Sächsischer Landtag
5. Wahlperiode

DRUCKSACHE 5/13032

Schutz des Persönlichkeitsrechts im nicht-öffentlichen Bereich

6. Tätigkeitsbericht

des

Sächsischen Datenschutzbeauftragten

Berichtszeitraum: 1. Januar 2011 bis 31. März 2013

Dem Sächsischen Landtag

vorgelegt zum 31. März 2013

gemäß § 30 des Sächsischen Datenschutzgesetzes

Eingegangen am: 12. Dezember 2013 Ausgegeben am: 12. Dezember 2013

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: 0351/493-5401
Fax: 0351/493-5490

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
AEO	Authorized Economic Operator (Zugelassener Wirtschaftsbeteiligter)
AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
AO	Abgabenordnung
ARGE	Arbeitsgemeinschaft (ehemalige Bezeichnung für die Jobcenter)
Aufl.	Auflage
Az.	Aktenzeichen
BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BewachV	Bewachungsverordnung
BFH	Bundesfinanzhof
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
BMV-Ä	Bundesmantelverträge - Teil A: Ärzte
BO	Berufsordnung
BUrlG	Bundesurlaubsgesetz
DOI	Double Opt In
DSL	Digital Subscriber Line (Digitaler Teilnehmeranschluss)
DV	Datenverarbeitung
EC	Electronic Cash
EDV	Elektronische Datenverarbeitung
Erfa-Kreis	Erfahrungsaustausch-Kreis
EU	Europäische Union
GbR	Gesellschaft bürgerlichen Rechts
GDD	Gesellschaft für Datenschutz und Datensicherung e.V.

GewO	Gewerbeordnung
GG	Grundgesetz
GmbH	Gesellschaft mit beschränkter Haftung
GPS	Global Positioning System
HGB	Handelsgesetzbuch
HIS	Hinweis- und Informationssystem der Versicherungswirtschaft
IfSG	Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten (Infektionsschutzgesetz)
InsO	Insolvenzordnung
InsoBekV	Verordnung zu öffentlichen Bekanntmachungen in Insolvenz-verfahren im Internet
IT	Informationstechnik
KG	Kommanditgesellschaft
KG	Kammergericht
KunstUrhG	Kunsturheberrechtsgesetz
KV	Kassenärztliche Vereinigung
LAG	Landesarbeitsgericht
LDA	Bayerisches Landesamt für Datenschutzaufsicht (Ansbach)
LG	Landgericht
MRT	Magnetresonanztomographie
NFC	Near Field Communication (Nahfeldkommunikation)
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
OWiG	Ordnungswidrigkeitengesetz
OWiZuVO	Ordnungswidrigkeiten-Zuständigkeitsverordnung
PartG	Parteiengesetz
PIN	Persönliche Identifikationsnummer
RDG	Rechtsdienstleistungsgesetz
Rdnr.	Randnummer
RDV	Recht der Datenverarbeitung
RöV	Röntgenverordnung
RStV	Rundfunkstaatsvertrag

SächsDSG	Sächsisches Datenschutzgesetz
SächsHKaG	Sächsisches Heilberufekammergesetz
SächsKitaG	Sächsisches Gesetz zur Förderung von Kindern in Tageseinrichtungen
SB	Selbstbedienung
SGB	Sozialgesetzbuch
SLÄK	Sächsische Landesärztekammer
SMS	Short Message Service (Kurznachrichtendienst)
StGB	Strafgesetzbuch
StVG	Straßenverkehrsgesetz
TB	Tätigkeitsbericht
TFG	Transfusionsgesetz
TKG	Telekommunikationsgesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
VG	Verwaltungsgericht
VwVfG	Verwaltungsverfahrensgesetz
WEG	Wohnungseigentumsgesetz
ZPO	Zivilprozessordnung

Vorwort

Der nunmehr sechste Tätigkeitsbericht der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich im Freistaat Sachsen weist eine Besonderheit auf. Anders als die vorangegangenen Berichte erstreckt er sich nicht über zwei Kalenderjahre, sondern geht mit dem Berichtszeitraum 1. Januar 2011 bis 31. März 2013 drei Monate darüber hinaus. Grund ist eine Änderung des Sächsischen Datenschutzgesetzes: Am 29. Juni 2011 hat der Sächsische Landtag in zweiter Lesung das „Zweite Gesetz zur Änderung des Sächsischen Datenschutzgesetzes“ beschlossen, welches u. a. auch eine Veränderung bzgl. des Berichtszeitraums bedingt. In § 30 Abs. 1 Satz 1 SächsDSG ist seitdem verankert, dass ich auch als Aufsichtsbehörde nach § 30a SächsDSG dem Sächsischen Landtag alle zwei Jahre jeweils zum 31. März einen Tätigkeitsbericht vorzulegen habe. In den Folgejahren werde ich dann wieder zum gewohnten Zweijahresrhythmus zurückkehren, dann allerdings nicht mehr kalenderjahrbezogen, sondern im Gleichklang mit dem öffentlichen Bereich über einen Zeitraum vom 1. April bis zum 31. März des übernächsten Jahres berichten.

Der vorliegende Bericht weist wiederum eine deutliche Steigerung sowohl bei den durchgeführten anlassbedingten Kontrollen als auch bei den eingegangenen Beratungsanliegen aus. Der besseren Vergleichbarkeit wegen auf einen Zweijahreszeitraum heruntergebrochen ist festzustellen, dass sich die Anzahl meiner auf konkrete Anhaltspunkte für einen Datenschutzverstoß zurückzuführende (Anlass-)Kontrollen um 24 % erhöht hat (absolut sogar um 40 %). Im Beratungsbereich ergibt sich fast ein identisches Bild. Hier habe ich bezogen auf einen Zweijahreszeitraum 25 % (absolut: 40 %) mehr Anfragen erhalten. Daneben haben meine Mitarbeiter immerhin auch noch sieben, d. h. fünf mehr als im vorangegangen Berichtszeitraum, umfangreichere anlassfreie Kontrollen, in erster Linie im Bereich der Wirtschaftsauskunfteien, durchgeführt.

Meine Personalausstattung hat sich leider vollkommen entgegengesetzt entwickelt. Im Berichtszeitraum fiel eine Stelle des höheren Dienstes im für die Datenschutzaufsicht im nicht-öffentlichen Bereich zuständigen Referat weg. Die tatsächliche Arbeitsbelastung meiner Mitarbeiter ist also in erheblich größerem Maße gestiegen, als das die oben beispielhaft erwähnten Zahlen wiedergeben. Tatsächlich konnte ich dieses Arbeitspensum u. a. nur bewältigen, weil mir über einen längeren Zeitraum eine sehr engagierte und fähige Praktikantin (!) zur Verfügung stand und mich bei meinen großen Kontrollaktionen im Bereich der Videoüberwachung (vgl. Pkt. 8.1.3) und der Auftragsdatenverarbeitung (vgl. Pkt. 4.2.2) sowie den durchgeführten Regelkontrollen (vgl. Pkt. 3) wirkungsvoll unterstützt hat, weil ich wiederum mit fast allen Anfragen zu Vorträgen oder Schulungen bzw. zur aktiven Teilnahme an Tagungen, Diskussionspodien oder

ähnlichen Veranstaltungen sehr restriktiv umgegangen bin und auch weil ich die Durchführung von - zweifellos notwendigen - anlassfreien Kontrollen auf ein Minimum beschränkt habe. Meine Vorstellungen von einer wirksamen, insbesondere auch präventiv ausgerichteten Datenschutzkontrolle sehen ganz anders aus, nur leider bin ich dazu auf eine deutlich bessere Personalausstattung angewiesen. Ich kann weiterhin allenfalls reagieren, selbst dies nicht immer mit der eigentlich gebotenen Schnelligkeit, keinesfalls aber agieren.

Insoweit wird sich in nächster Zukunft wohl auch nicht viel an meiner bei der Vorstellung des letzten TBs getroffenen Feststellung, dass es gerade im nicht-öffentlichen Bereich ein erhebliches Vollzugsdefizit gibt, ändern. Für die Datenschutzaufsicht über etwa 175.000 sächsische Unternehmen[1] - hinzukommen noch zahlreiche weitere Stellen wie Vereine, u. U. auch Privatpersonen - steht mir gerademal eine niedrige einstellige Zahl von Mitarbeitern zur Verfügung. Der hohe Kontrollbedarf, insbesondere in den Schwerpunktbereichen Videoüberwachung, Internet, Auftragsdatenverarbeitung und Betroffenenrechte, wird einerseits an der hohen Anzahl festgestellter Datenschutzverstöße - dies betraf beispielsweise mehr als ein Drittel (36 %) der anlassbedingten Kontrollen -, andererseits an der Anzahl der im Berichtszeitraum eingeleiteten Ordnungswidrigkeitenverfahren deutlich. Mit 79 Verfahren war deren Anteil so hoch wie noch nie. Auch der Kontrollaufwand ist deutlich gestiegen. So habe ich in 204 Fällen örtliche Überprüfungen bei 162 verantwortlichen Stellen durchgeführt und musste in erheblichem Maße förmliche Mittel (Heranziehungsbescheide, teilweise sogar mit Zwangsgeldfestsetzungen) anwenden, um von verantwortlichen Stellen überhaupt Auskünfte zu erhalten. Letzteres hat im Berichtszeitraum auch vermehrt zu Ordnungswidrigkeitenverfahren geführt, denn auch die nicht rechtzeitige und die nicht vollständige Auskunftserteilung an die Aufsichtsbehörde sind bekanntlich bußgeldbewehrt. Aus Sicht der Kontrollbehörde ist dabei weniger die nicht rechtzeitige Erteilung von Auskünften das entscheidende Problem, denn mit den zur Verfügung stehenden Aufsichtsinstrumenten lässt sich eine Auskunftserteilung letztendlich fast immer durchsetzen, sondern der damit verbundene administrative Aufwand, denn solche förmlichen Verfahren binden natürlich erhebliche personelle Ressourcen.

Gleichwohl ist anzumerken, dass das Datenschutzniveau in sächsischen Unternehmen tatsächlich wohl nicht ganz so schlecht ist, wie dies die genannten Zahlen zunächst vermuten lassen, denn ein nicht unerheblicher Anteil der durchgeführten förmlichen Verfahren (Heranziehung zur Auskunft, Zwangsgeld, Anordnungen) wie auch der Ordnungswidrigkeitenverfahren konzentriert sich auf einige wenige Unternehmen bzw.

[1] Nach Angaben des Statistischen Landesamtes gab es 2011 im Freistaat Sachsen 174.192 Unternehmen; http://www.statistik.sachsen.de/html/714.htm#article1303

Unternehmensgruppen, die insoweit also notgedrungen einen besonderen Schwerpunkt meiner Aufsichtstätigkeit darstellen.

Dass trotz der alles andere als günstigen Rahmenbedingungen im Berichtszeitraum bei den verantwortlichen Stellen dennoch zahlreiche Veränderungen zugunsten des Datenschutzes bewirkt werden konnten, können Sie dem vorliegenden Bericht entnehmen.

Dies alles steht aber künftig in Frage, wenn nicht schnellstens meine personellen Ressourcen aufgestockt werden. Um es klar zu sagen: Meine Behörde ist an die Grenze ihrer Leistungsfähigkeit gelangt; ihre Arbeitsfähigkeit ist akut gefährdet.

1 Datenschutzaufsicht im nicht-öffentlichen Bereich

Seit dem 1. Januar 2007 obliegt mir die Datenschutzaufsicht nach § 38 BDSG über nicht-öffentliche Stellen im Anwendungsbereich des Dritten Abschnitts des Bundesdatenschutzgesetzes (§ 30a Satz 1 SächsDSG). Zudem hat man mir zugleich die Funktion der Verwaltungsbehörde nach § 36 Abs. 2 OWiG (vgl. § 13 OWiZuVO) übertragen, d. h. ich bin auch für die Verfolgung von Ordnungswidrigkeiten nach § 43 BDSG zuständig.

Als Datenschutzaufsichtsbehörde überwache ich die Durchführung des Datenschutzes bei nicht-öffentlichen Stellen und öffentlich-rechtlichen Wettbewerbsunternehmen und kontrolliere 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 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)

Meine örtliche Zuständigkeit ist auch als Aufsichtsbehörde nach § 38 BDSG 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. Ich bin also immer dann zuständig, wenn sich die tatsächliche in der Verarbeitung personenbezogener Daten bestehende Geschäftstätigkeit der verantwortlichen Stelle 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).

Die Meldepflicht nach § 4d BDSG trifft zum einen alle Unternehmen, die personenbezogene Daten geschäftsmäßig zum Zweck der (gegebenenfalls auch anonymisierten) Übermittlung speichern (z. B. Wirtschaftsauskunfteien, Adresshändler, Markt- und Meinungsforschungsinstitute).

Zum anderen 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. März 2013 lagen insgesamt 30 Registermeldungen von 28 Unternehmen vor, die

- in 10 Fällen Verfahren von Handels- und Wirtschaftsauskunfteien,

- in 14 Fällen Verfahren von Markt- und Meinungsforschungsinstituten

sowie in je einem Fall den Betrieb eines Verfügungszentralregisters, eines Widerspruchsregisters, eines Adresshandels, eines Bewertungsportals, eines Handwerkerpools 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 Berichtszeitraums wurden keine diesbezüglichen Einsichtnahme- bzw. Auskunftsbegehren an mich herangetragen.

3 Regelaufsicht

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. Pkt. 4.1) regelmäßig ein konkreter Anhaltspunkt für eine mögliche Verletzung datenschutzrechtlicher Vorschriften besteht, handelt es sich bei einer Regelkontrolle im Schwerpunkt um eine reine Routineüberprüfung.

Die Erfahrungen aus früheren Berichtszeiträumen bestätigen die positiven, insbesondere auch breitgestreuten Effekte anlassfreier Kontrollen insbesondere immer dann, wenn sich diese nicht nur auf einzelne Unternehmen, sondern zugleich auf mehrere Unternehmen einer Branche erstrecken, und wenn diese dann auch noch unternehmensübergreifend ausgewertet werden. Die Unternehmen in der von der Kontrolle betroffenen Branche tauschen sich natürlich über deren Inhalt und Ergebnisse untereinander aus, unabhängig davon, ob sie direkter Adressat der Kontrolltätigkeit der Aufsichtsbehörde sind oder nicht. Mit vertretbarem Aufwand können so eine Vielzahl von Unternehmen erreicht und datenschutzrechtliche Verbesserungen in der gesamten Branche bewirkt werden.

Seitens der Aufsichtsbehörde setzt dies dessen ungeachtet natürlich die notwendigen personellen Ressourcen voraus, denn solche entsprechend groß angelegten Kontrollen müssen vorbereitet, durchgeführt, ausgewertet und insbesondere nachverfolgt werden. Denn natürlich reicht es nicht, im Rahmen der Kontrolle Mängel festzustellen - diese müssen dann auch tatsächlich beseitigt werden. Nicht immer sind die verantwortlichen Stellen aber der gleichen Auffassung wie die Aufsichtsbehörde und nicht immer lassen sich festgestellte Mängel von heute auf morgen abstellen. Insbesondere der Auswertungs- und Nachverfolgungsaufwand ist also regelmäßig doch beachtlich.

Für derartige Kontrollaktionen, wie sie einige Aufsichtsbehörden anderer Bundesländer durchaus praktizieren (können), fehlen mir aber ganz einfach die erforderlichen Mitarbeiter. Vorrang haben daher die Durchführung von Anlasskontrollen sowie die

Bearbeitung von Beratungsanliegen, deren Anzahl (Neueingänge) gegenüber dem letzten Berichtszeitraum wiederum markant (jeweils etwa um ein Viertel) gestiegen ist. Damit sind meine Mitarbeiter mehr als nur ausgelastet, nicht zuletzt weil mir wie bereits dargestellt zum 1. Januar 2012 im Rahmen allgemeiner Haushaltseinsparungen eine Stelle im nicht-öffentlichen Bereich ersatzlos gestrichen worden ist.

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	**01.01.11 31.03.13**
Auskunfteien	0	0	4	0	1	**5**
Markt- / Meinungsforschung	1	0	4	4	0	**0**
Auftragsdatenverarbeiter	10	1	0	1	0	**1**
Wohnungsunternehmen	0	46	19	15	0	**0**
Sparkassen / Banken	30	0	0	0	0	**0**
Verkehrsunternehmen	57	3	0	0	0	**0**
Versorgungsunternehmen	4	7	1	0	0	**0**
Altenpflegeheime	0	48	0	0	0	**0**
Wohlfahrtsverbände	0	0	10	7	0	**0**
Ärzte	0	0	0	25	0	**0**
Sonstige	2	5	7	3	1	**1**
Gesamtanzahl	104	110	45	55	2	**7**

Tab. 1: Anlassfreie Überprüfungen

Alle in vorstehender Tabelle ausgewiesenen Kontrollen sind als örtliche Überprüfung ausgestaltet gewesen. Die Wirtschaftsauskunfteien sind infolge der von ihnen bei der Aufsichtsbehörde vorliegenden Registermeldung (vgl. Pkt. 2) geprüft worden, die aufgeführte Kontrolle eines Auftragsdatenverarbeiters betraf ein Aktenvernichtungsunternehmen und bei dem unter Sonstige genannten Unternehmen hat es sich um eine Firma, die Medizinprodukte vertreibt, gehandelt.

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).

Anlasskontrollen der Aufsichtsbehörde setzen - wie die Bezeichnung schon sagt - Anhaltspunkte für eine Datenschutzverletzung voraus. Oftmals geht ein solcher Anhaltspunkt aus einer Anfrage oder Beschwerde eines Betroffenen hervor, in nicht wenigen Fällen können aber auch Pressemeldungen, Hinweisgeber oder Erkenntnisse aus Überprüfungen anderer Unternehmen, z. B. von Auftragsdatenverarbeitern, Auslöser einer Kontrolle sein. Im Berichtszeitraum sind - was nicht von Eingaben ausgehende Anlasskontrollen betrifft - zwei Kontrollaktionen besonders erwähnenswert: Zum einen habe ich bei der Kontrolle eines Auftragsdatenverarbeiters (Service-Rechenzentrum) festgestellt, dass keine schriftlichen Verträge mit den Auftraggebern abgeschlossen worden waren, was dann zu einer anlassbedingten Kontrolle auch aller Auftraggeber geführt hat (vgl. Pkt. 4.2.2). Zum anderen habe ich die Kontrolle der Videoüberwachung in einem Geschäft eines Einkaufszentrums zum Ausgangspunkt für eine Kontrolle der Einhaltung der Kennzeichnungspflicht in allen Geschäften dieses Einkaufszentrums genommen (vgl. Pkt. 8.1.3). Für diese Entscheidung maßgeblich war die Einlassung der verantwortlichen Stelle, dass das Einkaufszentrum doch insgesamt als videoüberwacht gekennzeichnet sei und im Übrigen auch andere Einzelhändler keine Kennzeichnung vorgenommen hätten.

Im Berichtszeitraum bin ich in insgesamt 918 Fällen Anhaltspunkten für einen Datenschutzverstoß nachgegangen, 14 Fälle resultierten dabei noch aus dem letzten Berichtszeitraum. Hinsichtlich der neu bearbeiteten Sachverhalte (904 Fälle) ist im Vergleich zum vorhergehenden Berichtszeitraum (648 Fälle) wiederum eine deutliche Steigerung um absolut 40 % bzw. relativ (auf den Zweijahreszeitraum bezogen) um immerhin noch 24 % zu verzeichnen. Zahlreiche telefonische Eingaben, die auch sofort telefonisch beantwortet werden konnten, habe ich nicht anzahlmäßig erfasst.

Im Regelfall führe ich Anlasskontrollen im schriftlichen Verfahren durch, daneben kontrolliere ich die betreffenden Firmen aber auch - insbesondere, wenn eine besondere Eilbedürftigkeit gegeben ist oder das Vorhandensein konkreter Daten oder konkreter spezifischer Umstände der Datenverarbeitung (z. B. Erfassungsbereiche bei Videoüber-

wachungen) bei der verantwortlichen Stelle zu prüfen sind - vor Ort. Im Berichtszeitraum habe ich in 204 Fällen örtliche Überprüfungen bei 162 verantwortlichen Stellen durchgeführt. Gegenüber dem vorangegangenen Berichtszeitraum stellt dies eine Steigerung um absolut 200 % bzw. relativ 167 % (Zweijahreszeitraum) dar.

Berichtszeitraum		2001 2002	2003 2004	2005 2006	2007 2008	2009 2010	**01.01.11 31.03.13**
Neueingänge		116	147	164	410	648	**904**
zzgl. Übernahme Vorjahr		3	6	9	15	29	**14**
bearbeitete Sachverhalte gesamt		**119**	**153**	**173**	**425**	**677**	**918**
davon	mit örtlichen Kontrollen	18	24	17	51	68	**162**
	Verstöße	50	65	62	87	152	**324**
	keine Zuständigkeit	27	26	31	57	160	**180**
	noch in Bearbeitung	6	9	15	29	14	**26**

Tab. 2: Anlasskontrollen

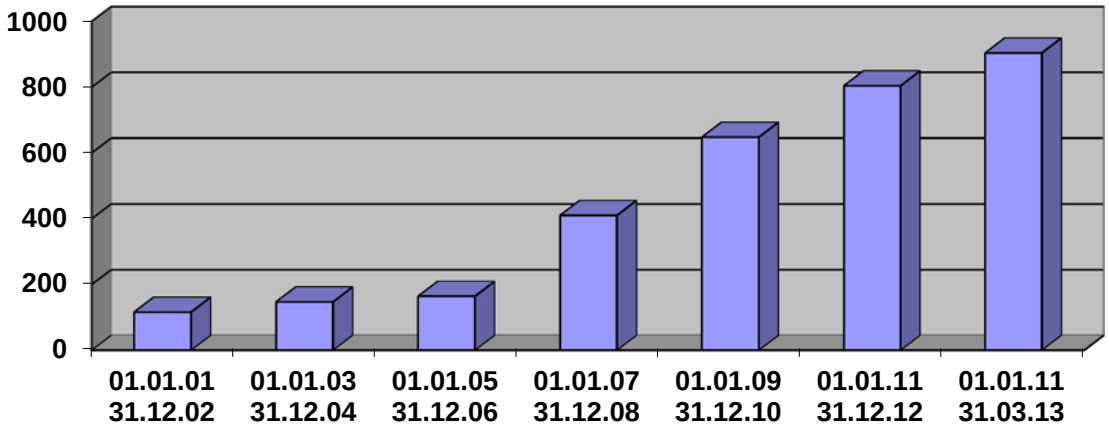

Abb. 1: Entwicklung der Anlasskontrollen (Neueingänge)

Die größte Anzahl der neu initiierten Anlasskontrollen (ca. 16,5 %) betraf wiederum den Umgang mit personenbezogenen Daten im Internet, wobei hier insbesondere die erhebliche Zahl der Beschwerden über unerwünschte Newsletter auffällig ist. Dicht darauf folgen die Videoüberwachung (15,7 %) sowie die Auftragsdatenverarbeitung (9,3 %) betreffende Anlasskontrollen, was u. a. auch den eingangs dieses Punktes beschriebenen komplexen Kontrollaktionen geschuldet ist. Dessen ungeachtet ist gerade die Videoüberwachung aber unverändert auch ein bedeutender Eingabeschwerpunkt. Deutlich nach oben entwickelt hat sich auch die Anzahl der Eingaben zur Gewährung von Betroffenenrechten (8,9 %).

Im Einzelnen verteilten sich die Schwerpunkte der anlassbedingten Kontrolltätigkeit der Aufsichtsbehörde (ohne Altfälle) im Berichtszeitraum wie folgt:

1.	Umgang mit Daten im Internet	149 Fälle
	davon Werbemails (Newsletter)	*94 Fälle*
2.	Videoüberwachung	142 Fälle
3.	Auftragsdatenverarbeitung	84 Fälle
4.	Rechte des Betroffenen	80 Fälle
5.	Arbeitnehmerdatenschutz	33 Fälle
6.	Gesundheitswesen	21 Fälle
7.	Tätigkeit von Auskunfteien	20 Fälle
8.	Datenschutzbeauftragter	19 Fälle
9.	Umgang mit Daten durch Kreditinstitute	18 Fälle
10.	Vermietung / Verpachtung	15 Fälle
	Bildungs-, Freizeitbereich	15 Fälle
11.	Personalausweisdaten	11 Fälle
	Einzelhandel	11 Fälle
12.	Datenverarbeitung durch Vereine / Verbände	9 Fälle
13.	Freie Träger im Sozialbereich	8 Fälle
	Gesprächsaufzeichnung	8 Fälle
14.	Werbung	7 Fälle
	Finanzdienstleistungen	7 Fälle
	Versicherungen	7 Fälle

In der Vergangenheit eher unauffällig gewesen sind der Bildungs- und Freizeitbereich sowie die freien Träger im Sozialbereich. Wie die oben stehende Auflistung verdeutlicht, haben die Eingaben in diesen Bereichen aber deutlich zugenommen. Besonders betroffen waren insoweit Bildungseinrichtungen und Kindertagesstätten in privater Trägerschaft. Die unter der Bezeichnung „Gesprächsaufzeichnung“ separat erwähnten Kontrollen habe ich fast ausschließlich in Einkaufszentren ein- und desselben Betreibers durchgeführt, nachdem ich in einem Einkaufszentrum eine unzulässige Aufzeichnung eingehender Kundenanrufe festgestellt hatte (vgl. Pkt. 8.5.1).

Bei etwa jeder dritten Kontrolle (ca. 36 %) habe ich im Ergebnis einen Verstoß gegen datenschutzrechtliche Vorschriften feststellen müssen. Dies ist deutlich mehr als noch im letzten Berichtszeitraum (ca. 22 %). Die bereichsspezifische Auswertung zeigt dabei bei den Spitzenreitern weitgehende Übereinstimmung mit der der durchgeführten Kontrollen:

1.	Auftragsdatenverarbeitung	81 Verstöße	(96 %)
2.	Videoüberwachung	68 Verstöße	(48 %)
3.	Umgang mit Daten im Internet *davon Werbemails (Newsletter)*	67 Verstöße *49 Verstöße*	(45 %) *(52 %)*
4.	Rechte des Betroffenen	29 Verstöße	(36 %)
5.	Gesundheitswesen	10 Verstöße	(48 %)
6.	Arbeitnehmerdatenschutz	7 Verstöße	(21 %)
	Tätigkeit von Auskunfteien	7 Verstöße	(35 %)

Wenig erstaunlich ist der Spitzenplatz der Auftragsdatenverarbeitung sowie auch die Tatsache, dass hier bei fast allen Kontrollen ein Datenschutzverstoß festgestellt worden ist, da die hier maßgebliche Kontrollaktion wie bereits eingangs dieses Punktes erwähnt alle Auftraggeber ein- und desselben Auftragnehmers (fehlende schriftliche Vereinbarungen) betroffen hat.

Deutlich über dem festgestellten Durchschnitt liegen die Werte bei den Kontrollen betreffend die Videoüberwachung, den Umgang mit personenbezogenen Daten im Internet sowie im Gesundheitswesen. In diesen Bereichen musste ich bei fast jeder zweiten Prüfung einen Verstoß gegen datenschutzrechtliche Vorschriften feststellen.

4.2 Umfang und Grenzen der aufsichtsbehördlichen Befugnisse

4.2.1 Kontrollbefugnis der Aufsichtsbehörde und Umfang der Auskunftspflicht

Ein großes Internetunternehmen weigerte sich gegenüber meiner Behörde, unverzüglich die mit seiner Geschäftigkeit verbundene Erhebung, Verarbeitung und Nutzung personenbezogener Daten unterschieden nach Geschäftsprozessen jeweils inhaltlich und örtlich vollständig offen zu legen. Gegen seine (förmliche) Heranziehung unter Androhung von Zwangsmitteln wandte es ein, die Datenschutzaufsicht sei jedenfalls ohne konkreten Anlass nicht zu einer solch umfassenden Prüfung allen Verarbeitungshandelns (Audit) befugt, die schon des Umfangs der Auskünfte und damit des Aufwandes der verantwortlichen Stelle wegen gerade bei kurzer Fristsetzung unverhältnismäßig sei. Vielmehr habe sich die Aufsicht auf die Klärung etwaig offener Einzelfragen bzw. Komplexe zu beschränken und sei zudem gehalten, das Verarbeitungshandeln anhand des Internetauftritts zunächst umfassend aus öffentlichen Quellen selbst aufzuklären, bevor es bei einer verantwortlichen Stelle hiernach fragen dürfe.

Dieser Argumentation folgten jedoch (im einstweiligen Rechtschutzverfahren) weder das VG Leipzig (Beschluss vom 3. Dezember 2012 - 5 L 1308/12 - juris), noch das OVG (Beschluss vom 17. Juli 2013 - 3 B 470/12 - juris). Die Gerichte bestätigten vollumfänglich meine Rechtsauffassung, dass meine Behörde nach § 38 Abs. 1 Satz 1 i. V. m. Abs. 3 und 4 BDSG befugt ist, verantwortliche Stellen jederzeit anlasslos und vollständig zu kontrollieren und alle hierzu notwendigen Auskünfte zu verlangen, da das öffentliche Interesse der Allgemeinheit an einem effektiven Schutz personenbezogener Daten und das grundrechtlich geschützte Recht Betroffener auf informationelle Selbstbestimmung den wirtschaftlichen Interessen der zu kontrollierenden Stellen im Einzelfall vorgehen.

Dessen ungeachtet sind jedoch in Bezug auf das konkrete Aufsichtsverfahren weitere Rechtsstreite anhängig. Die von mir verlangten Auskünfte habe ich bis heute nicht.

4.2.2 Auftragsdatenverarbeitung: Auskunft über Auftraggeber

Eher zufällig bin ich auf ein inhabergeführtes Service-Rechenzentrum aufmerksam geworden, dies eigentlich auch nur deshalb, weil ich im Rahmen der Bearbeitung einer Eingabe ein anderes, durch die gleiche Person geführtes Unternehmen zu kontrollieren hatte.

Die von mir durchgeführte örtliche Kontrolle, die in erster Linie den Zweck verfolgte, die Voraussetzungen für die Pflicht zur Bestellung eines Datenschutzbeauftragten zu überprüfen, ergab jedoch in anderer Hinsicht Erstaunliches: Der Inhaber des Rechenzentrums gab an, mit keinem seiner ca. 300 Auftraggeber einen schriftlichen Vertrag abgeschlossen zu haben.

Nun ist es bekanntermaßen natürlich möglich, Verträge auch mündlich abzuschließen. Das wird tagtäglich von fast jedem praktiziert, beispielsweise wenn man an die Zapfsäule einer Tankstelle fährt und Kraftstoff nachfüllt oder wenn man ein Verkehrsmittel nutzt. Auch unter Geschäftsleuten sind mündliche Verträge jedenfalls nicht ungewöhnlich. Allerdings gibt es diesbezüglich auch Grenzen, denn es gibt Konstellationen, in denen gesetzlich die Schriftform gefordert ist, wozu beispielsweise Verträge über den Erwerb von Grundstücken (vgl. § 311b BGB) gehören. Aber auch im Datenschutzrecht finden sich solche Vorgaben und diese sind insbesondere für Auftragsdatenverarbeiter wie eben beispielsweise Service-Rechenzentren einschlägig:

Im Fall einer Auftragsdatenverarbeitung fordert § 11 Abs. 2 Satz 2 BDSG einen schriftlichen Auftrag des Auftraggebers und gibt zugleich auch die darin festzulegenden Mindestinhalte vor.

Die diesbezügliche Verantwortung liegt nach § 11 Abs. 1 Satz 1 BDSG zwar bei den jeweiligen Auftraggebern, jedoch trifft den Auftragnehmer nach § 11 Abs. 3 Satz 2 BDSG zumindest auch eine diesbezügliche Hinweispflicht, d. h. er hat seine Auftraggeber darauf hinzuweisen, dass ein lediglich mündlich abgeschlossener Vertrag nicht den Formvorschriften des Bundesdatenschutzgesetzes genügt und das Gesetz darüber hinaus auch noch konkrete Regelungsinhalte für den schriftlich zu erteilenden Auftrag vorschreibt.

In solchen Fällen empfiehlt es sich ungeachtet der beim Auftraggeber liegenden Verantwortung regelmäßig, dass der Auftragnehmer einen den Anforderungen des § 11 Abs. 2 BDSG genügenden Mustervertrag entwirft und diesen den Auftraggebern zur Unterzeichnung vorlegt, zumal angesichts der vorgegebenen Vertragsinhalte ohnehin immer eine entsprechende Zuarbeit des Auftragnehmers - vor allem bei der schriftlichen Festlegung der getroffenen technischen und organisatorischen Maßnahmen - erforderlich ist. Die Erarbeitung eines Mustervertrages empfiehlt sich in besonderem Maße immer dann, wenn ein Unternehmen in vergleichbaren Konstellationen für eine Vielzahl von Auftraggebern tätig ist und es sich bei diesen darüber hinaus lediglich um Kleinunternehmer handelt, die mit der Umsetzung der Vorgaben des § 11 Abs. 2 BDSG nach meinen Erfahrungen in vielen Fällen überfordert sind.

Nachdem der Inhaber des Service-Rechenzentrums mir trotz mehrerer Aufforderungen weder die diesbezügliche Unterrichtung seiner Auftraggeber noch die Erarbeitung eines Vertragsentwurfs nachweisen konnte, habe ich mich gezwungen gesehen, die Kontrolle auch auf seine Auftraggeber auszudehnen, d. h. mich in dieser Angelegenheit direkt an sie zu wenden.

Dazu habe ich mich im förmlichen Auskunftsverfahren an das Service-Rechenzentrum gewandt und Auskunft über alle Auftraggeber (jeweils Name und Anschrift) verlangt.

Diese Auskunft ist mir zunächst verweigert worden. Als Begründung wurde angeführt, dass sich das Service-Rechenzentrum zur unbedingten Wahrung des Mandantengeheimnisses gegenüber jedermann verpflichtet habe und der Inhaber sich bei einer Verletzung dieser Verpflichtung der Gefahr einer strafrechtlichen Verfolgung aussetzen würde. Aus diesem Grund mache er von seinem Auskunftsverweigerungsrecht gegenüber der Aufsichtsbehörde Gebrauch.

Ich habe diese Begründung zurückgewiesen; die Inanspruchnahme des Auskunftsverweigerungsrechtes war in dem konkreten Fall nicht möglich.

Zunächst ist festzuhalten, dass die Kenntnis über die konkreten Auftraggeber vorliegend zwingend für meine Kontrolltätigkeit erforderlich gewesen ist (vgl. § 38 Abs. 3 Satz 1

BDSG). Ohne deren Kenntnis hätte ich meinen gesetzlichen Kontrollpflichten nicht nachkommen, insbesondere nicht überprüfen können, welche Auftraggeber in welchem Umfang ihren sich aus § 11 BDSG ergebenden Verpflichtungen nachgekommen sind.

Nach dem in § 38 Abs. 3 Satz 2 BDSG geregelten Auskunftsverweigerungsrecht kann der Auskunftspflichtige die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen seiner in § 383 Abs. 1 Nr. 1 bis 3 ZPO bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde.

Vorliegend war nicht ersichtlich, dass sich der Auftragnehmer mit der Auskunft über seine Auftraggeber der Gefahr eines Ordnungswidrigkeitenverfahrens aussetzen würde. Der durch mich festgestellte Verstoß gegen die Vorschrift des § 11 Abs. 2 Satz 2 BDSG betraf nicht sein Unternehmen, sondern stattdessen seine Auftraggeber. Gemäß § 11 Abs. 1 Satz 1 BDSG sind die Auftraggeber für die Einhaltung der Vorschriften des Bundesdatenschutzgesetzes verantwortlich, insbesondere haben auch diese den Auftrag schriftlich in dem durch § 11 Abs. 2 Satz 2 BDSG vorgeschriebenen Umfang zu erteilen.

Es war weiterhin auch nicht ersichtlich, dass sich der Auftragnehmer mit einer solchen Auskunft der Gefahr strafgerichtlicher Verfolgung aussetzen würde. Die von ihm mit der Auftragsannahme gegenüber seinen Auftraggebern eingegangene Verpflichtung - entsprechende Unterlagen konnte er schon wegen des nur mündlichen Vertragsabschlusses dazu nicht vorlegen - zur Wahrung des Mandanten- bzw. Geschäftsgeheimnisses ist anders als etwa bei Rechtsanwälten oder Ärzten ausschließlich zivilrechtlicher Natur. Verstöße dagegen besitzen keine strafrechtliche Relevanz.

Nachdem ich mit dieser Begründung die Inanspruchnahme des Auskunftsverweigerungsrechts zurückgewiesen hatte, sind mir die geforderten Auskünfte dann erteilt worden.

Auf deren Grundlage habe ich mich dann an alle Auftraggeber gewandt bzw. die für diese zuständigen Aufsichtsbehörden anderer Bundesländer informiert und sie auf die Pflicht zur schriftlichen Auftragserteilung hingewiesen. Damit kam dann auch endlich Bewegung in diese Angelegenheit, denn zumindest einige der Auftraggeber haben dann auch ihrerseits mit entsprechendem Nachdruck die Vorlage eines gesetzeskonformen Vertragsentwurfes vom Auftragnehmer gefordert. Vom Service-Rechenzentrum wurde mir daraufhin ein Vertragsentwurf vorgelegt, der nach auf meinen Hinweisen basierenden Überarbeitungen schließlich den gesetzlichen Vorgaben genügte. Gleichwohl dauerte es noch eine geraume Zeit, bis mir alle in meinem Zuständigkeitsbereich befind-

lichen Auftraggeber dann auch tatsächlich die schriftliche Auftragserteilung nachgewiesen hatten. In einigen Fällen bedurfte es aber auch dort noch förmlicher Auskunftsverfahren und in wenigen Fällen sogar noch der Verhängung von Zwangsgeldern (vgl. Pkt. 10.1) sowie im Nachgang dann der Festsetzung von Bußgeldern (vgl. Pkt. 11.1). Für den Inhaber des Service-Rechenzentrums bleibt festzustellen, dass er sich bei rechtzeitiger Befassung mit der Problematik viel Ärger mit der Aufsichtsbehörde und seinen Auftraggebern hätte ersparen können.

4.2.3 Medienprivileg als Hinderungsgrund einer Kontrolle

Im Zuge einer Eingabe war ich mit einer Internetseite befasst, auf der der Anbieter eigene und fremde journalistisch-redaktionelle Beiträge einstellte, für Dritte aufbereitete und teils auch selbst kommentierte. Zusätzlich ermöglichte er es den Nutzern, ergänzend eigene Kommentare zu den Inhalten einzustellen. Hiervon hatte ein Petent Gebrauch gemacht und einen Kommentar verfasst, der einer Praktikantin des Anbieters Anlass gab, hierauf einen weiteren Kommentar einzustellen, der jedoch die Identität des Petenten offenbarte, welche die Praktikantin aus den Anmeldedaten kannte. Deswegen bat der Betroffene mich, gegen den Seitenanbieter vorzugehen und eine Löschung des ihn betreffenden Beitrags zu erwirken.

Aus verfassungsrechtlichen Gründen gilt allerdings für den journalistisch-redaktionell tätigen Anbieter und seine Mitarbeiterin als Hilfsperson, dass diese nicht nur ihr Grundrecht auf Meinungsfreiheit aus Art. 5 Abs. 1 Satz 1 GG ausüben, sondern darüber hinaus auch den besonderen Schutz der Pressefreiheit aus Art. 5 Abs. 1 Satz 2 GG beanspruchen können. Denn ohne die Erhebung, Verarbeitung und Nutzung personenbezogener Daten auch ohne Einwilligung der jeweils Betroffenen wäre eine dem verfassungsrechtlichen Schutz der Pressefreiheit ausfüllende journalistische Arbeit nicht möglich. Dies gilt auch für eigene Kommentare journalistisch Tätiger im Kontext ihrer redaktionellen Arbeit. Deswegen schließt das sogenannte Medienprivileg in § 41 Abs. 1 BDSG i. V. m. § 57 Abs. 1 Satz 1 RStV eine Aufsicht meiner Behörde - anders als bei sonstigen Nutzerkommentaren - generell aus.

Dies habe ich dem Betroffenen mitgeteilt, allerdings auch, dass meine Beurteilung keine Aussage darüber beinhaltet, ob er rechtlich gehindert wäre, der Preisgabe seiner Identität mit außerdatenschutzrechtlichen Gründen, also allgemein-zivilrechtlich und insbesondere presserechtlich, entgegenzutreten.

5 Beratungstätigkeit

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 sind 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 enthalten:

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

Im Berichtszeitraum sind in 122 Fällen Beratungsanliegen an mich herangetragen worden. Gegenüber dem vorangegangenen Berichtszeitraum (87 Fälle) entspricht dies einer absoluten Steigerung um 40 % bzw. bezogen auf einen Zweijahreszeitraum einer relativen Steigerung um 25 %. Telefonische Anfragen, die auch sofort durch telefonische Beratung erledigt werden konnten, sind in dieser Zahl nicht enthalten - hierüber wurde keine Statistik geführt.

Analysiert man die Beratungstätigkeit im Berichtszeitraum, so ergeben sich faktisch die gleichen Schwerpunkte wie im vorhergehenden Berichtszeitraum:

- Betrieblicher Datenschutzbeauftragter (16 Fälle)

Den Hauptteil der Anfragen bildeten Fragen zur Notwendigkeit der Bestellung eines betrieblichen Datenschutzbeauftragten sowie zu den diesbezüglichen Formalitäten, daneben ging es aber auch um den Erwerb und den Erhalt der erforderlichen Fachkunde, um mögliche Interessenkollisionen und um Fragen der Führung des Verfahrensverzeichnisses.

Nicht alltäglich war die Frage eines externen Datenschutzbeauftragten, der mit seinem Unternehmen in die Insolvenz gegangen war. Hier stellte sich die Frage, ob auch die personenbezogenen Daten, die er in Ausübung seiner Tätigkeit zu Geschäftsbesorgungs-

zwecken erhalten hatte, an den Insolvenzverwalter herauszugeben sind (siehe dazu Pkt. 8.13.4).

- Videoüberwachung (13 Fälle)

Videoüberwachungsanlagen werden branchenübergreifend in erster Linie zum Eigentumsschutz eingesetzt. Diesbezügliche Anfragen haben mich daher auch von den verschiedensten verantwortlichen Stellen erreicht, beispielsweise von einem Seniorenzentrum, einem Verkehrsunternehmen, einer Stiftung, einem Autohaus, einem Museum, einem Theater, einem Einkaufszentrum und einer Wohnungsgesellschaft.

- Gesundheitswesen (10 Fälle)

Vergleichsweise oft haben sich wiederum auch Einrichtungen aus dem Gesundheitswesen an mich gewandt. Beraten wurden insoweit insbesondere Ärzte, Kliniken, Apotheken und Pflegeeinrichtungen sowie ein Blutspendedienst. Gegenstand der Beratung war u. a. die Frage, ob ein Patient einen Anspruch auf Löschung von Angaben, z. B. Verdachtsdiagnosen, aus einem Arztbrief hat (siehe dazu Pkt. 8.4.1), ob ein aus einer Gemeinschaftspraxis ausscheidender Arzt die Duplizierung der gemeinsamen Patientendatei verlangen kann (siehe dazu Pkt. 8.4.2) oder welche Fragestellungen im Selbstauskunftsbogen eines Blutspendedienstes zulässig sind (siehe dazu Pkt. 8.4.4).

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 mich 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 Persönlichkeitsrechts sind entsprechende Vertragsklauseln oder verbindliche Unternehmensregelungen vorzulegen.

Im Berichtszeitraum sind an mich keine derartigen Anträge gestellt worden.

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

http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/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 BDSG angemessenes Datenschutzniveau gegeben ist. Dazu gehören bislang Andorra, Argentinien, die Färöer, Guernsey, Israel, die Isle of Man, die Vogtei Jersey, Kanada (mit Einschränkungen), Neuseeland, die Schweiz, Uruguay sowie die USA (Safe Harbor). Bei einer Übermittlung in diese Länder ist gleichfalls keine Genehmigung durch die Aufsichtsbehörde erforderlich. Die diesbezüglichen Entscheidungen sind von der Internetseite der Europäischen Kommission abrufbar:

http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

8 Ausgewählte Sachverhalte

8.1 Videoüberwachung

8.1.1 Dashcames

Immer größerer Beliebtheit erfreuen sich sogenannte Dashcams, also auf andere Fahrzeuge bzw. den Straßenverkehr gerichtete Kameras an der Windschutzscheibe oder dem Armaturenbrett, die permanent Verkehrsabläufe im unmittelbaren Umfeld eines Fahrzeugs vorsorglich aufzeichnen, um ein mögliches Fehlverhalten anderer Verkehrsteilnehmer - etwa bei Unfällen - später dokumentieren zu können. Dementsprechend haben mich im Berichtszeitraum viele Anfragen zum Einsatz solcher Geräte erreicht, gerade auch, weil die Technik im Fachhandel immer preiswerter angeboten wird und im Ausland, beispielsweise in Russland, bereits sehr verbreitet ist.

