentlich zugängliche Bereiche, denn die Zugänglichkeit eines Spendesaals bestimmt sich nicht nach allgemeinen Merkmalen, die von jedermann erfüllt werden können. Vielmehr bedarf es hierfür bestimmter körperlicher Voraussetzungen sowie insbesondere der Zulassung durch einen Arzt. Die Anwendung von § 6b BDSG schied also aus.

Stattdessen kam hier als Maßstab und Rechtsgrundlage § 28 BDSG in Frage. Da vorliegend aber keine Aufzeichnung (Speicherung) erfolgte, war gemäß § 1 Abs. 2 Nr. 3 das BDSG und namentlich sein in § 4 Abs. 1 ausgesprochenes Verbot mit Erlaubnisvorbehalt und ebenso gemäß § 27 Abs. 1 insbesondere auch der dritte Abschnitt des BDSG nicht anwendbar: Bei bloßer Beobachtung werden keine personenbezogenen Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet (vgl. Simitis in: Simitis, BDSG, 6. Aufl., Rn. 26 zu § 27, Rn. 58 zu § 28).

Diese Kameras fielen somit nicht unter das Bundesdatenschutzgesetz und lagen mithin außerhalb der Kontrollzuständigkeit der Aufsichtsbehörde, ihre Zulässigkeit war demnach nicht zu bewerten. Das bedeutete allerdings nicht, dass der Betrieb dieser Kameras nicht nach allgemeinem Zivilrecht wegen Verletzung des allgemeinen zivilrechtlichen Persönlichkeitsrechtes, § 823 Abs. 1 BGB, unzulässig gewesen sein kann.

4.3.1.5 Einsatz von Nachtsichtgeräten in Kinosälen

Die Überwachung von Kinobesuchern zum Zweck der Verhinderung des Anfertigens von Raubkopien mit Nachtsichtgeräten unterliegt nicht der Kontrolle des Sächsischen Datenschutzbeauftragten. Da es sich bei Nachtsichtgeräten nicht um „optisch-elektronische Einrichtungen“ (Videoüberwachungsanlagen) im Sinne des § 6b BDSG handelt,

ist dessen Anwendungsbereich nicht eröffnet. Denn ebenso wie sonstige, rein optische Sehhilfen (z. B. Brille, Fernglas) verfolgen Nachtsichtgeräte allein den Zweck, die Sehfähigkeit unter besonderen Bedingungen (hier: Dunkelheit) zu verbessern. Ihr Einsatz ist auf die reine Beobachtung beschränkt.

Der zum Teil vertretenen abweichenden Auffassung (vgl. Alich: „Task force“ im Kinosaal, DuD 2010, 44 ff. m. w. N.) dazu, dass Nachtsichtgeräte aufgrund ihrer speziellen technischen Gegebenheiten anders als die sonstigen, rein optischen Sehhilfen zu behandeln seien, vermag sich der Sächsische Datenschutzbeauftragte nicht anzuschließen. Denn es besteht kein Grund dafür, die Beobachtung im Dunklen gegenüber derjenigen im Hellen anders zu behandeln.

Da durch die Nachtsichtgeräte - jedenfalls in dem konkret zu prüfenden Fall - keine Daten aufgezeichnet worden waren und auch eine automatisierte Auswertung von Daten weder möglich gewesen war noch hatte stattfinden sollen, ist das Bundesdatenschutzgesetz auch sonst nicht anwendbar und eine Kontrollzuständigkeit der Aufsichtsbehörde somit nicht gegeben gewesen.

4.3.2 Internet

4.3.2.1 Soziale Netzwerke

In der Öffentlichkeit machen in erster Linie die großen international (z. B. Facebook) oder zumindest bundesweit (z. B. VZ-Netzwerke) wirkenden sozialen Netzwerke immer wieder von sich reden. Die Aufsichtsbehörden haben deren Entwicklung von Anfang an kritisch begleitet und weisen ständig auf (datenschutzrechtliche) Mängel der Netzwerke einerseits sowie die sich daraus ergebenden Risiken für die Privatsphäre andererseits hin (vgl. hierzu auch den Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 18. April 2008 „Datenschutzkonforme Gestaltung sozialer Netzwerke“ - 4. TB, Pkt. 12.3.1).

Daneben gibt es aber auch zahlreiche regionale Anbieter sozialer Netzwerke, die sich wegen ihrer lokalen Ausrichtung, insbesondere was das (auch reale) Kennenlernen neuer Leute und die zahlreichen Informationen über örtliche oder regionale Veranstaltungen (Tanzveranstaltungen, Partys etc.) betrifft, gerade bei Jugendlichen sehr großer Beliebtheit erfreuen.

Der Sächsische Datenschutzbeauftragte war und ist - abgesehen von der Mitarbeit in der Arbeitsgruppe „Telekommunikation / Tele- und Mediendienste“ (vgl. Pkt. 12) - in erster Linie mit solchen eher regional ausgerichteten Netzwerken befasst. Auch deren datenschutzrechtliche Bewertung orientiert sich selbstverständlich an dem o. g. Beschluss der

obersten Datenschutzaufsichtsbehörden. Die dabei im Berichtszeitraum festgestellten Mängel betrafen u. a. die Vorgaben der §§ 9 BDSG und 13 TMG (technische und organisatorische Maßnahmen, z. B. verschlüsselte Datenübertragung insbesondere von Passwörtern, Registrierungsdaten oder Bankverbindungen), die Privatsphäreeinstellungen (Voreinstellungen), fehlende Datenschutzerklärungen, AGB-Inhalte (viel zu weit reichende Klausel für Nutzungs- und Bearbeitungsrechte des Betreibers) und natürlich den Minderjährigenschutz.

Der Minderjährigenschutz nimmt inzwischen auch in der Tätigkeit der Datenschutzaufsichtsbehörden einen immer größeren Raum ein. Gerade bei minderjährigen Nutzern kommt den durch den Netzwerkbetreiber vorgegebenen Standardeinstellungen immense Bedeutung zu, da diese häufig noch nicht die Kenntnisse und das notwendige Problembewusstsein besitzen, um diese Voreinstellungen, etwa was die Sichtbarkeit von Profildaten für Dritte betrifft, besitzen (vgl. hierzu auch den Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 25. November 2010 „Minderjährige in sozialen Netzwerken wirksamer schützen“ - Pkt. 13.6.2).

Minderjährige haben im Übrigen - genauso wie alle übrigen Teilnehmer - die AGB anzuerkennen und somit eine Reihe von Einverständniserklärungen bzw. Einwilligungen zu erteilen. Ist ein Nutzer minderjährig und deshalb nur beschränkt geschäftsfähig, bedarf es zur Wirksamkeit dieser Erklärungen zusätzlich der Einwilligung seines gesetzlichen Vertreters. Nach den von der Rechtsprechung für die Einwilligung Minderjähriger in einen Eingriff in ihr Persönlichkeitsrecht aufgestellten Regeln ist auch noch nach dem 15. Lebensjahr neben der Einwilligung des Minderjährigen diejenige der Erziehungsberechtigten erforderlich (Urt. des BGH v. 28. September 2004 - VI ZR 305/03, NJW 2005, 56 ff.). Für die Lösung dieser Problematik ist bei sozialen Netzwerken bislang noch keine zufriedenstellende Lösung gefunden worden.

4.3.2.2 Gebäude- und Straßenansichten

Am 18. November 2010 ist der Internetdienst Google Street View in Deutschland online gegangen. Seitdem können Nutzer Straßenpanoramen der 20 größten deutschen Städte im Internet abrufen. In Sachsen betrifft das die Städte Dresden und Leipzig.

Die Fa. Google hat auf den Panoramaaufnahmen Fahrzeugkennzeichen und Gesichter verpixelt; darüber hinaus gibt es eine Möglichkeit zur Meldung nicht oder nur unzureichend erfolgter Verpixelungen sowie eine Funktion zum Ausblenden kompletter Häuser. Die deutschen Datenschutzaufsichtsbehörden haben dazu unter Federführung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit ein Verfah-

ren vereinbart, wie Betroffene bei Google Widerspruch gegen eine Veröffentlichung sie (als Mieter oder Eigentümer) betreffender Abbildungen einlegen können.

Trotz des großen Medienechos und der vielen kontrovers geführten Diskussionen zu den Zulässigkeitsvoraussetzungen eines solchen Internetangebots, haben sich die diesbezüglich bei der sächsischen Datenschutzaufsichtsbehörde eingegangenen Beschwerden und Anfragen in Grenzen gehalten. Inzwischen (April 2011) ist bekannt geworden, dass Google darüber hinausgehende Veröffentlichungen nicht (mehr) plane. Grund sei die von den Aufsichtsbehörden geforderte und bezüglich der ersten 20 Städte auch umgesetzte Vorab-Widerspruchsfrist gegen die Veröffentlichung der Bilder. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat aus diesem Grund mit Google vereinbart, dass die Daten derjenigen, die bereits einen Vorab-Widerspruch für ein Gebäude außerhalb der 20 bereits abgebildeten Städte bei Google eingelegt haben, zügig gelöscht werden sollen.

Internetdienste zur Abbildung von Gebäude- und Straßenansichten werden aber längst nicht mehr nur von Google angeboten. Es gibt neben Google weitere Anbieter, die vergleichbare Dienste bundesweit oder aber auch nur regional oder auf ein Stadtgebiet beschränkt - so auch in Sachsen - anbieten wollen oder auch schon im Betrieb haben. Als Beispiel sei etwa der Dienst „Bilderbuch Köln“ genannt, der auch schon Gegenstand einer gerichtlichen Entscheidung war. Das LG Köln (Az. 28 O 578/09) hat am 13. Januar 2010 einen Unterlassungsanspruch der Miteigentümerin eines Gebäudes gegen die Veröffentlichung von Lichtbildern dieses Gebäudes im Internet verneint und dies einerseits mit dem Medienprivileg gemäß § 41 BDSG - in dem betreffenden Internetangebot sind nicht nur Bildaufnahmen, sondern auch zahlreiche ergänzende Informationen zur Stadtgeschichte, Architektur usw. abrufbar - begründet, andererseits die Veröffentlichung aber auch unter Zugrundelegung des § 29 BDSG als zulässig bewertet. Die danach erforderliche Abwägung ginge zugunsten der Veröffentlichung aus, weil die ebenfalls verfassungsrechtlich gewährleistete Kommunikations-, Informations- und Meinungsfreiheit in diesem Fall höher zu bewerten seien, als das unter den konkreten Umständen nur marginal - die veröffentlichten Informationen eröffnen sich in gleicher Weise auch jedem Passanten, der über die betreffende Straße ginge - berührte informationelle Selbstbestimmungsrecht der Klägerin.

Die Diskussionen um Street View und vergleichbare Internetdienste haben von verschiedenen Seiten, nicht zuletzt auch von den Datenschutzaufsichtsbehörden, Forderungen nach speziellen gesetzlichen Regelungen für den Datenschutz bei Geodatendiensten aufkommen lassen. Das BMI hat dann - nachdem der Bundesrat einen Gesetzentwurf zu einer diesbezüglichen Änderung des Bundesdatenschutzgesetzes (BR-Drs 259/10) schon beschlossen hatte - mit dem so genannten „Rote-Linie-Gesetz“ einen

Gegenentwurf vorgelegt. Dieses Gesetz beschränkt sich darauf, eine „rote Linie“ für Internetdienste festzulegen, die unter keinen Umständen überschritten werden darf, und setzt darüber hinaus auf die Selbstverpflichtung der Internetwirtschaft, wie etwa den Kodex für Geodatendienste des Branchenverbandes BITKOM der Internetwirtschaft, der den Umgang mit Panoramabildern im Internet regeln soll. Aus Sicht der Datenschutzaufsichtsbehörden gibt es bei den letztgenannten Vorschlägen noch erhebliche Defizite, insbesondere bleibt der Datenschutz-Kodex der BITKOM erheblich hinter dem mit Google bezüglich Street View bereits vereinbarten Datenschutzniveau zurück, während das „Rote-Linie-Gesetz“ mit seinen Minimalregelungen der tatsächlichen Gefährdungslage im Internet in keiner Weise gerecht wird.

Solange es diesbezüglich keine verbindlichen gesetzlichen Vorgaben gibt, werden die Datenschutzaufsichtsbehörden bei der Bewertung von Internetangeboten zum Abruf georeferenzierter Straßen- oder Gebäudeansichten unabhängig davon, ob es sich um lokale, regionale oder bundesweite Angebote handelt, die bei Google Street View bereits erfolgreich durchgesetzten Grundsätze als Maßstab anlegen, d. h. insbesondere regelmäßig auch die Bereitstellung von Möglichkeiten, noch vor der Veröffentlichung dagegen Widerspruch einzulegen, fordern.

4.3.2.3 Dauerthema Newsletter

Schwerpunkt der internetbezogenen Eingaben bildete zweifellos das Thema Newsletter (vgl. Pkt. 4.1). Empfänger von Newsletter oder anderer Werbemails haben sich an die Aufsichtsbehörde gewandt, weil sie - ihrer Meinung nach - ohne ihre Zustimmung E-Mails mit Werbung erhalten haben und ihren Auskunfts-, Löschungs- oder Widerspruchsforderungen durch die verantwortliche Stelle nicht oder nicht ausreichend entsprochen worden sei.

In diesem Zusammenhang stellte sich regelmäßig auch die Frage nach der Zulässigkeit des Newsletterversands. Soweit die Einwilligung (Opt-In oder - um Identitätsmissbrauch auszuschließen - besser noch Double-Opt-In) des Empfängers eingeholt worden ist, war dies sicherlich unproblematisch. Auffällig waren dabei die zahlreichen Fälle, in denen die Betroffenen sich daran erst wieder erinnern konnten, als die verantwortliche Stelle Auskunft über die Herkunft der Daten von einem Dritten und das dort dokumentierte DOI gegeben hatte.

Die Aufsichtsbehörde ist aber auch gefragt worden, ob unter konkreten Umständen statt dessen auch eine Widerspruchslösung ausreichend sein kann. Im Speziellen waren Neukunden eines Internetportals im Rahmen der Einrichtung eines Benutzerkontos darüber informiert worden, dass die in diesem Zusammenhang anzugebende E-Mail-Adresse

auch für den Newsletterversand genutzt werde, man allerdings die Möglichkeit habe, diese Datennutzung im „Benutzerbereich abzustellen“ oder über einen Abbestelllink oder per E-Mail zu deaktivieren. Ein Petent hatte dies als unrechtmäßig angesehen und auch in diesem Fall ein Opt-In-Erfordernis gesehen, d. h. die bloße Unterlassung eines Widerspruchs als für den Newsletterversand nicht ausreichend angesehen.

Tatsächlich war aber gegen eine solche Verfahrensweise nichts einzuwenden.

Ein wettbewerbesrechtlicher Verstoß (der sich ggf. auch auf eine Zulässigkeitsbetrachtung nach dem Bundesdatenschutzgesetz auswirkt) war unter den bestehenden Umständen nicht anzunehmen. Zwar verlangt § 7 Abs. 2 Nr. 3 UWG die vorherige ausdrückliche Einwilligung des Adressaten, jedoch gilt dies dann nicht mehr, wenn - wovon hier ausgegangen werden konnte - die Voraussetzungen des § 7 Abs. 3 UWG erfüllt sind, d. h.

1. ein Unternehmer im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten hat,
2. der Unternehmer die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet,
3. der Kunde der Verwendung nicht widersprochen hat und
4. der Kunde bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.

Anders als bei der bekannten Payback-Entscheidung des BGH vom 16. Juli 2008 (VIII ZR 348/06) sind in dem hier betrachteten Sachverhalt Newsletter nur an eigene Kunden versandt worden. Ein wettbewerbesrechtlicher Verstoß lag somit nicht vor. Darüber hinaus stand das Bundesdatenschutzgesetz der angewandten Widerspruchslösung aber auch sonst nicht entgegen (vgl. § 28 Abs. 3 Satz 2, 3 und 6 sowie § 28 Abs. 4 BDSG). Nach § 28 Abs. 3 Satz 2 BDSG ist die Verarbeitung oder Nutzung listenmäßig oder sonst zusammengefasster Daten über Angehörige einer Personengruppe (hier: eigene Kunden), die sich auf …, seinen Namen, … beschränken, für eigene Werbezwecke zulässig, wenn diese dafür erforderlich ist und die Daten im Rahmen eines Vertragsverhältnisses erhoben worden sind. Gemäß Satz 3 dürfen für diese Zwecke weitere Daten (hier: E-Mail-Adresse) hinzugespeichert werden. Die Zulässigkeit der Verarbeitung und Nutzung der Gesamtdaten (Namen, E-Mail-Adressen) richtet sich dann wieder nach Satz 3 i. V. m. Satz 6, d. h. die Erforderlichkeit der Verarbeitung und Nutzung für eigene Werbezwecke muss gegeben sein und es dürfen keine schutzwürdigen Betroffen-

eninteressen entgegenstehen. Des Weiteren müssen die Voraussetzungen des § 28 Abs. 4 BDSG erfüllt sein (Unterrichtungspflichten, Widerspruchsrecht).

Viele Betroffene haben sich im Übrigen auch nur deshalb an die Aufsichtsbehörde gewandt, weil sie über einen längeren Zeitraum schlichtweg erfolglos versucht hatten, die Newsletter einfach nur abzubestellen. Die Gründe, warum dies vergleichsweise oft nicht funktioniert hatte, waren vielfältig. Neben technischen Problemen, wie z. B. dem Nichtfunktionieren automatischer Abmeldeschnittstellen (Abmeldebutton am Ende eines Newsletters), war auch die mangelnde Schulung von Mitarbeitern als wesentliche Ursache zu erkennen. Damit sind insbesondere die Mitarbeiter gemeint, die für die Abarbeitung der an allgemeinen Service-Adressen, wie etwa *info@unternehmen.de, service@unternehmen.de* oder selbst *datenschutz@unternehmen.de,* eingehenden E-Mails zuständig gewesen sind. Hinzu kam, dass Werbe-E-Mails - wohl zur Umgehung der von Empfängern der Einfachheit halber eingerichteter Spamfilter - auch gern von mitarbeiterbezogenen E-Mail-Konten (*vorname.name@unternehmen.de*) versandt worden sind und somit unter Nutzung der Antwortfunktion versandte Widersprüche, Auskunftsverlangen usw. natürlich auch bei diesen - in Datenschutzfragen leider oftmals nicht geschulten - Mitarbeitern gelandet sind. Schließlich ist noch zu erwähnen, dass für den Newsletterversand genutzte E-Mail-Accounts mitunter gar nicht für den Empfang von E-Mails konfiguriert sind und daher die unter Nutzung der Antwortfunktion versandten E-Mails der Nutzer den beabsichtigten Empfänger schlichtweg nicht erreichen.

Satz 1 der Anlage zu § 9 BDSG bestimmt, dass die innerbetriebliche Organisation so zu gestalten ist, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Sind die mit der inhaltlichen Betreuung allgemeiner Service-Adressen eines Unternehmens befassten Mitarbeiter bzw. die für den Newsletterversand (unter eigener E-Mail-Adresse) zuständigen Mitarbeiter nicht ausreichend hinsichtlich des Umgangs mit eingehenden Widersprüchen, Auskunfts- und Löschungsverlangen geschult, stellt dies einen datenschutzrechtlichen Mangel in der innerbetrieblichen Organisation dar, der durch die Aufsichtsbehörde entsprechend beanstandet wird.

4.3.2.4 Massen-E-Mails mit offener Empfängerliste

In mehreren Fällen wandten sich E-Mail-Empfänger an die Aufsichtsbehörde und übergaben Kopien von E-Mails, die eine mitunter seitenlange Adressliste mit teils mehreren Hundert Empfängern enthielten, ohne dass dem eine zwischen Absender und Empfängern vereinbarte Vorgehensweise zugrunde gelegen hatte bzw. sämtliche E-Mail-Adressen ohnedies jedem der Empfänger bereits auf andere Weise bekannt gewesen waren. Auf diese Weise ist also jedem Empfänger Kenntnis über die E-Mail-Adressen sämtlicher Mitempfänger verschafft worden.

In allen untersuchten Fällen hatten die Verantwortlichen versehentlich eine falsche Versandart (CC anstatt BCC) gewählt.

Datenschutzrechtlich stellte dies eine unzulässige Übermittlung personenbezogener Daten dar (Verstoß gegen §§ 4, 28 BDSG). Da sich die jeweiligen Vorfälle jedoch durchweg als einmalige Versehen herausstellten und die jeweils verantwortlichen Stellen einsichtig gewesen und zukünftig größere Sorgfalt zugesichert haben, ist von weiteren Maßnahmen abgesehen worden.

4.3.2.5 Parteienwerbung an dienstliche E-Mail-Adresse eines kommunalen Wahlbeamten

Einem kommunalen Wahlbeamten, der unerwünschte Parteienwerbung an seine personalisierte dienstliche E-Mail-Adresse erhalten hatte, musste leider mitgeteilt werden, dass er dies auf datenschutzrechtlicher Grundlage nicht unterbinden könne. Denn auch die personalisierte dienstliche E-Mail-Adresse ist lediglich eine Teilanschrift der öffentlichen Stelle, in der der Bedienstete Dienst tut. Sie dient der Ausübung des Amtes und ist daher kein Datum, das dem Datenschutz unterliegt. Anders als eine Privatperson genießt die öffentliche Stelle kein Recht auf Datenschutz. Sie ist nicht Träger des Grundrechts auf informationelle Selbstbestimmung. Daher konnte sich der betroffene Bedienstete gegen die vorliegende Parteienwerbung weder in seiner Eigenschaft als Privatperson noch als Amtsinhaber zur Wehr setzen. Auch der betroffenen öffentlichen Stelle stand keine Handhabe gegen die Werbe-E-Mails zu, da sich diese nicht aus datenschutzrechtlichen Gründen gegen Zusendungen von jedermann wehren kann. Erst recht gilt das für Parteienwerbung, die gegenüber normaler, gewerblicher Werbung grundsätzlich rechtlich privilegiert ist.

4.3.2.6 Datenspeicherung bei fehlgeschlagener Reisebuchung

Gehäuft eingegangen sind Eingaben zu Unternehmen, welche Reise- und Flugportale im Internet verantworten. Ein Teil konzentrierte sich darauf, dass Reisewillige erst nach Preisgabe ihrer Daten am Ende der Buchungsstrecke erfuhren, dass die von ihnen gewählte Reiseleistung nicht bzw. nicht mehr verfügbar war, die zuvor eingegebenen Daten jedoch trotz der fehlgeschlagenen Buchung weiter gespeichert wurden.

Die Prüfung des Sachverhaltes ergab, dass bei den Portalen auf eine Suchanfrage der Nutzer die Internetangebote diverser Fluggesellschaften und Reiseanbieter im Wege des sog. „Screen-Scraping“ auf passende Offerten durchsucht werden. Im Fall einer erfolgreichen Suche werden dem Reiseinteressenten im Anschluss an die Suchroutine die mit der Anfrage übereinstimmenden Angebote unterschiedlicher Anbieter nach Preisen sortiert angezeigt. Wählt der Reisewillige ein Angebot aus und bestätigt er eine Erhebungs-

maske mit personenbezogenen Daten, übermitteln die Portalbetreiber diese dem Buchungssystem der späteren Leistungserbringer als Buchungsanfrage in fremdem Namen, sie erbringen jedoch keine eigenen Reiseleistungen bzw. treten nicht als Reiseveranstalter auf. Rechtlich gehen der Reiseinteressent und die Portalanbieter folglich einen Geschäftsbesorgungsvertrag (§§ 675, 631 ff. BGB) gerichtet auf die Vermittlung von Reiseleistungen ein.

Bereits dieses Rechtsgeschäft legitimiert die zur Geschäftsbesorgung erforderliche Erhebung, Speicherung und Übermittlung personenbezogener Daten (vgl. § 28 Abs. 1 Satz 1 Nr. 1 BDSG), ohne dass es auf den Erfolg der Geschäftsbesorgung, also das Zustandekommen eines Reisevertrags mit einem Dritten, ankommt. Die Geschäftsbesorgung als eigenes Handelsgeschäft bedingt ferner gesellschaftsrechtlich nach § 257 Abs. 1 Nr. 2 HGB und steuerrechtlich nach § 147 Abs. 1 Nr. 2 AO die Aufbewahrung der Daten nach Maßgabe dieser Vorschriften auch nach Abschluss einer aus Kundensicht erfolglosen Geschäftsbesorgung, also dem Fehlschlag der Reisevermittlung mangels Verfügbarkeit der Reiseleistung. Die aus der Geschäftsbesorgung gewonnenen Daten sind jedoch gemäß § 35 Abs. 3 Nr. 1 BDSG für andere Zwecke zu sperren.

Eine generell fehlende Verfügbarkeit der von den Portalen angezeigten Reiseleistungen, wie sie teilweise in den Eingaben vermutet wurde, ist im Rahmen der datenschutzrechtlichen Prüfung nicht festzustellen gewesen. Erst wenn ein fehlendes Angebot zur Nichtigkeit der Geschäftsbesorgung führt, kann der Datenpreisgabe die rechtliche Grundlage entzogen sein.

4.3.2.7 Beim Fremdanbieter liegende Buchungsstrecke - Affiliate Marketing

Ein Reisewilliger hat sich an die Aufsichtsbehörde gewandt, weil er die Besorgnis einer unzulässigen Übermittlung seiner Daten von einem Internet-Reisevermittlungsportal zu einem anderen hegte, als er zu der von ihm gebuchten Reise eine Leistungsbestätigung eines für ihn bis dahin fremden Vermittlungsportals mit Sitz in den USA erhielt, welches auch seine Kreditkarte belastete.

Die Prüfung des Sachverhaltes ergab, dass der Reisewillige nach der Angebotsrecherche zu Beginn der Buchungsstrecke auf die Seiten des anderen Reisevermittlungsportals umgeleitet worden war, die optische Gestaltung des Internetauftritts aus Marketing-Gründen jedoch nicht wechselte, so dass der Buchende glaubte, sich weiterhin auf den Seiten des von ihm ursprünglich aufgerufenen Reisevermittlers zu befinden.

Eine solche Weiterleitung zu fremden Angeboten oder die Einbettung derselben auf dem eigenen Portal im Wege einer Affiliate-Marketing-Kooperation auf Provisionsbasis ist heute im Internet nicht weiter ungewöhnlich, erleichtert dies doch die wechselseitige

Kundengewinnung. Hinsichtlich des Umgangs mit personenbezogenen Daten hat die Prüfung im vorliegenden Fall ergeben, dass die Buchungsanfrage und die damit einhergehenden Datenerhebungen und -verarbeitungen ausschließlich auf der externen Buchungsstrecke des Fremdanbieters erfolgt waren, also keine Übermittlung zwischen beiden Anbietern erfolgt war. Der notwendige Hinweis auf die Vertragsbeziehung des Buchenden zum Fremdanbieter und damit dessen Erhebungs- und Verarbeitungsbefugnis ergab sich dabei in hinreichender Weise aus der Einbeziehung der diesen als Verwender nennenden AGB und der ihn als verantwortliche verarbeitende Stelle nennenden Angaben zum Datenschutz.

4.3.2.8 Fehlversand von Rechnungen und Logindaten per E-Mail

Ein Unternehmen, welches Schließfachanlagen vermietet, hatte die Jahresrechnungen an seine Online-Kunden fehlversendet: E-Mail-Adresse und Rechnungsempfänger passten nicht zusammen. Die Rechnungen hatten auch die Mietvertragsnummer und die Vertrags-PIN der Online-Kunden enthalten, wodurch die jeweiligen Empfänger in die Lage versetzt worden sind, Kenntnis von den Stammdaten (u. a. auch Bankverbindung) des eigentlichen Rechnungsadressaten zu erlangen.

Gem. § 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 Übermittlung der Bestandsdaten, hier also insbesondere von Login und PIN, war für die genannten Zwecke nicht erforderlich und hat demnach einen Verstoß gegen diese Vorschrift dargestellt.

Auch die Übermittlung der Vertragsdaten ist rechtswidrig gewesen: Gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG (in seiner bis 31. August 2009 gültigen Fassung) war das Übermitteln personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke nur zulässig, wenn es der Zweckbestimmung des Vertragsverhältnisses mit dem Betroffenen gedient hat. Die Bekanntgabe der Rechnungsdaten an Dritte bzw. die durch Bekanntgabe der Logindaten eröffnete Zugriffsmöglichkeit auf die Stammdaten eines Online-Kunden hat aber sicherlich nicht der Zweckbestimmung des mit den Online-Kunden abgeschlossenen Mietvertrages gedient.

Die Ursache für diesen Fehlversand war Unternehmensangaben zufolge in einem Software-Fehler zu suchen, der dem Unternehmen insoweit nur bedingt anzulasten war. Die Geschäftsleitung hat sofort nach Bekanntwerden des Vorfalls eine Reihe wirksamer Gegenmaßnahmen getroffen und dabei insbesondere auch sofort die PINs aller betroffenen Kunden geändert.

Dessen ungeachtet ist es natürlich unzulässig gewesen, auch die vollständigen Logindaten, insbesondere also die Vertrags-PIN, mit in die per E-Mail versandten Jahresabrechnungen aufzunehmen. Zugangsdaten, insbesondere Passwörter oder eben PINs, sind, damit sie die ihnen zugedachte Funktion der Authentifikation des Nutzers auch zuverlässig erfüllen können, vertraulich zu behandeln und daher - ungeachtet des erfolgten Fehlversandes - nicht per offener E-Mail über das Internet zu übertragen. Das Unternehmen hat sein Fehlverhalten insoweit auch eingeräumt.

4.3.2.9 Scheinkäufer auf Versteigerungsplattformen

Ein Mitglied einer Versteigerungsplattform war wegen unlauteren Wettbewerbs abgemahnt worden. Es vermutete, die abmahnende Kanzlei habe seine Mitgliedsdaten von einem Mitbewerber erhalten, der als Mitglied der gleichen Versteigerungsplattform die Abläufe der elektronischen Kaufabwicklungsroutine des Versteigerungsportals in der Weise genutzt haben soll, einen Kauf nur zum Schein zu tätigen, um so von dem System die ansonsten nicht allgemein zugänglichen Kontaktdaten des Verkäufers zu erlangen.

Nach § 43 Abs. 2 Nr. 4 BDSG handelt ordnungswidrig bzw. macht sich im Fall einer vorsätzlichen Eigen- oder Drittbereicherungs- sowie bei Schädigungsabsicht nach § 44 Abs. 1 BDSG strafbar, wer die Übermittlung personenbezogener Daten, die nicht allgemein zugänglich sind, erschleicht. Erfasst sind nach dem Gesetz alle Fälle, in denen durch Täuschung - welcher Art auch immer - die Übermittlung geschützter personenbezogener Daten veranlasst wird (vgl. Gola/Schomerus, BDSG, 10. Auflage 2010, § 43 Rn. 23). Die für eine Ordnungswidrigkeit wie für eine Straftat über die Tatbestandserfüllung hinaus erforderliche Rechtswidrigkeit des Verhaltens ist allerdings ausgeschlossen, wenn ein allgemeiner Rechtfertigungsgrund vorliegt (vgl. Gola/Schomerus a. a. O. Rn. 26). Dieser könnte hier darin zu sehen sein, dass der mutmaßliche Scheinkäufer möglicherweise wettbewerbsrechtlich befugt war, Auskunft über die Identität eines Mitbewerbers zu erlangen. Diese außerhalb des Datenschutzrechts liegende, nach sonstigem Zivilrecht zu beurteilende Vorfrage war jedoch nicht mit der im Ordnungswidrigkeitenverfahren notwendigen Gewissheit zu beantworten.

Die Erlaubtheit der Übermittlung der aus der Kaufabwicklungsroutine gewonnenen Daten an den Anwalt zur Einleitung wettbewerbsrechtlicher Maßnahmen folgt jedenfalls aus der Befugnis, sich der Dienste eines Rechtsanwalts bedienen zu dürfen. Aus der Natur des Anwaltsvertrages folgt ferner die Befugnis des Anwalts, zur Erbringung seiner Dienstleistung auch Daten des Anspruchsgegners erheben und verarbeiten zu dürfen, so dass in § 28 Abs. 1 Satz 1 Nr. 1 BDSG eine hierfür ausreichende Rechtsgrundlage zu sehen ist (vgl. auch Simitis, BDSG, 6. Auflage 2006, § 28 Rn. 87).

4.3.2.10 Schwarze Listen

Regelmäßig wiederkehrend für die Aufsichtsbehörden ist auch die Thematik der Veröffentlichung schwarzer Listen (vgl. 1. TB - Pkt. 4.3.9 sowie 4. TB - Pkt. 4.2.2.4).

Wieder einmal hatte ein Unternehmer eine Liste von Personen, mit denen er schlechte Zahlungserfahrungen gemacht zu haben erklärte, mit dem Ziel, Interessierte vor diesen Personen zu warnen, ins Internet gestellt. Die Liste enthielt zu jedem „Schuldner" Angaben zum Kaufdatum, zum geschuldeten Betrag, Name, Anschrift sowie E-Mail-Adresse.

Der Unternehmer machte in diesem Fall allerdings geltend, dass eine Veröffentlichung im eigentlichen Sinne gar nicht vorliege und auch nicht beabsichtigt sei, da er diese Internetseite weder auf anderen Internetseiten verlinkt noch dort erwähnt und auch den Zugriff durch Suchmaschinen durch technische Vorkehrungen unterbunden habe. Zugang zu dieser Internetseite habe nur derjenige, der den entsprechenden Direktlink kenne; dieser wiederum werde per E-Mail nur an Betroffene („Schuldner") bekanntgegeben, d. h. nur an die, die selbst auch auf dieser Liste aufgeführt seien.

Auch wenn die Schuldnerliste damit in tatsächlicher Hinsicht nicht unbeschränkt veröffentlicht worden war, so sind doch die darin enthaltenen Daten auch Dritten bekanntgegeben worden, denn zumindest allen in der Liste aufgeführten Personen sind auf diese Weise auch die Daten der anderen „Schuldner" zur Kenntnis gelangt. Darüber hinaus hatte der Petent der Aufsichtsbehörde auch mitgeteilt, dass diese Liste auch noch nicht auf der Liste stehende Personen erhalten hatten, denen auf diese Weite zunächst nur damit gedroht worden war, sie - bei weiterhin ausbleibender Zahlung - gleichfalls in diese mit genauer URL bezeichnete Liste aufzunehmen. Schließlich ist noch zu berücksichtigen gewesen, dass der Link auf die Schuldnerliste den jeweiligen Empfängern per unverschlüsselter E-Mail über das Internet zur Kenntnis gegeben und auch der Seitenabruf selbst nur unverschlüsselt ermöglicht worden war. Somit haben auch Dritte, denen der Link infolge der ungesicherten E-Mail-Übertragung oder aber der bloße Seitenabruf möglicherweise zur Kenntnis gelangt ist, diese Daten abrufen gekonnt.

§ 28 Abs. 1 Satz 1 Nr. 2 BDSG bestimmt, dass das Übermitteln personenbezogener Daten für die Erfüllung eigener Geschäftszwecke zulässig ist, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Übermittlung überwiegt.

Eine Übermittlung liegt nach § 3 Abs. 4 Satz 2 Nr. 3 BDSG u. a. dann vor, wenn personenbezogene Daten einem Dritten in der Weise bekanntgegeben werden, dass dieser

Dritte zum Abruf bereitgehaltene Daten abruft. Für die Anwendbarkeit der o. g. Vorschrift des § 28 Abs. 1 Satz 1 Nr. 2 BDSG kommt es also nicht darauf an, dass die Daten tatsächlich veröffentlicht, also jedermann (breite Öffentlichkeit) zugänglich gemacht (Übermittlung an einen unbestimmten Empfängerkreis) werden, stattdessen reicht es aus, dass sie nur einem umgrenzten Personenkreis (Adressatenkreis der diesbezüglichen E-Mails) bekanntgegeben worden sind.

Das berechtigte Interesse des Unternehmers hat darin bestanden, dass dessen Kunden den für den Verkauf und Versand seiner Waren vereinbarten Kaufpreis entrichten. Es bestanden allerdings erhebliche Zweifel, dass hierfür auch unter den festgestellten Umständen (vergleichsweise kleine Zahlbeträge) eine Bekanntgabe der Schuldnerdaten an Dritte, und zwar einen Personenkreis, der nach Auffassung des Unternehmers nur aus ‚faulen' Schuldnern bestand, tatsächlich erforderlich, d. h. geeignet - dies wird wohl angesichts des teilweise eingetretenen Erfolges noch zu bejahen sein - gewesen ist und auch keine milderen Mittel, mit denen dieses Interesse gleichfalls verwirklicht werden kann, zur Verfügung gestanden haben. Dies konnte an dieser Stelle aber dahinstehen, da das schutzwürdige Interesse der Betroffenen am Ausschluss der mit der Einstellung in das Internet verbundenen Übermittlung höher zu bewerten war. Dies galt einerseits wegen der mit der Bekanntgabe an Dritte verbundenen Prangerwirkung und vor allem, weil es sich zudem um nicht von dritter zuständiger Stelle objektiv festgestellte Daten mit für den Betroffenen nachteiligen Angaben gehandelt hat.

4.3.2.11 Personenbezogene Daten in Suchmaschinenergebnissen

Über eine Suchmaschine hatte ein gegenüber einer obersten Landesbehörde in Erscheinung getretener Beschwerdeführer sein diesbezügliches Schreiben, besser gesagt nur ein so genanntes Snippet (Textauszug) davon, entdeckt, welches in diesem Fall seine vollständigen Kontaktdaten einschließlich Telefonnummer und E-Mail-Adresse sowie den Adressaten seines Schreibens enthielt. Er vermutete dabei eine Veröffentlichung durch den Empfänger des Schreibens und wandte sich dabei insbesondere gegen die umfassende Veröffentlichung seiner Kontaktdaten.

Die Aufsichtsbehörde konnte den Empfänger des Schreibens als Quelle der Veröffentlichung ausschließen. Aus dem Suchmaschinentreffer ging stattdessen hervor, dass die im Snippet enthaltenen Daten zunächst wiederum aus einer anderen (Personen-) Suchmaschine stammten. Diese Suchmaschine ist darauf programmiert, öffentlich im Internet verfügbare Informationen zu beliebigen Personen zu finden. Bei einem dieser Suchläufe hatte sie dabei offensichtlich auch eine Kopie des Schreibens des Petenten gefunden. Die dazu dort angegebene URL führte zu einer als Verein organisierten Bürgerinitiative. Obwohl das eigentliche Schreiben des Petenten dort gar nicht mehr gelistet

gewesen ist, war das betreffende Suchergebnis offenbar noch im Cache der Suchmaschine gespeichert und wurde folglich auch noch angezeigt, auch wenn die originäre Datei selbst gar nicht mehr im Netz verfügbar war.

Inwieweit die ursächliche Veröffentlichung mit Zustimmung des Petenten vorgenommen worden war, konnte durch die Aufsichtsbehörde mangels entsprechender Informationen nicht beurteilt werden, insbesondere war auch nicht bekannt, in welcher Beziehung er zu dieser Vereinigung gestanden hat. Allerdings hat sich der Petent auf diese Mitteilung auch nicht mehr gemeldet, so dass angenommen werden kann, dass die seinerzeitige Veröffentlichung seines Schreibens jedenfalls nicht ohne sein Wissen erfolgt war.

4.3.2.12 Fotos von Single-Tanzveranstaltungen

Ein Tanzcafe stellte nach Single-Tanzveranstaltungen regelmäßig Fotos der Veranstaltung zu Werbezwecken auf seine Internet-Repräsentanz. Unter den Bildern befanden sich auch solche, auf denen einzelne Personen oder Paare porträtartig abgebildet waren.

Datenschutzrechtlich bedeutet die Veröffentlichung eine Übermittlung personenbezogener Daten, welche im Allgemeinen der Einwilligung bedarf (§§ 4, 4a BDSG). Zudem dürfen gemäß § 22 Satz 1 KUG Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Soweit es sich nicht um Personen der Zeitgeschichte handelt, bedarf es nach § 23 Abs. 1 Nr. 3 KUG bei Veranstaltungsaufnahmen allein dann keiner Einwilligung, wenn bei den Aufnahmen die Veranstaltungen als solche und nicht die teilnehmenden Personen im Vordergrund stehen, diese also lediglich „Beiwerk“ des Ereignisses sind. Je mehr Bedeutung die abgebildeten Personen in einer Aufnahme erhalten, desto eher lebt die Einwilligungspflicht aus § 22 Satz 1 KUG wieder auf.

Die wegen des porträtartigen Charakters der Aufnahmen aus dem Tanzcafe hier zu fordernde Einwilligung wäre allenfalls dann entbehrlich, wenn die Betroffenen durch ihr Verhalten, zum Beispiel ein sichtbares Posieren, hinreichend deutlich gemacht hätten, dass sie fotografiert werden wollen (vgl. LG Berlin, Urteil v. 6. März 2007, Az. 27 O 1063/06 - juris) und dieses Einverständnis auch eine öffentliche Verbreitung einschließt. Angesichts des Umstandes, dass es sich bei einer Singleparty jedoch um ein Mittel der Partnersuche handelt und somit der Veranstaltung ein besonders persönlicher Charakter innewohnt, dürfen die Besucher allerdings auf ein gesteigertes Maß an Diskretion vertrauen. Aus dem Einverständnis mit der fotografischen Aufnahme, die auch allein zu privaten Erinnerungszwecken erteilt worden sein kann, darf jedenfalls nicht zwingend auf ein Einverständnis mit einer allgemeinen Veröffentlichung im Internet geschlossen

werden. Der Besuch einer Tanzveranstaltung beinhaltet als solcher noch nicht ein Einverständnis mit der Veröffentlichung des eigenen Bildnisses, selbst wenn in derartigen Lokalen üblicherweise entsprechende Fotografien gefertigt und zu Werbezwecken im Internet veröffentlicht werden (AG Ingolstadt, Urteil v. 3. Februar 2009, Az. 10 C 2700/ 08 - juris).

Da der Betreiber des Tanzcafes am Einlass mit einem sichtbaren Hinweisschild und während der Veranstaltung durch entsprechende Durchsagen kenntlich machte, dass Anwesende zur Veröffentlichung im Internet fotografiert werden können, wenn diese dem nicht widersprechen und sichergestellt war, dass bei einem Widerspruch eine Veröffentlichung ausgeschlossen ist, bestanden im vorliegenden Fall keine datenschutzrechtlichen Bedenken. Allerdings ist der Betreiber aus Gründen der Transparenz gebeten worden, auf dem Hinweisschild die Internetseite, auf der eine Veröffentlichung beabsichtigt ist, genau zu benennen, damit den Veranstaltungsbesuchern eine nachträgliche Kontrolle des Umgangs mit den Veranstaltungsaufnahmen erleichtert wird. Zudem sollte dort sowie im Internet der Hinweis ergänzt werden, dass auch im Nachhinein der Veröffentlichung widersprochen und die Entfernung der Bilder von der Homepage erwirkt werden kann.

4.3.2.13 Daten Verstorbener in einem Familienstammbaum

Ein für die Veröffentlichung eines Familienstammbaums im Internet Verantwortlicher fragte an, unter welchen Voraussetzungen er personenbezogene Daten verstorbener Familienmitglieder veröffentlichen dürfe.

In Familienstammbäumen oft gebräuchliche personenbezogene Daten sind Vor-, Nach- und Geburtsnamen, Geburts- und Sterbedaten nebst Ortsangaben, Familienstand, verwandtschaftliche Beziehungen, weitere biografische Angaben sowie Fotografien und Urkunden.

Soweit eine Privatperson als nicht-öffentliche Stelle personenbezogene Daten anderer natürlicher Personen dadurch automatisiert verarbeitet, dass sie diese Daten im Internet der Allgemeinheit zur Verfügung stellt, ist dies keine ausschließlich private und damit privilegierte Tätigkeit mehr, sondern fällt in den Anwendungsbereich des Bundesdatenschutzgesetzes (§ 1 Abs. 2 Nr. 2 BDSG; vgl. die sog. Lindqvist-Entscheidung des EuGH). Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist daher nur dann zulässig, wenn der Betroffene gemäß den Voraussetzungen des § 4a BDSG in die Veröffentlichung seiner personenbezogenen Daten eingewilligt hat (§ 4 Abs. 1 BDSG). Ohne Einwilligung des Betroffenen ist in grafischen Familienstammbäumen hinsichtlich dieser Personen jedoch eine anonymisierte Bezeichnung mit „N.N.“ oder

z. B. „Enkel Nr. 3 von Nr. 1234“ zulässig, also die Beschränkung auf die Angabe des Vorhandenseins eines Abkömmlings sowie dessen Geburtsdatum und Geburtsort.