Öffentlich zugängliche Bereiche dürfen nach § 6b Abs. 1 BDSG jedoch nur von Kameras beobachtet und aufgezeichnet werden, soweit dies zur Wahrnehmung des Hausrechts oder zur Wahrnehmung sonst berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Bei einer Fahrzeugaußenkamera kann sich der Kamerabetreiber jedoch nicht auf sein Hausrecht (§ 6b Abs. 1 Nr. 2 BDSG) berufen, da das Hausrecht (am Auto) nicht das Recht umfasst, angrenzende öffentliche Verkehrsflächen (Straßen, Wege, Parkplätze) zu erfassen, also allein auf das Fahrzeuginnere beschränkt ist. Eine darüber hinaus zulässige Wahrnehmung berechtigter Interessen (§ 6b Abs. 1 Nr. 3 BDSG) liegt ebenso nicht vor. Zwar mag ein berechtigtes Interesse des Fahrers (und Halters) bestehen, bei einem Verkehrsunfall das eigene und fremde Fahrverhalten mittels der Aufnahmen beweisen zu können. Allerdings überwiegen die schutzwürdigen Interessen bzw. Persönlichkeitsrechte der anderen Verkehrsteilnehmer, von einer präventiven Aufzeichnung verschont zu bleiben, denn der Einzelne hat das (Grund-)Recht, sich in der Öffentlichkeit frei und ungezwungen zu bewegen, ohne befürchten zu müssen, ungewollt zum Gegenstand einer Überwachungsmaßnahme zu werden, die selbst der Polizei nur unter ganz engen Voraussetzungen erlaubt wäre.

Zudem ist bei einer Fahrzeugaußenkamera fraglich, wie die Vorgabe des § 6b Abs. 2 BDSG, wonach der Umstand der Beobachtung und die verantwortliche Stelle kenntlich zu machen wäre, umgesetzt werden könnte, also den anderen Verkehrsteilnehmern mitgeteilt wird, dass und von wem sie gerade gefilmt werden.

8.1.2 Einkaufszentren

Medienberichterstattungen gaben mir Anlass, in mehreren Einkaufszentren eines bundesweit tätigen Betreibers dessen örtliche Videoüberwachung zu kontrollieren. Die Prüfung betraf allerdings nicht die Kameras in den einzelnen Läden, die eigenverantwortlich von jedem Mieter betrieben werden, sondern die allgemeinen Außen- und Innenbereiche der Anlage, die vom Betreiber des Objekts verantwortet werden.

Nach § 6b Abs. 1 Nr. 1 und 3 BDSG gestattet das Hausrecht des Betreibers und sein berechtigtes Interesse, zur Unfallverhütung, zum Schutz seines Eigentums sowie zur Gewährleistung des Betriebs und der Sicherheit seines Objekts, bestimmte Bereiche präventiv zu überwachen, solange schutzwürdige Interessen der Betroffenen nicht überwiegen. Dies ist aber dann der Fall, wenn ein Bereich des Einkaufszentrums im Besonderen zum Flanieren, Verweilen oder zum Aufenthalt bestimmt ist bzw. einlädt, also die Betroffenen dort Entspannung, Rückzug oder Intimität suchen und deswegen auf ihre Privatsphäre vertrauen dürfen. Daher halte ich eine Beobachtung der allgemeinen Ladenpassagen (Shopping-Mall), von Aufenthaltsbereichen mit Sitzgelegenheiten und insbesondere der gastronomisch genutzten Flächen für unzulässig. Auch bei den Zugängen zu Toiletten überwiegen die schutzwürdigen Interessen der Betroffenen.

Keine Einwände habe ich hingegen gegen eine Überwachung im Bereich der Parkdecks (Ein- und Ausfahrten bzw. Ein- und Ausgänge), der Anlieferungszonen, Müllanlagen und der Schließfächer sowie besonderer Fluchtwege soweit sich die Beobachtung jeweils allein hierauf erstreckt. Auch die begrenzte Beobachtung besonders unfallträchtiger Bereiche wie der Rolltreppen und Aufzugstüren sehe ich dem Grunde nach als zulässig an.

Eine Überwachung der Außenfassaden ist jedenfalls dann zulässig realisierbar, wenn dabei nicht auch öffentlich zugängliche Bereiche erfasst werden. Sollte dies nicht vermieden werden können, darf die Überwachung allerdings nur einen maximal einen Meter breiten Streifen entlang der Fassade erfassen und dies auch nur dann, wenn es sich bei diesen Bereichen nachweislich um besonders einbruchs- oder beschädigungsgefährdete Bereiche handelt.

Für eine Videoüberwachung der Ein- und Ausgangsbereiche von Einkaufszentren sehe ich - jedenfalls während der Öffnungszeiten - keinen zwingenden Grund. Während der Schließzeiten ist der Betrieb von Videokameras hingegen auch in diesen Bereichen stets zulässig.

Gemäß § 6b Abs. 2 BDSG besteht allgemein die Verpflichtung, überwachte Bereiche mit einem deutlich sichtbaren Hinweise auf die Videoüberwachung zu kennzeichnen.

Die zulässige Dauer der Speicherung von Videoaufzeichnungen ergibt sich aus § 6b Abs. 5 BDSG. Danach sind die Videoaufzeichnungen unverzüglich zu löschen, wenn sie zur Erreichung des angegebenen Zweckes nicht mehr erforderlich sind. Bei einer Öffnungszeit von sechs Tagen pro Woche ist eine regelmäßige Speicherdauer von maximal 48 Stunden gemeinhin ausreichend. Bei einem Vorkommnis können allerdings Teile der Aufzeichnungen aus dem DV-System exportiert und dann auch längerfristig gespeichert werden.

Gemessen an diesen Vorgaben habe ich bei den von mir kontrollierten Einkaufszentren, deren Videoüberwachungskonzept höchst unterschiedlich ausfiel, teilweise Korrekturbedarf gesehen, dem der Betreiber umgehend nachgekommen ist.

8.1.3 Kennzeichnungspflicht

Eine anlassbedingte Überprüfung der Videoüberwachung in einem Geschäft eines Einkaufszentrums, bei der u. a. auch ausgiebig die Problematik der Kennzeichnung diskutiert worden war, bildete den Ausgangspunkt für eine Kontrolle aller Geschäfte dieses Einkaufszentrums im Hinblick auf die Umsetzung der in § 6b Abs. 2 BDSG normierten Kennzeichnungspflicht.

Nach § 6b Abs. 2 BDSG sind der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen.

Die verantwortliche Stelle hatte in diesem Zusammenhang damit argumentiert, dass das Einkaufszentrum doch insgesamt als videoüberwacht gekennzeichnet sei und im Übrigen - das hört man häufig - auch andere Einzelhändler des Einkaufszentrums keine Kennzeichnung vorgenommen hätten. In der Tat musste auch ich auf dem Rückweg durch das Einkaufszentrum feststellen, dass durch die Einzelhändler in sehr unterschiedlicher Weise auf die Videoüberwachung in ihrem Geschäft hingewiesen wurde.

Ich habe diese Einzelfallprüfung daher zum Anlass genommen, das Einkaufszentrum insgesamt, d. h. ca. 200 Einzelhandelsgeschäfte, einer diesbezüglichen Überprüfung zu unterziehen. Nach meinen Feststellungen hatte etwa ein Viertel der Geschäfte Videokameras in den Geschäftsräumen installiert, davon wiederum musste ich in etwa 60 % der Fälle Mängel bei der Kennzeichnung feststellen. Soweit ich bei meinen Kontrollen eine unzureichende Kennzeichnung festgestellt hatte, habe ich das Verkaufspersonal auf die Problematik hingewiesen, ein entsprechendes Informationsblatt mit der Bitte um Weiterleitung an die Geschäftsführung übergeben und zugleich eine Wiederholungskontrolle in etwa vier Wochen angekündigt. In den Fällen, in denen ich auch bei der Wiederholungskontrolle noch keine ausreichende Kennzeichnung feststellen konnte, habe ich diese Angelegenheit anschließend im schriftlichen Verfahren weiter verfolgt.

Die erzielten Kontrollergebnisse lassen sich wie folgt unterteilen:

- Kameras aktiv; Kennzeichnung ausreichend!
- Kameras aktiv; Kennzeichnung fehlt!
- Kameras aktiv; Kennzeichnung unzureichend!
- Kamera-Attrappen / Kameras inaktiv; Kennzeichnung vorhanden!
- Kamera-Attrappen / Kameras inaktiv; keine Kennzeichnung!
- keine Kameras vorhanden; Hinweise auf Videoüberwachung vorhanden!

Die drei letzten Varianten waren - jedenfalls aus datenschutzrechtlicher Sicht - unkritisch. Da tatsächlich keine Erhebung, Verarbeitung und Nutzung personenbezogener Daten erfolgt, ist weder das Bundesdatenschutzgesetz anwendbar noch die Kontrollzuständigkeit der Aufsichtsbehörde gegeben. Eventuelle Streitfälle zwischen dem Händler und den Betroffenen sind daher ggf. auf dem Zivilrechtsweg zu klären.

Probleme bei der Auseinandersetzung mit den verantwortlichen Stellen haben im Übrigen nur die Fälle bereitet, in denen eine Kennzeichnung zwar vorhanden, jedoch unzureichend war. Der geradezu klassische Fall bestand dabei darin, dass die im Allgemeinen - anders als alle sonstigen, sofort ins Auge fallenden Hinweise etwa auf Zahlungsmöglichkeiten etc. - sehr unauffällig gestalteten Kennzeichnungen in Knie- oder Schuhhöhe angebracht und damit durch die Kunden natürlich nicht wahrzunehmen waren. In anderen Fällen waren die Hinweise durch ständige Werbeträger, Grünpflanzen o. Ä. verdeckt oder sie befanden sich an den tagsüber dauerhaft geöffneten und damit dem Sichtfeld der Kunden entzogenen Eingangstüren und konnten daher im Grunde genommen nur außerhalb der Öffnungszeiten wirklich wahrgenommen werden. Auch dann, wenn sich die Hinweise zu weit weg vom Eingangsbereich an den Schaufenstern befunden haben, habe ich entsprechende Änderungen verlangt. Besonders auffällig war dabei der Fall eines Bekleidungsgeschäfts, dessen Geschäftsidee offensichtlich darin besteht, seinen Kunden ein Einkaufserlebnis in abgedunkelten Räumen zu ermöglichen. Hier waren die transparent gehaltenen Hinweise rechts und links an den am weitesten vom Eingang entfernten Schaufenstern angebracht, dabei aber infolge des abgedunkelten Verkaufsraums selbst dann kaum erkennbar, wenn man unmittelbar davor stand. Der Videoüberwachungshinweis eines Mobilfunkgeschäftes, dass Webcams installiert seien, die Bilder ins Internet übertragen, hat sich bei näherer Betrachtung als falsch erwiesen.

Die an den Eingangstüren des Einkaufszentrums befindlichen Hinweise auf die Videoüberwachung bezogen sich auf die allgemeinen Publikumsbereiche des Einkaufszentrums und wiesen *deren Betreiber* als verantwortliche Stelle aus. Sie waren also

schon deshalb nicht geeignet, die in der Verantwortung der jeweiligen Einzelhändler liegende Videoüberwachung in deren Ladengeschäft erkennbar zu machen.

Die also an den einzelnen Geschäften anzubringenden Hinweise müssen so platziert werden, dass für die betroffenen Personen eine zumutbare Möglichkeit der Kenntnisnahme besteht. Sie müssen mithin ohne großen Suchaufwand wahrnehmbar sein, damit die betroffene Person der Videoüberwachung gegebenenfalls ausweichen oder ihr Verhalten danach ausrichten kann. Je größer und unübersichtlicher der Raum ist, desto höhere Anforderungen sind zu stellen (Scholz in Simitis, BDSG, 7. Aufl., Rdnr. 107 zu § 6b). Ich habe daher regelmäßig eine deutlich wahrnehmbare Kennzeichnung in Augenhöhe an beiden Seiten des Eingangs, alternativ auch mittig, gefordert, um die Erkennbarkeit vor Betreten des Raumes zu gewährleisten, unabhängig davon, von welcher Seite man sich dem Geschäft genähert hat.

Es reicht auch nicht aus, wenn die Kameras als solche deutlich sichtbar im Verkaufsraum angebracht sind. Maßstab für die Erkennbarkeit sind die subjektiven Möglichkeiten der betroffenen Personen, die typischerweise den Raum betreten und sich in ihm aufhalten (Scholz a. a. O.) und das sind nun einmal Kunden, die in erster Linie das Warenangebot interessiert. Es ist niemandem zumutbar, vor Betreten eines Raumes erst dessen Wände und Decken nach eventuell vorhandenen Kameras absuchen zu müssen, zumal eine Vielzahl von Einzelhandelsgeschäften - auch das hat die Kontrolle gezeigt - durchaus ohne Videokameras auskommt und damit anders als etwa in Bankfilialen nicht von vornherein damit zu rechnen ist. Konkludente Hinweise in Form sichtbarer Kameras reichen daher im Regelfall nicht aus, dies gilt insbesondere dann, wenn die Kameras erst erkennbar sind, wenn sich die Betroffenen bereits in deren Erfassungsbereich befinden (Scholz a. a. O.).

In diesem Sinne schlecht beraten war eine Geschäftsinhaberin, die durch ihren Rechtsanwalt mitteilen ließ, dass sie wegen der Hinweise an den Eingangstüren des Einkaufszentrums einerseits sowie der Tatsache, dass bei ihr die Kameras sichtbar angebracht worden seien, andererseits meiner Aufforderung, geeignete Hinweise zur Kennzeichnung der Videoüberwachung an ihrem Ladengeschäft anzubringen, nicht nachkommen werde. Der Rechtsanwalt teilte mir insoweit u. a. mit, dass seine Mandantin vor allem deshalb eine Videoüberwachungsanlage in ihren Geschäftsräumen unterhalte, weil sie dort bereits mehrfach überfallen worden sei. Demnach ging es der Geschäftsinhaberin also vor allem darum, für die Zukunft weitere Überfälle zu verhindern. Eine solche präventive Wirkung kann eine Videoüberwachungsanlage aber nur entfalten, wenn für jedermann deutlich wahrnehmbar ist, dass das Ladengeschäft videoüberwacht ist. Die von mir auf der Grundlage des § 6b Abs. 2 BDSG geforderte Kennzeichnung dient auch diesem Zweck. Unter diesem Aspekt erschloss sich mir die Argumentation

des Rechtsanwalts in keiner Weise, da sie insoweit jedenfalls nicht dem Interesse seiner Mandantin, weitere Überfälle möglichst zu vermeiden, gedient hat. Weitere Aufsichtsmaßnahmen waren in diesem Fall allerdings nicht erforderlich, da die Geschäftsinhaberin dann - natürlich ohne dass der Rechtsanwalt von seiner Rechtsauffassung abgerückt ist - doch noch die erforderliche Kennzeichnung vorgenommen hat.

Nachfolgend sind einige Beispiele festgestellter unzureichender Kennzeichnung der Videoüberwachung aufgeführt:

8.1.4 Kamera-Kundenmonitor-Systeme

Zahlreiche Einzelhändler (Fachgeschäfte wie Supermärkte) haben offenbar die Videokamera in Verbindung mit einem Großbildmonitor als Möglichkeit zur Steigerung der Aufmerksamkeit ihrer Kundschaft entdeckt. Im Falle einer entsprechenden Eingabe waren Kamera und Großbildmonitor kurz hinter der Zugangsschranke zu einem Supermarkt in etwa vier Meter Höhe installiert; auf dem Monitor wiedergegeben wurde ein Livestream vom Eingangsbereich. Personen, die den Supermarkt betraten (und weit genug nach oben blickten) konnten sich somit in Echtzeit auf sich zukommen sehen.

Soweit die Kamera, die sich vorliegend unmittelbar unterhalb des Monitors befunden hat, die erfassten Bilder ohne Speicherung oder Übertragung an andere Orte ausschließlich auf diesen Monitor darstellt, bestehen aus datenschutzrechtlicher Sicht keine Bedenken, denn ein solches Kamera-Monitor-System hat letzthin nur die Wirkung eines Spiegels. Eine solche Anlage erfüllt somit nicht den in § 6b BDSG geregelten Tatbestand der Beobachtung. Beobachten in diesem Sinne erfordert ein bewusstes Hinzutreten der verantwortlichen Stelle, um das entstandene Bildmaterial ggf. auszuwerten. Dies ist vorliegend aber nicht der Fall. Mithin besteht auch keine Pflicht zur Kenntlichmachung der Anlage nach § 6b Abs. 2 BDSG. Für ähnliche Anlagen an anderen Standorten, wie sie z. B. im Ausstellungsbereich von Großbildmonitoren vorkommen, gelten grundsätzlich die gleichen Aussagen.

Für alle verantwortlichen Stellen, die mit der Aufstellung eines ähnlichen „Blickfangs“ liebäugeln, ergibt sich jedoch als zwingende Voraussetzung, dass der Zweck der Maßnahme nicht in Richtung Überwachung ausgeweitet wird. Dies umfasst selbstverständlich jedwede Form der permanenten Speicherung für spätere Auswertungen. Aber auch schon die Übertragung des Livestreams an einen der Beobachtung dienenden Ort (z. B. Hausdetektiv-Raum) würde den Anwendungsbereich des § 6b BDSG eröffnen.

8.1.5 Pausenräume

Ein Petent schilderte mir, dass ein vom Arbeitgeber zur Verfügung gestellter Pausenraum, in dem sich auch für die Nutzung durch die Arbeitnehmer vorgesehene elektronische Geräte befanden, videoüberwacht werde. Als Hintergrund teilte er mir mit, dass es in diesem Pausenraum in der Vergangenheit zu Einbrüchen und Zerstörungen gekommen sei. Er bat mich um Unterstützung, da er und seine Kollegen sich durch die Videokameras in ihrem Persönlichkeitsrecht beeinträchtigt sahen.

Auf meine Anfrage wurde mir mitgeteilt, dass die Kameras Aufzeichnungen fertigen würden und die Videoüberwachung dem Zweck diene, Straftaten und Ordnungswidrigkeiten zu verhindern und aufzuklären. Das Eigentum des Arbeitgebers sollte auf diese

Weise geschützt werden. Die Videoüberwachung richte sich nicht gegen die eigenen Mitarbeiter. Während der Einbrüche seien keine Mitarbeiter vor Ort gewesen.

Meine Prüfung ergab, dass die vorgesehene Videoüberwachung - entgegen der Auffassung des Arbeitgebers - weder auf § 32 Abs. 1 Satz 2 BDSG noch auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG gestützt werden konnte.

§ 32 Abs. 1 Satz 2 BDSG gestattet die Erhebung personenbezogener Daten eines Beschäftigten - vorbehaltlich des Vorliegens weiterer Voraussetzungen -, wenn es zur Aufdeckung von Straftaten erforderlich ist. Bei der Einführung des § 32 BDSG war es nicht Intention des Gesetzgebers, die entwickelten Grundsätze des Beschäftigtendatenschutzes zu ändern. Ausgehend hiervon wäre daher für die Einführung einer Videoüberwachung das Bestehen eines räumlich oder funktional auf eine bestimmte Mitarbeitergruppe konkretisierten Verdachts erforderlich gewesen. Aufgrund der Mitteilung, dass sich die Videoüberwachung selbstverständlich nicht gegen die eigenen Mitarbeiter richte, musste ich vom Nichtbestehen eines solchen Verdachts ausgehen. Dies hatte zur Folge, dass § 32 Abs. 1 Satz 2 BDSG als Rechtsgrundlage für eine zulässige Videoüberwachung nicht in Betracht kam.

Darüber hinaus ist die Erhebung von Daten gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG zur 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 Verarbeitung überwiegt.

Wenngleich die Videoüberwachung der technischen Geräte im Pausenraum grundsätzlich zur Verhütung und/oder Aufklärung von Straftaten geeignet ist, habe ich diese im vorliegenden Fall nicht für erforderlich erachtet, da mildere Mittel hierzu existieren, jedenfalls aber schutzwürdige Belange der Betroffenen am Ausschluss der Verarbeitung überwiegen. Denn durch die Videoüberwachung werden hauptsächlich - wenn nicht sogar ausschließlich - Personen der Überwachung ausgesetzt, die hierfür keinen Anlass gegeben haben. Zu berücksichtigen war weiterhin, dass zwar keine Pflicht zur Nutzung des Pausenraums besteht, sich teilweise aus besonderen Umständen jedoch eine faktische Notwendigkeit ergeben konnte. Zudem fand die Überwachung zu Zeiten statt, in denen die Arbeitnehmer gerade nicht dem arbeitgeberseitigen Direktionsrecht unterstehen. Allein die Tatsache, dass die Aufnahmen nur im Falle eines besonderen Vorkommnisses ausgewertet würden, konnte - entgegen der arbeitgeberseitigen Auffassung - den Überwachungsdruck nicht beseitigen.

Dieser Auffassung wollte der betroffene Arbeitgeber zunächst nicht folgen. Erst im Rahmen einer Anhörung zum Erlass einer Anordnung erklärte sich der Arbeitgeber bereit, die Kameras zur Überwachung der elektronischen Geräte zu deaktivieren und lediglich die (Innen-)Kameras zur Überwachung der Eingänge weiterbetreiben zu wollen.

Wenngleich eine Videoüberwachung der Türen von außen nach meiner Auffassung vorzugswürdig gewesen wäre, habe ich mich hiermit einverstanden erklärt. Denn die Überwachung des Zugangs erachte ich im Hinblick auf den verfolgten Zweck und die Vorkommnisse der Vergangenheit als zulässig. Die Nutzung der Pausenräume steht den Mitarbeitern frei. Der durch die Überwachung des Zugangs entstehende Überwachungsdruck ist nicht so stark, als dass er die vom Arbeitgeber verfolgten Zwecke überwiegen würde.

Grundsätzlich gehe ich in Fällen wie dem vorliegenden davon aus, dass eine Überwachung der Zugänge von außen ausreichend ist. Sie wird neben dem arbeitgeberseitigen Interesse am Schutz seines Eigentums sowie der Verhütung und Aufklärung von Straftaten auch dem Interesse der Arbeitnehmer an der Wahrung von deren Persönlichkeitsrechten gerecht. Darüber hinaus käme in gleichgelagerten Fällen auch eine Videoüberwachung zu Zeiten, in denen sich bestimmungsgemäß keine Arbeitnehmer im Pausenraum aufhalten, in Betracht. Auch bestünde die Möglichkeit die Videoüberwachung an den (berechtigten) Zugang zum Pausenraum derart zu koppeln, dass dieser - zeitunabhängig - nur dann, wenn sich kein Mitarbeiter im Pausenraum aufhält, überwacht wird.

8.1.6 Bäckereien

Auffällig gehäuft haben sich im Berichtszeitraum Eingaben von Mitarbeitern von Bäckereien unterschiedlicher Größe. Dabei ging es regelmäßig um die Zulässigkeit von Innenkameras in den Produktionsräumen. Mit Videokameras überwacht worden sind Backstuben, Fettbackräume, Konditorei- und Kommissionierungsräume sowie auch Flure. In einem besonders krassen Fall gab es so praktisch keinen nicht überwachten Arbeitsraum.

Die von den Inhabern bzw. Geschäftsführern der Bäckereien angegebenen Gründe waren sehr vielfältig:

- Qualitätskontrolle bzw. -überwachung,
- Kontrolle der Einhaltung von Hygienevorschriften,
- Optimierung der Arbeitsabläufe,

- Schutz vor und Aufklärung von Einbrüchen,
- Schutz vor und Aufklärung von Diebstählen sowie
- Aufklärung besonderer betrieblicher Vorkommnisse.

Alle diese Gründe konnten eine Videoüberwachung jedoch nicht rechtfertigen:

Auch in den Großbäckereien, bei denen einzelne Mitarbeiter auf den Videobildern infolge ihrer einheitlichen Arbeitskleidung und großräumiger Aufnahmen für Dritte - ich nehme mich da nicht aus - nicht in jedem Fall schon aufgrund der erkennbaren Bilddetails ohne Weiteres identifizierbar waren, hat es sich bei den Videoaufnahmen zweifellos um personenbezogene Daten gehandelt, denn jedenfalls für den Arbeitgeber mit seinem Zusatzwissen über Arbeitsaufgaben und Arbeitszeiten war auch in diesen Fällen der Personenbezug problemlos herstellbar.

Die Beurteilung der Zulässigkeit einer Videoüberwachung von Bereichen, die nur für Mitarbeiter bestimmt sind, hier also den Arbeitsräumen, erfolgt auf der Grundlage des § 32 Abs. 1 BDSG.

Nach Satz 1 dieser Vorschrift dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. Ein solches, direkt aus der Natur des Arbeitsverhältnisses selbst abzuleitendes Erfordernis besteht vorliegend nicht, insbesondere ergibt sich dies auch nicht aus den von den Bäckereien angeführten Gründen.

Bei der Qualitätskontrolle und -überwachung sowie der Kontrolle der Einhaltung von Hygienevorschriften handelt es sich um originäre Aufgaben des jeweiligen Schichtleiters bzw. Bäckermeisters, zumal Verstöße ein sofortiges Einschreiten und nicht nur eine nachträgliche Auswertung erfordern, ganz abgesehen davon, dass die jeweiligen Arbeitgeber gar nicht in der Lage sein dürften, die Aufzeichnungen ganzer Nächte auf solche Verstöße hin auszuwerten. Die Videoüberwachung für diese Zwecke ist also weder geeignet noch angemessen und damit auch nicht erforderlich.

Die Optimierung der Arbeitsabläufe im Rahmen der Einführung neuer Produktionstechnik kann eine Videoüberwachung gleichfalls nicht rechtfertigen. Wenn diesbezüglich Probleme erkannt werden sollen, sollten die dafür verantwortlichen Personen stattdessen das Gespräch mit den jeweiligen Mitarbeitern suchen oder sich in der Einführungszeit persönlich und vor Ort ein Bild von den veränderten Arbeitsabläufen verschaffen.

Darüber hinaus dürfen gemäß § 32 Abs. 1 Satz 2 BDSG personenbezogene Daten eines Beschäftigten zur Aufdeckung von Straftaten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Eine dauerhafte, präventive Dauerüberwachung ist von dieser Vorschrift also nicht gedeckt. Eine Videoüberwachung ist nur dann und auch nur zeitweise zulässig, wenn tatsächliche Anhaltspunkte dafür bestehen, dass ein Beschäftigter im Beschäftigungsverhältnis eine Straftat begangen hat.

Soweit also zur Begründung der Videoüberwachung einzelne Diebstähle oder Manipulationen an Maschinen angeführt worden sind, kann dies zur Täterüberführung - in Abhängigkeit von dem eingetretenen Schaden - allenfalls eine zeitlich begrenzte Videoüberwachung eng umgrenzter Bereiche, keinesfalls jedoch eine dauerhafte Totalüberwachung des Personals rechtfertigen. Ich weise zudem darauf hin, dass die Videoüberwachung für diese Zwecke auch tatsächlich erforderlich sein muss, d. h. sie muss einerseits zur Zweckerreichung geeignet sein, andererseits darf es keine milderen Mittel geben, mit denen der angestrebte Zweck gleichfalls erreicht werden kann. Diese Voraussetzungen sind beispielsweise in Großbäckereien (bei voller Besetzung) dann nicht gegeben, wenn die Aufnahmebereiche so groß gewählt sind (um möglichst alle Bereiche abzudecken), dass ggf. relevante Handlungen gar nicht aus der Unmenge von Bildinformationen herausgefiltert werden können. An der Erforderlichkeit fehlt es in vielen Bereichen auch schon wegen der starken sozialen Kontrolle, da die meisten Mitarbeiter - jedenfalls in Großbäckereien - unter Anleitung und Kontrolle von Vorarbeitern tätig sind. Um Manipulationen an für die Produktion in besonderem Maße relevanten Maschinen und Anlagen zu verhindern, sind im Übrigen auch mildere Mittel denkbar. Dazu zähle ich - neben einer punktuellen Videoüberwachung - beispielsweise passwortgeschützte Steuerungen oder mechanische Schutzeinrichtungen (z. B. Schlüsselschalter), um unbefugte Schalthandlungen zu vermeiden.

Auch das Einverständnis der betroffenen Mitarbeiter kann eine über die genannten Aspekte hinausgehende Videoüberwachung nicht legitimeren, da eine solche Erklärung wegen des typischerweise im Arbeitsverhältnis bestehenden Über- und Unterordnungsverhältnisses der Arbeitsvertragsparteien grundsätzlich nicht als freiwillig im Sinne des § 4a Abs. 1 BDSG anzusehen ist.

In diesem Zusammenhang von Bedeutung ist zudem noch die höchstrichterliche Rechtsprechung des BAG, die eine dauerhafte Videoüberwachung von Arbeitnehmern ebenfalls für unzulässig erklärt hat:

Danach erfasst eine dauerhafte Überwachung am Arbeitsplatz die betroffenen Personen nicht nur kurzfristig und vorübergehend. Sie wiederholt sich vielmehr potenziell an jedem Arbeitstag und dauert jeweils mehrere Stunden bzw. erstreckt sich über die gesamte Arbeitszeit. Der Arbeitnehmer kann den Besuch des überwachten Bereichs weder vermeiden noch sich der Überwachung durch ein Verlassen seines Arbeitsplatzes entziehen. Zudem ist der überwachte Personenkreis dem Arbeitgeber von vornherein bekannt; der Überwachungsdruck daher für die betroffenen Mitarbeiter besonders groß (BAG 29. Juni 2004 - 1 ABR 21/03 - RDV 2005, 21 ff.). Wenn sich Arbeitsplätze dauerhaft im Blickfeld einer Kamera befinden, werden die dort tätigen Mitarbeiter - bewusst oder unbewusst - einem Anpassungsdruck dahingehend ausgesetzt, dass sie sich in jeder Hinsicht möglichst unauffällig verhalten müssen, um nicht Gefahr zu laufen, später in irgendeiner Weise Gesprächsobjekt zu werden und Vorhaltungen oder Verdächtigungen ausgesetzt zu sein. Dies stellt einen erheblichen Eingriff in das Persönlichkeitsrecht dar (BAG 14. Dezember 2004 - 1 ABR 34/03 - RDV 2005, 216 ff.).

Erfolgt eine Videoüberwachung präventiv zum Zweck des Einbruchs- und Diebstahlschutzes außerhalb der Arbeitszeiten bzw. außerhalb der Zeiten, in denen in den betreffenden Bereichen gearbeitet wird, ist sie auf diese Zeiträume zu beschränken. Um auch in diesen Fällen unnötigen, aus der bloßen Existenz der Überwachungstechnik resultierenden Überwachungsdruck für die Beschäftigten zu vermeiden, sind die Kameras dabei möglichst nur auf die insoweit kritischen Bereiche wie Türen, Tore und Fenster auszurichten.

8.1.7 Kennzeichenerfassung zur Ermittlung von Kundenströmen

Hinweisen zufolge sollte in einem großen Einkaufspark eine Erfassung und Überprüfung der Kennzeichen der auf die Parkplätze, Parkdecks und in die Tiefgarage einfahrenden und von dort jeweils wieder ausfahrenden Fahrzeuge stattfinden. Dem Vernehmen nach geschehe dies zur Unterstützung der Polizei bei der Ermittlung von Autodieben und Sachbeschädigern.

Bei meiner daraufhin durchgeführten Kontrolle konnte ich zunächst feststellen, dass alle Ein- und Ausfahrten der Parkplätze des Einkaufsparks videoüberwacht waren. Die betreffenden Kameras waren mit einer Bewegungserkennung ausgerüstet, die dem Betreiber eine Fahrzeugzählung sowie damit verbunden die Steuerung seines Parkplatzleitsystems ermöglichen sollte. Vier dieser Kameras (jeweils an den Parkplatzausfahrten)

verfügten darüber hinaus über eine Kennzeichenerkennung; bei drei Kameras war diese Kennzeichenerfassung auch tatsächlich aktiv.

Mit Hilfe der drei Kameras wurden von allen ausfahrenden Fahrzeugen Kennzeichen, Land, Ausfahrtsort, Ausfahrtszeit (Datum, Uhrzeit), Geschwindigkeit sowie verschiedene anlagenbezogene Daten erhoben und gespeichert. Die Speicherzeiten betrugen etwa sechs Wochen. Als (ursprünglichen) Zweck dieser Erhebung und Verarbeitung personenbezogener Kundendaten sind mir statistische Zwecke, insbesondere die Erfassung von Kundenfrequenzen und die Ermittlung der Einzugsgebiete angegeben worden; eine Nutzung dieser Daten habe bislang jedoch noch nicht stattgefunden.

Die Erhebung und Verarbeitung von Fahrzeugkennzeichen sowie weiterer personenbezogener Daten an den Parkplatzausfahrten war unzulässig.

Gemäß § 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.

Da das Einholen einer Einwilligung (vgl. § 4a BDSG) in die Erhebung, Verarbeitung und Nutzung der an den Parkplatzausfahrten erhobenen Daten von den Kunden allein schon aus praktischen Erwägungen nicht zur Debatte stand, kamen von den Zulässigkeitstatbeständen des BDSG nur § 28 Abs. 1 Satz 1 Nr. 1 und 2 in Betracht.

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. Die Parkplätze sind den Kunden kostenfrei zur Verfügung gestellt worden - ein wie auch immer geartetes, in unmittelbarem Zusammenhang mit der Parkplatznutzung stehendes Erfordernis, Fahrzeugkennzeichen und Ausfahrtsdaten von den Kunden zu erheben, war hier nicht ersichtlich.

Nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke weiter zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Das insoweit sicherlich berechtigte Interesse des Betreibers des Einkaufsparks bestand in der Ermittlung der Einzugsgebiete seiner Kunden. Eine Erhebung von Fahrzeugkenn-

zeichen und Ausfahrtsdaten wäre in diesem Zusammenhang aber nur erforderlich, wenn die erhobenen Daten einerseits zur Zweckerreichung geeignet sind und es andererseits keine milderen Mittel gibt, mit denen der angestrebte Zweck gleichfalls erreicht werden kann.

Für die Ermittlung der Einzugsgebiete kommt zunächst überhaupt nur das Fahrzeugkennzeichen bzw. dessen erster Teil in Betracht. Die Erhebung und Verarbeitung der übrigen Daten wie Ausfahrtsort, Ausfahrtszeit und Geschwindigkeit ist dafür ohne Bedeutung, deren Erhebung und Verarbeitung im Rahmen der angegebenen Zweckbestimmung also schon von vornherein unzulässig. Aus dem Fahrzeugkennzeichen selbst kann - gerade in Sachsen - nur sehr eingeschränkt auf den Wohnort des jeweiligen Kunden geschlossen werden. Einerseits ist seit September 2010 die Mitnahme des bisherigen Kfz-Kennzeichens bei einem Umzug innerhalb des Freistaates Sachsen möglich, andererseits - und das gilt überall - gibt es eine Vielzahl von Fällen, in denen das Fahrzeugkennzeichen keinen Rückschluss auf den jeweiligen Wohnort zulässt, etwa weil es sich auch um privat genutzte Dienstwagen oder um Leihwagen handelt. Insoweit ist also schon die Eignung der Fahrzeugkennzeichen für die Ermittlung der Einzugsgebiete zu verneinen. Der Betreiber hat mir gegenüber dann auch selbst eingeräumt, dass andere (bereits praktizierte) Methoden zur Ermittlung der Einzugsgebiete wesentlich geeigneter seien, so etwa die Abfrage der Postleitzahl beim Bezahlen oder die eigenständige Ermittlung der (theoretischen) Anreisezeiten. Diese Methoden stellen insoweit auch das mildere Mittel dar, da sie ohne eine Erhebung und Verarbeitung personenbezogener Daten auskommen. Eine Nutzung der erfassten Kennzeichendaten für die ursprünglich beabsichtigten Zwecke hat offensichtlich auch aus diesen Gründen bislang noch nicht stattgefunden. Der Betreiber ist daher meiner Aufforderung zur Einstellung der Erfassung der Ausfahrtsdaten auch umgehend gefolgt.

Auch wenn es damit auf eine Abwägung mit den schutzwürdigen Betroffeneninteressen nicht mehr ankam, ist festzuhalten, dass auch diese zur Unzulässigkeit der Erhebung und Verarbeitung von Fahrzeugkennzeichen und Ausfahrtsdaten geführt hätte. Die Tatsache, dass anhand der gespeicherten Daten die Häufigkeit und auch die konkreten (Ausfahrts-)Zeitpunkte der Besuche eines Einkaufsparks nachvollzogen werden können, verletzt klar schutzwürdige Interesse der Kunden, zumal diese Datenerhebung auch noch verdeckt, d. h. ohne Wissen der Betroffenen, erfolgt war.

8.1.8 Unterrichtung Betroffener bei Kamera-Attrappen

Soweit mir Petenten darlegen, dass sie von einer möglicherweise rechtswidrigen Videoüberwachungsanlage persönlich betroffen sind, es sich also nicht nur um bloße Hinweis-

geber handelt, haben sie regelmäßig einen Anspruch auf Mitteilung des Überprüfungsergebnisses (§ 38 Abs. 1 Satz 6 BDSG, vgl. dazu auch 5. TB, Pkt. 4.2.4).

Wenn ich bei der Überprüfung einer Videoüberwachungsanlage feststelle, dass es sich bei den installierten Kameras lediglich um Attrappen handelt, teile ich den Betroffenen daher mit, dass ich eine Überprüfung des geschilderten Sachverhalts vorgenommen und dabei keinen Verstoß gegen das Bundesdatenschutzgesetz festgestellt habe. Denn dessen Anwendungsbereich ist gemäß § 1 Abs. 2 Nr. 3 BDSG nur eröffnet, wenn tatsächlich personenbezogene Daten erhoben, verarbeitet und genutzt werden. Beim Einsatz von Kamera-Attrappen ist dies definitiv nicht der Fall; ein Verstoß gegen das Bundesdatenschutzgesetz kann folglich nicht vorliegen. Soweit jemand aus der Existenz und Blickrichtung der Kameras gleichwohl und unverändert einen Überwachungsdruck für sich ableitet, kann er auf dem Zivilrechtsweg dagegen vorgehen.

Soweit im Einzelfall angezeigt, teile ich darüber hinaus noch mit, dass spezielle, vom Petenten genannte Bereiche nicht mittels der in Rede stehenden Kameras überwacht werden und erläutere, dass allein aus der Existenz und Ausrichtung einer Kamera nicht notwendigerweise darauf geschlossen werden kann, dass überhaupt eine Überwachung stattfindet bzw. falls dies der Fall ist, welche Bereiche tatsächlich überwacht werden. Es gibt heute vielfältige technische Möglichkeiten, den Erfassungsbereich einer Kamera beispielsweise durch Ausblendungen entsprechend zu beschränken und damit Persönlichkeitsrechtsverletzungen auszuschließen.

Zu weitergehenden Auskünften oder Begründungen, insbesondere zur Mitteilung der Tatsache, dass es sich im konkreten Fall ggf. um eine Kamera-Attrappe handelt, bin ich weder befugt noch verpflichtet. Petenten haben zwar einen Rechtsanspruch, nach Abschluss der Ermittlungen darüber unterrichtet zu werden, ob eine Verletzung ihrer Rechte vorliegt oder nicht, nicht jedoch auf bestimmte tatsächliche oder rechtliche Feststellungen; eine ins Einzelne gehende Begründung ist nicht vorgeschrieben (vgl. Dammann in Simitis, BDSG, 7. Aufl., Rdnr. 20 zu § 21). Ich verweise auch darauf, dass ich bei der Ausübung meiner Kontrolltätigkeit amtlichen Verschwiegenheitspflichten unterliege und im Rahmen der Beantwortung von Eingaben Geschäftsgeheimnisse der verantwortlichen Stelle nicht unbefugt offenbaren darf. Dabei spielt auch eine Rolle, dass die präventive Wirkung einer Kameraüberwachung natürlich nur dann gegeben ist, wenn diese Tatsache nicht allgemein bekannt wird. § 38 Abs. 1 Satz 6 BDSG sieht eine (weitergehende) Unterrichtung der Betroffenen nur für den Fall vor, dass tatsächlich ein Datenschutzverstoß festgestellt worden ist.

Wenn mir die verantwortliche Stelle allerdings - einzelfallbezogen - die Erlaubnis erteilt, den Petenten darüber zu unterrichten, dass lediglich Kamera-Attrappen montiert sind, werde ich dies natürlich entsprechend mitteilen.

8.2 Internet

8.2.1 Beurteilung der Qualität des Schulessens

Ein das Gymnasium besuchender Fünftklässler hatte mehrmals über das Internet die Qualität des Schulessens kritisiert, woraufhin er schließlich eines Tages beim Empfang seines Essens durch das Küchenpersonal beschimpft und der Verbreitung von Unwahrheiten bezichtigt worden war.

Für die Essensbewertung hatte das beauftragte Catering-Unternehmen eine spezielle Bewertungsseite auf seinem Internetauftritt vorgehalten. Dort konnten Lehrer, Erzieher, Eltern und Schüler das Schulessen nach verschiedenen Kriterien bewerten, Kommentare und Erläuterungen dazu abgeben und auch angeben, ob in dieser Angelegenheit eine Rückkopplung durch das Catering-Unternehmen erwünscht war. Dazu bestand die Möglichkeit, entsprechende Kontaktdaten (Name, Telefon, E-Mail) anzugeben. Die jeweilige Kundennummer war jedoch als Pflichtfeld ausgewiesen.

Eine anonyme Essensbewertung war damit nicht möglich. Über die Kundennummer war das Catering-Unternehmen jederzeit in der Lage, die Identität des Bewerters zu ermitteln. Der betreffende Schüler hatte in keinem Fall den Wunsch einer Kontaktaufnahme durch den Essensanbieter angekreuzt und er hatte auch seinen Namen nicht im Bewertungsformular angegeben. Dennoch war er - über seine Kundennummer - bestimmt und das Servicepersonal über seine Identität unterrichtet worden. Eine derartige Nutzung der Angaben aus dem Bewertungsformular war zweifelsfrei unzulässig, zumal der Schüler seine Kritik sehr sachlich und konkret (zusammengeklebte Nudeln, Haar im Essen) formuliert hatte.

Dass die Reaktion des Personals auf die durch den Schüler geübte Kritik im Übrigen nicht in Ordnung gewesen war, bedarf sicher keiner weiteren Begründung. Eine leitende Mitarbeiterin hatte sich daher dann auch bei den Eltern des Schülers entschuldigt und auch das Servicepersonal hat sein Fehlverhalten eingeräumt und sich - nach Abstimmung mit den Eltern - im Rahmen eines Gesprächs gleichfalls bei dem Schüler entschuldigt.

In besonderem Maße kritisch gesehen und im Ergebnis als unzulässig bewertet habe ich neben dem Pflichtfeld „Kundennummer“ auch die Abfrage bzw. Erhebung der Kontaktdaten von Minderjährigen. Eine Notwendigkeit hierfür konnte ich nicht erkennen, ganz

abgesehen davon, dass jedenfalls die Angehörigen der unteren Klassenstufen überhaupt noch nicht in der Lage sind, die möglichen Folgen der Offenlegung ihrer Identität und ihrer Kontaktdaten einzuschätzen. Die Kontaktdaten waren zwar als solche nicht als Pflichtfelder gekennzeichnet, jedoch erschließt sich die Unterscheidung zwischen notwendigen und optionalen Kontaktangaben diesem in der Internetnutzung eher unerfahrenen Personenkreis im Regelfall noch nicht. Das Bewertungsformular bedurfte insoweit dringender und gründlicher Überarbeitung. Soll eine Bewertungsmöglichkeit für Schüler beibehalten werden, darf eine nachfolgende Eingabe der Kontaktdaten einschließlich der Kundennummer praktisch nicht mehr möglich sein. Dies könnte beispielsweise dadurch erreicht werden, dass die Abfrage der „Funktion“ bzw. Stellung des Bewerters - Lehrer, Erzieher, Eltern oder Schüler - an den Anfang gestellt und als obligatorisch deklariert wird. Abhängig von der hier getroffenen Auswahl könnten sich dann weitere Eingabefelder (z. B. für die Kontaktdaten) öffnen oder auch nicht.

8.2.2 Identitätsprüfung bei der Anlage von Nutzeraccounts

Gelegentlich erhalte ich Beschwerden von Nutzern, die unter Bezugnahme auf eine vermeintliche Mitgliedschaft vom Betreiber eines Webportals Werbemails bzw. Newsletter erhalten, ohne dass sie sich je bei diesem Portal angemeldet haben.

Meine Erfahrung zeigt, dass Nutzer mitunter auch schnell einmal vergessen, auf welchen Internetseiten sie unterwegs gewesen sind und wo sie sich überall einmal angemeldet haben (vgl. dazu auch 5. TB, Pkt. 4.3.2.3). Andererseits sind mir auch Fälle bekannt geworden, in denen solche Anmeldungen unbefugt durch Dritte vorgenommen worden sind. Insoweit ist der Nachweis eines rechtmäßigen Newsletterversands bei bestrittener Anmeldung regelmäßig schwer bis unmöglich. Die Betroffenen haben in solchen Fällen auch keine Möglichkeit, den Versand von Newslettern über entsprechende Einstellungen in ihrem Nutzerprofil zu unterbinden oder ihren Account gleich ganz zu löschen, denn die Zugangsdaten zu ihrem „eigenen“ Account sind ihnen bei dieser Fallgestaltung eben gerade nicht bekannt.

Noch komplizierter wird es dann, wenn Nutzer mehrere E-Mail-Adressen haben und damit adressierte E-Mails alle im gleichen Postfach eingehen. Reagiert der Betroffene dann unter einer anderen E-Mail-Adresse auf eingegangene Werbemails, wird er sich regelmäßig mit einer Weigerung der verantwortlichen Stelle, seinem Löschungs- oder Auskunftsverlangen zu entsprechen bzw. seinen Werbewiderspruch zu berücksichtigen, konfrontiert sehen. Denn - und das ist auch für mich nachvollziehbar - dann ist für die verantwortliche Stelle nicht ausreichend sicher erkennbar, dass der Absender dieser E-Mail mit dem Empfänger der Werbemail und Inhaber des Nutzeraccounts tatsächlich identisch ist.