Das vom Bundesdatenschutzgesetz zu schützende Recht des Einzelnen auf informationelle Selbstbestimmung schützt allerdings nur lebende Grundrechtsträger. Bereits verstorbene Personen sind somit keine Betroffenen i. S. v. § 3 Abs. 1 BDSG (mehr). Allerdings wirkt der sog. postmortale Schutz des Persönlichkeitsrechts als Ausprägung von Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG bezogen auf die Auslegung etwaiger zivilrechtlicher (Unterlassungs-)Ansprüche über den Tod hinaus fort. Dafür gibt es keine in jeder Hinsicht gesicherte Grenze. Allerdings dürften Stammbaumverantwortliche auf der sicheren Seite sein, wenn sie von einem auf zehn Jahre begrenzten Fortdauern des Persönlichkeitsrechtsschutzes nach dem Tode ausgehen (vgl. auch § 22 Satz 3 KUG, § 10 Abs. 1 Satz 3 SächsArchivG). Dasselbe gilt für das Einstellen von Fotografien verstorbener Personen ins Internet.

4.3.3 Arbeitnehmerdatenschutz

4.3.3.1 Rückgabe von Bewerbungsunterlagen

Mehrere Betroffene haben sich darüber beschwert, dass sie ihre (anlässlich einer Stellenanzeige) eingereichten Bewerbungsunterlagen nicht zurückerhalten hätten. Sie befürchteten in diesem Zusammenhang eine nicht bestimmungsgemäße Verwendung ihrer in den Unterlagen enthaltenen personenbezogenen Daten.

Bewerbungsunterlagen unterliegen einer konkreten Zweckbestimmung, d. h. sie sind nur im Rahmen der Entscheidung über die Besetzung der ausgeschriebenen Stelle zu verwenden. Im Fall der Ablehnung dürfen Bewerbungsunterlagen daher nur noch für einen begrenzten Zeitraum (s. u.) vorgehalten, dabei aber keinesfalls für andere Zwecke genutzt werden. Unzulässig ist es auch, die erhaltenen Bewerbungsunterlagen ohne ausdrückliches Einverständnis des Betroffenen bzw. ohne dass dies von vornherein so ausgeschrieben gewesen ist, noch für andere Stellenbesetzungen zu verwenden, für die Zukunft vorzuhalten, zu archivieren oder gar an Dritte weiterzureichen.

Der Betroffene muss die weitere Aufbewahrung seiner Bewerbungsunterlagen also keinesfalls dulden, sondern kann deren Rückgabe fordern. Allerdings ist dies kein datenschutzrechtlicher, sondern ein zivilrechtlicher Anspruch, der sich auf § 985 BGB (Herausgabeanspruch des Eigentümers) stützen lässt.

Klassisch datenschutzrechtlicher Natur ist (hilfsweise) der Löschungsanspruch, wenn die Rückgabe nicht erwünscht ist. Gemäß § 35 Abs. 2 Nr. 3 BDSG sind personenbezogene Daten zu löschen, sobald ihre Kenntnis für die Erfüllung des Zweckes der Speiche-

rung nicht mehr erforderlich ist. Dies ist bei einer erfolglosen Bewerbung der Fall, sofern nicht eine Verständigung über die weitere Verwendung der Unterlagen erfolgt ist.

Für die Fristen zur Herausgabe oder Löschung ist zu beachten, dass gemäß § 15 Abs. 4 AGG abgelehnte Bewerber innerhalb von zwei Monaten Ansprüche auf Schadensersatz wegen eines Verstoßes gegen ein Benachteiligungsverbot geltend machen können. Hierfür genügt der Nachweis von Indizien, wobei der Arbeitgeber gemäß § 22 AGG verpflichtet sein kann, das Gegenteil zu beweisen. Dies stellt zwar keine Aufbewahrungsfrist i. S. d. § 35 Abs. 3 Nr. 1 BDSG dar, gleichwohl ist der Arbeitgeber danach befugt, während dieses Zeitraums Bewerberdaten weiter zu speichern und erst nach dem Verstreichen der Beschwerdefrist zu löschen. Eine Verpflichtung zur sofortigen Löschung würde die Beweisführung für den Arbeitgeber erheblich und unzumutbar erschweren.

4.3.3.2 Nutzung von Bewerberdaten für Werbezwecke

In einer Eingabe war geschildert worden, dass die bei einer erfolglosen Bewerbung auf eine offene Stelle angegebene Wohnanschrift des Bewerbers im späteren Verlauf zur Versendung von Eigenwerbung genutzt worden ist. Als Grund der - mit dem Bewerber abgestimmten - Speicherung über den Zeitpunkt der ablehnenden Entscheidung hinaus war angegeben worden, auf die Bewerbung im Falle späterer Vakanzen wieder zurückkommen zu wollen (vgl. auch Pkt. 4.3.3.1).

Auf die erteilte Einwilligung zur weiteren Speicherung der Bewerberdaten für den Fall der Berücksichtigung in einem späteren Stellenbesetzungsverfahren konnte die Nutzung für Werbezwecke jedenfalls nicht gestützt werden. Auch nach § 32 Abs. 1 Satz 1 BDSG dürfen personenbezogene Daten eines Beschäftigten bzw. eines Bewerbers (vgl. § 3 Abs. 11 Nr. 7 BDSG) für Zwecke des Beschäftigungsverhältnisses nur genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich ist. Die - von der verantwortlichen Stelle als Versehen in einem Einzelfall dargestellte - Datennutzung für Werbezwecke war also rechtswidrig gewesen.

4.3.3.3 Krankenrückkehrgespräche

Nach entsprechenden Hinweisen ist im Rahmen einer örtlichen Kontrolle durch die Aufsichtsbehörde festgestellt worden, dass in einem Unternehmen im Rahmen so genannter Krankenrückkehrgespräche in zahlreichen Fällen auch Gesundheitsdaten (hier: die konkrete Art der die Arbeitsunfähigkeit verursachenden Erkrankung) von Mitarbeitern erhoben, verarbeitet und genutzt worden sind.

Die Überprüfung hat dabei ergeben, dass unter bestimmten Voraussetzungen (individuelle Krankenquote von mindestens 5 % bezogen auf die letzten 12 Monate) der Inhalt

dieser Gespräche in so genannten Gesprächsnotizen dokumentiert und in den (strukturiert geführten) Personalakten abgelegt worden war. In zahlreichen Fällen war dabei auch die Art der Erkrankung angegeben, wobei in nur sehr wenigen Fällen tatsächlich ein Zusammenhang mit der Arbeitstätigkeit bestanden hatte. Durch die Aufsichtsbehörde festgestellt worden ist dabei u. a., dass beispielsweise folgende Gesundheitsdaten gespeichert worden sind: Zehenprellung, Sprunggelenksverletzung, Allergie, Nierensteinentfernung, Blinddarmoperation, Leistenoperation, schwere Grippe, Erkältung oder auch eingeklemmter Nerv!

Die Zulässigkeit der Erhebung, Verarbeitung und Nutzung von Gesundheitsdaten bestimmt sich - soweit kein betriebliches Eingliederungsmanagement entsprechend § 84 Abs. 2 SGB IX durchgeführt wird (vgl. § 1 Abs. 3 BDSG) - nach § 28 Abs. 6 BDSG (das ist im Hinblick auf die Europäische Datenschutzrichtlinie nicht unproblematisch, aber nach dem Gesetzeswortlaut unzweifelhaft, vgl. Franzen, RDV 2003, 1, 3 f.).

Nummer 1 dieser Vorschrift kommt, auch bei wohl von Verfassungs wegen gebotener weiter Auslegung des Tatbestandsmerkmals „lebenswichtig“, niemals als Erhebungs-Erlaubnis für Krankenrückkehrgespräche in Frage, weil in solchen Gesprächen der Betroffene ja zur Erklärung einer wirksamen Einwilligung in der Lage wäre.

Nummer 3 der Vorschrift scheidet ebenfalls in aller Regel als Erlaubnisgrundlage aus. Denn es ist nicht ersichtlich, dass der Arbeitgeber Angaben des Arbeitnehmers (anders der Fall des § 69 Abs. 4 SGB X betreffend die Entgeltfortzahlung im Falle der Fortsetzungserkrankung) über die gesundheitlichen Verhältnisse des Arbeitnehmers benötigte, um eigene Ansprüche geltend zu machen, auszuüben oder zu verteidigen. Betroffenennützige (arbeitnehmernützige) Rechtshandlungen des Verarbeiters (Arbeitgebers) sind mit der Vorschrift (abweichend von Art. 8 Abs. 2 lit. b der Europäischen Datenschutzrichtlinie, 95/46/EG, ihrem klaren Wortlaut nach, vgl. Franzen RDV 2003, 1, 3 f.) nicht gemeint, schon gar nicht die (Realakte zur) Erfüllung der Fürsorgepflicht des Arbeitgebers. (Zur Gegenmeinung scheint Gola RDV 2000, 125, 127 lSp. zu neigen, ohne jedoch klar einer richtlinienkonformen erweiternden Auslegung das Wort zu reden, die, gegen den Wortlaut des Gesetzes, auch Ansprüche gegen den Arbeitgeber und gegen jede andere verarbeitende Stelle einbezöge.) Es geht in der Vorschrift um Rechte, nicht um Pflichten des Verarbeiters.

Somit bleibt nur die Einwilligung als mögliche Rechtfertigung der Erhebung von Gesundheitsdaten durch den Arbeitgeber im Rahmen von Krankenrückkehrgesprächen (mitsamt der anschließenden Verwendung der Daten). Gerade aus der engen Fassung von Nr. 1 und Nr. 3 des § 28 Abs. 6 BDSG kann man schließen, dass der Einwilligung des Betroffenen durchaus Raum gegeben wird. Dies muss auch im Arbeitsverhältnis

gelten, soweit die Erhebung der Daten durch den Arbeitgeber (beim Arbeitnehmer im Krankenrückkehrgespräch) mittels der Nutzung dieser Daten durch den Arbeitgeber auch konkrete Vorteile für den Arbeitnehmer hat oder zumindest zu haben verspricht, also auch in seinem Interesse ist.

Das ist dann der Fall,

- wenn es gilt, von der Arbeitstätigkeit ausgehende Gefahren zu beseitigen, die zur Erkrankung von Arbeitnehmern geführt haben,
- wenn es gilt, festzustellen, inwieweit ein Arbeitnehmer noch den Anforderungen seines Arbeitsplatzes gewachsen ist, d. h. die von ihm nach dem Arbeitsverhältnis geschuldete Arbeitsleistung noch zumutbar zu erbringen vermag,
- oder wenn ihm eine gesundheitliche Beeinträchtigungen gemäße Arbeit zuzuweisen ist
- oder ihm gesundheitliche Wiedereingliederungsmaßnahmen, etwa arbeitgeberseitig angebotene Krankengymnastik oder dergleichen angeboten werden könnten.

Über diese Fallgruppen hinaus ist jedoch kein Raum für eine solche Verarbeitung von Gesundheitsdaten des Arbeitnehmers durch den Arbeitgeber im Zusammenhang mit Krankenrückkehrgesprächen ersichtlich, da wegen des starken Abhängigkeitsverhältnisses zwischen Arbeitnehmer und Arbeitgeber die notwendige Voraussetzung der Freiwilligkeit mangels erkennbarer gesonderter Gegenleistungen bzw. Grundlage (Einverständnis) im Arbeitsvertrag nicht erfüllt ist.

Daher hätten die Arbeitnehmer zu Beginn der Krankenrückkehrgespräche datenschutzrechtlich in dieser Hinsicht belehrt werden müssen: Der Vorgesetzte hätte ihnen sagen müssen, dass sie dann, wenn einer der oben genannten vier Sachverhalte vorliegt und sie damit einverstanden sind, in ihrem eigenen Interesse diese Angaben machen könnten. Zu der für die Wirksamkeit der Einwilligung erforderlichen Aufklärung hätte es gehört, dass erläutert worden wäre, was mit den betreffenden Daten bzw. den aus diesen zu gewinnenden Erkenntnissen gegebenenfalls geschehen würde.

Demnach bestehen gegen eine Verarbeitung von Gesundheitsdaten jedenfalls dann keine Einwände, wenn

- es sich um die Folgen von Arbeitsunfällen handelt,
- sich aus der überstandenen Krankheit noch Einschränkungen bei der Einsatzfähigkeit des Arbeitnehmers ergeben oder
- sonst ein unmittelbarer Zusammenhang mit der Arbeitstätigkeit besteht

- **und** eine formgerechte und auch sonst rechtswirksame Einwilligung nach entsprechender Aufklärung erteilt worden ist.

In jedem Fall unzulässig ist die Verarbeitung von Gesundheitsdaten dann, wenn kein Zusammenhang mit der Arbeitstätigkeit besteht. Dies gilt insbesondere auch dann, wenn die betreffenden Arbeitnehmer die Art der überstandenen Krankheit unaufgefordert mitgeteilt haben.

In den Fällen, in denen ein Zusammenhang mit der Arbeitstätigkeit nur vage vermutet wird und außerdem konkrete Handlungsmöglichkeiten des Arbeitgebers nicht oder nur sehr eingeschränkt bestehen, ist die Verarbeitung von Gesundheitsdaten gleichfalls unzulässig. Dies betrifft solche Fälle wie eine schwere Bronchitis, bei der der betroffene Arbeitnehmer eine Ansteckung bei Kollegen vermutet oder auch die Aussage, dass nur ein Arzt einen eventuellen Zusammenhang zwischen einer durchgeführten Operation und der Arbeitstätigkeit ergründen könne.

Anders sind die Fälle zu bewerten, in denen sich entsprechende Reaktionsmöglichkeiten des Arbeitgebers ergeben, etwa die Überprüfung der Heizungsanlage bzw. die Ausgabe wärmerer Arbeitsschutzkleidung bei Erkältungen, die Ausgabe anderer Arbeitsschutzschuhe bei Fußbeschwerden oder die Umsetzung an einen anderen Arbeitsplatz bei Erschöpfungserscheinungen.

Abschließend sei zur Vermeidung von Missverständnissen noch klargestellt, dass die Aufsichtsbehörde weder die Berechtigung eines Arbeitgebers zur Durchführung von Krankenrückkehrgesprächen noch die zur Anfertigung diesbezüglicher Gesprächsnotizen in Abrede stellt, sondern lediglich dessen Befugnis zur Speicherung von Angaben zur Art der Erkrankung von den oben dargestellten Voraussetzungen abhängig macht.

Werden im Rahmen der Gespräche Gesundheits- oder andere personenbezogene Daten lediglich erfragt, anschließend jedoch nicht gespeichert, ist das Bundesdatenschutzgesetz nicht anwendbar; die Frage der Zulässigkeit einer diesbezüglichen Abfrage dann also jedenfalls keine datenschutzrechtlich zu klärende Problematik mehr. Die Anwendbarkeit des Bundesdatenschutzgesetzes ist nur dann gegeben, wenn die Erhebung mit dem Ziel der weiteren Verarbeitung (Speicherung) und Nutzung erfolgt. Andererseits ist die datenschutzrechtliche Zulässigkeit der Durchführung der Gespräche aber eben auch nicht von der Zulässigkeit einer sich anschließenden Speicherung zu trennen.

4.3.3.4 Aushang von Krankenlisten

Gleich in zwei Fällen ist die Aufsichtsbehörde auf firmeninterne Aushänge von Krankenlisten hingewiesen worden.

Im ersten Fall waren in einem Schaukasten zwei Tabellen ausgehängt worden, in denen personenbezogen der aktuelle Stand der Krankschreibungen analysiert worden war. Diese täglich aktualisierten Tabellen hatten in Form einer Rangliste jeweils 50 Mitarbeiter mit den in 2009 bis dahin meisten Krankschreibungen und den meisten Krankentagen aufgelistet und darüber hinaus auch die diesbezüglichen Endwerte dieser Mitarbeiter für das Jahr 2008 enthalten. Im zweiten Fall war am Schwarzen Brett im Pausenraum eines Unternehmens etwa zwei Wochen vor Weihnachten ein Balkendiagramm mit der Überschrift „Ausfalltage 2010 - Jahresüberblick“ ausgehängt worden, aus welchem für jeden Mitarbeiter die Zahl seiner Krankentage im Jahr 2010 zu entnehmen war.

Zweck der Aushänge soll es jeweils gewesen sein, unter den Mitarbeitern Transparenz hinsichtlich der individuellen Ausfalltage erzeugen und zugleich Anreize für eine Senkung des Krankenstandes geben zu wollen.

Die beschriebenen Aushänge haben in beiden Fällen gegen die §§ 4, 28 BDSG verstoßen und sind damit unzulässig gewesen.

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

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind gemäß § 4 Abs. 1 BDSG nur zulässig, soweit das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Weder hatten sich die Unternehmen auf eine Rechtsvorschrift außerhalb des Bundesdatenschutzgesetzes, die eine innerbetriebliche Bekanntgabe (Nutzung und auch Übermittlung) dieser Angaben erlauben würde, berufen, noch war eine solche erkennbar. Auch war nicht ersichtlich, dass eine vorherige Einwilligung der Mitarbeiter eingeholt worden wäre, die überdies mangels Freiwilligkeit ohnehin unwirksam gewesen wäre.

Daher bedurfte es einer Verarbeitungserlaubnis aus § 28 Abs. 6 bis 8 (vgl. § 28 Abs. 6 Satz 1) BDSG, denn die in den Listen enthaltenen Angaben zu Krankschreibungen bzw. zu Kranktagen fallen als Angaben über die Gesundheit unter die besonderen Arten personenbezogener Daten im Sinne von § 3 Abs. 9 BDSG (vgl. hierzu insbesondere Simitis in: Simitis, BDSG, 6. Aufl., Rn. 260 zu § 3, wonach auch die Feststellung, dass eine bestimmte Person inzwischen genesen oder überhaupt völlig gesund sei, zu den Angaben über die Gesundheit zählt - mithin muss dies also erst recht für die gegenteilige Aus-

sage, dass bzw. wie oft oder wie lange eine Person in einem bestimmten Zeitraum krank war, gelten), denn daraus lassen sich Rückschlüsse über die (mangelhafte) gesundheitliche Verfassung der in den Aushängen aufgeführten Mitarbeiter ziehen.

Nach § 28 Abs. 6 Nr. 3 BDSG wäre die Nutzung von Gesundheitsdaten zulässig, wenn dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich wäre und kein Grund zu der Annahme bestünde, dass das schutzwürdige Interesse der Betroffenen am Ausschluss einer solchen Nutzung überwiegt. Diese Voraussetzungen waren vorliegend nicht erfüllt. Der Aushang sollte lediglich der Mitarbeiterinformation dienen (Gewährleistung der Transparenz) - rechtliche Ansprüche waren damit also nicht verfolgt worden. Es waren unabhängig davon aber auch keine rechtlichen Ansprüche vorstellbar, die nur mit der Bekanntgabe dieser Gesundheitsdaten geltend gemacht, ausgeübt oder verteidigt hätten werden können. Die Aushänge waren also schon aus diesem Grunde unzulässig. Auf das Überwiegen von - zweifelsfrei bestehenden - schutzwürdigen Betroffeneninteressen kam es daher gar nicht mehr an.

Alle anderen dafür in Frage kommenden Verarbeitungserlaubnisse schieden ohnehin aus.

4.3.3.5 Aushang von Reklamationslisten

In dem unter Pkt. 4.3.3.4 erstgenannten Fall hatte das Unternehmen nicht nur den aktuellen Stand der Krankschreibungen personenbezogen analysiert, sondern in gleicher Weise auch die jeweils 50 Mitarbeiter mit den in 2009 bis dahin meisten Reklamationsfällen sowie den höchsten Reklamationsbeträgen aufgelistet.

Bei den Übersichten zum Reklamationsstand einzelner Mitarbeiter handelte es sich nicht um besondere Arten personenbezogener Daten im Sinne von § 3 Abs. 9 BDSG. Die Zulässigkeit der internen Bekanntgabe dieser Daten bestimmte sich daher nach § 28 Abs. 1 BDSG. (Der Vorfall hatte sich noch vor Inkrafttreten der BDSG-Novelle am 1. September 2009 ereignet.)

Gemäß § 28 Abs. 1 Satz 1 BDSG wäre die Nutzung oder Übermittlung dieser Daten zulässig gewesen, wenn dies der Zweckbestimmung des Arbeitsverhältnisses, d. h. der Wahrnehmung der hieraus resultierenden Rechte und Pflichten, gedient hätte. Für die Durchführung des einzelnen Arbeitsvertrages im Sinne einer Geltendmachung von Rechten und Erfüllung von Pflichten war es aber ohne Nutzen, die gesamte Belegschaft über die aktuelle (oder auch Vorjahres-) Reklamationsanzahl einzelner Mitarbeiter zu unterrichten. Soweit notwendig hätten damit verbundene Fragen im individuellen Gespräch zwischen Mitarbeiter und Vorgesetzten geklärt werden müssen. (Auch nach dem seit Inkrafttreten des novellierten Bundesdatenschutzgesetzes am 1. September 2009

anstelle des § 28 Abs. 1 Satz 1 BDSG für die datenschutzrechtliche Bewertung heranzuziehenden § 32 Abs. 1 Satz 1 BDSG hätte sich nichts anderes ergeben, da dieser sogar vorschreibt, dass die Übermittlung oder Nutzung personenbezogener Daten eines Beschäftigten für die Durchführung des Beschäftigungsverhältnisses erforderlich sein muss.)

Im Weiteren ergab sich auch aus § 28 Abs. 1 Satz 1 Nr. 2 BDSG, d. h. der Abwägung zwischen den berechtigten Arbeitgeberinteressen und den entgegenstehenden schutzwürdigen Betroffeneninteressen, keine Zulässigkeit dieser personenbezogenen Aushänge. Dem Arbeitgeberinteresse, bei den Mitarbeitern Transparenz über aktuelle Unternehmenskennziffern zu erzeugen, hätte durch auf das Gesamtunternehmen oder auf Organisationseinheiten bezogene Übersichten in ausreichender Weise entsprochen werden können. Hierfür war es nicht notwendig, die Mitarbeiter mit den diesbezüglich schlechtesten Werten anzugeben (und damit an den internen Pranger zu stellen). Selbst wenn - was insoweit nicht geltend gemacht worden ist - mit diesen Listen das Ziel verfolgt worden wäre, den Mitarbeitern Leistungsvergleiche zu ermöglichen bzw. Leistungsanreize zu schaffen, so hätte dafür eine anonymisierte Darstellung ausgereicht. Der Motivierungs- und Ansporneffekt tritt in aller Regel auch bei anonymisierten Listen ein, denn jeder Mitarbeiter dürfte seine eigenen Arbeitsergebnisse kennen und sich daher selbst an der richtigen Stelle in diese Listen einordnen können, ohne dass dabei ein diskriminierender Effekt für die Leistungsschwächeren eintreten würde. In diesem Diskriminierungseffekt lag überdies auch der Grund für ein überwiegendes schutzwürdiges Interesse der Betroffenen, nicht in diesen Ranglisten zu erscheinen. Die unternehmensweite Bekanntgabe hoher persönlicher Reklamationszahlen und somit schlechter Arbeitsergebnisse kann erhebliche Auswirkungen auf das Ansehen der Betroffenen inner- und auch außerhalb des Unternehmens haben. (Überlegungen, ob auch nach aktueller Rechtslage, d. h. nach Einführung des § 32 BDSG, im vorliegenden Fall § 28 Abs. 1 Satz 1 Nr. 2 BDSG überhaupt noch anwendbar ist, sind an dieser Stelle entbehrlich, da dies jedenfalls zu keinem anderen Ergebnis führen würde.)

4.3.3.6 Taschen- und Fahrzeugkontrollen

Pressemeldungen war zu entnehmen gewesen, dass eine Supermarktkette bei ihren Mitarbeitern regelmäßig Taschen- und Fahrzeugkontrollen durchführen ließ, um auf diese Weise zu verhindern bzw. in den konkreten Fällen auch auszuschließen, dass Waren ohne Bezahlung mit nach Hause genommen werden.

Die diesbezüglich durchgeführte Kontrolle hat dabei zunächst ergeben, dass die Taschenkontrollen nach dem Zufallsprinzip vorgenommen und dabei noch keine Diebstähle festgestellt worden sind. Sie sind also (bis dahin) ohne eine Verarbeitung perso-

nenbezogener Daten erfolgt und waren demnach - jedenfalls durch die Datenschutzaufsichtsbehörde - nicht zu bewerten.

Was die Fahrzeugkontrollen betraf, so waren diese - unter Anfertigung entsprechender Einsatzprotokolle - durch eine beauftragte Detektei vorgenommen worden. Damit war in jedem Fall eine datenschutzrechtliche Relevanz gegeben, denn zumindest die Namen der betroffenen Mitarbeiter und natürlich auch das Kontrollergebnis war ja in den Einsatzprotokollen dokumentiert worden.

Von den Kontrollen betroffen gewesen seien ausschließlich Mitarbeiter in Märkten mit hohen Inventurdifferenzen. Den Mitarbeitern sei grundsätzlich bekannt gewesen (von jedem Mitarbeiter unterzeichnete Mitarbeiter-Einkaufsregelung), dass derartige Kontrollen durchgeführt werden; die Auswahl erfolge nach dem Zufallsprinzip; ein konkreter Tatverdacht habe in keinem Fall vorgelegen. Unterschlagungen seien auf diese Weise noch nicht festgestellt worden, insbesondere könne bei fehlendem Kassenbeleg aber auch nicht festgestellt werden, woher die ggf. vorhandene Ware stammte.

Die Bedeutung der Fahrzeugkontrollen dürfte damit in erster Linie im präventiven Bereich gelegen haben. Maßnahmen der Missbrauchskontrolle sind durch das Bundesdatenschutzgesetz auch nach seiner letzten Novellierung im September 2009 nicht ausgeschlossen:

§ 32 Abs. 1 Satz 1 BDSG regelt u. a., dass personenbezogene Daten zu Beschäftigungszwecken erhoben, verarbeitet oder genutzt werden dürfen, wenn dies nach Begründung eines Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Der Arbeitgeber darf also zur Wahrnehmung seiner im Rahmen des Beschäftigungsverhältnisses bestehenden Rechte auch Verhaltenskontrollen bei seinen Beschäftigten durchführen, soweit diese zur Verhinderung von Straftaten oder sonstigen Rechtsverstößen, die im Zusammenhang mit dem Beschäftigungsverhältnis stehen, erforderlich sind.

Hohe Inventurdifferenzen im Einzelhandel sind anerkanntermaßen zu einem erheblichen Anteil auf Personaldiebstähle zurückzuführen. Insofern sind hohe Warenverluste bzw. eine hohe Inventurgefährdung zumindest auch ein Anzeichen für ein vertragswidriges Verhalten einzelner Beschäftigter. Die Durchführung entsprechender (Taschen- und) Fahrzeugkontrollen ist in diesen Fällen eine geeignete und notwendige Maßnahme, um derartiges Fehlverhalten zu verhindern bzw. ggf. auch zu erkennen. Soweit solche Kontrollen auf entsprechende Anlässe beschränkt bleiben, nach vorheriger Information der Arbeitnehmer sowie nach dem Zufallsprinzip vorgenommen und die Kontrollergebnisse - so sie keinen Anlass für eine weitere Verfolgung geben - nach Auswertung um-

gehend wieder gelöscht werden, ist dagegen jedenfalls aus datenschutzrechtlicher Sicht nichts einzuwenden.

Im Rahmen der bereits erwähnten Einsatzprotokolle waren die Kontrollergebnisse personenbezogen in Einsatzprotokollen festgehalten und somit Mitarbeiterdaten erhoben und gespeichert worden. Dies galt insbesondere auch dann, wenn bei den betroffenen Arbeitnehmern keine Waren im Fahrzeug aufgefunden worden waren bzw. wenn diese - was bis dahin noch nicht vorgekommen sein soll - ihre Zustimmung zu der Fahrzeugkontrolle verweigert hätten. Die Detektei hatte dabei nur die entsprechenden Feststellungen zu treffen, eine Bewertung dieser Feststellungen war der Markt- bzw. Unternehmensleitung vorbehalten gewesen.

Die Einsatzprotokolle waren anschließend der Revisionsabteilung des Unternehmens übergeben worden und sollten dort zusammen mit der jeweiligen Rechnung als Leistungsnachweis für die Zeitdauer von zehn Jahren aufbewahrt werden. Für die Einhaltung der handels- bzw. steuerrechtlichen Aufbewahrungsfristen wäre es allerdings ausreichend gewesen, lediglich die jeweiligen Rechnungen über den genannten Zeitraum aufzubewahren. Die eigentlichen Einsatzprotokolle unterliegen nicht der diesbezüglichen zehnjährigen Aufbewahrungspflicht. Stattdessen sind für deren Aufbewahrungsdauer die Vorschriften des § 35 BDSG zu Grunde zulegen. Nach § 35 Abs. 2 Satz 2 Nr. 3 BDSG sind personenbezogene Daten zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Dies dürfte im konkreten Fall spätestens dann der Fall sein, wenn einerseits die Korrektheit der Abrechnung der beauftragten Detektei geprüft worden ist und andererseits die Einsatzprotokolle keine für die Betroffenen negativen Feststellung enthalten, welche eine weitere (getrennte) Aufbewahrung notwendig machen könnte.

4.3.3.7 Mitarbeiter und Kunde zugleich

Ein Bankkaufmann, der - wie das wohl üblich ist - zugleich auch Kunde seines Arbeitgebers war, schilderte der Aufsichtsbehörde, dass er durch persönliche Probleme in finanzielle Schwierigkeiten geraten sei. Er habe, um seinen finanziellen Verpflichtungen nachkommen zu können, zunehmend seinen Dispositionskredit in Anspruch nehmen, seine Kreditkarte nutzen sowie auch bei einer anderen Bank einen Ratenkredit aufnehmen müssen. Infolgedessen habe sein Arbeitgeber eine Sonderprüfung seiner bei ihm geführten Konten durchgeführt und die dabei gewonnenen Erkenntnisse dann einerseits für kreditrechtliche Schritte (Bankkartensperrung, Kreditkarten- und Dispositionskreditkündigung), andererseits aber auch für arbeitsrechtliche Schritte bis hin zur Kündigung genutzt. Er sei über eine solche Analyse seiner Kontobewegungen nicht

informiert worden und fühle sich in den Konsequenzen im Vergleich zu anderen Kunden deutlich benachteiligt.

Zur datenschutzrechtlichen Zulässigkeit der Überprüfung und Auswertung der Kontobewegungen hat die betreffende Bank mitgeteilt, dass sie nach den Mindestanforderungen der BaFin an das Risikomanagement (MaRisk) verpflichtet sei, ein Verfahren zur Früherkennung von Risiken zu etablieren. Damit sollen Kreditnehmer, bei deren Engagement sich erhöhte Risiken abzuzeichnen beginnen, rechtzeitig identifiziert werden. Hierzu seien auf der Basis quantitativer und qualitativer Risikomerkmale Indikatoren für eine frühzeitige Risikoidentifizierung zu entwickeln. Ein klassischer Frühwarnindikator sei dabei die Kontoführung; besonderes Augenmerk sei dabei auf Konten zu richten, bei denen beispielsweise eingeräumte Kreditlinien nahezu stets in voller Höhe ausgenutzt werden, aus der Kontoführung Liquiditätsprobleme erkennbar sind oder Soll-Umsätze die Haben-Buchungen übersteigen. Im Rahmen einer der diesbezüglich regelmäßig durchgeführten Stichprobenkontrollen von Kundenkonten mit Liquiditätsproblemen sei dabei auch das Konto des Petenten aufgefallen und einer näheren Überprüfung unterzogen worden.

Die mit dieser Überprüfung verbundene Datennutzung war zulässig.

Gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist die Nutzung personenbezogener (Kunden-) Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Durchführung eines rechtsgeschäftlichen Schuldverhältnisses (hier: Girokonten- bzw. Kreditkartenvertrag) mit dem Betroffenen erforderlich ist.

Diese Voraussetzungen waren erfüllt. Nach den bankenaufsichtsrechtlichen Vorgaben zur frühzeitigen Erkennung und Beseitigung von Risiken war die Bank zur Kontrolle der Kontenbewegungen verpflichtet. Dies entspricht mithin zwangsläufig auch der Zweckbestimmung des mit den Kunden abgeschlossenen Girokonten- bzw. Kreditkartenverträgen. Datenschutzrechtliche Einwände gegen eine solche Datennutzung sind nicht begründet. Das Bundesdatenschutzgesetz sieht für den betrachteten Fall auch keine vorherige Unterrichtung des Betroffenen vor; über die Zweckbestimmungen der Erhebung, Verarbeitung und Nutzung seiner Daten ist ein Kunde insoweit einmalig bei Vertragsabschluss zu unterrichten (§ 4 Abs. 3 Satz 1 Nr. 2 BDSG). Ob die erfolgte Risikoeinschätzung dann im Einzelnen zutreffend war und inwieweit die daraufhin getroffenen Maßnahmen geeignet und auch gerechtfertigt waren, die erkannten Risiken zu beseitigen bzw. zumindest zu mindern, hat die Aufsichtsbehörde nicht zu beurteilen.

Im konkreten Einzelfall war auch die Verwendung der dabei gewonnenen Erkenntnisse im Rahmen des mit dem Kunden zugleich bestehenden Arbeitsverhältnisses zulässig.

Gemäß § 28 Abs. 2 Nr. 1 BDSG ist eine außerhalb der Zweckbestimmung eines rechtsgeschäftlichen Schuldverhältnisses liegende Datennutzung nur unter den Voraussetzungen des § 28 Abs. 1 Satz 1 Nr. 2 oder Nr. 3 BDSG zulässig (wobei sich Nr. 3 auf allgemein zugängliche Daten bezieht und demnach vorliegend nicht einschlägig ist). Nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist die Nutzung personenbezogener (Kunden-) Daten 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 am Ausschluss der Nutzung überwiegt.

Eine Bank ist zur Risikovermeidung beim Umgang mit Kundengeldern darauf angewiesen, nur zuverlässige Mitarbeiter zu beschäftigen. Zuverlässig bedeutet in diesem Zusammenhang insbesondere auch, dass die betreffenden Mitarbeiter in geordneten finanziellen Verhältnissen leben müssen, um nicht aus einer persönlichen finanziellen Zwangssituation heraus in die Versuchung zu geraten, Bankgelder zu veruntreuen. Damit besteht natürlich ein berechtigtes Interesse, solche Mitarbeiter rechtzeitig zu identifizieren, bei denen diese Voraussetzung nicht erfüllt ist. Bei konkreten Verdachtsmomenten muss es dabei auch erlaubt sein, die Personalabteilung über bestehende Risiken zu unterrichten, damit auch von deren Seite Maßnahmen zur Risikominimierung bzw. -vermeidung (z. B. Umsetzung) getroffen werden können. Dies gilt insbesondere dann, wenn finanzielle Probleme nicht nur einmalig bzw. vorübergehend, sondern wiederholt bzw. über einen längeren Zeitraum bestehen. Überwiegende schutzwürdige Interessen, die eine Weitergabe der aus den internen Kontrollen gewonnenen Informationen an die Personalabteilung ausschließen, sind unter solchen Voraussetzungen nicht ersichtlich.

Die im Ergebnis von der Personalabteilung getroffenen arbeitsrechtlichen Konsequenzen hat die Aufsichtsbehörde wiederum nicht zu bewerten.

Die von der betreffenden Bank zunächst vertretene Meinung, dass ein Kreditinstitut, das nicht nur Kreditgeber eines Kunden, sondern zugleich Arbeitgeber des Betreffenden ist, selbstverständlich und generell alle erlangten Daten in ihrer „Doppelfunktion“ verwenden darf, war allerdings zurückzuweisen: Sobald sich eine Bank bei einer solchen Datennutzung nicht auf konkrete Verdachtsmomente stützen, d. h. keine nennenswerten Risiken erkennen kann, ist eine interne Weitergabe an die Personalabteilung unzulässig. Es sind weder berechtigte Interessen ersichtlich, die eine solche Unterrichtung der Personalabteilung erforderlich machen könnten, noch kann dem Betroffenen unter solchen Voraussetzungen unterstellt werden, dass er kein entgegenstehendes (überwiegendes) schutzwürdiges Interesse hätte. Ein Mitarbeiter muss es nicht hinnehmen, dass die Personalabteilung im Detail über seine finanziellen Verhältnisse und Transaktionen unter-

richtet ist, sofern er sich bankgeschäftlich unauffällig, insbesondere vertragsgemäß verhält und daher kein Risiko für seinen Kredit- und Arbeitgeber zu erkennen gibt.

4.3.3.8 GPS in Außendienstfahrzeugen

Der Einsatz von Ortungstechnik in Fahrzeugen von Außendienstmitarbeitern setzt nach § 4 Abs. 1 BDSG voraus, dass die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch eine Rechtsvorschrift erlaubt wird oder dass die Betroffenen eingewilligt haben.

Im Arbeitsverhältnis lässt sich die Verarbeitung von Beschäftigtendaten allerdings nur begrenzt auf Einwilligungen der Beschäftigten stützen, denn aufgrund des Abhängigkeitsverhältnisses zum Arbeitgeber liegt - jedenfalls bei privaten Arbeitgebern - die für eine Einwilligung vorauszusetzende Freiwilligkeit der Entscheidung (vgl. § 4a Abs. 1 BDSG) vielfach nicht vor.

Darüber hinaus kann die mittels GPS erfolgende Verarbeitung personenbezogener Beschäftigtendaten nach § 32 Abs. 1 Satz 1 BDSG zulässig sein, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. Im Einzelnen kommt es also auf den Zweck der Datenverarbeitung, die technischen Möglichkeiten des Systems und dessen tatsächlichen Gebrauch an.

Die Nutzung von Ortungssystemen in der Weise, dass damit das Arbeitsverhalten von Beschäftigten dauernd kontrolliert wird, ist wegen des damit verbundenen permanenten Kontrolldrucks datenschutzrechtlich grundsätzlich unzulässig. Lediglich in begründeten Einzelfällen kann sich eine Zulässigkeit ergeben, wenn der Arbeitgeber tatsächliche Anhaltspunkte für arbeitsrechtliche Verfehlungen hat. In jedem Fall unzulässig ist die Nutzung der Ortungstechnik außerhalb der Arbeitszeit, d. h. während das Fahrzeug möglicher- und zulässigerweise privat genutzt wird.

Hinzuweisen ist zudem darauf, dass der Einbau von GPS-Geräten in Dienstfahrzeuge nach § 87 Abs 1 Nr. 6 BetrVG mitbestimmungspflichtig ist. Soweit also ein Betriebsrat vorhanden, in dieser Angelegenheit aber nicht beteiligt worden ist, führt dies grundsätzlich zur Unzulässigkeit und damit Rechtswidrigkeit der mit dem Einsatz eines solchen Systems verbundenen Datenverarbeitung bzw. auch des Einsatzes an sich. Das ArbG Kaiserslautern (Beschluss v. 27. August 2008, 1 BVGa 5/08) hat in einem ähnlichen Fall einem Arbeitgeber aufgegeben, bei Meidung eines Zwangsgeldes in Höhe von 500 € pro Tag, das in ein Betriebsfahrzeug eingebaute GPS-Gerät so lange wieder auszubauen, bis eine Einigung der Betriebspartner in Form einer Betriebsvereinbarung gefunden ist. Aus einer insoweit abgeschlossenen Betriebsvereinbarung könnte sich - soweit sie hinreichend bestimmt ist - dann auch die für den Betrieb des GPS-Systems

erforderliche Datenverarbeitungsbefugnis für den Arbeitgeber ergeben. Auf eine Prüfung auf der Grundlage des § 32 BDSG käme es dann nicht mehr an (§ 4 Abs. 1 BDSG).

4.3.3.9 Abgleich von Arbeitnehmerdaten mit „EU-Anti-Terrorlisten“

Ein Arbeitgeber hatte unter Bezugnahme auf zwei europarechtliche Verordnungen von einem Beschäftigten dessen schriftliches Einverständnis, seine Daten in regelmäßigen Abständen mit europäischen Listen terrorismusverdächtiger Personen und Organisationen („EU-Anti-Terrorlisten“) abgleichen zu dürfen, verlangt.

Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit es dieses Gesetz oder eine andere Rechtsvorschrift erlaubt oder anordnet oder der Betroffene eingewilligt hat. Die vom Arbeitgeber genannten europarechtlichen Verordnungen Nr. 881/2002 vom 27. Mai 2002 (ABl. 2002/L 139/9) und Nr. 2580/2001 vom 27. Dezember 2001 (ABl. 2001/L 344/70) verbieten als nach Art. 249 Abs. 2 des Vertrages zur Gründung der Europäischen Union unmittelbar geltendes Recht die finanzielle und wirtschaftliche Unterstützung solcher Terroristen und deren Organisationen, die in fortlaufend aktualisierten Listen namentlich und teils mit weiteren personenbezogenen Daten geführt werden. Als durch die Verordnungen verbotene finanzielle Unterstützung kann dabei auch der Arbeitslohn von Beschäftigten gelten. Die Verordnungen regeln allerdings nicht, welche organisatorischen Maßnahmen Unternehmen zur Umsetzung der Verordnungen ergreifen müssen, damit es zu keiner finanziellen oder sonst wirtschaftlichen Unterstützung kommt. Sie sind daher zu unbestimmt, um als Rechtsvorschrift für einen aus diesem Grunde beabsichtigten Abgleich der sog. „EU-Anti-Terrorlisten“ mit Beschäftigtendaten in Betracht kommen zu können. Ein solcher Abgleich kann daher nicht auf europäisches Recht gestützt werden. Somit verbleiben für eine entsprechende Befugnis allein die Vorschriften des Bundesdatenschutzgesetzes.

Nach § 32 Abs. 1 Satz 1 BDSG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach dessen Begründung für dessen Durchführung oder Beendigung erforderlich ist. Ein Abgleich der Beschäftigtendaten mit den „EU-Anti-Terrorlisten“ dient jedoch allein der Terrorismusbekämpfung, nicht der Zweckbestimmung des Beschäftigungsverhältnisses. § 32 Abs. 1 Satz 1 BDSG ist also ebenso keine zulässige Rechtsgrundlage für einen Datenabgleich mit Beschäftigtendaten.

Dasselbe gilt auch für § 28 Abs. 1 Satz 1 Nr. 1 BDSG, der vor dem 1. September 2009 auf Beschäftigungsverhältnisse anzuwenden war. Unverändert anwendbar ist jedoch § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Hiernach kann ein Arbeitgeber auch dann personenbezogene Daten erheben, speichern, verändern oder übermitteln bzw. sonst für eigene Geschäftszwecke nutzen, soweit dies zur Wahrung seiner berechtigten Interessen erforderlich ist und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des betroffenen Arbeitnehmers an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Ein berechtigtes Interesse der Arbeitgeber kann darin gesehen werden, personenbezogene Daten ihrer Beschäftigten in dem Umfang zu verarbeiten und zu nutzen, wie dies zur Umsetzung der genannten Verordnungen erforderlich ist, um insbesondere sicherzustellen, dass eine Gehaltsüberweisung nicht nach § 34 AWG - auch in fahrlässiger Weise - strafbar ist. Angesichts der anspruchsvollen Vorgaben des KWG (vgl. § 25c Abs. 2 Satz 1), wonach Kreditinstitute verpflichtet sind, angemessene Datenverarbeitungssysteme zu betreiben und zu aktualisieren, mittels deren sie in der Lage sind, Geschäftsbeziehungen und einzelne Transaktionen im Zahlungsverkehr, die geldwäsche- oder sonst terrorismusverdächtig sind, zu erkennen, ist das unternehmerische Risiko - ohne eine besondere und konkrete Gefährdungssituation - aber eher abstrakter Natur und daher im Regelfall nicht geeignet, die sonst überwiegenden schutzwürdigen Interessen der Beschäftigten an einem Ausschluss der Verarbeitung oder Nutzung zurücktreten zu lassen. Hierfür spricht auch, dass bisher den Datenschutzaufsichtsbehörden kein Fall bekannt ist, bei dem es wegen eines - auch nur fahrlässigen - Verstoßes gegen die genannten Verordnungen zu strafrechtlichen Schritten gekommen ist. Dies hat auch die Bundesregierung in ihrer Antwort auf eine Kleine Anfrage im Deutschen Bundestag mitgeteilt (Drs. 16/6236, Frage 4e).

Auch eine Einwilligung i. S. d. § 4 Abs. 1 BDSG durch den Arbeitnehmer kann hier keine Lösung bringen. Die nach § 4a Abs. 1 Satz 1 BDSG gebotene Freiwilligkeit ist jedenfalls nur dann zu bejahen, wenn eine einseitige, nicht durch Gegenleistung ausgeglichene Einwilligung nicht in einer Zwangslage oder unter Druck getroffen wurde; der Arbeitnehmer muss die Verarbeitung seiner Daten ohne die Befürchtung von Sanktionen verweigern können dürfen oder eine zuvor erteilte Einwilligung folgenlos widerrufen können. Genau hieran bestehen aber grundlegende Zweifel, da aufgrund des zwischen den Arbeitsvertragsparteien bestehenden Machtgefälles dem Beschäftigten häufig keine andere Wahl zu bleiben scheint, als der Datenverarbeitungsklausel zuzustimmen.