Ursächlich für die Missbrauchsproblematik, d. h. für die Möglichkeit der unbefugten Anmeldung durch Dritte, sind regelmäßig Unzulänglichkeiten bei der Gestaltung des Anmeldeprozesses. Soweit in einem Anmeldeprozess für ein Webportal keine wirksame Identitätsprüfung integriert ist, insbesondere nicht überprüft wird, ob der Inhaber der eingegebenen E-Mail-Adresse auch tatsächlich die Person ist, die die Anmeldung vornimmt, ist dem Missbrauch Tür und Tor geöffnet. In diesem Fall ist es ohne weiteres möglich, andere Personen mit deren E-Mail-Adresse ohne ihr Wissen auf dem betreffenden Webportal anzumelden und sie so auch ungewollt zum Empfänger von Werbemails zu machen. Diese Personen haben dann mangels Kenntnis ihrer Zugangsdaten auch keine Möglichkeit, ihr Profil zu bearbeiten oder zu löschen.

Abhilfe kann hier beispielsweise eine DOI-Lösung schaffen. Nach erfolgter Erstanmeldung erhalten die betreffenden Nutzer an die bei der Anmeldung angegebene Adresse eine E-Mail mit der Aufforderung, die Anmeldung noch einmal ausdrücklich zu bestätigen. Der Inhaber der bei der Anmeldung angegebenen E-Mail-Adresse muss also noch einmal aktiv werden, indem er auf diese E-Mail in der vom Absender vorgegebenen Weise reagiert, also etwa eine Antwort zurücksendet oder einen in der E-Mail enthaltenen Link anklickt.

8.2.3 Einrichtung von Nutzeraccounts für den Ticketerwerb

Durch eine Eingabe bin ich auf ein städtisches Theater aufmerksam geworden, das in Konkurrenz zu privaten Angeboten steht und daher die Vorgaben des Bundesdatenschutzgesetzes ebenso wie diese Stellen zu beachten hat, also nach diesem Rechtskreis meiner Aufsicht untersteht (§ 2 Abs. 3 SächsDSG).

Die Betroffene störte sich daran, dass der im Auftrag und damit in Verantwortung des Theaters (§ 11 BDSG) agierende Online-Ticket-Dienstleister mittels entsprechender Internet-Buchungsmasken eine Vielzahl von Angaben verlangte und die so erhobenen Daten offenbar - auch bei einem nur einmaligen Theaterbesuch - als Daueraccount unbegrenzt weiter speicherte.

Nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist eine Verarbeitung personenbezogener Daten aus Gründen eines Rechtsgeschäfts jedoch nur insoweit zulässig, wie dies zu dessen Durchführung erforderlich ist. Nach einem Hinweis auf die Rechtslage verzichtete das Theater daher auf die Erhebung des Geburtsdatums und die verpflichtende Angabe einer Telefonnummer, da zur Bestimmung der Person des Kartenkäufers allein dessen Adresse, zur Zahlung dessen Zahlungsdaten und zur kurzfristigen Kontaktaufnahme dessen E-Mail-Adresse ausreichten.

Weiterhin konnte ich erreichen, dass Nutzeraccounts spätestens nach 24 Monaten Inaktivität gelöscht werden, falls Kunden nicht über einen Bestätigungslink in einer Erinnerungsmail die Beibehaltung der Registrierung wünschen. Zudem kann der Account künftig auch sofort nach dem Theaterbesuch von den Kunden vorzeitig gelöscht werden. Beim Veranstalter bleiben somit (in gesperrter Form - § 35 Abs. 3 Nr. 1 BDSG) nur noch jene Daten, deren weitere Speicherung nach § 257 Abs. 1 Nr. 2 HGB handelsrechtlich und § 147 Abs. 1 Nr. 2 AO steuerrechtlich geboten ist. Sie dürfen erst nach Ablauf der dort vorgegebenen Zeiträume gelöscht werden.

8.2.4 Verarbeitung von Nutzerdaten bei abgebrochenen Buchungsvorgängen

Nachdem potentielle Kunden eines Reiseportals die Dateneingabe im Rahmen einer (zunächst gewollten) Buchung kurz vor Ende abgebrochen, d. h. den Buchungsvorgang bewusst nicht zu Ende geführt hatten, waren sie anschließend auf der Grundlage der bis zum Zeitpunkt des Abbruchs bereits erhaltenen (Kontakt-)Daten durch den Portalbetreiber bis zu dreimal innerhalb von drei Tagen mit dem Hinweis, dass die Buchung noch nicht abgeschlossen gewesen sei, angeschrieben worden. Dabei war ihnen über einen individuellen Link die Möglichkeit geboten worden, diese Buchung doch noch abzuschließen. Grund genug, mit der Bitte um Klärung der datenschutzrechtlichen Zulässigkeit an mich heranzutreten. Die Betroffenen machten mit Verweis auf ihre (bewusst) nicht abgeschlossene Buchung geltend, dass der Portalbetreiber ihre Daten nicht hätte speichern und für das Abbrechermailing verwenden dürfen.

Von den Fällen bewusster Buchungsabbrüche (z. B. wegen unerwarteter, d. h. vorher nicht avisierter Zusatzkosten) sind die Fälle unbewusster (mangels ausreichender Internetkenntnisse - der Portalbetreiber verwies hierbei auf das zunehmende Alter seiner Kunden) Buchungsabbrüche bzw. solcher infolge technischer Probleme zu unterscheiden. Für den Portalbetreiber ist insoweit sicherlich nicht ohne weiteres erkennbar, welche Ursache einer abgebrochenen Buchung letztendlich zugrunde gelegen hat. Bei mir schlagen dann naturgemäß nur die Fälle auf, in denen Nutzer den Buchungsprozess bewusst abgebrochen haben. Nach Angaben des Betreibers sollen etwa 6 % der daraufhin angeschriebenen Nutzer ihre Buchung anschließend doch noch vollständig abgeschlossen, d. h. eine verbindliche Buchungsanfrage ausgelöst haben.

Im Rahmen der Sachverhaltsermittlung wurde zunächst deutlich, dass es sich um einen zweistufigen Buchungsprozess handelte. In der ersten Buchungsmaske wurden u. a. die Kontaktdaten des Internetkunden erhoben, zudem war bereits hier die Kenntnisnahme der AGB und der Hinweise zum Datenschutz zu bestätigen. In der zweiten Buchungsmaske waren dann u. a. die Zahlungsdaten einzugeben; abschließend war der Button „Jetzt kaufen“ zu betätigen.

Ich habe diesen Sachverhalt wie folgt bewertet:

Soweit es infolge des Abbruchs eines Buchungsvorgangs nicht zum Abschluss eines Vermittlungsauftrags gekommen ist, nichtsdestoweniger aber bereits eine Reihe von Buchungsdaten, insbesondere Kontaktdaten, erhoben und gespeichert worden sind, ist die Vorgehensweise, sich angesichts nicht bekannter Ursachen für den Abbruch der Dateneingabe zunächst noch einmal an den (potentiellen) Kunden zu wenden und diesem die Möglichkeit zu bieten, seine Dateneingabe auf bequeme Art und Weise zu vollenden, zwar als zulässig anzusehen, jedoch wird aber dann kein Grund für die weitere Speicherung der bis zum Abbruch der Dateneingabe bereits erfassten Daten mehr gesehen, wenn der Kunde auf diese Erinnerung innerhalb eines angemessenen Zeitraums nicht reagiert oder sogar aktiv zu erkennen gegeben hat, dass er nicht mehr am Abschluss eines Vermittlungsauftrags interessiert ist. Keinesfalls zulässig ist es, die so erhobenen Daten darüber hinaus auch noch für andere (insbesondere Marketing-)Zwecke, beispielsweise die Newsletterzusendung, zu nutzen.

Die Zulässigkeit dieser Verfahrensweise ergibt sich aus § 28 Abs. 1 Satz 1 Nr. 1 BDSG, wonach das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig ist, wenn es für die Begründung eines rechtsgeschäftlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Der Kunde hat mit der Eingabe seiner Kontaktdaten, ggf. sogar auch schon seiner Zahlungsdaten, zu erkennen gegeben, dass er am Abschluss eines Vermittlungsauftrags interessiert ist und einen solchen auch abschließen will, denn für die bloße Recherche nach günstigen Reisen oder Flugverbindungen ist ein Ausfüllen der Buchungsmaske nicht notwendig. Insoweit ist also die Phase des Vertragsabschlusses bereits eingeleitet. Aus für den Portalbetreiber nicht bekannten Gründen ist der Vertragsabschluss dann aber kurz vor Ende doch noch gescheitert, d. h. der Kunde hat den Vermittlungsauftrag dann tatsächlich nicht verbindlich ausgelöst bzw. nicht auslösen können. Vor diesem Hintergrund dürfte eine Kontaktaufnahme mit dem Kunden zwecks Fortführung des Buchungsprozesses von § 28 Abs. 1 Satz 1 BDSG, alternativ aber auch von § 28 Abs. 1 Satz 1 Nr. 2 BDSG gedeckt sein.

Zwar kann man bei der heute gegebenen DSL-Abdeckung im Allgemeinen davon ausgehen, dass die ursprünglich als (alleiniger) Auslöser für den Versand von Erinnerungsmails angegebenen technisch bedingten Verbindungsabbrüche inzwischen eher die Ausnahme bilden - tatsächlich sind sie aber auch nicht auszuschließen. Ich habe daher - auch unter Berücksichtigung, dass darüber hinaus wie bereits dargestellt noch andere Gründe für nicht abgeschlossene Buchungen denkbar sind - das seitens des Betreibers insoweit bestehende Interesse am rechtskräftigen Abschluss des Buchungsvorgangs dennoch als berechtigt und eine (einmalige) Erinnerungsmail als zulässig angesehen.

Mit der Vorgabe, sich bei den Abbrechermailings auf eine einzige Erinnerungsmail mit einer zeitlichen Vorgabe zur Vollendung der Buchung und einem Hinweis auf die alternative Löschung der bereits gespeicherten Daten zu beschränken, sollte eigentlich ein durchaus angemessener Interessenausgleich erreicht worden sein.

Der Portalbetreiber beharrte nichtsdestoweniger auf der bis zu zweimaligen Wiederholung des Abbrechermailings. Er machte geltend, dass nicht nachweisbar sei, auf welches der drei Abbrechermailings der Kunde (bei den 6 % schließlich doch noch erfolgreichen Buchungsabschlüssen) schließlich reagiert habe. Ich bin dieser Position allerdings vehement entgegengetreten. Für mich war nicht nachvollziehbar, weshalb eine einzige Erinnerung, dass die abgebrochene Buchung auf einfache Art und Weise unter Beibehaltung der bereits erfassten Daten fortgesetzt werden könne, nicht ausreichen sollte. Der Sachverhalt ist damit dem Empfänger ausreichend bekannt gemacht, so dass er genügend Informationen hat, um zu entscheiden, ob er auf dieses Angebot eingeht oder nicht. Mehrfach wiederholte Erinnerungen bringen für ihn keinen neuen Erkenntniswert und sind damit nicht erforderlich. Zudem setzen in kurzer zeitlicher Abfolge versandte, inhaltsgleiche Aufforderungen den Empfänger grundlos unter Druck und verletzen damit dessen schutzwürdige Interessen. Dies alles führt zur Unzulässigkeit der damit verbundenen Datennutzung (§ 28 Abs. 1 Satz 1 Nrn. 1, 2 BDSG).

Daraufhin ist mir der Vorschlag eines Belästigungs-Buttons unterbreitet worden. Abbrecher-Kunden soll auf diese Weise die Möglichkeit eingeräumt werden, weitere, mithin also die beiden folgenden Erinnerungsmails zu unterbinden. Ich habe aber auch diesen Vorschlag zurückgewiesen. Erfahrungsgemäß dürften die wenigsten Nutzer mit weiteren Erinnerungsmails rechnen und somit auch gar nicht erst in Erwägung ziehen, diese mit der Betätigung eines Belästigungsbuttons zu unterbinden. Schon die Notwendigkeit, sich gegen weitere Erinnerungsmails aktiv wehren zu müssen, stellt eine Belästigung dar und führt somit zur Untauglichkeit dieser Lösung.

8.2.5 Einsehbarkeit von Flugbuchungen im Internet

Infolge der Recherche eines Computermagazins wurde ich darauf aufmerksam, dass ein meiner Aufsicht unterfallendes Internetportal Flugreisen einer Billigfluglinie in der Weise vermittelte, dass alle Buchungen bei der Airline nur über einen einzigen gemeinsamen Nutzeraccount abgewickelt wurden. Infolge dieses von der Geschäftsführung verfolgten Buchungsprinzips konnten alle Kunden des Internetportals auf der Seite der Airline nicht nur ihre eigenen Reisedaten, sondern auch die namentlich hinterlegten Flugdaten aller anderen Kunden einsehen und in böswilliger Absicht auch ändern. Bis zur Schließung der Sicherheitslücke waren zeitweise über 4700 personenbezogene

Buchungen (Passagiernamen, Flugnummer, Flugstrecke, Reisetag und Flugzeiten) jeweils wechselseitig einseh- und manipulierbar.

Das betroffene Internetportal hat die Sicherheitslücke nach dem öffentlichen Bekanntwerden der Vorwürfe und unter dem Eindruck einer von mir getroffenen Anordnung sodann zwar zügig geschlossen, gleichwohl kam es, wie die Rechercheergebnisse des Computermagazins nahe legen, zu einer unbefugten Übermittlung personenbezogener Daten unbekannten Ausmaßes. Ich habe deswegen gegen das betroffene Buchungsportal einen Bußgeldbescheid erlassen, der jedoch infolge Einspruchs bisher noch nicht rechtskräftig ist.

8.2.6 Gesamtansicht eines Doppelhauses im Internet beim Verkauf von nur einer Gebäudehälfte

Die Bewohnerin einer Doppelhaushälfte fragte mich, ob es dem Eigentümer der anderen Doppelhaushälfte gestattet sei, wegen des geplanten Verkaufs seines Gebäudeteils das gesamte Haus in einer Internetannonce abbilden zu dürfen.

Mit der Veröffentlichung der Straßenansicht eines Doppelhauses in Verbindung mit seiner Adresse oder einem sonstigen (näheren) Ortsbezug werden personenbezogene Daten der Bewohner in Gestalt ihrer Wohnverhältnisse übermittelt, die in dieser Form und in diesem Kontext so auch nicht allgemein öffentlich zugänglich sind. Ohne Einwilligung der Betroffenen gestattet § 28 Abs. 1 Satz 1 Nr. 2 BDSG daher die Verarbeitung nur, soweit sie zur Verfolgung legitimer eigener Geschäftszwecke erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der Betroffenen an dem Ausschluss der Verarbeitung überwiegen.

Legitimer Geschäftszweck ist hier Veräußerungsabsicht. Da Doppelhäuser als ein Gebäude eine bauliche Einheit bilden, ist es auch erforderlich, diesen objektbezogenen Zusammenhang darzustellen, um die Attraktivität (bzw. den Wert) einer Immobilie Kaufinteressenten vermitteln zu können. Vergleichbare Konstellationen bestehen auch bei Wohnungseigentümergemeinschaften in Mehrparteienobjekten, wenn dort lediglich eine Wohneinheit (z. B. Etage) zum Verkauf steht.

Schutzwürdige Interessen der übrigen (Mit-)Bewohner (andere Eigentümer/Mieter), ihre Wohn- und damit Lebensumstände insoweit nicht preisgeben zu müssen, sind zwar betroffen, überwiegen aber nicht, denn diese haben sich auf das gemeinschaftliche Wohnumfeld eingelassen. Abbildungen eines von mehreren Personen bewohnten Objektes haben daher einen zurechenbaren datenschutzrechtlichen Doppelbezug, der nicht einseitig auflösbar ist. Zudem ist eine gewichtige Persönlichkeitsrechtsverletzung fern-

liegend, wenn lediglich die Verbreitung einer von einer allgemein zugänglichen Stelle jederzeit möglichen Außenansicht des Gebäudes oder Grundstücks in Rede steht.

Für eine andere rechtliche Bewertung sehe ich nur dann Anlass, wenn die Veröffentlichung einer Gebäudeansicht durch eine Stelle erfolgt, die zur Veräußerung weder befugt, noch mit dieser (vermittelnd) betraut ist. Auch muss sich im Kontext der Aufnahme ergeben, welche Wohneinheit von den (Verkaufs-)Angaben betroffen ist, damit keine falschen Personenbezüge entstehen. In dieser Weise habe ich der Petentin geantwortet.

8.2.7 Babygalerien

Es ist heutzutage üblich, dass Geburtskliniken mit Fotografen kooperieren und über ihre Internetseite eine Babygalerie betreiben, in der Neugeborene mit Foto und weiteren Angaben der Öffentlichkeit präsentiert werden. Die Fotografen bieten dabei in eigenem Interesse zunächst die kostenpflichtige Erstellung von Fotomappen unterschiedlicher Größe mit Aufnahmen direkt aus der Klinik an oder auch einen späteren exklusiven Foto-Shooting-Termin, mitunter sogar Jahresverträge mit mehreren Shootings. Darüber hinaus wird in diesem Zusammenhang regelmäßig angeboten, kostenlos ein Foto in krankenhausinternen Publikationen, auf der Website des Krankenhauses (Babygalerie) oder auch in regionalen Tageszeitungen zu veröffentlichen.

Ein junger Vater hatte sich bei mir darüber beschwert, dass ein solcher Fotograf nach der Geburt seines Kindes ein Foto von ihm angefertigt und ohne Einwilligung der Kindesmutter, letztendlich sogar entgegen deren mündlich ausdrücklich geäußerten Willen, in der im Internet auf der Website des Krankenhauses geführten, nichtsdestoweniger aber (lt. Impressum) vom Fotografen verantworteten Babygalerie veröffentlicht hatte.

Datenschutzrechtlich stellt die Veröffentlichung von Fotos von Personen im Internet eine Übermittlung personenbezogener Daten dar. Sie ist nach § 4 Abs. 1 BDSG nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder die abgebildeten Personen (bei Minderjährigen: deren Eltern) nach § 4a Abs. 1 BDSG eingewilligt haben. Auch nach § 22 Satz 1 KunstUrhG dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Eine solche Einwilligung, für die nach § 4a BDSG die Schriftform vorgeschrieben ist, hat mir der Fotograf in diesem Fall nicht vorlegen können. Die Veröffentlichung war somit unzulässig gewesen. Der Fotograf hatte das betreffende Foto bereits auf die erste, vom Kindsvater direkt an ihn gerichtete Beschwerde hin aus der Babygalerie entfernt und mir gegenüber die versehentliche Veröffentlichung mit Anlaufschwierigkeiten entschuldigt. Er habe die Zusammenarbeit

mit der Klinik gerade begonnen, es sei der erste (Groß-)Auftrag in dieser Dimension für ihn gewesen.

Die vom Fotografen genutzten Auftragsvordrucke waren als solche nicht zu beanstanden, denn sie enthielten eine separat zu unterzeichnende Einwilligungserklärung mit einzelnen Ankreuzfeldern für die Veröffentlichung auf der Website des Krankenhauses, in krankenhausinternen Publikationen und auch in regionalen Tageszeitungen.

Ich habe die Beschwerde dennoch zum Anlass einer stichprobenhaften Kontrolle der betreffenden Babygalerie genommen und dabei überprüft, ob dem Fotografen von den Eltern der dort abgebildeten Babys eine wirksame Einwilligung in die diesbezügliche Veröffentlichung erteilt worden war. In fast allen von mir überprüften Fällen konnte der Fotograf mir eine solche Einwilligung vorlegen, allerdings gab es auch einige wenige Fälle, in denen die Eltern die Erklärung zwar unterzeichnet, jedoch keines der Felder angekreuzt oder aber anders herum das Feld für die Babygalerie zwar angekreuzt, die Erklärung aber nicht unterzeichnet hatten.

Prinzipiell waren diese Einwilligungserklärungen daher unwirksam. Da ich jedoch nicht beurteilen konnte, ob die betreffenden Erklärungen lediglich aus Versehen nicht unterzeichnet oder gekreuzt worden waren oder ob die Eltern mit der Veröffentlichung tatsächlich nicht einverstanden gewesen waren, habe ich davon abgesehen, vom Fotografen die Entfernung der Fotos aus der Babygalerie zu verlangen. Stattdessen habe ich die betroffenen Eltern noch einmal schriftlich auf diese Veröffentlichung hingewiesen und weitere Aktivitäten in deren Ermessen gestellt.

8.2.8 Veröffentlichung von Bankverbindungsdaten als Reaktion auf Kundenkritik

Ein Online-Versandhändler war mit einer ganzen Reihe negativer Bewertungen und Kommentaren in einem externen Verbraucherschutzforum konfrontiert. Immer wieder beklagten Kunden, von diesem Shop nach Vorauskasse keine Lieferung und nach entsprechender Reklamation schließlich auch keine Rückzahlung erhalten zu haben. Der Händler war bemüht, die Vorwürfe soweit es ging zu entkräften und den Banken die Schuld für die fehlgeschlagenen Rücküberweisungen zuzuweisen. An die betroffenen Kunden versandte er dazu sogar Kopien der (vermeintlichen) Einzahlungsbelege. Als ihm im Forum diesbezüglich auch noch der Fälschungsvorwurf unterstellt worden war, wusste er sich nicht mehr anders zu helfen, als die Rückforderungsmail eines Betroffenen einschließlich der darin angegebenen Bankverbindungsdaten und eine Kopie seines Einzahlungsbeleges (mit den gleichen Bankverbindungsdaten) im Internet zu veröffentlichen und in einem seiner Forumsbeiträge zu verlinken.

Dagegen wandte sich der betroffene Kunde mit seiner Eingabe an die Aufsichtsbehörde und das zu Recht.

Für die rechtliche Bewertung einschlägig ist § 28 Abs. 1 Satz 1 Nr. 1 BDSG. Nach dieser Vorschrift wäre das Übermitteln personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke dann zulässig, wenn es für die Durchführung eines rechtsgeschäftlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Diese Voraussetzung war vorliegend nicht erfüllt. Für die Rückerstattung des Vorkassenbetrags war eine Bekanntgabe der Bankverbindungsdaten des Kunden gerade nicht erforderlich.

Auch sonst waren keine Gründe ersichtlich, die zu einer Zulässigkeit einer solchen Bekanntgabe hätten führen können, insbesondere ergab sich die Zulässigkeit auch nicht aus einer Interessenabwägung gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Denn die Veröffentlichung von Bankverbindungsdaten im Internet birgt für den Betroffenen vielfältige Risiken und eröffnet eine Reihe von Missbrauchsmöglichkeiten durch Dritte. Das sich daraus ergebende schutzwürdige Interesse überwiegt das hier ggf. zu unterstellende Interesse, sich auf diese Weise gegen Anschuldigungen in einem Verbraucherschutzforum zu wehren, bei Weitem, zumal das Einstellen eines Einlieferungsbelegs auch gar nicht geeignet, mithin auch nicht erforderlich im Sinne des § 28 Abs. 1 Satz 1 Nr. 2 BDSG, ist, die behauptete Einzahlung des Erstattungsbetrags zu beweisen, denn Dritte können weder die Echtheit der teilanonymisierten Rückforderungs-E-Mail noch die des Einzahlungsbelegs in irgendeiner Weise nachprüfen. Einen solchen Einzahlungsbeleg auf einer Internetseite zu fälschen stellt überhaupt kein Problem dar.

8.2.9 Anbieterübergreifende Steuerung von Werbeeinblendungen

Gleich mehrfach erreichten mich Eingaben besorgter Petenten, weil diese sich im Internet auf den Seiten eines bestimmten Anbieters Angebote und Produkte angesehen hatten und später auf den Seiten anderer Anbieter zu gleichen bzw. ähnlichen Dingen Werbung eingeblendet bekamen.

Hier habe ich insoweit zur Aufklärung beitragen können, als ich den Betroffenen dieses Phänomen erklären konnte. Ursächlich sind nämlich sogenannte „Cookies“, also Textdateien, die - oft unbemerkt - auf dem Computer in speziellen Ordnern angelegt werden, um Informationen zum Seitenbesuch zu speichern. Ihr Vorteil ist, dass sich die Ladezeiten der Internetseite bei einem erneuten Aufruf durch die bereits auf dem Rechner befindlichen Daten erheblich verkürzen und Inhalte schon den Präferenzen des Nutzers entsprechend angepasst werden können.

Diese Dateien stellen allerdings keine unmittelbaren Personenbezüge zum Computernutzer her, sind aber im Kontext anderer Informationen nicht frei vom Risiko mittelbarer Bezüge. Daher empfiehlt sich das Setzen von Cookies zu unterbinden bzw. diese regelmäßig zu löschen. Gängige Browser bieten hierfür entsprechende Einstellungsmöglichkeiten. Meine Aufsicht wird sich zudem künftig verstärkt mit den telemedienrechtlichen und weiteren Vorgaben für Cookies auseinandersetzen.

8.2.10 Keine Einwilligung in die Datennutzung für Werbezwecke in den AGB

Immer wieder wenden sich Internetnutzer an mich, weil sie nach Anmeldung an einem Webportal oder einem Kauf in einem Webshop telefonisch, per SMS, E-Mail oder per Briefpost im Rahmen von Marketingmaßnahmen kontaktiert worden sind. Ein Online-Reisevermittler berief sich dabei dem Kunden gegenüber auf seine AGB, die folgende Regelung enthielten:

„Die von Ihnen angegebenen Daten stehen der XY GmbH für Post, E-Mail, SMS und Telefonmarketing zur Verfügung. Hierfür erteilen Sie Ihr ausdrückliches Einverständnis. Dieses kann jederzeit widerrufen werden.“

Ich habe die verantwortliche Stelle darauf hingewiesen, dass sie - unbeschadet etwaiger anderer Zulässigkeitstatbestände (§§ 28 Abs. 3 BDSG, 7 Abs. 3 UWG - vgl. dazu auch 5. TB, Pkt. 4.3.2.3) - aus dieser Formulierung keine wirksame Einwilligung ihrer Kunden in die werbliche Nutzung ihrer personenbezogenen Daten ableiten kann.

Die Einwilligung in eine Werbung unter Verwendung von elektronischer Post (E-Mail und SMS) nach § 7 Abs. 2 Nr. 3 UWG erfordert eine gesonderte, nur auf die Einwilligung in eine solche Werbung bezogene Zustimmungserklärung des Betroffenen. Eine Einwilligung, die in Textpassagen enthalten ist, die auch andere Erklärungen oder Hinweise enthalten, wird diesen Anforderungen nicht gerecht (BGH, Urteil vom 16. Juli 2008 - VIII ZR 348/06). Für die Einwilligung in eine Werbung mit einem Telefonanruf gegenüber Verbrauchern nach § 7 Abs. 2 Nr. 2 Fall 1 UWG ist - ebenso - eine gesonderte, nur auf die Einwilligung in die Werbung mit einem Telefonanruf bezogene, Zustimmungserklärung des Betroffenen erforderlich (BGH, Beschluss vom 14. April 2011 - I ZR 38/10). Auch das OLG Köln (Urteil vom 29. April 2009 - 6 U 218/08) hat damit übereinstimmend festgestellt, dass der Schutz der Privatsphäre wegen der mit Werbeanrufen verbundenen massiven Beeinträchtigungen eine Einwilligung in die Telefonwerbung durch Allgemeine Geschäftsbedingungen ausschließt.

Soweit sich angesichts dessen die Datennutzung für Marketingzwecke nicht aus anderen Zulässigkeitstatbeständen - so bei Briefwerbung u. U. aus § 28 Abs. 3 BDSG und bei E-Mail-Werbung u. U. aus § 28 Abs. 3 BDSG unter Berücksichtigung von § 7 Abs. 3

UWG - ergibt, ist die werbliche Nutzung der erhobenen Daten also unzulässig. Für eine telefonische Kundenansprache für Marketingzwecke besteht unter diesen Umständen keinerlei Spielraum.

8.3 Arbeitnehmerdatenschutz

8.3.1 Urlaubsanträge nur mit Begründung?

Ein Arbeitnehmer wollte von mir wissen, inwieweit sein Arbeitgeber im Urlaubsantrag nach den Gründen sowie der Gestaltung des beabsichtigten Urlaubs fragen dürfe. Ihm habe ich mitgeteilt, dass § 32 Abs. 1 Satz 1 BDSG dem Arbeitgeber eine solche Erhebung nur insoweit gestattet, wie die Angaben für die Durchführung des Arbeitsverhältnisses objektiv erforderlich sind.

Nach § 7 Abs. 1 BUrlG hat ein Arbeitgeber bei der von ihm zu treffenden zeitlichen Festlegung des Urlaubs die Urlaubswünsche seines Beschäftigten zu berücksichtigen, also im Regelfall den erbetenen Urlaub ohne weitere Nachfrage zu gewähren. Allerdings gilt dies nicht, wenn dringende betriebliche Belange, etwa ein hoher Auftragsbestand, dem entgegenstehen oder die Urlaubswünsche anderer Beschäftigter unter sozialen Gesichtspunkten als vorrangig betrachtet werden müssen.

Nach § 7 Abs. 2 BUrlG hat der Arbeitgeber auch darauf hinzuwirken, dass der Arbeitnehmer seinen Urlaub in der Weise zeitlich zusammenhängend nimmt, dass der mit dem Urlaub verfolgte Erholungszweck gewährleistet ist, da jedenfalls bei häufigen Kurzzeiturlauben keine nachhaltige Regenerierung der Arbeitskraft erwartet werden kann. So sieht das Gesetz insbesondere vor, dass einer der Urlaubsteile mindestens zwölf aufeinanderfolgende Werktage umfassen muss (§ 7 Abs. 2 Satz 2 BUrlG). Mithin kann eine anderweitige Erwerbstätigkeit während des Urlaubs den Erholungszweck infrage stellen (§ 8 BUrlG). Insofern besteht - gerade bei einem kürzeren Urlaubswunsch des Arbeitnehmers - durchaus ein objektives Erfordernis, die Gründe des Urlaubs und die beabsichtigte Gestaltung hinterfragen zu dürfen.

Dies bedeutet aber nicht, dass der Arbeitgeber befugt wäre, in jedem Fall (pauschal mittels eines Formulars) die Urlaubsabsichten aller Beschäftigten stets näher hinterfragen zu dürfen. Denn das Recht des Arbeitnehmers, seine Freizeit grundsätzlich frei gestalten zu dürfen sowie sein Recht auf Privatsphäre bzw. auf informationelle Selbstbestimmung gebieten, die Erhebungsbefugnis auf die o. g. erforderlichen Fallgruppen zu beschränken:

1. Der Arbeitgeber sieht angesichts der gewünschten Urlaubszeiten betriebliche Hinderungsgründe, die es mit dem Urlaubsinteresse des Arbeitnehmers abzuwägen gilt.
2. Der Arbeitgeber muss wegen gleichzeitiger und deswegen unvereinbarer Abwesenheitswünsche mehrerer Beschäftigter deren Urlaubsinteresse gegeneinander abwägen.
3. Der Arbeitnehmer hat im Kalenderjahr noch keinen zusammenhängenden Urlaub von mindestens zwölf Werktagen genommen oder zumindest beantragt, so dass der Arbeitgeber Gefahr läuft bei Gewähr eines weiteren Kurzurlaubes gegen das Stücklungsverbot zu verstoßen.
4. Die Kürze des Urlaubs oder andere Gründe geben im Einzelfall Anlass zu der Besorgnis, der Urlaubszweck könne nicht erreicht werden.

8.3.2 Gleitzeiterfassung mittels Fingerabdrücken

Zur automatisierten Erfassung der Arbeitszeiten setzen Unternehmen leider zunehmend auch fingerabdruckbasierte Zeiterfassungssysteme ein.

Ich habe erhebliche Bedenken, dass der Einsatz eines solchen Systems - von Ausnahmen in besonders sicherheitsrelevanten Bereichen abgesehen - rechtmäßig ist, insbesondere habe ich Zweifel, dass der Einsatz solcher Verfahren den datenschutzrechtlichen Grundsätzen der Erforderlichkeit und der Verhältnismäßigkeit entspricht.

Biometrische Merkmale sind zweifellos personenbezogene Daten mit besonderer Sensibilität. Die Speicherung derartiger Merkmale beim Arbeitgeber bedingt besondere Risiken für das Persönlichkeitsrecht der Arbeitnehmer, da sie - im Gegensatz zu anderen Identifikationsmitteln wie beispielsweise Transpondern - dauerhaft bzw. lebenslang und je nach System auch relativ eindeutig - keinesfalls jedoch fälschungssicher - mit dem Betroffenen verbunden sind und ihn nicht nur bei dem jeweiligen technischen System (hier: Zeiterfassung) identifizieren können, sondern - gerade was Fingerabdrücke betrifft - auch noch in unzähligen anderen Lebenssituationen. Biometrische Merkmale kann man nicht einfach löschen oder austauschen. Das Risiko einer zweckwidrigen Nutzung ist daher hier besonders groß, zumal diese Identifikationsmöglichkeit auch nach Beendigung des Arbeitsverhältnisses beim Arbeitgeber verbleibt (jedenfalls besteht diese Gefahr), während die üblichen Identifikationsmittel bei Beendigung der Tätigkeit dem Arbeitgeber zurückgegeben werden müssen und deren weitere Verwendung dann nicht mehr zu Lasten des ausgeschiedenen Arbeitnehmers gehen kann. Die Verknüpfung biometrischer Daten mit dem Betroffenen besteht aber unabhängig vom jeweiligen IT-System und damit insbesondere auch über den eigentlichen Einsatzzweck hinaus und kann technisch auch in anderen IT-Systemen bzw. in anderen Einsatzumgebungen und

vor allem auch zeitlich unbegrenzt verwendet werden. Fingerabdrücke hinterlassen Betroffene - auch im Arbeitsumfeld - ständig und überall, damit besteht hier die besondere Gefahr, dass Betroffenen auf der Grundlage der in das System eingespeisten Vergleichsmuster auch andere Handlungen in oder außerhalb des betrieblichen Umfelds zugerechnet werden können oder sollen. Der Chaos Computer Club hat zudem bereits demonstriert, dass es mit Bordmitteln ohne Probleme möglich ist, in etwa zehn Minuten mit Hilfe eines fremden Fingerabdruckes ein Muster zu erzeugen, welches die gängigen Lesegeräte ohne weiteres täuschen kann. Ebenso ist es natürlich im Hinblick auf die o. g. Risiken auch möglich, falsche Spuren zu legen und den Betroffenen so ggf. in die Situation zu bringen, sich für nicht begangene Handlungen rechtfertigen zu müssen.

Angesichts der besonderen Sensibilität solcher körperbezogenen Daten wie Fingerabdrücke ist eine Nutzung für Zwecke der Zutrittskontrolle aus Verhältnismäßigkeitsgründen auf besondere Ausnahmefälle zu beschränken. Dazu gehören in erster Linie Anwendungsfälle mit besonderen Sicherheitsanforderungen (Zutrittskontrolle in Sicherheitsbereichen, vgl. dazu auch Seifert in Simitis, BDSG, 7. Aufl., Rdnr. 97 zu § 32), auch sollten dann vorzugsweise besonders datenschutzfreundliche Verfahren zum Einsatz kommen, bei denen etwa beim Arbeitgeber selbst keine Daten gespeichert werden, weil die Fingerabdrücke stattdessen ausschließlich auf einem im Besitz des Betroffenen befindlichen und unter seiner Kontrolle stehenden Chip gespeichert sind und die Authentifizierung durch Vergleich des tatsächlichen biometrischen Musters mit dem gespeicherten Muster direkt auf der Karte (Comparison on Card) erfolgt.

Fragt man bei verantwortlichen Stellen nach den Gründen für den Einsatz fingerabdruckbasierter Zeiterfassungssysteme, so sind die Antworten teilweise doch sehr banal. Mitunter geht es einzig und allein darum zu vermeiden, dass die Mitarbeiter eine weitere Karte im Scheckkartenformat bzw. ein anderes Identifikationsmittel mit sich führen müssen. Daneben spielen aber natürlich auch Missbrauchserwägungen (Stichwort: Übergabe des Identifikationsmittels an Dritte oder Arbeitszeitmanipulation) eine Rolle. Dies ist für sich betrachtet sicherlich richtig, kann aber die Nachteile bzw. Risiken eines solchen Systems natürlich nicht überwiegen. Zudem kann regelmäßig nicht davon ausgegangen werden, dass Arbeitnehmer sich generell rechtswidrig verhalten.

Für bloße Zwecke der Zeiterfassung sind biometrische Verfahren auch mangels Erforderlichkeit nicht einsetzbar, denn dafür stehen bekanntlich wesentlich weniger in das Persönlichkeitsrecht der Arbeitnehmer eingreifende Verfahren zur Verfügung. Eine Erforderlichkeit besteht immer dann nicht, wenn von mehreren gleichermaßen wirksamen Maßnahmen die den Arbeitnehmer stärker belastende gewählt wird (vgl. Gola/ Schomerus, BDSG, 11. Aufl., Rdnr. 12 zu § 32, gleiche Auffassung: Seifert in Simitis, BDSG, 7. Aufl., Rdnr. 97 zu § 32). Das Ziel „Erfassung der Arbeitszeit“ kann keinen so

weitreichenden Eingriff rechtfertigen (Däubler in Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl., Rdnr. 86 zu § 32).

8.3.3 Führerscheinkontrolle durch externen Dienstleister des Arbeitgebers

Der Arbeitgeber eines Betroffenen beabsichtigte wegen der Überlassung von Firmenfahrzeugen an seinen beruflich kraftfahrenden Beschäftigten dessen Führerscheininhaberschaft mittels eines externen Dienstleisters turnusmäßig zu prüfen. Hintergrund ist die Pflicht des Halters aus § 21 Abs. 1 Nr. 2 StVG sowie die versicherungsrechtliche Obliegenheit, sich bei einer Fahrzeugüberlassung der gültigen Fahrerlaubnis eines Fahrers vergewissern zu müssen.

Das Geschäftsmodell des Dienstleisters, das in Anspruch genommen werden sollte, sah vor, dass der Arbeitgeber auf dem Führerschein seines Beschäftigten einen fälschungssicheren und nicht beschädigungsfrei ablösbaren Barcode mit einer einmal vergebenen Ordnungsnummer klebt. Zu diesem legt er in der Datenbank des Dienstleisters einen Datensatz an. Dieser enthält je nach Entscheidung des Arbeitgebers entweder den Namen des Kraftfahrers (personalisierte Variante) oder ein Pseudonym in Gestalt einer Beschäftigtenkennzahl. Wenn nach dem vom Arbeitgeber bestimmten Prüfungsintervall eine Kontrolle der Fahrerlaubnis vorgenommen werden soll, erhält der Beschäftigte unter einer gleichfalls im System hinterlegten Mobilfunkrufnummer und/oder E-Mail, im Eingabefall die private Rufnummer und E-Mail-Adresse des Beschäftigten, die Aufforderung, seinen Führerschein zur Sichtung bei einem Kooperationspartner des Anbieters, einem bundesweit tätigen Tankstellenunternehmen, vorzulegen, dessen Verkaufspersonal nach Einsichtnahme des Führerscheins den aufgeklebten Barcode scannt und so dem Dienstleister elektronisch meldet, dass ein gültiges Dokument vorgelegt wurde. Zeitpunkt und Ort der Prüfung werden zu dem Datensatz gespeichert und bleiben als Prüfhistorie wahlweise für die Dauer von fünf bis zu zehn Jahren gespeichert. Falls der Führerschein auch nach einer Mahnung nicht vorgelegt wurde, erhält der Arbeitgeber von dem Dienstleister eine entsprechende Nachricht.

Auf die Frage des Beschäftigten, ob das Ansinnen seines Arbeitgebers zulässig sei, habe ich ihm Folgendes mitgeteilt:

Die Erhebung und Verarbeitung privater Telefonnummern oder E-Mail-Adressen eines Beschäftigten durch seinen Arbeitgeber ist außer für Zwecke der Rufbereitschaft bzw. dringenden Erreichbarkeit mangels Erfordernisses für die Erbringung der Arbeitsleistung nicht zulässig, zumal der Beschäftigte ein schutzwürdiges Interesse daran hat, dass private Kommunikationsmittel als seiner Privatsphäre zugehörig respektiert werden (§ 32 Abs. 1 Satz 1 bzw. § 28 Abs. 1 Satz 1 Nr. 2 BDSG). Wegen des im Arbeitsver-

hältnis typischen Über- und Unterordnungsverhältnisses ist eine darüber hinausgehende Einwilligung des Beschäftigten mangels Freiwilligkeit ausgeschlossen (§ 4a Satz 1 BDSG).

Falls allerdings stattdessen allein betriebliche Rufnummern oder andere betriebsbezogene Daten zur Person des Beschäftigten verarbeitet werden, bestehen jedoch keine Bedenken, wenn diese und weitere notwendige Daten unter Einhaltung der Maßgaben von § 11 BDSG für die vom Arbeitgeber verfolgten Zwecke der zur Erbringung der Arbeitsleistung notwendigen Führerscheinprüfung durch den externen Dienstleister verarbeitet werden und in das Auftragsdatenverarbeitungsverhältnis auch der Kooperationspartner, der die Sichtprüfung vornimmt, wirksam einbezogen ist (§ 32 Abs. 1 Satz 1 BDSG).

Da jedoch ohne besonderen Anlass wenige Turnusprüfungen ausreichend sind (vgl. in strafrechtlicher Hinsicht: KG Berlin, Beschluss vom 19. Juni 2005, Az. 1 Ss 340/05 - juris), folgt jedoch aus dem datenschutzrechtlichen Erforderlichkeitsgrundsatz eine Begrenzung auf ein Prüfungsverlangen je Quartal. Ferner bedarf es lediglich der Speicherung der letzten Sichtprüfung, wenn kein Vorfall (Unfall o. Ä.) die Dokumentation vorhergehender Prüfungen gebietet, zumal die hier in Anspruch genommene Dienstleistung schon für sich genommen dem Arbeitgeber den Nachweis der Erfüllung seiner Obliegenheiten verschaffen soll.

8.3.4 Einsichtsrechte des Betriebsrats in Zeiterfassungsdaten

Ein Unternehmen wandte sich an meine Behörde mit der Frage, ob es datenschutzrechtlich gehindert sei, seinem Betriebsrat eine personenbezogene Auflistung der aktuellen Zeiterfassungsdaten aller Arbeitnehmer zu geben, insbesondere weil einzelne Beschäftigte zum Ausdruck gebracht hätten, dass sie dies nicht wünschten.

Dem Unternehmen habe ich mitgeteilt, dass eine Weitergabe solcher Daten an seinen Betriebsrat datenschutzrechtlich keine Übermittlung an einen Dritten ist, sondern eine Verarbeitung für eigene Zwecke der verantwortlichen Stelle, da der Betriebsrat deren Bestandteil ist (vgl. BAG, Beschluss vom 7. Februar 2012, RDV 2012, S. 192 bis 197). Diese Verarbeitung ist nach § 32 Abs. 1 Satz 1 BDSG auch ohne bzw. gegen die Einwilligung der Betroffenen zulässig, soweit dies zur Durchführung des Beschäftigungsverhältnisses erforderlich ist. Zwecke der Durchführung des Beschäftigungsverhältnisses erfassen auch solche Verarbeitungen, die wegen der Unterrichtungspflicht des Arbeitgebers aus § 80 Abs. 2 Satz 1 BetrVG erforderlich sind, weil der Betriebsrat die Angaben wegen seiner Rechte aus § 80 Abs. 1 Nr. 1 BetrVG beanspruchen kann.

Hierzu stellt das BAG (a. a. O.) fest: „*Die Überwachungsaufgabe des Betriebsrats nach § 80 Abs. 1 Nr. 1 BetrVG ist nicht von einer vorherigen Einwilligung der von der Vorschrift begünstigten Arbeitnehmer abhängig. Der Gesetzeswortlaut enthält eine entsprechende Einschränkung nicht. Das Beteiligungsrecht aus § 80 Abs. 1 Nr. 1 BetrVG dient der Sicherstellung eines ordnungsgemäßen Normvollzugs durch den Arbeitgeber. Seine Wahrnehmung steht nach der Konzeption des BetrVG nicht zur Disposition der Arbeitnehmer.*“

8.3.5 Übermittlung von Daten eines ehemaligen Arbeitsplatzbewerbers an dessen aktuellen Arbeitgeber

Ein Unternehmen des Wach- und Sicherungsgewerbes wollte einen insoweit bewährten Praktikanten fest einstellen.

Der Stellenbewerber wurde daher zum Zwecke der Zuverlässigkeitsprüfung der zuständigen Gewerbebehörde nach Maßgabe des § 9 BewachV gemeldet. Ohne eine solche Überprüfung darf eine Tätigkeit in einem Wachunternehmen nicht ausgeübt werden.

Als das Ergebnis der Überprüfung schließlich beim Wachunternehmen eintraf, war das Praktikum längst vorbei und der ehemalige Praktikant hatte inzwischen - ohne seine Bewerbung zurückgezogen zu haben - eine Stelle in der örtlichen Stadtverwaltung, Sachgebiet Ordnung und Sicherheit, gefunden. Gewisse Parallelen zu seiner früheren Praktikantentätigkeit waren dabei offensichtlich.

Leider war das Ergebnis der Überprüfung aber negativ. Laut Mitteilung der Gewerbebehörde waren die im Bundeszentralregister zu dem ehemaligen Praktikanten enthaltenen Eintragungen so umfangreich und auch so schwerwiegend, dass eine Einstellung in das Wachunternehmen nicht möglich gewesen wäre. Für den Geschäftsführer des Unternehmens war diesbezüglich nicht nachvollziehbar, weshalb ein Bewerber, den er wegen bestehender Eintragungen im Bundeszentralregister nicht hätte einstellen dürfen, gleichwohl von der öffentlichen Verwaltung eine Stelle in der Stadtbestreifung, also für Tätigkeiten, die typischerweise auch ein Wachunternehmen durchführen kann, erhalten hatte. Seinen Ärger darüber machte er in einem Schreiben an den Bürgermeister Luft, in dem er auf den konkreten Sachverhalt, insbesondere auf die durch das Gewerbeamt festgestellte Unzuverlässigkeit des Mitarbeiters, hinwies und den Bürgermeister zur Stellungnahme aufforderte.