Nach alledem war der vom Unternehmen beabsichtigte fortlaufende Abgleich von Beschäftigtendaten mit den sog. „EU-Anti-Terrorlisten“ datenschutzrechtlich unzulässig (vgl. hierzu den diesbezüglichen Beschluss des Düsseldorfer Kreises - Pkt. 13.1.1).

4.3.3.10 Betriebliche Altersvorsorge

Im 4. TB war unter Pkt. 4.2.3.3 über einen Fall der unzulässigen Weitergabe der (für betriebliche Notfälle beim Arbeitgeber hinterlassenen) privaten Telefonnummern von Arbeitnehmern zur Angebotserstellung betreffend die betriebliche Altersvorsorge an einen damit beauftragten Versicherungsmakler berichtet worden. Dieser hatte dann mit einzelnen Arbeitnehmern unter deren privaten Telefonnummern Kontakt aufgenommen, um die Möglichkeiten eines Vertragsabschlusses zu erkunden und zu einer Informationsveranstaltung einzuladen.

Vom Grundsatz her ähnlich gelagert, von der tatsächlichen Datenübermittlung jedoch wesentlich umfangreicher war ein Fall aus dem aktuellen Berichtszeitraum:

Das System der freiwilligen betrieblichen Altersvorsorge, insbesondere der Entgeltumwandlung, stellt eine sehr komplexe Materie dar, die angesichts der steuerlichen und sozialversicherungsrechtlichen Vor- und Nachteile und der Vielzahl der möglichen Varianten nicht von jedermann immer gleich durchdrungen wird. Notwendig ist daher eine umfassende Information und Beratung der Arbeitnehmer, für die viele Arbeitgeber externe Beratungsunternehmen verpflichten. Üblicherweise handelt es sich bei dem Informations- und Beratungsprozess um ein dreistufiges Verfahren:

1. allgemeine Information der Beschäftigten über Möglichkeiten der zusätzlichen betrieblichen Altersvorsorge
2. Betriebsversammlung mit detaillierten Informationen zum Versorgungswerk
3. (freiwillige) Einzelgespräche

Von besonderer Bedeutung ist dabei der Übergang von der zweiten zur dritten Stufe. Infolge der komplexen Materie habe es sich nach den Erfahrungen eines Beratungsunternehmens als vorteilhaft erwiesen, wenn den Arbeitnehmern anhand eines zweiten (fiktiven) Lohnzettels die Auswirkungen der betrieblichen Altersvorsorge verdeutlicht würden. Dies erfordere beim Arbeitgeber aber einen zweiten Gehaltslauf. Da dies den Arbeitgebern oftmals zu aufwändig sei, würde diese Aufgabe dann dem jeweiligen Beratungsunternehmen übertragen. Hierfür müssten dann natürlich entsprechende Mitarbeiterlisten (u. a. Namen, Geburtsdatum, Bruttoeinkommen) übermittelt werden, auf deren Basis das Beratungsunternehmen dann in der Lage sei, die Einzelgespräche in ausreichender Weise vorzubereiten.

In dem durch die Aufsichtsbehörde untersuchten Fall waren derartige Listen ohne Wissen der Betroffenen per E-Mail an das Beratungsunternehmen übermittelt worden. Damit war durch den betreffenden Arbeitgeber gleich zweifach gegen das Bundesdatenschutzgesetz verstoßen worden, zum einen wegen der fehlenden Einwilligung der

Arbeitnehmer, zum anderen wegen der unverschlüsselten Internetübertragung. Im Einzelnen:

Gemäß § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit das Bundesdatenschutzgesetz selbst, hier insbesondere § 32, oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Eine Einwilligung war nicht eingeholt worden. Zwar waren die betroffenen Arbeitnehmer nach den der Aufsichtsbehörde vorliegenden Unterlagen mehr oder weniger deutlich auf die Zusammenarbeit mit dem Beratungsunternehmen hingewiesen worden, jedoch genügte dies nicht den vom Bundesdatenschutzgesetz an eine wirksame Einwilligung (vgl. § 4a BDSG) gestellten Anforderungen. Eine andere Rechtsvorschrift, die eine solche Übermittlung erlaubt oder anordnet, war nicht ersichtlich:

§ 32 BDSG bestimmt, dass personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet und genutzt werden dürfen, soweit dies für die Entscheidung über die Begründung des Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Diese Voraussetzung war vorliegend gleichfalls nicht erfüllt gewesen. Selbst wenn den Arbeitgeber eine vergleichsweise umfassende Informations- und Beratungspflicht träfe, könnte diese nicht die Weitergabe von Arbeitnehmerdaten an ein auf Fragen der betrieblichen Altersvorsorge spezialisiertes Beratungsunternehmen rechtfertigen. Denn: Auch für eine notwendigerweise auf die Besonderheiten des einzelnen Falles Bezug nehmende und nur von Fachleuten darauf spezialisierter Beratungsunternehmen vorzunehmende Berechnung ist eine pseudonymisierte Übermittlung von Datensätzen zu einzelnen Arbeitnehmern ausreichend.

Im Ergebnis bestehen betreffend die Information und Beratung von Arbeitnehmern in Fragen der betrieblichen Altersversorgung folgende Alternativen für eine Zusammenarbeit zwischen Arbeitgeber und Beratungsunternehmen:

a) Der Arbeitgeber holt von den (beratungswilligen) Arbeitnehmern vor der Übermittlung eine schriftliche Einwilligung gemäß § 4a BDSG ein und beschränkt die Übermittlung natürlich auch auf diesen Personenkreis.
b) Der Arbeitgeber verzichtet auf eine personenbezogene Datenübermittlung, beschränkt sich insoweit also auf die Weitergabe der für die Berechnung nötigen Daten und ein vom Arbeitgeber eigens für diesen Zweck vergebenes besonderes Pseudonym. Für die später beim Beratungsunternehmen vorsprechenden Arbeit-

nehmer kann dann nach Nennung des Pseudonyms eine für sie zutreffende (vorbereitete) Beispielrechnung aufgerufen und besprochen werden.

c) Es wird generell auf eine vorherige Datenübermittlung verzichtet. Stattdessen werden die benötigten Daten von den interessierten Arbeitnehmern direkt während des Beratungsgespräches erhoben.

Der ungeschützte Versand der Mitarbeiterlisten über das Internet hat im Übrigen auch gegen § 9 BDSG verstoßen.

Gemäß Nr. 4 der Anlage zu § 9 BDSG ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Wahrung der Vertraulichkeit). Der Versand von Mitarbeiterlisten per unverschlüsselter E-Mail über das Internet genügt diesen Vorgaben offensichtlich nicht. Für zukünftige Übermittlungen personenbezogener Mitarbeiterlisten bedeutet dies, dass ein Versand per E-Mail nur bei Einsatz eines ausreichend sicheren Verschlüsselungsverfahrens erfolgen darf. Ist dies nicht möglich, ist auf den herkömmlichen Postweg auszuweichen.

4.3.3.11 Individueller Ausdruck von Entgeltbescheinigungen

Die Mitarbeiter eines Unternehmens sollten ihre Entgeltabrechnungen nicht mehr wie vormals üblich in verschlossenen Umschlägen per Hauspost erhalten, sondern sich diese jetzt selbst über Internet aufrufen und ausdrucken.

Eine solche Verfahrensweise ist nicht von vornherein unzulässig. Voraussetzung dafür ist jedoch, dass die sich aus § 9 BDSG - Technische und organisatorische Maßnahmen - ergebenden Sicherheitsanforderungen eingehalten werden. Gemäß der Anlage zu § 9 BDSG sind u. a. Maßnahmen zu treffen, die geeignet sind, zu gewährleisten, dass

- die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle gemäß Nr. 3 der Anlage zu § 9 BDSG),
- personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Weitergabekontrolle gemäß Nr. 4 der Anlage zu § 9 BDSG),
- nachträglich überprüft und festgestellt werden kann, von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle gemäß Nr. 5 der Anlage zu § 9 BDSG).

Die der Aufsichtsbehörde geschilderte Verfahrensweise ließ allerdings nicht erkennen, dass diesbezüglich ausreichende Maßnahmen getroffen worden waren. Anzuerkennen war zunächst zwar, dass durch die Einrichtung einer verschlüsselten Internetverbindung zumindest eine insoweit ausreichende Weitergabekontrolle gewährleistet war. Nicht den Anforderungen entsprachen aber die festgelegten Verfahrensweisen bei erstmaliger Anmeldung an das System sowie bei vergessenem Passwort. In beiden Fällen war für eine Anmeldung lediglich die Eingabe der - für alle Mitarbeiter gleich strukturierten - E-Mail-Adresse notwendig. Danach konnte ein neues Passwort festgelegt werden. (Bei vergessenem Passwort war vorher zunächst ein entsprechend gekennzeichnetes Feld anzuklicken, wodurch automatisch eine Nachricht an die EDV-Abteilung generiert worden ist, die das zu der angegebenen E-Mail-Adresse gehörige Passwort dann so zurücksetzte, dass bei der nächsten Anmeldung keine Passworteingabe mehr erforderlich war.) Infolge dieser Verfahrensweise konnten sich andere Beschäftigte und darüber hinaus auch externe Personen, die Kenntnis von E-Mail-Adressen oder bei Kenntnis der Adressstruktur auch nur von Namen der Mitarbeiter dieses Unternehmens hatten, ohne Weiteres Zugang zu den Gehaltsdaten eines Mitarbeiters verschaffen. Zwar hat der betroffene Mitarbeiter im Fall des Weges über die „Passwort vergessen“-Funktion eine E-Mail mit der Information, dass sein Passwort zurückgesetzt worden ist, erhalten; bevor er darauf dann jedoch im Einzelfall mit der Festlegung eines neuen Passwortes reagiert hat, konnte ein Dritter bereits Zugriff auf seine Daten erhalten haben. Zugriffs- und auch Eingabekontrolle waren in diesem Fall also nicht ausreichend gewährleistet.

Das Unternehmen hatte die beschriebene Verfahrensweise dann zunächst dahingehend geändert, dass die Nutzer bei erstmaliger Anmeldung oder bei vergessenem Passwort nunmehr ein automatisch generiertes Passwort, welches beim erstmaligen Gebrauch zwingend geändert werden muss, an ihre E-Mail-Adresse gesandt bekamen. Auch diese Verfahrensweise entsprach aber nicht den datenschutzrechtlichen Anforderungen, denn der Versand von Zugangsdaten (hier: Passwörter) per E-Mail widerspricht 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. Etwas anderes würde nur dann gelten, wenn die betreffenden E-Mails verschlüsselt versendet worden wären. Davon ist aber erfahrungsgemäß nicht auszugehen, insbesondere ist dies durch das Unternehmen auch nicht dargelegt worden. In diesem Zusammenhang ist insbesondere zu beachten, dass gerade Passwörter dazu dienen, in einem Datenverarbeitungssystem vorgenommene bzw. vorzunehmende Aktionen eindeutig einer konkreten Person, nämlich dem Inhaber des Passwortes, zuzuordnen bzw. nur diesem überhaupt zu ermöglichen. Der Wahrung der Vertraulichkeit kommt deshalb insbesondere bei Passwörtern eine besondere Bedeutung zu. Für die Erstanmeldung generierte Passwörter sind daher beispielsweise auf herkömm-

liche Weise in einem verschlossenen Umschlag an die Nutzer zu verteilen. Dies gilt im Prinzip auch für die Verfahrensweise bei vergessenen Passwörtern, wobei hier der Einfachheit und Schnelligkeit halber auch eine telefonische Mitteilung denkbar ist und im Allgemeinen wohl auch praktiziert wird (interne Störungshotline).

Ein weiteres, damit verbundenes Problem stellte das Ausdrucken der Gehaltsmitteilung dar. Da weder vorauszusetzen war, dass jeder Mitarbeiter einen privaten Internetzugang besitzt, noch überhaupt verlangt werden konnte, dass Gehaltsmitteilungen privat zuhause abzurufen und auszudrucken sind, müssen auch im Arbeitsumfeld Möglichkeiten bereitgestellt werden, die einen sicheren Ausdruck der Gehaltsmitteilungen ermöglichen. Dabei darf nicht die Gefahr bestehen, dass andere Mitarbeiter die Ausdrucke während oder nach dem Druckvorgang zur Kenntnis nehmen können. Soweit jeder Mitarbeiter einen eigenen Drucker am Arbeitsplatz zur Verfügung hat, sollte dies kein Problem darstellen. Wenn jedoch Mitarbeiter im Unternehmen darauf angewiesen sind, zentrale Drucker zu nutzen, müssen diese mindestens einen so genannten geschützten Druck ermöglichen. Dies bedeutet, dass der jeweilige Druckauftrag erst dann tatsächlich abgearbeitet wird, wenn der auslösende Mitarbeiter unmittelbar am Drucker sein diesbezüglich vorher (beim Druckbefehl) selbst festgelegtes Kennwort eingegeben hat.

4.3.4 Gesundheitswesen

4.3.4.1 Abbruch des Arztbesuches im ersten Anamnesegespräch

Einem Patienten, der um Mithilfe bei der Löschung seiner im Rahmen eines erst- und einmaligen Arztbesuches erhobenen Daten gebeten hatte, musste mitgeteilt werden, dass er eine umgehende Löschung der Daten nicht beanspruchen kann.

Jeden Arzt in einer Praxis oder Krankenanstalt treffen gemäß § 10 BO der Sächsischen Landesärztekammer die dort beschriebenen Dokumentationspflichten. Diesen zufolge hat der Arzt über die in Ausübung seines Berufs gemachten Feststellungen und getroffenen Maßnahmen Aufzeichnungen zu fertigen. Die Aufzeichnungen sind sodann für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren. Da die Dokumentations- und Aufbewahrungspflicht sowohl zivil- als auch standesrechtlich zur Sorgfaltspflicht des Arztes gegenüber seinen Patienten gehört und deren Verletzungen im Prozessfall beweisrechtliche Konsequenzen nach sich zieht, konnte dem Löschungsverlangen nicht stattgegeben werden. In diesem Zusammenhang war es insbesondere auch unerheblich, dass es in diesem konkreten Einzelfall gar nicht zu einer Behandlung gekommen war. Denn auch wenn der Arztbesuch bereits im ersten Anamnesegespräch abgebrochen wird, sind entsprechende Dokumentationen zu fertigen und aufzubewahren.

4.3.4.2 Einsichtnahme in die Patientenakte

Streitigkeiten zwischen Patient und Arzt wegen tatsächlich oder vermeintlich unvollständiger Einsichtnahme in die eigene Patientenakte sind keine Seltenheit. Die Gründe dafür sind vielfältig: Mal betrifft dies Unterlagen, die der Arzt eigentlich gar nicht aufbewahren müsste, mal solche, die dem Patienten nach Meinung des Arztes ohnehin schon bekannt sind. In einem anderen Fall hatte der Arzt seine Praxis-Software gewechselt, wobei es Fehler bei der Übernahme älterer Unterlagen in das neue System gegeben hatte. Es gibt aber natürlich auch (wenige) Fälle, in denen die Einsichtnahme in einzelne Unterlagen zu Recht verweigert worden ist.

Der die Dokumentationspflicht der Ärzte regelnde, auf die Rechtsprechung der Zivilgerichte zurückgehende § 10 Abs. 2 BO der Sächsischen Landesärztekammer bestimmt Folgendes:

Der Arzt hat dem Patienten auf dessen Verlangen grundsätzlich in die ihn betreffenden Krankenunterlagen Einsicht zu gewähren; ausgenommen sind diejenigen Teile, welche subjektive Eindrücke oder Wahrnehmungen des Arztes enthalten. Auf Verlangen sind dem Patienten Kopien der Unterlagen gegen Erstattung der Kosten herauszugeben.

Darüber hinaus unterliegen Ärzte nach dem Bundesdatenschutzgesetz konkreten Auskunftspflichten gegenüber ihren Patienten. § 34 Abs. 1 Sätze 1 und 2 BDSG bestimmt dazu seit dem 1. April 2010:

Die verantwortliche Stelle hat dem Betroffenen auf Verlangen Auskunft zu erteilen über
1. *die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,*
2. *den Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und*
3. *den Zweck der Speicherung.*

Der Betroffene soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen.

Das Datenschutzrecht als solches kennt also nur den Anspruch auf Auskunft, nicht jedoch einen Anspruch auf Einsicht. Für den sich aus dem allgemeinen Zivilrecht ergebenden (weitgehenden) Anspruch auf Einsicht in die eigenen Patientenunterlagen ist die Aufsichtsbehörde nach § 38 BDSG nicht zuständig. Allerdings wird der datenschutzrechtliche Auskunftsanspruch vielfach am einfachsten durch eine mittels Überlassung von Ablichtungen zu bewerkstelligende Einsichtsgewährung erfüllt.

In gewisser Weise ist das Auskunftsrecht gemäß § 34 BDSG sogar weitergehender als das Einsichtnahmerecht gemäß § 10 Abs. 2 BO, denn letzteres betrifft nur die den Patienten betreffenden Krankenunterlagen, mithin die durch den Arzt in Ausübung seines Berufs gemachten Feststellungen und getroffenen Maßnahmen, über die er die erforderlichen Aufzeichnungen angefertigt hat (vgl. § 10 Abs. 1 BO). Es gibt also durchaus Unterlagen, die zwar dem Auskunftsrecht, nicht jedoch dem Einsichtnahmerecht unterfallen. Nur als Beispiel sei etwa eine Befundanforderung durch den Ärztlichen Dienst der Bundesagentur für Arbeit genannt.

Ausnahmsweise können Ärzte ihren Patienten Unterlagen bzw. gewisse medizinische Erkenntnisse aus therapeutischen Gründen, d. h. dann, wenn aufgrund medizinischer Fachkenntnis damit gerechnet werden muss, dass eine Offenlegung der Erkenntnisse der gesundheitlichen Entwicklung des Patienten schaden könnte, auch bewusst vorenthalten (sogenanntes „therapeutisches Privileg“). Dass Ärzte ein solches Recht (und sogar die Pflicht!) haben, ist von der Rechtsprechung anerkannt (vgl. z. B. BGH, Urt. v. 23. November 1982 VI ZR 222/79 - NJW 1983, 328 ff.). Ob die diesbezüglichen Voraussetzungen, die nach der Rechtsprechung sehr streng sind, im Einzelfall tatsächlich vorliegen, hat die Aufsichtsbehörde aber nicht zu beurteilen. Im Bundesdatenschutzgesetz wird ein solcher Sachverhalt in § 34 Abs. 7 i. V. m. § 33 Abs. 2 Satz 1 Nr. 3 BDSG abgebildet, wonach Daten, die ihrem Wesen nach geheim gehalten werden müssen, nicht zu beauskunften sind (vgl. Dix in: Simitis, BDSG, 6. Auflage, Rn. 76 zu § 33).

4.3.4.3 Übergabe von Patientendaten an Praxisnachfolger

Gegenstand gleich mehrerer Anfragen im Berichtszeitraum war die Weitergabe von Patientendaten an einen Praxisnachfolger.

Ohne die eindeutige und unmissverständliche Einwilligung des Patienten verstößt die Weitergabe der ihn betreffenden Patientenakten im Fall einer Praxisübernahme an einen fremden Arzt gegen § 203 StGB. Da sich die Arzt-Patienten-Vertrauensbeziehung nicht ohne Weiteres auf einen Praxisnachfolger übertragen lässt, sieht der BGH darin eine Verletzung des Rechts auf informationelle Selbstbestimmung und einen Verstoß gegen die ärztliche Schweigepflicht (z. B. BGH, NJW 1995, 2026; NJW 1996, 773 f.).

Datenschutzrechtlich vertretbar und in der Regel gängige Praxis ist jedoch das so genannte „Zwei-Schrank-Modell“. Hiernach verpflichtet sich der Nachfolger, manuell geführte Patientenkarteien in einem verschlossenen Schrank gesondert zu verwahren. Deren datenschutzrechtliche Verfügungsbefugnis verbleibt - ungeachtet des Gewahrsams - beim Vorgänger. Die alte Akte darf nur bei einem entsprechenden Einverständnis des Patienten entnommen und durch den Erwerber fortgeführt und mit einer lau-

fenden Patientenkartei zusammengeführt werden (vgl. auch § 10 Abs. 4 Satz 2 BO der Sächsischen Landesärztekammer). Aktenzugriffe und das Einverständnis sind jeweils zu dokumentieren. Bei elektronisch geführten Patientendaten muss der alte Bestand gesperrt und der Zugriff (z. B. durch Passwortschutz) jeweils gesichert werden. Die Freischaltung und weitere Nutzung des elektronischen Datensatzes durch den Nachfolger bedarf wie bei der manuellen Patientenkartei der Zustimmung des Patienten.

4.3.4.4 Kundenkarten in Apotheken

Die zulässige Verarbeitung personenbezogener Daten aus Verschreibungen ist für Angehörige der gesetzlichen Krankenkassen in § 300 Abs. 1 und 2 SGB V geregelt. Das SGB V geht als bereichsspezifische Vorschrift insoweit den Regelungen des Bundesdatenschutzgesetzes vor (vgl. § 1 Abs. 3 Satz 1 BDSG). Bei der Abgabe von auf einem Privatrezept verordneten Medikamenten werden in diesem Zusammenhang üblicherweise keine Kundendaten elektronisch erfasst.

Für darüber hinausgehende, weder aus dem SGB V oder anderen Spezialgesetzen noch aus den in diesem Fall maßgeblichen Vorschriften des § 28 Abs. 6 und 7 BDSG zu rechtfertigende Verarbeitungen, beispielsweise im Rahmen des Einsatzes von Kundenkarten, ist die Einwilligung der Betroffenen notwendig (vgl. § 4 Abs. 1 BDSG). Diese muss den Anforderungen des § 4a BDSG, wegen der Verarbeitung sensitiver Daten (hier: Gesundheitsdaten - vgl. § 3 Abs. 9 BDSG) insbesondere auch dessen Absatz 3 genügen.

Danach ist die Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform. Soll sie zusammen mit anderen Erklärungen erteilt werden, ist sie besonders hervorzuheben. Zudem muss sich die Einwilligung ausdrücklich auf die dabei verarbeiteten Gesundheitsdaten beziehen. Die unzureichende Umsetzung dieser gesetzlichen Vorgaben kann zur Nichtigkeit der Erklärung und damit zur Rechtswidrigkeit der darauf gestützten Datenverarbeitung führen. Empfohlen wird darüber hinaus ein ausdrücklicher Hinweis auf die Widerrufsmöglichkeit.

In jedem Fall sind in der Erklärung alle mit der Kundenkarte verfolgten Zwecke konkret zu benennen. Eine Nutzung für andere Zwecke wäre unzulässig. Damit den Kunden der Umfang der erteilten Einwilligungen bewusst wird und bleibt, sollte ihnen zudem ein Duplikat der Einwilligungserklärung oder ein entsprechendes Informationsblatt übergeben werden.

Mitunter enthalten die von Apotheken genutzten Kundenbindungssysteme schon vorformulierte Einwilligungserklärungen des jeweiligen Herstellers. Die Nutzung dieser Erklärungen ist aber erfahrungsgemäß kein Garant für eine datenschutzrechtliche einwandfreie Lösung, insbesondere kann sich die jeweilige Apotheke mit Verweis auf den betreffenden Softwarehersteller auch nicht von ihrer diesbezüglichen Verantwortung befreien. Es ist nicht (allein) Aufgabe der Hersteller von Kundenbindungssystemen, eine den gesetzlichen Anforderungen entsprechende Einwilligungserklärung in den von ihnen vertriebenen Systemen bereitzustellen. Die jeweiligen Firmen können allenfalls unterstützend tätig werden, indem sie die Vorgaben ihrer Kunden, mithin also der Apotheken entsprechend umsetzen. Verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG sind die Apotheken - diese müssen die entsprechenden Vorgaben zur inhaltlichen Ausgestaltung der Einwilligungserklärung machen, insbesondere auch die mit der Kundenkarte verfolgten Zwecke klar benennen, damit diese in die Einwilligungserklärung eingearbeitet werden können. Möglich sind insoweit etwa auch Ankreuzlösungen, d. h. eine Auflistung verschiedener für Apotheken in Frage kommender Verwendungszwecke, die dann von jeder Apotheke individuell vor der Unterzeichnung durch den Betroffenen ausgewählt werden können.

4.3.4.5 Aufbewahrungsfristen für Pflegedokumentationen

Wiederholt haben Pflegedienste angefragt, welche Aufbewahrungsfristen für Pflegedokumentationen gelten würden. Hierzu ist Folgendes auszuführen:

In der stationären Pflege sind die Aufbewahrungspflichten von Bewohnerakten, zu denen auch die Pflegedokumentation zählt, durch § 13 Abs. 2 HeimG mit der Vorgabe von fünf Jahren klar definiert.

Für die Aufbewahrung von Pflegedokumentationen ambulanter Pflegedienste findet § 13 HeimG keine Anwendung. Wenngleich Pflegedokumentationen nicht vordergründig zu diesem Zweck gefertigt werden, so kommen sie doch als Beweismittel in Haftungsfällen in Betracht. Daher ist die insoweit geltende Verjährungsfrist bei der Bemessung der Aufbewahrungsfrist zu berücksichtigen. Gemäß § 199 Abs. 2 BGB verjähren Schadensersatzansprüche, die auf der Verletzung des Lebens, des Körpers, der Gesundheit oder der Freiheit beruhen, ohne Rücksicht auf ihre Entstehung und die Kenntnis oder grobfahrlässige Unkenntnis in 30 Jahren von der Begehung der Handlung, der Pflichtverletzung oder dem sonstigen, den Schaden auslösenden Ereignis an. Daher können Pflegedokumente bis zum Ablauf dieser Frist aufbewahrt werden.

4.3.4.6 Nutzung von Gesundheitsdaten für Werbezwecke

Ein an Diabetes Erkrankter hatte seine ärztlichen Verordnungen in Verkaufsgeschäften eines auf Diabetesprodukte spezialisierten Unternehmens eingelöst. Nachdem er einige Zeit später von diesem Unternehmen Informationen über die kostenlose Nutzung eines Blutzuckermessgerätes erhalten hatte, hat sich für ihn die Frage gestellt, ob die Nutzung seiner, aus den ärztlichen Verordnungen stammenden, personenbezogenen Daten für diesen Zweck rechtlich zulässig gewesen war.

Dies ist in der Tat nicht der Fall gewesen. Für das Informationsschreiben genutzt worden sind nicht nur Name und Anschrift des Betroffenen, sondern eben auch das Datum „Bezieher von Diabetiker-Artikeln“. Bei diesem Datum hat es sich um eine Angabe über die Gesundheit, mithin um ein personenbezogenes Datum besonderer Art im Sinne des § 3 Abs. 9 BDSG, gehandelt. Die Voraussetzungen, unter denen das Erheben, Verarbeiten und Nutzen derartiger Daten auch ohne Einwilligung des Betroffenen zulässig ist, sind abschließend in den Sondervorschriften des § 28 Abs. 6 bis 9 BDSG geregelt. Von diesen Erlaubnistatbeständen kam vorliegend allenfalls § 28 Abs. 7 BDSG (medizinische Versorgung) in Betracht. Da Informationen über neue Produkte im Diabetesbereich und kostenlose Nutzungsmöglichkeiten eines Blutzuckermessgerätes aber nicht den in § 28 Abs. 7 BDSG konkret benannten Zwecken, d. h. der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung zugeordnet werden können und auch für die Verwaltung von Gesundheitsdiensten nicht erforderlich sind, sondern gerade und nur der Werbung dienen, kam also auch eine Nutzung auf Grundlage des § 28 Abs. 7 BDSG nicht in Betracht.

Eine Nutzung dieser Daten für Werbezwecke wäre daher nur bei Vorliegen einer entsprechenden Einwilligungserklärung gemäß § 4a BDSG, wobei insbesondere auch Absatz 3 dieser Vorschrift zu beachten ist, zulässig gewesen.

4.3.4.7 Administratorrechte für Aufsichtsratsmitglieder?

Die Geschäftsführerin einer gemeinnützigen, in der Altenpflege tätigen GmbH hat die Frage aufgeworfen, ob Mitgliedern des Aufsichtsrats in der Weise unbeschränkter Zugriff auf alle Datenbestände des Unternehmens und damit auch auf personenbezogene Daten gewährt werden dürfe, wie ihn Administratoren nehmen könnten.

Hinsichtlich der Verarbeitung personenbezogener Daten unterscheidet das Bundesdatenschutzgesetz für das Außenverhältnis der verantwortlichen Stelle zum Betroffenen nicht zwischen der Verantwortung der Geschäftsführung einer GmbH und ihres Aufsichtsrats bzw. den einzelnen Organen einer verantwortlichen Stelle i. S. d. § 3 Abs. 7 BDSG. Datenschutzrechtlich ist die GmbH als juristische Person, wenn sie personen-

bezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt, insgesamt verpflichtet, die technischen und organisatorischen Maßnahmen zu treffen, die nach Maßgabe der Anlage zu § 9 BDSG zur Einhaltung der besonderen Anforderungen des Datenschutzes zur Datensicherheit erforderlich sind. Hiernach ist die innerbetriebliche Organisation so zu gestalten bzw. sind insbesondere Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind, u. a. zu gewährleisten, dass

- personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle) und
- nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle).

Die Vergabe von Administratorrechten muss im Lichte dieser Vorgaben gesehen werden. Die organschaftliche Ermächtigung des Aufsichtsrats aus dem gemäß § 52 Abs. 1 GmbHG anwendbaren § 111 Abs. 2 Satz 1 AktG, Bücher und Schriften der Gesellschaft, mithin deren Datenbestände zu prüfen, setzt keine Administratorrechte voraus, da der Wortlaut der Vorschrift lediglich von einer Einsichtnahme zum Zwecke der Prüfung spricht. Die umfassenden Zugriffsrechte des Systemadministrators rechtfertigen sich allein aus dessen Verantwortlichkeit für die Funktionsfähigkeit der informationstechnischen Infrastruktur. Es gibt daher keinen Grund, weshalb der Aufsichtsrat, dem keine derartige Aufgabe zukommt, gleiche Zugriffsrechte benötigen soll. Die Einsichtsbefugnis des Aufsichtsrats in personenbezogene Daten findet jenseits der Frage nach der Vergabe von (globalen) Administratorrechten schon allgemein ihre Schranke, wenn die Nutzung der Daten zur Wahrung der berechtigten Interessen des Aufsichtsrats, also der seiner Kontrollbefugnis, nicht erforderlich ist oder Grund zur Annahme besteht, dass schutzwürdige Interessen Betroffener dem entgegenstehen (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG). Dies zu beurteilen, ist allerdings eine Frage des Einzelfalls. Die pauschale Vergabe von Administratorrechten an die Mitglieder des Aufsichtsrats einer GmbH zum Zweck der Ausübung ihrer organschaftlichen Kontrolle über die Geschäftsführung ist datenschutzrechtlich aber in keinem Fall zulässig.

4.3.5 Einzelhandel

4.3.5.1 Schuldanerkenntnisse an Tankstellen

Es scheint kein Einzelfall zu sein, dass Tankstellenkunden nach dem Tanken feststellen, dass sie ihre Kredit- oder EC-Karte vergessen haben oder dass diese nicht funktioniert

und sie auch kein Bargeld bei sich führen. Während man bei sonstigen Einkäufen in solchen Fällen die Ware erst einmal beim Händler lassen kann, geht das beim Tanken bekanntlich nicht so ohne Weiteres, zumal man das betankte Fahrzeug natürlich regelmäßig dazu benötigt, um die fehlenden Zahlungsmittel heranzuschaffen.

Die Kundin einer Tankstelle hat der Aufsichtsbehörde berichtet, dass von ihr - nachdem sie aufgrund einer nicht funktionsfähigen EC-Karte den zu leistenden Geldbetrag nicht hatte sofort begleichen können - das Ausfüllen und Unterzeichnen eines Schuldanerkenntnisses verlangt worden sei. Die von ihr in den Vordruck eingetragenen Angaben seien anschließend von der Kassiererin mit dem Personalausweis verglichen und ergänzt worden. Nachdem die Kundin dann noch am selben Tag den ausstehenden Geldbetrag bar beglichen habe, sei ihr allerdings die Aushändigung des Schuldanerkenntnisses verweigert worden.

Durch die Aufsichtsbehörde ist zunächst festgestellt worden, dass das Personalausweisgesetz der dargestellten Verfahrensweisen nicht entgegengestanden hat, denn § 4 Abs. 1 PAuswG regelt, dass der Personalausweis auch im nicht-öffentlichen Bereich, d. h. also auch gegenüber einem Einzelhandelsunternehmen und nicht wie teilweise angenommen nur gegenüber Behörden, als Ausweis- und Legitimationspapier benutzt werden darf. Dies war letztendlich auch nicht das Problem der Beschwerdeführerin. Ihr kam es vielmehr darauf an, dass nach Begleichen des ausstehenden Zahlbetrages keine Daten mehr von ihr beim Tankstellenbetreiber verbleiben sollten, denn dafür bestand nach ihrer Auffassung keine Notwendigkeit.

Natürlich hatte die Kundin damit auch recht. Das Unternehmen, welches diese und eine Vielzahl weiterer Tankstellen betrieb, ist dieser Auffassung dann auch sofort gefolgt und hat umgehend die Vernichtung der in den Tankstellen ggf. noch vorhandenen (eingelösten) Schuldanerkenntnisse angewiesen. Der Datenschutzbeauftragte der Tankstellenkette hat den Vorfall zudem zum Anlass genommen, das Formular für das Schuldanerkenntnis den datenschutzrechtlichen Erfordernissen anzupassen, insbesondere nicht benötigte Daten, wie beispielsweise die Personalausweisnummer, aus dem Vordruck zu entfernen. Zukünftig wird einem Kunden, der - aus welchem Grund auch immer - nicht zahlen kann, nach dem Ausfüllen und der Unterzeichnung des Schuldanerkenntnisses sowie der Überprüfung der Angaben anhand des Personalausweises (oder eines anderen Nachweises), eine Kopie des ausgefüllten Formulars mit seinen Daten übergeben. Nach Begleichung des ausstehenden Geldbetrages wird dem Kunden dann auch das Original ausgehändigt.

4.3.5.2 Werbewiderspruch und Auskunftsanspruch bei Adressmiete

Eine Petentin hat sich an die Aufsichtsbehörde gewandt, weil ein Möbelhaus nicht auf ihr schriftliches Auskunftsverlangen und den damit verbundenen Widerspruch gegen die weitere Verarbeitung oder Nutzung ihrer Daten für Werbezwecke geantwortet hatte. Einräumen musste sie dabei allerdings, dass sie seitdem über einen Zeitraum von immerhin fünf Monaten auch keine weiteren Werbeschreiben mehr erhalten hatte.

Infolge dieser Sachlage war also zunächst davon auszugehen, dass der Werbewiderspruch durch das Möbelhaus entsprechend beachtet und umgesetzt worden war. Eine Verpflichtung, Betroffene darüber entsprechend zu informieren, ergibt sich aus dem Bundesdatenschutzgesetz nicht.

Darüber hinaus hatte die Petentin aber auch ihr Auskunftsrecht geltend gemacht, insbesondere hat sie wissen wollen, woher das Möbelhaus ihre Adressdaten bezogen hatte. Genau diese Information hätte die Petentin durch eine etwas genauere Betrachtung des letzten Werbeschreibens aber auch selbst in Erfahrung bringen können. Etwa in der Mitte des Werbeschreibens war neben dem notwendigen Hinweis auf das Widerspruchsrecht auch die verantwortliche Stelle - nicht das Möbelhaus - benannt (§ 28 Abs. 4 Satz 2 BDSG) - beides durch eine entsprechende Einrahmung auch ausreichend deutlich hervorgehoben. Aus dieser Angabe war also abzulesen, dass das Möbelhaus die Anschrift nur gemietet und (üblicherweise durch einen externen Dienstleister) einmalig verarbeitet, nicht jedoch selbst gespeichert hatte. Unter diesen Voraussetzungen (keine Speicherung durch das Möbelhaus) kam auch das Auskunftsrecht des § 34 BDSG nicht zum Tragen. Es besteht keine rechtliche Pflicht, jemanden über die „Nichtspeicherung“ von Daten zu unterrichten. Der in solchen Fällen dessen ungeachtet bestehenden Verpflichtung, den Betroffenen bei der Ansprache zu Werbezwecken die für die Nutzung der Daten verantwortliche Stelle eindeutig erkennbar zu machen, war mit dem oben erwähnten Hinweis in ausreichender Weise entsprochen worden.

Um zu verhindern, dass ihre Anschrift auch weiterhin an andere Unternehmen für Werbezwecke weitergegeben bzw. vermietet wird, hat sich die Betroffene an die im Werbeschreiben benannte verantwortliche Stelle wenden müssen.

4.3.5.3 Kopierdienstleistungen

Ein Petent hat sich darüber beschwert, dass ein bisher im Kundenraum eines Geschäfts befindliches Kopiergerät hinter die Verkaufstheke verlegt worden sei, womit die Kunden nunmehr nicht mehr selbst kopieren könnten, sondern das Verkaufspersonal dies übernehmen müsse. Dabei könne nicht ausgeschlossen werden, dass das die Kopien anfertigende Personal den Inhalt der Kopien zumindest teilweise zur Kenntnis nimmt,

denn schließlich müsse sichergestellt werden, dass die Originale korrekt in den Kopierer eingelegt werden und die Kopien in ausreichender Lesbarkeit angefertigt worden sind.

Der Shop-Inhaber hat der Aufsichtsbehörde daraufhin drei Gründe genannt, die zu dieser Entscheidung geführt haben. Zum einen sei dies die Tatsache, dass vielen Kunden ohnehin beim Kopieren geholfen werden müsse, und so habe man kurze Wege und müsse die übrige Kundschaft nicht lange warten lassen. Zum anderen kämen Kunden gelegentlich auch nicht mit dem Kopiergerät zurecht, was bereits zu entsprechenden Schäden geführt habe. Schließlich sei noch von Bedeutung, dass man durch die zwingende Einbeziehung des Geschäftspersonals auch eine bessere Kontrolle darüber habe, dass keine urheberrechtlich geschützten Werke kopiert werden.

Diese Argumente waren zwar nur bedingt geeignet, die Standortverlegung des Kopiergerätes hinter die Verkaufstheke nachvollziehbar zu erklären, jedoch erwuchs daraus allein noch kein Verstoß gegen datenschutzrechtliche Vorschriften.

Der Argumentation, dass vielen Kunden geholfen werden müsste und dadurch die übrige Kundschaft mit Wartezeiten belegt würde, war entgegenzuhalten, dass das ausschließliche Kopieren durch das Personal insgesamt sicherlich noch mehr personelle Ressourcen bindet. Auch der Verweis auf den Urheberrechtsschutz war wenig geeignet, den Standort des Kopierers hinter der Verkaufstheke zu rechtfertigen, denn den Inhalt der Kopiervorlagen (will und) kann das Personal im Regelfall gar nicht so erfassen, dass eine solche Beurteilung überhaupt möglich wäre, geschweige denn, dass das Personal überhaupt in der Lage wäre, solch eine Beurteilung dann auch wirklich vorzunehmen.

Grundsätzlich wird daher zwar die Auffassung vertreten, dass es datenschutzrechtlich sicher problematisch ist, wenn Kunden ihre Kopien nicht selbst anfertigen können, sondern hierfür die Originale an das Personal des Kopiergeschäftes übergeben müssen. Gleichwohl ist einzuräumen, dass jeder Unternehmer - innerhalb der durch das Datenschutzrecht gezogenen Grenzen - natürlich das Recht hat, zu entscheiden, auf welche Art er seinen Kunden Datenverarbeitungsdienstleistungen anbieten will und in welcher Weise er dabei sein Personal zum Einsatz bringt. Auch bei im Verkaufsraum befindlicher, durch die Kunden selbst zu bedienender Kopiertechnik ist schließlich oftmals ein unterstützendes Eingreifen des Personals in die Kopiervorgänge, etwa bei Bedienungsunsicherheiten von Kunden oder Funktionsfehlern des Gerätes, notwendig. Voraussetzung ist in jedem Fall, dass mit den jeweiligen Aufgaben nur befugte, d. h. eingewiesene und auf das Datengeheimnis verpflichtete Mitarbeiter betraut werden.

Im Übrigen müssen die Kunden selbst entscheiden, ob sie ihre Unterlagen auf diese Weise vervielfältigen lassen oder eben in einem alternativen Copy-Shop selbst kopieren.

In der gleichen Eingabe ist darüber hinaus auch die Problematik der (Zwischen-) Speicherung der angefertigten Kopien auf den heute überwiegend im Einsatz befindlichen Digitalkopierern angesprochen worden. Die dem Petenten hierzu vom Verkaufspersonal erteilten Auskünfte hätten ihn in keiner Weise befriedigt; es sei noch nicht einmal verbindlich zu erfahren gewesen, ob überhaupt eine Speicherung stattfindet.

Auch die der Aufsichtsbehörde erteilten Auskünfte zeigten, dass sich das Verkaufspersonal dieser Problematik weder bewusst war noch sich irgendwie in der Lage fühlte, die diesbezüglichen Eigenschaften des Kopiergerätes zu ermitteln oder gar entsprechende Einstellungen vorzunehmen. Dies lag wohl nicht zuletzt darin begründet, dass es sich hierbei nicht um eine offenkundige, jedermann zur Verfügung stehende Funktionalität eines Digitalkopierers handelt. Stattdessen erschließt sich eine solche Möglichkeit wahrscheinlich erst aus genauerem Studium der Betriebsanleitung oder der Konsultation eines fachkundigen Servicetechnikers. Insoweit ist das Risiko einer unbefugten Offenlegung von auf dem jeweiligen Gerät kopierten Unterlagen in der Praxis möglicherweise auch kleiner als allgemein vermutet. Dies ändert aber nichts an der datenschutzrechtlichen Relevanz dieses Themas. Soweit digitale Kopien (Dateien) auch nach erfolgtem Ausdruck weiter auf der Festplatte gespeichert bleiben, kann durch mit entsprechender Fachkenntnis ausgestattete Personen auf die darin ggf. enthaltenen personenbezogenen Daten auch zu einem späteren Zeitpunkt, beispielsweise nach Verkauf bzw. Aussonderung eines Gerätes, noch zugegriffen werden.

Aus datenschutzrechtlicher Sicht besteht daher die Forderung, diese Geräte so einzustellen, dass nach jedem Kopiervorgang die zugehörige Datei auf der Festplatte überschrieben wird. Soweit bekannt, wird eine Löschfunktion in dieser Form bislang noch nicht von allen Herstellern unterstützt. Abhängig von Hersteller und Gerätetyp sollten bei modernen Geräten nichtsdestoweniger zumindest Einstellmöglichkeiten bestehen, dass die (zwischen-)gespeicherten Daten nach jedem Druckauftrag, nach jedem Neustart des Gerätes oder nach einer vordefinierten Zeit gelöscht werden. Alternativ sollten die gespeicherten Dateien zumindest manuell gelöscht werden können.

Im Übrigen gilt aber auch hier: Wenn einem Kunden dieses Thema wichtig ist und der jeweilige Geschäftsinhaber ihm diesbezüglich keine zufriedenstellende Auskunft geben kann, sollte er sich einen anderen Copy-Shop suchen und dies auch entsprechend zum Ausdruck bringen.

4.3.6 Sparkassen / Banken

4.3.6.1 Online-Banking: Gemeinsame Verwaltung privater und betrieblicher Konten

Betroffen war die Kundin eines Kreditinstituts, die in ihrer Eigenschaft als Arbeitnehmerin für ihren Arbeitgeber Bankgeschäfte tätigte und dabei auch am Online-Banking teilnahm. Zu diesem Zweck war für sie als Privatperson ein Online-Banking-Zugang eingerichtet worden, für den sie dann eine Freischaltung des Firmenkontos erhalten hatte. Nachdem sie wohl am Online-Banking Gefallen gefunden hatte, entschloss sie sich, auch für ihre Privatkonten die Teilnahme am Online-Banking zu beantragen. Das Kreditinstitut schaltete daraufhin auch ihre Privatkonten für ihren bereits bestehenden Online-Banking-Zugang frei und teilte ihr in diesem Zusammenhang mit, dass die ihr bereits zur Verfügung stehenden Sicherungsmittel (PIN, TAN) auch weiterhin ihre Gültigkeit behielten.

Als die Kundin das nächste Mal für ihren Arbeitgeber Bankgeschäfte online erledigen wollte, stellte sie entsetzt fest, dass über ihren - ihrer Meinung nach betrieblichen - Online-Banking-Zugang auch ihre Privatkonten zugänglich waren. Damit aber nicht genug: Prompt kam auch ihre Geschäftsführerin auf sie zu und sprach sie mit Verweis auf das Online-Banking auf ihre konkrete finanzielle Situation an. Natürlich vermutete sie sofort einen Datenschutzverstoß des Kreditinstituts; tatsächlich trug sie selbst aber die Hauptschuld an diesem Vorfall:

Das Kreditinstitut hat auf Nachfrage mitgeteilt, dass die Sicherungsmittel nicht konto- sondern personengebunden vergeben würden. Sie seien durch die jeweils berechtigte Person sicher zu verwahren; eine Weitergabe an andere Personen sei - was sich praktisch von selbst versteht, denn nur so können Transaktionen auch eindeutig konkreten Nutzern zugeordnet werden - vertraglich untersagt und verstoße gegen die Sorgfaltspflichten des Online-Banking-Teilnehmers.

In der Tat hatte die Kundin die ihr zugesandten Sicherungsmittel unzulässigerweise (vertragswidrig) auch ihrer Geschäftsführerin zugänglich gemacht. Diese hatte damit in gleicher Weise auf den Online-Banking-Zugang der Kundin zugreifen können wie diese selbst und demnach auch deren Privatkonten zu sehen bekommen. In erster Linie war die Petentin also an dieser Datenschutzpanne selbst schuld. Zwar hatten zusätzlich auch die Antragsformulare des Kreditinstituts für das Online-Banking einige - anschließend behobene - unklare Formulierungen aufgewiesen, jedoch war dies vorliegend nicht entscheidend, weil dies allein keinesfalls dazu geführt hätte, dass die Geschäftsführerin Zugriff auf die Privatkonten der Kundin erhalten konnte. Für die Geschäftsführerin ist im weiteren Verlauf der Angelegenheit schließlich ein eigener Online-Banking-Zugang

eingerichtet worden, über den sie dann natürlich ausschließlich Zugang zum Firmenkonto erhalten hat. Alternativ wäre es nach Auskunft des Kreditinstituts auch möglich gewesen, deren spezielle Zugangssoftware für Unternehmen zum Einsatz zu bringen. Mittels dieser Software können Firmenkunden für mehrere Mitarbeiter separate Zugänge zum Firmenkonto einrichten, so dass diese Bankgeschäfte für ihren Arbeitgeber nicht über ihren persönlichen (privaten) Online-Banking-Zugang abwickeln müssen.

4.3.6.2 Auswertung von Kontobewegungen für Vertragsangebote

Dem Kunden eines Kreditinstituts war ein sogenanntes „Gegenangebot Haftpflichtversicherung“ gemacht worden. Ihm war dabei mitgeteilt worden, dass bei der Durchsicht seiner Kontounterlagen aufgefallen sei, dass er an eine Versicherung einen bestimmten monatlichen Betrag für seine Haftpflichtversicherung zahle. Diesem Schreiben war das Angebot einer mit dem Kreditinstitut verbundenen Versicherung beigelegt worden, aus der sich ergab, dass diese ihm eine Haftpflichtversicherung für einen günstigeren jährlichen Gesamtbeitrag anbieten könne.

Das von dem Kreditinstitut für die Versicherung abgegebene Angebot war mehr als bloße Werbung im Sinne der diesbezüglichen Vorschriften des Bundesdatenschutzgesetzes. Es war eine auf das Individuum im Hinblick auf den Einfluss persönlicher Eigenschaften auf eine mögliche künftige Vertragsgestaltung zugeschnittene Einladung, ein Vertragsangebot abzugeben oder einzuholen. Das war etwas anderes als etwa ein Werbeprospekt, in dem ein Kleidungsstück oder eine Reise zu einem festen Preis beworben wird, der für alle gleich ist.

Auf die daher - mangels Werbung im Sinne des § 28 Abs. 3 BDSG - grundsätzlich anwendbare Vorschrift des § 28 Abs. 1 Satz 1 Nr. 1 BDSG, wonach die Nutzung personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig ist, wenn es für die Durchführung eines rechtsgeschäftlichen Schuldverhältnisses erforderlich ist, ließ sich die von dem Kreditinstitut vorgenommene Datennutzung nicht stützen. Denn die Nutzung war nicht zur Durchführung des Girovertrages erforderlich gewesen, auch nicht zur ordnungsgemäßen Durchführung eines sonstigen Rechtsverhältnisses des Kreditinstituts mit dem betroffenen Kunden; insbesondere hatte der Bankkunde auch keinen Makler-, Vermittlungs- oder Beraterauftrag erteilt.

Das Kreditinstitut hat auf entsprechende Anfrage daraufhin mitgeteilt, dass es diese Auffassung vom Grundsatz her zwar teile, jedoch hierzu mangels ausreichender Kenntnis des Einzelfalles keine abschließende Aussage treffen könne. Zunächst müsse davon ausgegangen werden, dass der betreffende Berater einen konkreten und nachvollziehbaren Anlass hatte, die Umsätze auf dem Konto des betreffenden Kunden einzusehen.

Solche Anlässe könnten beispielsweise die Beantragung eines Kredites, die Erhöhung einer bestehenden Dispositionskreditlinie oder das Vorliegen eines Finanzchecks gewesen sein. Hinzu komme, dass das Kreditinstitut schon langjährig mit der Versicherung kooperiere und es daher möglich sei, dass der betreffende Berater in diesem Fall die falsche Einschätzung getroffen habe, dass es sich um ein - u. U. zulässiges - eigenes Angebot gehandelt habe.

Eine weitere Prüfung und insbesondere abschließende Bewertung des dargestellten Sachverhaltes war leider nicht möglich, denn dies hätte eine genaue Prüfung des Einzelfalles und damit die Offenlegung der Identität des Petenten erfordert. Dazu war dieser aber nicht bereit, sondern bestand auf vertraulicher Behandlung der durch ihn vorgebrachten Angelegenheit.

Das betreffende Kreditinstitut hat diesen Vorgang nichtsdestoweniger zum Anlass genommen, seine Mitarbeiter hinsichtlich der gesetzlichen Rahmenbedingungen für die Nutzung personenbezogener Daten für Werbe- und Angebotszwecke weiter zu sensibilisieren. Darüber hinaus soll zukünftig sichergestellt werden, dass alle Werbemaßnahmen, die unter Nutzung personenbezogener Kundendaten erfolgen, zuvor jeweils hinsichtlich ihrer rechtlichen Unbedenklichkeit geprüft werden.

4.3.7 Vereine / Verbände

4.3.7.1 Eintrittskartenverkauf bei beschränktem Kartenkontingent

Von einem Fußballfan ist die Aufsichtsbehörde auf die Zulässigkeit der Erhebung von Zuschauerdaten im Zusammenhang mit dem Verkauf von Eintrittskarten angesprochen worden. Nach dessen Schilderung sollten Eintrittskarten (pro Person eine Karte) für ein stark nachgefragtes Auswärtsspiel an Mitglieder gegen Vorlage des Mitgliedsausweises und an Nichtmitglieder gegen Vorlage eines Lichtbildausweises verkauft werden. Im Rahmen des Verkaufs - so sei vereinsintern angekündigt worden - würden insbesondere auch die Daten von Nichtmitgliedern erfasst und deren Namen auf den gekauften Eintrittskarten vermerkt werden.

Die tatsächliche Verfahrensweise hat der Fußballverein dann allerdings wie folgt beschrieben:

Bei Auswärtsspielen mit einem begrenzten Kartenkontingent erfolge der Eintrittskartenverkauf in zwei Phasen. Zunächst hätten Vereinsmitglieder ein Vorkaufsrecht; in der zweiten Phase könnten dann auch externe Fans jeweils eine Karte erwerben (freier Verkauf). In der ersten Verkaufsphase würden in der Mitgliederliste diejenigen Personen markiert, die eine Karte erworben haben. Damit solle verhindert werden, dass

Mitglieder mehrere Tickets erwerben. In der zweiten Verkaufsphase würden von jedem Käufer Vorname, Nachname, Anschrift und Geburtsdatum erfasst. Dies diene der Verhinderung des Verkaufs an Personen mit bundesweitem Stadionverbot. Der Verein sei verpflichtet, entsprechend den diesbezüglichen Richtlinien des DFB zu handeln und dabei insbesondere den Verkauf von Eintrittskarten an Personen mit bundesweitem Stadionverbot zu unterlassen. Die erhobenen Daten seien inzwischen, konkret am Tag nach dem betreffenden Spiel, wieder gelöscht worden.

Gegen die Verfahrensweise in der ersten Verkaufsphase bestanden aus datenschutzrechtlicher Sicht keine Einwände. Soweit die interne Regelung besteht, dass wegen des beschränkten Kontingents pro Mitglied nur eine Karte verkauft werden soll, ist zu deren Umsetzung eine solche Registrierung ein geeignetes und erforderliches Mittel. Natürlich ist es geboten, dass diese Verkaufsliste wieder gelöscht wird, sobald diese erste Verkaufsphase abgeschlossen ist. Denn unabhängig davon, ob zu diesem Zeitpunkt bereits alle Karten verkauft sind oder aber die zweite, freie Verkaufsphase startet, besteht dann keine Notwendigkeit mehr, diese interne Beschränkung noch weiter zu überwachen bzw. aufrechtzuerhalten, zumal dies nach den Ausführungen des Vereins der einzige Zweck der diesbezüglichen Erhebung, Verarbeitung und Nutzung von Mitgliederdaten war.

Die in der zweiten Verkaufsphase erfolgende Erhebung, Verarbeitung und Nutzung der Daten von Nichtmitgliedern sollte nach den Angaben des Vereins einzig der Verhinderung des Kartenverkaufs an Personen mit bundesweitem Stadionverbot dienen. Für dieses sicherlich berechtigte Interesse war allerdings keine Speicherung von Namen, Anschrift und Geburtsdatum der Käufer von Eintrittskarten erforderlich. Ziel der Kontrolle war es ja gerade, den Kartenverkauf an Personen mit Stadionverbot zu verhindern. Dies konnte - wenn überhaupt (Eintrittskarten können auch weitergegeben werden.) - wirkungsvoll nur beim Kartenverkauf selbst, also durch sofortigen Abgleich mit der Liste der von den Stadionverboten Betroffenen erfolgen. Eine weitere Speicherung der Daten der Käufer war dafür nicht erforderlich, zumal auch dadurch nicht verhindert werden konnte, dass regulär erworbene Eintrittskarten durch andere Personen, insbesondere solche mit einem bundesweiten Stadionverbot, genutzt werden.

4.3.7.2 Fotodokumentation der Parzellen eines Kleingartenvereins

Ein Kleingartenverein hatte sämtliche Parzellen fotografisch erfasst. Die sich hiergegen gerichtete Eingabe eines Kleingärtners blieb ohne Erfolg. Die in der fotografischen Dokumentation zu sehende Datenerhebung war sowohl gemäß § 28 Abs. 1 Satz 1 Nr. 2 als auch Nr. 3 BDSG zulässig.

§ 28 Abs. 1 Satz 1 Nr. 2 erlaubt das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke, soweit dies zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Verarbeitung oder Nutzung überwiegt. Nach Auskunft des betroffenen Schrebervereins handelte es sich bei der Kleingartenanlage um eine öffentlich zugängliche Anlage, die Bestandteil eines Kleingartenparks ist. Zweck der Fotodokumentation sei die Nachweisführung (Gemeinnützigkeit) gegenüber der Stadt als Generalverpächterin. Zudem wurde mitgeteilt, dass die Fotodokumentation auch dem Zweck diene, das Inventarverzeichnis und die Chronik des Vereins zu ergänzen sowie in eventuell auftretenden Versicherungsfällen Nachweise zur vorhandenen Substanz führen zu können. Da auf den gefertigten Fotos auch keine Personen zu sehen sein sollten, waren entgegenstehende Interessen etwaiger Betroffener an dem Ausschluss der Verarbeitung oder Nutzung, die das Vereinsinteresse hätten überwiegen können, nicht ersichtlich.

Da die Gartenparzellen als Gegenstand der Fotodokumentation zudem insoweit öffentlich zugänglich waren, als dass die Aufnahmen ausschließlich von den frei zugänglichen Wegen der Kleingartenanlage angefertigt worden waren, war die Fotodokumentation auch nach § 28 Abs. 1 Satz 1 Nr. 3 BDSG zu rechtfertigen. Entgegenstehende überwiegende schutzwürdige Interessen der Kleingärtner waren auch insoweit nicht ersichtlich.

4.3.7.3 Herausgabe von Mitgliederlisten an Vereinsmitglieder

Einigen Mitgliedern einer als Verein organisierten Interessengemeinschaft von Personen mit einem im Vereinsnamen genannten Krankheitsbild war vom Wahlausschuss des Vereins eine Mitgliederliste vorenthalten worden, die sie für ein persönliches Kandidatenanschreiben aus Anlass der bevorstehenden Vorstandswahl erbeten hatten.

Nach der Rechtsprechung des BGH kann ein Vereinsmitglied nicht schon aufgrund seiner Mitgliedschaft die Kenntnis der Namen und Anschriften anderer Vereinsmitglieder beanspruchen. Vielmehr muss es, wenn es sich auf eine von seinem Mitgliedschaftsrecht abgeleitete Kenntnis berufen will, darlegen, ein berechtigtes Interesse an diesen Informationen zu haben, dem kein überwiegendes Interesse des Vereins oder berechtigte Belange der Vereinsmitglieder entgegenstehen (vgl. BGH, Beschluss vom 21. Juni 2010, Az. II ZR 219/09, Leitsatz 1 - in juris). Wie der BGH in derselben Entscheidung (BGH a. a. O., Rn. 6) ausführt, ist die Frage, unter welchen Voraussetzungen ein berechtigtes Interesse des einzelnen Vereinsmitglieds, Kenntnis von Namen und Anschriften der anderen Mitglieder zu erhalten, anzunehmen wäre, keiner abstrakt generellen

Klärung zugänglich, sondern allein aufgrund der konkreten Umstände des Einzelfalls zu beantworten:

Zunächst ist die Berechtigung des Interesses des Mitglieds an der Kenntnis der Daten in Ansehung der Vereinskultur und des Vereinszwecks zu bestimmen. Kennen sich die Mitglieder aufgrund der Größe des Vereins bereits mehrheitlich gegenseitig oder stellt die Pflege des Kontakts der Mitglieder untereinander einen wichtigen Bestandteil des Vereinszwecks dar, dann wäre die Kenntnis der Mitgliederliste schon im Rahmen des Vereinsverhältnisses als vertragsähnlichen Vertrauensverhältnisses nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG zulässig.

In größeren Vereinen, bei denen die wechselseitige Kenntnis der Identität des Einzelnen für die Teilnahme am Vereinsleben keine besondere Rolle spielt und persönliche Kontakte der Mitglieder untereinander eher bei Gelegenheit denn aus Anlass der Vereinstätigkeit bestehen sowie insbesondere dann, wenn die Kontaktpflege der Vereinsmitglieder untereinander zur Erreichung des Vereinszwecks nachrangig ist, bedarf es einer Abwägung des Interesses des einzelnen Vereinsmitgliedes an der Kenntnis der Mitgliederliste mit etwaigen entgegenstehenden schutzwürdigen Interessen anderer Vereinsmitglieder (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG).

Als unmittelbar vom Mitgliedschaftsrecht abgeleitetes berechtigtes Interesse anerkannt hat der BGH ausdrücklich den glaubhaften Wunsch nach Mitwirkung an der Willensbildung im Verein, also der satzungsmäßigen Wahrnehmung von vereinsrechtlichen Mitgliedschafts- und Teilhaberrechten (BGH a. a. O.). Dem Vereinsmitglied wäre also beispielsweise dann Zugang zur Mitgliederliste bzw. den zur Kontaktaufnahme notwendigen Daten zu gewähren, wenn es sich wegen einer Kandidatur, einer Satzungsänderung oder weil es sich - etwa wegen Kritik an der Vereins- oder Vorstandstätigkeit - mit einem Mitgliederbrief an andere Mitglieder wenden will, und dem kein überwiegendes Interesse des Vereins oder berechtigte Belange der Vereinsmitglieder entgegenstehen. Letzteres wäre etwa bei besonders sensiblen Vereinen, wie Lohnsteuerhilfevereinen oder Selbsthilfegruppen (z. B. „anonyme Alkoholiker“), anzunehmen.

Bei einer als Verein organisierten Interessengemeinschaft von Personen mit aus dem Vereinsnamen ersichtlichen Krankheitsfolgen, beinhaltet jedoch die Kenntnis der Mitgliedschaft zugleich die Kenntnis von einer entsprechenden Erkrankung, also eines besonderen personenbezogenen (Gesundheits-)Datums im Sinne des § 3 Abs. 9 BDSG, also eines Datums, hinsichtlich dessen an die Erlaubtheit seiner Verarbeitung besonders strenge Anforderungen zu stellen sind. Vor diesem Hintergrund ist die Weigerung des Wahlausschusses als berechtigt angesehen worden.

Allgemein ist Vereinen zu empfehlen, in ihrer Satzung den Umfang der Daten, welche Eingang in die Mitgliederliste finden sollen, im Einzelnen zu regeln und die Vereinsmitglieder bei Eintritt oder Satzungsänderung darauf hinzuweisen, dass ihre Daten bei hinreichender Darlegung eines berechtigten Interesses durch Vorstandsbeschluss anderen Mitgliedern gemäß der o. g. Grundsätze zugänglich gemacht werden können. Weiterhin ist es ratsam, die Mitglieder jeweils im Einzelfall darüber zu informieren, an wen welche Daten zu welchem Zweck weitergegeben werden. Zudem sollten Empfänger der Daten darauf hingewiesen werden, dass die Daten allein zu Vereinszwecken verwendet werden dürfen und eine Verwendung für andere (insbesondere kommerzielle und berufliche) Zwecke ebenso wenig zulässig ist, wie eine Weitergabe an außenstehende Dritte.

4.3.7.4 Listenmäßige Dokumentation ausgezahlter Ehrenamtspauschalen

Ein ehrenamtlich in einem Verein engagierter Bürger beklagte sich zu Recht darüber, dass für die Auszahlung von Ehrenamtspauschalen keine Einzelbelege mehr akzeptiert würden, sondern die Empfänger nunmehr den Erhalt der Auszahlung auf einer Liste quittieren müssten, aus der auch die Auszahlungen an andere Ehrenamtliche ersichtlich sei.

Der vom Projektträger geäußerten Auffassung, dass sich in der Auszahlungsliste keine relevanten personenbezogenen Daten befänden, war nicht zu folgen. Müssen sämtliche ehrenamtliche Mitarbeiter eines Projekts den Empfang der Aufwandsentschädigung auf einer Liste quittieren, können sie zur Kenntnis nehmen, in welcher Höhe ein anderer Mitarbeiter eine Aufwandsentschädigung erhalten hat. Dies ist insbesondere dann aufschlussreich, wenn die Aufwandsentschädigung in unterschiedlicher Höhe ausgezahlt wird. Auch das Argument, dass bei einer Einzelabrechnung unnötig viel Papier zusätzlich verwendet und für zehn Jahre aufbewahrt werden müsse, konnte diese Vorgehensweise nicht rechtfertigen.

Nichtsdestoweniger ist eine listenmäßige Dokumentation ausgezahlter Ehrenamtspauschalen - nicht zuletzt im Interesse des Umweltschutzes - dann aber als unproblematisch zu betrachten, wenn mittels geeigneter Schablonen die bereits erfolgten Auszahlungen an andere Mitglieder abgedeckt werden.

4.3.8 Energieversorgungsunternehmen

4.3.8.1 Erweiterte (elektronische) Verbrauchsmessung - Smart Meter

Neuerdings werden immer häufiger sogenannte „intelligente“ Stromzähler (auch „Smart Meter“ genannt) eingebaut, die nicht nur Gesamtverbrauchswerte eines Abrechnungs-

zeitraumes, sondern auch die Momentan-Verbrauchswerte zeitlich eng beieinander liegender Messpunkte erheben, speichern und dem Anschlussnutzer sichtbar machen können und darüber hinaus sogar diese Daten dem Stromversorger über ein Kommunikationsnetz kontinuierlich übermitteln können. Zunächst einmal sollen die Geräte dem Kunden die zeitgenaue Kontrolle seines Verbrauchs ermöglichen. Zusätzlich möchte die Stromwirtschaft diese Daten aber auch für eine Verbesserung des eigenen Netz- und Lastmanagements nutzen. Als Begründung für den Einsatz der neuen Messgeräte dient der Stromwirtschaft zudem die Einführung lastzeitvariabler oder tageszeitabhängiger Tarife.

Die Angabe über die an einem Haushaltsanschluss in einem bestimmten Zeitraum abgenommene, also verbrauchte, Strommenge ist ein personenbezogenes Datum zumindest betreffend die Person des Anschlussinhabers (Vertragspartners des Versorgungsunternehmens). Beim Ein-Personenhaushalt sind im Regelfall zumindest auch Rückschlüsse auf den Umfang und die Zeit der Nutzung der Wohnung (Tagesrhythmus) des Wohnungsinhabers möglich. Je enger die zeitlichen Messpunkte einer Verbrauchserhebung beieinander liegen, desto größer ist die Eignung der gewonnenen Daten, zusammengeführt zu einem Verbrauchsprofil die Lebensgewohnheiten einer Person oder der Gesamtheit der Haushaltsmitglieder wiederzuspiegeln. Die Einführung solcher erweiterten Stromverbrauchsmessgeräte führt dann, wenn die Daten an das Versorgungsunternehmen übermittelt werden, zu einem nicht unerheblichen Eingriff in das Recht des Anschlussinhabers auf informationelle Selbstbestimmung. Dies müsste noch mehr gelten, wenn Geräte dieser Art über den Stromverbrauch hinaus auch für den Verbrauch von Gas oder Wasser zum Einsatz kämen und die Möglichkeit der Zusammenführung dieser Daten entstünde. Eine Auswertung der durch diese Geräte gewonnenen Daten bis hin zu einem bestimmten Endgerätetypus (z. B. Waschmaschine) ist technisch möglich.

Obgleich der Einbau der neuartigen Geräte vom Stromkunden zu dulden ist (§ 21c Abs. 1 EnWG), darf - wie ich schon zur bisherigen Rechtslage (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG) hiesigen Versorgern gegenüber vertreten habe - die Belieferung mit Energie, also der Zugang zu einzelnen Tarifangeboten, auch bei geplanten lastzeitvariablen oder tageszeitabhängigen Stromtarifen, nicht von der Angabe personenbezogener Daten abhängig gemacht werden, die für die Rechnungslegung im jeweiligen Tarifmodell nicht zwingend erforderlich sind - dies hat der Gesetzgeber nunmehr im Sommer 2011 in § 21g Abs. 6 Satz 3 EnWG nochmals klargestellt. Auch bei lastzeitvariablen oder tageszeitabhängigen Stromtarifen muss der Versorger zu Abrechnungszwecken nur die Gesamtverbrauchswerte des Kunden innerhalb einer Last- und Tarifzeit, nicht jedoch den genauen Verbrauchszeitpunkt wissen. Die *haushaltsgenaue* und damit personenbezogene Kenntnis des momentanen Stromverbrauchs ist für das Netz- und Lastmana-

gement nicht erforderlich. Die Erreichung des Zwecks, dem Stromkunden seinen jeweiligen Verbrauch detailliert erkennbar zu machen, macht eben gerade kein Fernwirken bzw. Fernmessen durch den Stromlieferanten erforderlich, weil es - sei es auch mit anderen Endgeräten als jenen, die von der Stromwirtschaft bevorzugt werden - möglich ist, die Daten dem Kunden dort, wo sie entstehen, also in dessen Haushalt (etwa am Zähler selbst), zugänglich zu machen. In diesem Sinne hat der Gesetzgeber mit dem neuen § 21g Abs. 6 Satz 4 EnWG das klargestellt, was schon vorher meine dezidiert vertretene Rechtsauffassung gewesen ist, nämlich dass Fernwirken und Fernmessen durch den Stromlieferanten am sich beim Kunden befindenden Messgerät bei Stromverbrauchsmessgeräten nur dann stattfinden dürfen, wenn der Letztverbraucher zuvor über den Verwendungszweck sowie über Art, Umfang und Zeitraum der Übermittlung unterrichtet worden ist und in freier Entscheidung, also unabhängig vom Zugang zu einem Tarifmodell, in diese Übermittlung eingewilligt hat.

4.3.8.2 Geburtsdatum im Energieliefervertrag

Der Kunde eines Stromversorgers weigerte sich, diesem sein Geburtsdatum anzugeben, und war allenfalls bereit, sein Geburtsjahr mitzuteilen. Der Stromversorger hatte ihm dazu nur allgemein mitgeteilt, dass die dem Vertragsverhältnis zugrunde liegenden personenbezogenen Daten, mithin auch das Geburtsdatum, zur Vertragsdurchführung benötigt würden.

Tatsächlich ergibt sich die Zulässigkeit der Erhebung und Speicherung des Geburtsdatums aus § 2 Abs. 3 Satz 3 Nr. 1 StromGVV; § 2 Abs. 3 Satz 4 stellt darüber hinaus klar, dass der Kunde verpflichtet ist, das Geburtsdatum auf Verlangen mitzuteilen. Wäre durch den Stromversorger insoweit gleich auf diese Rechtsgrundlage verwiesen worden, hätte sich die Aufsichtsbehörde gar nicht erst mit dieser Angelegenheit befassen müssen.

Im Bereich der Gasversorgung existiert im Übrigen eine analoge Regelung (§ 2 Abs. 3 Satz 3 Nr. 1, Satz 4 GasGVV).

4.3.8.3 Zählerstandsmitteilung per Postkarte

Die Kundin eines Energieversorgers fragte nach, ob es datenschutzrechtlich gestattet sei, den Kunden die turnusmäßige Mitteilung ihrer Zählerstände durch Übersendung einer offenen Antwortpostkarte abzuverlangen.

Die Feststellung der Höhe der in einem bestimmten Zeitraum verbrauchten Energie einer Verbrauchsstelle einer natürlichen Person ist eine Erhebung eines personenbezogenen Datums im Sinne des § 3 Abs. 1 BDSG, da der Verbrauch von Energie grund-

sätzlich geeignet ist, Auskunft über persönliche und sachliche Lebensverhältnisse des Verbrauchers zu geben.

Zur Abrechnung und der damit einhergehenden Erhebung des Energieverbrauchs sind die Lieferanten einerseits gemäß § 40 Abs. 2 EnWG gesetzlich verpflichtet, andererseits ist die Erhebung, Verarbeitung und Nutzung der Daten auch als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, da sie für die Durchführung eines rechtsgeschäftlichen Schuldverhältnisses, hier des Energieliefervertrages, erforderlich sind (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG).

Bei einer vom Verbraucher selbst ausgefüllten Ablese- bzw. Antwortpostkarte handelt es sich jedoch jenseits der Erhebungs- und Verarbeitungsbefugnis des Versorgers um eine eigenverantwortliche Datenweitergabe durch den Betroffenen selbst. Sie mag zwar auf eine Anforderung des Energielieferanten zurückgehen und auch seinem Begehren folgen, hierbei eine bestimmte, vorgefertigte, offene und in der Regel unentgeltliche Antwortkarte zu benutzen. Dessen ungeachtet ist der Betroffene aber in solchen Fällen nicht verpflichtet, diese auch tatsächlich zu verwenden; insbesondere ist es ihm unbenommen, seine Antwort in einem verschlossenen Umschlag zurückzusenden oder falls die Möglichkeit besteht, über das Internet zu melden. Insoweit ist ihm der Schutz seiner Daten auch nicht entzogen. Zudem hindern anfallende Portokosten einer Kuvertsendung den Kunden jedenfalls nicht ernstlich, das Niveau des Schutzes seiner personenbezogenen Daten vor der unbefugten Einsichtnahme durch Dritte selbst zu bestimmen. Ob die Portokosten dem Kunden oder dem Energielieferanten obliegen, berührt daher vorrangig das sonstige vertragliche, nicht aber das datenschutzrechtliche Verhältnis der Beteiligten.

Ein Verstoß des Energielieferanten gegen seine Pflicht als erhebende Stelle, ausreichende technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten zu ergreifen (§ 9 BDSG), bestünde nur dann, wenn eine Übermittlung durch den Betroffenen im verschlossenen Umschlag grundsätzlich ausgeschlossen ist, weil diese nicht bearbeitet wird oder werden kann. Eine solche Einengung des Betroffenen in der Wahl seines Datenschutzniveaus bei der Weitergabe personenbezogener Daten wäre in der Tat bedenklich. Dies war dem Sachverhalt aber nicht zu entnehmen. Angesichts der vergleichsweise sehr geringen Sensibilität der hier in Rede stehenden Daten erscheint eine turnusmäßige Mitteilung von Zählerständen mittels Antwortpostkarte, selbst wenn Vertragspartner und deren Kundennummer auf dieser ebenso vermerkt sind, nicht grundlegend bedenklich. Dies gilt umso mehr, als eine Übersendung mittels Postkarte auch keine völlig ungeschützte Form der Weitergabe ist, sondern stets das Postgeheimnis gilt (vgl. Art. 10 Abs. 1 GG, § 39 Abs. 1 PostG) und ein Verstoß gegen selbiges in § 206 StGB strafbewehrt ist.

4.3.8.4 Kundenportal eines Stromlieferanten im Internet

Der Wettbewerb auf dem Strommarkt hat bekanntlich verschiedene neue Anbieter auf den Plan gerufen, die den gestandenen Anbietern über Niedrigpreise entsprechende Marktanteile abnehmen wollen. Die Kommunikation mit den Kunden erfolgt dabei häufig, manchmal ausschließlich, über das Internet; dies hilft Kosten zu senken und ist natürlich auch Folge und Ausdruck der bundesweiten Vertriebstätigkeit. Leider geht dies gelegentlich auch zu Lasten des Datenschutzes, indem die datenschutzrechtlichen Vorgaben nur ungenügend beachtet, insbesondere die diesbezüglich erforderlichen Kundenportale in funktioneller und rechtlicher Hinsicht völlig unausgereift zum Einsatz gebracht werden, und im Ergebnis zu Verärgerung bei den Kunden und viel Arbeit bei den Aufsichtsbehörden führen:

Einem Stromkunden war per unverschlüsselter E-Mail eine Aufforderung zur Eingabe seines aktuellen Zählerstandes über das Kundenportal des Stromanbieters zugesandt worden, in der u. a. seine Kunden- und seine Zählernummer enthalten und somit für Dritte einsehbar waren. Die geforderte Zählerstandsmitteilung war aber nur nach vorheriger Registrierung im Kundenportal des Stromanbieters möglich und erforderte in einem ersten Schritt die Eingabe eben dieser zuvor per E-Mail mitgeteilten Daten.

Die geschilderte Vorgehensweise widersprach damit 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, und eröffnete zugleich eine Missbrauchsmöglichkeit, indem sich Dritte mit diesen Daten im Namen des Betroffenen zu diesem Online-Service hätten anmelden können.

Auch das daraufhin von dem betreffenden Stromanbieter neugestaltete Anmeldeverfahren wurde den datenschutzrechtlichen Anforderungen noch nicht in vollem Umfang gerecht. Zwar sollte den Kunden die für die Anmeldung am Kundenportal erforderliche Kundennummer (Benutzername) nun im Rahmen der schriftlichen Auftragsbestätigung mitgeteilt werden, das für die Anmeldung darüber hinaus erforderliche Initialpasswort sollte aber wiederum per E-Mail an die Kunden versandt werden. Man mag einwenden können, dass eine Missbrauchsgefahr nicht besteht, solange nicht auch die (auf dem Postweg an den Kunden bekanntgegebene) Kundennummer bekannt ist. Darauf kommt es nach dem Wortlaut der o. g. Vorschrift jedoch gar nicht an. Entscheidend ist, dass auf diese Weise nicht gewährleistet ist, dass das Kennwort nicht durch Unbefugte, insbesondere an der Übertragung Beteiligte, gelesen, kopiert, verändert oder entfernt werden kann. Abgesehen davon stellte das neue Verfahren noch nicht einmal sicher, dass dieses Initialkennwort bei der ersten Anmeldung zwingend durch den Nutzer

geändert werden muss. Da für das Kundenportal darüber hinaus auch keine SSL-Verschlüsselung vorgesehen war, genügte es im Übrigen auch nicht den Vorgaben des § 13 Abs. 4 Satz 1 Nr. 3 TMG, wonach der Diensteanbieter durch technische und organisatorische Vorkehrungen sicherzustellen hat, dass der Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann.

Erst im dritten Versuch hat der Stromanbieter dann in seinem Kundenportal eine Verfahrensweise umsetzen können, die die aufgezeigten datenschutzrechtlichen Mängel beseitigte. Die (initialen) Logindaten (Benutzername, Passwort) werden jetzt auf schriftlichem Wege mitgeteilt; das Initialpasswort ist bei erstmaliger Anmeldung an dem nun SSL-verschlüsselten Kundenportal zwingend zu ändern.

4.3.8.5 Veröffentlichung der Anschriften von Solaranlagenbesitzern

Der Eigentümer einer Solaranlage beschwerte sich darüber, dass auf der Internetseite eines Energieversorgers konkrete Postanschriften von Solaranlagenbesitzern sowie deren Anlagenleistung und die jeweiligen Vergütungszahlungen veröffentlicht worden sind.

Die datenschutzrechtliche Überprüfung ergab, dass diese Veröffentlichung auf einer wirksamen Rechtsgrundlage beruhte. So sieht § 52 EEG vor, dass bestimmte, dort im Einzelnen genannte Daten von Netzbetreibern und Elektrizitätsversorgungsunternehmen auf deren Internetseiten unverzüglich nach dem 30. September eines Jahres zu veröffentlichen und bis zum Ablauf des Folgejahres vorzuhalten sind. Zu diesen zu veröffentlichten Daten gehört gemäß § 46 Abs. 2 EEG insbesondere auch der Standort der Anlage, d. h. der Ort, an dem sich die Anlage befindet. Da dieser insbesondere durch die genaue Angabe der Adresse bzw. des Flurstücks, des Ortsnamens und der Postleitzahl gekennzeichnet wird, war die Veröffentlichung der Anschrift zulässig.

4.3.9 Handels- und Wirtschaftsauskunfteien / Inkassobüros

4.3.9.1 Umfang der Auskunftspflicht gegenüber Betroffenen

Mit den zum 1. April 2010 in Kraft getretenen BDSG-Änderungen ist u. a. das Auskunftsrecht gegenüber Auskunfteien für Betroffene erweitert worden. Über das bis dahin bestehende Auskunftsrecht zu

- den zur eigenen Person gespeicherten Daten,
- Herkunft und Empfänger der Daten, soweit nicht das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt, sowie zum

- Zweck der Speicherung

hinaus, ist seitdem auch Auskunft zu erteilen über Daten, die

- gegenwärtig noch keinen Personenbezug aufweisen, bei denen ein solcher aber im Zusammenhang mit der Auskunftserteilung von der verantwortlichen Stelle hergestellt werden soll,
- die verantwortliche Stelle nicht speichert, aber zum Zweck der Auskunftserteilung nutzt.

Überdies kann nun jeder Auskunft über die zu seiner Person berechneten und ggf. bereits übermittelten Scorewerte (Wahrscheinlichkeitswerte für ein bestimmtes zukünftiges Zahlungsverhalten) verlangen. Insbesondere ist dabei Auskunft zu erteilen über

- die innerhalb der letzten zwölf Monate übermittelten Wahrscheinlichkeitswerte,
- die Namen und letztbekannten Anschriften der Empfänger der Wahrscheinlichkeitswerte,
- den aktuellen Wahrscheinlichkeitswert und die zur Berechnung der Wahrscheinlichkeitswerte genutzten Datenarten sowie
- das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte.

Sowohl das Zustandekommen als auch die Bedeutung des Wahrscheinlichkeitswertes sind dabei einzelfallbezogen und nachvollziehbar in einer allgemein verständlichen Form darzulegen.

Insbesondere die Regelung, dass Betroffene auch von Stellen, die personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung speichern, einmal je Kalenderjahr eine unentgeltliche Auskunft in Textform verlangen können (§ 34 Abs. 8 BDSG), hat offensichtlich zu einer Häufung solcher Auskunftsverlangen bei Handels- und Wirtschaftsauskunfteien geführt. Die Aufsichtsbehörde hatte sich daher mit der Frage zu befassen, wie mit solchen Auskunftsverlangen zu verfahren ist, wenn keine Daten zu dem Betroffenen vorhanden sind, die Anfrage also praktisch ins Blaue hineingestellt worden ist:

§ 34 Abs. 1 Satz 1 Nr. 1 BDSG beschränkt die Auskunftspflicht auf die zur Person des Betroffenen gespeicherten Daten. Im Umkehrschluss bedeutet dies, dass immer dann, wenn keine personenbezogenen Daten des Auskunftsersuchenden gespeichert sind, auch keine Auskunftspflicht besteht, d. h. es muss somit in diesem Fall auch keine Negativauskunft (Mitteilung der Nichtspeicherung) erteilt werden.

Dies ergibt sich im Übrigen auch aus § 27 Abs. 1 Satz 1 Nr. 1 BDSG, wonach die Vorschriften des Dritten Abschnittes des Bundesdatenschutzgesetzes, hier also § 34 BDSG, auf nicht-öffentliche Stellen nur dann anwendbar sind, wenn personenbezogene Daten (tatsächlich) verarbeitet (gespeichert), genutzt oder dafür erhoben werden.

Gleichwohl könnte die verantwortliche Stelle zur Vermeidung weiterer Auseinandersetzungen mit den Betroffenen in Erwägung ziehen, diese kurz über die Nichtspeicherung zu informieren. Dies muss dann aber mangels Anwendbarkeit des § 34 BDSG nicht notwendigerweise in Textform (vgl. § 34 Abs. 6 BDSG) - das Schriftformerfordernis besteht seit dem 1. April 2010 nicht mehr, d. h. ein Auskunftsverlangen kann ohnehin beispielsweise auch per E-Mail erledigt werden -, sondern kann ggf. auch telefonisch erfolgen.

4.3.9.2 Auskunftsrecht: Identifikation Betroffener mittels Ausweiskopie

Auskunfteien verlangen zunehmend von Betroffenen, dass diese im Rahmen eines Auskunftsverlangens nach § 34 BDSG eine Personalausweiskopie als Identitätsnachweis beibringen.

Da das Auskunftsrecht nach § 34 BDSG ausschließlich dem Betroffenen zusteht, hat sich die verantwortliche Stelle vor Erteilung einer Auskunft grundsätzlich der Identität des Auskunftsersuchenden zu vergewissern. Diese Verpflichtung folgt aus dem sanktionsbewehrten Verbot, Daten unbefugt zu übermitteln (Ordnungswidrigkeit nach § 43 Abs. 2 Nr. 1 BDSG). Aus Datenschutzsicht ist somit zur Vermeidung von missbräuchlichen Abrufen von Auskünften durch Nichtberechtigte eine eindeutige Identifizierung des Auskunftsersuchenden zulässig und sogar geboten.

Grundsätzlich ist der Personalausweis auch im nicht-öffentlichen Bereich als Identitätsnachweis und Legitimationspapier verwendbar (vgl. § 20 Abs. 1 PAuswG). Soweit - was der Regelfall sein dürfte - der Betroffene sein Auskunftsrecht dabei nicht persönlich bei der verantwortlichen Stelle geltend machen kann, bleibt praktisch nur der Weg über eine Ausweiskopie. Allerdings darf die Anforderung einer Ausweiskopie nicht zum Regelfall werden, sondern muss gemäß dem Erforderlichkeitsprinzip auf solche Einzelfälle beschränkt bleiben, bei denen Zweifel an der Identität der auskunftsersuchenden Person bestehen, etwa weil gespeicherte Daten nicht eindeutig dieser Person zugeordnet werden können. Dies wird beispielsweise dann der Fall sein, wenn zu einem Namen mehrere Anschriften gespeichert sind, was seine Ursache in einem Umzug, in mehreren Wohnsitzen, in der Namensgleichheit mit anderen Personen oder eben auch in einer missbräuchlichen Anfrage unter falschem Namen haben kann. Eine generelle Obliegenheit des Betroffenen zum Nachweis seiner Legitimation hätte einer ausdrück-

lichen gesetzlichen Regelung bedurft, wie das beispielsweise in § 4 Abs. 4 GwG der Fall ist.

Die Forderung nach Vorlage einer Ausweiskopie muss demnach auf strittige Fälle einer nicht eindeutigen Identifizierbarkeit des Antragstellers beschränkt bleiben. Nicht erforderlich ist die Vorlage einer Ausweiskopie beispielsweise auch dann, wenn ein Betroffener sich bereits an die Aufsichtsbehörde gewandt hat und diese daher insoweit die Identität des Antragstellers bestätigen kann.

Die Grundsätze der Datensparsamkeit und Erforderlichkeit erlauben es dem Betroffenen im Übrigen, Daten, die nicht zu Identifizierungszwecken benötigt werden, auf der Kopie zu schwärzen. Dies gilt insbesondere für sämtliche auf dem Ausweis befindlichen Nummern. Die Betroffenen sind von der verantwortlichen Stelle auf diese Möglichkeit hinzuweisen.

Das BMI hatte noch im Oktober 2010 auf der Grundlage durchaus nachvollziehbarer sicherheits- und datenschutzrechtlicher Erwägungen die Auffassung vertreten, dass die Vervielfältigung von Pässen und Personalausweisen durch Fotokopieren, Scannen oder sonstige Ablichtung grundsätzlich unzulässig sei. Allerdings ließ sich das aufgestellte ausnahmslose Kopierverbot weder eindeutig aus dem Gesetz - es fehlt eine ausdrückliche gesetzliche Regelung zum Kopierverbot - herleiten, noch war es in allen Fällen mit den praktischen Notwendigkeiten vereinbar und führte so im Einzelfall beispielsweise zu erheblichen Schwierigkeiten insbesondere bei der praktischen Umsetzung des Auskunftsrechts der Betroffenen nach § 34 BDSG. Die diesbezügliche Intervention der Datenschutzaufsichtsbehörden hat dann aber zu einer Neubewertung des Sachverhalts durch das BMI geführt. Danach ist jetzt auch nach Auffassung des BMI die Anfertigung von Ausweiskopien im Einzelfall zulässig, wenn

- die Erstellung einer Kopie erforderlich und insbesondere ein Vermerk, dass der Personalausweis vorgelegen hat, nicht ausreichend bzw. nicht möglich ist, weil der Betroffene eben nicht persönlich vorsprechen konnte,
- die Kopie ausschließlich zu Identifikationszwecken verwendet wird,
- die Kopie als solche erkennbar ist,
- nicht für die Identifikation erforderliche Daten, hier insbesondere die auf dem Ausweis enthaltenen Zugangs- und Seriennummern, geschwärzt werden können und die Betroffenen darauf hingewiesen werden,
- die Kopie unverzüglich vernichtet wird, sobald der damit verfolgte Zweck erreicht ist und
- keine automatisierte Speicherung der Ausweisdaten erfolgt (unzulässig nach § 20 Abs. 2 PAuswG).

4.3.9.3 Datenempfänger als Geschäftsgeheimnis?

Eine Petentin hatte mitgeteilt, dass eine Auskunftei auf ihr Verlangen nicht mitgeteilt habe, an wen Daten über sie übermittelt worden sind. Als Begründung sei angegeben worden, dass das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber ihrem Informationsinteresse als Betroffene überwiege.

Nach § 34 Abs. 1 Satz 1 Nr. 2 BDSG ist Betroffenen Auskunft über den Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben worden sind, zu erteilen. Die Auskunft über die Empfänger kann allerdings verweigert werden, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt (§ 34 Abs. 1 Satz 4 BDSG).

Die Auskunftei hatte sich in diesem Fall aufgrund einer vertraglichen Diskretionsverpflichtung gegenüber ihren Mitgliedern (Datenempfänger) daran gehindert gesehen, der Betroffenen mitzuteilen, wer eine Auskunft zu ihrer Person angefordert und auch erhalten hatte.