Die Verärgerung des Geschäftsführers konnte ich durchaus verstehen. Gute Fachkräfte werden bekanntlich immer rarer und offensichtlich hatte sich der Praktikant während seines Praktikums im Unternehmen sehr gut bewährt. Dass er jetzt in der öffentlichen

Verwaltung vergleichbaren Tätigkeiten nachgehen durfte, dort also geringere Anforderungen an die Zuverlässigkeit gestellt worden waren, war für ihn wenig nachvollziehbar. Dies kann jedoch eine Übermittlung des Ergebnisses der Zuverlässigkeitsüberprüfung an den aktuellen Arbeitgeber eines (ehemaligen) Bewerbers nicht rechtfertigen. § 32 Abs. 1 Satz 1 BDSG regelt insoweit unmissverständlich, dass personenbezogene Daten eines Beschäftigten, wozu nach § 3 Abs. 11 Nr. 7 BDSG auch Stellenbewerber gehören, für Zwecke des Beschäftigungsverhältnisses nur erhoben, verarbeitet oder genutzt werden dürfen, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich ist. Die Einstellung des ehemaligen Praktikanten hatte sich aber schon allein wegen dessen neuer Beschäftigungsstelle erledigt und wäre wie dargestellt auch wegen des negativen Überprüfungsergebnisses nicht in Frage gekommen, mithin war die Übermittlung für die (bereits getroffene) Entscheidung über die Begründung eines Beschäftigungsverhältnisses nicht erforderlich und damit unzulässig. Soweit man unterstellt, dass es dem Geschäftsführer weniger um den konkreten Einzelfall als vielmehr um die generelle Frage der Anforderungen an (auch) mit Sicherheitsaufgaben zu beauftragenden Stellenbewerbern im öffentlichen Dienst gegangen ist, war die Übermittlung der personenbezogenen Daten ebenso wenig erforderlich (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG), denn diese Problematik hätte auch in allgemeinerer Form, d. h. ohne Bezugnahme auf den ehemaligen Praktikanten, diskutiert werden können.

8.3.6 Übermittlung von Beschäftigtendaten an potentielle Unternehmenskäufer (Due Diligence-Prüfung)

Potentielle Käufer eines Unternehmens wollen vor einer Kaufentscheidung zumeist genaue Details zur Qualifikation, Bezahlung, Altersstruktur und zum Krankenstand der Beschäftigten als für den Unternehmenswert und die Unternehmensattraktivität maßgebliche Faktoren, da diese Informationen neben anderen Parametern die Kaufentscheidung beeinflussen können. Derartige Prüfungen erfolgen im Zuge einer typischen Due Diligence-Prüfung.

Ein Beschäftigter eines sächsischen Unternehmens, das verkauft werden sollte, fragte mich nach den rechtlichen Vorgaben einer solchen Datenweitergabe, insbesondere auch dazu, ob er zu einer Einwilligung in die Übermittlung verpflichtet werden könne. Ihm habe ich mitgeteilt, dass solange allein anonyme Daten übermittelt werden, es also für den Empfänger unmöglich ist, die Identität des Trägers eines Datums in Erfahrung zu bringen, es keiner Einwilligung des Beschäftigten bedarf, da es sich mangels Personenbezugs nicht um eine vom Anwendungsbereich des Bundesdatenschutzgesetzes erfasste Verarbeitung handelt (§ 1 Abs. 1 BDSG).

Sollen allerdings zumindest personenbeziehbare Beschäftigtendaten an den Kaufinteressenten übermittelt werden, ist das Verarbeitungshandeln zwar für die Durchführung des bestehenden Beschäftigungsverhältnisses ohne Relevanz und findet somit keine Rechtsgrundlage in § 32 Abs. 1 Satz 1 BDSG. Gleichwohl liegt wegen der Kaufabsicht ein berechtigtes Interesse des kaufenden Unternehmens an den für eine Unternehmensanalyse objektiv erforderlichen Daten vor, woraus die Befugnis des zum Verkauf stehenden Unternehmens folgt, diese Daten auch ohne Einwilligung des Beschäftigten übermitteln zu dürfen (§ 28 Abs. 2 Nr. 2a BDSG).

Im Regelfall ausreichend und damit allein erforderlich ist allerdings nur die Übermittlung i. S. v. § 3 Abs. 6a BDSG pseudonymisierter Daten (vgl. Seifert in Simitis, BDSG, 7. Auf. 2011, § 32 Rdnr. 123), also ohne die Nennung des Namens des Betreffenden, jedoch mit seiner Funktionsangabe (z. B. „Buchhalter 1“, „Prokurist“, „Sekretärin 4“, „Geschäftsführer“ usw.). Die Übermittlungsbefugnis schließt ferner ein, die Angabe des Geschlechts, des Alters (in Jahren), der Dauer der Betriebszugehörigkeit (in Jahren), der Merkmale des Beschäftigungsverhältnisses (z. B. „unbefristeter Arbeitsvertrag“, „Probezeit“, „Altersteilzeit“ usw.), der Vergütung und der Qualifikation.

Die pseudonyme Übermittlung der Krankheitszeiten einer für den Empfänger schon gegenwärtig ohne unangemessenen Aufwand gleichwohl bestimmbaren Person, also eines besonderen personenbezogenen Datums i. S. d. § 3 Abs. 9 BDSG, ist wegen § 28 Abs. 8 Satz 1 BDSG jedoch ausgeschlossen, da die engen Voraussetzungen von § 28 Abs. 6 Nr. 1 bis 4 BDSG und § 28 Abs. 7 Satz 1 BDSG nicht vorliegen.

Wegen des im Beschäftigungsverhältnis typischen Abhängigkeitsverhältnisses des Beschäftigten zu seinem Arbeitgeber besteht über die genannten Übermittlungsbefugnisse hinaus in der Regel kein Raum für (darüber hinausgehende) Einwilligungen, da diese nicht in der von § 4a Abs. 1 Satz 1 BDSG gebotenen Weise freiwillig wären. Allerdings machen sie Sinn bei Personen, deren pseudonyme Angaben aufgrund einer Alleinstellung und wegen einer herausgehobenen Funktion auch für das Käuferunternehmen leicht individualisierbar sind (z. B. beim Prokuristen des Unternehmens). Da es sich zugleich häufig um Führungspersonen handelt, darf allerdings erwartet werden, dass diese sich des Arbeitgeberverlangens leichter als andere Beschäftigte erwehren können, es sich also um einen Personenkreis handelt, der auch im Beschäftigungsverhältnis einwilligungsfähig ist. Ob diese Betroffenen arbeitsrechtlich verpflichtet werden können, einzuwilligen, ist jenseits des Datenschutzrechts allerdings eine im Kern arbeitsrechtliche Frage, zu deren Beantwortung ich nicht befugt bin.

Wegen der Übermittlung pseudonymer, aus Empfängersicht größtenteils anonymer Daten an eine Stelle, die sich nicht EU-Datenschutzgrundsätzen unterworfen hat, habe

ich - soweit sich die Übermittlung im Rahmen des Vorstehenden bewegt - keine datenschutzrechtlichen Bedenken, die das Übermittlungsinteresse des Empfängers überwögen. Angesichts jüngster Zweifel an der Datenschutzkonformität des Handelns außereuropäischer Stellen, bedarf es jedoch hier einer genauen Prüfung des Einzelfalls. Es mag für das übermittelnde Unternehmen geboten sein, mit dem Empfänger der Daten vertragliche (sanktionsbewährte) Vereinbarungen zum Schutz der Datenschutzinteressen der Beschäftigten abzuschließen.

8.4 Gesundheitswesen

8.4.1 Kein Anspruch auf Löschung von Angaben im Arztbrief

Bei einem Kurklinikaufenthalt (hier: Mutter-Kind-Kur) erstellt die Klinik einen Bericht zum Kurverlauf, den dabei durchgeführten Maßnahmen und zu deren Ergebnissen. All dies erhält der zuständige Arzt als Zusammenfassung in einem sogenannten Arztbrief. Der Patient kann diesen Arztbrief jederzeit einsehen. Fraglich ist, ob er auch eine Änderung bzw. Berichtigung oder Löschung darin enthaltener Angaben beanspruchen kann.

Zum Anwendungsbereich des Bundesdatenschutzgesetzes:

Zunächst ist zwischen ambulanten Arztpraxen und privaten Kliniken auf der einen und kommunalen und Landeskliniken auf der anderen Seite zu unterscheiden. Für ambulante Praxen und private Kliniken - auch soweit zwischen der privaten Klinik und den Krankenkassen ein Versorgungsvertrag nach § 111a SGB V für Leistungen nach § 24 SGB V besteht - findet das Bundesdatenschutzgesetz Anwendung, im öffentlich-rechtlichen Bereich (z. B. für Universitätskliniken und kommunale Krankenhäuser) das Sächsische Datenschutzgesetz. Weitere gesetzliche Regelungen zum Verhältnis zwischen Arzt und Patient finden sich im Bürgerlichen Gesetzbuch, im Strafgesetzbuch und insbesondere in der Berufsordnung der SLÄK.

Zur Änderung beziehungsweise Berichtigung von Angaben im Arztbrief:

Es besteht seitens des Patienten ein Recht auf Auskunft und Einsicht in die Krankenunterlagen, ohne dass er ein besonderes Interesse erklären oder nachweisen muss. Der Arzt ist verpflichtet, Auskunft über die zu der Person des Patienten gespeicherten Daten zu erteilen. Soweit vertragliche Beziehungen zwischen Arzt und Patient bestehen, ergibt sich das Einsichtsrecht als vertragliches Nebenrecht. Anderenfalls folgt es aus § 810 BGB. Danach kann derjenige, der ein rechtliches Interesse daran hat, eine in fremdem Besitz befindliche Urkunde einzusehen, vom Besitzer die Gestattung der Einsichtnahme verlangen, wenn die Urkunde in seinem Interesse errichtet worden ist. Das Einsichtsrecht des Patienten bezieht sich auch auf den Arztbrief.

Nach § 35 Abs. 1 BDSG sind personenbezogene Daten, die unrichtig sind, zu berichtigen. Dies kann allerdings z. B. nicht für Verdachtsdiagnosen gelten, denn diese sind im Regelfall keine inhaltlich falschen Daten, sondern objektive Angaben über die Behandlung zu einem bestimmten Zeitpunkt. Ein Anspruch auf Berichtigung oder gar Löschung der patientenbezogenen Daten kommt zudem nicht in Betracht, solange eine (sich aus dem Behandlungsvertrag oder aus dem Berufsrecht ergebende) Dokumentationspflicht - die gerade ja auch Beweiszwecken dienen soll - besteht. Dies ist gemäß § 10 BO bei Behandlungsunterlagen regelmäßig der Fall und gilt auch für die Erstellung des Arztbriefes, der Teil der Behandlungsunterlagen wird. So zumindest im Ergebnis auch das Urteil des LG Aachen vom 17. Dezember 1998 - 6 S 190/98, wonach ein Patient keinen Anspruch auf Korrektur eines Arztbriefs hat, der seiner Meinung nach eine falsche Diagnose enthält. Das LG Aachen wies die entsprechende Klage eines Mannes ab, der einen seiner Ansicht nach unrichtigen Arztbrief eines Facharztes an seinen Hausarzt korrigiert bekommen wollte. Der Arztbrief beinhalte nämlich eine eigenständige ärztliche Bewertung, auf die der Patient keinen Einfluss nehmen könne. Schließlich könne der Patient den Hausarzt auf die in seinen Augen bestehende Fehlerhaftigkeit des Briefes hinweisen. Eine Ausnahme kann nach Auffassung des Gerichts nur für „objektiv nicht haltbare, ehrverletzende Diagnosen“ gelten.

Bei falschen, aber dokumentationspflichtigen Daten sollte auf Verlangen des Patienten für die gesamte Dauer der Speicherung eine Gegendarstellung des Patienten beigefügt werden. Werden dann Daten übermittelt, darf dies nicht ohne diese Gegendarstellung erfolgen (vgl. § 35 Abs. 6 Sätze 2 und 3 BDSG).

8.4.2 Keine Duplizierung der Patientendatei beim Ausscheiden eines Arztes aus der Gemeinschaftspraxis

Im Berichtszeitraum erreichte mich die Anfrage eines Arztes, der aus der bisherigen, in Form einer GbR betriebenen Gemeinschaftspraxis auszuscheiden beabsichtigte. Da die Patientendaten sämtlicher Ärzte in einem Datenbestand zusammengefasst waren, kristallisierten sich Probleme bei der Trennung des Datenbestands heraus. Diese sollten umgangen werden, indem der gesamte Datenbestand dupliziert und sowohl der verbleibenden (Rest-)Gemeinschaftspraxis als auch dem ausscheidenden Arzt zur Verfügung gestellt wird. Um diese Vorgehensweise zu rechtfertigen, berief man sich zusätzlich darauf, dass bei der Trennung noch nicht vorhersehbar sei, welchen Arzt die Patienten zukünftig wählen würden.

Ich bin diesem Vorhaben mit folgender Begründung entgegengetreten:

Bei Gemeinschaftspraxen muss die freie Arztwahl gewährleistet bleiben. Folglich ist der behandelnde Arzt nicht beliebig austauschbar, selbst wenn der Patient zu Beginn nicht die Behandlung durch einen bestimmten Arzt gewünscht hat. Denn auch ein Patient, der sich auf die Behandlung durch einen bestimmten, z. B. zuständigen oder gerade freien Arzt einlässt, geht davon aus, zukünftig weiterhin von diesem betreut zu werden.

Hiermit übt der Patient (ggf. konkludent) sein Recht auf freie Arztwahl aus. Folge dieser Arztwahl ist, dass der ausgewählte Arzt zur Erhebung und Verarbeitung von Daten, die zur Berufsausübung erforderlich sind, berechtigt ist. Die Einwilligung erstreckt sich - soweit ausdrücklich nichts Gegenteiliges erklärt ist - nur auf den ausgewählten Arzt, nicht hingegen auf die Gemeinschaftspraxis als solche. Daher darf der behandelnde Arzt die Patientendaten lediglich exklusiv, d. h. allein und für seine Behandlungszwecke erheben und verarbeiten.

Darüber hinaus ist zu berücksichtigen, dass Ärzte der ärztlichen Schweigepflicht unterliegen. Diese gilt auch innerhalb aller Formen der ärztlichen Kooperation. Denn nur ein (behandelnder) Arzt persönlich, nicht hingegen eine Gemeinschaftspraxis, kann Täter einer Schweigepflichtsverletzung sein.

Ärzte haben demnach auch in ärztlichen Kooperationen die ärztliche Schweigepflicht und den Datenschutz derart zu beachten, dass die Patientendaten exklusiv durch den jeweiligen Arzt verarbeitet werden. Infolge dieser berufsrechtlich zwingend vorgesehenen Trennung der Datenverarbeitung sollten Probleme bei der Trennung der Datenbestände beim Ausscheiden eines Arztes aus einer Gemeinschaftspraxis bereits deshalb nicht entstehen, weil es einer solchen aufgrund der von vornherein getrennten Datenverarbeitung gar nicht mehr bedarf.

Da es - soweit beim Betrieb der Gemeinschaftspraxis datenschutzrechtliche Vorschriften eingehalten werden - also eigentlich keine Probleme bei der Trennung der Datenbestände geben dürfte, kommt eine Duplizierung des Datenbestands nicht in Betracht. Unabhängig davon wäre ein mit der „Datentrennung“ einhergehender Aufwand nicht geeignet, das Vorliegen einer Rechtsgrundlage für die Datenübermittlung zu ersetzen.

Da im Übrigen davon auszugehen ist, dass die Auseinandersetzung der Gemeinschaftspraxis mit einem gewissen zeitlichen Vorlauf erfolgt, besteht ohne weiteres die Möglichkeit, die Patienten über das bevorstehende Ausscheiden des betreffenden Arztes aus der Gemeinschaftspraxis zu informieren und um Mitteilung zu bitten, in welcher Praxis bzw. von welchem Arzt sie später weiterbehandelt werden möchten.

Sämtliche Daten von Patienten, die zunächst keine Erklärung abgeben, würden sodann zunächst in der (Rest-)Gemeinschaftspraxis verbleiben, während Daten von Patienten, die von dem ausscheidenden Arzt weiter betreut werden möchten, an diesen übergeben werden müssten. Letztere sind anschließend von der Gemeinschaftspraxis zu löschen.

8.4.3 Aufbewahrung von Patientenunterlagen bei unter Betreuung stehendem Arzt

Soweit ein Arzt, der aus gesundheitlichen Gründen unter Betreuung gestellt ist, nicht mehr in der Lage ist, seine Praxis selbständig zu führen und auch keine Praxisnachfolge geregelt ist, ist mit den in der Arztpraxis gelagerten Patientenunterlagen zwecks Sicherstellung der Aufbewahrung wie folgt zu verfahren:

Jeder Arzt hat als zivilrechtliche Nebenpflicht zum Behandlungsvertrag eine Dokumentationspflicht, die, wird sie nicht beachtet, zu erheblichen negativen Folgen für den niedergelassenen Arzt führen kann (Beweislastfragen). Auch die Aufbewahrungspflicht stellt daher meiner Auffassung nach eine zivilrechtliche Nebenpflicht dar. Denn die Dokumentation des Behandlungsverlaufs ist nur dann sinnvoll, wenn der Dokumentation auch die Pflicht zur Aufbewahrung der dokumentierten Krankenunterlagen folgt, damit Arzt und Patient sich später darauf berufen können. Der Aufbewahrungspflicht von Ärzten unterliegen „alle in Ausübung ihres Berufs gemachten Feststellungen und getroffenen Maßnahmen“ oder anders ausgedrückt alle „ärztlichen Aufzeichnungen und Untersuchungsbefunde“, kurz alle Krankenunterlagen. Hierunter fällt „die Summe aller Daten, die der Arzt und seine Hilfspersonen zur Erfüllung der ärztlichen Aufgabenstellung im Wege der Übermittlung durch den Patienten oder durch eigene Erhebung ermittelt oder selbst erzeugt haben“. Dazu gehören die Patientenkartei, einerlei ob sie handschriftlich, maschinenschriftlich oder EDV-technisch erzeugt worden ist, alle Fremdbefunde und Arztbriefe, Operations- und Transfusionsberichte, alle Ergebnisse von bildgebenden Verfahren (Röntgen, Sonographie, MRT etc.) und sonstige patientenbezogenen Datensammlungen.

Ärzte sind gemäß § 10 BO der SLÄK i. d. F. der Änderungssatzung vom 23. November 2007 ferner standesrechtlich dazu verpflichtet, die Dokumentations- und Aufbewahrungspflicht einzuhalten. Denn sie haben über die in Ausübung ihres Berufs gemachten Feststellungen und getroffenen Maßnahmen die erforderlichen Aufzeichnungen zu machen, § 10 Abs. 1 BO. Diese sind nicht nur „Gedächtnisstützen“ für den Arzt, sondern dienen auch dem Interesse der Patienten an einer ordnungsgemäßen Dokumentation. Ärztliche Aufzeichnungen sind nach § 10 Abs. 3 BO für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach gesetzlichen Vorschriften eine längere Aufbewahrungspflicht besteht (z. B. gemäß § 28 Abs. 4 Nr. 1

RöV: 30 Jahre nach der letzten Behandlung bei Aufzeichnungen über Röntgenbehandlungen).

Bei dieser Aufbewahrungspflicht dürfte es sich rechtlich um eine auf der Grundlage des Sächsischen Heilberufekammergesetzes geschaffene, öffentlich-rechtliche Pflicht handeln.

Die öffentlich-rechtliche Aufbewahrungspflicht gilt - sollte man wie wohl hier bereits die faktische Aufgabe der Arztpraxis aufgrund objektiver Unmöglichkeit des (weiteren) Betreibens der Praxis als ausreichend ansehen - berufsrechtlich ausdrücklich über den Zeitpunkt der Aufgabe der Praxis hinaus. Denn Ärzte haben ihre ärztlichen Aufzeichnungen und Untersuchungsbefunde auch nach Praxisaufgabe aufzubewahren oder dafür Sorge zu tragen, dass sie in gehörige Obhut gegeben werden (§ 10 Abs. 4 BO).

Vertragsärzte unterliegen neben der zivil- und standesrechtlichen Aufbewahrungspflicht noch einer weiteren öffentlich-rechtlichen Aufbewahrungspflicht aus dem Kassenarztrecht. Sie folgt aus § 57 Abs. 2 BMV-Ä sowie aus bundesgesamtvertraglichen Regelungen, die für den einzelnen Vertragsarzt über die jeweilige Satzung der Kassenärztlichen Vereinigung verbindlich sind (§ 81 Abs. 3 Nr. 1 SGB V).

Fraglich ist, ob als Lösungsweg die Aushändigung der Krankenunterlagen an den jeweiligen Patienten in Betracht käme:

Es ist streitig, ob sich der niedergelassene Arzt, der seine Praxis aufgibt, dadurch seiner über die Praxisaufgabe hinausreichenden öffentlich-rechtlichen Pflicht zur Aufbewahrung der Krankenunterlagen entledigen kann, dass er sie kurzer Hand seinen Patienten im Original aushändigt, damit diese sie einem von ihnen gewählten weiterbehandelnden Arzt aushändigen. Zivilrechtlich dürfte die Aufbewahrungspflicht entfallen, weil der Patient durch die Annahme der Krankenunterlagen konkludent auf die Nebenpflicht des Arztes zur weiteren Aufbewahrung seiner Krankenunterlagen verzichtet. Die öffentlich-rechtlich durch die ärztliche Berufsordnung und die Bundesmantelverträge dem (Vertrags-)Arzt auferlegte Aufbewahrungspflicht besteht demgegenüber jedoch ohne Rücksicht auf zivilrechtliche Erklärungen des Patienten, denn die Gefahr, dass Krankendaten verloren werden, ist beim Patienten sehr viel größer als beim (Vertrags-)Arzt. Es ist daher berufs- und vertragswidrig, wenn der (Vertrags-)Arzt Krankenunterlagen im Original aushändigt (Ausnahme: § 28 Abs. 6 RöV, der den Arzt verpflichtet, dem Patienten Originalröntgenaufnahmen vorübergehend zu überlassen).

Eine Aushändigung der Unterlagen z. B. an den Sohn des Praxisinhabers scheidet insoweit ebenfalls aus. Nur wenn die Ursache für die Praxisaufgabe der Tod des Praxisinhabers ist, geht die Praxis mit allen Rechten und Pflichten auf die Erben über (§ 1922

BGB). Die Schweigepflicht, an die der Arzt gemäß § 203 StGB und nach Berufsordnung gebunden war, geht zwar auf die Erben nicht über (wenn sie nicht selbst Ärzte sind), da die Schweigepflicht des Arztes aber wie die Dokumentations- und Aufbewahrungspflicht ebenfalls eine Nebenpflicht aus den früher geschlossenen Behandlungsverträgen darstellt, geht diese Nebenpflicht auf diejenigen Personen über, welche als Erben die Patientenkartei aus dem Nachlass erlangen. Von ihnen ist zu verlangen, dass sie - wie ein Arzt - alle zumutbaren Maßnahmen ergreifen, um eine ordnungsgemäße Aufbewahrung der Patientenkartei zu ermöglichen.

Zu überlegen ist, ob die Aufbewahrung von Krankenunterlagen aus nicht übergebenen Arztpraxen als Teil der Aufgabe der KV nach § 75 SGB V angesehen werden kann:

Der Sicherstellungsauftrag umfasst zunächst die Aufgabe, eine ausreichende vertragsärztliche Versorgung (auch Notdienst) sicherzustellen, mithin eine ausreichende Anzahl an Leistungserbringern zuzulassen. Der erweiterte Sicherstellungsauftrag nach § 75 Abs. 3 ff. SGB V umfasst lediglich die Ausdehnung des Sicherstellungsauftrags auf bestimmte Personen und Einrichtungen, nicht jedoch die Durchführung der Ausübung des zugelassenen Arztes. Der Gewährleistungsauftrag, also die Pflicht der KV, gegenüber den Krankenkassen die Gewähr dafür zu übernehmen, dass die vertragsärztliche Versorgung den gesetzlichen und vertraglichen Erfordernissen entspricht (§ 75 Abs. 1 Satz 1 SGB V), umfasst auch die Überwachungspflicht nach § 75 Abs. 2 Satz 2 SGB V: Danach haben sie die Erfüllung der den Vertragsärzten obliegenden Pflicht zu überwachen und - wenn nötig - unter Anwendung der in § 81 Abs. 5 SGB V vorgesehenen Maßnahmen zur Erfüllung der Pflichten anzuhalten. Das heißt, die Einhaltung der Pflichten kann mit den in der Satzung der jeweiligen KV vorgesehenen Disziplinarmaßnahmen durchgesetzt werden.

Der insoweit eindeutige Wortlaut des § 75 SGB V i. V. m. § 81 Abs. 5 SGB V zeigt, dass die KV lediglich zur Beseitigung von Pflichtverletzungen anhalten, also auffordern darf, dies ggf. mit den in § 81 Abs. 5 SGB V (abschließend genannten) Maßnahmen. Die Möglichkeit einer „Ersatzvornahme“, hier die Aufbewahrung der Krankenunterlagen zur Vermeidung einer andauernden nicht ordnungsgemäßen Aufbewahrung von Krankenunterlagen durch die KV, scheidet daher aus.

Fraglich ist weiterhin, ob eine Entsorgung der Krankenunterlagen („als materiell wertlos“) in Betracht kommt:

Eine Vernichtung von Krankenunterlagen durch den Arzt unter bewusstem Verstoß gegen die Aufbewahrungspflicht wäre rechtswidrig, weil der Arzt dadurch einerseits gegen alle Behandlungsverträge verstößt, die er jemals abgeschlossen hat und aufgrund

deren er noch Krankenunterlagen aufbewahrt. Denn er kann die aus diesen Verträgen resultierenden Nebenpflichten zur Aufbewahrung der Krankendaten nicht mehr erfüllen. Andererseits verstößt der (Vertrags-)Arzt damit gegen die Berufsordnung und gegen die Bundesmantelverträge. Dies dürfte bei einem Vertragsarzt zu einem kassenarztrechtlichen Verfahren wegen Pflichtverletzung (siehe § 6 der Satzung der KV vom 11. Mai 2007) sowie, wie bei einem Arzt, der privat niedergelassen war, zu einem berufsgerichtlichen Verfahren führen. Insbesondere aber kann eine solche Vernichtung zu einer Umkehr der Beweislast in einem Haftungsprozess gegen den Arzt führen und Schadensersatzansprüche wegen nicht mehr möglicher Auskunftserteilung aus den vernichteten Unterlagen auslösen. Eine Vernichtung der Unterlagen scheidet mithin aus.

Es verbleibt daher bei der Zuständigkeit des Betreuers, für eine ordnungsgemäße Aufbewahrung der Unterlagen zu sorgen. Der Betreuer sollte in diesem Fall darauf aufmerksam gemacht werden, dass es auch in Sachsen ansässige Unternehmen gibt, die als Auftragsdatenverarbeiter Patientendaten für ärztliche Stellen aufbewahren, was selbstverständlich mit entsprechenden finanziellen Aufwendungen verbunden ist.

8.4.4 Fragebogen für Blutspender

Im Kontext der Beratung eines Blutspendedienstes richtete sich meine Aufmerksamkeit auch auf dessen Fragebogen für Blutspender.

Nach § 11 Abs. 1 und 2 i. V. m. § 5 Abs. 1 TFG dürfen Spendeeinrichtungen personenbezogene (Gesundheits-)Daten spendewilliger und spendender Personen erheben, verarbeiten und nutzen, soweit dies für eine nach dem Stand der medizinischen Wissenschaft und Technik erforderliche (positive) Auswahl der Spender bzw. einen Ausschluss oder eine Zurückstellung einzelner Personen aus Gründen der Risikovermeidung erforderlich ist.

Nach den gemäß § 12a TFG erlassenen Richtlinien der Bundesärztekammer „*zur Gewinnung von Blut und Blutbestandteilen und zur Anwendung von Blutprodukten (Hämotherapie)*“ sind nach dem Stand der medizinischen Wissenschaft folgende Personen wegen besonderer Infektionsrisiken dauerhaft von der Blutspende auszuschließen:

- heterosexuelle Personen mit sexuellem Risikoverhalten, z. B. Geschlechtsverkehr mit häufig wechselnden Partnern,
- Männer, die Sexualverkehr mit Männern haben,
- männliche und weibliche Prostituierte,

- Drogenabhängige,
- Häftlinge.

Es besteht also nach diesen Regelwerken, die ich nicht weiter zu hinterfragen habe, ein Bedürfnis im Sinne von § 11 Abs. 2 Satz 1 TFG, eine Risikogruppenzugehörigkeit erfragen und damit erheben zu müssen.

Nicht erforderlich ist jedoch die Kenntnis, welcher einzelnen bzw. konkreten Risikogruppe der Spendewillige jeweils zugehörig ist, da bei allen Risikogruppen gleichermaßen ein Ausschluss von der Spende erfolgt. Es muss also nach Antwort auf die vom Spendedienst gewählte Fragestellung offen bleiben (können), welches konkrete Risiko der Spendewillige verwirklicht hat. Zudem muss sich die Fragestellung mit übrigem Recht, wie auch dem Recht der diskriminierungsfreien Gleichbehandlung, vereinbaren lassen - andernfalls stünde dies einer datenschutzrechtlichen Erhebungsbefugnis ebenso entgegen. Deshalb ist ein Spendedienst nicht befugt, im Sinne einer positiven oder negativen Diskriminierung (vermeintlich) weitere Risikogruppen in seine Abfrage einzubeziehen oder eine von der Bundesärztekammer wissenschaftlich anerkannte Risikogruppe auszunehmen.

Einen solchen, die datenschutzrechtliche Gestattung von Fragen hindernden Mangel habe ich vorliegend insoweit gesehen, dass der Blutspendedienst es zwar für geboten erachtete, bei den besonders infektionsgefährdeten Personengruppen explizit nach homo- oder bisexuellen Männern sowie Prostituierten zu fragen, nicht aber - wie von der Bundesärztekammer vorgesehen - auch nach heterosexuellen Personen mit sexuellem Risikoverhalten, z. B. Geschlechtsverkehr mit häufig wechselnden Partnern. Auch war nicht ersichtlich, weshalb jenseits anderer Gruppen mit risikogeneigtem Sexualverhalten nochmals ausdrücklich nach Prostituierten und deren „Kunden“ gefragt wurde.

Für datenschutzrechtlich unzulässig habe ich ferner die explizite Frage nach dem Sexualverhalten des - jedenfalls bei gemeinsamen Wohnsitzen auch für den Blutspendedienst bestimmbaren - Partners spendewilliger Frauen gehalten, da § 11 Abs. 2 Satz 1 TFG den Spendedienst nicht zur Datenerhebung über Dritte ohne deren Einwilligung ermächtigt, wobei dies hier sogar besondere personenbezogene Daten im Sinne des § 3 Abs. 9 BDSG betrifft.

Der betroffene Blutspendedienst hat seinen Fragebogen eingedenk meiner Vorbehalte in Absprache mit dem aufsichtsführenden Paul-Ehrlich-Institut, Bundesinstitut für Impfstoffe und biomedizinische Arzneimittel, inzwischen überarbeitet und dabei meinen Bedenken weitgehend Rechnung getragen. Soweit keine Abhilfe erfolgt ist, muss ich jedoch respektieren, dass ich nicht dazu befugt bin, medizinische Bewertungen infrage

zu stellen, zumal die Spender letztendlich frei sind, ob sie bei einem bestimmten Blutspendedienst unter Preisgabe der von ihm gewünschten Daten ihr Blut spenden wollen.

8.5 Handel, Gewerbe, Dienstleistungen

8.5.1 Heimliche Aufzeichnung eingehender Telefonate

Bei der Prüfung eines Einkaufszentrums stellte ich zufällig fest, dass das Management routinemäßig alle im Einkaufszentrum unter der zentralen Rufnummer eingehenden Telefonate für die Dauer von mehreren Tagen heimlich aufzeichnete. Dies erfolgte offenbar, weil der Betreiber Drohanrufe fürchtete.

Eine Aufzeichnung aus diesem Grund ist jedoch bei einem allein abstrakten Risiko nicht verhältnismäßig und damit unzulässig (vgl. Pkt. 8.8.1). Wegen des Verdachts einer Straftat nach § 201 StGB, also einer Verletzung der Vertraulichkeit des nicht-öffentlich gesprochenen Wortes durch eine unbefugte Aufzeichnung, habe ich noch vor Ort die Polizei hinzugezogen und ihr die weiteren Ermittlungen übergeben, da ich über die Aufsicht hinaus nicht selbst für eine Strafverfolgung persönlichkeitsrechtsrelevanter Straftaten zuständig bin, sondern dies der Staatsanwaltschaft und ihren Ermittlungspersonen obliegt.

Eine Ahndung setzte allerdings nach § 205 Abs. 1 StGB einen Strafantrag voraus, den meine Behörde als Institution jedoch nicht hat stellen können, da dies in § 38 Abs. 1 Satz 6 BDSG nicht vorgesehen ist und somit nur Geschädigte hierzu befugt sind. Da einer meiner Mitarbeiter allerdings bei der telefonischen Ankündigung meiner Kontrolle ebenso aufgezeichnet worden war, konnte er durch einen höchstpersönlichen Strafantrag das Verfolgungshindernis beseitigen.

Die Strafverfolgung scheiterte jedoch letztendlich an der fehlgeschlagenen Auswertung des veralteten und teilweise defekten Aufzeichnungsgeräts und dem Nachweis persönlicher Verantwortlichkeiten.

Örtliche Kontrollen anderer Einkaufzentren des gleichen Betreibers - auch durch meine Kollegen in anderen Bundesländern - haben weiterhin Anhaltspunkte dafür ergeben, dass die Verantwortlichen unmittelbar nach meinem Auffinden des Aufzeichnungsgeräts alle anderen Geräte im Bundesgebiet sofort abgebaut und jede weitere Aufzeichnung umgehend beendet haben - dies ist im Ergebnis auch ein aufsichtlicher Erfolg.

8.5.2 Ausweiskopien beim Schrottaufkauf

Metallhändler und Recyclingbetriebe, die den Erwerb von Diebesgut zumindest billigend in Kauf nehmen, können sich der Hehlerei strafbar machen (§ 259 Abs. 1 StGB).

Zudem kann gutgläubig kein Eigentum an Diebesgut erworben werden (§ 935 Abs. 1 Satz 1 BGB). Metallhändler und Recyclingbetriebe haben somit wegen des Erwerbs von Altmetallen ein berechtigtes rechtliches Interesse zu dessen Herkunft und damit zur Identität des Verkäufers personenbezogene Daten zu erheben und zur Dokumentation (der Redlichkeit) des Rechtsgeschäfts sowie aus steuer- und handelsrechtlichen Gründen zweckgebunden nach Maßgabe der hierfür einschlägigen Fristen zu speichern, insbesondere weil Metalldiebstähle derzeit sehr weit verbreitet sind, also kein lediglich abstraktes Risiko darstellen (§ 28 Abs. 1 Satz 1 Nr. 1 und 2 BDSG).

Zwischen den Aufsichtsbehörden und der Interessenvertretung der Metallrecyclingwirtschaft ist jedoch streitig, inwieweit deswegen auch ein Erfordernis besteht, inländische Ausweisdokumente zur Person des Metallverkäufers fotokopieren zu müssen.

Gegenüber verantwortlichen Stellen, die meiner Aufsicht unterfallen, habe ich bisher die Auffassung vertreten, dass zu Dokumentationszwecken in nicht-automatisierter Weise ausreichend vermerkt werden kann, welches Dokument zu welcher Person (Name, Anschrift) mit welcher Nummer beim Verkauf vorgelegen hat, da im Bedarfsfall die Ermittlungsbehörden alle sonst zu dem Dokument hinterlegten Daten einschließlich des Lichtbilds bei den kommunalen Ausweisbehörden abrufen können.

Das von der Metallrecyclingwirtschaft behauptete Verlangen der Finanzverwaltung oder anderer Behörden, Ausweise von Metallverkäufern wegen des Risikos des Ankaufs von Diebesgut immer zu kopieren, konnte von den verantwortlichen Stellen bisher nicht belegt werden, zumal die Rechtsprechung im Allgemeinen auch nur eine Einsicht verlangt (BFH, Urteil vom 10. März 1999 - Az. XI R 10/09 - juris). Andere Aufsichtsbehörden haben gegenteilige Vorgaben bisher ebenso nicht feststellen können.

Vorbehaltlich einer abschließenden gemeinsamen Position der Aufsichtsbehörden, gestehe ich der hiesigen Metallrecyclingwirtschaft eine Kopierbefugnis ohne besondere Gründe des Einzelfalls erst dann zu, wenn die Summe der Verkäufe durch eine Person den Veräußerungswert 50,00 Euro überschreitet, es sich also nicht nur um geringfügige Gelegenheitsverkäufe ohne auffälligen Gewerbecharakter handelt. Weiterhin sind solche Daten des Ausweises, die nicht zwingend zur Identifizierung benötigt werden, sowie insbesondere die bei neuen Personalausweisen aufgedruckte Zugangsnummer für Online-Funktionalitäten, zu schwärzen.

8.5.3 Auftragsdatenverarbeitungsverträge: Schriftform und Inhalte

Sicher war der unter Pkt. 4.2.2 dargestellte Fall eines Service-Rechenzentrums, welches mit seinen etwa 300 Auftraggebern keine schriftlichen Auftragsdatenverarbeitungsverträge abgeschlossen hatte, ein seltener - zugegebenermaßen extremer - Ausnahme-

fall. Schon häufiger musste ich bei meinen Kontrollen allerdings feststellen, dass schriftliche Verträge zwar abgeschlossen worden waren, diese jedoch den inhaltlichen Vorgaben des § 11 Abs. 2 Satz 2 BDSG nicht genügten.

Kaum Probleme bereiten naturgemäß die Festlegung von Gegenstand und Dauer des Auftrags (§ 11 Abs. 2 Satz 2 Nr. 1 BDSG), da dies keine ausschließlich datenschutzbezogenen Inhalte sind. Bezüglich der übrigen, in § 11 Abs. 2 Satz 2 BDSG unter den Nummern 2 bis 10 vorgegebenen Vertragsinhalte stelle ich jedoch immer wieder fest, dass diesbezügliche Regelungen nicht oder nur unzureichend vereinbart worden sind oder aber auch nur der bloße Wortlaut des Gesetzes wiedergegeben ist. Folgende typische Mängel sind diesbezüglich zu benennen:

- Umfang, Art und Zweck der Erhebung, Verarbeitung und Nutzung von Daten (§ 11 Abs. 2 Satz 2 Nr. 2 BDSG) sind oftmals nur unzureichend festgelegt. Erforderlich sind hier konkrete generelle Weisungen bezogen auf die einzelnen Verarbeitungsschritte (Petri in Simitis, BDSG, 7. Aufl., Rdnr. 68 zu § 11), mithin eine genaue Beschreibung der vom Auftragnehmer zu erbringenden Leistungen (Gabel in Taeger/Gabel, Kommentar zum BDSG, Rdnr. 43 zu § 11). Konkret zu benennen sind also beispielsweise die durchzuführenden Berechnungen und die zu erstellenden Übersichten, Bescheinigungen, Meldungen und Auswertungen.
- Die Beschreibung der Art der Daten (§ 11 Abs. 2 Satz 2 Nr. 2 BDSG) ist in vielen Fällen zu allgemein gehalten und daher wenig aussagekräftig sowie auch unvollständig. Viel zu allgemein gehalten ist beispielsweise die Formulierung „personenbezogene Daten“, da dies Anwendungsvoraussetzung des Bundesdatenschutzgesetzes und damit auch der Vorschriften zur Auftragsdatenverarbeitung ist und somit auf alle in diesem Zusammenhang bedeutsame Datenarten zutrifft. Dem Regelungsziel von § 11 Abs. 2 Satz 2 BDSG entsprechend müssen die Angaben zu den Datenarten wesentlich konkreter gefasst werden, globale Bezeichnungen genügen jedenfalls nicht (Petri in Simitis, BDSG, 7. Aufl., Rdnr. 70 zu § 11).
- Hinsichtlich der nach § 9 BDSG zu treffenden technischen und organisatorischen Maßnahmen ist häufig lediglich der Inhalt der Anlage zu § 9 BDSG wiedergegeben; darüber hinaus werden diesbezüglich oft noch unbestimmte Zusicherungen und Absichtserklärungen abgegeben. Dies ist nicht ausreichend. § 11 Abs. 2 Satz 2 Nr. 3 BDSG fordert insoweit die schriftliche Festlegung konkreter Einzelmaßnahmen, mit denen die in der Anlage zu § 9 BDSG formulierten Sicherungsziele erreicht werden können. Dieser Forderung kann sicherlich auch durch die Bezugnahme auf ein beim Auftragnehmer bestehendes Datensicherheitskonzept entsprochen werden, allerdings ist dieses dann ausdrücklich als Vertragsbestandteil zu deklarieren und dem Vertrag auch beizufügen.

- Soweit der Vertrag keine Regelung der Berechtigung zur Begründung von Unterauftragsverhältnissen enthält, bedeutet dies letztendlich, dass der Auftragnehmer auch nicht berechtigt ist, Unterauftragsverhältnisse einzugehen. Tatsächlich ist dies im Regelfall weder gewollt noch wird es so praktiziert, denn zumeist kommt auch ein Auftragnehmer nicht ohne Unterauftragsverhältnisse aus. Typische Beispiele sind dabei die Akten- und Datenträgervernichtung und die (Fern-)Wartung der eigenen Datenverarbeitungsanlage.

8.5.4 Werbeanrufe: Schriftliche Bestätigung nicht schriftlich erteilter Einwilligungen

§ 28 Abs. 3a BDSG schreibt für Einwilligungen, die gemäß § 4a Abs. 1 Satz 3 BDSG nicht in Schriftform erteilt worden sind und die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke der Werbung betreffen, vor, dass sie nachträglich schriftlich zu bestätigen sind. Erst dann stellen sie eine Rechtsgrundlage für die betreffende Datenverwendung dar (§ 28 Abs. 3 Satz 1 BDSG).

Auf diese Vorschrift wollte sich auch ein Autohaus, das seine Kunden in eigener Initiative angerufen, von diesen das mündliche Einverständnis eingeholt und dieses anschließend schriftlich bestätigt hatte, berufen.

Allerdings war allein schon dieser Anruf unzulässig. Zwar ist die Frage, ob Anrufe, die ausschließlich der Einholung eines Einverständnisses mit der werblichen Nutzung der Daten des Angerufenen dienen, zulässig sind, ist in erster Linie ein - außerhalb meiner Zuständigkeit liegendes - wettbewerbsrechtliches Problem. Die diesbezüglichen Wertungen des Gesetzgebers sind aber auch für die Interessenabwägung unter datenschutzrechtlichen Gesichtspunkten (§ 28 Abs. 3 Satz 6 BDSG) von Bedeutung. Insoweit ist auf zwei Entscheidungen des LG Leipzig (Urteil vom 5. April 2005 - Az. 5 O 512/05 sowie Beschluss vom 9. Oktober 2009 - Az. 5 O 3424/09; jeweils in juris) hinzuweisen, die beide die telefonische Kontaktaufnahme zwecks Einholung eines Einverständnisses mit der Datennutzung für Werbezwecke für wettbewerbswidrig erklären. Unter dieser Voraussetzung stellten die diesbezüglichen Anrufe dann aber wiederum auch unter datenschutzrechtlichen Gesichtspunkten eine unzulässige Datennutzung dar, denn wettbewerbswidrige Anrufe verletzen nicht nur schutzwürdige Interessen der Wettbewerber sondern auch der Betroffenen.

Alternativ wollte das Autohaus seine Bestandskunden ohne vorherigen Anruf anschreiben und ihnen unter Bezugnahme auf die bisherige Praxis noch einmal die Verwendung der Telefonnummern auch für werbliche Anrufe „bestätigen“. Auch dies wäre jedoch unzulässig gewesen, denn Voraussetzung für die Anwendbarkeit von § 28 Abs. 3a

Satz 1 BDSG ist, dass bereits eine (nicht-schriftliche) Einwilligungserklärung abgegeben worden ist. Der Sachverhalt, dass noch überhaupt keine Einwilligung vorliegt, erfüllt die Voraussetzungen des § 4a Abs. 1 Satz 3 BDSG gerade nicht, denn es liegt ja überhaupt keine Erklärung des Betroffenen vor, und nicht etwa ein Umstand, der nur die Schriftlichkeit der Erklärung als entbehrlich hat erscheinen lassen.

8.6 Sparkassen / Banken

8.6.1 Automatische Kontostandsanzeige bei Geldautomaten

Auf eine Kundenbeschwerde hin, dass an einem Geldautomaten einer Sparkasse nach der Geldentnahme weithin sichtbar noch für eine geraume Zeit der aktuelle Kontostand angezeigt würde, habe ich kurzerhand zum Selbstversuch gegriffen. Eine meiner Mitarbeiterinnen, ihrerseits gleichfalls Kundin einer (anderen) Sparkasse erklärte sich bereit, den Vorfall nachzustellen, d. h. im Beisein von Kollegen an einem Geldautomaten dieser Sparkasse einmal Geld abzuheben.

Dabei musste ich feststellen, dass nach Entnahme der EC-Karte und des Geldes in der Tat noch für ganze sieben Sekunden der aktuelle Kontostand angezeigt wurde und von schräg dahinter stehenden (wartenden) Kunden mühelos eingesehen werden konnte. Streng genommen wäre dieser Selbstversuch gar nicht nötig gewesen, denn als ich am Geldautomaten eintraf, hob ohnehin gerade ein Kunde Geld ab und verschwand - nachdem er sein Geld entnommen hatte - sofort wieder vom Geldautomaten, so dass alle wartenden Kunden praktisch freien Blick auf den Bildschirm hatten.