Eine vertragliche Verpflichtung zur Diskretion zwischen der Auskunftei und ihren Geschäftspartnern reicht jedoch nicht aus, um sich bei Auskunftsersuchen Betroffener generell auf ein das Informationsinteresse des Betroffenen überwiegendes Interesse an der Wahrung des Geschäftsgeheimnisses zu berufen. Es ist vielmehr eine einzelfallbezogene Abwägung zwischen den Interessen der verantwortlichen Stelle und des Betroffenen vorzunehmen. Bei einer solchen Interessenabwägung sind nur wenige Ausnahmefälle vorstellbar, in denen das Geschäftsgeheimnis der Auskunftei im Interesse des Auskunfteikunden eine Nennung des Auskunftsempfängers nicht zulässt. Dies wäre beispielsweise der Fall, wenn ein Verwandter des Betroffenen oder ein in unmittelbarer Nachbarschaft des Betroffenen ansässiger Handwerker die Anfrage gestellt hat. Gleiches gilt, wenn Anhaltspunkte dafür bestehen, dass der Auskunftsempfänger die Anfrage nicht stellen würde, wenn er damit rechnen müsste, dass es bei diesbezüglicher Kenntnis des Betroffenen zu keiner Geschäftsbeziehung kommen würde. Die Grenze ist also dort zu ziehen, wo die Bekanntgabe des Auskunftsempfängers die Geschäftsbeziehung nachhaltig stören oder gar zu deren Abbruch führen würde (Zu den weiteren Fallkonstellationen, in denen eine Berufung auf das Geschäftsgeheimnis nicht zulässig ist, vgl. 2. TB - Pkt. 4.3.8!).

Im vorliegenden Fall hat es sich bei dem Auskunftsempfänger um ein bundesweit tätiges Unternehmen gehandelt; besondere Konfliktlagen im oben genannten Sinne waren nicht zu erwarten. Es schien sich um eine Anfrage im Vorfeld der Lieferung von Baustoffen zu handeln. Bei derartigen Geschäftsbeziehungen sind Bonitätsabfragen durch-

aus üblich und daher auch entsprechend zu erwarten. Ein besonderes Interesse des Auskunftsempfängers, die Tatsache seiner Anfrage dem Betroffenen nicht zu offenbaren, war nicht zu erkennen. Zudem war zu berücksichtigen, dass es sich bei der Petentin als Betroffene um eine natürliche Person handelte, deren - als Ausfluss des Rechts auf informationelle Selbstbestimmung - grundrechtlich geschütztes Informationsinteresse regelmäßig höher zu bewerten ist als das einer juristischen Person oder einer Gesellschaft.

Der Petentin war somit mitzuteilen, wem die Auskunftei Daten zu ihrer Person übermittelt hatte.

4.3.9.4 Inkasso von Bußgeldern aus dem EU-Ausland

Zur Ahndung eines durch einen deutschen Staatsangehörigen begangenen Verstoßes gegen die italienische Straßenverkehrsordnung war von der italienischen Polizeibehörde ein in Italien ansässiges Inkassounternehmen mit der Geltendmachung und Eintreibung der diesbezüglichen Geldstrafe beauftragt worden. Das Inkassounternehmen hatte den Betroffenen zunächst (in deutscher Sprache) zur Zahlung einer reduzierten Geldstrafe aufgefordert (ähnlich dem deutschen Verwarnungsverfahren). Nachdem dieser keine entsprechende Zahlung geleistet hatte, erfolgte im nächsten Schritt die förmliche Zustellung eines Protokollbescheides über ein verwaltungsrechtliches Strafgeld der italienischen Polizeibehörde. Von der Möglichkeit gegen diesen Bescheid innerhalb von 60 Tagen Einspruch einzulegen, hatte der Betroffene keinen Gebrauch gemacht, so dass der Protokollbescheid schließlich (mit einer erhöhten Summe) rechtskräftig und somit vollstreckbar geworden ist.

Nachdem auch die darauffolgende letztmalige Zahlungsaufforderung des italienischen Inkassounternehmens unbeantwortet geblieben war, hat dieses dann ein Inkassounternehmen in Deutschland mit dem weiteren Inkasso des Strafgeldes beauftragt. Nachdem dieses mit weiteren Zahlungsaufforderungen an den Betroffenen herangetreten war, stellte sich vor dem Hintergrund, dass es zu diesem Zeitpunkt noch nicht möglich war, Strafgelder italienischer Behörden in Deutschland im Wege der Vollstreckung beizutreiben, die Frage nach der Zulässigkeit der diesbezüglichen Verarbeitung und Nutzung der Daten des Betroffenen durch das deutsche Inkassounternehmen.

Als Befugnisnorm konnte vorliegend auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG zurückgegriffen werden. Danach ist eine Verarbeitung und Nutzung personenbezogener Daten zulässig, soweit dies zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Verarbeitung oder Nutzung überwiegt.

Auch wenn eine Durchsetzung der Forderung im Rahmen der Vollstreckung innerhalb Deutschlands zu diesem Zeitpunkt noch nicht möglich war, hat es sich doch um ein nach italienischem Recht rechtskräftiges vollstreckbares Strafgeld gehandelt. Insoweit war ein berechtigtes Interesse des Inkassobüros, dem der weitere Forderungseinzug übertragen worden war, zu bejahen. Ein Grund zu der Annahme, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Verarbeitung oder Nutzung überwiegen könnte, war nicht ersichtlich, insbesondere hatte dieser die Rechtmäßigkeit der Forderung weder gegenüber der italienischen Behörde noch gegenüber den eingeschalteten Inkassobüros bestritten.

Ergänzend sei in diesem Zusammenhang noch auf die inzwischen geänderte Rechtslage hingewiesen: Am 28. Oktober 2010 ist das „Gesetz zur Umsetzung des Rahmenbeschlusses 2005/214/JI des Rates vom 24. Februar 2005 über die Anwendung des Grundsatzes der gegenseitigen Anerkennung von Geldstrafen und Geldbußen“ in Kraft getreten. Damit sind nunmehr auch in Deutschland rechtskräftige Buß- oder Strafgeldbescheide aus dem gesamten EU-Ausland ab einem Betrag von 70,00 € vollstreckbar.

4.3.10 Markt- und Meinungsforschung; wissenschaftliche Forschung

4.3.10.1 Telefonumfragen

Inhaber von Telefonanschlüssen fühlten sich durch Anrufe eines Markt- und Meinungsforschungsunternehmens belästigt und forderten daher die Aufsichtsbehörde auf, derartige Anrufe zu unterbinden und darüber hinaus aufzuklären, wie das Unternehmen an ihre in keinen Telefonverzeichnissen enthaltenen Rufnummern gelangt war.

Die durch das Markt- und Meinungsforschungsunternehmen genutzten Telefonnummern sind mit dem RLD-Verfahren (engl.: Randomized Last Digit = zufällige letzte Ziffer), einer wissenschaftlich anerkannten Form der Stichprobenziehung, generiert worden. Bei diesem Verfahren werden aus Nummernblöcken der Regulierungsbehörde (vergebene Rufnummernbereiche) die so genannten Stammnummern entnommen und durch einen automatisierten Zufallsprozess mit beliebigen Endziffern ergänzt. Auf diese Weise wird gewährleistet, dass die Stichprobe methodisch einwandfrei ist und die Umfrageergebnisse ausreichend repräsentativ sind. In der Natur des Verfahrens liegt es, dass dabei natürlich auch Rufnummern erzeugt und angewählt werden, die in keinen Telefonverzeichnissen enthalten sind.

Ob bzw. ab welchem Zeitpunkt bei solcherart generierten Anrufen der Anwendungsbereich des Bundesdatenschutzgesetzes überhaupt eröffnet ist, hängt davon ab, ob das Markt- und Meinungsforschungsunternehmen eine Telefonnummer - etwa aufgrund der Tatsache, dass die betreffende Person im Telefonbuch eingetragen ist oder weil sie sich

nachträglich selbst als Rufnummerninhaber identifiziert hat - überhaupt einer natürlichen Person zuordnen kann. Soweit der Angerufene geltend macht, nicht in Telefonverzeichnissen enthalten zu sein und sich auch nicht selbst identifiziert zu haben, ist der Anwendungsbereich des Bundesdatenschutzgesetzes nicht eröffnet, mithin auch keine Kontrollzuständigkeit der Aufsichtsbehörde nach § 38 BDSG gegeben, denn für das Markt- und Meinungsforschungsunternehmen stellt eine so generierte Rufnummer mangels (aus ihrer Sicht) Bestimmbarkeit des Rufnummerninhabers kein personenbezogenes Datum dar.

Unabhängig davon haben Betroffene jedoch die Möglichkeit, für die Zukunft derartige Anrufe eines konkreten Umfrageinstituts zu unterbinden, indem sie ihre Telefonnummer dort auf die Sperrliste setzen lassen. Seriöse Markt- und Meinungsforschungsunternehmen bieten eine solche Möglichkeit an und setzen diese auch entsprechend um. Voraussetzung ist aber, dass Betroffene diese Forderung selbst (dies ist nicht etwa Aufgabe der Aufsichtsbehörde) deutlich gegenüber dem jeweiligen Institut zum Ausdruck bringen und dabei natürlich auch die Telefonnummern benennen, für die dies gelten soll. Dabei sollten weitere ggf. auf den gleichen Anschluss geschaltene Rufnummern bzw. die Mobiltelefonen ggf. zugeordneten Homezone-Nummern nicht vergessen werden, andernfalls kann eine erneute Kontaktierung auf einer der ggf. vorhandenen anderen Rufnummern natürlich nicht ausgeschlossen werden.

Die Anwendbarkeit des Bundesdatenschutzgesetzes vorausgesetzt wären Anrufe zu Marktforschungszwecken im Übrigen nur dann von vornherein - also bevor bekannt wird, dass der Betroffene solche Anrufe ablehnt - als unzulässige Nutzung im Sinne des Bundesdatenschutzgesetzes zu betrachten, wenn sich aus anderen Rechtsvorschriften eindeutig die Rechtswidrigkeit solcher Anrufe ergäbe (Ergebnis der in § 30a Abs. 1 Satz 1 BDSG vorgeschriebenen Interessenabwägung). Dies ist aber derzeit nicht der Fall. Während etwa die Amtsgerichte in Frankfurt (Urt. v. 8. Januar 2007 - 32 C 1115/06) oder Hamburg-St. Georg (Urt. v. 27. Oktober 2005 - 918 C 413/05) entschieden haben, dass derartige Anrufe - jedenfalls solange der Angerufene dem Anrufer gegenüber noch nicht seinen entgegenstehenden Willen zum Ausdruck gebracht hat - zulässig sind und noch keine rechtswidrige Verletzung des allgemeinen Persönlichkeitsrechts darstellen, gehen das Amtsgericht Schöneberg (Urt. v. 23. Mai 2006 - 4 C 218/05 oder das Landgericht Hamburg (Urt. vom 30. Juni 2006 - 309 S 276/05, hier allerdings mit der Einschränkung, dass der Anruf im Auftrag eines anderen Unternehmens durchgeführt wird und mittelbar der Absatzförderung dient), vom Gegenteil aus.

4.3.10.2 Erfassung von Gesundheitsdaten in einer Basisbefragung

Auf einem Internetportal war interessierten Personen die Teilnahme an Online-Umfragen angeboten worden. Hierzu war es zunächst erforderlich, dass sich diese Personen registrieren, d. h. ein Benutzerkonto einrichten, und im Rahmen einer so genannten Basisbefragung weitere Auskünfte über sich erteilen. Anschließend sollten sie per E-Mail zu weiteren, ihrem aus den Ergebnissen der Basisbefragung erstellten Profil entsprechenden Online-Umfragen eingeladen werden. Im Rahmen der Basisbefragung sind auch Gesundheitsdaten *(„Unter welchen der folgenden Krankheiten leiden Sie?“)* zu den Panel-Teilnehmern erhoben worden.

Eine solche Datenerhebung war rechtswidrig.

Die Zulässigkeit der geschäftsmäßigen Datenerhebung und -speicherung für Zwecke der Markt- und Meinungsforschung bestimmt sich nach § 30a BDSG. Abs. 1 Satz 2 dieser Vorschrift, wonach Gesundheitsdaten nur für ein bestimmtes Forschungsvorhaben erhoben, verarbeitet oder genutzt werden dürfen, war für die Basisbefragung nicht einschlägig, da es sich dabei nicht um ein konkretes Forschungsvorhaben gehandelt hatte. Stattdessen war damit lediglich die Absicht verfolgt worden, möglichst viele Informationen über die Panel-Teilnehmer (Probandenstammdaten) zu sammeln, um auf dieser Basis dann für konkrete Umfrageprojekte den zur Befragung einzuladenden Teilnehmerkreis gezielt auswählen zu können.

Gemäß § 30a Abs. 5 BDSG kamen daher im Weiteren die Vorschriften des § 28 Abs. 6 bis 9 BDSG zur Anwendung. Da aber keiner der dort aufgeführten Erlaubnistatbestände erfüllt war, verblieb nach § 28 Abs. 6 BDSG nur eine Einwilligung der Betroffenen gemäß § 4a BDSG. Für diese wiederum ist jedoch die Schriftform vorgeschrieben (§ 4a Satz 3 BDSG), wobei zwar nach § 126 Abs. 3 BGB auch die elektronische Form nicht ausgeschlossen ist, diese allerdings eine qualifizierte elektronische Signatur nach dem Signaturgesetz voraussetzt (§ 126a Abs. 1 BGB). Da eine wirksame Einwilligung demnach nicht erteilt worden war, ist die Abfrage von Gesundheitsdaten in der Basisbefragung rechtswidrig gewesen.

Der anschließende Versuch der verantwortlichen Stelle, die Angelegenheit durch den in die Basisbefragung aufzunehmenden Hinweis auf eine später geplante Umfrage, in der auch Gesundheitsdaten von Bedeutung sein könnten, zu bereinigen, war ebenso abzulehnen. Eine Abfrage von Gesundheitsdaten im Hinblick auf eine eventuelle, zum Zeitpunkt der Abfrage keinesfalls feststehende Teilnahme an einer solchen Studie zu einem späteren Zeitpunkt *(„Haben Sie prinzipiell Interesse, an dieser Studie mitzuwirken?“)* ist ohne wirksame Einwilligung (s. o.) gleichfalls unzulässig, zumal die abgefragten

Daten auch weiterhin in den Probandenstammdaten und damit völlig losgelöst von der angekündigten Studie gespeichert werden sollten. Es war kein Grund ersichtlich, weshalb sich die verantwortliche Stelle in der Basisbefragung nicht auf die Abfrage dieses prinzipiellen Teilnahmeinteresses beschränken und die Abfrage der Gesundheitsdaten dann in die Umfrage im Rahmen der angekündigten Studie integrieren können sollte.

4.3.10.3 Veröffentlichung personenbezogener Daten in einer zeitgeschichtlichen Abhandlung zum Wissenschaftsbetrieb

Zu dem mir vom Verfasser vorgelegten Entwurf eines Aufsatzes, in dem es um Aktivitäten im Wissenschaftsbetrieb aus der Zeit vor der Revolution von 1989/1990 in der DDR ging und in dem die handwerklichen Leistungen sowie die Tatsache der politischen Indienstnahme sowie des Sich-selbst-in-Dienst-nehmen-Lassens behandelt werden sollten, habe ich folgende datenschutzrechtliche Beurteilung abgegeben:

(1) Zuständig war ich insoweit, als der Verfasser mittels automatisierter Datei (Text-Datei) bzw. Einsatz von Datenverarbeitungsanlagen (vermutlich PC), also im Anwendungsbereich des dritten Abschnittes des Bundesdatenschutzgesetzes (§ 27 Abs. 1 Satz 1 BDSG), eine Veröffentlichung in Zeitschriften-Form (vielleicht auch zusätzlich in elektronischer Form) veranlassen (herbeiführen) wollte, in der personenbezogene Daten enthalten sein würde, also datenschutzrechtlich gesprochen eine Verarbeitung personenbezogener Daten in Gestalt einer *Übermittlung* an die Öffentlichkeit stattfinden sollte.

(2) Für die Bearbeitung der Thematik ergaben sich über die - wissenschaftlich notwendigen - bibliographischen Nachweise Bezüge zu bestimmten namentlich genannten oder feststellbaren Verfassern, darunter mutmaßlich auch noch Lebenden, und damit Angaben, die in datenschutzrechtlicher Terminologie *personenbezogene Daten* darstellen. Außerdem enthielt der Text Angaben zu innerhalb des Wissenschaftsbetriebes geäußerten Auffassungen aus den Jahren 1990 und später im Vergleich zu grundlegenden historischen bzw. historisch-politischen Standpunkten der betreffenden als DDR-Historiker aus der Zeit bis zum Herbst 1989.

(3) Die maßgeblichen datenschutzrechtlichen Vorschriften waren § 28 Abs. 1 Satz 1 Nr. 2 und Nr. 3 BDSG. In der Anwendung beider Vorschriften ergab sich die datenschutzrechtliche Erlaubtheit der geplanten Veröffentlichung:

Gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist namentlich auch die *Übermittlung* personenbezogener Daten erlaubt, soweit sie zur *Wahrung berechtigter Interessen desjenigen, der die Übermittlung vornimmt, erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Über-*

mittlung überwiegt. Gemäß Nr. 3 der Vorschrift ist die Übermittlung erlaubt, wenn die übermittelten Daten *allgemein zugänglich sind oder derjenige, der die Übermittlung vornimmt, sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Übermittlung gegenüber dem berechtigten Interesse des Übermittelnden offensichtlich überwiegt*.

Bei Anwendung beider Vorschriften ergibt sich ganz offensichtlich, dass das Interesse derjenigen, die innerhalb des Wissenschaftsbetriebes oder im Bereich wissenschaftsnaher Publizistik sich in gedruckter, veröffentlichter Form äußern, daran, dass das von ihnen Publizierte dann von anderen nicht mehr zitiert oder in anderer Weise wiedergegeben und dass daran keine gedanklichen Folgerungen geknüpft werden, von der Rechtsordnung *nicht* als ein einer Übermittlung entgegenstehender Umstand anerkannt wird. Dies ergibt sich sowohl speziell aus dem von der Gewährleistung der Wissenschaftsfreiheit (gemäß Art. 5 Abs. 3 Satz 1 GG) in besonderer Weise umfassten Schutz freier öffentlicher wissenschaftlicher Diskussion und namentlich *Kritik* an mit wissenschaftlichem Anspruch gemachten Äußerungen als auch unter dem Gesichtspunkt der (in Art. 5 Abs. 1 Satz 1 GG gewährleisteten) dem freien Gedankenaustausch im Gemeinwesen dienenden Meinungsfreiheit. In beiden Fällen gehört zur Kennzeichnung einer Meinung, mit der sich der sich Äußernde auseinandersetzt, auch die Angabe, wer die anderen Meinungen, auf die er sich bezieht, vertreten hat bzw. vertritt. Dabei ist insbesondere dem Wissenschaftsbetrieb das personenbezogen, d. h. sich als Äußernder bekennende Äußern als wissenschaftlich begründet geäußerter Meinungen wie auch deren ebenso öffentliche und personenbezogene Beurteilung durch andere immanent.

Dies gilt in besonderer Weise auch für beamtete oder in ähnlicher Weise vom Staat beschäftigte Wissenschaftler, auch wenn sie nicht das von vornherein auf öffentliche Äußerung gerichtete Amt eines Hochschullehrers („ordentlicher öffentlicher Professor“, „Professor publicus“, wie die traditionellen Bezeichnungen lauten) ausüben. Denn auch ein etwa als außerhalb des akademischen Betriebes tätiger mit Forschungs- bzw. Publizistikaufgaben betrauter Historiker genießt für diese Tätigkeit keinen Datenschutz, und zwar weil er sowohl am Wissenschaftsbetrieb (in diesem Fall außerhalb des Hochschulbereiches) teilnimmt als auch außerdem insoweit *als Amtsträger in Ausübung seines Amtes tätig ist*, so dass auch aus diesem Grunde dafür kein Datenschutz besteht (das ist ein allgemeiner, in § 10 Abs. 2 Satz 3 SächsArchivG zum Ausdruck kommender Grundsatz des Datenschutzrechtes).

Diese Gesichtspunkte gelten insbesondere für die Geschichtswissenschaft, die sich traditionell in weiten Bereichen an ein breiteres Publikum, über die engere Fachöffentlichkeit hinaus, richtet.

(4) Mit den genannten rechtlichen Regeln und deren Anwendung befindet sich das Datenschutzrecht meiner Einschätzung nach (aus Gründen der Einheitlichkeit der Rechtsordnung) notwendig in Übereinstimmung mit dem (über das Datenschutzrecht hinausreichenden) allgemeinen zivilrechtlichen Persönlichkeitsrechtsschutz. Dieser ist sicherlich nicht schwächer als derjenige im Datenschutzrecht, da er nicht die besonderen Gefährdungen des Persönlichkeitsrechts durch die maschinelle Verwendung personenbezogener Daten zu berücksichtigen hat.

4.3.11 Versicherungen

4.3.11.1 Bekanntgabe von Passwörtern im Schadensfall

Ein Versicherungsnehmer war nach Geltendmachung eines Sachversicherungsfalls aufgefordert worden, einem insoweit von der Versicherungsgesellschaft mit der Schadensfeststellung beauftragten Sachverständigenbüro das Passwort des beschädigten Rechners mitzuteilen. Er bezweifelte allerdings, dass das Kennwort für eine hardwaretechnische Diagnose tatsächlich erforderlich und dessen Erhebung damit zulässig ist, zumal die Versicherung vorsorglich auch darauf hingewiesen hatte, dass sowohl das Sachverständigenbüro als auch die Versicherung im Rahmen der Prüfung ggf. Kenntnis von auf dem Rechner gespeicherten Daten erhalten könne.

Ob das Sachverständigenbüro für seine Tätigkeit tatsächlich Kenntnis der vom Versicherungsnehmer vergebenen Passwörter benötigt, hängt von der Art des Schadens und natürlich auch davon ab, auf welcher Ebene (z. B. BIOS, Bootmanager, Betriebssystem) dieser Passwörter vergeben hat. Weiterhin ist von Bedeutung, ob der Computer anschließend - soweit möglich - wieder in einen betriebsfähigen Zustand versetzt werden soll. Im Regelfall ist allerdings davon auszugehen, dass für die Tätigkeit eines Sachverständigenbüros die Kenntnis der vergebenen Passwörter - jedenfalls bis zur Betriebssystemebene - erforderlich ist, um die entsprechenden Diagnoseprogramme überhaupt einsetzen und Art und Umfang sowie Ursachen des Schadens zweifelsfrei feststellen zu können.

Soweit ein PC-Besitzer in Kenntnis der konkreten Schadensumstände diesbezüglich anderer Auffassung ist, könnte er auf die Angabe der Passwörter zunächst auch verzichten und das Sachverständigenbüro bitten, sich bei entsprechender Notwendigkeit noch einmal an ihn zu wenden. Letztendlich ist es dann seine Entscheidung, ob er in diesem Fall auf dem Versicherungsfall besteht oder im Wissen um die Sensibilität der auf seinem Rechner gespeicherten Daten auf die Inanspruchnahme der Versicherung verzichtet.

Unabhängig davon ist darauf hinzuweisen, dass es zum Betriebsrisiko eines jeden Rechners gehört, dass dieser (aus den verschiedensten Ursachen) auch ausfallen kann und daher gegebenenfalls zur Reparatur oder zumindest eben zur Schadensfeststellung an einen Dritten gegeben werden muss, der dabei meist auch notwendig Datenzugang erhält. PC-Besitzer haben dabei - neben einer regelmäßigen Datensicherung (Backup) sowie gegebenenfalls auch einer verschlüsselten Datenspeicherung - gegenüber Dritten, wenn sie diese betreffenden Daten speichern, selbst die Pflicht, vor Weggabe des Gerätes für die Sicherung der Daten vor unbefugter Kenntnisnahme zu sorgen. Ist eine Löschung aus technischen Gründen - etwa weil der Rechner überhaupt nicht mehr funktioniert - nicht möglich, dann ist dem beauftragten Sachverständigenbüro mitzuteilen, dass personenbezogene Daten auf der Festplatte vorhanden sind, verbunden mit der konkreten Anweisung, wie damit - etwa bei einem Festplattendefekt - zu verfahren ist.

Was die mögliche Kenntnisnahme von auf einem (defekten) Rechner gespeicherten Daten betrifft, so ist dies als ein lediglich vorsorglicher, standardmäßig auf dem Versicherungsbogen enthaltener Hinweis der Versicherungsgesellschaft zu betrachten. Da eine (zufällige) Kenntnisnahme von Nutzerdaten je nach Schadensart und -umfang nicht vollkommen auszuschließen ist und letztendlich auch schon Angaben zu der auf dem Rechner gegebenenfalls vorhandenen (Schad-) Software als personenbezogene Daten zu betrachten sind, weist das Versicherungsunternehmen auf diese Möglichkeit hin. Eine zielgerichtete inhaltliche Analyse gespeicherter Dateien mit Nutzerdaten wäre zweifelsfrei unzulässig. In der vorliegenden Konstellation, dass die Versicherung ein Sachverständigenbüro mit der Schadensfeststellung beauftragt hat, darf dieses im Übrigen nur die für die Schadensbeurteilung relevanten Daten erheben und an die Versicherungsgesellschaft weitergeben.

4.3.12 Mietverhältnisse

4.3.12.1 Fernabfrage von Verbrauchswerten

Aus den Schilderungen eines Mieters einer genossenschaftlich vermieteten Wohnanlage ergab sich, dass seine Wohnungsbaugenossenschaft aus Anlass eines Streites über die Ursache von Schimmelbefall zu verschiedenen Zeitpunkten sein Momentanheizverhalten mittels Fernauslese der elektronischen Heizungssteuerungs- und -verbrauchsmessanlage (sog. „Wohnungsmanager“) heimlich erhoben und ihm als Beweismittel zum Nachweis des behaupteten Heizverhaltens vorgehalten hatte. Wegen des Vorfalls hegte der Mieter den Verdacht, mittels des „Wohnungsmanagers“ würden raum- und stundengenau alle Verbrauchswerte im Gerät gespeichert und könnten von der Wohnungsbaugenossenschaft beliebig fernausgelesen und zu einem Profil zusammengeführt werden.

Die Feststellung der von einer natürlichen Person in einem bestimmten Zeitraum verbrauchten Heizenergie ist eine Erhebung personenbezogener Daten im Sinne des § 3 Abs. 1 BDSG, da diese grundsätzlich geeignet sind, Auskunft über persönliche und sachliche (Lebens-)Verhältnisse zu geben. Beispielhaft genannt sei etwa der Rückschluss auf den Grad der Nutzung einer Wohnung. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist jedoch nur zulässig, soweit das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt, anordnet oder der Betroffene eingewilligt hat (§ 4 Abs. 1 BDSG). Nach § 4 Abs. 1 i. V. m. Abs. 2 Satz 1 HeizkostenV ist der Gebäudeeigentümer verpflichtet, den anteiligen Verbrauch der Nutzer an Wärme und Warmwasser zu erfassen und hierzu die Räume mit Ausstattungen zur Verbrauchserfassung zu versehen. Ohne jedoch eindeutig die Art der zu verarbeitenden Daten im Einzelnen festzulegen, reicht diese Vorschrift als eigenständige Erlaubnisnorm nicht aus. Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist jedoch nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG u. a. auch dann zulässig, wenn es für die Durchführung eines rechtsgeschäftlichen Schuldverhältnisses, hier der Abrechnung mietvertraglich geschuldeter Betriebskosten, erforderlich ist. Die Vorschrift begrenzt die Erhebung personenbezogener Daten allerdings schon nach ihrem Wortlaut auf das für die Erfüllung des vertraglichen Abrechnungszweckes Erforderliche.

Die stundengenaue Erfassung der Heizverbrauchswerte ist für die Abrechnung eines turnusmäßigen, in der Regel lediglich einmal jährlich zu ermittelnden Gesamtverbrauchs ohne Relevanz, so dass die Erforderlichkeit einer Erhebung und Verarbeitung solcher weitergehender Daten durch den Vermieter nicht erkennbar ist. Soweit die Daten zur Steuerung der Haustechnik oder zum persönlichen Energiemanagement des Mieters dienen, bedarf es hierzu jedenfalls keiner Verarbeitung und Nutzung, also eigenen Fernauslese der Daten durch den Vermieter. Falls das System auch der Aufklärung bzw. Dokumentation etwaiger Störungen dient, kann dem jedenfalls immer noch durch eine bedarfsweise Vor-Ort-Auslesung unter direkter Mitwirkung des Mieters Rechnung getragen werden, zumal personenbezogene Daten grundsätzlich beim Betroffenen zu erheben sind (§ 4 Abs. 2 BDSG). Soweit also der Mieter nicht ausdrücklich in die Erhebung, Verarbeitung und Nutzung dieser Daten durch den Vermieter sowie insbesondere in einen Fernabruf schriftlich eingewilligt hat (§§ 4 Abs. 1, 4a Abs. 1 BDSG - Widerruf jederzeit durch den Betroffenen möglich), wäre ein solcher Umgang mit personenbezogenen Daten unzulässig, zumal die Beachtung des Grundsatzes der Direkterhebung gemessen an der immer noch gängigen Praxis einer Vor-Ort-Ablesung keinen unverhältnismäßigen Aufwand i. S. d. § 4 Abs. 2 Satz 2 Nr. 2b BDSG bedeutet und die potentielle Eignung qualifizierter Verbrauchsdaten zur Erstellung personenbezogener Verbrauchsprofile gleichwohl überwiegende schutzwürdige Interessen der Betroffenen

beeinträchtigen kann. Eine Fernabfrage ohne Einwilligung des Betroffenen ist daher nur dann datenschutzrechtlich vertretbar, wenn diese - nach vorheriger Information des Betroffenen - allein anlassbezogen einmal jährlich zum Zweck der Turnusrechnung oder aus Gründen eines Mieterwechsels erfolgt sowie allein die zum Stichtag vorhandenen Zählerstände abgefragt werden, also kein Rückschluss auf das Verbrauchsverhalten weiter eingrenzbarer Zeiträume möglich ist.

Für die von dem Mieter geäußerte Besorgnis, seine Wohnungsbaugenossenschaft erhebe kontinuierlich im Wege der Fernauslese über das Abrechnungserfordernis hinaus profiltaugliche Heizwerte, haben sich keine Anhaltspunkte finden lassen. Dessen ungeachtet datenschutzrechtlich zu würdigen blieb jedoch die von der Wohnungsbaugenossenschaft getätigte, insoweit außerordentliche stichprobenartige Erhebung des Verbrauchs- bzw. Heizstatus des Mieters aus Anlass eines Dissenses über die Ursachen einer Schimmelbildung:

Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn dies für die Durchführung des rechtsgeschäftlichen Schuldverhältnisses, hier also des Mietverhältnisses, erforderlich ist. Zwar schuldete die Wohnungsbaugenossenschaft dem Mieter eine funktionstüchtige Heizungsanlage, jedoch ist für die Gewähr der Funktionsfähigkeit eine hierauf gerichtete Fernabfrage, insbesondere ohne Kenntnis des Betroffenen, jedenfalls dann nicht zwingend erforderlich, wenn die Funktionstüchtigkeit auch unter Mitwirkung des Betroffenen ermittelt werden kann (§ 4 Abs. 2 Satz 1 BDSG). Die Erhebung der hier in Rede stehenden personenbezogenen Daten findet zudem auch keine Rechtsgrundlage in § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Die Ermittlung der Funktionsfähigkeit und Funktionstüchtigkeit einer Heizungsanlage mag zwar ein berechtigtes Interesse der Wohnungsbaugenossenschaft sein. Dies gilt insbesondere dann, wenn diese zumindest mitursächlich für eine etwaige Schimmelbildung sein könnte. Gleichwohl ist eine „verdeckte“ Fernabfrage zur Wahrung dieses berechtigten Interesses jedenfalls dann nicht erforderlich, wenn eine Mitwirkung des Betroffenen an der Erhebung der Daten erwartet werden darf, zumal im begründeten Einzelfall eine Duldung einer offenen Erhebung vertraglich geschuldet sein dürfte. Wegen der Intensität eines Eingriffs in die informationelle Selbstbestimmung des Betroffenen durch eine heimliche Erhebung seiner Verbrauchs- und damit Lebensgewohnheiten besteht zudem Grund zu der Annahme, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss dieser Form der Erhebung überwiegt.

Von der Wohnungsbaugenossenschaft wurde in Auswertung dieses Sachverhaltes die Zusicherung gegeben, durch eine schriftliche Arbeitsanweisung sämtliche Mitarbeiter

zu verpflichten, zukünftig vor jeder außerordentlichen Fernabfrage das ausdrückliche Einverständnis der betroffenen Mieter einzuholen.

4.3.12.2 Angabe von Vergleichswohnungen zur Begründung eines Mieterhöhungsverlangens

Eine Mieterin war darüber informiert worden, dass Angaben zu ihrer Wohnung (Name, Lage, Grundmiete) im Zuge eines Mieterhöhungsverlangens einer anderen Mieterin in der gleichen Wohnanlage mitgeteilt worden waren.

Eine solche Vorgehensweise begegnet keinen datenschutzrechtlichen Bedenken:

Gemäß § 558a Abs. 2 BGB hat der Vermieter verschiedene Möglichkeiten, ein Mieterhöhungsverlangen zu begründen. Jede dieser Möglichkeiten dient dazu, dem Mieter im Interesse einer außergerichtlichen Einigung die Tatsachen mitzuteilen, die er zur Prüfung einer vom Vermieter begehrten Mieterhöhung benötigt.

Erfolgt die Begründung anhand von Vergleichswohnungen (§ 558a Abs. 2 Nr. 4 BGB), so soll der Mieter durch die Benennung einzelner Wohnungen die Möglichkeit haben, sich über die Vergleichswohnungen zu informieren und die behauptete Vergleichbarkeit nachzuprüfen (BGH, Urteil vom 18. Dezember 2002, Az. VIII ZR 141/02). Die Vergleichswohnungen müssen deshalb so genau bezeichnet werden, dass der Mieter sie ohne nennenswerte Schwierigkeiten auffinden kann. Wenn sich in einem Mehrfamilienhaus mit mehreren Geschossen auf derselben Ebene mehr als eine Wohnung befinden, sind nach Auffassung des BGH für die Auffindbarkeit der Wohnung über die Angabe der Adresse und des Geschosses hinaus weitere Angaben erforderlich. Solche Angaben könnten z. B. die Lage der Wohnung im Geschoss, die Bezeichnung einer nach außen hin erkennbaren Wohnungsnummer oder der Name des Mieters sein. Für die Überprüfung der vom Vermieter gemachten Angaben reicht also zum Beispiel der pauschale Verweis auf Wohnblöcke nicht aus. Durch derart anonymisierte Angaben zu den Vergleichswohnungen setzte sich der Vermieter der Gefahr aus, dass das Mieterhöhungsverlangen vor Gericht keinen Bestand hat, da die Vergleichswohnungen nicht hinreichend genau benannt worden sind. So hat der BGH in seinem oben erwähnten Urteil ein Mieterhöhungsverlangen für unwirksam erachtet, da sich aus diesem nicht ergab, welche von zwei Wohnungen auf derselben Etage eines Wohnhauses als Vergleichswohnung gemeint war.

Die Mitteilung der Namen der zu Vergleichszwecken herangezogenen Mieter im Erhöhungsschreiben ist somit gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG gerechtfertigt; einer (vorherigen) Zustimmung der Mieter, die als Vergleichsmieter benannt werden, in die Weitergabe bedarf es dabei also nicht:

Auf Seiten der übermittelnden Vermieter besteht nach geltendem Mietrecht ein berechtigtes Interesse, ein Mieterhöhungsverlangen so zu begründen, dass es vor Gericht Bestand hat. In § 558a Abs. 2 Nr. 4 BGB wird den Vermietern die Möglichkeit eröffnet, die Begründung anhand von drei Vergleichswohnungen vorzunehmen. Der Vermieter hat daher auch ein von der Rechtsordnung, nämlich dem Mietrecht, anerkanntes berechtigtes Interesse, diese so genau zu beschreiben, wie es erforderlich ist, damit eine Begründung des Mieterhöhungsverlangens wirksam ist. Die Angabe des Mietzinses betrifft allerdings auch die Privatsphäre des betreffenden Mieters der Vergleichswohnung und lässt Rückschlüsse auf dessen Wohn- und Lebensverhältnisse zu. Insofern ist zweifellos ein schutzwürdiges Interesse an der Geheimhaltung dieser den intimen Lebensbereich Wohnung betreffender Details anzunehmen. Im Rahmen der gebotenen Interessenabwägung besteht angesichts der gesetzlichen Wertung des § 558a BGB, wonach dem Informationsinteresse des Adressaten des Erhöhungsverlangens und der Möglichkeit der Nachprüfung ein hoher Stellenwert eingeräumt wird, jedoch grundsätzlich kein Grund zur Annahme, dass dieses Interesse gegenüber dem berechtigten Interesse des Vermieters überwiegen könnte (zumal es sich dabei zugleich um ein ihn betreffendes Datum handelt, um ein sogenanntes Datum mit Doppelbezug).

An der Rechtmäßigkeit einer solchen Vorgehensweise eines Vermieters ändert sich auch dann nichts, wenn für die betreffende Kommune ein sogenannter qualifizierter Mietspiegel nach § 558d BGB existiert, denn § 558a Abs. 2 Nr. 1 BGB sieht den (einfachen wie qualifizierten) Mietspiegel als mögliches Begründungsmittel an, ohne dass sich aus der Reihenfolge der in § 558a Abs. 2 BGB (nicht abschließend) genannten Begründungsmittel eine Rangfolge ergäbe. Der Vermieter ist also nicht gehindert, trotz Vorliegens eines Mietspiegels sein Mieterhöhungsverlangen mit anderen Tatsachen, also zum Beispiel eben mit entsprechenden Vergleichswohnungen, zu begründen, dies folgt aus § 558a Abs. 3 BGB. Liegt allerdings ein qualifizierter Mietspiegel vor, der auch tatsächlich die konkrete Wohnlage erfasst und sind ihm Aussagen über die betreffende Wohnung zu entnehmen, hat der Vermieter gemäß § 558a Abs. 3 BGB die entsprechenden Angaben aus dem Mietspiegel zwingend in seinem Mieterhöhungsverlangen anzugeben, auch dann, wenn er die Mieterhöhung auf ein anderes Begründungsmittel stützt.

4.3.12.3 Keine Abwehr rechtmäßiger Faxsendungen

Eine Ärztin, die sich mit dem Vermieter ihrer Praxisräume in einem Mietrechtsstreit befand, beschwerte sich bei der Aufsichtsbehörde darüber, dass die Anwältin ihres Vermieters ihr wiederholt und gegen ihren ausdrücklich geäußerten Willen diese Mietrechtsstreitigkeit betreffende Nachrichten an ihr Praxisfax gesandt habe. Dadurch hätten

diese Nachrichten von ihren Mitarbeitern bzw. dem Reinigungspersonal zur Kenntnis genommen werden können.

Ein datenschutzrechtlicher Verstoß seitens des Absenders der Faxsendungen war jedoch nicht festzustellen. Der Mietrechtsstreit betraf die Ärztin nicht als Privatperson, sondern als Unternehmerin. In dieser Eigenschaft hat sie ein Faxgerät betrieben und durch die Bekanntgabe der dazugehörigen Faxnummer für andere Personen und Stellen einen diesbezüglichen Kommunikationszugang eröffnet. Vor diesem Hintergrund war es nicht zu beanstanden, wenn ihr - auch ohne ihr Einverständnis - Nachrichten, die sie als Unternehmerin betrafen (und die mit der Rechtsordnung im Einklang stehen), auf dieses Faxgerät gesendet werden.

Um zu vermeiden, dass der Inhalt eingehender Faxsendungen unbefugt durch Mitarbeiterinnen oder das Reinigungspersonal zur Kenntnis genommen werden könnte, hätte sie statt dessen selbst entsprechende technische oder organisatorische Maßnahmen treffen, d. h. auf geeignete Art und Weise dafür sorgen müssen, dass nur sie selbst bzw. von ihr autorisierte Personen Zugang zum Faxgerät erhalten.

4.3.12.4 Belehrungsbuch in einem Alternativhotel

Der Gast eines als Erlebnishotel ausgestalteten Beherbergungsbetriebes hatte sich daran gestört, dass in dem zum bestimmungsgemäßen Verhalten geführten und in Form einer fortlaufenden Liste angelegten Belehrungsbuch jeder neu eincheckende Gast Zugriff auf die Einträge aller im Buch zuvor dokumentierten Gäste hatte. Ohne umzublättern habe er zumindest Name, Vorname, Datum und Unterschrift der auf derselben Seite aufgeführten, d. h. im Wesentlichen zeitgleich mit ihm angereisten, Gäste einsehen können. Das Unternehmen war ursprünglich der Auffassung gewesen, es handele sich um ein gewöhnliches Gästebuch, wie es in zahlreichen gastronomischen Einrichtungen ausliegt. Dagegen wandte sich der Beschwerdeführer jedoch mit der Einlassung, vorliegend sei das Zustandekommen des Beherbergungsvertrages kausal mit der Unterschriftsleistung für die Belehrung verbunden gewesen; andernfalls wäre er abgewiesen worden.

Die Abgrenzbarkeit zur (freiwilligen, für das Zustandekommen eines Beherbergungsvertrages irrelevanten) Eintragung in ein gewöhnliches Gästebuch war insoweit offenkundig. Aus datenschutzrechtlicher Sicht entsprach die dargestellte Verfahrensweise einer Übermittlung personenbezogener Daten, die nach dem hier einschlägigen § 28 Abs. 1 Satz 1 Nr. 1 BDSG nur dann zulässig gewesen wäre, wenn dafür eine Erforderlichkeit für die Durchführung des Beherbergungsvertrages mit dem Betroffenen bestanden hätte.

Zwar kann der Akt des durch Unterschriftsleistung bekräftigten Bekenntnisses, die Belehrung empfangen und gelesen zu haben, in Anbetracht der in einem Erlebnishotel mitunter ungewöhnlichen Gefahrenlagen nicht in Zweifel gezogen werden; für die darüber hinausgehende Übermittlung der Gästedaten an eine unbestimmte Anzahl nachfolgender Gäste bestand aber offensichtlich kein Erfordernis. Auch die alternativ durchzuführende Abwägung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG führt dabei zu keinem anderen Ergebnis. Auch hier fehlte es an einem berechtigten Übermittlungsinteresse der verantwortlichen Stelle - mit der Dokumentation sind ausschließlich Nachweiszwecke verfolgt worden -, zudem standen zweifelsfrei schutzwürdige Betroffeneninteressen einer Übermittlung der Tatsache, welche Personen wann in diesem - nicht gerade preiswerten - Erlebnishotel übernachtet haben, entgegen.

Das Unternehmen hat daraufhin zugesichert, durch organisatorische Voraussetzungen künftig dafür Sorge zu tragen, dass die Belehrungsdokumentation für Dritte nicht mehr zugänglich ist.

4.3.13 Outsourcing

4.3.13.1 Beauftragung eines Subauftragnehmers

Der Datenschutzbeauftragte eines mittelständigen Unternehmens hatte sich wegen des Vorwurfs der unautorisierten Weitergabe von Mitarbeiterdaten durch seinen Auftragnehmer an den Sächsischen Datenschutzbeauftragten gewandt. Streitpunkt war der von besagtem mittelständigem Unternehmen nicht genehmigte Rückgriff des Auftragnehmers auf einen Subauftragnehmer. Gegenstand des betreffenden Vertrages war die Entgeltabrechnung; durch den Auftragnehmer an einen Subauftragnehmer ausgelagert worden waren der Ausdruck und die Kuvertierung der Lohnzettel.

Bei dem zwischen dem mittelständigen Unternehmen und seinem Auftragnehmer bestehenden Vertragsverhältnis hatte es sich datenschutzrechtlich um einen Fall der Auftragsdatenverarbeitung gehandelt. Der damit einschlägige § 11 BDSG legte in Abs. 2 Satz 2 seiner bis 31. August 2009 geltenden Fassung zum einen fest, dass die im Rahmen eines solchen Vertragsverhältnisses erfolgende Einbeziehung von Subauftragnehmern einer vorherigen schriftlichen Festlegung durch den Auftraggeber bedarf, zum anderen regelte Absatz 3, dass der Auftragnehmer die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen darf.

Der in besagtem Fall bestehende Vertrag enthielt keine Regelung über die etwaige Einbeziehung von Subauftragnehmern. Stattdessen war vom Auftragnehmer vertraglich sogar zugesichert worden, dass der Ausdruck und die Kuvertierung in der hauseigenen Druckerei des Auftragnehmers erfolge. Der Rückgriff auf einen Subauftragnehmer war

damit weder vertraglich noch anderweitig mit dem Auftraggeber vereinbart und somit unzulässig.

Zwar hatte der Auftragnehmer dem Auftraggeber vorher schriftlich angekündigt, den Druck der Lohndokumente zukünftig durch einen konkret benannten Subauftragnehmer durchführen zu lassen, jedoch hatte der Auftraggeber darauf auch umgehend reagiert und mitgeteilt, dass er mit der Beauftragung eines Subunternehmens (noch) nicht einverstanden sei und zunächst weitere Informationen und Unterlagen zu diesem Unterauftragsverhältnis benötige. Diese waren ihm aber trotz Mahnung und nochmaligen Widerspruchs gegen die (sofortige) Einbeziehung des Subauftragnehmers nicht bereitgestellt worden. Dem Auftragnehmer waren also zudem noch zwei eindeutige Weisungen gemäß § 11 Abs. 3 Satz 1 BDSG erteilt worden, die von diesem nicht befolgt worden waren. Auch aus diesem Grund ist die Beauftragung des Subauftragnehmers also unzulässig gewesen.

In diesem Zusammenhang ist darauf hinzuweisen, dass sich auch nach dem Bundesdatenschutzgesetz in seiner seit dem 1. September 2009 gültigen Fassung keine andere Bewertung ergeben hätte. Auch nach der aktuell gültigen Fassung ist die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen schriftlich festzulegen (§ 11 Abs. 2 Satz 2 Nr. 6 BDSG) und auch die Weisungsgebundenheit des Auftragnehmers ist unverändert (§ 11 Abs. 3 Satz 1 BDSG) gesetzlich vorgeschrieben.

Den Vertragsparteien wurde daher abschließend aufgegeben, im Zuge der wegen besagter Gesetzesänderung ohnehin notwendigen Vertragsüberarbeitung auch die Problematik der Einbeziehung des Subauftragnehmers einer Klärung und vertraglichen Regelung zuzuführen.

4.3.13.2 Weitergabe von Kontodaten an Geschäftspartner

Ein Cateringunternehmen belieferte im Rahmen der Mittagsversorgung etwa 6000 Kunden u. a. in Kindertagesstätten und Schulen. Die Bezahlung erfolgte im Wege des Lastschriftverfahrens; hierfür hatten die Kunden dem Caterer eine Einzugsermächtigung erteilt. Aus steuerlichen Gründen hat das Cateringunternehmen dann Anfang 2009 den Belieferungsservice ausgegliedert und eine Dienstleistungsfirma mit dem Transport und der Essensausgabe beauftragt. Die nächste den Kunden zugegangene Rechnung enthielt daraufhin den Hinweis: *„Ab sofort wird die Fa. [...] die Servicebeiträge der Firma direkt mit Ihnen verrechnen.“*

Im darauffolgenden Monat mussten die Kunden des Caterers dann unter ihrer dort bestehenden Kundennummer zwei Lastschriften auf ihren Kontoauszügen feststellen. Neben der Lastschrift mit dem Empfängernamen des Cateringunternehmens war auf den

Kontoauszügen auch eine Lastschrift für die Dienstleistungsfirma ausgewiesen. Diese Tatsache belegte eine Übermittlung der Bankverbindungsdaten durch das Cateringunternehmen an die von ihr beauftragte Dienstleistungsfirma.

Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG (in seiner bis 31. August 2009 gültigen Fassung) wäre das Übermitteln personenbezogener Daten, hier insbesondere der Kontoverbindungen, als Mittel für die Erfüllung eigener Geschäftszwecke zulässig gewesen, wenn es der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen gedient hätte.

Zweck der Vertragsverhältnisse zwischen dem Cateringunternehmen und deren Kunden war die Zubereitung und Lieferung des Mittagessens. Zur Erfüllung dieser Verträge konnte sich das Cateringunternehmen sicherlich auch der Unterstützung anderer Unternehmen, beispielsweise für die Belieferung, bedienen. Soweit der jeweilige Subunternehmer dazu personenbezogene Kundendaten - etwa zur Speisenauslieferung oder Ausgabe des Essens - benötigte, durften ihm diese auf der Grundlage des § 28 Abs. 1 Satz 1 Nr. 1 BDSG auch übermittelt werden. Vertragspartner der belieferten Kunden ist dabei jedoch immer das Cateringunternehmen geblieben, d. h. Zahlungen waren auch nur an dieses zu leisten. Die übermittelten Bankverbindungsdaten stammten aus Einzugsermächtigungen, die ausschließlich dem Cateringunternehmen erteilt worden waren. Wenn unter diesen Umständen also die Kontoverbindungsdaten der Kunden an einen eingeschalteten Subunternehmer herausgegeben worden sind, damit dieser dem Cateringunternehmen im Innenverhältnis zustehende Anteile des Gesamtentgeltes, das der Kunde zu entrichten hat, selbst von den Kunden einziehen kann, so diente dies nicht mehr der Zweckbestimmung der mit den Kunden abgeschlossenen Verträge.

Eine Erlaubnis zur Übermittlung personenbezogener Daten ergab sich im Weiteren auch nicht aus § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Nach dieser Vorschrift wäre eine Datenübermittlung zulässig gewesen, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich gewesen wäre und kein Grund zu der Annahme bestanden hätte, dass das schutzwürdige Interesse der Betroffenen am Ausschluss der Übermittlung überwogen hat.

Eine Erlaubnis unmittelbar nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG scheiterte daran, dass insoweit eine Übermittlung gemäß § 28 Abs. 1 Satz 2 nur zu dem Zweck erfolgen darf, der bei der Datenerhebung konkret festgelegt worden ist. Die Bankverbindungsdaten waren jedoch nicht zu dem Zweck erhoben worden, sie anschließend an die Dienstleistungsfirma zu übermitteln. Eine Zulässigkeit der Datenübermittlung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG kam daher nur über § 28 Abs. 2 BDSG in Betracht, der die Übermittlung von Daten für andere als die bei der Erhebung festgelegten Zwecke unter

den Voraussetzungen dieser Vorschrift gestattet. Es fehlte aber hier daran, dass die Übermittlung der Daten zur Wahrung berechtigter Interessen des Cateringunternehmens erforderlich gewesen ist. Der Caterer hätte ebenso gut selbst das „Serviceentgelt“ einziehen und an die Dienstleistungsfirma überweisen können. Darüber hinaus hat auch Grund zu der Annahme bestanden, dass das schutzwürdige Interesse der Betroffenen am Ausschluss der Übermittlung überwogen hat: Natürlich hatten die betroffenen Kunden ein schutzwürdiges Interesse daran, dass ihre Bankverbindungsdaten nicht ohne ihre Zustimmung bzw. sogar ohne ihr Wissen anderen Unternehmen, mit denen sie in keinem Vertragsverhältnis stehen, zur Kenntnis und Nutzung für den Forderungseinzug übermittelt werden. Davon zeugte nicht zuletzt die Tatsache, dass etwa 350 Kunden auch sofort dem Lastschrifteinzug durch die Dienstleistungsfirma bei ihrer jeweiligen Bank widersprochen hatten.

Eine Erlaubnis zur Übermittlung personenbezogener Daten ergab sich des Weiteren auch nicht aus § 28 Abs. 3 BDSG. Nach Nr. 1 dieser Vorschrift wäre eine Datenübermittlung zulässig gewesen, soweit es zur Wahrung berechtigter Interessen eines Dritten erforderlich gewesen wäre und kein Grund zu der Annahme bestanden hätte, dass Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hatten.

Ein berechtigtes Interesse der Dienstleistungsfirma, für ihre Serviceleistungen bezahlt zu werden, ist zweifellos vorhanden gewesen, jedoch war dieses Interesse vorliegend nicht gegenüber den Kunden des Caterers, sondern direkt diesem gegenüber als Auftraggeber geltend zu machen gewesen. Insoweit ist also auch aus Sicht des Empfängers eine Übermittlung der Bankverbindungsdaten nicht erforderlich gewesen. Es hätte ausgereicht, wenn das Cateringunternehmen das „Serviceentgelt“ als monatliche Gesamtsumme an die Dienstleistungsfirma überwiesen hätte. Überdies wäre es bei dieser Vorschrift nicht auf ein überwiegendes schutzwürdiges Interesse der Betroffenen angekommen, sondern eine Erlaubtheit bereits dann gescheitert, wenn diese, wie hier offensichtlich der Fall, ein der Übermittlung entgegenstehendes schutzwürdiges Interesse haben.

Die Übermittlung war damit rechtswidrig (vgl. dazu auch Pkt. 11.1).

4.3.14 Öffentlicher und Individualverkehr

4.3.14.1 Kontrollbildschirme bei der Sicherheitskontrolle am Flughafen

Ein Reisender informierte darüber, dass bei der Kontrolle von Bordkarten an der Schleuse vor dem Einlass zur Personen-/Gepäckkontrolle eines sächsischen Flughafens der dortige Kontrollbildschirm so aufgestellt bzw. einsehbar gewesen wäre, dass über das Kontrollpersonal hinaus auch Dritte Kenntnis von der dort angezeigten Identität des

Bordkarteninhabers hätten nehmen können, da der Bildschirm schon aus geringer Entfernung für jedermann einsehbar gewesen sei.

Ist ein Kontrollbildschirm so aufgestellt bzw. einsehbar, dass über das Kontrollpersonal hinaus auch Dritte Kenntnis von der Identität des Bordkarteninhabers erlangen können, handelt es sich bei der Kenntnisverschaffung um eine unzulässige Übermittlung personenbezogener Daten, da weder das Bundesdatenschutzgesetz noch eine andere Vorschrift über den Datenschutz dies erlauben und der Betroffene nicht in die Übermittlung eingewilligt hat (§ 4 Abs. 1 BDSG). Mithin läge darin auch ein Verstoß gegen die in der Anlage zu § 9 BDSG niedergelegten Grundsätze zur Datensicherheit, da nach Satz 2 Nr. 3 solche technischen und organisatorischen Maßnahmen zu treffen sind, die gewährleisten, dass personenbezogene Daten bei der Verarbeitung und Nutzung nicht unbefugt gelesen werden können.

Der Flughafenbetreiber hat daraufhin zusätzliche Sichtschutzmaßnahmen und eine Softwareänderung zugesagt, so dass künftig statt der Identität des Bordkarteninhabers am Bildschirm nur noch ein „Go“ oder „Not Go“ angezeigt wird.

4.3.14.2 Berechnung von Parkplatzgebühren mittels EC-Karte

Mehrere Eingaben beinhalteten den Sachverhalt, dass die Benutzung eines Parkplatzes nur noch mit Hilfe einer EC-Karte möglich sei. Damit sich die Schranke zum Parkplatz öffnet und dieser genutzt werden könne, müsse die EC-Karte in ein Lesegerät eingesteckt werden, das Kontonummer, Bankleitzahl sowie die Ankunftszeit speichere. Bei Ausfahrt sei die EC-Karte erneut einzustecken, damit zusätzlich die Ausfahrtszeit ermittelt werden könne. Auf Grundlage der so erhobenen Daten würden dann die Parkgebühren errechnet und sodann vom Konto abgebucht.

Der Betrieb eines solchen Systems wurde als zulässig erachtet. Gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Das in Rede stehende System liest von der EC-Karte die Kontonummer und Bankleitzahl aus und speichert zudem die An- und Abfahrtszeit. Eine Zuordnung der Bankdaten zu bestimmten Personen ist nicht möglich. Die Datensätze derjenigen Personen, die innerhalb der kostenfrei angebotenen Grundparkzeit den Parkplatz wieder verlassen, werden umgehend nach dem Verlassen gelöscht; auch wurden die gespeicherten Daten hinreichend durch technische und organisatorische Maßnahmen gesichert.

Die Anschaffungs- und Betriebskosten für Kassenautomaten sind demgegenüber deutlich höher, darüber hinaus fallen dabei Zusatzkosten für die Tickets sowie für eine häufigere Wartung an. Im Übrigen wird mit dem beschriebenen System infolge des Verzichts auf Umgang mit Bargeld auch die Vandalismusgefahr reduziert.

4.3.14.3 Verfolgung von Parkverstößen auf privat betriebenen Parkplätzen

Im Berichtszeitraum mehrfach eingegangen sind Beschwerden über einen privaten Parkplatzbetreiber bzw. dessen Inkasso-Partner über deren Vorgehen bei behauptetem Verstoß gegen die für die entgeltliche Parkplatznutzung geltend gemachten AGB.

Von speziellen Ausgestaltungen der Einzelfälle und den sich daraus ergebenden Rechtsfragen soll hier abgesehen werden. Einheitlich war bei allen Sachverhalten der Umstand, dass die betroffenen Kraftfahrzeugführer zuvor in einen der keine Zugangssperre (Schranken etc.) besitzenden Parkplätze eingefahren waren und nach (in Einzelfällen bereits extrem kurzer) Überschreitung der auf dem Parkschein ausgewiesenen Parkberechtigungsdauer die Beobachtung angegeben haben, dass ein Mitarbeiter des Parkplatzbetreibers das Fahrzeug des Betroffenen zu fotografieren begann. Die spätere Kostennote des Inkassobüros (wegen Schadensersatz aufgrund der unberechtigten Blockierung des Parkraums) habe sich auf das solcherart festgestellte amtliche Kennzeichen und die auf dessen Basis durchgeführte Halterabfrage bei den Kraftfahrzeugzulassungsstellen gestützt.

Wesentlich für die datenschutzrechtliche Bewertung der vom Betreiber durchgeführten Erhebungsmaßnahmen (Fotodokumentation und Halterabfrage) ist die Klärung der Wirksamkeit einer AGB-Klausel, die letztlich bereits den Verdacht nahelegt, dass die Schadensersatzforderung selbst der Zweck des gesamten Geschäftsmodells sein könnte. Allerdings ist es nicht Aufgabe einer Datenschutzaufsichtsbehörde, die Wirksamkeit nicht das Datenschutzrecht betreffender AGB-Klauseln zu prüfen, auch kann eine darauf beruhende Datenerhebung jedenfalls solange, wie über deren Unwirksamkeit noch nicht anderweitig (zivilrechtlich) entschieden worden ist, nicht schon deswegen als unzulässig bewertet werden.

Für eine Halteranfrage nach § 39 Abs. 1 StVG ist lediglich die Darlegung erforderlich, dass „die Daten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt“ werden. Die Erfolgswahrscheinlichkeit, einen Anspruch dann auch durchsetzen zu können, ist insoweit ohne Belang. Indem der Parkplatzbetreiber

einen Verstoß gegen seine AGB behauptet, erfüllt er jedenfalls diese formale und leicht zu erbringende Voraussetzung an eine Halterauskunft.

Soweit die Voraussetzungen der Halterauskunft erfüllt sind, ergibt sich folgerichtig, dass der Anspruchsteller auch die rechtlich erheblichen Tatsachen dokumentieren darf. Der Fotobeweis gehört dabei zu den geeigneten und von den Gerichten anerkannten Mitteln. Allerdings - da der behauptete Parksünder nicht mit dem Halter identisch sein muss - ergeben sich Zweifel hinsichtlich der Geeignetheit dieses Instruments. In einem - sofern überhaupt vom Parkplatzbetreiber gewagten - gerichtlichen Verfahren ergeben sich daher Lücken in der Beweisführung, die eine Abwehr des Anspruchs ermöglichen könnten.

4.3.14.4 Mittelbare Erhebung aus polizeilichen Datenbeständen

Ein Unfallgeschädigter hatte sich nach einem Unfall mit leichtem Sachschaden und Fahrerflucht die Autonummer des Unfallgegners gemerkt und sich nachfolgend über einen Bekannten bei der Polizei Detailinformationen über den Halter des betreffenden Fahrzeuges beschafft.

Daraus ergab sich die Frage, ob es sich insoweit um einen datenschutzrechtlichen Verstoß seitens des Unfallgeschädigten, d. h. um ein unbefugtes Verschaffen personenbezogener Daten gehandelt hatte. (Die Frage der Zulässigkeit des Abrufs und der Übermittlung der Daten des Fahrzeughalters durch den dabei tätig gewordenen Polizeibeamten war durch die Aufsichtsbehörde aus Zuständigkeitsgründen nicht zu klären.)

Dies konnte aus folgenden Gründen verneint werden:

Die Datenerhebung durch den Unfallgeschädigten, in Gestalt der Beschaffung von Daten aus polizeilichen Datenbeständen war, auch als Datenerhebung ohne Beteiligung des Betroffenen, gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG rechtmäßig. Das ergibt sich aus dem Gesichtspunkt der Einheit (Widerspruchsfreiheit) der Rechtsordnung: Die Daten, die der Unfallgeschädigte erhoben hatte, waren nicht über diejenigen Daten hinausgegangen, auf die er als Geschädigter gegenüber dem Schädiger, der sich rechtswidrig, vermutlich auch strafbar, von der Unfallstelle entfernt hatte, zu bekommen ein Recht gehabt hatte.

Die Tatsache, dass derjenige, der ihm die Daten übermittelt hat, rechtswidrig gehandelt hat, macht die Datenerhebung noch nicht rechtswidrig. Die Anstiftung zur rechtswidrigen Datenübermittlung durch den Datenempfänger ist vom Erhebungsbegriff des Bundesdatenschutzgesetzes nicht umfasst.

4.3.14.5 OWi-Anzeige unter Beifügung privater Beweisfotos

Weil er wegen vermeintlich ordnungswidrigen Parkens auf einer Grünfläche von einem Nachbarn fotografiert worden war und dieser das Bild der Verfolgungsbehörde übermittelt hatte, fragte ein Petent nach der datenschutzrechtlichen Gestattung der Aufnahme und deren Weitergabe an die Verfolgungsbehörde durch den privaten Anzeigeerstatter.

Unter der Annahme einer automatisierten Erhebung bzw. Verarbeitung unter Einsatz einer Datenverarbeitungsanlage etwa durch den Einsatz einer Digitalkamera oder elektronischen Übermittlung eines (ebenso elektronischen) Bildes (Anwendungsvoraussetzung des Bundesdatenschutzgesetzes) ist die Erhebung personenbezogener Daten durch Private und deren Übermittlung an eine Behörde gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig, wenn hierdurch mutmaßliche Rechtsverstöße angezeigt werden und die der Behörde gemachten Angaben zutreffend oder auch infolge nur leichter Fahrlässigkeit unzutreffend sind. Dies ergibt sich aus der gefestigten verwaltungsrechtlichen Rechtsprechung (vgl. BVerwG, Urteil vom 23. Juni 1982, Az.: 1 C 222/79) zum Schutz des redlichen Hinweisgebers gegen (datenschutzrechtliche oder verwaltungsverfahrensrechtliche) Auskunftsansprüche des Betroffenen in Verbindung mit dem Gebot der Widerspruchsfreiheit der Rechtsordnung.

4.3.15 Personalausweisdaten

4.3.15.1 Das neue Personalausweisgesetz - Gesetzliche Verarbeitungs- und Nutzungsbeschränkungen für nicht-öffentliche Stellen

Am 1. November 2010 ist das Gesetz über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften (BGBl. I 2009, 1346 ff.) in Kraft getreten, welches in Artikel 1 das novellierte Personalausweisgesetz enthält.

Neu und insbesondere bedeutsam für nicht-öffentliche Stellen ist u. a. zunächst die Regelung in § 1 Abs. 1 Satz 3 PAuswG, wonach vom Ausweisinhaber nicht verlangt werden darf, den Personalausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben. Damit ist die in der Vergangenheit vielerorts geübte Praxis, den Personalausweis als Pfandobjekt zu verwenden, etwa im Rahmen der Einlasskontrolle zu sensiblen Unternehmensbereichen oder auch im Zusammenhang mit der Ausleihe technischer Geräte in Museen, nunmehr nicht mehr rechtskonform und daher zu beenden.

In § 20 PAuswG ist darüber hinaus die Verwendung durch öffentliche und nicht-öffentliche Stellen geregelt:

(1) Der Inhaber kann den Ausweis bei öffentlichen und nichtöffentlichen Stellen als Identitätsnachweis und Legitimationspapier verwenden.

(2) Außer zum elektronischen Identitätsnachweis darf der Ausweis durch öffentliche und nichtöffentliche Stellen weder zum automatisierten Abruf personenbezogener Daten noch zur automatisierten Speicherung personenbezogener Daten verwendet werden.

(3) Die Seriennummern, die Sperrkennwörter und die Sperrmerkmale dürfen nicht so verwendet werden, dass mit ihrer Hilfe ein automatisierter Abruf personenbezogener Daten oder eine Verknüpfung von Dateien möglich ist. Dies gilt nicht für den Abgleich von Sperrmerkmalen durch Diensteanbieter zum Zweck der Überprüfung, ob ein elektronischer Identitätsnachweis gesperrt ist.

Aus dieser Regelung in Verbindung mit § 14 Nr. 2 PAuswG, wonach die Erhebung und Verwendung personenbezogener Daten aus dem Ausweis oder mithilfe des Ausweises durch nicht-öffentliche Stellen *ausschließlich* nach Maßgabe der §§ 18 bis 20 erfolgen darf, hatte das BMI zunächst ein grundsätzliches Vervielfältigungsverbot für Personalausweise (sowie Pässe) durch Fotokopieren, Scannen oder sonstige Ablichtung abgeleitet. Wohl in erster Linie auf die diesbezügliche Intervention der Datenschutzaufsichtsbehörden, die mit Nachdruck auf die daraus resultierenden erheblichen Probleme bei der Identifikation Betroffener im Rahmen von Auskunftsverlangen nach § 34 BDSG hingewiesen hatten, hat das BMI seine Position dann aber wieder revidiert und die Anfertigung von Ausweiskopien unter - allerdings engen Voraussetzungen - als zulässig bewertet. Für Details dazu wird auf die Ausführungen unter Pkt. 4.3.9.2 verwiesen.

Dessen ungeachtet bietet der neue Personalausweis mit seiner neuen Funktion des elektronischen Identitätsnachweises zugleich aber die Möglichkeit, zukünftig auch im Rahmen von Auskunftsverlangen nach § 34 BDSG nicht mehr auf Ausweiskopien zurückgreifen zu müssen. Voraussetzung ist natürlich, dass die verantwortlichen Stellen, hier also in erster Linie die Auskunfteien, das diesbezügliche Verfahren entsprechend implementieren, die Betroffenen bereits einen elektronischen Personalausweis besitzen und die eID-Funktion auch aktiviert haben.

4.3.15.2 Ausweiskopien bei Kreditkartenzahlung im Internet

Vermehrt eingegangen sind Beschwerden zu Unternehmen, die Waren oder Dienstleistungen über das Internet vertreiben und im Falle einer Kreditkartenzahlung vom Kunden noch Kopien der Kreditkarte und des Personalausweises verlangen.

Die Abforderung einer Kopie einer auf einem Internetportal zur Bezahlung eingesetzten Kreditkarte begegnet vom Grundsatz her zunächst ebenso wenig datenschutzrechtlichen

Bedenken wie das Verlangen nach Vorlage einer Kopie des Reisepasses bzw. Personalausweises. Gemäß § 20 Abs. 1 PAuswG kann das Personaldokument auch im nicht-öffentlichen Bereich als Identitätsnachweis benutzt werden. Den besonderen Umständen des genutzten Mediums ist es dabei geschuldet, dass sich die verantwortliche Stelle in diesem Fall nicht unmittelbar durch Einsichtnahme in das Personaldokument von der Identität ihres Kunden überzeugen kann, sondern hierfür auf die Überlassung und anschließende Sichtkontrolle einer Ausweiskopie ausweichen muss. Während das bloße Vorzeigenlassen in einem Ladengeschäft nicht den datenschutzrechtlich relevanten Vorgang der (Erhebung und) Speicherung aller manuell auslesbaren Merkmale beinhaltet und somit datenschutzrechtlich unkritisch ist, ist die Aushändigung einer Kopie wegen der damit verbundenen Datenspeicherung nach dem Maßstab des Bundesdatenschutzgesetzes zu beurteilen. Gleichwohl ist diese Verfahrensweise bei Einhaltung konkreter Rahmenbedingungen zulässig. Denn nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist das Erheben, Speichern und Nutzen personenbezogener Daten zulässig, wenn dies für die Begründung eines rechtsgeschäftlichen Schuldverhältnisses - hierzu gehört auch die Authentifizierung des Geschäftspartners - mit dem Betroffenen erforderlich ist. Überhaupt ist ein Authentifizierungsverlangen im Geschäftsverkehr in der Regel als mit datenschutzrechtlichen Vorschriften vereinbar zu betrachten. Durch die verantwortliche Stelle ist dabei aber eine ggf. durch den Betroffenen vorgenommene Teilschwärzung nicht für die Identifikation des Vertragspartners erforderlicher Ausweisdaten anzuerkennen.

Die zu dieser Problematik angeschriebenen verantwortlichen Stellen haben auf die Missbrauchsrisiken beim Kreditkarteneinsatz im Internet verwiesen. Bei der Kreditkartennutzung im Internet kann der Händler nicht überprüfen, ob er die Kartendaten vom Berechtigten erhalten hat, d. h. er kann nicht überprüfen, ob der Berechtigte selbst handelt (Besitz- und Unterschriftsprüfung). Zudem fehlt ihm für das Geltendmachen seiner Forderungen ein Nachweis in Form des unterzeichneten Leistungsbelegs.

Bestreitet der berechtigte Karteninhaber den Karteneinsatz, können weder Händler noch Kartengesellschaft den Vollbeweis dafür erbringen, dass der berechtigte Karteninhaber verfügt bzw. wenigstens schuldhaft zum Kartenmissbrauch beigetragen hat. In der Regel sehen die Verträge zwischen den Kreditkartengesellschaften und den Händlern Rückforderungsklauseln für den Fall vor, dass eine Kreditkartenzahlung im Fernabsatz angenommen wurde und ihre Veranlassung vom Karteninhaber bestritten wird.

Nach den Erfahrungen der jeweiligen Firmen besteht ein erhöhtes Missbrauchsrisiko beispielsweise dann, wenn

- Kunden mit einer Kreditkarte einer nicht in Deutschland ansässigen Bank bezahlen wollen

  Für solche Kreditkarten, die Verbraucher zunehmend über das Internet statt bei ihrer Hausbank bestellten, bestünde ein in tatsächlichen Erfahrungen begründetes erhöhtes Missbrauchsrisiko. Karten dieser Kartenherausgeber seien wegen oftmals nicht hinreichend sicherer Identifizierung und Authentifizierung der Vertragspartner nachweislich in besonderem Maß von Missbrauch und Zahlungsausfällen betroffen.

- Rechnungsadresse (Anschrift des Karteninhabers) und Lieferanschrift nicht übereinstimmen

  In diesem Fall nehmen Firmen häufig eine zusätzliche Adressprüfung bei dem jeweiligen Kartenemittenten bzw. dem von diesem beauftragten Zahlungsdienstleister vor. Soweit der Kartenemittent bzw. dessen Zahlungsdienstleister einen solchen Service nicht anbietet oder aber die Adressprüfung negativ verläuft (weil die abweichende Lieferanschrift nicht bei der Kreditkartengesellschaft hinterlegt ist), werden die betreffenden Kunden aufgefordert, Kopien ihres Personalausweises und ihrer Kreditkarte beizubringen (als Besitznachweis) oder eine alternative Zahlungsmethode zu wählen.

- (Einzel-)Flüge (für Dritte) gebucht werden

  Besondere Aufmerksamkeit sei zunächst immer dann geboten, wenn Flüge für Dritte gebucht würden, d. h. Kreditkarteninhaber und Reisender nicht identisch sind. In diesen Fällen bestehe ein erhöhtes Risiko, dass die Flugbuchung unter Verwendung gestohlener Kreditkarten(-daten) erfolgt sein könnte. Darüber hinaus seien insbesondere mit Buchungen von Flügen aus dem osteuropäischen Raum negative Erfahrungen gemacht worden. Hier hätten dubiose Reisevermittler Betrugsmethoden entwickelt, deren Hauptgeschädigte oftmals die wahren Inhaber der Kreditkarten seien. Um solche Betrugsdelikte weitgehend zu unterbinden, lasse man sich daher im Einzelfall, z. B. bei einem Einzelticket (ohne Rückflug) vom Ausland ins Inland, die genannten Kopien zusenden, um auf dieser Grundlage zu überprüfen, dass die den Flug buchende Person auch Inhaber der Kreditkarte ist.

Eine stichprobenhafte bzw. auf konkrete Kauf- bzw. Buchungsumstände beschränkte Kontrolle ist daher aus datenschutzrechtlicher Sicht nicht zu beanstanden.

Von wesentlicher Bedeutung ist darüber hinaus die Bereitstellung eines sicheren Übertragungsweges für die Übersendung der Ausweis- und Kreditkartenkopien. Soweit dabei von den Betroffenen eine Zusendung dieser Kopien per E-Mail oder Fax, mithin über unsichere Übertragungswege, gefordert und nicht ein sicherer Kommunikationskanal - z. B. eine SSL-geschützte Möglichkeit zum Hochladen der Kopien - eröffnet wird, ist dies unzulässig (vgl. Nr. 4 der Anlage zu § 9 Satz 1 BDSG; § 13 Abs. 4 Nr. 3 TMG). Letztendlich führt dies dazu, dass die zur Authentifizierung des Kunden herangezogenen Kopien ihren Beweiswert verlieren, da sie während der Übertragung von Dritten eingesehen, kopiert, manipuliert und anschließend missbräuchlich verwendet werden können.

Die wesentlichen Grundsätze für eine datenschutzkonforme Verfahrensweise bei der Identitätsprüfung nach Kreditkarteneinsatz können wie folgt zusammengefasst werden:

1. Bereits im Buchungsprozess ist der Kunde darauf hinzuweisen, dass beim Einsatz einer Kreditkarte im Rahmen eines nachfolgenden Authentifizierungsverlangens ggf. weitere Datenerhebungen (Ausweiskopie) folgen können.

2. Damit der Kunde dies ohne Nachteil für die Buchungsmöglichkeit vermeiden kann, sind ihm bereits im Buchungsprozess alternative Zahlungsmöglichkeiten anzubieten.

3. Im Rahmen eines Authentifizierungsverlangens ist der Kunde auf die Möglichkeit des Schwärzens nicht erforderlicher Daten in den Ausweiskopien hinzuweisen.

4. Es ist ein sicherer Übertragungsweg (z. B. SSL-gesicherte Übermittlung) für die Kopien bereitzustellen; alternativ ist hinreichend deutlich über die Risiken (Vertraulichkeitsverlust, Identitätsdiebstahl) der angebotenen „unsicheren“ Übertragungsmöglichkeiten (E-Mail, Fax) zu informieren und zusätzlich auf den Postweg zu verweisen.

5. Die Ausweiskopien dürfen ausschließlich zur Identitätsprüfung und insbesondere die Seriennummern nicht so verwendet werden, dass mit ihrer Hilfe ein automatisierter Abruf personenbezogener Daten oder eine Verknüpfung von Dateien möglich ist (vgl. §§ 20 und 32 Abs. 1 Nr. 8 PAuswG).

6. Nach erfolgreichem Abschluss des Bezahlvorganges, ca. acht bis zwölf Wochen nach Zahlungseingang, sind die Ausweiskopien zu vernichten bzw. zu löschen.

4.3.15.3 Ausweiskopien bei Telefonverträgen

Gleichfalls verstärkt sind Kunden von Mobilfunk-Shops an die Aufsichtsbehörde herangetreten, weil sie zum Abschluss oder zur Änderung eines Mobilfunkvertrages zur Aushändigung ihres Personaldokuments zwecks Anfertigung einer Kopie aufgefordert

worden waren. Wie durchgehend festzustellen war, sind die Kopien zusammen mit den Vertragsunterlagen an den jeweiligen Mobilfunk-Diensteanbieter abgegeben worden; eine Aufbewahrung in den Mobilfunk-Shops konnte nicht festgestellt werden.

Da die angefertigten Kopien vom jeweiligen Mobilfunk-Shop vollumfänglich und unverzüglich an den Diensteanbieter weitergereicht worden waren, waren die Petenten insoweit auf die Kontrollzuständigkeit des BFDI zu verweisen. Dessen ungeachtet ist dabei aber auf die Regelung des § 95 Abs. 4 TKG hingewiesen worden, aus der sich die grundsätzliche Erlaubnis zur Anfertigung von Ausweiskopien (auch bei Vertragsänderungen) ergibt. Inwieweit die Diensteanbieter davon Gebrauch machen (bzw. zur Datenvermeidung beitragen), entscheiden diese selbst. Im Übrigen sind auch die Diensteanbieter verpflichtet, die angeforderten Kopien unverzüglich nach Feststellung der für die Vertragsänderung erforderlichen Angaben eines Teilnehmers zu vernichten (§ 95 Abs. 4 Satz 3 TKG).

4.3.15.4 Ausweiskopien bei Kontaktanzeigen

Ein Kontaktanzeigenkunde eines Zeitungsverlages war bei der Anzeigenaufgabe zur Aushändigung seines Personalausweises aufgefordert worden, um davon eine Kopie für die Unterlagen des Verlages zu erstellen. Als Begründung war ihm angegeben worden, dass er seine Kontaktanzeige nicht unter einer Chiffre-Nummer, sondern stattdessen mit (s)einer Mobiltelefonnummer versehen veröffentlichen wollte. Der Einwand des Kunden, dass er zugleich Abonnent einer von diesem Verlag herausgegebenen Zeitung und mithin als Kunde identifiziert sei, hatte bei dem Verlag keine Berücksichtigung gefunden.

Die Erforderlichkeit dieser Verfahrensweise ist vom Verlag wie folgt begründet worden: Die Angabe der Telefonnummer eines unbeteiligten Dritten in einer Kontaktanzeige gegen seinen Willen könne zu einer erheblichen Rufschädigung und zur Verletzung seiner Persönlichkeitsrechte führen. Für den Fall einer derartigen missbräuchlichen Verwendung von Telefonnummern Dritter durch den Anzeigenkunden solle dem Betroffenen dann mittels der Ausweiskopie ermöglicht werden, seine Rechte gegenüber dem Anzeigenkunden selbst weiter zu verfolgen. Gleiches gelte für die Durchsetzung etwaiger eigener Regressansprüche durch den Verlag. Auch hierfür sei eine eindeutige Verifizierung des Anzeigenkunden und eine später sichere Nachweisbarkeit der insoweit geprüften Daten zwingend erforderlich. Schließlich ist auch noch darauf verwiesen worden, dass auch die Strafverfolgungsbehörden wiederholt Auskunft (insbesondere wegen Straftaten gegen die sexuelle Selbstbestimmung) über die Daten von Anzeigenkunden verlangt hätten und man der insoweit bestehenden Auskunftspflicht nur dann vollständig nachkommen könne, wenn man eine Ausweiskopie vorhalte.

Die Einlassungen des Verlags waren ihrem Grundanliegen nach durchaus nachvollziehbar. Da nichtsdestoweniger aber nicht erkennbar war, dass für die Anzeigenschaltung (Vertragszweck) die Erhebung und Verarbeitung der Daten des Anzeigenkunden erforderlich gewesen sein sollten, kam als Zulässigkeitstatbestand insoweit nur § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Frage. An den berechtigten Interessen des Verlagshauses (s. o.) bestand kein Zweifel, allerdings hätte zur späteren sicheren Identifikation des Anzeigenkunden auch die Erfassung der Adressdaten, ggf. noch des Geburtsdatums sowie die augenscheinliche Überprüfung dieser Daten durch Einsichtnahme in den Personalausweis einschließlich eines entsprechenden Vermerks, dass diese Überprüfung auch tatsächlich stattgefunden hat, vollkommen ausgereicht. Nur unter diesen Voraussetzungen konnte davon ausgegangen werden, dass das schutzwürdige Interesse des Anzeigenkunden am Ausschluss der Erhebung und Speicherung der seiner (ggf. späteren) Identifizierung dienenden Daten nicht überwiegt. Erst recht musste dies bei einem Anzeigenkunden gelten, der dem Verlagshaus schon aus einer anderweitigen Vertragsbeziehung bekannt war.

Die Anfertigung einer Ausweiskopie ist in diesem Fall daher unzulässig gewesen.

4.3.15.5 Erhebung der Personalausweisnummer durch Kreditinstitute

Ein Sparkassenkunde hatte angefragt, ob seine Sparkasse berechtigt sei, von ihm die Personalausweisnummer zu erheben und in ihrem Datenverarbeitungssystem zu speichern.

Gegen die Erhebung der Personalausweisnummer bestehen keine Bedenken. Das Geldwäschegesetz verpflichtet Kreditinstitute bereits bei der Begründung einer Geschäftsbeziehung zur Identifizierung ihrer Vertragspartner (§ 3 Abs. 1 Nr. 1, Abs. 2 Nr. 1 GwG). Zur Überprüfung der Identität des Vertragspartners hat sich das Kreditinstitut dabei anhand eines gültigen amtlichen Lichtbildausweises zu vergewissern, dass die von diesem angegebenen Identifizierungsdaten zutreffend sind (§ 4 Abs. 4 Satz 1 Nr. 1 GwG). Hierüber sind entsprechende Aufzeichnungen anzufertigen, wozu auch die Art, die Nummer und die ausstellende Behörde des vorgelegten Ausweisdokuments gehören (§ 8 Abs. 1 Satz 2 GwG).

Die Sparkasse ist demnach sogar gesetzlich verpflichtet, die Personalausweisnummer zu erheben und zu speichern; dies kann im Übrigen auch durch Anfertigung und Aufbewahrung einer Ausweiskopie erfolgen (§ 8 Abs. 1 Satz 3 GwG; zur Problematik vgl. auch 1. TB, Pkt. 4.3.18).

4.3.15.6 Identifikation von LKW-Fahrern bei der Ladungsaufnahme

Ein Berufskraftfahrer war an der Pforte zu einem Speditionsgelände aufgefordert worden, seine Privatanschrift und die Ausweisnummer in eine entsprechend vorbereitete Kladde einzutragen. Nach Ablehnung dieses Ansinnens war ihm die Zufahrt zwar erlaubt worden, jedoch wollte er im Anschluss von der Aufsichtsbehörde dennoch wissen, ob solche Angaben überhaupt verlangt werden dürfen.

Zu Identifizierungszwecken ist der Personalausweis auch im Privatrechtsverkehr ausdrücklich zugelassen (§ 20 Abs. 1 PAuswG). Es kann daher für das Betreten eines Betriebsgeländes und vor allem für die Ladungsaufnahme durchaus als geeignet und erforderlich anzusehen sein, sich den Ausweis vorlegen zu lassen. Das Verlangen nach Angabe des Namens und Vorzeigen des Ausweises sowie das Notieren der Personalausweisnummer vor Zugang auf ein Betriebsgelände ist nach § 28 Abs. 1 Satz 1 Nr. 1 oder zumindest Nr. 2 BDSG als gerechtfertigt anzusehen. Auch § 20 Abs. 3 Satz 1 PAuswG, wonach Seriennummern nicht so verwendet werden dürfen, dass mit ihrer Hilfe ein automatisierter Abruf personenbezogener Daten oder eine Verknüpfung von Dateien möglich ist, steht der geschilderten Verfahrensweise nicht entgegen. Eine Lastwagenfracht kann erheblichen Wert darstellen. Der Spediteur hat damit den Beweis, den Ausweis des Kraftfahrers tatsächlich eingesehen und seine Identität geprüft und auch einen Nachweis, die Ladung tatsächlich übergeben zu haben. Der hier vorliegende Umstand, dass dem Betriebsfremden die Zufahrt nach verweigerter Eintragung - quasi als Ermessensentscheidung des Pförtners - dennoch gestattet worden war, widerlegt diese Rechtsauffassung nicht.

Anders steht es mit der Erhebung und Speicherung der Privatanschrift - diese ist für den die Ware übergebenden Spediteur ohne Bedeutung. Gerade im Handel ist wohl generell davon auszugehen, dass alle real abzuwickelnden Geschäftsvorgänge mit Unterlagen aus den „Büchern“ korrespondieren, d. h. die Kraftfahrer nicht ohne Dokumente (Ladepapiere) anreisen dürften, die sie ihrem entsendenden Unternehmen eindeutig zuordnen lassen.

4.3.16 Betrieblicher Datenschutzbeauftragter

4.3.16.1 Bestellungspflicht für Dentallabore

Wie der Aufsichtsbehörde mitgeteilt worden ist, enthalten die von den Zahnärzten an Dentallabore erteilten Aufträge in der Regel Vor- und Zunamen sowie den Versicherungsstatus des jeweiligen Patienten, mithin also personenbezogene Daten. Wegen der Tatsache, dass es Zweck des erteilten Auftrages ist, durch das Dentallabor nach entsprechenden Vorgaben Zahnersatz anfertigen zu lassen, handelt es sich dabei um Angaben

zur Gesundheit des Patienten, mithin um besondere Arten personenbezogener Daten gemäß § 3 Abs. 9 BDSG.

Nur dann, wenn das Dentallabor die genannten Daten anschließend auch selbst - etwa für Abrechnungszwecke (Rechnungserstellung) - automatisiert verarbeitet, greift die Pflicht zur Vorabkontrolle gemäß § 4d Abs. 5 BDSG. Diese Pflicht könnte dadurch umgangen werden, dass bei der automatisierten Verarbeitung entweder - falls möglich - auf die Angaben von Vor- und Zunamen verzichtet wird oder aber gleich mit den Zahnärzten vereinbart wird, dass Aufträge zukünftig nur unter Verzicht auf die Angabe von Vor- und Zunamen erteilt werden. Die Zahnärzte könnten stattdessen Auftragsnummern oder andere Kennzeichnungen für Einzelaufträge vergeben.

Gemäß § 4d Abs. 6 BDSG obliegt die Vorabkontrolle dem betrieblichen Datenschutzbeauftragten. Ist ein Datenschutzbeauftragter nicht schon aus anderen Gründen (vgl. § 4f Abs. 1 Sätze 1, 3 und 4 BDSG) zu bestellen, resultiert (daher) aus der Pflicht zur Durchführung einer Vorabkontrolle auch die Pflicht zur Bestellung eines Datenschutzbeauftragten (§ 4f Abs. 1 Satz 6 BDSG). Eine Kleinunternehmerregelung oder sonstige entlastende Regelungen für kleine Betriebe sieht das Bundesdatenschutzgesetz in diesem Zusammenhang nicht vor.

4.3.16.2 Ersatz eines internen durch einen externen Datenschutzbeauftragten?

Der betriebliche Datenschutzbeauftragte einer Wohnungsgenossenschaft war mit Wirkung zum 31. August 2009 - es darf wohl vermutet werden, dass dies im Zusammenhang mit den am 1. September 2009 in Kraft getretenen Kündigungsschutz- und Kostenübernahmeregelungen in § 4f Abs. 3 Sätze 5 bis 7 BDSG stand - ohne Angabe von Gründen von dieser Funktion abberufen worden. Gleichzeitig hatte der Datenschutzbeauftragte eine diesbezügliche Teilkündigung erhalten. Aus der vorsorglich erfolgten Anhörung des Betriebsrates, dem der Datenschutzbeauftragte ebenso angehörte, ergab sich diesbezüglich allerdings, dass damit das Ziel verfolgt worden war, ab dem 1. September 2009 eine externe Person als Datenschutzbeauftragter zu bestellen.

Diese Abberufung war zweifellos rechtswidrig und damit unwirksam:

§ 4f Abs. 3 Satz 4 BDSG regelt die Widerrufsmöglichkeiten der Bestellung eines betrieblichen Datenschutzbeauftragten durch die verantwortliche Stelle. Nach dieser Vorschrift kann die Bestellung in entsprechender Anwendung von § 626 BGB oder auf Verlangen der Aufsichtsbehörde widerrufen werden. Dieses Widerrufsrecht schließt jede weitere rechtliche Möglichkeit der verantwortlichen Stelle, die Bestellung einseitig zu beenden, aus (vgl. Simitis, BDSG, 6. Auflage, Rn. 184 zu § 4f).

Der betreffende Datenschutzbeauftragte war bereits 2002 schriftlich und unbefristet bestellt worden. Aus der Tatsache, dass ab dem 1. September 2009 ein externer Datenschutzbeauftragter bestellt werden sollte, war abzuleiten, dass auch weiterhin die Voraussetzungen für die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten erfüllt, insbesondere in der Regel auch mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt waren. Damit hätte die Bestellung in entsprechender Anwendung des § 626 BGB nur aus wichtigem Grund widerrufen werden können. Es müssten also Tatsachen oder Umstände gegeben gewesen sein, die unter Berücksichtigung des Einzelfalls und unter Abwägung der beiderseitigen Interessen die Fortsetzung der Tätigkeit als Datenschutzbeauftragter unzumutbar gemacht hätten. Derartige Voraussetzungen waren durch den Vorstand der Wohnungsgenossenschaft nicht geltend gemacht worden; er hatte offensichtlich lediglich beabsichtigt, den bislang internen durch einen danach externen Beauftragten zu ersetzen. Dies ist aber kein wichtiger, die weitere Tätigkeit als Datenschutzbeauftragter unmöglich machender Grund im Sinne des § 626 BGB. Wäre es anders, könnte ein Unternehmer einen unbequemen Datenschutzbeauftragten jederzeit und entgegen dem Benachteiligungsverbot des § 4f Abs. 3 Satz 3 BDSG mit Verweis auf die unternehmerische Entscheidung, zukünftig auf einen externen Datenschutzbeauftragten zurückgreifen zu wollen, aus dem Amt drängen. Die vom Gesetz beabsichtigte Unabhängigkeit des betrieblichen Datenschutzbeauftragten wäre damit nicht einmal ansatzweise gewährleistet.