Man sollte meinen, das Problem sei offensichtlich und eine Beseitigung nur eine Frage kurzer Zeit. Doch weit gefehlt - die Sparkasse war alles andere als bereit, hier kurzfristig Abhilfe zu schaffen. Auch der Verweis auf einen vergleichbaren Sachverhalt (automatische Kontostandsanzeige unmittelbar nach Authentifikation des Kunden, also zu einem früheren Zeitpunkt innerhalb des Geldabhebevorgangs) im ersten TB für den nicht-öffentlichen Bereich (Pkt. 4.3.19) beeindruckte die Sparkasse nicht. Erst nachdem ich nach längerer Diskussion eine datenschutzrechtliche Anordnung in Aussicht gestellt und bereits die dazugehörige Anhörung versandt hatte, lenkte man dort ein und unterband die automatische Kontostandsanzeige.

Schon der Petentin gegenüber hatte die Sparkasse kein Verständnis für die Problematik gezeigt. Die den Geldabhebevorgang abschließende Kontostandsanzeige sei auf vielfachen Kundenwunsch eingerichtet worden und nur wenn sich noch eine Reihe mehr Kunden beschweren würden, könne man darüber nachdenken, diesen Automatismus wieder abzuschalten. Gegenüber mir argumentierte die Sparkasse mit einem dadurch verbesserten Kundenservice, der von den Kunden überwiegend positiv zur Kenntnis

genommen worden sei. Spezielles Sicherungsglas, Sichtschutzblenden und auch die eingerichteten Diskretionszonen verhinderten die seitliche Einsichtnahme in den Bildschirminhalt durch Dritte und im Übrigen habe es der Kunde selbst in der Hand, sich so vor dem Bildschirm zu positionieren und insbesondere (nach dem Geldempfang) auch noch solange davor zu verweilen, dass eine Einsichtnahme durch Dritte nicht möglich sei. Zu guter Letzt wurde meine Forderung auch noch aus Verhältnismäßigkeitsgründen abgelehnt. Den Kunden koste es nur einen sehr geringen persönlichen Aufwand, unbefugtes Mitlesen zu verhindern, während die erforderliche Softwareumstellung nur mit hohen Kosten und hohem Aufwand durch die Sparkasse zu bewerkstelligen sei.

Diese Argumente der Sparkasse trugen aber nicht:

Gemäß § 9 BDSG haben verantwortliche Stellen die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine Ausführung der Vorschriften des Bundesdatenschutzgesetzes, insbesondere die in der Anlage (zu § 9 Satz 1) genannten Anforderungen, zu gewährleisten.

Die erforderlichen technischen und organisatorischen Maßnahmen sind durch die verantwortliche Stelle, vorliegend also durch die Sparkasse, zu treffen. Dieser Vorschrift ist demnach nicht genüge getan, wenn im Falle der automatischen Kontostandsanzeige die diesbezügliche Verantwortung auf den Betroffenen verschoben wird, indem dieser auf die Möglichkeit verwiesen wird, dass nur er selbst durch ein Verweilen vor dem Bildschirm bis zum Verlöschen der Kontostandsanzeige sicherstellen kann, dass keine unberechtigte Einsichtnahme durch Dritte erfolgt. Stattdessen ist die Gefahr der Einsichtnahme durch Dritte bereits durch entsprechende Maßnahmen der verantwortlichen Stelle auf ein Mindestmaß zu reduzieren. Diese hat im Rahmen der Zutrittskontrolle (vgl. Satz 2 Nr. 1 der Anlage zu § 9 BDSG) geeignete Maßnahmen zu treffen, die gewährleisten, dass Unbefugten die räumliche Annäherung an den Geldautomaten solange verwehrt wird, wie an diesem personenbezogene Daten Dritter sichtbar sind. Zutritt im Sinne der Zutrittskontrolle beschränkt sich dabei nicht auf das Betreten eines Raums oder Bereichs. Zutritt hat auch, wer durch Glaswände, ungenügende Abschirmung oder nicht rechtzeitiges Löschen von Bildschirmanzeigen personenbezogene Daten Dritter zur Kenntnis nehmen kann (vgl. Ernestus in Simitis, BDSG, 7. Aufl., Rdnr. 77 zu § 9). Da praktisch nicht verhindert werden kann, dass Kunden nach Erhalt ihrer EC-Karte und des Geldes sofort - was nachvollziehbar ist - den Geldautomaten verlassen, muss die verantwortliche Stelle also zusätzlich zu den - in diesem Fall offensichtlich allein nicht ausreichenden - räumlichen Sicherungsmaßnahmen dafür sorgen, dass nach Abschluss des Geldabhebens, also spätestens mit dem Öffnen des Geldfachs, keine personenbezogenen Daten mehr am Bildschirm sichtbar sind.

Meine Forderung der Abschaltung dieser Funktionalität war auch nicht unverhältnismäßig (vgl. § 9 Satz 2 BDSG). Genauso einfach wie die ausschließlich auf Kundenwunsch erfolgte Einführung der automatischen Kontostandsanzeige gewesen war, musste sich doch eigentlich auch deren Abschaltung darstellen. Angesichts der besonderen Sensibilität des Kontostands wäre aber auch ein höherer Aufwand für die Umsetzung dieser Maßnahme ohne weiteres zu rechtfertigen gewesen.

Die - üblichen - im Vorfeld von der Sparkasse benannten Sicherungsmaßnahmen wie Sichtschutzblenden, Diskretionszonen und Sicherungsglas haben zwar allesamt ihre Berechtigung, jedoch sind diese eben nicht geeignet, den Risiken der automatischen Kontostandsanzeige am Ende des Geldabhebevorgangs tatsächlich wirksam entgegenzuwirken. Als logische Folge verbleibt als Lösungsmöglichkeit demnach ausschließlich die Abschaltung dieser Funktionalität. Bei der Bewertung dieses Sachverhalts ist im Übrigen zu berücksichtigen, dass an Geldautomaten auch bei anderen Geldinstituten für eigene Kunden die Möglichkeit besteht, sich den Kontostand anzeigen zu lassen. Nur bedarf es hierzu einer entsprechenden individuellen Anforderung durch den Kunden; eine Serviceverschlechterung ist insoweit nicht zu erkennen. Die Lösung mit einem Anforderungs-Button ist aus datenschutzrechtlicher Sicht auch nicht zu beanstanden. Problematisch ist lediglich die Verfahrensweise, dass der Kontostand standardmäßig, d. h. ohne Anforderung durch den Kunden und zudem auch noch nach Abschluss des Geldabhebevorgangs angezeigt wird.

Unabhängig davon hatte ich schon bei der Überprüfung einiger Filialen im Rahmen meines Selbstversuchs feststellen müssen, dass bei dieser Sparkasse eben gerade nicht in jeder SB-Filiale eine ausreichende räumliche Abtrennung, ein Sichtschutz oder eine Diskretionszone vorhanden waren. Direkt hinter oder neben dem Geldautomaten befand sich zumeist ein Kontoauszugsdrucker, so dass ein Einhalten von Diskretionszonen, soweit vorhanden, bei gleichzeitiger Nutzung der Geräte nicht möglich war. Aufgrund der Raumgröße sowie der räumlichen Anordnung der Geräte war in allen von mir besichtigten Filialen ein Einsehen des Bildschirms durch wartende Kunden problemlos möglich. Auch verhinderte der an einigen Geldautomaten angebrachte Sichtschutz (spezielles Sicherungsglas) nicht wirklich, dass Nichtberechtigte den Bildschirm des Geldautomaten einsehen können.

8.7 Vereine / Verbände

8.7.1 Personalisierung von Eintrittskarten

Die Personalisierung von Eintrittskarten insbesondere bei Auswärtsspielen wird zunehmend als eine Möglichkeit gesehen, die in letzter Zeit verstärkt aufgetretenen Zuschauerausschreitungen bei Fußballspielen zukünftig wirkungsvoller zu verhindern.

Datenschutzrechtliche Vorgaben stehen einer solchen Personalisierung - datenschutzrechtlich handelt es sich um eine Nutzung, ggf. auch um eine Übermittlung personenbezogener Daten (mindestens an den gastgebenden Verein) - nicht von vornherein entgegen; allerdings ist deren Durchführung an eine Reihe von Zulässigkeitsvoraussetzungen gebunden.

Personalisierung von Eintrittskarten bedeutet, dass sie mittels geeigneter Hilfsmittel eindeutig einem konkreten Zuschauer zugeordnet werden können. Dessen Name kann dabei - mit dem Ziel einer vergleichsweise einfachen Kontrollmöglichkeit - auf der Eintrittskarte vermerkt sein, muss es aber nicht. Wesentlich ist stattdessen das Vorhandensein einer Zuordnungsfunktion zwischen der in diesem Fall notwendigerweise zu erstellenden Zuschauerliste und den durchnummerierten bzw. anderweitig gekennzeichneten Eintrittskarten.

Für die datenschutzrechtliche Bewertung maßgeblich ist § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Der genannte Erlaubnistatbestand setzt also zunächst voraus, dass die Personalisierung für den beabsichtigten Zweck erforderlich ist, d. h. der Zweck muss mit der Personalisierung auch tatsächlich erreicht werden können und es darf keine milderen Mittel geben, mit denen der angestrebte Zweck gleichfalls erreicht werden kann.

Eine Personalisierung ist dabei aber nur dann geeignet, bestimmten Personengruppen (z. B. Personen mit Stadionverbot, bekannten Hooligans und Gewalttätern) tatsächlich den Zugang zum Stadion zu verwehren und gleichzeitig einen Ermittlungsansatz für ggf. dennoch auftretende Zwischenfälle im Stadion zu haben (namentliche Bekanntheit der Zuschauer), wenn sie mit einer sicheren Identifikation jedes Zuschauers beim Kartenkauf, dem Verbot einer Weiterveräußerung der erworbenen Eintrittskarte sowie einer nochmaligen, konsequenten Überprüfung der Nutzungsberechtigung beim Einlass ins Stadion einschließlich einer Ausweispflicht für die Zuschauer verbunden wird. Solange dies nicht gewährleistet ist, ist eine Personalisierung der Eintrittskarten zur Zweckerreichung, unerwünschten Personenkreisen tatsächlich den Zugang zum Stadion zu verwehren, nicht geeignet und somit unzulässig. Entscheidender Aspekt sind dabei die Identitätskontrollen am Stadioneinlass. Soweit hier keine konsequente Kontrolle der Karteninhaber erfolgt (Abgleich von Ausweisdaten [Name, Vorname, Anschrift] mit der beim Kauf erstellten Zuschauerliste bzw. zumindest Abgleich von Ausweisdaten

[Name, Vorname] mit dem ggf. erfolgten Aufdruck dieser Daten auf der Eintrittskarte und Zurückweisung aller nichtberechtigten Karteninhaber), kann eine missbräuchliche Nutzung der Eintrittskarten und damit der Zutritt durch unerwünschte Personen auch nicht verhindert werden.

Der in der Presse und auch von den Vereinen immer wieder genannte Zweck, Personen mit Stadionverbot keine Eintrittskarten zu verkaufen bzw. - was entscheidender ist - diesen keinen Zutritt zum Stadion zu gewähren, rechtfertigt für sich allein noch keine Personalisierung der Eintrittskarten, denn dies kann auch auf andere, das Recht auf informationelle Selbstbestimmung schonendere Art und Weise gewährleistet werden. Ersteres könnte durch einen einfachen Abgleich der Käuferdaten (Online-Verkauf) mit einer um die Personen mit Stadionverbot bereinigten Mitgliederliste bzw. mit einer sich auf die Personen mit Stadionverbot beschränkenden Sperrliste erfolgen; Letzteres hingegen mit diesbezüglich wirksamen Einlasskontrollen (gleichfalls unter Verwendung der genannten Sperrliste) erreicht werden.

Nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG darf darüber hinaus kein Grund zu der Annahme bestehen, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Verarbeitung oder Nutzung überwiegt. Nach wie vor verhält sich auch bei Auswärtsspielen der weitaus überwiegende Teil der Zuschauer im Stadion friedlich und gibt damit keinen Anlass für eine Überwachung seines Freizeitverhaltens, insbesondere der Erhebung und Speicherung der Tatsache, dass er ein konkretes Auswärtsspiel seines Fußballvereins besucht hat. Durch die Personalisierung der Eintrittskarten müssen sich diese Fans jedoch in nachvollziehbarer Weise unter Verdacht gestellt fühlen. Sie haben natürlich ein schutzwürdiges Interesse daran, dass diese Daten nicht gespeichert werden, also dass nicht nachvollzogen werden kann, was sie in ihrer Freizeit unternommen haben, geschweige dann, dass sie vielleicht gerade deshalb auch - unberechtigterweise - in den Blick von Ermittlungsbehörden geraten können. Allerdings sind die Vorkommnisse bei den Auswärtsspielen einiger Vereine zuletzt so gravierend gewesen, dass nicht mehr ohne weiteres unterstellt werden kann, dass die einer Personalisierung entgegenstehenden schutzwürdigen Interessen der Fans das berechtigte Sicherheitsinteresse des Vereins, das insoweit wegen der diesbezüglichen Verantwortung des Vereins zugleich ein öffentliches Interesse ist, in jedem Fall überwiegen. Gerade bei sogenannten Risikospielen hat das berechtigte Interesse des Vereins an einer Personalisierung nach den in der Vergangenheit gemachten Erfahrungen ein solch hohes Gewicht, dass jedenfalls bei derartigen Spielen eine Personalisierung der Eintrittskarten datenschutzrechtlich zulässig erscheint. Allerdings müssen dazu weitere Voraussetzungen erfüllt sein:

(1) Schaffung einer größtmöglichen Transparenz für die an einem Kartenkauf interessierten Vereinsmitglieder:

Diesen muss ausreichend erläutert werden, welche personenbezogenen Daten im Rahmen der Personalisierung durch wen zu welchen Zwecken erhoben, verarbeitet und genutzt werden. Es muss deutlich werden, wer für den Kartenverkauf des jeweiligen Auswärtsspiels verantwortlich ist - Gastgeber- oder Gastverein - und welche Mitgliederdaten an den Gastgeberverein direkt (Zuschauerliste zur Einlasskontrolle bei Kartenverkauf in Verantwortung des Gastvereins - s. o.) oder indirekt (Mitgliederdatei zum Datenabgleich bei beschränktem Eintrittskartenverkauf in Verantwortung des Gastgebervereins) übermittelt werden.

(2) Wirksame Identitätsprüfung:

Bereits beim Kartenkauf muss eine ausreichende Identitätsprüfung erfolgen. Beim Onlinekauf geschieht dies im Allgemeinen dadurch, dass die erworbenen Eintrittskarten nach Überprüfung der Mitgliedschaft per Post an die Käufer versandt werden. Beim Kauf an einer Vorverkaufsstelle wäre in diesem Fall eine Sichtkontrolle des Personal- bzw. Mitgliedsausweises vorzunehmen.

Vom Verein zu klären ist, auf welche Weise dann die eigentliche Personalisierung erfolgen soll. Gilt der Käufer zugleich als Ticketinhaber und darf jedes Vereinsmitglied nur eine Karte erwerben, stellt dies sicherlich kein Problem dar. Anders verhält es sich, wenn Käufer und Ticketnutzer auseinanderfallen (dürfen) oder wenn Mitglieder mehr als eine Eintrittskarte erwerben können. Soweit dabei - wie ich feststellen musste - beliebige Vor- und Zunamen (auch Fantasienamen!) für den Aufdruck auf der Eintrittskarte angegeben werden können und dies letztendlich auch folgenlos bleibt, kann (und muss) man sich die Personalisierung auch sparen. Dabei steht und fällt diese Problematik mit der tatsächlichen Kontrollpraxis am Stadioneinlass. Müssen die Besucher hier mit wirksamen Identitätskontrollen - was ich ja eingangs bereits als notwendige Voraussetzung für die Zulässigkeit der Personalisierung von Eintrittskarten erklärt habe - und ggf. trotz Eintrittskarte wegen nicht übereinstimmender Namensangaben mit einem Zutrittsverbot rechnen, sollte sich die Angabe von Fantasienamen ganz schnell von selbst erledigt haben.

(3) Löschung der Personalisierungsdateien:

Gemäß § 35 Abs. 2 Nr. 3 BDSG sind personenbezogene Daten zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist.

Jedenfalls dann, wenn feststeht, dass es bei dem betreffenden Auswärtsspiel keine besonderen, die Tätigkeit der Strafverfolgungsbehörden auslösenden bzw. dem Verein die Erteilung von Stadionverboten oder die Geltendmachung von Schadensersatzforderungen ermöglichenden Vorkommnissen gegeben hat, sind die Personalisierungsdateien zu löschen. Im Regelfall dürfte der Verein dies nach einer Woche beurteilen können.

8.7.2 Auslegen des Mitgliedsausweises im Fahrzeug als Nachweis der Parkberechtigung

In der Parkordnung eines Sportvereins waren für Vereinsmitglieder Sonderkonditionen für die Nutzung des Vereinsparkplatzes an seiner Trainings- und Wettkampfhalle festgelegt. Wenn die Mitglieder ihren Mitgliedsausweis sichtbar im Fahrzeug auslegen, konnten sie nach Betätigung der „Mitgliedertaste“ am Parkautomaten zwei Stunden kostenfrei dort parken.

Die datenschutzrechtliche Relevanz dieser Regelung bestand darin, dass auf diese Weise - die Mitgliedsausweise enthalten auf der Vorderseite den vollständigen Namen, die Abteilungszugehörigkeit und die Mitgliedsnummer des jeweiligen Mitglieds - Dritten eine Reihe personenbezogener Daten der parkenden Vereinsmitglieder bekanntgegeben worden waren. Dazu gehören beispielsweise die Informationen, welchem Vereinsmitglied welches Fahrzeug gehört, welches Vereinsmitglied mit Sicherheit gerade in der Halle anwesend ist oder auch welches Vereinsmitglied ggf. seine kostenfreie Parkzeit überschritten hat. Für die Erfüllung des Zwecks, Vereinsmitgliedern besondere Konditionen bei der Parkplatznutzung einzuräumen, waren diese Bekanntgaben jedoch nicht erforderlich, die damit verbundenen Übermittlungen folglich unzulässig.

Der Sportclub hat auf meinen diesbezüglichen Vorhalt hin eingeräumt, bei der Einführung dieser Regelung nicht bedacht zu haben, dass die Mitgliederausweise (auf der Vorderseite) die eingangs personenbezogenen Daten enthalten, die auf diese Weise Dritten praktisch offengelegt werden. Um die daraus resultierenden Persönlichkeitsrechtsbeeinträchtigungen der Vereinsmitglieder zu vermeiden, hat der Verein daher die Parkordnung dahingehend ergänzt, dass die Mitgliedsausweise mit der Rückseite zuoberst im Fahrzeug auszulegen sind. Die dort enthaltenen - ausschließlich vereinsbezogenen - Informationen sind für die Überprüfung der Parkberechtigung vollkommen ausreichend.

8.7.3 Herausgabe von Mitgliederlisten in einem Selbsthilfeverein Kranker

Im Berichtszeitraum war ich mit der Frage befasst, ob ein Vereinsmitglied einer Selbsthilfegruppe von Personen mit einem bestimmten Krankheitsbild eine Adressliste der

übrigen Vereinsmitglieder seines Vereins erhalten dürfe, um aus Anlass einer bevorstehenden Vorstandswahl ein Schreiben zur internen Willensbildung zu versenden.

Nach der Rechtsprechung des BGH kann das 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 - juris).

Wie der BGH in derselben Entscheidung (BGH a. a. O., Rdnr. 6) ausführt, ist die Frage, unter welchen Voraussetzungen ein berechtigtes Interesse des einzelnen Vereinsmitglieds anzunehmen wäre, Kenntnis von Namen und Anschriften der anderen Mitglieder zu erhalten, keiner abstrakt generellen Klärung zugänglich, sondern allein aufgrund der konkreten Umstände des Einzelfalls zu beantworten. In diesem Zusammenhang als unmittelbar vom Mitgliedschaftsrecht abgeleitetes berechtigtes Interesse anerkannt hat der BGH in dieser Entscheidung allerdings ausdrücklich den glaubhaften Wunsch nach Mitwirkung an der Willensbildung im Verein, also der satzungsmäßigen Wahrnehmung von vereinsrechtlichen Mitgliedschafts- und Teilhabrechten (BGH a. a. O.).

Einem Vereinsmitglied wäre also beispielsweise dann Zugang zur Mitgliederliste bzw. den zur Kontaktaufnahme notwendigen Daten zu gewähren, wenn es sich - wie in diesem Fall - 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“), jedoch anzunehmen. Bei einer als Verein organisierten Interessengemeinschaft von Personen mit einem bestimmten Krankheitsbild beinhaltet die Kenntnis der Mitgliedschaft zugleich die Kenntnis von einer entsprechenden Erkrankung, also eines besonderen personenbezogenen (Gesundheits-)Datums im Sinne des § 3 Abs. 9 BDSG, für dessen Verarbeitung besonders strenge Anforderungen bestehen. Angesichts dessen überwiegen im hier genannten Fall schutzwürdige Interesse der Betroffenen. Es mag aber eine (vereinsrechtliche) Verpflichtung des Vereinsvorstandes bestehen, eine Versendung im Auftrag vorzunehmen. Dies ist aber keine Frage des Datenschutzrechtes.

8.7.4 Kranzspenden: Mitteilung der Spender an die Hinterbliebenen

Hinterbliebene fordern in Traueranzeigen häufig zu sogenannten Kranzspenden auf, also zu Spenden an gemeinnützige Organisationen anstelle von Blumenschmuck als alternative Form der Beileidsbekundung.

Eine solche Einrichtung, die in meinem Beratungsfall ausgewählt worden war, weil sie sich um Erkrankte kümmert, die das Schicksal des Verstorbenen teilten, fragte an, ob sie befugt sei, den Ausrichtern der Beerdigung als Initiatoren des Spendenaufrufs die Identität der Spender und die Höhe ihrer jeweiligen Spende mitteilen zu dürfen, auch um die Zusendung von Dankesschreiben zu ermöglichen.

Ob eine Person aus dem Kreis der Trauergäste jedoch tatsächlich gespendet hat und wenn ja welche Summe, sind allerdings schutzwürdige Angaben, die einer Übermittlung entgegenstehen, denn ein diesbezügliches Geheimhaltungsinteresse überwiegt dem ansonsten berechtigten Interesse der Spendeninitiatoren, den Erfolg ihres Aufrufs personenbezogen in Erfahrung zu bringen (§ 28 Abs. 2 Nr. 2a BDSG). Die Freiwilligkeit einer Spende wäre nämlich in Frage gestellt, könnte ein Spendenaufrufer das von ihm gewünschte Wohlverhalten im Nachhinein kontrollieren.

Anders verhielte es sich allein dann, wenn die Spender vorab auf die spätere Übermittlung einer Spenderliste an den Initiator des Aufrufs ausdrücklich hingewiesen wurden und Spenden in Kenntnis dieses Umstands eingehen. Trotzdem habe ich davon abgeraten, für künftige Fälle eine Einwilligungskonstruktion zu wählen, da jedenfalls bei einer engen Sozialbeziehung der Spender zum Initiator des Aufrufs im Einzelfall gleichwohl die Freiwilligkeit der Einwilligung zweifelhaft wäre.

Der gemeinnützigen Organisation habe ich daher empfohlen, den Ausrichtern der Beerdigung die Zahl der Spender und den vereinnahmten Gesamtbetrag mitzuteilen und ihnen eine Übersendung von Dankesschreiben anzubieten, so dass die Notwendigkeit der Übermittlung der Daten entfällt.

8.8 Energieversorgungsunternehmen

8.8.1 Gesprächsaufzeichnung bei Service-Rufnummern

Ein Petent teilte mir mit, er habe an einem kalten Dezembertag die allgemeine Entstörungsrufnummer seiner Stadtwerke, eine sogenannte 0800er-Nummer, anrufen müssen, weil seine Heizungsanlage ausgefallen war.

Bevor er mit einem Mitarbeiter verbunden war, wurde ihm im Wege einer Bandansage mitgeteilt, dass sein Anruf aufgezeichnet werde. Hiermit war der Petent jedoch nicht

einverstanden und bat zu Beginn des Gesprächs darum, die Aufzeichnung manuell zu unterbinden. Sein Gesprächspartner teilte ihm jedoch mit, dass dies technisch nicht möglich sei und er als Mitarbeiter der Stadtwerke das Gespräch sofort beenden müsse, falls ein Anrufer mit der Aufzeichnung nicht einverstanden sei. Wegen der witterungsbedingten Dringlichkeit seines Anliegens und des Fehlens einer alternativen Kontaktmöglichkeit sah sich der Betroffene allerdings trotz seiner Vorbehalte veranlasst, das Gespräch auch ohne eine Beendigung der Aufzeichnung fortzusetzen. Er fragte mich jedoch hinterher, ob das Handeln der Stadtwerke datenschutzrechtlich zulässig gewesen sei. Ihm habe ich Folgendes mitgeteilt:

Datenschutzrechtlich ist die Aufzeichnung von Telefongesprächen eine Verarbeitung personenbezogener Daten, auf welche die Vorschriften des Bundesdatenschutzgesetzes wegen der in Call-Centern bzw. allgemein in der Kommunikationstechnik üblichen digitalisierten Aufzeichnung mittels einer Datenverarbeitungsanlage in der Mehrzahl der Fälle Anwendung findet (vgl. §§ 1 Abs. 2 Nr. 3, 27 Abs. 1 Satz 1 Nr. 1 BDSG).

Nach § 4 Abs. 1 BDSG ist eine solche Erhebung und Verarbeitung personenbezogener Daten allerdings nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder angeordnet oder der Betroffene eingewilligt hat. Zwar kann eine konkludente Einwilligung dann angenommen werden, wenn dem Anrufer bekannt ist, dass sein Gespräch aufgezeichnet wird, er jedoch dennoch anruft bzw. das Gespräch nach dem Hinweis auf die Speicherung und die fehlende Möglichkeit einer Aufzeichnungsunterbrechung gleichwohl fortsetzt. Sollte allerdings die Situation des Anrufers, insbesondere die Dringlichkeit seines Anliegens, dessen Entschließungsfreiheit beeinträchtigen, stünde die nach § 4a Abs. 1 Satz 1 BDSG gebotene Freiwilligkeit in Frage.

Die von dem Betroffenen geschilderte Situation, die Fortsetzung des Telefongespräches sei für ihn alternativlos gewesen, weil es eine andere adäquate Kommunikationsmöglichkeit, eine schnelle Behebung des winterlichen Fernwärmeausfalls zu erwirken, nicht gegeben habe, betrifft genau eine solche Fallkonstellation, bei der sich die Aufzeichnung nicht mehr auf eine konkludente Einwilligung stützen lässt.

Ohne die Einwilligung des Betroffenen wäre die Sprachaufzeichnung nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG allein dann gestattet, wenn dies zur Durchführung des Versorgungsvertrags erforderlich wäre. Weder die Natur des Versorgungsvertrags noch die Beseitigung einer Versorgungs- und damit zunächst einer typischen vertraglichen Leistungsstörung bedingen jedoch eine Aufzeichnung des Gesprächs, denn die zur Entstörung notwendigen Angaben können auch ohne eine Sprachaufzeichnung erhoben werden. Andernfalls wäre auch die Aufzeichnung jeder anderen Service-Hotline, bei der (Leistungs-)Störungen geltend gemacht werden können, zu gestatten (z. B. Kabelfernsehen

oder Telefonanbieter). Das (zivilrechtliche) Beweisinteresse einer Vertragspartei wird von der Vorschrift nicht erfasst.

Soweit über die Leistungsstörung hinaus wegen der Störung eine konkrete Gefahr für Leib und Leben oder andere hochrangige Rechtsgüter ausgeht und deswegen ein Erfordernis einer Aufzeichnung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG anzunehmen wäre, steht allerdings diesem (einzig schutzwürdigen) berechtigten Interesse bereits entgegen, dass es sich bei einer Störungshotline nicht um eine allgemeine Notrufnummer handelt. Diese ist allein die in § 108 Abs. 1 Satz 1 TKG genannte Nummer sowie die nach Absatz 2 Satz 1 Nr. 1 der Vorschrift durch Rechtsverordnung zusätzlich festgelegten nationalen Notrufnummern. Ihnen allein kommt der Strafrechtsschutz nach § 145 Abs. 1 Nr. 1 StGB zu. Hinter der abschließenden Regelung des § 108 TKG steht die Einschätzung, dass gerade bei einer Gefahr für Leib und Leben der Anruf bei anderen Stellen zur effektiven und koordinierten Gefahrenabwehr untauglich ist, weil sich deren Gefahrenabwehrvermögen auf die eigenen Anlagen und Möglichkeiten beschränkt, andere begleitend gebotene Maßnahmen der Gefahrenabwehr hingegen nicht selbst eingeleitet werden können bzw. dürfen.

Dass es sich bei der Störungsrufnummer eines Energieversorgers nicht um eine der Gefahrenabwehr zuzurechnende Notrufnummer handelt, ist auch daraus ersichtlich, dass ungeachtet des tatsächlichen Erreichens einer Gefährdungsschwelle im o. g. Sinne auch nach Angaben der betroffenen Stadtwerke nur 6,6 % aller Telefonate überhaupt als „sicherheitsrelevant“ klassifiziert werden. Die unterschiedslose Aufzeichnung aller eingehenden Telefonanrufe ist somit weder geeignet, noch verhältnismäßig, der Abwehr konkreter Gefahren für hochrangige Rechtsgüter zu dienen.

Wegen meiner datenschutzrechtlichen Vorbehalte haben mir die betroffenen Stadtwerke folgende Änderungen zugesagt:

- Die Mitarbeiter der Leitstelle haben künftig die Möglichkeit, die Aufzeichnung des Gesprächs auf Verlangen des Anrufers manuell zu beenden. Dazu wird die vorgeschaltete Bandansage um einen Hinweis ergänzt, dass auf Verlangen des Anrufers die Aufzeichnung abgebrochen wird.
- Sollten sich im Verlauf eines nicht mitgeschnittenen Telefongesprächs Anzeichen für strafrechtlich relevante Handlungen ergeben, wie beispielsweise die Bedrohung von Personen oder technischen Einrichtungen z. B. durch Bombendrohung oder Ähnliches, besteht für die Mitarbeiter der Leitstelle die Möglichkeit, die Gesprächsaufzeichnung zu Beweissicherungszwecken manuell zu (re)aktivieren.

- Sofern die Speicherung der Gesprächsaufzeichnung zum Zweck der Beweissicherung nicht mehr erforderlich ist, erfolgt die Löschung der Aufzeichnung nach maximal 72 Stunden.

Mit diesen Änderungen hatte ich hinsichtlich der Aufzeichnung eingehender Telefonate keine datenschutzrechtlichen Bedenken (mehr).

8.9 Handels- und Wirtschaftsauskunfteien / Inkassobüros

8.9.1 Kontrolle der Zweigstellen von Wirtschaftsauskunfteien mit Hauptsitz in anderen Bundesländern

Mit 130 Gesellschaften in ganz Deutschland ist Creditreform eine der größten Wirtschaftsauskunfteien. In Sachsen ist Creditreform dabei an fünf Standorten vertreten: Dresden, Leipzig, Görlitz, Chemnitz und Zwickau. Während die Auskunfteien in Dresden, Leipzig und Görlitz durch eigenständige Gesellschaften betrieben werden, handelt es sich bei Standorten in Chemnitz und Zwickau um Geschäftsstellen der Creditreform Hof Lippoldt & Ritter KG mit Sitz im bayerischen Hof.

Nicht zuletzt infolge der bei geschäftsmäßiger Speicherung personenbezogener Daten zum Zweck der Übermittlung generell bestehenden Meldepflicht nach § 4d Abs. 1 BDSG (vgl. Pkt. 2) befinden sich Auskunfteien im besonderen Fokus der anlassfreien Kontrolltätigkeit der Datenschutzaufsichtsbehörden. Immer dann, wenn Hauptsitz und Geschäftsstelle auseinanderfallen und sich zudem in unterschiedlichen Bundesländern befinden, stellt sich dabei die Frage der zuständigen Kontrollbehörde.

Nach dem Sitzprinzip wäre im konkreten Fall das LDA die zuständige Datenschutzaufsichtsbehörde, nach dem Territorialprinzip hingegen wäre meine Kontrollzuständigkeit gegeben. Fakt ist aber, dass die bayerischen Kollegen natürlich keine örtlichen Überprüfungen in Chemnitz oder Zwickau durchführen können und auch ich kann natürlich zentral organisierte, nichtsdestoweniger auch für die Geschäftsstellen bedeutsame Unternehmensbereiche nicht in Hof kontrollieren. Es steht insoweit außer Frage, dass ich mich bei datenschutzrechtlichen Fragen, die das Gesamtunternehmen betreffen, also beispielsweise bei der Bestellung eines Datenschutzbeauftragten oder bei der Beurteilung eines Backup-Konzepts bezüglich der zentralen IT-Landschaft zurückzuhalten und die Bewertung den Kollegen in Bayern zu überlassen habe.

Die ideale Lösung liegt wie so oft in der Mitte, d. h. in einer Arbeitsteilung. Ich kontrolliere die Bereiche, die in den Geschäftsstellen entschieden und verantwortet werden, und treffe im Übrigen bei meinen örtlichen Kontrollen allenfalls Feststellungen - die abschließende Bewertung überlasse ich dann den bayerischen Kollegen.

Ihre gesetzliche Grundlage findet diese Arbeitsteilung in § 3 Abs. 1 Nr. 2 VwVfG, wonach in Angelegenheiten, die sich auf den Betrieb eines Unternehmens oder einer seiner Betriebsstätten beziehen, die (Datenschutzaufsichts-)Behörde örtlich zuständig ist, in deren Bezirk das Unternehmen oder die Betriebsstätte betrieben wird. Als Betriebsstätte im Sinne der Vorschrift ist dabei eine organisatorisch mit einer gewissen Selbständigkeit ausgestattete, räumlich vom Hauptbetrieb getrennte Teileinheit zu betrachten (Kopp/Ramsauer, VwVfG, 9. Aufl., Rdnr. 24 zu § 3). Für die Creditreform-Geschäftsstellen trifft dies unzweifelhaft zu.

Bei der praktischen Umsetzung gab es diesbezüglich überhaupt keine Probleme - die Zusammenarbeit mit dem LDA verlief vollkommen reibungslos.

Grundsätzlich gilt dies natürlich nicht nur für die Kontrolle von Wirtschaftsauskunfteien, sondern für alle Branchen und auch nicht nur für die anlassfreie Kontrolltätigkeit, sondern vor allem auch für Anlasskontrollen. Dazu hat es inzwischen auch bereits eine - unmittelbar das Bundesdatenschutzgesetz betreffende - gerichtliche Entscheidung gegeben. Das VG Hannover hat am 6. November 2012 entschieden (Az. 10 A 4805/11), dass (für eine Auskunftsverpflichtung gegenüber der Aufsichtsbehörde - vgl. § 38 Abs. 3 BDSG) nicht der Handelsregistereintrag bzw. der dort vermerkte Unternehmenssitz für die örtliche (Kontroll-)Zuständigkeit entscheidungserheblich ist, sondern maßgeblich ist insoweit - in entsprechender Anwendung von § 3 Abs. 1 Nr. 2 VwVfG - an welchem Ort die Tätigkeiten tatsächlich stattfinden, auf die sich die in Frage stehende Verwaltungstätigkeit bezieht.

8.9.2 Trefferanzeigen nach Personensuche im Internet

Mehrere Betroffene haben sich an mich gewandt, weil sie im Rahmen einer Eigenrecherche (Personensuche) über eine Internet-Suchmaschine Treffer angezeigt bekommen hatten, die zum Webportal einer Wirtschaftsauskunftei führten. In einigen Fällen hatte der Treffer dabei auch die vollständige Anschrift des Betroffenen enthalten.

Dies stellte eine unzulässige Übermittlung personenbezogener Daten dar.

Gemäß § 29 Abs. 2 Satz 1 BDSG ist die Übermittlung personenbezogener Daten zulässig, wenn der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat.

Ein berechtigtes Abfrageinteresse Betroffener konnte allenfalls dann angenommen werden, wenn ein Interessent unmittelbar auf dem betreffenden Portal nach einer Person gesucht hätte, um festzustellen, ob über diese Wirtschaftsauskunftei ggf. eine Bonitäts-

auskunft erhältlich ist. Anfragen bei Suchmaschinen verfolgen hingegen das Ziel, alle bzw. möglichst viele Internetveröffentlichungen aufgelistet zu bekommen, die auch den Namen des Betroffenen enthalten bzw. direkt ihn betreffen. Dies ist beim Webportal einer Wirtschaftsauskunftei aber nicht der Fall. Die diesbezüglichen Internetseiten enthalten selbst keine Angaben zu den Betroffenen, sondern bieten nur eine Zugangsmöglichkeit zu weiteren, nicht allgemein zugänglichen Datenbanken. Ein berechtigtes Interesse der die jeweilige Suche auslösenden Internetnutzer ist damit nicht erkennbar. Zudem stehen der in der Bekanntgabe des Suchergebnisses zu sehenden Datenübermittlung auch schutzwürdige Betroffeneninteressen gegenüber. Die Tatsache, dass über sie weitere Informationen in nicht öffentlich zugänglichen Datenbanken verfügbar sind, lässt gerade den unbedarften, wegen einer allgemeinen Personenanfrage über eine Suchmaschine eben nicht an einer Bonitätsauskunft interessierten und daher mit den diesbezüglichen Regularien auch nicht vertrauten, Internetnutzer vermuten, dass der Betroffene finanzielle Probleme haben könnte, die andere dazu veranlassen, dessen finanziellen Verhältnisse besonders aufmerksam zu prüfen und zu beobachten. Dies wurde im konkreten Fall noch dadurch verstärkt, dass der Portalbetreiber nicht nur Wirtschaftsauskünfte vertrieb, sondern darüber hinaus auch Inkassodienstleistungen angeboten hatte. Dass im Übrigen die Bekanntgabe der vollständigen, den Betroffenen somit eindeutig identifizierenden, Anschrift dessen schutzwürdigen Interessen verletzt hatte, bedarf an dieser Stelle sicher keiner weiteren Erläuterung.

Ich habe den Portalbetreiber daher aufgefordert, geeignete Maßnahmen zu treffen, dass Suchanfragen zu konkreten Personen in externen Suchmaschinen nicht mehr zu Treffern führen, aus denen sich ergibt, dass zu den gesuchten Personen Bonitätsauskünfte über sein Webportal bezogen werden können.

8.9.3 Online-Registrierungsprozess bei einer Wirtschaftsauskunftei

Eine Wirtschaftsauskunftei hatte seinen registrierten (Internet-)Kunden die Möglichkeit eröffnet, zunächst kostenlos zu ermitteln, ob zu dem interessierenden Unternehmen überhaupt Informationen vorhanden sind. Über eine Ähnlichkeitssuche - nicht immer ist der vollständige und exakte Name eines Unternehmens bekannt - wurde dann zunächst eine Liste (Name, Anschrift) mit allen infrage kommenden Unternehmen erstellt und als Ergebnis angezeigt. Klar ist, dass bereits mit diesen Trefferanzeigen auch personenbezogene Daten übermittelt worden sind. Im nächsten Schritt konnte dann zu dem ausgewählten Unternehmen eine kostenpflichtige Bonitätsauskunft angefordert werden.

Dies alles stellte für sich genommen noch kein Problem dar. Ich bin dann aber darauf hingewiesen worden, dass das für die Online-Registrierung angewandte Verfahren keine sichere Identifikation garantierte und stattdessen missbräuchliche Registrierungen ohne

weiteres ermöglichte. Die im Rahmen der Registrierung anzugebenden Nutzerdaten waren frei wählbar und wurden - abgesehen von einer Plausibilitätsprüfung hinsichtlich der Übereinstimmung von Postleitzahl und Ort - in keiner Weise überprüft. Dies hatte zur Folge, dass sich Nutzer mit beliebigen Phantasiedaten an diesem Webportal anmelden und anschließend zumindest die o. g. Suchanfragen starten konnten. Darüber hinaus wurde durch die fehlende Authentifizierung aber auch Bonitätsabfragen unter falscher Identität Vorschub geleistet. Voraussetzung für die Online-Erteilung der Auskünfte war lediglich der entsprechende Zahlungseingang (Vorkasse) oder die Angabe einer (ggf. fremden) Kreditkartennummer. In beiden Fällen, d. h. bereits bei bloßer Nutzung der Suchfunktion, aber auch bei einer Bonitätsabfrage unter falscher Identität, hätte dies in der Folge zu einer unzulässigen und damit rechtswidrigen Übermittlung (an unbekannte Empfänger) geführt, zudem hätte die Wirtschaftsauskunftei in diesen Fällen auch nicht ihrer Verpflichtung zur stichprobenhaften Überprüfung des berechtigten Interesses nachkommen können, denn dazu bedarf es nun mal der Kenntnis der Identität des Auskunftsempfängers.

Ich habe die Auskunftei daher aufgefordert, durch geeignete technische Maßnahmen im Rahmen der Zugangs- und Weitergabekontrolle (vgl. Nrn. 2 und 4 der Anlage zu § 9 BDSG) eine missbräuchliche Nutzung ihres Webportals durch Unbefugte auszuschließen und darüber hinaus in ausreichender Weise sicherzustellen, dass sie ihrer Pflicht zur stichprobenhaften Überprüfung des berechtigten Interesses auch tatsächlich nachkommen kann, indem sie für eine sichere Identifikation ihrer Nutzer sorgt. Diesbezügliche Möglichkeiten bestehen beispielsweise im Abschluss einer schriftlichen und per Post übersandten Online-Nutzervereinbarung, wie es nach meiner Kenntnis auch andere, bundesweit aktive Wirtschaftsauskunfteien praktizieren.

8.9.4 Veröffentlichung von Insolvenzdaten

Ein Inkassounternehmen hatte Insolvenz-Meldungen auf seiner Webseite veröffentlicht. Dagegen beschwerten sich zu Recht mehrere Betroffene. Diese Veröffentlichung stellte eine unbefugte Übermittlung personenbezogener Daten dar und war damit rechtswidrig erfolgt.

Für die Bewertung der Zulässigkeit der erfolgten Veröffentlichung (Übermittlung an einen unbestimmten Empfängerkreis) einschlägig waren die Regelungen des § 29 BDSG.

Die Zulässigkeit der Datenverarbeitung durch Inkassounternehmen bestimmt sich vom Grundsatz her zwar nach § 28 BDSG, im Speziellen nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG, jedoch gilt das nur dann, wenn das Inkassounternehmen personenbezogene Daten für eigene Geschäftszwecke, also im Rahmen eigener Inkasso-Verfahren verarbeitet.

Im vorliegenden Fall ging es jedoch um eine Übermittlung personenbezogener Daten aus gerichtlichen Bekanntmachungen zu Insolvenzverfahren. Diese, nur im Ausnahmefall eigene Verfahren betreffenden Daten waren über das Internet veröffentlicht und einer Vielzahl von Empfängern übermittelt worden. Geschäftszweck war daher nicht mehr die Durchführung eigener Inkasso-Verfahren, sondern die Übermittlung bzw. Veröffentlichung der Daten, mithin also keine Datenverarbeitung für eigene Zwecke, sondern eine geschäftsmäßige Datenerhebung und -speicherung zum Zwecke der Übermittlung (also für fremde Zwecke). Einschlägig war damit § 29 BDSG.

Gemäß § 29 Abs. 1 Nr. 2 BDSG ist das geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen personenbezogener Daten zum Zwecke der Übermittlung zulässig, wenn die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt.

Insolvenzdaten werden nach § 9 Abs. 1 InsO auf der Internetseite www.insolvenzbekanntmachungen.de im Internet amtlich bekannt gegeben. Die Einzelheiten dieser amtlichen Veröffentlichung sind nach § 9 Abs. 2 InsO durch die Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet vom 12. Februar 2002 geregelt. Gemäß § 2 Abs. 1 Nr. 3 InsoBekV sind Insolvenzdaten nur innerhalb der ersten zwei Wochen der öffentlichen Bekanntmachung ungehindert für jedermann abrufbar und insoweit allgemein zugänglich.

Vor diesem Hintergrund bestanden gegen die Zulässigkeit der Erhebung, Speicherung und ggf. auch Nutzung der Insolvenzdaten zunächst keine Bedenken (§ 29 Abs. 1 Satz 1 Nr. 2 BDSG); das Internet ist eine allgemein zugängliche Quelle.

Anders sah es aber hinsichtlich der weiteren Veröffentlichung dieser Daten aus. Eine Übermittlung darf nach § 29 Abs. 2 Satz 1 BDSG nur erfolgen, wenn der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Nach Beendigung der amtlichen Veröffentlichung, mithin also nach zwei Wochen, besteht aber Grund zu der Annahme, dass die Betroffenen ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung haben. Die in der Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet genannten Bedingungen sind auch durch private Anbieter bei Veröffentlichungen von Insolvenzdaten im Internet entsprechend einzuhalten, da andernfalls die für amtliche Insolvenzbekanntmachungen

getroffenen Regelungen unterlaufen würden. Die Veröffentlichung von Insolvenzdaten im Internet hat zudem wohl unbestritten auch die Wirkung eines Prangers, was dazu führt, dass einer Veröffentlichung entgegenstehende schutzwürdige Betroffeneninteressen überwiegen. Lediglich für den Zeitraum der amtlichen Veröffentlichung der Insolvenzdaten kann unterstellt werden, dass Betroffene jedenfalls kein schutzwürdiges Interesse am Ausschluss der Übermittlung haben. Werden also Insolvenzdaten durch private Anbieter über den in der Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet vorgesehenen Zeitraum hinaus veröffentlicht bzw. übermittelt, liegt ein Verstoß gegen § 29 Abs. 2 Satz 1 BDSG vor.