Der betroffene Arbeitnehmer hat sich gegen diese Abberufung erfolgreich vor Gericht zur Wehr gesetzt. Auch das Gericht hat dabei die Auffassung vertreten, dass kein wichtiger Grund für die Abberufung vorgelegen hatte.

Inzwischen ist diese Frage (in einem anderen Fall) auch höchstrichterlich geklärt worden. Das BAG hat in einem fast identischen Fall am 23. März 2011 entschieden (Az. 10 AZR 562/09), dass die Bestellung zum Beauftragten für den Datenschutz nicht mit der Begründung widerrufen werden kann, dass die Aufgaben zukünftig von einem externen Dritten wahrgenommen werden sollen oder der Beauftragte Mitglied im Betriebsrat sei.

4.3.17 Informationspflichten bei Datenpannen

Seit dem 1. September 2009 sind verantwortliche Stellen nach § 42a BDSG verpflichtet, festgestellte Fälle unrechtmäßiger Datenübermittlung oder sonstiger unrechtmäßiger Kenntniserlangung durch Dritte der Aufsichtsbehörde unter bestimmten Voraussetzungen - namentlich wenn die in § 42a Satz 1 BDSG aufgezählten Datenarten betroffen sind und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen - mitzuteilen.

Bei der Aufsichtsbehörde sind daraufhin im Berichtszeitraum sechs solcher Meldungen eingegangen. Nach entsprechender Prüfung ist in zwei Fällen festgestellt worden, dass die Voraussetzungen für die Informationspflichten nicht erfüllt gewesen waren:

- In einem Fall fehlte es an der örtlichen Zuständigkeit des Sächsischen Datenschutzbeauftragten. Zwar waren von dem betreffenden Vorfall Arbeitnehmer der sächsischen Niederlassung des meldenden Unternehmens betroffen, jedoch hatte sich der eigentliche Vorfall außerhalb des Freistaates Sachsen ereignet.
- Im zweiten Fall war der Aufsichtsbehörde eine DDoS-Attacke auf die Website eines sächsischen Unternehmens gemeldet worden. Ein solcher Angriff zielt aber darauf ab, eine Website durch entsprechende Überlastung lahmzulegen, nicht jedoch dort Daten abzugreifen.

Die verbleibenden vier Meldungen betrafen

- in zwei Fällen das Ausspähen von Kartendaten an Geldautomaten (Skimming),
- den Verlust eines Datenträgers mit Lohnbuchhaltungsdaten beim Postversand, wobei der Datenträger allerdings später wieder aufgefunden worden ist, sowie
- einen Datendiebstahl mittels SQL-Injection im Online-Auftritt einer Apotheke.

Nach Eintreffen entsprechender Meldungen prüft die Aufsichtsbehörde

- die Vollständigkeit der eingegangenen Meldung (§ 42a Satz 4 BDSG),
- die ordnungsgemäße Benachrichtigung der Betroffenen (§ 42a Sätze 2, 3 BDSG) und insbesondere,
- ob ausreichende Maßnahmen getroffen worden sind, die eine Wiederholung des jeweiligen Vorfalls ausschließen (Beseitigung der Sicherheitslücke) und - abhängig vom Einzelfall - den eingetretenen oder zu erwartenden Schaden so weit als möglich minimieren.

Im Fall des Datendiebstahls aus dem Online-Auftritt einer Apotheke ist Letzteres angesichts des komplexen Sachverhalts mit einer örtlichen Kontrolle verbunden worden. Letztendlich war aber durch die verantwortlichen Stellen in allen Fällen ordnungsgemäß gehandelt worden, d. h. sowohl Aufsichtsbehörde als auch Betroffene waren jeweils umgehend und ausreichend informiert und auch ausreichende Maßnahmen zur zukünftigen Vermeidung bzw. Schadenminimierung getroffen worden.

4.3.18 Auch das gibt's

Auch in der Tätigkeit einer Datenschutzaufsichtsbehörde gibt es Fälle, die zunächst zum Schmunzeln anregen, bei näherer Betrachtung dann aber eine eigentlich erschreckende Naivität in Bezug auf datenschutzrechtliche Anforderungen offenbaren. Hier eine kleine Auswahl:

Vorhalt der Aufsichtsbehörde:	Frei zugänglicher Serverraum!
Antwort des Unternehmens:	Die freie Zugänglichkeit ist wichtig, weil sich in diesem Raum der Schalter für das Flurlicht befindet!
Vorhalt der Aufsichtsbehörde:	Zweckfremde Nutzung des Serverraums zum Abstellen von Fahrrädern!
Antwort des Unternehmens:	Keine zweckfremde Nutzung, da es sich um einen kombinierten Server- und Fahrradabstellraum handelt!
Frage der Aufsichtsbehörde:	Welche Absicherung gegen plötzliche Stromausfälle haben Sie seit meinem Kontrollbesuch getroffen?
Antwort des Unternehmens:	Ich bezahle seitdem meine Stromrechnung pünktlich!

5 Beratungstätigkeit

5.1 Überblick

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).

Dazu korrespondierende Vorschriften in § 4g Abs. 1 Sätze 1 bis 3 BDSG:

Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin. Zu diesem Zweck kann sich der Beauftragte für den Datenschutz in Zweifelsfällen an die für die Datenschutzkontrolle bei der verantwortlichen Stelle zuständige Behörde wenden. Er kann die Beratung nach § 38 Abs. 1 Satz 2 in Anspruch nehmen.

und in § 4d Abs. 6 Satz 3 BDSG:

Bei der Durchführung der Vorabkontrolle hat sich der Beauftragte für den Datenschutz in Zweifelsfällen an die Aufsichtsbehörde zu wenden.

Im Berichtszeitraum sind in 87 Fällen Beratungsanliegen an den Sächsischen Datenschutzbeauftragten herangetragen worden. Gegenüber dem Zeitraum 2007/2008 (34 Beratungsfälle) entspricht dies einer Steigerung um 156 %. 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 Betroffener (vgl. unten, Pkt. 5.2.3).

Die Analyse der Beratungstätigkeit hat für die Jahre 2009 und 2010 folgende Schwerpunkte ergeben:

- betrieblicher Datenschutzbeauftragter (17 Fälle) - hier ging es vor allem um Bestellungsvoraussetzungen und -formalitäten (9), um die erforderliche Fachkunde (2) sowie um die Wahrnehmung der gesetzlich vorgegebenen Aufgaben wie der Führung des Verfahrensverzeichnisses (2) und der Durchführung der Vorabkontrolle (2); im Übrigen aber auch um die vertraglichen Beziehungen zwischen externem Datenschutzbeauftragten und verantwortlicher Stelle sowie um Fragen der Abberufung bzw. Kündigung
- Gesundheitswesen (10 Fälle) - beraten wurden Krankenhäuser (3), Pflegedienste (2), eine Apotheke, ein Therapeut, ein Vertriebsunternehmen, ein Dienstleister und eine wissenschaftliche Fachgesellschaft

- Videoüberwachung (7 Fälle) - hierbei wurden der Einzelhandel (2), Nahverkehrsunternehmen (2), ein Arzt, der Betreiber eines Freizeitbades sowie ein mittelständisches Unternehmen beraten
- Anfragen aus dem Bereich der Forschung (5 Fälle)

5.2 Grenzen der Beratungspflicht

5.2.1 Anonyme Beratungsersuchen

Im Bereich der Anlasskontrolle (vgl. Pkt. 4.1) kommt es gelegentlich vor, dass die Aufsichtsbehörde anonyme Beschwerden bzw. Hinweise auf mögliche Datenschutzverletzungen erhält. Ob und in welcher Weise diesen Eingaben nachgegangen wird, ist jeweils eine Einzelfallentscheidung, die u. a. davon abhängt, wie plausibel und ausreichend detailliert der betreffende Sachverhalt beschrieben ist und inwieweit die Gründe für die Anonymität des Einsenders (angesichts der für die Mitarbeiter der Aufsichtsbehörde bestehenden Verschwiegenheitspflichten im Regelfall zwar nicht zwingend aber) zumindest nachvollziehbar sind.

Anders im Bereich der Beratung: Anonym eingehende Beratungsanfragen werden durch die Aufsichtsbehörde nicht bearbeitet!

Im Berichtszeitraum hat die Aufsichtsbehörde erstmalig eine Beratungsanfrage erhalten, aus der weder der individuelle Absender noch überhaupt die verantwortliche Stelle hervorging. Zwar ist eine Beantwortung des per E-Mail eingegangenen Anliegens in diesem Fall nicht schon deswegen ausgeschlossen gewesen, weil keine Rücksendeadresse vorhanden war, allerdings war der Absender aus der (bei einem großen Freemail-Anbieter geführten) E-Mail-Adresse für die Aufsichtsbehörde nicht erkennbar. Im Gegensatz zu Eingaben ist hier aber noch nicht einmal ansatzweise ein berechtigtes Interesses erkennbar, im Rahmen der begehrten Beratung gegenüber der Aufsichtsbehörde anonym zu bleiben. Angesichts der strengen Verschwiegenheitsregeln, die für die Aufsichtsbehörde gelten, gibt es auch im Hinblick auf die Besonderheiten des Datenschutzrechtes keinen Grund, dass eine Datenschutzaufsichtbehörde - anders als andere staatliche Stellen - Leistungen an anonym bleibende Personen oder Stellen erbringt. Von einer verantwortlichen Stelle ist zu erwarten, dass sie, wenn sie von der Aufsichtsbehörde verbindliche (und im Freistaat Sachsen immer noch kostenlose!) Aussagen oder Empfehlungen zu konkreten Sachverhalten begehrt, sich auch entsprechend zu erkennen gibt, ganz abgesehen davon, dass die Kenntnis von Art, Größe und Branche des Unternehmens für viele datenschutzrechtliche Bewertungen auch durchaus wesentlich ist. Ein von der Aufsichtsbehörde nicht selbst hinreichend geklärter Sachverhalt ist keine hinreichende Grundlage für einen Rechtsrat an Betroffene und im Gesetz so auch

nicht vorgesehen. Auch deshalb, weil der Aufsichtsbehörde Beratungen nur innerhalb ihres örtlichen Zuständigkeitsbereiches erlaubt sind, hat eine Beantwortung in solchen Fällen zu unterbleiben.

Nur der Vollständigkeit halber sei diesbezüglich abschließend erwähnt, dass es sich im konkreten Fall - zumindest das war ersichtlich - beim Absender um einen Rechtsanwalt gehandelt hat.

5.2.2 Abgelehnte Beratungsersuchen

§ 38 Abs. 1 Satz 2 BDSG begrenzt die Beratungspflicht und damit verbunden natürlich auch die (Rechts-)Beratungsbefugnis einerseits hinsichtlich der zu beratenden Stellen auf die Beauftragten für den Datenschutz und die verantwortlichen Stellen und andererseits in inhaltlicher Hinsicht auch auf deren typische Bedürfnisse.

Daraus ergibt sich zum einen eine Einschränkung dahingehend, dass die zu beratenden Stellen selbst personenbezogene Daten erheben, verarbeiten oder nutzen müssen, um ihr Recht auf Beratung durch die Aufsichtsbehörde geltend machen zu können. Andererseits müssen diese Beratungsanliegen natürlich auch im Zusammenhang mit der tatsächlichen und typischen Datenverarbeitung dieser Stellen stehen.

Aus Gründen des wiederum gewachsenen Arbeitsanfalles (Beschwerden und Beratungswünsche) bei unveränderter Personalsituation musste sich die Aufsichtsbehörde im Berichtszeitraum strikt an die Grenzen des § 38 Abs. 1 Satz 2 BDSG halten und einige der eingegangenen Beratungswünsche entsprechend ablehnen. Dies war beispielsweise bei folgenden Konstellationen der Fall:

- unspezifische Beratungsanliegen externer Datenschutzbeauftragter

  Anfragen externer Datenschutzbeauftragter kann, auch wenn sie selbst im Freistaat Sachsen ansässig sind, nur dann entsprochen werden, wenn sich diese im Hinblick auf einzelne bestimmte verantwortliche Stellen, die ihren Sitz zudem im Freistaat Sachsen haben müssen bzw. hier tatsächlich Daten erheben, verarbeiten oder nutzen, an die Aufsichtsbehörde wenden.

- unspezifische Beratungsanliegen verantwortlicher Stellen

  Lediglich allgemein gehaltene Bitten um Aufklärung über datenschutzrechtliche Bestimmungen in Bezug auf personenbezogene Daten, die im Arbeitsalltag einer verantwortliche Stelle anfallen, übersteigen die Grenzen der in § 38 Abs. 1 Satz 2 BDSG bestimmten Beratungspflicht und -befugnis der Aufsichtsbehörde.

- Beratungsanliegen von Beratungsunternehmen

  Soweit sich Beratungsunternehmen mit ihrer Mandantschaft betreffenden Anliegen an die Aufsichtsbehörde wenden, sind sie nicht selbst verantwortliche Stelle und damit keine Stelle, die sich nach § 38 Abs. 1 Satz 2 BDSG an die Aufsichtsbehörde wenden kann.

- Beratungsanliegen von Systemhäusern, Softwareherstellern u. ä. im Hinblick auf deren eigenes Produktfolio

  Auch Systemhäuser oder Softwarehersteller verarbeiten insoweit selbst keine personenbezogenen Daten, sondern entwickeln für andere (verantwortliche) Stellen lediglich Software bzw. Datenverarbeitungskonzepte.

- Begutachtung kompletter Datenverarbeitungskonzepte oder Geschäftsmodelle

  Die allgemeine Begutachtung eines Datenverarbeitungskonzeptes oder eines Geschäftsmodells übersteigt die Grenzen der in § 38 Abs. 1 Satz 2 BDSG ausgesprochenen Beratungspflicht der Datenschutzaufsichtsbehörde. Das Bundesdatenschutzgesetz sieht daher eine umfassende Prüfung von Datenverarbeitungskonzepten auch nicht vor. Erst wenn sich in diesem Zusammenhang spezifische, aufgearbeitete Fragen ergeben, kann in Bezug auf die tatsächliche verantwortliche Stelle der Bereich der Beratungspflicht und -befugnis nach § 38 Abs. 1 Satz 2 BDSG erreicht sein (vgl. auch 4. TB, Pkt. 5.2.1).

- durch Dritte abgelehnte Datenübermittlungen

  Die Aufsichtsbehörde hat nicht die Aufgabe und nicht die Befugnis, Stellen zu beraten, die davon betroffen sind, dass andere verantwortliche Stellen die Verarbeitung (Übermittlung) der sich auf dritte Personen beziehenden Daten unter Berufung auf datenschutzrechtliche Gründe ablehnen oder sonst unterlassen, denn in diesem Fall erfolgt die Anfrage nicht als verarbeitende (verantwortliche) Stelle, sondern stattdessen lediglich für diese. Zudem gilt: Eventuelle Pflichten zur Übermittlung - worum es in solchen Fällen regelmäßig geht - sind nur mittelbar Gegenstand datenschutzrechtlicher Überlegungen, weil aus der Pflicht die Befugnis folgt.

  Mit anderen Worten: Die Aufsichtsbehörde ist keine allgemeine Beratungsbehörde für Fragen, die im Zusammenhang mit der möglichen Verarbeitung personenbezogener Daten entstehen.

Im Fall der Ablehnung eines Beratungswunsches wird die betreffende Stelle bzw. Person regelmäßig auf die Möglichkeit der Inanspruchnahme von Vertretern der rechtsberatenden Berufe oder geeigneter Beratungsunternehmen verwiesen.

5.2.3 Beratungswünsche Betroffener

Wie unter Pkt. 5.2.2 bereits dargestellt, begrenzt § 38 Abs. 1 Satz 2 BDSG die Beratungsbefugnis auf die Beauftragten für den Datenschutz und die verantwortlichen Stellen.

Dies setzt der Tätigkeit der Datenschutzaufsichtsbehörde demnach auch dann Grenzen, wenn sich Betroffene bei der Aufsichtsbehörde für sich selbst oder auch für andere lediglich allgemein Rechtsrat holen wollen. Die Erteilung allgemeiner Rechtsauskünfte an Betroffene sieht das Bundesdatenschutzgesetz nicht vor. Für derartige Anliegen zuständig sind die Angehörigen der rechtsberatenden Berufe.

Voraussetzung für eine Befassung durch die Aufsichtsbehörde (als Eingabe, vgl. Pkt. 4.1) ist, dass vom Absender dargelegt wird, von einer konkreten Verarbeitungshandlung einer im Freistaat Sachsen ansässigen bzw. hier verarbeitenden verantwortlichen Stelle bereits betroffen und dabei aus datenschutzrechtlichen Gründen in seinen Rechten verletzt zu sein, und er ggf. sein Einverständnis erteilt, dass sich die Aufsichtsbehörde je nach Sachverhalt allgemein oder auf den speziellen Einzelfall bezogen an die betreffende verantwortliche Stelle wendet. Eine verlässliche rechtliche Beurteilung lässt sich regelmäßig erst nach Klärung des Sachverhaltes und damit nach Anhörung der verantwortlichen Stelle erarbeiten, weil die Aufsichtsbehörde nicht abstrakt sämtliche Umstände, die möglicherweise eine Datenerhebung, -verarbeitung oder -nutzung rechtfertigen, im Hinblick auf einen konkreten Sachverhalt kennen kann.

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.

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

Werden die von der Europäischen Kommission festgelegten (auch in deutscher Sprache verfügbaren) Standardvertragsklauseln, vgl.

http://ec.europa.eu/justice/policies/privacy/modelcontracts/index_en.htm

verwendet, ist die Genehmigung der Datenübermittlungen durch die Aufsichtsbehörde nicht mehr erforderlich.

Bei einer Reihe von Staaten hat die europäische Kommission in diesem Zusammenhang bereits formell festgestellt, dass dort ein im Sinne des § 4b angemessenes Datenschutzniveau gegeben ist. Dazu gehören bislang Andorra, Argentinien, die Färöer, Guernsey, Israel, die Isle of Man, die Vogtei Jersey, Kanada (mit Einschränkungen), die Schweiz sowie die USA (Safe Harbor). Bei einer Übermittlung in diese Länder ist gleichfalls keine Genehmigung durch die Aufsichtsbehörde mehr erforderlich. Die diesbezüglichen Entscheidungen sind von der Website der Europäischen Kommission abrufbar:

http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm

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 seine Verpflichtung, die Öffentlichkeit alle zwei Jahre über die Tätigkeit der Aufsichtsbehörde zu informieren.

Darüber hinaus werden auch im Internetauftritt des Sächsischen Datenschutzbeauftragten - *http://www.datenschutz.sachsen.de* - aktuelle Datenschutzthemen behandelt sowie Materialien zur Unterstützung der Tätigkeit der verantwortlichen Stellen und ihrer Datenschutzbeauftragten zum Abruf bereitgehalten und auch Informationen für Betroffene veröffentlicht.

Die bewährte Zusammenarbeit mit der GDD, insbesondere mit dem GDD-Erfa-Kreis Sachsen, an deren Veranstaltungen Vertreter der Aufsichtsbehörde regelmäßig und aktiv teilgenommen haben, 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. Darüber hinaus hat sich der Sächsische Datenschutzbeauftragte - in Ermangelung ausreichender personeller Ressourcen allerdings nur in einigen wenigen Fällen - noch an anderen Tagungen oder Fachveranstaltungen mit Fachvorträgen beteiligt, so etwa im Januar 2009 an einer Podiumsdiskussion der Verbraucherzentrale Sachsen zum Thema „Meine Daten gehören mir“ oder aber bei einer Informationsveranstaltung des Landesseniorenverbandes Sachsen e. V. zum Thema „Datenschutz in Seniorenvereinen und Datenschutz für Senioren“ im März 2009.

Tatsächlich lagen dem Sächsischen Datenschutzbeauftragten darüber hinaus zahlreiche weitere Anfragen für Vorträge oder zur Teilnahme an Diskussionsveranstaltungen vor.

Da derartige Veranstaltungen, deren Nützlichkeit nicht bestritten wird, die Grenzen der in § 38 Abs. 1 Satz 2 BDSG verankerten Beratungs- und Unterstützungspflicht (für betriebliche Datenschutzbeauftragte und die verantwortlichen Stellen selbst) übersteigen und die Erfüllung der gesetzlich vorgegebenen Kontroll- und Beratungsaufgaben (vgl. § 38 Abs. 1 BDSG) in jedem Fall vorrangig ist (vgl. die wiederum stark gestiegene Anzahl der Eingaben und Beratungswünsche - Pkte. 4.1 und 5.1), musste in solchen Fällen daher regelmäßig auf freiberuflich tätige Datenschutzfachleute bzw. gewerbliche Anbieter von Schulungsveranstaltungen verwiesen werden.

9 Gerichtliche Verfahren der Aufsichtsbehörde nach § 38 BDSG

9.1 Klage einer Religionsgemeinschaft vor dem VG Dresden gegen meine Kontrollen betreffend die Verarbeitung personenbezogener Daten durch Funktionsträger sog. Versammlungen dieser Religionsgemeinschaft

Im November 2007 hat mich eine Religionsgemeinschaft verklagt, weil sie von mir im Sommer 2007 - überwiegend unangekündigt - vorgenommene Kontrollen der Verarbeitung personenbezogener Daten durch Funktionsträger örtlicher, keinen festen Bürobetrieb unterhaltenden Gemeinden dieser Religionsgemeinschaft für rechtswidrig gehalten hat.

Nach dem Wechsel umfangreicher Schriftsätze ist es erst im Jahr 2011 zur mündlichen Verhandlung gekommen. In dieser ist die 6. Kammer des VG Dresden der - meiner unveränderten Auffassung nach abwegigen - Auffassung der Klägerseite gefolgt, dass schon vor der sog. „Zweitverleihung“ der Rechte einer Körperschaft des öffentlichen Rechtes durch den Freistaat Sachsen für das Gebiet des Freistaates Sachsen das Verhältnis der Behörden des Freistaates zu der Religionsgemeinschaft durch die Verleihung dieser Rechte im Lande Berlin in der Weise gestaltet worden sei (es war von „Ausstrahlung“ die Rede), dass die Behörden des Freistaates sämtliche Tätigkeit von Untergliederungen dieser (in vielen Teilen der Welt tätigen) Religionsgemeinschaft im Freistaat Sachsen als Tätigkeit einer Körperschaft des öffentlichen Rechtes hätte ansehen müssen, so dass namentlich eine datenschutzrechtliche Kontrolle durch die staatlichen Behörden nicht mehr zulässig gewesen sei. Das impliziert die Rechtsauffassung, dass ein Bundesland im Rahmen seiner Landes-Zuständigkeit sein Verhältnis zu einer Organisation in einer Weise und mit der Rechtswirkung ausgestalten kann, dass dadurch genau das entsprechende jeweilige Verhältnis anderer Bundesländer zu der betreffenden Organisation durch denselben Rechtsakt in genau derselben Weise wie in dem betreffenden handelnden Bundesland ausgestaltet ist: Im vorliegenden Falle also mit Wirkung über die Gesetzgebungszuständigkeit des betreffenden Landes hinaus den rechtlichen Status der Religionsgemeinschaft qualifizierend, insbesondere in den anderen Bundesländern die betreffende Organisation dem bundesrechtlichen Zivilrecht entziehend. (Eine ganz andere rechtliche Frage ist, ob eine z. B. im Lande Berlin existierende Körperschaft des öffentlichen Rechtes in einem anderen Bundesland zivilrechtsfähig ist, also z. B. Grundstückseigentümer sein kann.)

Dass dies nicht richtig sein kann, liegt auf der Hand. Allerdings zeigt die von der genannten Kammer des VG Dresden in der mündlichen Verhandlung vorgebrachte

Rechtsmeinung, dass keine Datenschutzaufsichtsbehörde in den Ländern, in denen noch keine Anerkennung der betreffenden Religionsgemeinschaft als Körperschaft des öffentlichen Rechtes stattgefunden hat, sicher darauf vertrauen kann, dass die betreffende Religionsgemeinschaft nicht gegen Kontrollmaßnahmen bei Gericht lediglich wegen eines öffentlich-rechtlichen Status in einem anderen Bundesland Erfolge erzielt.

Darüber hinaus hat die Kammer jegliche durch die kontrollbedingte zeitliche Inanspruchnahme von Funktionsträgern der Religionsgemeinschaft (die erfahrungsgemäß immer in Mehrzahl amtieren und zugegen sind) stattfindende Einwirkung auf deren Beteiligung an (den unter der Woche abendlich stattfindenden) gottesdienstlichen Handlungen als unangemessenen Eingriff in die Freiheit der Religionsausübung angesehen. Das Verwaltungsgericht hat gemeint, die Kontrollen hätten, eben abgesehen von der fehlenden Zuständigkeit, rechtmäßigerweise nur im Anschluss an die gottesdienstlichen Handlungen, also in der Regel ungefähr ab 20:30 Uhr, stattfinden dürfen (statt ab ca. 18:45 Uhr, wie geschehen), wenn sie unangekündigt haben stattfinden sollen. Anlasslosen Kontrollen hat das Gericht im Hinblick auf die Bedeutung der Freiheit der Religionsausübung nahezu gänzlich abweisend gegenübergestanden. Die Bedeutung der Datenschutzkontrolle für die innerreligionsgemeinschaftliche Religionsfreiheit ist vom Gericht nicht akzeptiert worden, ebenso wie mein Hinweis auf die sich abzeichnende EU-rechtliche Unzulässigkeit der Ausnehmung öffentlich-rechtlicher Religionsgemeinschaften von der staatlichen Datenschutzkontrolle (vgl. die Entscheidung des EuGH vom 6. November 2003, C 101/01 - „Lindquist“, RDV 2004, 16 ff., mit Anm. Dammann; Dammann in: Simitis, BDSG, 6. Auflage Rn. 106 zu § 2).

Angesichts der Vehemenz, mit der die Kammer diese beiden Auffassungen zur Frage der Rechtmäßigkeit der seinerzeit vorgenommenen Kontrollen, die ich aufgrund einer Eingabe begonnen hatte und die dann auf eine weitere „Versammlung“ der betreffenden Religionsgemeinschaft ausgedehnt worden waren, habe ich es vorgezogen, die Gelegenheit einer halbwegs gütlichen Einigung zu nutzen, statt gegenüber dem zu erwartenden Urteil die ungewisse Chance eines Berufungsverfahrens wahrzunehmen.

Im Falle der betreffenden Religionsgemeinschaft hat sich die Aufgabe der Aufsichtsbehörde nach § 38 BDSG erledigt, denn diese Religionsgemeinschaft hat inzwischen auch für Sachsen (aber, soweit mir bekannt, noch nicht für alle anderen Bundesländer) den Status einer öffentlich-rechtlichen Körperschaft. Auch für deren gottesdienstliche Handlungen, konkret den Predigtinhalt, gilt aber nicht, dass sie ohne Weiteres grundrechtlich Vorrang vor dem verfassungsrechtlichen Persönlichkeitsrecht genießen: BVerwG, Beschluss v. 8. August 2011 - 7 B 41/11, NVwZ 2011, 1278.

10 Durchsetzung der Rechte und Befugnisse der Aufsichtsbehörde

10.1 Auskunftsrecht

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).

Wenn eine verantwortliche Stelle nach entsprechender Aufforderung und Mahnung ihren Auskunftspflichten gegenüber der Aufsichtsbehörde nicht nachkommt, wird gegen diese Stelle ein förmlicher Auskunftsheranziehungsbescheid erlassen, mittels dessen sie zur Erteilung der bislang nicht erteilten Auskünfte verpflichtet wird. Ein solcher Bescheid ist mit entsprechenden Kosten (Gebühren und Auslagen) verbunden. 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.

Diese Verfahrensweise hat sich grundsätzlich bewährt. Einzuräumen ist zwar, dass sich die Bearbeitungszeit durch die mit dem Heranziehungsbescheid verbundene einmonatige Widerspruchsfrist erheblich verlängert, ganz zu schweigen davon, dass die verantwortliche Stelle dagegen Widerspruch einlegen oder nachfolgend sogar Klage erheben kann, allerdings bestünde die Alternative dazu wohl nur darin, dass auf die geforderten Auskünfte ggf. noch länger gewartet oder sogar ganz verzichtet werden müsste. Nichtsdestoweniger ist aber festzustellen, dass die gewünschten Auskünfte nach den Erfahrungen in dem hier maßgeblichen Berichtszeitraum etwa in der Hälfte der Fälle noch innerhalb der Widerspruchsfrist erteilt worden sind und diese Auskunftserzwingungsverfahren damit in diesem Stadium abgeschlossen werden konnten. Unbenommen bleibt in jedem Fall - jedenfalls solange kein Widerspruch eingelegt worden ist - eine nachträgliche Verfolgung als Ordnungswidrigkeit, da angesichts des vorangegangenen nichtförmlichen Auskunftsersuchens einschließlich der anschließenden Mahnung in jedem Fall ein Verstoß gegen die Pflicht zur *unverzüglichen* Auskunftserteilung vorliegt.

Von den sieben im Berichtszeitraum diesbezüglich eingeleiteten Verfahren sind so die geforderten Auskünfte in drei Fällen bereits nach Erlass des Heranziehungsbescheides erteilt worden; in den anderen vier Fällen musste hierfür ein Zwangsgeld festgesetzt werden. In zumindest einem dieser Fälle ist das Zwangsgeld auch bezahlt worden; gleichzeitig wurde die Auskunft erteilt. Die anderen Verfahren waren zum Ende des

Berichtszeitraumes noch nicht abgeschlossen; teilweise befanden sie sich bezüglich des Zwangsgeldes aber bereits in der Zwangsvollstreckung.

10.2 Anordnungsbefugnis

Zur Gewährleistung der Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz kann die Aufsichtsbehörde Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnen. Bei schwerwiegenden Verstößen oder Mängeln, insbesondere solchen, die mit einer besonderen Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie die Erhebung, Verarbeitung oder Nutzung oder den Einsatz einzelner Verfahren untersagen, wenn die Verstöße oder Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden (§ 38 Abs. 5 Sätze 1 und 2 BDSG).

Seit dem 1. September 2009 ist die Aufsichtsbehörde nicht mehr nur bei technischen oder organisatorischen Mängeln befugt, Maßnahmen zur Mängelbeseitigung anzuordnen, sondern auch dann, wenn die festgestellten Mängel Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten betreffen.

Probleme ergeben sich dabei in der Praxis immer dann, wenn die einzige Möglichkeit der Mängelbeseitigung darin besteht, eine Verarbeitung insgesamt einzustellen. Als Beispiel sei die Videoüberwachung der Schrankenanlage an einem öffentlichen Geh- und Fahrweg durch einen Kleingartenverein genannt. Da der einzige Zweck dieser Videoüberwachung in der unzulässigen Überwachung der Schranke bestand, kam als Mängelbeseitigung nur die Einstellung der Videoüberwachung in Frage. Zu einer solchen Anordnung wäre die Aufsichtsbehörde aber nur bei schwerwiegenden Verstößen (dies kann an dieser Stelle dahingestellt bleiben) und nach vorheriger Aufforderung zur Mängelbeseitigung einschließlich einer Zwangsgeldfestlegung befugt gewesen. Das war aber nicht möglich, da dies bereits der Verfahrensuntersagung gleichgekommen wäre.

11 Ordnungswidrigkeitenverfahren

11.1 Überblick

Als Verwaltungsbehörde nach § 36 Abs. 2 OWiG (§ 13 OWiZuVO) ist der Sächsische Datenschutzbeauftragte zuständig für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 43 BDSG.

Im Berichtszeitraum sind durch den Sächsischen Datenschutzbeauftragten 24 Bußgeldverfahren eingeleitet worden; zwei weitere Verfahren stammten noch aus dem Jahr 2008 (vgl. 4. TB, Pkt. 9.1).

Von den somit im Berichtszeitraum insgesamt 26 anhängigen Verfahren sind neun eingestellt worden, drei befanden sich zum Ende des Berichtszeitraumes noch in der Anhörungsphase.

Damit sind im Berichtszeitraum schließlich 14 Verfahren mit einem Bußgeldbescheid abgeschlossen worden; die Bußgeldsumme belief sich insgesamt auf 24.800 €:

- Mit zwei Bußgeldbescheiden (1.000 € und 10.000 €) wurden Verstöße gegen die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten (§ 43 Abs. 1 Nr. 2 BDSG) geahndet. In einem Fall (10.000 €) ist dagegen Einspruch eingelegt worden; die Entscheidung über diesen Einspruch stand zum Ende des Berichtszeitraumes noch aus.
- Wegen Verletzung der Meldepflichten (Unterlassung der Meldung) ist gegen ein im Bereich der Markt- und Meinungsforschung tätiges Unternehmen ein Bußgeldbescheid über 2.500 € erlassen worden (§ 43 Abs. 1 Nr. 1 BDSG).
- In Werbeschreiben unterlassene Unterrichtungen über das Widerspruchsrecht haben bei einem Einrichtungshaus zu einem Bußgeld in Höhe von 1.500 € geführt (§ 43 Abs. 1 Nr. 3 BDSG).
- Ein Bußgeldbescheid in Höhe von gleichfalls 1.500 € betraf Verstöße gegen die Schriftform und anschließend auch noch gegen die inhaltlichen Vorgaben bei einem Auftragsdatenverarbeitungsvertrag (§ 43 Abs. 1 Nr. 2b BDSG).
- Wegen unbefugter Erhebung oder Verarbeitung (§ 43 Abs. 2 Nr. 1 BDSG) wurden in sieben Fällen Bußgelder verhängt:
  - unterlassene Beräumung (keine Vernichtung von Unterlagen mit personenbezogenen Daten) eines Asylbewerberheimes nach dessen Schließung (2-mal 300 €),
  - Videoüberwachung der Schrankenanlage an einem öffentlichen Geh- und Fahrweg durch einen Kleingartenverein (300 €),

- Videoüberwachung öffentlicher Gehwege vor einem Nachtklub (900 € - nachfolgend allerdings Einstellung durch das Amtsgericht, vgl. Pkt. 11.3),
- Weitergabe der Daten von Versicherungsmaklern an Vertriebspartner zwecks Erschließung neuer Absatzmärkte (500 € - Einspruchrücknahme vor dem Amtsgericht),
- Weitergabe der Bankverbindungsdaten eigener Kunden an einen Auftragnehmer zwecks eigenständigen Einzugs ihm zustehender Servicegelder (750 € - Einspruch durch das Amtsgericht abgewiesen, Rechtsbeschwerde jedoch erfolgreich [ungenügende Sachverhaltsaufklärung durch das Amtsgericht], Ausgang nach Zurückverweisung an das Amtsgericht noch offen),
- Aushang von Listen der bezüglich Krankenstand und Reklamationseingang jeweils „führenden“ 50 Mitarbeiter am Schwarzen Brett (5.000 €).

- Wegen unbefugtem Datenabrufs (§ 43 Abs. 2 Nr. 4 BDSG) wurden in einem Fall zwei Bußgeldbescheide erlassen:
  - unbefugte Einsichtnahme in eine Datei mit Personaldaten im persönlichen Unterverzeichnis eines anderen Mitarbeiters (2-mal 125 € - Einspruch, Entscheidung des Amtsgerichts steht noch aus),

Im 4. Tätigkeitsbericht war unter Pkt. 9.1 berichtet worden, dass in einem mit einer Geldbuße von 750 € geahndeten Fall des Verstoßes gegen die Pflicht zur Bestellung eines Datenschutzbeauftragten nach eingelegtem Einspruch die Entscheidung des zuständigen Amtsgerichts noch aussteht. Inzwischen ist dieser Fall entschieden worden: Der Betroffene hat seinen Einspruch in der mündlichen Verhandlung zurückgenommen.

11.2 Änderung der Justizorganisationsverordnung

Bereits 2008 war nach Regelungen der Sächsischen Justizorganisationsverordnung die Zuständigkeit zur Entscheidung über den Einspruch gegen einen Bußgeldbescheid vom bis dahin zuständigen Amtsgericht Dresden (Amtsgericht am Sitz der Verwaltungsbehörde) auf die Amtsgerichte am jeweiligen Begehungsort übergegangen.

Diese Änderung wird jedenfalls für datenschutzrechtliche Ordnungswidrigkeitenverfahren mit großer Skepsis betrachtet.

Zunächst ist festzuhalten, dass die Anzahl datenschutzrechtlicher Ordnungswidrigkeitenverfahren - etwa im Vergleich zu Ordnungswidrigkeitenverfahren im Verkehrsrecht - sehr klein war. Noch geringer - im einstelligen Bereich - war die Anzahl eingelegter Einsprüche. Selbst das bis Ende 2007 allein zuständige Amtsgericht Dresden war mit datenschutzrechtlichen Ordnungswidrigkeitenverfahren seinerzeit nur sehr selten befasst. Durch die Verteilung der Entscheidungszuständigkeit auf mehrere Amtsgerichte

ist die Bearbeitung derartiger Einsprüche für diese aber noch wesentlich aufwändiger als sie es selbst bei einem allein zuständigen Amtsgericht schon war. Im Einzelfall können Jahre vergehen, bis ein Amtsgericht überhaupt oder wieder einen solchen Fall zu entscheiden hat. Im Ergebnis fehlt es an diesbezüglichen Erfahrungswerten, etwa was die Bedeutung datenschutzrechtlicher Ordnungswidrigkeiten, insbesondere auch die Bemessung der Geldbuße, oder auch die bisherige Vollzugspraxis betrifft. Eine Schwerpunktsetzung / Spezialisierung innerhalb der Amtsgerichte kann dieses Manko - so sie überhaupt sinnvoll möglich ist - daher auch nur bedingt verringern, keinesfalls jedoch beseitigen. Gleiches gilt im Prinzip für die in den jeweiligen Amtsgerichtsbezirken zuständigen Staatsanwaltschaften. Dass dies einer sachgerechten Entscheidung eher abals zuträglich ist, liegt dabei auf der Hand. Nur der Vollständigkeit halber ist zu erwähnen, dass auch für den Sächsischen Datenschutzbeauftragten die Teilnahme an den mündlichen Verhandlungen deutlich zeit- und kostenintensiver ist.

Erfahrungen aus anderen Bundesländern zeigen in diesem Zusammenhang, dass die Rechtsprechung bei einer solchen Zuständigkeitsregelung bei identischen Sachverhalten sehr uneinheitlich, sogar gegensätzlich sein kann und damit den Bestrebungen zur verbesserten Akzeptanz datenschutzrechtlicher Vorschriften zuwiderläuft. Dies betrifft nicht nur die Höhe der letztendlich festgelegten Bußgelder, sondern selbst die Tatsache bzw. Gefahr, dass bei gleicher Aktenlage weitgehend identische Bußgeldbescheide durch ein Amtsgericht aufgehoben, durch ein anderes hingegen bestätigt werden, während wieder andere Amtsgerichte sich für eine Verfahrenseinstellung entschließen könnten.

11.3 Aufhebung von Bußgeldentscheidungen

Kann einem Einspruch nicht abgeholfen werden, wird die Bußgeldakte über die jeweilige Staatsanwaltschaft an das zuständige Amtsgericht abgegeben. Damit verbunden wird die Bitte um Unterrichtung über den Termin der Hauptverhandlung sowie den Ausgang des Verfahrens (§ 76 Abs. 1 Satz 3, Abs. 4 OWiG).

Auch wenn damit die Herrschaft über das Verfahren von der Verwaltungsbehörde auf die Staatsanwaltschaft übergeht, bestehen auch danach für die Verwaltungsbehörde noch gewisse Einflussnahmemöglichkeiten. Dies wäre zum einen eine Sensibilisierung der Staatsanwaltschaft für datenschutzrechtliche Fragen generell bzw. für den betreffenden Einzelfall, da diese wie bereits dargestellt auch nur selten mit datenschutzrechtlichen Verfahren zu tun hat. Abschnitt 272 Abs. 1 RiStBV bestimmt hierzu, dass der Staatsanwalt im Interesse einer sachgerechten Beurteilung und einer gleichmäßigen Behandlung die Belange der Verwaltungsbehörde zu berücksichtigen und sich ihre be-

sondere Sachkunde zunutze zu machen hat. Dies gilt namentlich bei Verstößen gegen Rechtsvorschriften, die nicht zum vertrauten Arbeitsgebiet des Staatsanwalts gehören.

Zum anderen hat die Verwaltungsbehörde natürlich die Möglichkeit der Teilnahme an der Hauptverhandlung. Ist sie dort anwesend - was durch den Sächsischen Datenschutzbeauftragten regelmäßig praktiziert wird - muss ihr dort auf Verlangen das Wort erteilt werden (§ 76 Abs. 1 Satz 4 OWiG). Im Regelfall bieten die Amtsrichter den Vertretern der Verwaltungsbehörde aber schon von sich aus an, die aus ihrer Sicht entscheidungswesentlichen Dinge noch einmal vorzutragen bzw. sich zum bisherigen Ablauf der Hauptverhandlung zu äußern.

Diese Einflussnahmemöglichkeiten laufen jedoch ins Leere, wenn die von der Verwaltungsbehörde erbetenen Unterrichtungen unterbleiben bzw. die (gesetzlich) vorgesehenen Beteiligungsmöglichkeiten der Verwaltungsbehörde vom Gericht und der Staatsanwaltschaft nicht genutzt werden:

Im Fall des wegen unzulässiger Videoüberwachung öffentlicher Gehwege (vgl. auch Pkt. 4.3.1.3 sowie Pkt. 11.1) mit einem Bußgeld in Höhe von 900 € durch die Verwaltungsbehörde abgeschlossenen Verfahrens, wogegen der Betroffene Einspruch erhoben hatte, ist der Verwaltungsbehörde erst viel später auf entsprechende Nachfrage mitgeteilt worden, dass dieses Verfahren - mit Zustimmung der Staatsanwaltschaft – eingestellt worden sei. Als Grund dafür war den Akten zu entnehmen, dass der Betroffene bislang noch nicht in Erscheinung getreten sei, aktiv an der Sachverhaltsaufklärung mitgewirkt und die kritischen Kameras auch entfernt habe.

11.4 Datenschutzrechtliche Einordnung des „Bediensteten-Exzesses“

Es kommt vor, dass Behörden-Bedienstete außerhalb der Erfüllung ihrer dienstlichen Aufgaben, die sich aus dem jeweils durchzuführenden Gesetz, etwa im Bereich des Sozialgesetzbuches für Sozialbehörden oder der Strafprozessordnung für Strafverfolgungsbehörden ergeben, also zu ihrem „Privatvergnügen“, personenbezogene Daten unter Ausnutzung der der Behörde zu Gebote stehenden Datenzugriffsmöglichkeiten - rechtswidrig - erheben. Fälle aus der Praxis sind dienstlich nicht veranlasste Recherchen von Polizeibeamten in polizeilichen Auskunftssystemen oder Zugriffe von Bediensteten von Sozialleistungsträgern auf Meldedaten, die sich auf Kollegen und deren Familienangehörige beziehen.

Es fragt sich dann für die Praxis in meiner Behörde insbesondere, welche Ordnungswidrigkeits-Tatbestände anzuwenden sind; entsprechendes gilt für Strafbarkeits-Tatbestände.

Richtigerweise ist für die Anwendung dieser Vorschriften darauf abzustellen, welchem Anwendungsbereich der handelnde Daten-Verwender zuzuordnen ist. Das ist derjenige Normbereich, der für das Verarbeitungshandeln der Behörde gilt, in welcher der Bedienstete tätig geworden ist, auch wenn er die ihm als Bedienstetem offenstehenden Datenverarbeitungsmöglichkeiten zu gänzlich außerdienstlichen Zwecken genutzt hat. Dies ist die Auffassung der Rechtsprechung (vgl. BGH Urt. v. 22. Juni 2000 - 5 StR 268/99, RDV 2001, 99; OLG Koblenz, Beschl. v. 3. Juni 2008 - 1 Ss 13/08, NJW 2008, 2794, 2795 rSp. unten). Dieser Rechtsauffassung folge ich; der abweichenden Auffassung von Ehmann in Simitis, Rn. 13 bis 15 zu § 43 BDSG ist nicht zu folgen - so sieht dies auch die einhellige Praxis der Datenschutzaufsichtsbehörden in den Bundesländern, soweit sie für die Durchführung von Ordnungswidrigkeitenverfahren zuständig sind.