In dem durch mich zu bewertenden Fall kam hinzu, dass die Insolvenzdaten über Suchmaschinen recherchierbar waren. Dies bedeutet, dass Internetnutzer ohne gezielte Suche nur durch Eingabe von Vorname und Name eines Betroffenen auf die Veröffentlichung der Insolvenzdaten auf dem betreffenden Portal gestoßen sind. § 29 Abs. 2 Satz 1 Nr. 1 BDSG fordert jedoch, dass der Abrufende sein berechtigtes Interesse an der Kenntnis der Daten glaubhaft darlegen und - da es sich um ein automatisiertes Abrufverfahren handelt - auch dokumentieren bzw. aufzeichnen muss. Internetnutzer, die aber nur allgemein mittels Suchmaschinen unter Angabe von Vorname und Name im Internet recherchieren, haben (im Regelfall) weder ein berechtigtes Interesse an der Kenntnis der Insolvenzdaten, noch können Suchmaschinen dieses Interesse gegenüber der verantwortlichen Stelle nachweisen. Würden die Insolvenzdaten stattdessen in einer Weise zur Übermittlung bereitgehalten, dass sie von Suchmaschinen nicht recherchiert werden können, reduzierten sich die potentiellen Übermittlungen auf den Personenkreis, der die jeweilige Website gezielt aufruft. Da das Inkasso-Unternehmen keine Maßnahmen gegen den Zugriff durch Suchmaschinen getroffen hatte, war die Übermittlung bzw. Veröffentlichung in diesem Fall also von Anfang an rechtswidrig.

8.9.5 Datenübermittlung an Inkassounternehmen bei bestrittener Forderung

Die Bevollmächtigte einer Petentin bat mich aufsichtlich gegen ein Unternehmen tätig zu werden, das die Daten ihrer Mandantin an einen Inkassodienstleister weitergegeben hatte, obwohl der geltend gemachten Forderung ausdrücklich widersprochen wurde.

Die datenschutzrechtlichen Vorbehalte der Anwältin habe ich allerdings nicht teilen können, denn die Inanspruchnahme eines registrierten Inkassounternehmens zur Einziehung einer Forderung ist eine nach dem Rechtsdienstleistungsgesetz allgemein zulässige außergerichtliche Rechtsdienstleistung (§§ 2 Abs. 2, 10 Abs. 1 Satz 1 Nr. 1 RDG). § 28 Abs. 1 Satz 1 Nr. 2 BDSG erlaubt deshalb auch schon die Übermittlung der Daten eines nur vermeintlichen Schuldners. Denn schon das Behaupten bzw. Geltendmachen einer Forderung mittels eines Rechtsdienstleisters begründet, sofern es nicht völlig willkür-

lich oder gar arglistig geschieht, ein berechtigtes (rechtliches) Interesse an einer (zunächst außergerichtlichen) Klärung des Schuldverhältnisses, das dem Interesse auch des nur vermeintlichen Schuldners an einem Ausschluss der Übermittlung vorgeht, da dieser sich der Forderung rechtlich erwehren und eine abschließende Klärung des zivilrechtlichen Anspruchs ohnehin nur gerichtlich herbeigeführt werden kann, mit der Folge, dass eine außerhalb des Datenschutzrechtes liegende rechtliche Vorfrage in Rede steht, die von der Aufsichtsbehörde nicht mit Wirkung für die Parteien zu beantworten ist (so im Ergebnis auch Abel gestützt auf eine Entscheidung des AG Kiel, II 39 OWi 20/11, Datenschutzberater 10/2011, S. 8 f.).

Wie zudem aus der Alleinstellung des § 28a Abs. 1 BDSG folgt, der nur Auskunfteien betrifft, ist es die bewusste und einleuchtende, ja zwingend richtige Entscheidung des Gesetzgebers, bestrittene Forderungen nicht schlechthin von einer Übermittlungsbefugnis auszunehmen, sondern nur dann, wenn wegen einer Übermittlung an eine Auskunftei das besondere Risiko besteht, wegen unberechtigter Forderungen in der Bonität Dritten gegenüber herabgewürdigt zu werden.

8.10 Versicherungen

8.10.1 Einmeldungen in das Hinweis- und Informationssystem der Versicherungswirtschaft

Versicherungsgesellschaften melden an ein zentrales Hinweis- und Informationssystem (HIS), das von einer nicht meiner Aufsicht unterstehenden Firma im Auftrag der Versicherungswirtschaft als Warndatei betrieben wird, zur Person ihrer Versicherten besondere Auffälligkeiten aus Versicherungsfällen, wie atypische Schadenshäufigkeiten, besondere Schadenfolgen oder erschwerte Risiken.

Eine Betroffene fühlte sich dort von einem in Sachsen ansässigen Versicherer, der ihren Schaden nicht reguliert hatte, zu Unrecht eingemeldet, insbesondere weil sie der Weitergabe ihrer Daten ausdrücklich widersprochen hatte. Ihr habe ich hierauf allerdings mitgeteilt, dass solche Informationen auf Grundlage von § 28 Abs. 2 Nr. 2a BDSG gleichwohl übermittelt werden dürfen und der Betrieb einer Warndatei, also die geschäftsmäßige Erhebung und Speicherung zum Zweck der Übermittlung, nach § 29 BDSG zulässig ist.

Einer Einwilligung der Betroffenen bedarf es nach diesen Vorschriften nicht, da das System der Wahrung berechtigter Interessen der Versicherungsunternehmen bei der Risikoeinschätzung künftiger Versicherungswagnisse dient und schutzwürdige Interessen der Betroffenen dem gegenüber nicht überwiegen - dieses ist die gemeinsame Auffassung aller in der Arbeitsgemeinschaft Versicherungswirtschaft vertretenen Daten-

schutzaufsichtsbehörden. Demgemäß habe ich die Betroffene darauf aufmerksam gemacht, dass sie lediglich einen Anspruch auf Löschung oder Berichtigung ihrer Daten durch das einmeldende Versicherungsunternehmen hat, wenn kein Anlass zu der erfolgten Meldung bestanden hat bzw. dieser nachträglich entfallen ist.

Nicht selten sind allerdings das Vorliegen eines Versicherungsschadens sowie dessen Umfang, Gründe oder etwaige Verantwortlichkeiten bzw. Einstandspflichten im Streit begriffen. Diese zivilrechtlichen Vorfragen, die für die Befugnis zur Datenverarbeitung von Bedeutung sind, können (und dürfen) allerdings von meiner Behörde in der Regel nicht aufgeklärt werden, so dass ich die Betroffenen bei einem solchen Sachverhalt auf den Zivilrechtsweg verweisen muss, es sei denn, sie tragen Tatsachen vor, die nach jeder in Betracht kommenden Sicht eindeutig die Befugnis zur Einmeldung oder die weitere Speicherung der Daten hindern, z. B. durch die Angabe, dass sie nicht Vertragspartner des Unternehmens sind, ihre Identität verwechselt wurde oder über den Sachverhalt eine gerichtliche Entscheidung (rechtskräftig) ergangen ist.

8.10.2 Datenschutzrechtliche Einwilligungen mittels digitaler Unterschriftenpads

Eine Unternehmens-Gruppe der Versicherungsbranche mit mehreren Geschäftszweigen fragte bei meiner Behörde an, ob es Versicherern und deren Maklern gestattet sei, datenschutzrechtliche Einwilligungen allein mittels digitaler Unterschrift auf einem Unterschriftenpad, auch Signaturpad oder Schreibtablet genannt, einzuholen.

Dem Unternehmen habe ich mitgeteilt, dass nach § 4a Abs. 1 Satz 3 BDSG datenschutzrechtliche Einwilligungen regelmäßig der Schriftform bedürfen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Solche Umstände liegen aber nicht vor, wenn bei einem Vertreterbesuch der Erklärende und der Erklärungsempfänger bzw. dessen Bevollmächtigter sich einander physisch gegenübersitzen, also problemlos „in klassischer Weise“ schriftlich kontrahieren können. Demgemäß sind hinsichtlich der Abgabe der Signatur, wie für alle Schriftformerfordernisse des Privatrechts, die Vorgaben der §§ 126, 126a BGB zu beachten. Diese lassen aber eine elektronische Unterschriftsleistung nicht zu, da die Unterschrift nicht in der gesetzlich gebotenen Weise dauerhaft und eigenhändig verkörpert ist, sondern ausschließlich als virtuelles Abbild gespeichert wird (vgl. OLG München, Urteil vom 4. Juni 2012 - 19 U 771/12 - juris).

Ich habe der Unternehmensgruppe daher mitgeteilt, dass sich eine meiner Aufsicht unterfallende Stelle nicht auf eine allein elektronisch verkörperte Unterschrift als Nachweis einer datenschutzrechtlichen Einwilligung berufen kann. Verfährt sie anders, läuft sie Gefahr, aufsichtliche und bußrechtliche Konsequenzen befürchten zu müssen.

Mit meiner rechtlichen Bewertung war das Unternehmen allerdings nicht einverstanden, offenbar auch deshalb, weil Unterschriftenpads von Konkurrenten bereits eingesetzt würden und deshalb (vermeintlich) Wettbewerbsnachteile drohten. Die Unternehmensgruppe wandte sich daher an für sie unzuständige Aufsichtsbehörden des Bundes und der Länder, erhielt jedoch keine andere Rechtsauskunft bzw. die Mitteilung, dass meine Behörde gemäß den Gesetzen des Föderalismus innerhalb ihrer Zuständigkeit ihre Aufsicht autonom ausüben könne. Insbesondere musste die Unternehmensgruppe erkennen, dass der Sächsische Datenschutzbeauftragte wegen der entsprechenden Vorgabe in Art. 28 Abs. 1 Satz 2 der EU-Datenschutz-Richtlinie seine Aufsicht in völliger Unabhängigkeit wahrnimmt, also weder vom Bundesbeauftragten für den Datenschutz, noch anderen Stellen zu einer anderen Rechtsauffassung verpflichtet werden kann. Dessen ungeachtet steht gegen förmliche Entscheidungen meiner Behörde selbstverständlich jedem der Rechtsweg offen.

Hinsichtlich der aufgeworfenen Problematik zum Einsatz digitaler Unterschriftenpads ist mir bisher keine andere Aufsichtsbehörde bekannt, die einen abweichenden Rechtsstandpunkt einnimmt.

8.11 Mietverhältnisse

8.11.1 Übermittlung von Mieterdaten an die ARGE

Eine Hausverwaltung hatte die ARGE unaufgefordert über die veränderte Mietzahlung (Mietminderung) eines Mieters unterrichtet. Der betreffende Mieter hatte dies zufälligerweise bei einem Termin in der ARGE erfahren. Über den Leistungsbezug als solchen war die Hausverwaltung dadurch informiert gewesen, dass der Mieter vorher regelmäßig eine Mietbescheinigung mit der Bitte um Bestätigung vorgelegt hatte.

Die Hausverwaltung war der Auffassung, dass es sich bei diesem Schreiben um nichts anderes als eine erweiterte Mietbescheinigung gehandelt habe. Es seien also nur Daten weitergegeben worden, die der Leistungsträger wissen müsse, um Überzahlungen zu vermeiden. Mit der Information der ARGE habe die Hausverwaltung einerseits vermeiden wollen, dass der Verdacht der Deckung einer Straftat auf sie fällt, andererseits sollte auf diese Weise die missbräuchliche Verwendung von Steuergeldern verhindert werden.

Ich habe diese Datenübermittlung als unzulässig bewertet.

Da die Hausverwaltung mit dem Schreiben an das Arbeitsamt keine eigenen Geschäftsinteressen verfolgt hatte, sondern dieses ausschließlich dazu dienen sollte, den Leistungsträger über die veränderte Mietzahlung des Mieters zu unterrichten, kommt als

Zulässigkeitstatbestand für die damit verbundene Übermittlung personenbezogener Daten einzig § 28 Abs. 2 Nr. 2a BDSG in Betracht.

Zulässig ist eine Übermittlung nach dieser Vorschrift dann, wenn sie zur Wahrung berechtigter Interessen eines Dritten, hier der ARGE, erforderlich ist und kein Grund zu der Annahme besteht, dass der Mieter ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. Eine Verpflichtung zur Datenübermittlung ist aus dieser Vorschrift in keinem Fall abzuleiten.

Ob die Übermittlung zur Wahrung berechtigter Interessen der ARGE erforderlich gewesen sein könnte, hat die Hausverwaltung in diesem Fall aber gar nicht beurteilen können. Denn ihr hat weder ein entsprechendes Verlangen der ARGE vorgelegen, noch hatte sie tatsächliche Anhaltspunkte für einen Leistungsmissbrauch des betreffenden Mieters. Grundsätzlich gilt im Datenschutzrecht das Direkterhebungsprinzip, d. h. die verantwortliche Stelle hat personenbezogene Daten zuerst beim Betroffenen selbst zu erheben und nur dann, wenn dies nicht möglich ist oder wenn Ansatzpunkte dafür bestehen, dass Betroffene unwahre Angaben gemacht haben oder ihren Mitteilungspflichten nicht nachgekommen sind, dürfen personenbezogene Daten davon abweichend auch bei Dritten erhoben werden. In diesem Fall hätte sich die ARGE dann aber zunächst an die Hausverwaltung mit einer entsprechenden Nachfrage wenden müssen. Allein aus der Tatsache, dass auch Mietminderungen für die Höhe des Leistungsbezugs von Bedeutung sind, und der demnach bloßen, durch nichts hinterlegten, Vermutung, dass der Mieter dies nicht bereits selbst der ARGE mitgeteilt hatte, konnte die Hausverwaltung für sich noch keine Übermittlungsbefugnis ableiten, insbesondere gibt es auch keine diesbezüglichen Mitteilungspflichten für Vermieter oder Hausverwaltungen. Es ist nicht die Aufgabe von Vermietern oder Hausverwaltungen, Leistungsmissbrauch im Sozialbereich zu bekämpfen. Wenn dies vom Gesetzgeber beabsichtigt gewesen wäre, hätte er eine entsprechende Übermittlungsvorschrift geschaffen. Solange demnach keine Anhaltspunkte für einen Leistungsmissbrauch, insbesondere auch keine konkrete Anfrage des Leistungsträgers vorliegt, ist eine Unterrichtung des zuständigen Sozialleistungsträgers damit schon mangels Erforderlichkeit unzulässig.

Im Weiteren verletzt gerade auch die heimlich, d. h. ohne Wissen des Betroffenen, vorgenommene Datenübermittlung an die ARGE auch dessen schutzwürdige Interessen. Einerseits unterstellt ihm diese Datenübermittlung unredliches Handeln, d. h. die unterlassene eigene Mitteilung an den Leistungsträger, andererseits schränkt das ihm nicht bekannte Wissen des Leistungsträgers seine tatsächlichen Handlungsmöglichkeiten entsprechend ein bzw. zwingt ihn ggf. auch zu Handlungen oder Rechtfertigungen, die andernfalls nicht notwendig gewesen wären.

Hinzu kommt, dass die ohne Wissen des Betroffenen vorgenommene Unterrichtung der ARGE dem Transparenzprinzip des Datenschutzrechts zuwiderläuft. Aus § 4 Abs. 3 BDSG ergibt sich für die Hausverwaltung die allgemeine Pflicht zur Unterrichtung des Betroffenen über mögliche Datenempfänger - dies gilt namentlich dann, wenn wie hier der Betroffene nach den Umständen des Einzelfalls nicht mit einer Übermittlung an diese rechnen muss.

8.11.2 Wechselseitige Bekanntgabe individueller Verbräuche bei Gemeinschaftseigentum

Ein Mitglied einer Wohnungseigentümergemeinschaft störte sich daran, dass die Hausverwaltung allen Miteigentümern eine Aufstellung der Jahresheizwerte zusandte, aus der die Verbräuche der einzelnen Wohnungen hervorging, verbunden mit einer Farbkennzeichnung, die darauf aufmerksam machen sollte, dass bestimmte Verbrauchsstände das Risiko von Schimmel und Bauschäden förderten.

Datenschutzrechtliche Bedenken gegen das Handeln der Wohnungsverwaltung hatte ich jedoch nicht. Nach § 28 Abs. 3 WEG haben die Mitglieder einer Wohnungseigentümergemeinschaft gegen ihren Verwalter einen Anspruch auf jährliche Abrechnung. Um die Richtigkeit der Abrechnung, mithin die Tätigkeit der Hausverwaltung, wirksam überprüfen zu können, ist es erforderlich, dass alle von der Verbrauchsrechnung betroffenen Wohnungseigentümer Einsicht in alle die gemeinsame Wohnanlage betreffenden Abrechnungsunterlagen nehmen können, also auch in solche, die den anteiligen Wärmeverbrauch ausweisen. Die entsprechende Verpflichtung des Verwalters, Einsicht in die genannten Unterlagen zu gewähren, ergibt sich aus § 28 Abs. 3 WEG, §§ 675, 666 BGB i. V. m. § 259 BGB und dem Verwaltervertrag.

Mit dem Anspruch auf Einsicht korrespondiert der Anspruch auf Übersendung, also Übermittlung dieser Daten, wenn Beschlüsse der Wohnungseigentümergemeinschaft oder die ordnungsgemäße Verwaltung des Gemeinschaftseigentums dies bedingen (§ 27 Abs. 1 WEG). Dem steht auch das Bundesdatenschutzgesetz nicht entgegen, da die Wohnungseigentümergemeinschaft keine anonyme Gemeinschaft ist und die Einsichtnahme bzw. Informationsverschaffung dem Zweck des Gemeinschaftsverhältnisses dient, § 28 Abs. 1 Satz 1 Nr. 1 BDSG (vgl. hierzu OLG München, Beschluss vom 9. März 2007, Az. 32 Wx 177/06, Rdnr. 9 - juris).

Die Befugnis, auch die jeweilige Schimmel- und Baukörpergefährdung der Wohnungen den übrigen Wohnungseigentümern übermitteln zu dürfen, folgt aus der Obliegenheit des Verwalters aus § 27 Abs. 1 Nr. 2 bzw. 3 WEG, Vorsorgemaßnahmen zum Erhalt

des gemeinschaftlichen Eigentums zu treffen, auch durch präventive Mitteilungen zur baulichen Gefährdung des Objekts.

Eine Erforderlichkeit im Sinne dieser Vorschrift und damit eine Übermittlungsbefugnis nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG besteht allerdings nur, wenn sich die Einschätzung des Verwalters, bestimmte Wohnungen seien anfällig für Schimmel und eventuelle Bauschäden, auf einen diesbezüglich hinreichend baufachlich gesicherten Erkenntnisstand gründet, also nicht willkürlich ist. Andernfalls wäre die Übermittlung dieses Datums wegen seines rein spekulativen Gehalts und damit fehlenden tatsächlichen Erfordernisses nicht von der Übermittlungsbefugnis erfasst. Dem war hier jedoch nicht so.

8.12 Schulen / Kindertagesstätten

8.12.1 Offene Verhaltensbewertung in einer Privatschule

Die Mutter eines Schülers einer privaten Grundschule wandte sich an meine Behörde, weil sie es als datenschutzrechtlich unzulässig empfand, dass auf einer Tafel im Klassenraum zur Person ihres Kindes eine Bewertung seines Sozialverhaltens (Punktsystem) öffentlich aushing und so von jedem Mitschüler sowie allen Besuchern des Raumes (andere Eltern, Großeltern und Dritte) eingesehen werden konnte.

Nach § 2 Abs. 2 Satz 1 des Gesetzes über Schulen in freier Trägerschaft können private (Grund-)Schulen ihre Lehr- und Unterrichtsmethoden allerdings weitgehend frei gestalten; dies unterscheidet sie grundlegend von staatlichen Schulen. Die datenschutzrechtliche Verarbeitungsbefugnis einer Privatschule korrespondiert mit ihrer pädagogischen Freiheit, Verarbeitungsbeschränkungen staatlicher Schulen können also nur bedingt zum Vergleich herangezogen werden. § 28 Abs. 1 Satz 1 Nr. 1 BDSG gestattet einer genehmigten Privatschule eine Datenverarbeitung zu pädagogischen und organisatorischen Zwecken somit immer dann, wenn diese nach anerkannten (nicht unbedingt herrschenden) pädagogischen Auffassungen zur Erfüllung des eigenen Bildungsauftrags bzw. -konzepts erforderlich ist.

Da pädagogische Gründe, über die ich nicht zu befinden habe, jedenfalls im Grundsatz dafür sprechen können, das Betragen eines Schülers anderen Schülern (oder im schulischen Umfeld nicht gänzlich fremden Personen - z. B. Verwandten im Klassenraum) mitzuteilen, um durch eine (teilweise) öffentliche Belobigung oder Missbilligung Einfluss auf das Sozialverhalten des Schülers zu nehmen, halte ich eine damit verbundene Übermittlung personenbezogener Daten rechtlich für vertretbar, zumal mit der elterlichen Entscheidung über den Besuch einer Privatschule auch deren pädagogisches Konzept (so) akzeptiert wird. Dieses habe ich der betroffenen Mutter entsprechend mitgeteilt.

8.12.2 Bekanntgabe des Auftretens ansteckender Krankheiten

Die Mutter eines Kindes, das in einer Kindertagesstätte in freier Trägerschaft betreut wurde, wandte sich mit der Frage an mich, ob bei der Bekanntgabe des Auftretens ansteckender Krankheiten in der Kindertageseinrichtung die Gruppe mit angegeben werden dürfe bzw. müsse. Sie war der Auffassung, dass hierin ein Verstoß gegen datenschutzrechtliche Bestimmungen zu sehen sei, da im Falle des Fehlens nur eines Kindes der betreffenden Gruppe Rückschlüsse auf das erkrankte Kind möglich seien.

§ 34 Abs. 8 IfSG regelt, dass das Gesundheitsamt gegenüber der Leitung einer Gemeinschaftseinrichtung anordnen kann, dass das Auftreten einer Erkrankung oder eines hierauf gerichteten Verdachts ohne Hinweis auf die Person in der Gemeinschaftseinrichtung bekannt gegeben wird. Mit der Regelung soll der Schutz ungeimpfter Kinder sichergestellt werden.

Ich habe die Auffassung vertreten, dass es ausreichend ist, das Auftreten der Erkrankung oder eines Verdachts hierauf einrichtungsbezogen bekannt zu geben. Zwar weist ein „gruppenbezogener“ Aushang ebenso wie ein „einrichtungsbezogener“ noch keinen Personenbezug auf, jedoch kann ein solcher aufgrund der kleineren Vergleichsgruppe wesentlich eher hergestellt werden. Grundsätzlich besteht aber auch im Falle der einrichtungsbezogenen Bekanntgabe von Erkrankungen die Möglichkeit der Herstellung eines Personenbezugs, nämlich dann, wenn in der gesamten Einrichtung nur eine Person fehlt.

Die einrichtungsbezogene Bekanntgabe des Auftretens bestimmter Erkrankungen ist das mildeste Mittel zum Schutz ungeimpfter Kinder sowie zur Verhinderung des Ausbreitens dieser Erkrankungen. Sie ist zur Erreichung der vorgenannten Zwecke geeignet und erforderlich und stellt gleichzeitig den geringstmöglichen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Für diese Auffassung spricht zudem auch der Wortlaut des § 34 Abs. 8 IfSG, dessen Bezugsobjekt jeweils die Gemeinschaftseinrichtung ist.

8.12.3 Gewährung von Geschwisterermäßigungen

Eine Mutter, deren Kinder verschiedene Kindertageseinrichtungen besuchten, wandte sich mit folgender Eingabe an mich:

Für den Besuch der Kindertagesstätte eines freien Trägers hatte sie für ihr Kind eine so genannte Geschwisterermäßigung in Anspruch genommen. Als das andere Kind keine Kindertagesstätte mehr besuchte und somit die Voraussetzungen für die Inanspruchnahme der Geschwisterermäßigung weggefallen waren, hatte sie dies - obgleich sie

hierzu verpflichtet war - dem freien Träger nicht mitgeteilt. Durch Rückfrage bei der die andere Kindertageseinrichtung betreibenden Gemeinde hatte der freie Träger diese Tatsache aber in Erfahrung gebracht und ihr folglich die Ermäßigung gestrichen. Die Mutter sah in der Rückfrage eine Verletzung datenschutzrechtlicher Vorschriften.

Eine solche Verletzung datenschutzrechtlicher Vorschriften lag aber nicht vor.

Der die Kindertagesstätte betreibende freie Träger der Jugendhilfe ist gemäß § 15 Abs. 1 Satz 3 Nr. 2 SächsKitaG verpflichtet, für Eltern mit mehreren Kindern, die gleichzeitig eine Kindertageseinrichtung besuchen, Absenkungen der Elternbeiträge vorzusehen. Diese Absenkungsbeträge sind dem Träger der Einrichtung vom örtlichen Träger der öffentlichen Jugendhilfe gemäß § 16 Abs. 5 SächsKitaG zu erstatten. Hierfür muss der Träger der Kindertageseinrichtung einen Antrag stellen. Im Rahmen dessen ist anzugeben, welches Geschwisterkind welche andere Einrichtung besucht. Sollte sich später herausstellen, dass die Voraussetzungen nicht vorlagen, ist eine Rückforderung möglich.

Ich habe im Hinblick darauf, dass der Träger der Kindertageseinrichtung im Rahmen des Erstattungsverfahrens korrekte Angaben machen muss und der Träger sich bei Unrichtigkeit seiner Angaben verzinslichen Rückforderungsansprüchen ausgesetzt sieht, die Rückfrage für zulässig gehalten. Im vorliegenden Fall war die in der Rückfrage zu sehende Datenerhebung gemäß § 28 Abs. 1 Nr. 2 BDSG zulässig, da sie zur Wahrung berechtigter Interessen der verantwortlichen Stelle (hier: Vermeidung von Falschangaben im Erstattungsantrag und Vermeidung verzinslicher Rückforderungsansprüche) erforderlich war und zudem kein Grund zu der Annahme bestand, dass schutzwürdige Interessen der betroffenen Mutter am Ausschluss der Verarbeitung überwiegen würden. Letzteres war insbesondere deshalb der Fall, weil die betroffene Mutter ohnehin zur Preisgabe der Daten verpflichtet und dieser Verpflichtung bereits über mehrere Monate nicht nachgekommen war.

8.13 Betrieblicher Datenschutzbeauftragter

8.13.1 Immer wieder Fragen zur Bestellungspflicht

Unverändert erhalte ich Anfragen zur Notwendigkeit der Bestellung eines Datenschutzbeauftragten, weil verantwortlichen Stellen die diesbezüglichen Voraussetzungen nicht klar sind.

Gemäß § 4f Abs. 1 Sätze 1 und 4 BDSG haben nicht-öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten und hierfür in der Regel mehr als neun Personen ständig beschäftigen, einen betrieblichen Datenschutzbeauftragten zu bestellen.

Unter automatisierter Verarbeitung ist dabei die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen zu verstehen (§ 3 Abs. 2 Satz 1 BDSG). Auf den Anteil der dafür aufgewendeten Arbeitszeit kommt es nicht an (vgl. Simitis, BDSG, 6. Aufl., Rdnr. 23 zu § 4f; Scheja in Taeger/Gabel, Kommentar zum BDSG, Rdnr. 21 zu § 4f).

Bei Mitarbeitern mit Büroarbeitsplätzen kann im Allgemeinen davon ausgegangen werden, dass diese bei der Ermittlung der für die Bestellungspflicht relevanten Personen zu berücksichtigen sind, da diese etwa im Rahmen der Nutzung von Textverarbeitungs- oder E-Mail-Programmen regelmäßig auch personenbezogene Daten verarbeiten oder zumindest nutzen (z. B. E-Mail-Adressen aus internen Adressverzeichnissen). Eine Ausnahme, wie sie etwa das Sächsische Datenschutzgesetz in Bezug auf das Verfahrensverzeichnis kennt (§ 10 Abs. 5 Nr. 2 SächsDSG), wonach Verfahren, die ausschließlich der Unterstützung der allgemeinen Bürotätigkeit dienen, vom Anwendungsbereich einzelner datenschutzrechtlicher Vorschriften ausgenommen sind, gibt es im Bundesdatenschutzgesetz nicht, also insbesondere auch nicht in Bezug auf die Bestellungspflicht eines Datenschutzbeauftragten.

8.13.2 Bekanntgabe im Internet?

Zumeist im Zusammenhang mit Beschwerden erhalte ich öfter auch Hinweise auf mögliche Verstöße gegen die Bestellungspflicht. Wenn sich datenschutzrechtlich sensibilisierte Petenten beispielsweise Internetseiten näher anschauen und dort keine Datenschutzerklärung und insbesondere auch keine Informationen über den betrieblichen Datenschutzbeauftragten finden, kommt es schon vor, dass mir dies - als vermeintlicher Verstoß - entsprechend mitgeteilt wird.

Natürlich gehe ich auch solchen Hinweisen konsequent nach, jedoch bin ich einerseits nicht befugt, den Petenten mangels Verletzung seiner eigenen Rechte über in diesem Zusammenhang ggf. festgestellte Verstöße zu unterrichten, andererseits ist insoweit auch festzuhalten und jedenfalls dies teile ich den Hinweisgebern natürlich mit, dass nicht-öffentliche Stellen nur unter ganz konkreten Voraussetzungen (vgl. § 4f Abs. 1 BDSG) verpflichtet sind, einen betrieblichen Datenschutzbeauftragten zu bestellen, und darüber hinaus auch keine Vorschrift existiert, die eine nicht-öffentliche Stelle verpflichtet, ihren ggf. bestellten Datenschutzbeauftragten auf ihrer Website namentlich zu nennen. Gleichwohl empfiehlt es sich für eine verantwortliche Stelle im Interesse einer angemessenen Außendarstellung natürlich, die Bestellung eines Datenschutzbeauftragten (und damit den Stellenwert, den man im Unternehmen dem Datenschutz beimisst) entsprechend zu kommunizieren und in diesem Zusammenhang auch dessen - ggf. nur funktionsbezogene - Kontaktdetails zu veröffentlichen.

8.13.3 Unwirksame Bestellung eines Mitinhabers und Finanzleiters

Im Zuge der Aufsicht einer Holding mit mehreren Einzelunternehmen wurde ich darauf aufmerksam, dass diese jeweils ihren Finanzleiter zum betrieblichen Datenschutzbeauftragten bestellt hatte, der zudem als Mitgesellschafter erheblich an ihr beteiligt war.

Beide Umstände hindern jedoch die objektiv gebotene Zuverlässigkeit und damit die Möglichkeit der Bestellung. So verlangt § 4f Abs. 2 Satz 1 BDSG nach der Rechtsprechung (LAG Niedersachsen, Urteil vom 19. August 2010 - 7 Sa 1131/09, Rdnr. 56, juris), *„dass der Datenschutzbeauftragte frei ist von anderen Aufgaben, die mit seiner Kontrollfunktion nicht zu vereinbaren sind und die ihn deshalb in Interessenkonflikte bringen könnten. Dies wäre mit dem vom Gesetz verfolgten Gedanken einer qualifizierten internen Kontrolle nicht zu vereinbaren. Der Datenschutzbeauftragte soll und muss die Rechte Dritter […] gegen mögliche Beeinträchtigungen durch Datenverarbeitung schützen können. Seine besondere Stellung wird unterstrichen durch die Weisungsfreiheit und den Benachteiligungsschutz gemäß § 4f Abs. 3 Satz 2 und Satz 3 BDSG. Mit seiner Stellung und Funktion wäre es nicht zu vereinbaren, wenn er in erster Linie seine eigene Tätigkeit kontrollieren müsste.*“

In der Inhaberschaft oder zumindest in einer signifikanten Teilinhaberschaft wird daher gemeinhin und quasi als Lehrbuchfall eine die Bestellung objektiv hindernde Interessenkollision gesehen (vgl. Gola/Schomerus, BDSG, 11. Aufl. 2012, § 4f Rdnr. 26), weil der Miteigentümer bzw. Mitinhaber wegen seines höchsteigenen finanziellen Interesses gehindert ist, die für die Aufgabe des betrieblichen Datenschutzbeauftragten notwendige Unabhängigkeit gegenüber dem wirtschaftlichen Interesse des auch ihm gehörenden Unternehmens aufzubringen, da es mit seinem finanziellen Interesse identisch ist.

Die gleiche Besorgnis besteht für einen Finanzleiter, denn dieser ist primär den Finanzinteressen des Unternehmens verpflichtet. Zudem folgt schon aus der organisatorischen Vorgabe in § 4f Abs. 3 Satz 1 BDSG, dass kein Mitglied der Unternehmensführung zum betrieblichen Datenschutzbeauftragten bestellt werden darf.

Tätigt eine verantwortliche Stelle - wie im Falle der Holding und ihrer Unternehmen - gleichwohl die Bestellung einer im o. g. Sinne unzuverlässigen Person, ist der diesbezügliche Akt unwirksam, mit der Folge, dass kein Datenschutzbeauftragter bestellt worden ist (Gola/Schomerus, BDSG, § 4f Rdnr. 23). Dementsprechend habe ich auf Grundlage von § 38 Abs. 5 Satz 1 BDSG die gesetzlich vorgeschriebene Bestellung jeweils angeordnet.

Nach langem Zögern sind die betroffene Holding und ihre Einzelunternehmen meinen Anordnungen schließlich gefolgt, allerdings ist zur Frage der Rechtmäßigkeit meiner Verwaltungsakte weiterhin eine gerichtliche Auseinandersetzung anhängig.

8.13.4 Insolvenz eines externen Datenschutzbeauftragten

Ein insolvent gewordener externer betrieblicher Datenschutzbeauftragter fragte mich, was mit jenen personenbezogenen Daten zu geschehen habe, die er von seinen Auftraggebern zur Erfüllung seiner Aufgaben erhalten habe.

Unter Verweis auf eine insoweit vergleichsweise heranzuziehende Entscheidung des OLG Düsseldorf (Urteil vom 27. September 2012 - I-6 U 241/11 - juris) habe ich ihm geantwortet, dass jene Daten, die er als externer Datenschutzbeauftragter zu Geschäftsbesorgungszwecken erhalten habe, gemäß den §§ 667 1. Alt., 675 BGB i. V. m. § 47 InsO unter Beachtung datenschutzrechtlicher Grundsätze durch den Insolvenzverwalter von der Insolvenzmasse auszusondern wären und (nach Anbietung) auf Verlangen den Auftraggebern herauszugeben sind. Sie gehören nicht zur Insolvenzmasse.

8.13.5 Auch politische Parteien brauchen einen Datenschutzbeauftragten

Im Berichtszeitraum fragte der Landesverband einer politischen Partei bei meiner Behörde an, ob er wie alle anderen nicht-öffentlichen Stellen ebenso verpflichtet sei, einen betrieblichen Datenschutzbeauftragten zu bestellen, da die Voraussetzungen einer gesetzlich vorgeschriebenen Bestellung zwar an sich vorlägen, jedoch offen sei, ob für politische Parteien nicht wegen ihres besonderen Verfassungsauftrags aus Art. 21 GG befreiende Ausnahmeregelungen gelten würden.

Dem Landesverband habe ich hierauf mitgeteilt, dass politische Parteien frei gebildete Personenvereinigungen sind, die sich auf der Basis des privaten Rechts nach den vereinsrechtlichen Regelungen des Bürgerlichen Gesetzbuches gründen, also im Rechtsverkehr als rechtsfähige oder nicht-rechtsfähige Vereine auftreten.

Als somit nicht-öffentliche Stellen im Sinne von § 2 Abs. 4 Satz 1 BDSG haben sie daher - in Ermangelung anderweitiger Regelungen - jeweils für ihre Gliederungen auch einen eigenen betrieblichen Datenschutzbeauftragten gemäß § 4f BDSG zu bestellen, soweit diese jeweils rechtlich eigenständig sind bzw. eine Aktiv- bzw. Passivlegitimation nach § 3 Satz 2 PartG besteht.

Hierauf hat der betroffene Landesverband einen betrieblichen Datenschutzbeauftragten förmlich bestellt.

8.14 Rechte Betroffener

8.14.1 Vereitelung datenschutzrechtlicher Auskunftsersuchen

Ein Internetportal, das eine fragwürdige Geschäftspraktik verfolgt, bei der Verbraucher unbeabsichtigt ein kostenpflichtiges Abonnement eingehen, konfrontierte mich mit einer bis dahin neuen Problematik des Zugangs datenschutzrechtlicher Auskunftsersuchen.

Wollten Betroffene mittels E-Mail ihren Auskunftsanspruch geltend machen, bestritt das Unternehmen stets den Zugang. Wollten die Betroffenen (stattdessen) ihr Verlangen per Telefax unter der im Internet angebenden Nummer senden, scheiterte dies daran, dass das Unternehmen den Faxeingang offenbar auf bestimmte Rufnummern beschränkte (sogenannte Whitelist), um sich vor „Belästigungen“ durch „unerwünschte“ Kontaktaufnahmewünsche seiner „Kunden“ zu schützen. Bei (einfachen) postalischen Auskunftsersuchen stritt das Unternehmen ebenso den Zugang ab.

Somit blieb den Betroffenen oft nur die Zusendung mittels Einschreiben. Solche nahm das Unternehmen aber schlichtweg nicht entgegen.

Deshalb machte ich die Geschäftsführung auf die Rechtsprechung des BGH aufmerksam, nach der ein Adressat sich jedenfalls dann so behandeln lassen muss, als sei ihm das Schreiben im Zeitpunkt der Annahmeverweigerung zugegangen, wenn er grundlos die Annahme eines Einschreibebriefes verweigert und er - wie hier - im Rahmen vertraglicher Beziehungen mit rechtserheblichen Mitteilungen des Absenders rechnen musste (BGH, Urteil vom 27. Oktober 1982 - V ZR 24/82 - juris).

Weiterhin verhängte ich gegen beide Geschäftsführer jeweils ein Bußgeld, da ich in einem Fall das systematische Vereiteln der Geltendmachung des datenschutzrechtlichen Auskunftsanspruchs habe nachweisen können. Die Bußgeldbescheide sind inzwischen rechtskräftig.

8.14.2 Vereitelung der Auskunftserteilung durch Löschung

Nach § 34 Abs. 1 Satz 1 BDSG hat die verantwortliche Stelle dem Betroffenen auf Verlangen Auskunft zu erteilen über die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen, den Empfänger oder die Kategorien von Empfängern, an die Daten weitergegeben werden, und den Zweck der Speicherung.

Betroffene verbinden ihre diesbezüglichen Auskunftsforderungen insbesondere dann, wenn sie der Meinung sind, die verantwortliche Stelle habe ihre Daten unbefugt verar-

beitet (z. B. nach Erhalt von Werbemails), häufig mit einer Löschungsforderung. Zuvor hätten sie eben aber doch gern gewusst, welche (weiteren) Daten über sie gespeichert sind, aus welchen Quellen sie stammen und wohin sie ggf. schon übermittelt worden sind.

Ich habe in diesen Fällen wiederholt feststellen müssen, dass verantwortliche Stellen ihre Auskunftspflicht dadurch umgehen wollen, dass sie dem Löschungsverlangen sofort entsprechen und zuvor allenfalls noch eine lediglich rudimentäre, d. h. in jedem Fall unvollständige Auskunft erteilen. Haken Betroffene dann entsprechend nach, werden sie damit abgespeist, dass ihre Daten ja wunschgemäß gelöscht worden seien und daher keine weitere Auskunft mehr erteilt werden könne, insbesondere weder nachvollzogen werden könne, woher die Daten stammten noch an wen sie bereits übermittelt worden sind. Wird dann versucht, über mich eine weitere Sachverhaltsaufklärung zu erreichen, erhalte ich die gleiche Antwort. Tatsächlich ist also oftmals auch für mich nicht mehr aufklärbar, woher die Daten bezogen und auf welcher Rechtsgrundlage sie verarbeitet und genutzt worden sind.

Was ich an dieser Stelle allerdings feststellen kann, ist ein Verstoß gegen die Auskunftspflicht nach § 34 BDSG. Die Nichterteilung einer Auskunft kann immer dann nicht mit der Löschung der Daten gerechtfertigt werden, wenn das Auskunftsbegehren des Betroffenen bereits vor Löschung der Daten bekannt gewesen ist.

Es mag zutreffen, dass beispielsweise die Auskunft über die Datenempfänger nach Löschung des Datensatzes nicht mehr erteilt werden kann. Dies wäre dann der Fall, wenn diese Angaben zuvor auch tatsächlich im Datensatz des Betroffenen gespeichert gewesen waren und somit gleichfalls gelöscht worden wären. Dies zugunsten der verantwortlichen Stelle unterstellt ändert jedoch nichts an der Tatsache, dass sie jedenfalls zum Zeitpunkt des Auskunftsersuchens, mithin also vor der Löschung, in der Lage gewesen wäre, auch Auskunft über die Datenempfänger zu erteilen. Wenn also der Betroffene von Anfang an auch Auskunft über die Empfänger seiner Daten gefordert hatte, diese jedoch trotz der demnach bestandenen Möglichkeit nicht erhalten hat, ist unzweifelhaft der Bußgeldtatbestand des § 43 Abs. 1 Nr. 8a BDSG verwirklicht worden. Die verantwortliche Stelle kann sich einer Auskunftsverpflichtung nach § 34 Abs. 1 BDSG nicht dadurch entziehen, dass sie die betreffenden Daten löscht und somit eine Auskunftserteilung unmöglich macht.

8.14.3 Auskunftsrechte juristischer Personen

Eine interne Datenschutzbeauftragte wandte sich an mich, weil eine verantwortliche Stelle ihrem Arbeitgeber ein nach § 34 Abs. 1 BDSG gestelltes Auskunftsersuchen nicht

beantwortet hatte, welches sich auf Daten des Unternehmens und - im Kontext hierzu - mittelbar auch auf eine Beschäftigte bezog.

Ihr habe ich mitteilen müssen, dass das Recht auf informationelle Selbstbestimmung und damit der dritte Abschnitt des Bundesdatenschutzgesetzes nur zugunsten natürlicher Personen wirkt, also nach dem Anwendungsbereich des Bundesdatenschutzgesetzes keine Verpflichtung besteht, wegen § 34 Abs. 1 BDSG Daten zu juristischen Personen mitzuteilen, da sie gerade nicht personenbezogen sind (§§ 1 Abs. 1, 3 Abs. 1 BDSG).

Dass die erfragten Daten sich (jedenfalls teilweise) wegen des bei juristischen Personen typischen Handelns natürlicher Personen auch auf eine Beschäftigte beziehen lassen, bewirkt nicht, dass § 34 Abs. 1 BDSG gleichwohl einschlägig wäre, selbst wenn der Auskunftsanspruch unmittelbar von der Beschäftigten geltend gemacht worden wäre. Denn die juristische Person kann sich nicht auf den Umweg über den Datenschutz der für sie handelnden natürlicher Personen, also ihrer Mitarbeiter, solche Rechte verschaffen, die ihr nach der Systematik des Bundesdatenschutzgesetzes wegen des alleinigen Schutzes natürlicher Personen ansonsten nicht zukommen.

8.15 Informationspflichten bei Datenpannen

Nach § 42a BDSG sind die verantwortlichen Stellen 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.

Im Berichtszeitraum sind bei mir zwölf solcher Meldungen eingegangen. In sechs Fällen habe ich nach entsprechender Prüfung eine Meldepflicht verneint, weil entweder meine örtliche Zuständigkeit nicht gegeben war oder aber die Voraussetzungen des § 42a BDSG nicht erfüllt gewesen sind.

Bei weiteren drei Meldungen war die Prüfung der Meldepflicht zum Ende des Berichtszeitraums noch nicht abgeschlossen.

Die verbleibenden drei Meldungen betrafen

- einen Diebstahl von Kinderkarten mit Gesundheitsdaten in einer Kindertageseinrichtung (16 Betroffene),
- einen Skimming-Fall (Ausspähen von Kartendaten und PIN an Geldautomaten) bei einer Sparkasse (336 Betroffene) und

- die Entwendung eines Laptops mit Gesundheits- und Bankverbindungsdaten nach Einbruch in das Kundendienstbüro einer Versicherungsvermittlerin (237 Betroffene).

In allen drei Fällen sind die Betroffenen ordnungsgemäß benachrichtigt (§ 42a Sätze 2 und 3 BDSG) und zudem auch ausreichende Maßnahmen getroffen worden, die - abhängig vom Einzelfall - die Gefahr einer Wiederholung des jeweiligen Vorfalls ausschließen bzw. verringern und den eingetretenen oder zu erwartenden Schaden so weit als möglich minimieren.

9 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 erfülle ich meine Verpflichtung, die Öffentlichkeit alle zwei Jahre über die Tätigkeit der Aufsichtsbehörde zu informieren. Der um drei Monate verlängerte Berichtszeitraum ergibt sich aus einer diesbezüglichen Änderung des Sächsischen Datenschutzgesetzes: Seit dem 31. Juli 2011 ist in § 30 Abs. 1 Satz 1 SächsDSG verankert, dass ich auch als Aufsichtsbehörde nach § 30a SächsDSG dem Sächsischen Landtag alle zwei Jahre jeweils zum 31. März einen Tätigkeitsbericht vorzulegen habe.

In meinem Internetauftritt - *http://www.datenschutz.sachsen.de* - halte ich ebenso Informationen zu aktuellen Datenschutzthemen wie auch Materialien zur Unterstützung der Tätigkeit der verantwortlichen Stellen und ihrer Datenschutzbeauftragten zum Abruf bereit.

Die bewährte Zusammenarbeit mit dem GDD-Erfa-Kreis Sachsen habe ich im Berichtszeitraum fortgeführt. An den vierteljährlich stattfindenden Veranstaltungen haben Vertreter meiner Behörde regelmäßig und aktiv teilgenommen, indem sie dort Vorträge über aktuelle Themen wie beispielsweise die Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten (§ 42a BDSG) gehalten und rege an den in diesem Kreis geführten datenschutzrechtlichen Diskussionen teilgenommen haben.