Diese Auffassung hat zusätzlich den Vorteil, dass sie nicht dazu führt, dass die sanktionsrechtliche Einordnung von der aufsichtsrechtlichen abweicht. Denn es wäre wohl schwerlich richtig, wenn die aufsichtsrechtliche Kontrolle der betreffenden Verarbeitungshandlungen eines solchen Bediensteten der Aufsichtsbehörde für den nicht-öffentlichen Bereich zustünde, wenn also derartige Vorgänge aufsichtsrechtlich durch eine für die Behörde als solche gar nicht sachlich zuständige Datenschutzaufsichtsbehörde durchzuführen wäre.

Kurz: Derartige Vorgänge gehören nicht in den Zuständigkeitsbereich der Aufsichtsbehörde für den nicht-öffentlichen Bereich, also der Aufsichtsbehörde nach § 38 BDSG. (Vgl. auch Abschnitt 10.2.2 des 15. TB für den öffentlichen Bereich).

11.5 Mehrfachzuständigkeit (Internetdienste)

Eine Petentin hatte ihrer Tageszeitung entnommen, dass der Hamburgische Datenschutzbeauftragte ein Bußgeldverfahren gegen ein soziales Netzwerk mit Sitz in den Vereinigten Staaten eingeleitet hatte. Der Tatvorwurf betraf die auch von der Petentin als eigene Erfahrung beschriebene und so vom Hamburgischen Datenschutzbeauftragten vermutete Praxis des Netzwerkes, im Rahmen von Einladungs- und Synchronisierungsfunktionen die E-Mail- und Handy-Adressbücher seiner Nutzer auszuwerten. Dabei sollen auch Daten von Nichtnutzern ohne deren Einwilligung erhoben, langfristig gespeichert und zu Vermarktungszwecken genutzt worden sein. Die Kontaktvorschläge, die das Netzwerk in „Freundschaftseinladungen“ unterbreitet, gaben dem Hamburgischen Datenschutzbeauftragten jedenfalls Anlass zu der Vermutung, die aus den Adressbüchern der Nutzer erhobenen Daten dienten auch zur Erstellung von Beziehungsprofilen von Nichtnutzern.

Auch der Sächsische Datenschutzbeauftragte beobachtet aufmerksam das Geschäftsgebaren des populären Netzwerkes soweit dieses auf in Sachsen belegene Mittel, etwa durch das Setzen von Cookies auf dem Rechner hiesiger Nutzer, technisch zurückgreift und sich das Internetangebot inhaltlich erkennbar ebenso an Adressaten im Freistaat Sachsen richtet. Wegen der Verbreitung des deutschsprachigen Angebots auf alle den dritten Abschnitt des Bundesdatenschutzgesetzes gleichermaßen ausführenden Länder besteht hinsichtlich etwaig zusammenhängender Ordnungswidrigkeiten dabei zunächst eine Verfolgungszuständigkeit jeder einzelnen zur Ahndung von Ordnungswidrigkeiten nach dem Bundesdatenschutzgesetz berufenen Landesbehörde (§ 38 OWiG). Geht man jedoch, was nach hiesiger Auffassung geboten ist, von einer - gegebenenfalls - zumindest durch Fortsetzungszusammenhang zustande kommenden einheitlichen Handlung im Rechtssinne aus, bzw. - gegebenenfalls - einem Dauerdelikt (verübt durch Wirksamwerdenlassen einer bestimmten Programmgestaltung), dann ist infolge der durch den Hamburgischen Datenschutzbeauftragten im Wege der Anhörung zum Ordnungswidrigkeitenvorwurf bereits eingeleiteten ersten Vernehmung allerdings seiner Behörde nach § 39 Abs. 1 Satz 1 OWiG der Vorzug in der örtlichen Zuständigkeit einzuräumen, so dass von einem eigenen Ordnungswidrigkeitenverfahren hinsichtlich des hier in Rede stehenden Sachverhalts abzusehen war. Die Petentin ist jedoch darauf hingewiesen worden, dass es ihr unbenommen sei, den sie betreffenden Sachverhalt der im o. g. Sinne vorzugsweise zuständigen Behörde über deren schon vorhandene allgemeine Kenntnis hinaus auch ihren Einzelfall betreffend zur Kenntnis zu bringen bzw. anzuzeigen.

12 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; darüber hinaus geschieht dies zusätzlich auch im schriftlichen Verfahren. Der Freistaat Sachsen wird im Düsseldorfer Kreis durch den Sächsischen Datenschutzbeauftragten vertreten. 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. 13 dieses Berichts abgedruckt.

Der Sächsische Datenschutzbeauftragte hat den meisten dieser Beschlüsse zugestimmt; lediglich bei folgenden Beschlüssen hat er sich der Stimme enthalten:

- Beschluss des Düsseldorfer Kreises vom 13. Juli 2009: „Unzulässige Übermittlungen von Passagierdaten an britische Behörden verhindern!“
- Beschluss des Düsseldorfer Kreises vom 22. Oktober 2009: „Bonitätsauskünfte über Mietinteressenten nur eingeschränkt zulässig“
- Beschluss des Düsseldorfer Kreises vom 26./27. November 2009: „Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten“

Der Sächsische Datenschutzbeauftragte ist darüber hinaus auch ständiges Mitglied in dessen Arbeitsgruppen „Telekommunikation / Tele- und Mediendienste“, „Beschäftigtendatenschutz“ und „Kreditwirtschaft“. Weitere ständige - es gibt regelmäßig auch noch eine Reihe von Adhoc-Arbeitsgruppen wie im Berichtszeitraum beispielsweise die AG „Elektronisches Lastschriftverfahren“ - Arbeitsgruppen beschäftigen sich intensiv mit den Themenbereichen „Versicherungswirtschaft“, „Internationaler Datenverkehr“ und „Auskunfteien“; eine Beteiligung daran war aufgrund der personellen Ausstattung bisher leider nur in recht beschränktem Ausmaß möglich, obwohl auch 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. 2009 fand der Workshop im Innenministerium von Baden-Württemberg in Stuttgart, 2010 im Innenministerium des Saarlandes in Saarbrücken statt. An beiden Veranstaltungen hat der Sächsische Datenschutzbeauftragte mit eigenen Beiträgen teilgenommen.

13 Beschlüsse des Düsseldorfer Kreises

13.1 Beschlüsse der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 23./24. April 2009 in Schwerin

13.1.1 Datenschutzrechtliche Aspekte des Mitarbeiter-Screenings in international tätigen Unternehmen

Viele Unternehmen sind dazu übergegangen, ihre Mitarbeiter gegenüber Listen abzugleichen, die terrorverdächtige Personen und Organisationen enthalten. Insbesondere Unternehmen, die internationalen Konzernen angehören, werden von ihren teilweise in Drittländern ansässigen Muttergesellschaften hierzu aufgefordert. Letztere stellen auch darüber hinaus gehende Listen z. B. mit gesuchten Personen zur Verfügung, die aufgrund nationaler Vorschriften in den Drittländern einzusetzen sind.

Nach § 4 Abs. 1 BDSG sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Zwar kann § 28 Abs. 1 BDSG eine Rechtsgrundlage im Sinne des BDSG sein, diese Vorschrift kann jedoch für ein Screening nicht herangezogen werden. Der Abgleich mit den Listen dient nicht dem Vertragsverhältnis. Eine Abwägung der Unternehmens- und Betroffeneninteressen führt zu überwiegenden schutzwürdigen Interessen der Betroffenen. Dies gilt insbesondere vor dem Hintergrund, dass die Rechtsstaatlichkeit des Zustandekommens der Listen nachvollziehbar und gesichert sein muss, sowie Rechtsschutzmöglichkeiten bestehen müssen. Angesichts der fehlenden Freiwilligkeit einer solchen Erklärung im Arbeitsverhältnis kann auch das Vorliegen einer Einwilligung eine konkrete Rechtsgrundlage nicht ersetzen.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich stellen daher fest, dass im Geltungsbereich des Bundesdatenschutzgesetzes lediglich solche Listen verwendet werden dürfen, für die eine spezielle Rechtsgrundlage im Sinne des § 4 Abs. 1 BDSG vorliegt.

In diesem Zusammenhang weisen die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich auch auf die Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006 in Magdeburg hin.

13.1.2 Telemarketing bei NGOs

Auch die so genannten NGOs (non-governmental organization), also nichtstaatliche Organisationen die gemeinnützig oder auch als Interessenverbände tätig sind, haben in den

letzten Jahren zunehmend damit begonnen, Telefonmarketing zu betreiben. Beworben werden insbesondere Personen, die schon einmal für die jeweilige NGO gespendet haben. Wenn der Spender seine Telefonnummer in den früheren Kontakten nicht angegeben hat, wird dieses Datum mit Hilfe des Telefonbuches oder einer Telefon-CD ermittelt.

Die Aufsichtsbehörden erklären, dass auch NGOs ohne Einwilligung der Betroffenen nicht zu telefonischer Werbung berechtigt sind. Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu diesem Zweck ist ohne Einwilligung rechtswidrig.

13.2 Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 13. Juli 2009

13.2.1 Unzulässige Übermittlungen von Passagierdaten an britische Behörden verhindern!

Der Düsseldorfer Kreis stellt fest, dass die Übermittlung von Passagierdaten (Ausweis- und Reservierungsdaten) durch Fluggesellschaften in Deutschland an die britischen Zoll- und Sicherheitsbehörden für innereuropäische Flüge unzulässig ist. Die Bundesregierung wird gebeten, entsprechenden Forderungen der britischen Behörden entgegenzutreten.

Großbritannien verlangt im Rahmen des sog. eBorders-Projekts die Erhebung und Übermittlung von Ausweisdaten der Reisenden für innereuropäische Flüge von und nach Großbritannien und die Übermittlung von Daten aus den Reservierungsdatenbanken der Fluggesellschaften. Die britischen Behörden berufen sich bei ihrer Forderung auf die britische Gesetzgebung für Grenzkontrollen. Diese durch das eBorders-Projekt konkretisierte Gesetzgebung berührt einerseits den freien Reiseverkehr in der Europäischen Union. Andererseits bezieht sie sich auf Sachverhalte, die nicht alleine in der Regelungskompetenz des britischen Gesetzgebers liegen, weil sie Datenerhebungen in anderen Mitgliedstaaten der Europäischen Union vorschreibt und Übermittlungen aus Datenbanken verlangt, die sich in anderen Mitgliedstaaten befinden.

Die Übermittlung von Reservierungsdaten der Passagiere an britische Grenzkontrollbehörden, die sich in Datenbanken der verantwortlichen Fluggesellschaften in Deutschland befinden, ist nach deutschem Recht nicht erlaubt. Insbesondere enthält das Bundesdatenschutzgesetz (BDSG) keine Rechtsgrundlage, auf die die Fluggesellschaften die geforderte Übermittlung stützen könnten.

Bereits bei entsprechenden Forderungen der USA, Kanadas und Australiens bestand in Europa Konsens, dass die Übermittlung nicht zur Erfüllung der Flugreiseverträge

erfolgt (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG) und wegen der Zwangslage nicht auf eine Einwilligung (§ 4a BDSG) der Reisenden gestützt werden kann. Sie dient auch nicht den berechtigten Interessen der Fluggesellschaften, die selbst den Forderungen der britischen Behörden entgegentreten, weil sie sich als Reiseunternehmen und nicht als Gehilfen der Grenzkontrollbehörden verstehen. Außerdem besteht ein überwiegendes Interesse der Flugreisenden daran, dass eine Übermittlung ihrer Daten unterbleibt, solange die Vereinbarkeit der britischen Forderung mit vorrangigem europäischen Recht nicht geklärt ist (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG). Schließlich kann eine solche verdachts- oder gefahrunabhängige Übermittlung der Daten aller Reisenden für Sicherheitszwecke nicht auf § 28 Abs. 3 Satz 1 Nr. 2 BDSG gestützt werden, da diese Vorschrift das Vorliegen einer konkreten Gefahr oder Straftat voraussetzt.

Die Übermittlung der Reservierungsdaten ist außerdem verfassungsrechtlich bedenklich und auch fraglich im Hinblick auf die Vereinbarkeit mit der Europäischen Menschenrechtskonvention.

Was die Erhebung von Ausweisdaten anbelangt, gehen die britischen Behörden über die Europäische Richtlinie 2004/82/EG über die Verpflichtung von Beförderungsunternehmen, Angaben über beförderte Personen zu übermitteln, insoweit hinaus, als Daten auch für innereuropäische Flüge erhoben werden sollen. Die Europäische Kommission prüft zurzeit, ob diese einseitige Regelung eine Verletzung der Richtlinie 2004/82/EG darstellt. Jedenfalls dürfte eine solche Maßnahme im Hinblick auf die Freizügigkeit in der Europäischen Union kontraproduktiv sein. Der Düsseldorfer Kreis erwartet, dass die Erhebung und Übermittlung von Pass- und Ausweisdaten für innereuropäische Flüge bis zu einer Bewertung durch die Europäische Kommission unterbleiben.

13.3 Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 22. Oktober 2009

13.3.1 Bonitätsauskünfte über Mietinteressenten nur eingeschränkt zulässig

Häufig holen Vermieter Informationen bei Auskunfteien über die Bonität von Mietinteressenten ein, bevor sie Wohnraum vermieten. Hierfür gelten folgende Anforderungen:

1. Vermieter dürfen erst dann eine Auskunft zu einem Mietinteressenten einholen, wenn der Abschluss des Mietvertrags mit diesem Bewerber nur noch vom positiven Ergebnis einer Bonitätsprüfung abhängt.

2. Es dürfen nur folgende Datenkategorien nach Darlegung eines konkreten berechtigten Interesses an Vermieter übermittelt werden, sofern diese Daten zulässigerweise an die Auskunftei übermittelt bzw. von dieser erhoben wurden:

- Informationen aus öffentlichen Schuldner- und Insolvenzverzeichnissen;

- sonstige Daten über negatives Zahlungsverhalten, bei denen
  - die dem jeweiligen Eintrag zugrunde liegende Forderung noch offen ist oder - sofern sie sich zwischenzeitlich erledigt hat - die Erledigung nicht länger als ein Jahr zurückliegt und
  - eine Bagatellgrenze von insgesamt 1.500 € überschritten wird.

3. Die Übermittlung von Scorewerten an Vermieter ist unzulässig, sofern darin andere als die unter Nummer 2. erwähnten Daten verwendet werden.

4. Vermieter dürfen weitergehende als die unter 2. genannten Daten grundsätzlich auch nicht im Wege einer Einwilligung oder einer Selbstauskunft des Mietinteressenten von einer Auskunftei erheben.

Hintergrund:

Nach § 29 Absatz 2 Nr. 1a Bundesdatenschutzgesetz ist die Erteilung von Bonitätsauskünften nur zulässig, wenn der Vermieter ein berechtigtes Interesse hieran hat und wenn kein Grund zu der Annahme besteht, dass der betroffene Mietinteressent ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Da Vermieter mit dem Abschluss eines Mietvertrages das Risiko eingehen, dass ein Mieter aufgrund von Zahlungsunfähigkeit oder –unwilligkeit den Mietzins oder Nebenkosten nicht begleicht, erkennen die Aufsichtsbehörden an, dass Vermieter aufgrund dieses finanziellen Ausfallrisikos grundsätzlich ein berechtigtes Interesse an einer Bonitätsauskunft über einen Mietinteressenten haben.

Bei der erforderlichen Abwägung sind allerdings auch die schutzwürdigen Belange der Mietinteressenten im Hinblick auf die Bedeutung der Wohnung für die Lebensgestaltung zu berücksichtigen. Ferner ist zu beachten, dass Mietkautionen in Höhe von bis zu drei Monatsmieten, das Vermieterpfandrecht und die bei nachträglicher Zahlungsunfähigkeit vielfach in die Zahlungspflicht eintretenden Sozialbehörden das finanzielle Risiko der Vermieter teilweise reduzieren.

Schließlich ist zu berücksichtigen, dass Auskunfteien an Vermieter nur Bonitätsdaten übermitteln dürfen, die eindeutig Rückschlüsse auf Mietausfallrisiken zulassen. Da das Zahlungsverhalten je nach Vertragsverhältnis unterschiedlich sein kann und teilweise auch ist, lassen zu spät oder nicht gezahlte Kleinbeträge etwa aus Handyverträgen und Internetgeschäften nicht unbedingt einen spezifischen Rückschluss auf die Zahlungsmoral bei Mietverträgen zu.

Aufgrund dieser Erwägungen haben die Aufsichtsbehörden nach Gesprächen mit den Auskunfteien und der Wohnungswirtschaft bereits im Jahr 2004 festgestellt, dass Auskunfteien keine uneingeschränkten Bonitätsauskünfte über Mietinteressenten erteilen dürfen. Vorzuziehen - so der damalige Beschluss - seien branchenspezifische Auskunftssysteme, die auf gesicherte Daten zu negativem Zahlungsverhalten aus öffentlichen Schuldnerverzeichnissen und dem Mietbereich beschränkt sind.

Die eingangs dargelegten Anforderungen berücksichtigen wesentliche Kritikpunkte der Wohnungswirtschaft und der Auskunfteien. So enthält der nunmehr definierte Katalog weder eine Beschränkung auf Daten aus dem Mietbereich noch eine Beschränkung auf titulierte Negativmerkmale. Eine derartige Beschränkung hatten mehrere Aufsichtsbehörden bislang auf Grundlage des Beschlusses aus dem Jahr 2004 gefordert und gegenüber so genannten Mieterwarndateien auch durchgesetzt.

Selbstverständlich dürfen nur Daten, die zulässigerweise bei der Auskunftei eingemeldet wurden, von dieser an Vermieter übermittelt werden. Das heißt, die allgemeinen Einmeldevoraussetzungen, die der Gesetzgeber im neuen § 28a BDSG präzisiert hat und die bereits bisher von den Aufsichtsbehörden gefordert wurden, müssen eingehalten werden.

Die Bagatellgrenze von 1500 € errechnet sich aus drei Monatsmieten der durchschnittlichen Kaltmiete. Nach der jüngsten Einkommens- und Verbrauchsstichprobe des Statistischen Bundesamtes beträgt sie monatlich 515 €.

Auch wenn die Speicher- bzw. Überprüfungsfrist der Auskunfteien bei Forderungen, die nach der Einmeldung beglichen wurden, drei Jahre beträgt (§ 35 Abs. 2 Nr. 4, 2. Halbsatz BDSG neu), ist ein berechtigtes Interesse von Vermietern an der Kenntnis solcher Daten nur für ein Jahr anzuerkennen. Daher ist auch nur innerhalb dieses Zeitraums eine Übermittlung an Vermieter zulässig. Ansonsten wäre dem Schuldner die Eingehung eines Mietverhältnisses unvertretbar erschwert.

Die Unzulässigkeit der Übermittlung von Scorewerten an Vermieter ergibt sich daraus, dass abgesehen von der allgemeinen Problematik der Scoreberechnung im Mietbereich die besondere Problematik besteht, dass die spezifischen Einschränkungen unterlaufen würden, wenn eine Scoreberechnung mit Daten erfolgte, die über den unter Nummer .2 genannten Katalog hinausgehen.

Die Einforderung von unbegrenzten Selbstauskünften oder Einwilligungen zur Einholung weit gefasster Auskünfte vom Mietinteressenten würde eine Umgehung der sich aus der Abwägung nach § 29 BDSG ergebenden gesetzlichen Begrenzungen darstellen, was demzufolge nicht zulässig ist.

Die bisherige Praxis der Auskunfteien entsprach den hier gestellten Anforderungen nicht bzw. nicht in ausreichendem Maße. Obwohl den Auskunfteien ausdrücklich die Möglichkeit eingeräumt wurde, ggf. alternative Lösungen zu den im Beschluss genannten Anforderungen zu entwickeln, die auf das jeweilige Geschäftsmodell der Auskunfteien und deren speziellen Datenbestand zugeschnitten sind, haben die Auskunfteien diese Möglichkeit bislang nicht genutzt.

Die Aufsichtsbehörden haben in Gesprächen mit den Auskunfteien angekündigt, dass sie bei datenschutzwidrigen Übermittlungen ggf. aufsichtsrechtliche Maßnahmen ergreifen werden.

13.4 Beschlüsse der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 26./27. November 2009 in Stralsund

13.4.1 Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten

Viele Web-Seitenbetreiber analysieren zu Zwecken der Werbung und Marktforschung oder bedarfsgerechten Gestaltung ihres Angebotes das Surf-Verhalten der Nutzerinnen und Nutzer. Zur Erstellung derartiger Nutzungsprofile verwenden sie vielfach Software bzw. Dienste, die von Dritten kostenlos oder gegen Entgelt angeboten werden.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen darauf hin, dass bei Erstellung von Nutzungsprofilen durch Web-Seitenbetreiber die Bestimmungen des Telemediengesetzes (TMG) zu beachten sind. Demnach dürfen Nutzungsprofile nur bei Verwendung von Pseudonymen erstellt werden. Die IP-Adresse ist kein Pseudonym im Sinne des Telemediengesetzes.

Im Einzelnen sind folgende Vorgaben aus dem TMG zu beachten:

- Den Betroffenen ist eine Möglichkeit zum Widerspruch gegen die Erstellung von Nutzungsprofilen einzuräumen. Derartige Widersprüche sind wirksam umzusetzen.
- Die pseudonymisierten Nutzungsdaten dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. Sie müssen gelöscht werden, wenn ihre Speicherung für die Erstellung der Nutzungsanalyse nicht mehr erforderlich ist oder der Nutzer dies verlangt.
- Auf die Erstellung von pseudonymen Nutzungsprofilen und die Möglichkeit zum Widerspruch müssen die Anbieter in deutlicher Form im Rahmen der Datenschutzerklärung auf ihrer Internetseite hinweisen.

- Personenbezogene Daten eines Nutzers dürfen ohne Einwilligung nur erhoben und verwendet werden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Jede darüber hinausgehende Nutzung bedarf der Einwilligung der Betroffenen.
- Die Analyse des Nutzungsverhaltens unter Verwendung vollständiger IP-Adressen (einschließlich einer Geolokalisierung) ist aufgrund der Personenbeziehbarkeit dieser Daten daher nur mit bewusster, eindeutiger Einwilligung zulässig. Liegt eine solche Einwilligung nicht vor, ist die IP-Adresse vor jeglicher Auswertung so zu kürzen, dass eine Personenbeziehbarkeit ausgeschlossen ist.

Werden pseudonyme Nutzungsprofile durch einen Dienstleister erstellt, sind darüber hinaus die Vorgaben des Bundesdatenschutzgesetzes zur Auftragsdatenverarbeitung durch die Anbieter einzuhalten.

13.4.2 Keine Internetveröffentlichung sportgerichtlicher Entscheidungen

Entgegen der Auffassung des OLG Karlsruhe in seinem Urteil vom 30. Januar 2009 gehen die zuständigen Aufsichtsbehörden in Anwendung des BDSG davon aus, dass die uneingeschränkt zugängliche Veröffentlichung von sportgerichtlichen Entscheidungen im Internet unzulässig ist. Entsprechendes gilt auch für die Veröffentlichung von personenbezogenen Sperrlisten.

Eine Veröffentlichung in geschlossenen Benutzergruppen ist zulässig, wenn gewährleistet ist, dass in den Vereinen nur zuständige Personen zugreifen können. Soweit der Personenbezug nicht erforderlich ist, sind sportgerichtliche Entscheidungen zu anonymisieren.

Bei der mit der Veröffentlichung im Internet verbundenen Datenübermittlung an Dritte wird der Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen meist deswegen als besonders gravierend empfunden, weil hierdurch nicht nur ein weltweiter Zugriff auf die Daten, sondern darüber hinaus vor allem eine elektronische Recherchierbarkeit ermöglicht wird, welche auch zur Erstellung eines Persönlichkeitsprofils genutzt werden kann.

Der beabsichtigten „Prangerwirkung“ mit Abschreckungsfunktion könnte bereits dadurch Genüge getan werden, dass entsprechende Ahndungen organisations-/verbandsintern in zugriffsgeschützten Internetforen „für die, die es angeht“, publizieren würden. Die intendierte Information der Öffentlichkeit über das Vorgehen gegen Rechtsverstöße könnte ohne Personenbezug im Rahmen einer Ahndungsstatistik erfolgen.

13.4.3 Gesetzesänderung bei der Datenverwendung für Werbezwecke

Vom 1. September 2009 an gelten nach § 28 Abs. 3 BDSG neue Datenschutzregelungen bei der Datenverwendung für Werbezwecke. Diese Regelungen gelten spätestens ab dem 31. August 2012, jedoch sofort für Daten, die nach dem 1. September 2009 erhoben oder von einer Stelle erstmalig gespeichert werden.

Die Datenschutzaufsichtsbehörden weisen darauf hin, dass für Daten, deren erstmalige Speicherung nicht eindeutig erkennbar ist, die neuen Regelungen angewendet werden. Sie weisen weiterhin darauf hin, dass eine Übermittlung für Werbezwecke nur zulässig ist, wenn Herkunft der Daten und Empfänger gespeichert werden und eine Gruppenauswahl nach einem Merkmal erfolgt (Listenübermittlung). Bei der Werbemaßnahme muss die erstmalig erhebende Stelle den Adressaten mitgeteilt werden. Die bisher weit verbreitete Praxis der Übermittlung von nach mehr als einem Merkmal selektierten Adressen ist unzulässig, wenn keine Einwilligung vorliegt.

13.5 Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 28./29. April 2010 in Hannover

13.5.1 Prüfung der Selbst-Zertifizierung des Datenimporteurs nach dem Safe Harbor-Abkommen durch das Daten exportierende Unternehmen

Seit dem 26. Juli 2000 besteht eine Vereinbarung zwischen der EU und dem Handelsministerium (Department of Commerce) der USA zu den Grundsätzen des sog. „sicheren Hafens“ (Safe Harbor)[1]. Diese Vereinbarung soll ein angemessenes Datenschutzniveau bei US-amerikanischen Unternehmen sicherstellen, indem sich Unternehmen auf die in der Safe Harbor-Vereinbarung vorgegebenen Grundsätze verpflichten. Durch die Verpflichtung und eine Meldung an die Federal Trade Commission (FTC) können sich die Unternehmen selbst zertifizieren. So zertifizierte US-Unternehmen schaffen damit grundsätzlich die Voraussetzungen, dass eine Übermittlung personenbezogener Daten aus Europa an sie unter denselben Bedingungen möglich ist, wie Übermittlungen innerhalb des europäischen Wirtschaftsraumes (EU/EWR). Das US-Handelsministerium veröffentlicht eine Safe Harbor-Liste aller zertifizierten Unternehmen im Internet.

[1] Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. L 215 vom 25.8.2000, S. 7.

Solange eine flächendeckende Kontrolle der Selbstzertifizierungen US-amerikanischer Unternehmen durch die Kontrollbehörden in Europa und den USA nicht gewährleistet ist, trifft auch die Unternehmen in Deutschland eine Verpflichtung, gewisse Mindestkriterien zu prüfen, bevor sie personenbezogene Daten an ein auf der Safe Harbor-Liste geführtes US-Unternehmen übermitteln.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen in diesem Zusammenhang darauf hin, dass sich Daten exportierende Unternehmen bei Übermittlungen an Stellen in die USA nicht allein auf die Behauptung einer Safe Habor-Zertifizierung des Datenimporteurs verlassen können. Vielmehr muss sich das Daten exportierende Unternehmen nachweisen lassen, dass die Safe Harbor-Selbstzertifizierungungen vorliegen und deren Grundsätze auch eingehalten werden. Mindestens muss das exportierende Unternehmen klären, ob die Safe Habor-Zertifizierung des Importeurs noch gültig ist. Außerdem muss sich das Daten exportierende Unternehmen nachweisen lassen, wie das importierende Unternehmen seinen Informationspflichten nach Safe Harbor[2] gegenüber den von der Datenverarbeitung Betroffenen nachkommt. Dies ist auch nicht zuletzt deshalb wichtig, damit das importierende Unternehmen diese Information an die von der Übermittlung Betroffenen weitergeben kann.

Diese Mindestprüfung müssen die exportierenden Unternehmen dokumentieren und auf Nachfrage der Aufsichtsbehörden nachweisen können. Sollten nach der Prüfung Zweifel an der Einhaltung der Safe Harbor-Kriterien durch das US-Unternehmen bestehen, empfehlen die Aufsichtsbehörden, der Verwendung von Standard-Vertragsklauseln oder bindenden Unternehmensrichtlinien zur Gewährleistung eines angemessenen Datenschutzniveaus beim Datenimporteur den Vorzug zu geben.

Stellt ein Daten exportierendes Unternehmen bei seiner Prüfung fest, dass eine Zertifizierung des importierenden Unternehmens nicht mehr gültig ist oder die notwendigen Informationen für die Betroffenen nicht gegeben werden, oder treten andere Verstöße gegen die Safe Harbor-Grundsätze zu Tage, sollte außerdem die zuständige Datenschutzaufsichtsbehörde informiert werden.

---

[2] Informationspflicht: Die Organisation muss Privatpersonen darüber informieren, zu welchem Zweck sie die Daten über sie erhebt und verwendet, wie sie die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können, an welche Kategorien von Dritten die Daten weitergegeben werden und welche Mittel und Wege sie den Privatpersonen zur Verfügung stellt, um die Verwendung und Weitergabe der Daten einzuschränken. Diese Angaben sind den Betroffenen unmissverständlich und deutlich erkennbar zu machen, wenn sie erstmalig gebeten werden, der Organisation personenbezogene Daten zu liefern, oder so bald wie möglich danach, auf jeden Fall aber bevor die Organisation die Daten zu anderen Zwecken verwendet als denen, für die sie von der übermittelnden Organisation ursprünglich erhoben oder verarbeitet wurden, oder bevor sie die Daten erstmalig an einen Dritten weitergibt.

Eine Schlüsselrolle im Hinblick auf die Verbesserung der Einhaltung der Grundsätze kommt dabei der Zusammenarbeit der FTC mit den europäischen Datenschutzbehörden zu. Hierfür ist es erforderlich, dass die FTC und die europäischen Datenschutzbehörden die Kontrolle der Einhaltung der Safe Harbor-Grundsätze intensivieren. Die mit der Safe Harbor-Vereinbarung beabsichtigte Rechtssicherheit für den transatlantischen Datenverkehr kann nur erreicht werden, wenn die Grundsätze auch in der Praxis effektiv durchgesetzt werden.

13.6 Beschlüsse der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 24./25. November 2010 in Düsseldorf

13.6.1 Datenschutz im Verein: Umgang mit Gruppenversicherungsverträgen

Bei sog. Gruppenversicherungsverträgen handelt es sich um Rahmenverträge zwischen Vereinen/Verbänden und Versicherungsunternehmen, die den Mitgliedern unter bestimmten Voraussetzungen den Abschluss von Einzelversicherungsverträgen zu günstigeren als den üblichen Konditionen ermöglichen.

Werden für die Werbung zum Abschluss solcher Verträge personenbezogene Daten der Mitglieder an ein Versicherungsunternehmen übermittelt, setzt dies die Einwilligung der Betroffenen voraus.

In Bezug auf Altmitglieder wurde bisher eine Information mittels Avisschreibens mit der Möglichkeit des Widerspruchs für ausreichend gehalten. Die Aufsichtsbehörden stellen fest, dass auch für Altmitglieder die vorherige Einholung einer informierten Einwilligungserklärung erforderlich ist.

13.6.2 Minderjährige in sozialen Netzwerken wirksamer schützen

Soziale Netzwerke spielen in unserer Lebenswirklichkeit eine zunehmend wichtige Rolle. Minderjährige beteiligen sich in großer Zahl an solchen Netzen. Ihrer besonderen Schutzbedürftigkeit muss über die Anforderungen hinaus Rechnung getragen werden, die grundsätzlich an eine datenschutzgerechte Ausgestaltung solcher Angebote zu stellen sind (vgl. Beschluss des Düsseldorfer Kreises vom 18. April 2008). Hier besteht ein erheblicher Schutz-, Aufklärungs- und Informationsbedarf:

- Das Schutzniveau sozialer Netzwerke wird wesentlich dadurch bestimmt, dass die Betreiber Standardeinstellungen vorgeben, z. B. für die Verfügbarkeit von Profildaten für Dritte. Minderjährige Nutzer haben häufig weder die Kenntnisse noch das Problembewusstsein, um solche Voreinstellungen zu ändern. Die Auf-

sichtsbehörden fordern die Anbieter sozialer Netzwerke auf, generell datenschutzfreundliche Standardeinstellungen für ihre Dienste zu wählen, durch welche die Privatsphäre der Nutzer möglichst umfassend geschützt wird. Diese Standardeinstellungen müssen besonders restriktiv gefasst werden, wenn sich das Portal an Minderjährige richtet oder von ihnen genutzt wird.

- Es muss erreicht werden, dass die gesetzlich bzw. durch die Betreiber vorgegebenen Grenzen für das Mindestalter der Nutzer eingehalten und wirksam überprüft werden. Dies könnte durch die Entwicklung und den Einsatz von Altersverifikationssystemen oder Bestätigungslösungen gelingen. Solche Verifikationssysteme lösen zwar ihrerseits Datenverarbeitungsvorgänge aus und müssen berücksichtigen, dass die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym möglich bleiben muss (§ 13 Abs. 6 Telemediengesetz); dies begründet aber kein Hindernis für ihren Einsatz.
- Minderjährigen und ihren Eltern wird die Einschätzung, welche der angebotenen Dienste sozialer Netzwerke altersgerecht sind, wesentlich erleichtert, wenn die Betreiber eine freiwillige Alterskennzeichnung von Internetinhalten vornehmen. Denkbar ist auch der Einsatz von Jugendschutzprogrammen, die Alterskennzeichnungen automatisch auslesen und für Minderjährige ungeeignete Inhalte sperren. Die Möglichkeiten, die der Entwurf für einen neuen Jugendmedienschutz-Staatsvertrag hierzu anbietet, müssen intensiv genutzt werden.
- Ebenso wichtig ist die Bewusstseinsbildung bei den minderjährigen Nutzem sozialer Netzwerke für die Nutzungsrisiken und für einen sorgsamen und verantwortungsbewussten Umgang mit den eigenen Daten und den respektvollen Umgang mit den Daten anderer. Die Betreiber sozialer Netzwerke, aber auch staatliche Behörden, Schulen und nicht zuletzt die Eltern stehen in der Pflicht, über bestehende datenschutzfreundliche Nutzungsmöglichkeiten aufzuklären.

13.6.3 Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f Abs. 2 und 3 Bundesdatenschutzgesetz (BDSG)

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben bei der Kontrolle verantwortlicher Stellen festgestellt, dass Fachkunde und Rahmenbedingungen für die Arbeit der Beauftragten für den Datenschutz (DSB) in den verantwortlichen Stellen angesichts zunehmender Komplexität automatisierter Verfahren zum Umgang mit personenbezogenen Daten nicht durchgängig den Anforderungen des BDSG genügen.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen darauf hin, dass die Aus- und Belastung der DSB maßgeblich beeinflusst wird durch

die Größe der verantwortlichen Stelle, die Anzahl der zu betreuenden verantwortlichen Stellen, Besonderheiten branchenspezifischer Datenverarbeitung und den Grad der Schutzbedürftigkeit der zu verarbeitenden personenbezogenen Daten. Veränderungen bei den vorgenannten Faktoren führen regelmäßig zu einer proportionalen Mehrbelastung der DSB.

Nachfolgende Mindestanforderungen sind zu gewährleisten:

I. Erforderliche Fachkunde gemäß § 4f Abs. 2 Satz 1 BDSG

§ 4 f Abs. 2 Satz 1 BDSG legt fest, dass zum Beauftragten für den Datenschutz (DSB) nur bestellt werden darf, wer die erforderliche Fachkunde und Zuverlässigkeit besitzt. Weitere Ausführungen dazu enthält das Gesetz nicht. Vor dem Hintergrund der gestiegenen Anforderungen an die Funktion des DSB müssen diese mindestens über folgende datenschutzrechtliche und technisch-organisatorische Kenntnisse verfügen:

1. Datenschutzrecht allgemein - unabhängig von der Branche und der Größe der verantwortlichen Stelle

- Grundkenntnisse zu verfassungsrechtlich garantierten Persönlichkeitsrechten der Betroffenen und Mitarbeiter der verantwortlichen Stelle und
- umfassende Kenntnisse zum Inhalt und zur rechtlichen Anwendung der für die verantwortlichen Stellen einschlägigen Regelungen des BDSG, auch technischer und organisatorischer Art,
- Kenntnisse des Anwendungsbereiches datenschutzrechtlicher und einschlägiger technischer Vorschriften, der Datenschutzprinzipien und der Datensicherheitsanforderungen insbesondere nach § 9 BDSG.

2. Branchenspezifisch - abhängig von der Branche, Größe oder IT-Infrastruktur der verantwortlichen Stelle und der Sensibilität der zu verarbeitenden Daten

- Umfassende Kenntnisse der spezialgesetzlichen datenschutzrelevanten Vorschriften, die für das eigene Unternehmen relevant sind,
- Kenntnisse der Informations- und Telekommunikationstechnologie und der Datensicherheit (physische Sicherheit, Kryptographie, Netzwerksicherheit, Schadsoftware und Schutzmaßnahmen, etc.),
- betriebswirtschaftliche Grundkompetenz (Personalwirtschaft, Controlling, Finanzwesen, Vertrieb, Management, Marketing etc.),

- Kenntnisse der technischen und organisatorischen Struktur sowie deren Wechselwirkung in der zu betreuenden verantwortlichen Stelle (Aufbau- und Ablaufstruktur bzw. Organisation der verantwortlichen Stelle) und
- Kenntnisse im praktischen Datenschutzmanagement einer verantwortlichen Stelle (z. B. Durchführung von Kontrollen, Beratung, Strategieentwicklung, Dokumentation, Verzeichnisse, Logfile-Auswertung, Risikomanagement, Analyse von Sicherheitskonzepten, Betriebsvereinbarungen, Videoüberwachungen, Zusammenarbeit mit dem Betriebsrat etc.).

Grundsätzlich müssen die erforderlichen rechtlichen, technischen sowie organisatorischen Mindestkenntnisse **bereits zum Zeitpunkt des Bestellung** zum DSB im ausreichenden Maße vorliegen. Sie können insbesondere auch durch den Besuch geeigneter Aus- und Fortbildungsveranstaltungen und das Ablegen einer Prüfung erlangt sein. Um eventuell zu Beginn der Bestellung noch bestehende Informationsdefizite auszugleichen, empfiehlt sich der Besuch von geeigneten Fortbildungsveranstaltungen. Der Besuch solcher Veranstaltungen ist auch nach der Bestellung angezeigt, um auf dem aktuellen, erforderlichen Informationsstand zu bleiben, und um sich Kenntnisse über die sich ändernden rechtlichen und technischen Entwicklungen anzueignen.

II. Anforderungen an die Unabhängigkeit der/des Beauftragten gem. § 4f Abs. 3 BDSG

Gemäß § 4f Abs. 3 Satz 2 BDSG sind DSB in Ausübung ihrer Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Um die Unabhängigkeit der DSB zu gewährleisten, sind eine Reihe betriebsinterner organisatorischer Maßnahmen erforderlich:

1. DSB sind dem Leiter/der Leiterin der verantwortlichen Stelle organisatorisch unmittelbar zu unterstellen (§ 4f Abs. 3 Satz 1 BDSG). Sie müssen in der Lage sein, ihre Verpflichtungen ohne Interessenkonflikte erfüllen zu können. Dieses ist durch entsprechende Regelungen innerhalb der verantwortlichen Stelle bzw. vertragliche Regelungen sicher zu stellen und sowohl innerhalb der verantwortlichen Stelle als auch nach außen hin publik zu machen. Den DSB ist ein unmittelbares Vortragsrecht beim Leiter der Stelle einzuräumen.

2. DSB dürfen wegen der Erfüllung ihrer Aufgaben in Hinblick auf ihr sonstiges Beschäftigungsverhältnis, auch für den Fall, dass die Bestellung zum DSB widerrufen wird, nicht benachteiligt werden (vgl. § 4f Abs. 3 Satz 3 ff BDSG). Analog muss bei der Bestellung von externen DSB der Dienstvertrag so ausgestaltet sein, dass eine unabhängige Erfüllung der gesetzlichen Aufgaben durch entsprechende Kündigungsfristen, Zahlungsmodalitäten, Haftungsfreistellungen und Dokumentationspflichten

gewährleistet wird. § 4f Abs. 3 BDSG schränkt insoweit die grundsätzliche Vertragsfreiheit ein. Empfohlen wird grundsätzlich eine Mindestvertragslaufzeit von 4 Jahren, bei Erstverträgen wird wegen der Notwendigkeit der Überprüfung der Eignung grundsätzlich eine Vertragslaufzeit von 1 - 2 Jahren empfohlen.

3. Datenschutzbeauftragte sind zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit sie nicht davon durch die Betroffenen befreit wurden. Dies gilt auch gegenüber der verantwortlichen Stelle und deren Leiter (§ 4f Abs. 4 BDSG).

III. Erforderliche Rahmenbedingungen innerhalb der verantwortlichen Stelle zur Fachkunde und Unabhängigkeit des DSB

1. Die Prüfpflichten der DSB (vgl. § 4g BDSG) setzen voraus, dass ihnen die zur Aufgabenerfüllung erforderlichen Zutritts- und Einsichtsrechte in alle betrieblichen Bereiche eingeräumt werden.

2. DSB müssen in alle relevanten betrieblichen Planungs- und Entscheidungsabläufe eingebunden werden. Sie führen das Verfahrensverzeichnis (§ 4g Abs. 2 BSDG) und haben hierfür die erforderlichen Unterlagen zu erhalten.

3. Zur Erhaltung der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde haben die verantwortlichen Stellen den DSB die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen. Bei der Bestellung von externen DSB kann die Fortbildung Bestandteil der vereinbarten Vergütung sein und muss nicht zusätzlich erbracht werden.

4. Internen DSB muss die erforderliche Arbeitszeit zur Erfüllung ihrer Aufgaben und zur Erhaltung ihrer Fachkunde zur Verfügung stehen. Bei Bestellung eines externen DSB muss eine bedarfsgerechte Leistungserbringung gewährleistet sein. Sie muss in angemessenem Umfang auch in der beauftragenden verantwortlichen Stelle selbst erbracht werden. Ein angemessenes Zeitbudget sollte konkret vereinbart und vertraglich festgelegt sein.

5. Die verantwortlichen Stellen haben den DSB bei der Erfüllung ihrer Aufgaben insbesondere durch die zur Verfügungstellung von Personal, Räumen, Einrichtung, Geräten und Mitteln zu unterstützen (§ 4f Abs. 5 BDSG).

13.6.4 Umsetzung der Datenschutzrichtlinie für elektronische Kommunikationsdienste

Gegenwärtig wird über die Umsetzung der überarbeiteten Datenschutzrichtlinie für elektronische Kommunikationsdienste („ePrivacy Directive“) in nationales Recht beraten, die bis zum 24. Mai 2011 abgeschlossen sein muss. Die Richtlinie enthält in ihrem Artikel 5 Absatz 3 eine Regelung, die die datenschutzrechtlichen Voraussetzungen auch beim Umgang mit „cookies“ neu festlegt: Die bisherige Opt-Out-Lösung wird durch eine Opt-In-Lösung mit einer vorherigen umfassenden Information über die Zwecke der Verarbeitung ersetzt. Durch die Änderung der Richtlinie wird nun eine Anpassung des Telemediengesetzes hin zu einer informierten Einwilligung erforderlich, da im geltenden Telemediengesetz eine Widerspruchslösung umgesetzt ist (§ 15 Abs. 3 TMG).

Eine solche Änderung stößt auf erhebliche Widerstände auf Seiten des zuständigen Ministeriums, das eine Einwilligungslösung schon durch die in § 12 Abs. 1 und 2 TMG definierten allgemeinen Grundsätze realisiert sieht. Würde man dieser Auslegung folgen, müsste eine „alte“ Vorschrift zukünftig in „neuer“, zudem auch strengerer Weise ausgelegt und angewendet werden. Dies wäre nur schwer vermittelbar und möglicherweise kaum durchsetzbar.

Die Datenschutz-Aufsichtsbehörden betrachten bei ihrer Kontroll- und Aufsichtstätigkeit im Bereich der Telemedien § 15 Abs. 3 TMG als einschlägig für die Verwendung von „cookies“ in diesem Zusammenhang. Demnach sind Nutzungsprofile nur unter Verwendung eines Pseudonyms und vorbehaltlich eines Widerspruchs des Betroffenen zulässig. Nutzungsprofile werden in der Regel mit Hilfe von „cookies“ erstellt, die im „cookie“ gespeicherte eindeutige Identifikationsnummer (cookie-ID) wird entsprechend als Pseudonym angesehen. Diese Auslegung hat sich in der Praxis bewährt und wird allgemein anerkannt.

Die Umsetzung der „ePrivacy Directive“ erfordert daher eine gesetzliche Anpassung des TMG.