Im Berichtszeitraum haben mich auch wieder zahlreiche Anfragen wegen einer Referententätigkeit bei verschiedenen Fach- und Fortbildungsveranstaltungen erreicht. So sehr ich das Interesse der jeweiligen Veranstalter an Datenschutzfragen begrüße, musste ich gleichwohl um Verständnis dafür bitten, dass es mir aufgrund der - gerade im nicht-öffentlichen Bereich - sehr hohen Arbeitsbelastung und der äußert angespannten Personalsituation meiner Dienststelle nicht möglich war und auch weiterhin nicht möglich ist, die insoweit jeweils gewünschten Beiträge zu den betreffenden Veranstaltungen zu leisten. Da § 38 Abs. 1 Satz 2 BDSG eine - unternehmensspezifische - Beratungs- und Unterstützungspflicht nur gegenüber betrieblichen Datenschutzbeauftragten und den verantwortlichen Stellen vorsieht, würde es sich insoweit um eine darüber hinausgehende Leistung handeln, die voraussetzte, dass die dafür erforderlichen Kapazitäten ohne Beeinträchtigung der Erfüllung meiner gesetzlichen vorgegebenen Aufgaben auch tatsächlich verfügbar wären, und zwar gleichmäßig für alle derartigen Weiterbildungsveranstaltungen, was eben nicht der Fall ist.

10 Durchsetzung der Rechte und Befugnisse der Aufsichtsbehörde

10.1 Förmliche Heranziehung zur Auskunft

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).

Förmliche Auskunftsheranziehungsbescheide verpflichten die verantwortliche Stelle zur Auskunftserteilung und dienen damit der Durchsetzung des Auskunftsrechts der Aufsichtsbehörde (vgl. dazu auch 5. TB, Pkt. 10.1). Derartige Bescheide werden im Regelfall immer dann erlassen, wenn eine verantwortliche Stelle die geforderten Auskünfte auch nach wiederholter Aufforderung nicht erteilt. Adressaten sind dabei zumeist Unternehmen, die auf formlose schriftliche Auskunftsaufforderungen überhaupt nicht reagieren. Nur in Ausnahmefällen wird die Auskunft aktiv verweigert.

Leider musste dieses Aufsichtsinstrument im Berichtszeitraum verstärkt zur Anwendung kommen. Auch wenn sich dies letztendlich als sehr wirksam herausgestellt und in den meisten Fällen dann - früher oder später - zur Auskunftserteilung geführt hat, so ist auch festzustellen, dass sich dadurch die Bearbeitungszeit von Eingaben erheblich verlängert und zudem viele der ohnehin sehr knapp bemessenen Ressourcen der Aufsichtsbehörde gebunden werden.

In 23 der 31 im Berichtszeitraum durchgeführten förmlichen Verfahren hat bereits der Erlass eines - mit der Androhung eines Zwangsgeldes verbundenen - Heranziehungsbescheides zur Auskunftserteilung geführt. In sechs weiteren Verfahren musste anschließend aber ein Zwangsgeld festgesetzt werden, bevor die geforderten Auskünfte schließlich doch noch erteilt wurden.

Lediglich in zwei Fällen haben die verantwortlichen Stellen keine Auskünfte erteilt und stattdessen (erfolglos) gegen die Bescheide geklagt (vgl. dazu Pkt. 4.2.1).

Insgesamt ist festzuhalten, dass sich die Zahl der förmlichen Verfahren zur Auskunftserzwingung mehr als vervierfacht hat. Dies bedeutet aber nicht, dass sich auch die Anzahl der verantwortlichen Stellen, die gegen ihre Auskunftspflicht verstoßen haben, in gleicher Weise vervielfacht hat, denn allein 13 der 32 durchgeführten Verfahren haben insoweit eine einzige Unternehmensgruppe betroffen. Die stark gestiegene Anzahl der förmlichen Verfahren spiegelt sich auch in der gleichfalls erhöhten Anzahl der

daraus resultierenden, mithin also Verstöße gegen die Auskunftspflicht betreffenden Ordnungswidrigkeitenverfahren wider (vgl. Pkt. 11.1).

10.2 Anordnungen

Zur Gewährleistung der Einhaltung des Bundesdatenschutzgesetzes 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).

Im Berichtszeitraum sind erstmals acht - gleichlautende - Anordnungen erlassen worden. Die betreffenden, alle der gleichen Unternehmensgruppe angehörigen verantwortlichen Stellen sind aufgefordert worden, umgehend einen Datenschutzbeauftragten zu bestellen, da zwar ein Datenschutzbeauftragter bestellt gewesen war, dessen Bestellung aber wegen von vornherein bestehender Interessenkollisionen unwirksam war. Die verantwortlichen Stellen sind zwar einerseits gegen die Verpflichtung auf dem Klageweg vorgegangen, haben andererseits aber auch der Forderung der Aufsichtsbehörde entsprochen und eine andere Person (ohne Interessenkollisionen) zum Datenschutzbeauftragten bestellt (vgl. Pkt. 8.13.3).

Im Fall der Einsehbarkeit personenbezogener Flugbuchungsdaten über das Internet (vgl. Pkt. 8.2.5) habe ich gegenüber der verantwortlichen Stelle angeordnet, dass sie diesen Mangel unverzüglich durch geeignete technische und organisatorische Maßnahmen zu beheben hat. Wegen der besonderen Eilbedürftigkeit dieser Angelegenheit habe ich die Frist für die erforderliche Anhörung auf wenige Stunden verkürzt und dann auch die sofortige Vollziehbarkeit des Bescheides angeordnet. Die verantwortliche Stelle ist meiner Anordnung dann auch umgehend gefolgt.

In weiteren fünf Fällen haben die verantwortlichen Stellen bereits nach Erhalt des Anhörungsschreibens den Forderungen der Aufsichtsbehörde entsprochen. Der Erlass einer Anordnung war daher in diesen Fällen entbehrlich.

11 Ordnungswidrigkeitenverfahren / Strafanträge

11.1 Ordnungswidrigkeitenverfahren

Als Verwaltungsbehörde nach § 36 Abs. 2 OWiG (§ 13 OWiZuVO) bin ich auch für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 43 BDSG zuständig.

Im 5. TB hatte ich unter Pkt. 11.1 ein Ordnungswidrigkeitenverfahren wegen Nichtbestellung eines Datenschutzbeauftragten erwähnt, über das nach einem Einspruch das zuständige Amtsgericht zu entscheiden hatte. So weit ist es dann aber jedenfalls in diesem Verfahren doch nicht mehr gekommen. Die verantwortliche Stelle hat kurz vor dem angekündigten Verhandlungstermin ihren Einspruch zurückgenommen, womit der Bußgeldbescheid über 10.000 Euro dann doch noch bestandskräftig geworden ist.

Anders in den zwei anderen offenen Fällen aus dem letzten TB. Die wegen unbefugtem Datenabrufs (unbefugte Einsichtnahme in eine Datei mit Personaldaten im persönlichen Unterverzeichnis eines anderen Mitarbeiters) erlassenen zwei Bußgeldbescheide hat das zuständige Amtsgericht aufgehoben und das Verfahren eingestellt. Ebenso unbefriedigend ist der weitere Verlauf in dem Bußgeldverfahren wegen Weitergabe der Bankverbindungsdaten eigener Kunden an einen Auftragnehmer zwecks eigenständigen Einzugs ihm zustehender Servicegelder. Hier hatte das Amtsgericht den Einspruch zunächst abgewiesen, wogegen der Betroffene aber erfolgreich Rechtsbeschwerde einlegen konnte. Das OLG hat das Verfahren wegen seiner Auffassung nach ungenügender Sachverhaltsaufklärung wieder an das Amtsgericht zurückverwiesen, wo das Verfahren dann leider eingestellt worden ist. Da der Sächsische Datenschutzbeauftragte als Verwaltungsbehörde nach dem Ordnungswidrigkeitengesetz bei gerichtsanhängigen Verfahren nicht mehr Herr des Verfahrens ist, sind die diesbezüglichen Einflussnahmemöglichkeiten sehr begrenzt und setzen dabei insbesondere eine rechtzeitige Information über alle aktuellen Verfahrensschritte voraus. Leider hat es die zuständige Staatsanwaltschaft in diesem Fall versäumt, rechtzeitig auf die Fortsetzung des Verfahrens betreffende Aufforderungen des Amtsgerichts zu reagieren und insbesondere auch mich als Verwaltungsbehörde dabei mit einzubeziehen.

Im Berichtszeitraum sind durch den Sächsischen Datenschutzbeauftragten 79 Bußgeldverfahren neu eingeleitet worden; drei weitere Verfahren stammten noch aus dem Jahr 2010 (vgl. 5. TB, Pkt. 11.1).

Von den somit im Berichtszeitraum insgesamt 82 anhängigen Verfahren sind 16 eingestellt worden, 29 Verfahren waren zum Ende des Berichtszeitraums noch nicht abgeschlossen.

Damit sind im Berichtszeitraum schließlich 36 Verfahren mit einem Bußgeldbescheid und ein Verfahren mit einem Verwarnungsgeld abgeschlossen worden; die Bußgeldsumme belief sich insgesamt auf 54.095 Euro und hat sich damit gegenüber dem vorangegangenen Berichtszeitraum mehr als verdoppelt.

Aus dem Bereich des § 43 Abs. 1 BDSG (formale Rechtsverstöße) sind folgende Sachverhalte mit Bußgeldern belegt worden (insgesamt 24 Fälle):

- Verstoß gegen die Meldepflichten nach § 4d BDSG (ein Fall)
- unterlassene Bestellung eines Datenschutzbeauftragten (§ 4f Abs. 1 BDSG) (vier Fälle)
- Verstöße gegen die Auskunftspflichten gegenüber der Aufsichtsbehörde (§ 38 Abs. 3 BDSG) (sechs Fälle)
- in Werbeschreiben unterlassene Unterrichtungen über das Widerspruchsrecht (§ 28 Abs. 4 Satz 2 BDSG) (drei Fälle)
- unterlassene oder nicht rechtzeitige Erteilung von Auskünften an den Betroffenen (§ 34 Abs. 1 BDSG) (neun Fälle)
- Verstoß gegen die inhaltlichen Vorgaben bei einem Auftragsdatenverarbeitungsvertrag (§ 11 Abs. 2 Satz 2 BDSG) (ein Fall)

Wegen materieller Rechtsverstöße (43 Abs. 2 BDSG) wurden in 13 Fällen Bußgelder verhängt:

- Speicherung einer E-Mail-Adresse ohne Einwilligung (anschließende Nutzung für Werbezwecke)
- Videoüberwachung eines Friseursalons (Warte- und Frisierbereiche)
- Anfertigung von Wohnungsfotos ohne Wissen des Mieters und Veröffentlichung im Internet durch Immobilienmakler
- unberechtigter Abruf steuerlicher Daten durch Angestellten einer Steuerkanzlei und Versand an eigene private E-Mail-Adresse
- Erhebung, Verarbeitung und Nutzung von Mobilfunkrufnummern für private Kontaktanbahnung durch Mitarbeiter eines Telefon-Shops
- Videoüberwachung von an das eigene Grundstück angrenzenden öffentlichen Verkehrsbereichen (Straßen, Gehwege, Kreuzung)
- unzulässige Datenübermittlung innerhalb einer Unternehmensgruppe durch Zugriffsgewährung
- unzulässiger Datenabruf innerhalb einer Unternehmensgruppe
- innerbetrieblicher Aushang einer personenbezogenen Krankenstatistik

- Erschleichen personenbezogener Daten durch Vortäuschung der rechtlichen Interessenvertretung des Betroffenen
- wiederholte Nichtbeachtung eines Werbewiderspruchs durch ein Autohaus
- Erschleichung einer Wirtschaftsauskunft durch Behauptung einer beabsichtigten bzw. bestehenden Geschäftsbeziehung und Übermittlung an einen Bekannten
- unterlassene Meldung eines Vorfalls nach § 42a BDSG

Wenn die Bußgelder mehr als 200 Euro betragen, werden die betreffenden Bußgeldentscheidungen in das Gewerbezentralregister eingetragen (§ 149 Abs. 2 Nr. 3 GewO). Dies betrifft auch nach § 30 OWiG gegen juristische Personen festgesetzte Geldbußen, wobei dabei auch die sonstigen Voraussetzungen des § 149 Abs. 2 Nr. 3 GewO gegeben sein müssen, d. h. Grundlage für die Festsetzung des Bußgeldes muss die Ordnungswidrigkeit eines Vertreters oder Beauftragten sein. Die im Berichtszeitraum bestandskräftig mit einem Bußgeldbescheid abgeschlossenen Verfahren haben in 31 Fällen zu solch einem Gewerbezentralregistereintrag geführt.

11.2 Strafanträge

Nach § 44 Abs. 2 BDSG haben die Datenschutzaufsichtsbehörden ein eigenständiges Strafantragsrecht bei Straftatbeständen nach dem Bundesdatenschutzgesetz.

Als Straftat nach dem Bundesdatenschutzgesetz verfolgbar sind dabei nur die in § 43 Abs. 2 BDSG genannten materiellen Datenschutzverstöße und dies auch nur dann, wenn die Tat vorsätzlich in Bereicherungs- oder Schädigungsabsicht oder gegen Entgelt begangen worden ist (vgl. § 44 Abs. 1 BDSG).

In jedem Fall erforderlich ist ein Strafantrag (§ 44 Abs. 2 Satz 1 BDSG) - antragsberechtigt ist neben dem Betroffenen selbst und der verantwortlichen Stelle insbesondere auch die Datenschutzaufsichtsbehörde. Die Aufsichtsbehörde kann dieses Recht grundsätzlich auch gegen den Willen des Betroffenen ausüben, wird diese Entscheidung in sich auf einen einzelnen Betroffenen beschränkenden Fällen aber zumeist diesem überlassen. Anders in den Fällen, in denen es eine Vielzahl Betroffener gibt und diese möglicherweise noch nicht einmal Kenntnis von dem Datenverstoß erlangt haben. Hier wird die Aufsichtsbehörde regelmäßig von ihrem Strafantragsrecht Gebrauch machen (müssen), dies einerseits wegen des dahinter stehenden öffentlichen Interesses an der Strafverfolgung und andererseits auch, um sich nicht darauf verlassen zu müssen, dass Betroffene - nach entsprechender Unterrichtung - tatsächlich auch noch rechtzeitig - die Antragsfrist beträgt drei Monate nach Kenntniserlangung von der Tat und der Person des Täters (§ 77b Abs. 1 StGB) - selbst einen Strafantrag stellen.

Im Berichtszeitraum habe ich insgesamt acht Strafanträge gestellt. Auf Einzelheiten kann ich nicht eingehen, da Ermittlungsverfahren noch andauern.

12 Zusammenarbeit mit anderen Aufsichtsbehörden

Die Datenschutzaufsichtsbehörden der Bundesländer treffen sich im Regelfall 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. Die im Berichtszeitraum gefassten Beschlüsse sind unter Pkt. 13 dieses Berichts enthalten.

Meine Mitarbeiter sind darüber hinaus - ungeachtet der damit verbundenen erheblichen Zusatzbelastung - auch in den meisten Arbeitsgruppen des Düsseldorfer Kreises vertreten. Ich messe diesen Arbeitsgruppen große Bedeutung bei, da dort - auch wenn das nicht immer hundertprozentig gelingt - einerseits Rechtsauffassungen zu wichtigen aktuellen Grundsatzfragen untereinander und auch mit Vertretern der Wirtschaft diskutiert und abgestimmt und andererseits aber auch Erfahrungen aus der jeweiligen Kontroll- und Sanktionspraxis zwischen den Vertretern der Aufsichtsbehörden ausgetauscht werden. In den Arbeitsgruppen werden zudem auch viele Beschlüsse für den Düsseldorfer Kreis vorbereitet. Im Berichtszeitraum war meine Behörde in den Arbeitsgruppen

- Auskunfteien
- Beschäftigtendatenschutz
- Kreditwirtschaft
- Sanktionen
- Telemedien
- Versicherungswirtschaft
- Videoüberwachung
- Werbung und Adresshandel

vertreten.

Eher praktischer Natur und im Übrigen keiner der fach- bzw. branchenspezifischen Arbeitsgruppen zuordenbar 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. 2011 fand der Workshop im LDA Bayern in Ansbach und 2012 bei Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit statt. An beiden Veranstaltungen hat der Sächsische Datenschutzbeauftragte aktiv mit eigenen Beiträgen teilgenommen.

13 Beschlüsse des Düsseldorfer Kreises

13.1 Beschluss des Düsseldorfer Kreises vom 8. April 2011

13.1.1 Datenschutz-Kodex des BITKOM für Geodatendienste unzureichend - Gesetzgeber gefordert

Am 1. März 2011 hat der Branchenverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM) einen Datenschutz-Kodex für Geodatendienste vorgelegt, der den schutzwürdigen Interessen der Eigentümer und Bewohner bei der Veröffentlichung der sie betreffenden Gebäudeansichten im Internet Rechnung tragen soll. Das Bundesministerium des Innern hatte der Internetwirtschaft in Aussicht gestellt, bei der Vorlage einer angemessenen und mit den Datenschutzbehörden des Bundes und der Länder abgestimmten Selbstverpflichtung auf gesetzliche Spezialregelungen für Internet-Geodatendienste wie Google Street View zu verzichten.

Der Düsseldorfer Kreis stellt fest, dass die Selbstregulierung der Internetwirtschaft mit dem vom BITKOM vorgelegten Datenschutz-Kodex nicht gelingt. Der Kodex entspricht in wesentlichen Bereichen nicht den datenschutzrechtlichen Anforderungen und ist nicht mit den Datenschutzbehörden des Bundes und der Länder abgestimmt.

Der Kodex sieht zwar ein Widerspruchsrecht gegen die Veröffentlichung von Gebäudeansichten im Internet vor, ohne dass Gründe dargelegt werden müssen. Der Widerspruch ist jedoch erst nach der Veröffentlichung vorgesehen. Alle Gebäudeansichten sind deshalb zunächst im Internet verfügbar. Bereits mit der Veröffentlichung der Bilder wird aber das Recht auf informationelle Selbstbestimmung verletzt. Auch bei weiteren Regelungen weist der Datenschutz-Kodex datenschutzrechtliche Defizite auf: Viele Veröffentlichungen, die die Privatsphäre beeinträchtigen, werden vom Kodex nicht erfasst, so etwa Schrägaufnahmen aus der Luft. Hinzu kommt, dass der Datenschutz-Kodex nur für die Unternehmen bindend ist, die ihn unterzeichnet haben.

Deshalb ist jetzt der Gesetzgeber gefordert, das Recht auf informationelle Selbstbestimmung im Internet mit einer umfassenden Regelung zu schützen, die dem besonderen Gefährdungspotential für das Persönlichkeitsrecht im Internet Rechnung trägt. Hierzu zählt insbesondere ein gesetzlich verbrieftes Widerspruchsrecht gegen die Veröffentlichung, das es den Betroffenen ermöglicht, bereits vor der Veröffentlichung personenbezogener Daten im Internet Widerspruch einzulegen.

Ein solches Vorab-Widerspruchsrecht entspricht den Anforderungen, die der Düsseldorfer Kreis in seinem Beschluss vom 13./14. November 2008 nach Auslegung des

geltenden Rechts konkretisiert hat. Besonders wichtig sind demnach die folgenden Punkte:

- Gesichter und Kfz-Kennzeichen sind unkenntlich zu machen.
- Eigentümer und Bewohner eines Hauses müssen die Möglichkeit erhalten, die Veröffentlichung der Gebäudefassade durch einen Widerspruch zu verhindern; die Widerspruchsmöglichkeit muss vor wie auch nach der Veröffentlichung bestehen.
- Die geplante Datenerhebung und der Hinweis auf die Widerspruchsmöglichkeit sind rechtzeitig bekannt zu geben.

13.2 Beschlüsse des Düsseldorfer Kreises vom 4./5. Mai 2011

13.2.1 Datenschutzgerechte Smartphone-Nutzung ermöglichen!

Smartphones sind Mobiltelefone, die insbesondere im Zusammenhang mit der Nutzung des Internet über deutlich mehr Computerfunktionalitäten und Kommunikationsmöglichkeiten verfügen als herkömmliche Mobiltelefone. Smartphones werden für eine Vielzahl von Aktivitäten genutzt und sind damit in weitaus größerem Umfang als sonstige Geräte der Informations- und Kommunikationstechnik „persönliche“ Geräte, die den Nutzer im Alltag permanent begleiten. Über das Telefonieren hinaus eröffnen auf den Geräten installierbare Programme („Apps“), Lokalisierungsfunktionen (GPS) und Bewegungssensoren eine breite Palette von Anwendungsbereichen. Die dabei anfallenden Daten lassen detaillierte Rückschlüsse auf Nutzungsgewohnheiten, Verhaltensweisen oder Aufenthaltsorte der Nutzer zu.

Im Gegensatz zu herkömmlichen PCs bieten Smartphones den Nutzern jedoch nur rudimentäre Möglichkeiten, die Preisgabe personenbezogener Daten zu kontrollieren oder zu vermeiden; gängige Funktionen des Selbstdatenschutzes können nicht genutzt werden. Häufig werden personenbezogene Daten ohne Wissen der Nutzer an die Anbieter von Diensten übermittelt. Mit einiger Berechtigung wird davon gesprochen, ein solches Gerät sei ein „Spion in der Hosentasche“.

Vor diesem Hintergrund ist aus datenschutzrechtlicher Sicht insbesondere Folgendes zu fordern:

- Transparenz bezüglich der Preisgabe personenbezogener Daten:

In allen aktuellen Untersuchungen zeigt sich, dass in einer Vielzahl von Fällen durch die Geräte selbst mittels Betriebssystemen oder durch Anwendungen eindeutige Gerätekennungen, Standortdaten, E-Mail- und Telefontakte, SIM-Kartennummer und

weitere personenbezogene Daten ohne Unterrichtung der Nutzer an Gerätehersteller, Provider oder Anbieter von Analysediensten übermittelt werden. Die Nutzer müssen in die Lage versetzt werden, diese Übermittlungen nachzuvollziehen. Sie müssen auch über den jeweiligen Zweck der Datennutzungen unterrichtet werden.

- Steuerungsmöglichkeiten der Nutzer für die Preisgabe personenbezogener Daten:

Die Konzepte gängiger Smartphones sind oftmals darauf reduziert, dass, wenn überhaupt, lediglich während der Installation einer Anwendung der Nutzer pauschal einen Datenzugriff steuern kann. Auch erhalten zugelassene Anwendungen meist eine generelle Zugriffsmöglichkeit z. B. auf Kontaktinformationen. Den Nutzern müssen Möglichkeiten an die Hand gegeben werden, mit denen aus der Nutzungssituation heraus gesteuert werden kann, ob und welche Daten einer Applikation zugänglich gemacht werden und an wen sie übermittelt werden.

- Einflussmöglichkeiten auf das Löschen von Spuren bei der Internet-Nutzung:

Im Gegensatz zu der für herkömmliche PCs bestehenden Situation fehlt es im Smartphonebereich weitgehend an Möglichkeiten, Datenspuren, die bei der Internet-Nutzung auf dem Gerät entstehen, zu vermeiden, zu reduzieren, mindestens jedoch, diese erkennbar zu machen und ggf. zu löschen. Solche Möglichkeiten müssen geschaffen und angeboten werden.

- Anonyme und pseudonyme Nutzungsmöglichkeiten:

Generell sollte die Möglichkeit geschaffen werden, Smartphones und die über sie vermittelten Dienste anonym oder pseudonym zu nutzen.

Die Anbieter entsprechender Geräte beziehungsweise Betriebssysteme und die jeweiligen Diensteanbieter müssen möglichst datenschutzfreundliche Funktionalitäten vorsehen und Schwachpunkte eliminieren. Der Grundsatz der Datensparsamkeit ist ernst zu nehmen und umzusetzen. Von besonderer Bedeutung ist die umfassende Information der Nutzer über die Erhebung und Verwendung ihrer Nutzungsdaten. Dies gilt sowohl für die grundlegenden Betriebssysteme einerseits wie für die darauf aufbauenden Funktionalitäten (Apps) andererseits. Diese Anforderungen lassen sich unter den Begriff „Privacy by Design“ fassen; auf den Inhalt und die Bedeutung dieses Punktes hat jüngst die Internationale Konferenz der Datenschutzbeauftragen hingewiesen (Resolution on Privacy by Design v. 29.10.2010).

Der Aufgabe, den Selbstdatenschutz zu stärken, kommt im Bereich der Smartphone-Nutzung eine besondere Bedeutung zu. Die Datenschutzaufsichtsbehörden unterstützen

alle entsprechenden Anstrengungen, insbesondere auch die der European Network and Information Security Agency (ENISA; vgl. Empfehlungen der ENISA vom Dezember 2010 über Informationssicherheitsrisiken, Möglichkeiten und Empfehlungen für Nutzer von Smartphones; http://www.enisa.europa.eu/act/it/oar/smartphones-information-security-risksopportunities-and-recommendations-for-users/at_download/fullReport).

13.2.2 Datenschutzkonforme Gestaltung und Nutzung von Krankenhausinformationssystemen

Krankenhausinformationssysteme sind heute zu unverzichtbaren Hilfsmitteln ärztlicher Behandlung in Krankenhäusern geworden. Ein Abruf der darin elektronisch gespeicherten Patientendaten ist jederzeit, ortsungebunden und sekundenschnell möglich und bietet damit die Grundlage für effiziente Behandlungsentscheidungen. Diesen Vorteilen stehen allerdings erhebliche Datenschutzrisiken gegenüber. Die Möglichkeiten für Klinikpersonal, Behandlungsdaten von Bekannten, Kolleginnen und Kollegen oder Prominenten einzusehen und privat zu nutzen, sind groß. Prüfungen der Datenschutzaufsichtsbehörden und bekannt gewordene Missbrauchsfälle belegen dies.

Das Datenschutzrecht und die ärztliche Schweigepflicht gebieten, dass ein Zugriff auf die Daten von Kranken grundsätzlich nur denjenigen Krankenhausbeschäftigten möglich sein darf, die diese Kranken behandeln oder die Behandlung verwaltungsmäßig abwickeln. Die Aufsichtsbehörden im nichtöffentlichen Bereich fordern daher die datenschutzkonforme Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten in der Informationstechnik von Krankenhäusern.

Es besteht das dringende Bedürfnis, hierbei zu einem bundesweit und trägerübergreifend einheitlichen Verständnis der datenschutzrechtlichen Anforderungen zu gelangen, zumindest soweit dies Divergenzen in der Landeskrankenhausgesetzgebung erlauben. Zu diesem Zweck wurde von den Datenschutzbeauftragten der Länder unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und der Katholischen Kirche eine Orientierungshilfe erarbeitet. Im Rahmen eines Kommentierungsverfahrens und bei Expertenanhörungen wurden Hersteller von Krankenhausinformationssystemen, Betreiber und Datenschutzbeauftragte von Krankenhäusern einbezogen.

Die Orientierungshilfe konkretisiert in ihrem ersten Teil die Anforderungen, die sich aus den datenschutzrechtlichen Regelungen sowie den Vorgaben zur ärztlichen Schweigepflicht für den Krankenhausbetrieb und den Einsatz von Informationssystemen in Krankenhäusern ergeben. In Teil 2 werden Maßnahmen zu deren technischer Umsetzung beschrieben. Für die Hersteller von Krankenhausinformationssystemen, die diese nutzenden Krankenhäuser und die internen Datenschutzbeauftragten von Kranken-

häusern liegt damit erstmals ein Orientierungsrahmen für eine datenschutzkonforme Gestaltung und einen datenschutzgerechten Betrieb entsprechender Verfahren vor.

Die Aufsichtsbehörden im nichtöffentlichen Bereich werden sich an dem vorliegenden Dokument als Leitlinie bei der künftigen Bewertung konkreter Verfahren im Rahmen ihrer Kontroll- und Beratungstätigkeit orientieren. Dabei ist zu berücksichtigen, dass ein Teil der am Markt angebotenen Lösungen nach den Erkenntnissen der Datenschutzbehörden in technischer Hinsicht gegenwärtig noch hinter den darin enthaltenen Anforderungen zurückbleibt. Es ist daher von der Notwendigkeit einer angemessenen Übergangsfrist für erforderliche Anpassungen durch die Hersteller auszugehen.

Stellen die Aufsichtsbehörden im Zuge ihrer Kontrolltätigkeit Defizite im Vergleich zu den dargelegten Maßstäben fest, so werden sie auf die Krankenhäuser einwirken und sie dabei unterstützen, in einem geordneten Prozess unter Wahrung der Patientensicherheit Wege zur Behebung der Defizite zu finden und zu begehen. Die Deutsche Krankenhausgesellschaft und die jeweiligen Landeskrankenhausgesellschaften werden dabei einbezogen.

Die Erfahrungen der Prüftätigkeit sollen in eine regelmäßige Überarbeitung und Aktualisierung der Orientierungshilfe unter Berücksichtigung der technischen Weiterentwicklung einfließen.

Die Aufsichtsbehörden nehmen die Orientierungshilfe zustimmend zur Kenntnis.

13.2.3 Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze

Niedergelassene Ärztinnen und Ärzte sowie andere Angehörige von Heilberufen übermitteln vielfach medizinische Daten an andere Stellen mithilfe von Netzwerken. Dies dient Abrechnungs-, Behandlungs- und Dokumentationszwecken. Seit dem 1. Januar 2011 müssen beispielsweise an der vertragsärztlichen Versorgung teilnehmende Ärzte Abrechnungsdaten leitungsgebunden an die jeweilige Kassenärztliche Vereinigung übermitteln (§ 295 Abs. 4 SGB V in Verbindung mit den Richtlinien der Kassenärztlichen Bundesvereinigung für den Einsatz von IT-Systemen in der Arztpraxis zum Zweck der Abrechnung; siehe http://www.kbv.de/rechtsquellen/24631.html).

An medizinische Netze sind hohe Anforderungen hinsichtlich der Vertraulichkeit und Integrität zu stellen, denn sowohl in den Netzen selbst als auch auf den angeschlossenen Praxissystemen werden Daten verarbeitet, die der ärztlichen Schweigepflicht (§ 203 StGB) unterliegen. Bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze ist daher die „Technische Anlage zu den Empfehlungen zur ärztlichen Schweige-

pflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung (siehe Deutsches Ärzteblatt, Jg. 105, Heft 19 vom 9. Mai 2008) zu beachten.

An die Anbindung von Praxis-EDV-Systemen an medizinische Netze sind folgende Mindestanforderungen zu stellen:

1. Die Kommunikation im Netz muss verschlüsselt ablaufen. Hierzu sind dem Stand der Technik entsprechende Verfahren zu nutzen.

2. Ein unbefugter Zugriff auf die internen Netze der Praxis oder Einrichtung muss ausgeschlossen sein.

3. Die Auswirkungen von Fehlkonfigurationen im internen Netz müssen wirksam begrenzt werden.

4. Die Endpunkte der Kommunikation müssen sich gegenseitig durch dem Stand der Technik entsprechende Verfahren authentisieren.

5. Die Wartung der zum Netzzugang eingesetzten Hard- und Software-Komponenten muss kontrollierbar sein, indem die Wartung durch eine aktive Handlung freizuschalten ist und alle Wartungsaktivitäten protokolliert werden.

6. Zum Netzzugang sind zertifizierte Hard- und Software-Komponenten einzusetzen.

7. Grundstandards - wie beispielsweise die Revisionssicherheit - sind einzuhalten.

Für die verwendeten Verschlüsselungs- und Authentisierungskomponenten sollten Hardware-Lösungen genutzt werden, da bei Software ein erhöhtes Manipulationsrisiko besteht.

Software-Lösungen kommen allenfalls in Ausnahmefällen in Betracht, wenn die zur Kommunikation mit anderen Stellen genutzten Rechner und Komponenten nicht mit dem internen Netz der Praxis verbunden sind. Zusätzlich ist sicherzustellen, dass entweder

a) nur solche Daten gesendet werden, die bereits innerhalb des Praxisnetzes verschlüsselt und integritätsgeschützt wurden

oder

b)
- eine Zwei-Faktor-Authentifikation des Berechtigten stattfindet,
- mit der zum Zugang verwendeten Hard- und Software ausschließlich Zugang zu medizinischen Netzen besteht sowie
- die KBV-Richtlinien zur Online-Anbindung von Praxis-EDV-Systemen an das KVSafeNet eingehalten werden.

13.3 Beschlüsse des Düsseldorfer Kreises vom 22./23. November 2011

13.3.1 Datenschutzkonforme Gestaltung und Nutzung von Cloud-Computing

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich fordern Cloud-Anbieter auf, ihre Dienstleistungen datenschutzkonform zu gestalten. Cloud-Anwender hingegen dürfen Cloud-Services nur dann in Anspruch nehmen, wenn sie in der Lage sind, ihre Pflichten als verantwortliche Stelle in vollem Umfang wahrzunehmen und die Umsetzung der Datenschutz- und Informationssicherheitsanforderungen geprüft haben. Dies betrifft neben den Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit der Daten insbesondere die in diesem Umfeld schwierig umzusetzenden Anforderungen an Kontrollierbarkeit, Transparenz und Beeinflussbarkeit der Datenverarbeitung. Cloud-Computing darf nicht dazu führen, dass Daten verarbeitende Stellen, allen voran ihre Leitung, nicht mehr in der Lage sind, die Verantwortung für die eigene Datenverarbeitung zu tragen.

Zu verlangen sind also mindestens

- offene, transparente und detaillierte Informationen der Cloud-Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption, damit die Cloud-Anwender einerseits entscheiden können, ob Cloud-Computing überhaupt in Frage kommt und andererseits Aussagen haben, um zwischen den Cloud-Anbietern wählen zu können,

- transparente, detaillierte und eindeutige vertragliche Regelungen der Cloud-gestützten Datenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und zur Interoperabilität,

- die Umsetzung der abgestimmten Sicherheits- und Datenschutzmaßnahmen auf Seiten von Cloud-Anbieter und Cloud-Anwender und

- aktuelle und aussagekräftige Nachweise (bspw. Zertifikate anerkannter und unabhängiger Prüfungsorganisationen) über die Infrastruktur, die bei der Auftragserfüllung

in Anspruch genommen wird, die insbesondere die Informationssicherheit, die Portabilität und die Interoperabilität betreffen.

Die Datenschutzaufsichtsbehörden des Bundes und der Länder bieten ihre Unterstützung bei der Entwicklung und bei der Nutzung von Cloud-Computing-Diensten an. Details zur datenschutzgerechten Ausgestaltung dieser Dienste sind einer Orientierungshilfe[1] der Arbeitskreise „Technik“ und „Medien“ zu entnehmen, die der Düsseldorfer Kreis zustimmend zur Kenntnis genommen hat.

13.3.2 Beschäftigtenscreening bei AEO-Zertifizierung wirksam begrenzen

Der Düsseldorfer Kreis hat sich bereits mehrfach mit dem Problem des Mitarbeiterscreenings befasst, zuletzt durch Beschluss vom 23./24.04.2009. Es gibt Anlass, die Problematik erneut aufzugreifen.

In den letzten Jahren ist insbesondere die Zollverwaltung im Rahmen der Bewilligung des zollrechtlichen Status eines „zugelassenen Wirtschaftsbeteiligten“ (AEO-Zertifizierungen) dazu übergegangen, von den Unternehmen umfangreiche Screenings von Mitarbeitern - und gegebenenfalls Daten Dritter - zu verlangen. Diese Screenings werden zum Teil in Abständen von wenigen Wochen ohne konkreten Anlass und undifferenziert durchgeführt. In diesem Geschäftsfeld betätigen sich bereits spezialisierte Dienstleister, die sich die bestehende Unsicherheit bei den Unternehmen zunutze machen. Dies ist auch der Grund, warum diese Screenings immer häufiger durchgeführt werden. Nach den praktischen Erfahrungen der Aufsichtsbehörden mangelt es an klaren Regelungen, wie mit den Ergebnissen von Datenscreenings umzugehen ist (Treffermanagement). Das Bundesministerium der Finanzen hat zwar am 14. Juni 2010 anlässlich dieser Praxis einschränkende Vorgaben erlassen, diese werden jedoch von den zuständigen Zollbehörden nicht einheitlich umgesetzt.

Der Düsseldorfer Kreis hält in seinem vorgenannten Beschluss derartige Screenings nur aufgrund einer speziellen Rechtsgrundlage für zulässig. Eine solche Rechtsgrundlage fehlt.

Weder die geltenden EU-Antiterrorverordnungen noch andere Sanktionslisten erfüllen die Anforderungen an eine solche spezielle Rechtsgrundlage. Diese Verordnungen enthalten lediglich die allgemeine Handlungspflicht, den in den Anlagen genannten Personen und Institutionen keine rechtlichen Vorteile zu gewähren, verpflichten jedoch nicht zu Screenings von Mitarbeitern, Kunden oder Lieferanten.

[1] http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf.

Auch die Bundesregierung ist der Auffassung, dass die Terrorismusverordnungen keinen systematischen, anlassunabhängigen Abgleich von Mitarbeiterdateien mit den Sanktionslisten verlangen. Allenfalls nach Maßgabe von Sorgfaltspflichten und differenzierend nach verschiedenen Verkehrskreisen und Risikolagen seien solche Abgleiche zulässig. Es bleibe den Unternehmen überlassen, wie sie die Einhaltung der Terrorismusverordnungen sicherstellen (Bundestags-Drucksache 17/4136 vom 03.12.2010).

Vor diesem Hintergrund empfiehlt und fordert der Düsseldorfer Kreis:

- Unternehmen sollten Datenscreenings nicht pauschal und anlasslos durchführen. Da die Lohnzahlung nur unbar erfolgt, die Kreditinstitute nach § 25c Kreditwesengesetz (KWG) ohnehin Abgleiche mit den Terrorlisten vornehmen, ist ein Datenabgleichverfahren innerhalb des Unternehmens mit Mitarbeiterdaten nicht geboten.
- Die Zollbehörden werden aufgefordert, die rechtsstaatlichen Vorgaben im Rahmen der AEO-Zertifizierung zu beachten. Eine einheitliche Praxis nach diesen Vorgaben gibt den Unternehmen Rechtssicherheit.
- Die Bundesregierung wird gebeten, die derzeitige AEO-Zertifizierungspraxis einer baldigen und umfassenden Evaluation zu unterziehen.

13.3.3 Anonymes und pseudonymes elektronisches Bezahlen von Internet-Angeboten ermöglichen!

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben zur Kenntnis genommen, dass zahlreiche Internet-Anbieter planen, ihre Geschäftsmodelle so umzustellen, dass ihre Angebote - insbesondere Informationsdienste und Medieninhalte - nicht mehr nur werbefinanziert, sondern auch gegen Bezahlung angeboten werden. Das darf nicht dazu führen, dass den Nutzern die Möglichkeit genommen wird, sich im Internet anonym zu bewegen und Inhalte zur Kenntnis zu nehmen, ohne dass sie sich identifizieren müssen.

Das Recht, sich möglichst anonym aus öffentlichen Quellen zu informieren, ist durch das Recht auf informationelle Selbstbestimmung und durch Artikel 5 GG (Recht auf Informationsfreiheit) verfassungsrechtlich geschützt. Dementsprechend ist in § 13 Abs. 6 Telemediengesetz vorgeschrieben, dass die Möglichkeit bestehen muss, Telemedien anonym oder unter Pseudonym zu nutzen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeiten zu informieren.

Diese Rechte sind in Gefahr, wenn Daten über die Nutzung einzelner Medienangebote entstehen. Wenn Inhalte gegen Bezahlung angeboten werden sollen, muss verhindert

werden, dass personenbeziehbare Daten über jeden einzelnen Abruf von Beiträgen aus Online-Zeitungen oder einzelner Sendungen im Internet-TV entstehen.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich fordern die Anbieter von Telemedien auf, ihren gesetzlichen Verpflichtungen aus § 13 Abs. 6 des Telemediengesetzes bei der Einführung von kostenpflichtigen Inhalten nachzukommen. Es muss ein Bezahlungsverfahren angeboten werden, das „auf der ganzen Linie“ anonym oder mindestens pseudonym ausgestaltet ist. Eine Zahlung über pseudonyme Guthabenkarten würde die datenschutzrechtlichen Anforderungen erfüllen. Es reicht dagegen nicht aus, wenn sich z. B. der Inhalteanbieter für die Abwicklung der Zahlverfahren eines Dritten bedient und dieser eine Identifizierung der Betroffenen verlangt.

Die Kreditwirtschaft hat es bisher versäumt, datenschutzgerechte Verfahren mit ausreichender Breitenwirkung anzubieten oder zu unterstützen. Die Aufsichtsbehörden fordern diese auf, zu überprüfen, inwieweit bereits im Umlauf befindliche elektronische Zahlungsmittel (wie z. B. die Geldkarte) zu einem zumindest pseudonymen Zahlungsmittel für Telemedien weiterentwickelt werden können. Dies könnte z. B. durch die Ausgabe nicht personengebundener „White Cards“ erfolgen, die über Einzahlungsautomaten bei Banken und anderen Kreditinstituten anonym aufgeladen werden können.

Schließlich nehmen die Aufsichtsbehörden mit Sorge zur Kenntnis, dass ein aktueller Gesetzentwurf der Bundesregierung zum Geldwäschegesetz (BT-Drs. 17/6804) die Gefahr birgt, dass das anonyme elektronische Bezahlen gesetzlich unterbunden wird. Die Intention des Telemediengesetzes, die pseudonyme bzw. anonyme Nutzung von Telemedien zu ermöglichen, würde zunichte gemacht. Die Aufsichtsbehörden unterstützen die Forderung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München, die Möglichkeit zum elektronischen anonymen Bezahlen insbesondere für Kleinbeträge (sog. „Micropayment“) zu erhalten.[1]

13.4 Beschluss des Düsseldorfer Kreises vom 8. Dezember 2011

13.4.1 Datenschutz in sozialen Netzwerken

Der Düsseldorfer Kreis sieht die Bemühungen von Betreibern von sozialen Netzwerken als Schritt in die richtige Richtung an, durch Selbstverpflichtungen den Datenschutz von Betroffenen zu verbessern. Er unterstreicht, dass eine Anerkennung von Selbstverpflichtungen durch die Datenschutzaufsichtsbehörden gemäß § 38a Bundesdatenschutzgesetz

[1] vgl. Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München: „Anonymes elektronisches Bezahlen muss möglich bleiben!“

(BDSG) die Gewähr dafür bietet, dass die Anforderungen des geltenden Datenschutzrechts erfüllt werden und ein Datenschutzmehrwert entsteht.

Ungeachtet dieser allgemeinen Bemühungen um eine Verbesserung des Datenschutzes in sozialen Netzwerken müssen die Betreiber schon heute das Datenschutzrecht in Deutschland beachten. Für deutsche Betreiber ist dies unumstritten. Aber auch Anbieter, die außerhalb des Europäischen Wirtschaftsraumes ansässig sind, unterliegen hinsichtlich der Daten von Betroffenen in Deutschland gemäß § 1 Abs. 5 Satz 2 BDSG dem hiesigen Datenschutzrecht, soweit sie ihre Datenerhebungen durch Rückgriff auf Rechner von Nutzerinnen und Nutzern in Deutschland realisieren. Dies ist regelmäßig der Fall. Die Anwendung des BDSG kann in diesen Fällen nicht durch das schlichte Gründen einer rechtlich selbstständigen Niederlassung in einem anderen Staat des Europäischen Wirtschaftsraumes umgangen werden (§ 1 Abs. 5 Satz 1 BDSG). Nur wenn das soziale Netzwerk auch in der Verantwortung dieser europäischen Niederlassung betrieben wird, kann die Verarbeitung der Daten deutscher Nutzerinnen und Nutzer unter Umständen dem Datenschutzrecht eines anderen Staates im Europäischen Wirtschaftsraum unterliegen.

Betreiber von sozialen Netzwerken müssen insbesondere folgende Rechtmäßigkeitsanforderungen beachten, wenn sie in Deutschland aktiv sind:

- Es muss eine leicht zugängliche und verständliche Information darüber gegeben werden, welche Daten erhoben und für welche Zwecke verarbeitet werden. Denn nur eine größtmögliche Transparenz bei Abschluss des Vertrags über eine Mitgliedschaft bzw. informierte Einwilligungen gewährleisten die Wahrung des Rechts auf informationelle Selbstbestimmung. Die Voreinstellungen des Netzwerkes müssen auf dem Einwilligungsprinzip beruhen, jedenfalls soweit nicht der Zweck der Mitgliedschaft eine Angabe von Daten zwingend voraussetzt. Eine Datenverarbeitung zunächst zu beginnen und nur eine Widerspruchsmöglichkeit in den Voreinstellungen zu ermöglichen, ist nicht gesetzmäßig.
- Es muss eine einfache Möglichkeit für Betroffene geben, ihre Ansprüche auf Auskunft, Berichtigung und Löschung von Daten geltend zu machen. Grundvoraussetzung hierfür ist die Angabe von entsprechenden Kontaktdaten an leicht auffindbarer Stelle, damit die Betroffenen wissen, wohin sie sich wenden können.
- Die Verwertung von Fotos für Zwecke der Gesichtserkennung und das Speichern und Verwenden von biometrischen Gesichtserkennungsmerkmalen sind ohne ausdrückliche und bestätigte Einwilligung der abgebildeten Person unzulässig.
- Das Telemediengesetz erfordert jedenfalls pseudonyme Nutzungsmöglichkeiten in sozialen Netzwerken. Es enthält im Hinblick auf Nutzungsdaten - soweit keine

Einwilligung vorliegt - ein Verbot der personenbeziehbaren Profilbildung und die Verpflichtung, nach Beendigung der Mitgliedschaft sämtliche Daten zu löschen.

- Das direkte Einbinden von Social Plugins, beispielsweise von Facebook, Google+ oder Twitter, in Websites deutscher Anbieter, wodurch eine Datenübertragung an den jeweiligen Anbieter des Social Plugins ausgelöst wird, ist ohne hinreichende Information der Internetnutzerinnen und -nutzer und ohne ihnen die Möglichkeit zu geben, die Datenübertragung zu unterbinden, unzulässig.
- Die großen Mengen an teils auch sehr sensiblen Daten, die in sozialen Netzwerken anfallen, sind durch geeignete technisch-organisatorische Maßnahmen zu schützen. Anbieter müssen nachweisen können, dass sie solche Maßnahmen getroffen haben.
- Daten von Minderjährigen sind besonders zu schützen. Datenschutzfreundlichen Standardeinstellungen kommt im Zusammenhang mit dem Minderjährigenschutz besondere Bedeutung zu. Informationen über die Verarbeitung von Daten müssen auf den Empfängerhorizont von Minderjährigen Rücksicht nehmen und also auch für diese leicht verständlich sein.
- Betreiber, die außerhalb des Europäischen Wirtschaftsraumes ansässig sind, müssen gemäß § 1 Abs. 5 Satz 3 BDSG einen Inlandsvertreter bestellen, der Ansprechperson für die Datenschutzaufsicht ist.

In Deutschland ansässige Unternehmen, die durch das Einbinden von Social Plugins eines Netzwerkes auf sich aufmerksam machen wollen oder sich mit Fanpages in einem Netzwerk präsentieren, haben eine eigene Verantwortung hinsichtlich der Daten von Nutzerinnen und Nutzern ihres Angebots. Es müssen zuvor Erklärungen eingeholt werden, die eine Verarbeitung von Daten ihrer Nutzerinnen und Nutzer durch den Betreiber des sozialen Netzwerkes rechtfertigen können. Die Erklärungen sind nur dann rechtswirksam, wenn verlässliche Informationen über die dem Netzwerkbetreiber zur Verfügung gestellten Daten und den Zweck der Erhebung der Daten durch den Netzwerkbetreiber gegeben werden können.

Anbieter deutscher Websites, die in der Regel keine Erkenntnisse über die Datenverarbeitungsvorgänge haben können, die beispielsweise durch Social Plugins ausgelöst werden, sind regelmäßig nicht in der Lage, die für eine informierte Zustimmung ihrer Nutzerinnen und Nutzer notwendige Transparenz zu schaffen. Sie laufen Gefahr, selbst Rechtsverstöße zu begehen, wenn der Anbieter eines sozialen Netzwerkes Daten ihrer Nutzerinnen und Nutzer mittels Social Plugin erhebt. Wenn sie die über ein Plugin mögliche Datenverarbeitung nicht überblicken, dürfen sie daher solche Plugins nicht ohne weiteres in das eigene Angebot einbinden.

13.5 Beschluss des Düsseldorfer Kreises vom 17. Januar 2012

13.5.1 Einwilligungs- und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft

Der Düsseldorfer Kreis hat sich dafür eingesetzt, die Einwilligungs- und Schweigepflichtentbindungserklärungen in der Versicherungswirtschaft transparenter zu gestalten. Gemeinsam mit dem Gesamtverband der deutschen Versicherungswirtschaft e. V. haben die Datenschutzaufsichtsbehörden eine Mustererklärung erarbeitet. Die Versicherungsunternehmen sind aufgefordert, die bisherigen Einwilligungstexte zeitnah durch neue zu ersetzen, die der Mustererklärung entsprechen. Der Text lautet wie folgt:

Einwilligung in die Erhebung und Verwendung von Gesundheitsdaten und Schweigepflichtentbindungserklärung[a]

Die Regelungen des Versicherungsvertragsgesetzes, des Bundesdatenschutzgesetzes sowie anderer Datenschutzvorschriften enthalten keine ausreichenden Rechtsgrundlagen für die Erhebung, Verarbeitung und Nutzung von Gesundheitsdaten durch Versicherungen. Um Ihre Gesundheitsdaten für diesen Antrag und den Vertrag erheben und verwenden zu dürfen, benötigt die Versicherung XY[1] daher Ihre datenschutzrechtliche(n) Einwilligung(en). Darüber hinaus benötigt die Versicherung XY Ihre Schweigepflichtentbindungen, um Ihre Gesundheitsdaten bei schweigepflichtigen Stellen, wie z. B. Ärzten, erheben zu dürfen. Als Unternehmen der Lebensversicherung (Krankenversicherung)[2] benötigt die Versicherung XY Ihre Schweigepflichtentbindung ferner, um Ihre Gesundheitsdaten oder weitere nach § 203 Strafgesetzbuch geschützte Daten, wie z. B. die Tatsache, dass ein Vertrag mit Ihnen besteht, an andere Stellen, z. B. …[3] weiterleiten zu dürfen.

Die folgenden Einwilligungs- und Schweigepflichtentbindungserklärungen[4] sind für die Antragsprüfung sowie die Begründung, Durchführung oder Beendigung Ihres Versicherungsvertrages in der Versicherung XY unentbehrlich. Sollten Sie diese nicht abgeben, wird der Abschluss des Vertrages in der Regel nicht möglich sein.[5]

Die Erklärungen betreffen den Umgang mit Ihren Gesundheitsdaten und sonstiger nach § 203 StGB geschützter Daten

- durch die Versicherung XY [Versicherungsgesellschaft, mit der der Versicherungsvertrag abgeschlossen wird] selbst (unter 1.),
- im Zusammenhang mit der Abfrage bei Dritten (unter 2.),

[a] Der Text der Einwilligungs-/Schweigepflichtentbindungserklärung wurde 2011 mit den Datenschutzaufsichtsbehörden inhaltlich abgestimmt.

- bei der Weitergabe an Stellen außerhalb der Versicherung XY (unter 3.) und
- wenn der Vertrag nicht zustande kommt (unter 4.).

Die Erklärungen gelten für die von Ihnen gesetzlich vertretenen Personen wie Ihre Kinder, soweit diese die Tragweite dieser Einwilligung nicht erkennen und daher keine eigenen Erklärungen abgeben können.[6]

1. Erhebung, Speicherung und Nutzung der von Ihnen mitgeteilten Gesundheitsdaten durch die Versicherung XY

Ich willige ein, dass die Versicherung XY die von mir in diesem Antrag und künftig mitgeteilten Gesundheitsdaten erhebt, speichert und nutzt, soweit dies zur Antragsprüfung sowie zur Begründung, Durchführung oder Beendigung dieses Versicherungsvertrages erforderlich ist.

2. Abfrage von Gesundheitsdaten bei Dritten

2.1. Abfrage von Gesundheitsdaten bei Dritten zur Risikobeurteilung und zur Prüfung der Leistungspflicht[7]

Für die Beurteilung der zu versichernden Risiken kann es notwendig sein, Informationen von Stellen abzufragen, die über Ihre Gesundheitsdaten verfügen. Außerdem kann es zur Prüfung der Leistungspflicht erforderlich sein, dass die Versicherung XY die Angaben über Ihre gesundheitlichen Verhältnisse prüfen muss, die Sie zur Begründung von Ansprüchen gemacht haben oder die sich aus eingereichten Unterlagen (z. B. Rechnungen, Verordnungen, Gutachten) oder Mitteilungen z. B. eines Arztes oder sonstigen Angehörigen eines Heilberufs ergeben.

Diese Überprüfung erfolgt nur, soweit es erforderlich ist. Die Versicherung XY benötigt hierfür Ihre Einwilligung einschließlich einer Schweigepflichtentbindung für sich sowie für diese Stellen, falls im Rahmen dieser Abfragen Gesundheitsdaten oder weitere nach § 203 Strafgesetzbuch geschützte Informationen weitergegeben werden müssen.

Sie können diese Erklärungen bereits hier (I) oder später im Einzelfall (II) erteilen. Sie können Ihre Entscheidung jederzeit ändern. Bitte entscheiden Sie sich für eine der beiden nachfolgenden Möglichkeiten:

Möglichkeit I:

□ Ich willige ein, dass die Versicherung XY - soweit es für die Risikobeurteilung oder für die Leistungsfallprüfung erforderlich ist - meine Gesundheitsdaten bei Ärzten,

Pflegepersonen sowie bei Bediensteten von Krankenhäusern, sonstigen Krankenanstalten, Pflegeheimen, Personenversicherern, gesetzlichen Krankenkassen, Berufsgenossenschaften und Behörden[8] erhebt und für diese Zwecke verwendet.

Ich befreie die genannten Personen und Mitarbeiter der genannten Einrichtungen von ihrer Schweigepflicht, soweit meine zulässigerweise gespeicherten Gesundheitsdaten aus Untersuchungen, Beratungen, Behandlungen sowie Versicherungsanträgen und -verträgen aus einem Zeitraum von bis zu zehn Jahren[9] vor Antragstellung an die Versicherung XY übermittelt werden.

Ich bin darüber hinaus damit einverstanden, dass in diesem Zusammenhang - soweit erforderlich - meine Gesundheitsdaten durch die Versicherung XY an diese Stellen weitergegeben werden und befreie auch insoweit die für die Versicherung XY tätigen Personen von ihrer Schweigepflicht.

Ich werde vor jeder Datenerhebung nach den vorstehenden Absätzen unterrichtet, von wem und zu welchem Zweck die Daten erhoben werden sollen, und ich werde darauf hingewiesen, dass ich widersprechen und die erforderlichen Unterlagen selbst beibringen kann.10

Möglichkeit II:

□ Ich wünsche, dass mich die Versicherung XY in jedem Einzelfall informiert, von welchen Personen oder Einrichtungen zu welchem Zweck eine Auskunft benötigt wird. Ich werde dann jeweils entscheiden, ob ich

- in die Erhebung und Verwendung meiner Gesundheitsdaten durch die Versicherung XY einwillige, die genannten Personen oder Einrichtungen sowie deren Mitarbeiter von ihrer Schweigepflicht entbinde und in die Übermittlung meiner Gesundheitsdaten an die Versicherung XY einwillige
- oder die erforderlichen Unterlagen selbst beibringe.

Mir ist bekannt, dass dies zu einer Verzögerung der Antragbearbeitung oder der Prüfung der Leistungspflicht führen kann.

Soweit sich die vorstehenden Erklärungen auf meine Angaben bei Antragstellung beziehen, gelten sie für einen Zeitraum von fünf Jahren[11] nach Vertragsschluss. Ergeben sich nach Vertragsschluss für die Versicherung XY konkrete Anhaltspunkte[12] dafür, dass bei der Antragstellung vorsätzlich unrichtige oder unvollständige Angaben gemacht wurden und damit die Risikobeurteilung beeinflusst wurde, gelten die Erklärungen bis zu zehn Jahre nach Vertragsschluss.

2.2. Erklärungen für den Fall Ihres Todes

Zur Prüfung der Leistungspflicht kann es auch nach Ihrem Tod erforderlich sein, gesundheitliche Angaben zu prüfen. Eine Prüfung kann auch erforderlich sein, wenn sich bis zu zehn Jahre nach Vertragsschluss für die Versicherung XY konkrete Anhaltspunkte dafür ergeben, dass bei der Antragstellung unrichtige oder unvollständige Angaben gemacht wurden und damit die Risikobeurteilung beeinflusst wurde. Auch dafür bedürfen wir einer Einwilligung und Schweigepflichtentbindung. Bitte entscheiden Sie sich für eine der beiden nachfolgenden Möglichkeiten:[13]

Möglichkeit I:

□ Für den Fall meines Todes willige ich in die Erhebung meiner Gesundheitsdaten bei Dritten zur Leistungsprüfung bzw. einer erforderlichen erneuten Antragsprüfung ein wie im ersten Ankreuzfeld beschrieben (siehe oben 2.1. - Möglichkeit I).

Möglichkeit II:

□ Soweit zur Prüfung der Leistungspflicht bzw. einer erforderlichen erneuten Antragsprüfung nach meinem Tod Gesundheitsdaten erhoben werden müssen, geht die Entscheidungsbefugnis über Einwilligungen und Schweigepflichtentbindungserklärungen auf meine Erben oder - wenn diese abweichend bestimmt sind - auf die Begünstigten des Vertrags über.

3. Weitergabe Ihrer Gesundheitsdaten und weiterer nach § 203 StGB geschützter Daten an Stellen außerhalb der Versicherung XY

Die Versicherung XY verpflichtet die nachfolgenden Stellen vertraglich auf die Einhaltung der Vorschriften über den Datenschutz und die Datensicherheit.[14]

3.1. Datenweitergabe zur medizinischen Begutachtung

Für die Beurteilung der zu versichernden Risiken und zur Prüfung der Leistungspflicht kann es notwendig sein, medizinische Gutachter einzuschalten. Die Versicherung XY benötigt Ihre Einwilligung und Schweigepflichtentbindung, wenn in diesem Zusammenhang Ihre Gesundheitsdaten und weitere nach § 203 StGB geschützte Daten übermittelt werden. Sie werden über die jeweilige Datenübermittlung unterrichtet.[15]

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten an medizinische Gutachter übermittelt, soweit dies im Rahmen der Risikoprüfung oder der Prüfung der Leistungspflicht erforderlich ist und meine Gesundheitsdaten dort zweckentsprechend verwendet und die Ergebnisse an die Versicherung XY zurück übermittelt werden. Im

Hinblick auf meine Gesundheitsdaten und weitere nach § 203 StGB geschützte Daten entbinde ich die für die Versicherung XY tätigen Personen und die Gutachter von ihrer Schweigepflicht.

3.2. Übertragung von Aufgaben auf andere Stellen (Unternehmen oder Personen)

Die Versicherung XY führt bestimmte Aufgaben, wie zum Beispiel die Risikoprüfung, die Leistungsfallbearbeitung oder die telefonische Kundenbetreuung, bei denen es zu einer Erhebung, Verarbeitung oder Nutzung Ihrer Gesundheitsdaten kommen kann, nicht selbst durch, sondern überträgt die Erledigung einer anderen Gesellschaft der XY-Gruppe oder einer anderen Stelle. Werden hierbei Ihre nach § 203 StGB geschützten Daten weitergegeben, benötigt die Versicherung XY Ihre Schweigepflichtentbindung für sich und[16] soweit erforderlich für die anderen Stellen.[17]

Die Versicherung XY führt eine fortlaufend aktualisierte Liste[18] über die Stellen[19] und Kategorien von Stellen[20], die vereinbarungsgemäß Gesundheitsdaten für die Versicherung XY erheben, verarbeiten oder nutzen unter Angabe der übertragenen Aufgaben. Die zurzeit gültige Liste ist als Anlage der Einwilligungserklärung angefügt.[21] Eine aktuelle Liste kann auch im Internet unter (*Internetadresse*) eingesehen oder bei (*Ansprechpartner nebst Anschrift, Telefonnummer, ggf. E-Mailadresse*) angefordert werden. Für die Weitergabe Ihrer Gesundheitsdaten an und die Verwendung durch die in der Liste genannten Stellen benötigt die Versicherung XY Ihre Einwilligung.

Ich willige ein,[22] dass die Versicherung XY meine Gesundheitsdaten an die in der oben erwähnten Liste genannten Stellen übermittelt und dass die Gesundheitsdaten dort für die angeführten Zwecke im gleichen Umfang erhoben, verarbeitet und genutzt werden, wie die Versicherung XY dies tun dürfte. Soweit erforderlich, entbinde ich die Mitarbeiter der XY Unternehmensgruppe und sonstiger Stellen[23] im Hinblick auf die Weitergabe von Gesundheitsdaten und anderer nach § 203 StGB geschützter Daten von ihrer Schweigepflicht.

3.3. Datenweitergabe an Rückversicherungen

Um die Erfüllung Ihrer Ansprüche abzusichern, kann die Versicherung XY Rückversicherungen einschalten, die das Risiko ganz oder teilweise übernehmen. In einigen Fällen bedienen sich die Rückversicherungen dafür weiterer Rückversicherungen, denen sie ebenfalls Ihre Daten[24] übergeben. Damit sich die Rückversicherung ein eigenes Bild über das Risiko oder den Versicherungsfall machen kann, ist es möglich, dass die Versicherung XY Ihren Versicherungsantrag oder Leistungsantrag der Rückversicherung

vorlegt. Das ist insbesondere dann der Fall, wenn die Versicherungssumme besonders hoch ist oder es sich um ein schwierig einzustufendes Risiko handelt.

Darüber hinaus ist es möglich, dass die Rückversicherung die Versicherung XY aufgrund ihrer besonderen Sachkunde bei der Risiko- oder Leistungsprüfung sowie bei der Bewertung von Verfahrensabläufen unterstützt.

Haben Rückversicherungen die Absicherung des Risikos übernommen, können sie kontrollieren, ob die Versicherung XY das Risiko bzw. einen Leistungsfall richtig eingeschätzt hat.

Außerdem werden Daten über Ihre bestehenden Verträge und Anträge im erforderlichen Umfang an Rückversicherungen weitergegeben, damit diese überprüfen können, ob und in welcher Höhe sie sich an dem Risiko beteiligen können.[25] Zur Abrechnung von Prämienzahlungen und Leistungsfällen können Daten über Ihre bestehenden Verträge an Rückversicherungen weitergegeben werden.

Zu den oben genannten Zwecken werden möglichst anonymisierte bzw. pseudonymisierte Daten, jedoch auch personenbezogene Gesundheitsangaben verwendet.

Ihre personenbezogenen Daten werden von den Rückversicherungen nur zu den vorgenannten Zwecken verwendet. Über die Übermittlung Ihrer Gesundheitsdaten an Rückversicherungen werden Sie durch die Versicherung XY unterrichtet.[26]

Ich willige ein, dass meine Gesundheitsdaten - soweit erforderlich - an Rückversicherungen übermittelt und dort zu den genannten Zwecken verwendet werden. Soweit erforderlich, entbinde ich die für die Versicherung XY tätigen Personen im Hinblick auf die Gesundheitsdaten und weiteren nach § 203 StGB geschützter Daten von ihrer Schweigepflicht.

3.4. Datenaustausch mit dem Hinweis- und Informationssystem (HIS)[27]

Die Versicherungswirtschaft nutzt zur genaueren Risiko- und Leistungsfalleinschätzung das Hinweis- und Informationssystem HIS, das derzeit die informa Insurance Risk and Fraud Prevention GmbH (informa IRFP GmbH, Rheinstraße 99, 76532 Baden-Baden, www.informa-irfp.de) betreibt. Auffälligkeiten, die auf Versicherungsbetrug hindeuten könnten, und erhöhte Risiken kann die Versicherung XY an das HIS melden. Die Versicherung XY und andere Versicherungen fragen Daten im Rahmen der Risiko- oder Leistungsprüfung aus dem HIS ab, wenn ein berechtigtes Interesse besteht.[28] Zwar werden dabei keine Gesundheitsdaten weitergegeben, aber für eine Weitergabe Ihrer nach § 203 StGB geschützten Daten benötigt die Versicherung XY Ihre Schweige-

pflichtentbindung. Dies gilt unabhängig davon, ob der Vertrag mit Ihnen zustande gekommen ist oder nicht.

Ich entbinde die für Versicherung XY tätigen Personen von ihrer Schweigepflicht, soweit sie Daten aus der Antrags- oder Leistungsprüfung an den jeweiligen Betreiber des Hinweis- und Informationssystems (HIS)[29] melden.

Sofern es zur Prüfung der Leistungspflicht erforderlich ist, können über das HIS Versicherungen ermittelt werden, mit denen Sie in der Vergangenheit in Kontakt gestanden haben, und die über sachdienliche Informationen verfügen könnten. Bei diesen können die zur weiteren Leistungsprüfung erforderlichen Daten erhoben werden (siehe unter Ziff. 2.1).

3.5. Datenweitergabe an selbstständige Vermittler

Die Versicherung XY gibt grundsätzlich keine Angaben zu Ihrer Gesundheit an selbstständige Vermittler weiter. Es kann aber in den folgenden Fällen dazu kommen, dass Daten, die Rückschlüsse auf Ihre Gesundheit zulassen, oder gemäß § 203 StGB geschützte Informationen über Ihren Vertrag Versicherungsvermittlern zur Kenntnis gegeben werden.

Soweit es zu vertragsbezogenen Beratungszwecken erforderlich ist, kann der Sie betreuende Vermittler Informationen darüber erhalten, ob und ggf. unter welchen Voraussetzungen (z. B. Annahme mit Risikozuschlag, Ausschlüsse bestimmter Risiken) Ihr Vertrag angenommen werden kann.

Der Vermittler, der Ihren Vertrag vermittelt hat, erfährt, dass und mit welchem Inhalt der Vertrag abgeschlossen wurde. Dabei erfährt er auch, ob Risikozuschläge oder Ausschlüsse bestimmter Risiken vereinbart wurden.

Bei einem Wechsel des Sie betreuenden Vermittlers auf einen anderen Vermittler kann es zur Übermittlung der Vertragsdaten mit den Informationen über bestehende Risikozuschläge und Ausschlüsse bestimmter Risiken an den neuen Vermittler kommen. Sie werden bei einem Wechsel des Sie betreuenden Vermittlers auf einen anderen Vermittler vor der Weitergabe von Gesundheitsdaten informiert sowie auf Ihre Widerspruchsmöglichkeit hingewiesen.

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten und sonstigen nach § 203 StGB geschützten Daten in den oben genannten Fällen - soweit erforderlich - an den für mich zuständigen selbstständigen Versicherungsvermittler übermittelt und diese dort erhoben, gespeichert und zu Beratungszwecken genutzt werden dürfen.

4. Speicherung und Verwendung Ihrer Gesundheitsdaten wenn der Vertrag nicht zustande kommt[30]

Kommt der Vertrag mit Ihnen nicht zustande, speichert die Versicherung XY Ihre im Rahmen der Risikoprüfung erhobenen Gesundheitsdaten für den Fall, dass Sie erneut Versicherungsschutz beantragen. Außerdem ist es möglich, dass die Versicherung XY zu Ihrem Antrag einen Vermerk an das Hinweis- und Informationssystem meldet, der an anfragende Versicherungen für deren Risiko- und Leistungsprüfung übermittelt wird (siehe Ziffer 3.4.). Die Versicherung XY speichert Ihre Daten auch, um mögliche Anfragen weiterer Versicherungen beantworten zu können. Ihre Daten werden bei der Versicherung XY und im Hinweis- und Informationssystem bis zum Ende des dritten Kalenderjahres nach dem Jahr der Antragstellung[31] gespeichert.

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten - wenn der Vertrag nicht zustande kommt - für einen Zeitraum von drei Jahren ab dem Ende des Kalenderjahres der Antragstellung zu den oben genannten Zwecken speichert und nutzt.[32]

Ort, Datum	Unterschrift Antragsteller/in oder mitzuversichernde Person
Ort, Datum	Unterschrift gesetzlich vertretene Person (bei Vorliegen der erforderlichen Einsichtsfähigkeit, frühestens ab Vollendung des 16. Lebensjahres)
Ort, Datum	Unterschrift des gesetzlichen Vertreters

Hinweise zur Anwendung der Einwilligungs- und Schweigepflichtentbindungserklärung für die Erhebung und Verwendung von Gesundheitsdaten und sonstiger nach § 203 StGB geschützter Daten

Der vorliegende Text einer Einwilligungs- und Schweigepflichtentbindungsklausel ist vom GDV mit den Datenschutzaufsichtsbehörden abgestimmt worden. Der Verbraucherzentrale Bundesverband war ebenfalls an den Gesprächen beteiligt. Die Klausel

wird flankiert durch Verhaltensregeln für den Umgang mit personenbezogenen Daten in der Versicherungswirtschaft (Code of Conduct). Zweck ist, lediglich für die tatsächlich einwilligungsbedürftigen Datenerhebungs- und -verwendungsprozesse eine Einwilligungs- und Schweigepflichtentbindungserklärung einzuholen. Andere Datenverarbeitungen werden in einem Code of Conduct konkretisiert. Sowohl die Klausel als auch der Code of Conduct werden in regelmäßigen Abständen gemeinsam überarbeitet, um aktuelle Entwicklungen der Datenverarbeitung und gesetzliche Änderungen zu berücksichtigen.

Hinweise zur Klausel - BAUSTEINSYSTEM

Die Texte stellen einen maximalen Rahmen für Einwilligungs- und Schweigepflichtentbindungserklärungen dar. Wegen des im BDSG verankerten Prinzips der Datensparsamkeit sind nur die Textpassagen zu verwenden, die benötigt werden. Soweit im Rahmen einer Versicherungssparte oder eines Versicherungsprodukts bestimmte Datenverarbeitungen nicht erfolgen, wie etwa die Erhebung von Gesundheitsdaten bei Dritten zur Risikoprüfung, ist der Text entsprechend zu kürzen. Werden Datenverarbeitungen beschrieben, die das Unternehmen nicht durchführt oder nicht plant, wie zum Beispiel die Datenweitergabe zur medizinischen Begutachtung oder die Datenweitergabe an Rückversicherer, ist der entsprechende Absatz / Satz nicht zu verwenden.

Zu beachten ist dabei jedoch, dass die in Abschnitt 2.1. angebotenen Wahlmöglichkeiten bestehen bleiben müssen. Das heißt, wenn für die Datenerhebung bei Dritten mit dem Antrag eine Einwilligung eingeholt werden soll, müssen auch beide Alternativen (Pauschaleinwilligung / Einzelfalleinwilligung) angeboten werden. Erfolgt keine Wahl, muss spätestens unmittelbar vor der Datenerhebung eine Einwilligung eingeholt werden. Die dafür zu gestaltenden Erklärungen sollten sich an den hier vorliegenden orientieren.

Die vorliegende Einwilligungs- und Schweigepflichtentbindungsklausel bezieht sich auf Gesundheitsdaten und darüber hinaus auf weitere nach § 203 Abs. 1 StGB geschützte Daten, wie die Tatsache des Bestehens eines Versicherungsvertrags. Gesundheitsdaten können in allen Versicherungssparten anfallen, auch dort, wo dies nicht sofort vermutet wird, z. B. in der Reisegepäckversicherung (Verletzungen durch Raub) und in der Kfz-Versicherung (Verletzungen durch Unfall). Die Einwilligungs- und Schweigepflichtentbindungserklärungen müssen vor der jeweils ersten Verarbeitung von Gesundheitsdaten im Unternehmen dem Antragsteller bzw. Versicherungsnehmer vorgelegt werden, soweit sie für bevorstehende Datenerhebungen, -verarbeitungen oder -nutzungen benötigt werden.

Sollen andere besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG erhoben, verarbeitet oder genutzt werden, wie bspw. die Information über eine Gewerkschaftszugehörigkeit zur Prämienberechnung in speziellen Tarifen gewerkschaftsnaher Unternehmen, ist mit dem betreffenden Antrag eine entsprechende Einwilligungserklärung vom Antragsteller einzuholen. Diese kann z. B. wie folgt formuliert und gestaltet werden:

Ich willige in die Erhebung, Verarbeitung und Nutzung meiner Angaben zur Gewerkschaftszugehörigkeit ein, soweit dies zur Antragsprüfung sowie zur Begründung, Durchführung oder Beendigung dieses Vertrages, insbesondere zur Berechnung meiner Versicherungsprämie, erforderlich ist.

---

[1] Hier und im Folgenden kann anstelle von „die Versicherung XY“ der Name des verwendenden Unternehmens oder nach einmaliger Nennung (etwa „wir, die Versicherung XY“) jeweils „wir“ eingefügt werden.

[2] Hier kann die konkrete Sparte genannt werden.

[3] Das Beispiel soll verdeutlichen, dass Versicherer diese Daten nicht willkürlich an x-beliebige Stellen weitergeben. Daher können hier einige für die verwendende Versicherung typische Beispiele genannt werden, die die Breite der Weitergabemöglichkeiten erkennen lassen, wie z. B. Assistancegesellschaften, HIS-Betreiber oder IT-Dienstleister.

[4] Die Klausel ist zunächst nur für Kranken-, Lebens- und Berufsunfähigkeitsversicherungen zu verwenden, weil in diesen Sparten von Vertragsbeginn an Gesundheitsdaten erhoben und verwendet werden. In anderen Sparten ist der Text entsprechend anzupassen und ggf. nur auszugsweise zu verwenden. In Abstimmung mit den Sparten Unfall und Haftpflicht wird den Unternehmen ein angepasster Vorschlag zur Verfügung gestellt.

[5] Verweis auf die Folgen der Verweigerung der Einwilligung gemäß § 4a Abs. 1 Satz 2 BDSG.

[6] Werden bei einem Versicherungsprodukt generell keine Kinder und / oder gesetzlich vertretende Personen mitversichert, ist der Absatz bzw. der entsprechende Satz zu streichen. Werden Kinder oder andere gesetzlich vertretene Personen mitversichert, unterschreiben diese ab dem 16. Lebensjahr eine eigene Erklärung, wenn davon auszugehen ist, dass diese einsichtsfähig sind. Diese Erklärung ist aus zivilrechtlichen Gründen auch vom gesetzlichen Vertreter (in der Regel dem Versicherungsnehmer) zu unterzeichnen

(siehe unten, Unterschriftenfelder). Damit verbleibt die Entscheidung über das tatsächliche Bestehen der Einsichtsfähigkeit bei dem gesetzlichen Vertreter.

7 Wenn Unternehmen stets eine Einwilligung im Einzelfall einholen, wird Ziffer 2.1 gestrichen und der Erläuterungstext über dem grauen Kasten wird für die Einzelfalleinwilligung entsprechend angepasst.

8 Der 2008 in Kraft getretene § 213 VVG führt enumerativ die Stellen auf, bei denen der Versicherer mit Einwilligung des Betroffenen dessen Gesundheitsdaten erheben darf. Hinsichtlich der fehlenden sonstigen Heilberufe (Heilpraktiker, Physiotherapeut, Psychotherapeut) sowie der Versicherer, die keine Personenversicherer im herkömmlichen Sprachgebrauch sind, aber dennoch zur Regulierung von Personenschäden Gesundheitsdaten verarbeiten, wird § 213 VVG weit ausgelegt, vgl. auch Eberhardt in: Münchener Kommentar, § 213 VVG, Rn. 35-40.

9 Entsprechend der Annahmepolitik der Versicherungsunternehmen kann für alle oder bestimmte Antragsfragen ein kürzerer Zeitraum zugrunde gelegt werden.

10 Umsetzung der Unterrichtungs- und Hinweispflicht nach § 213 Abs. 2 Satz 2 i. V. m. Abs. 4 VVG.

11 Bei der privaten Krankenversicherung ist wegen § 194 Abs. 1 Satz 4 VVG eine Frist von drei Jahren einzusetzen. Bei vorsätzlichem Verhalten gilt auch für die PKV die Zehn-Jahresfrist.

12 Anhaltspunkte für vorsätzlich falsche Angaben können sich etwa aus Unstimmigkeiten zwischen der Erkrankung und den Angaben im Antrag ergeben. Eine Überprüfung kann dann ergeben, dass es am Vorsatz fehlt und die Datenerhebung für den Betroffenen keine negativen Konsequenzen hat.

13 Bei Abschnitt 2.2 ist es möglich, das zweite Ankreuzfeld nicht zu nutzen, sodass keine Wahlmöglichkeit besteht und nur das erste Feld angekreuzt werden kann. Der letzte erläuternde Satz vor dem grau unterlegten Feld entfällt dann. Wird das erste (einzige) Ankreuzfeld dann nicht angekreuzt, würde bei einer gerichtlichen Prüfung entweder eine andere Willenserklärung herangezogen (z.B. Testament) oder bei Fehlen einer solchen auf den mutmaßlichen Willen des Betroffenen abgestellt. Ein automatischer Übergang der höchstpersönlichen Verfügungsbefugnis auf Erben oder Bezugsberechtigte des Vertrags erfolgt regelmäßig nicht. Bei Anbieten einer echten Wahlmöglichkeit und einem vorliegenden Kreuz erscheint der Bestand der Erklärungen vor Gericht als wahrscheinlicher, sodass die Bezugnahme auf den mutmaßlichen Willen in einem möglichen Zivilprozess nicht nötig erscheint.

14 Die vertragliche Verpflichtung auf Einhaltung von Datenschutz und Datensicherheit auch für Stellen, die eigenverantwortlich Aufgaben übernehmen, ergibt sich aus dem künftigen Art. 21 Abs. 4 Code of Conduct (CoC). Diese Verpflichtung wurde dort für die Funktionsübertragung an Dienstleister als datenschutzrechtlicher Mehrwert für die Betroffenen vereinbart. Rückversicherer werden nicht als Dienstleister des Erstversicherers im Sinne von Art. 21 angesehen, wenn sie den Erstversicherer im Rahmen von Rückversicherungsverträgen bei der Risiko- und Leistungsprüfung unterstützen. Sofern der Erstversicherer Rückversicherer außerhalb von Rückversicherungsverträgen als Dienstleister einsetzt und diese noch nicht vertraglich auf die Einhaltung von Datenschutz und Datensicherheit verpflichtet hat, ist dies nachzuholen (vgl. auch Hinweis 18).

15 Die Unterrichtungspflicht wurde aufgenommen, um mehr Transparenz zu schaffen. Hierfür ist mitzuteilen, welche konkreten Daten, für welchen Zweck, an welche Stelle übermittelt werden sollen.

16 Der Satzteil “für sich und” ist nur für die Kranken, Lebens- und Unfallversicherung zu verwenden.

17 Die Mitarbeiter anderer Stellen werden von ihrer Schweigepflicht entbunden, wenn sie ihrerseits im Rahmen der von ihnen zu erledigenden Aufgaben nach § 203 StGB geschützte Daten an den Versicherer oder an andere Stellen, wie z. B. mit der IT-Wartung beauftragte Subunternehmen weitergeben.

18 In der Liste werden die Stellen und Kategorien von Stellen aufgezählt, die Gesundheitsdaten erheben, verarbeiten oder nutzen. Ebenfalls gemeint sind Stellen und Kategorien von Stellen, die einfache personenbezogene Daten, die nach § 203 StGB geschützt sind, wie z. B. die Information, dass ein Lebensversicherungsvertrag besteht, verwenden. Nicht gemeint sind Stellen, die im Rahmen der ihnen zugewiesenen Aufgaben keine Gesundheitsdaten verarbeiten, diese aber theoretisch einsehen können (Bspw. Personen oder Unternehmen, die mit der IT-Wartung betraut sind). In die Liste werden sowohl Dritte im datenschutzrechtlichen Sinn als auch Auftragsdatenverarbeiter, bei denen Abgrenzungsschwierigkeiten zur Funktionsübertragung bestehen (siehe Endnote 23), aufgenommen. Rückversicherer werden als Dienstleister des Erstversicherers angesehen, wenn sie ohne einen Rückversicherungsvertrag nur als Dienstleister des Erstversicherers tätig werden.

19 Werden Aufgaben im Wesentlichen von einem Unternehmen an ein anderes Unternehmen der XY-Versicherungsgruppe oder an eine externe Stelle abgegeben, ist die andere Stelle namentlich anzugeben unter Bezeichnung der Aufgabe. Hierunter fallen

z. B. Stellen, die die Aufgaben Risikoprüfung, Leistungsfallbearbeitung oder Serviceleistung für das Unternehmen übernehmen.

20 Fehlt es an einer systematischen automatisierten Datenverarbeitung, können die Stellen, an die Gesundheitsdaten weitergegeben werden bzw. die zur Erfüllung ihrer Aufgabe selbst Gesundheitsdaten erheben, in Kategorien zusammengefasst werden unter Bezeichnung der Aufgabe. Dies gilt auch für Stellen, die nur einmalig tätig werden, wie z. B. Krankentransporte.

21 Die Liste der Dienstleister soll in der Form, in der die Einwilligungs- und Schweigepflichtentbindungserklärung erteilt wird, als Anlage mitgegeben werden.

22 Die Einwilligung gilt in jedem Fall für die Datenübermittlung an eigenverantwortliche Dienstleister. Sie ist außerdem bei Abgrenzungsschwierigkeiten zwischen Auftragsdatenverarbeitung und Funktionsübertragung einzuholen. Das Einwilligungserfordernis gilt nicht, wenn es sich in Übereinstimmung mit der zuständigen Datenschutzaufsichtsbehörde um eine eindeutige Auftragsdatenverarbeitung handelt. In diesen Fällen sollte dennoch eine Schweigepflichtentbindung eingeholt werden.

23 „und sonstige Stellen“ - Dieser Passus wird gestrichen, wenn keine schweigepflichtgebundenen Dienstleister und Auftragnehmer eingeschaltet sind.

24 Sollen Gesundheitsdaten an den Rückversicherer des Rückversicherers übermittelt werden, ist eine spezielle Einwilligung zu prüfen.

25 Für die Kumulkontrolle ist eine Schweigepflichtentbindung erforderlich, da nach § 203 StGB geschützte Daten weitergegeben werden, jedoch keine Gesundheitsdaten.

26 Die Unterrichtungspflicht des Erstversicherers ersetzt die anderenfalls von den Datenschutzbehörden geforderte ausführliche Erklärung entsprechend dem Baustein 2.1. zur Erhebung von Gesundheitsdaten bei Dritten. Zu unterrichten ist über die konkret übermittelten Daten, den Zweck der Übermittlung und den Empfänger der Daten.

27 Da keine einwilligungsbedürftigen besonderen Arten personenbezogener Daten nach § 3 Abs. 9 BDSG (Gesundheitsdaten) an das HIS gemeldet werden, betrifft die Schweigepflichtentbindung nur die nach § 203 StGB geschützten Daten, hier etwa die Tatsache, dass ein Versicherungsvertrag besteht. Da nur die Sparten Unfall und Leben von § 203 Abs. 1 Nr. 6 StGB erfasst werden und mit dem HIS arbeiten, ist der Passus für die anderen Sparten zu streichen. Im Fall der Nutzung ist die Information des Versicherungsnehmers über das Hinweis- und Informationssystem dann in anderer Weise sicher-

zustellen. Soweit Gesundheitsdaten im Leistungsfall im Rahmen der Detailanfrage ausgetauscht werden, gelten die Einwilligungserklärungen unter 2.1.

28 Ein berechtigtes Interesse für die Abfrage zum Zweck der Risiko- und Leistungsprüfung ist stets gegeben mit Ausnahme des Erlebensfalls in der Lebensversicherung.

29 Durch die Formulierung „an den jeweiligen Betreiber“ sowie die Aufnahme von „derzeit“ im ersten Satz des erläuternden Textes wird deutlich gemacht, dass sich der Betreiber des HIS ändern kann. Die Schweigepflichtentbindungserklärung soll auch künftige Betreiber erfassen.

30 Der Passus ist zu streichen, wenn eine Speicherung von Antragsdaten bei Nichtzustandekommen des Vertrags nicht erfolgt. Daten über nicht zustande gekommene Verträge sind bei dem Versicherungsunternehmen spätestens drei Jahre gerechnet vom Ende des Kalenderjahres nach Antragstellung zu löschen. Auch im Hinweis- und Informationssystem werden diese Daten entsprechend gelöscht. Gesetzliche Aufbewahrungspflichten oder -befugnisse bleiben hiervon unberührt. Werden Schadensersatzansprüche gegen das Unternehmen geltend gemacht oder bei Prüfungen durch Behörden kann sich eine längere Aufbewahrung auch aus § 28 Abs. 6 Nr. 3 BDSG rechtfertigen.

31 Es zählt das Datum der Unterschrift im Antrag.

32 Die Nutzung ist nur zu eigenen Zwecken des Versicherers zulässig. Die Übermittlung an ein anderes Unternehmen ist nur auf der Basis einer von diesem einzuholenden Einwilligung/ Schweigepflichtentbindung nach Ziffer 2.1. zulässig.

13.6 Beschluss des Düsseldorfer Kreises vom 18./19. September 2012

13.6.1 Near Field Communication (NFC) bei Geldkarten

Es ist datenschutzrechtlich problematisch, wenn beim Einsatz von Near Field Communication (NFC) bei Geldkarten eine eindeutige Kartennummer, Geldbeträge und Transaktionshistorien unverschlüsselt von unberechtigten Dritten auslesbar sind. Die Geldkartenanbieter haben gemäß § 9 BDSG im Rahmen der Verhältnismäßigkeit mit angemessenen technisch-organisatorischen Maßnahmen dafür zu sorgen, dass Dritten kein unberechtigtes Auslesen von Daten möglich wird.

Datenschutzrechtlich erstrebenswert ist die Einräumung einer Wahlmöglichkeit für die Betroffenen, ob sie eine Geldkarte mit NFC-Funktionalität einsetzen wollen. Insoweit nehmen die Aufsichtsbehörden die Ankündigung der Deutschen Kreditwirtschaft zur Kenntnis, das Kartenbetriebssystem so bald wie möglich so zu ändern, dass die Betroffenen die NFC-Funktionalität ein- und ausschalten können. Die Gefahr des (unbe-

merkten) unberechtigten Auslesens der Transaktionsdaten durch Dritte kann auch dadurch verringert werden, dass insofern nur das kontaktbehaftete Auslesen der Daten zugelassen wird.

Zudem sind die Vorgaben des § 6c BDSG zu beachten. Die Betroffenen müssen ausreichend informiert werden, insbesondere über die Funktionsweise des Mediums, die per NFC auslesbaren Daten, die Schutzmöglichkeiten für die Daten und ihre Rechte als Betroffene nach den §§ 34 und 35 BDSG.

13.7 Beschluss des Düsseldorfer Kreises vom 26./27. Februar 2013

13.7.1 Videoüberwachung in und an Taxis

Leben, Gesundheit und Freiheit der Taxifahrer sind hohe Rechtsgüter, die es nachhaltig zu schützen gilt. Zu diesem Zweck kann auch der Einsatz von Videokameras in Betracht kommen. Allerdings müssen die Persönlichkeitsrechte der Fahrgäste, der angestellten Taxifahrer sowie anderer Verkehrsteilnehmer gewahrt bleiben. Der Einsatz von Videokameras muss daher unter Würdigung der berechtigten Sicherheitsinteressen und schutzwürdigen Belange aller Betroffenen auf das erforderliche Mindestmaß beschränkt bleiben.

Die Zulässigkeit einer Videoüberwachung durch Taxi-Unternehmen bestimmt sich nach § 6b Bundesdatenschutzgesetz (BDSG). Gemäß § 6b Abs. 1 Nr. 3, Abs. 3 BDSG ist eine Beobachtung und Aufzeichnung mittels Videokameras nur zulässig, soweit dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

1. Innenkameras

Das betroffene Taxi-Unternehmen muss als verantwortliche Stelle vorrangig alternative und weniger einschneidende Schutzmaßnahmen berücksichtigen, bevor eine Videoüberwachung erwogen werden kann. In Betracht zu ziehen sind beispielsweise die Möglichkeit der anlassbezogenen Auslösung eines „stillen Alarms“ oder eines GPS-gestützten Notrufsignals.

Taxifahrern kann die Möglichkeit eröffnet werden, die Videoaufzeichnung selbsttätig (z. B. über einen Schalter) zu aktivieren, wenn nach ihrer eigenen Einschätzung eine bedrohliche Situation gegeben ist und es mithin einen Anlass für die Aufzeichnung gibt.

Eine anlasslose Videoüberwachung, die ohne Einflussnahmemöglichkeit des Fahrers generell und automatisch einsetzt und bei der sowohl die Fahrgäste als auch das ge-

samte Geschehen im Fahrgastbereich permanent aufgezeichnet werden, ist weder erforderlich noch verhältnismäßig. Unter Berücksichtigung sowohl der Sicherheitsinteressen des Fahrpersonals als auch der Persönlichkeitsrechte der betroffenen Fahrgäste ist die Videoaufzeichnung vielmehr in der Regel auf das Anfertigen einzelner Standbilder der Fahrgäste beim Einsteigen zu beschränken.

Soweit Bilder zulässigerweise aufgezeichnet wurden, sind diese gemäß § 6b Abs. 5 BDSG unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. Gab es kein Schadensereignis, sind die Bildaufnahmen der Innenkameras im Regelfall innerhalb von 24 Stunden, spätestens aber nach 48 Stunden zu löschen.

Dem Transparenzgebot des § 6b Abs. 2 BDSG folgend müssen durch deutlich sichtbare Beschilderungen an den Fahrgasttüren potentielle Fahrgäste vor dem Einsteigen auf den Umstand der Videoüberwachung und die hierfür verantwortliche Stelle hingewiesen werden.

Schließlich haben die Taxi-Unternehmen durch geeignete technische und organisatorische Maßnahmen zu gewährleisten, dass nur berechtigten Personen ein Zugriff auf die Bildaufzeichnungen möglich und ein unbefugtes Auslesen der Daten ausgeschlossen ist.

2. Außenkameras

Die Voraussetzungen des § 6b Abs. 1, Abs. 3 BDSG sind bei Außenkameras, mit denen der öffentliche Verkehrsraum - etwa zwecks vorsorglicher Beweis sichernder Dokumentation für den Fall eines Schadensereignisses - einer Überwachung unterzogen werden soll, nicht erfüllt. Unerheblich ist dabei, ob die Kameras mobil sind und eventuell nur die nähere Umgebung des Taxis erfassen. Mit derartigen Kameras sollen gezielt personenbezogene Daten (Bilder, auf denen Personen, Kfz-Kennzeichen, Aufschriften auf Fahrzeugen etc. erkennbar sind) erhoben werden, um später anhand der Aufnahmen beispielsweise Verantwortlichkeiten von Verkehrsteilnehmern und Haftungsfragen klären zu können. Das Recht auf informationelle Selbstbestimmung umfasst jedoch die Möglichkeit, sich in der Öffentlichkeit frei und ungezwungen zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Eine Rechtsgrundlage für diese Datenerhebung gibt es nicht. Eine andere Beurteilung ergibt sich auch nicht, wenn § 28 BDSG zugrunde gelegt wird.

Die Ausstattung von Taxis mit „Unfallkameras“, wie sie von Versicherungsunternehmen vorgeschlagen wird, ist daher unzulässig. Die Taxiunternehmen müssen sich darüber im Klaren sein, dass nicht das Versicherungsunternehmen, sondern sie selbst in der datenschutzrechtlichen Verantwortlichkeit stehen.

Stichwortverzeichnis