Sächsischer Landtag
6. Wahlperiode

DRUCKSACHE 6/10550

Schutz des Persönlichkeitsrechts im nicht-öffentlichen Bereich

8. Tätigkeitsbericht

des

Sächsischen Datenschutzbeauftragten

Berichtszeitraum: 1. April 2015 bis 31. März 2017

Dem Sächsischen Landtag

vorgelegt zum 31. März 2017

gemäß § 30 des Sächsischen Datenschutzgesetzes

Eingegangen am: 27. Oktober 2017 Ausgegeben am: 27. Oktober 2017

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
Alt.	Alternative
AMG	Arzneimittelgesetz
AO	Abgabenordnung
Art.	Artikel
Aufl.	Auflage
Az.	Aktenzeichen
BAG	Bundesarbeitsgericht
BCR	Binding Corporate Rules
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BIC	Bank Identifier Code
BMV-Ä	Bundesmantelvertrag – Ärzte
BO	Berufsordnung
BT-Drs.	Bundestagsdrucksache
DS-GVO	Datenschutz-Grundverordnung
EC	Electronic Cash
EG	Europäische Gemeinschaft
Erfa-Kreis	Erfahrungsaustausch-Kreis
EU	Europäische Union
FAQ	Frequently Asked Questions
FTP	File Transfer Protocol
GBV	Grundbuchverfügung
GDD	Gesellschaft für Datenschutz und Datensicherung e. V.
GenG	Genossenschaftsgesetz
GewO	Gewerbeordnung
GG	Grundgesetz
GKV	Gesetzliche Krankenversicherung

GPS	Global Positioning System
GwG	Geldwäschegesetz
HAACP	Hazard Analysis and Critical Control Points
HGB	Handelsgesetzbuch
HBV	Hepatitis-B-Virus
HCV	Hepatitis-C-Virus
HIV	Humanes Immundefizienz-Virus
IBAN	International Bank Account Number
IFS	International Featured Standards
i. V. m.	in Verbindung mit
InsO	Insolvenzordnung
InsoBekV	Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet
jurisPK	juris Praxis-Kommentar
KiTa	Kindertagesstätte
KunstUrhG	Kunsturheberrechtsgesetz
LArbG	Landesarbeitsgericht
LG	Landgericht
LSG	Landessozialgericht
LuftVO	Luftverkehrs-Ordnung
MSM	Männer mit gleichgeschlechtlichen Sexualkontakten (**M**änner, die **S**ex mit **M**ännern haben)
m. w. N.	mit weiteren Nachweisen
OWiG	Ordnungswidrigkeitengesetz
OWiZuVO	Ordnungswidrigkeiten-Zuständigkeitsverordnung
PAN	Primary Account Number (Zahlungskartennummer)
PassG	Passgesetz
PAuswG	Personalausweisgesetz
PIPEDA	(Canadian) Personal Information Protection and Electronic Documents Act
Pkw	Personenkraftwagen
QR	Quick Response
Rdnr.	Randnummer

SächsDSG	Sächsisches Datenschutzgesetz
SächsGVBl.	Sächsisches Gesetz- und Verordnungsblatt
SächsEGovG	Sächsisches E-Government-Gesetz
SächsKHG	Sächsisches Krankenhausgesetz
SächsVwVG	Sächsisches Verwaltungsvollstreckungsgesetz
SEPA	Single Euro Payments Area (Einheitlicher Euro-Zahlungsverkehrsraum)
SGB	Sozialgesetzbuch
SSL	Secure Sockets Layer (Verschlüsselungsmethode)
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TB	Tätigkeitsbericht
TFG	Transfusionsgesetz
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TPG	Transplantationsgesetz
UKlaG	Unterlassungsklagengesetz
URL	Uniform Resource Locator
UWG	Gesetz gegen den unlauteren Wettbewerb
VerpackV	Verpackungsverordnung
VwVfG	Verwaltungsverfahrensgesetz
VG	Verwaltungsgericht
VwV	Verwaltungsvorschrift
WEG	Wohnungseigentümergemeinschaft
WRV	Weimarer Reichsverfassung

Verweise im Text auf Ausführungen in früheren Tätigkeitsberichten des Sächsischen Datenschutzbeauftragten sind durch Angabe der Nummer des jeweiligen Tätigkeitsberichtes sowie der jeweiligen Abschnitt-Nr. – getrennt durch einen Schrägstrich – gekennzeichnet (z. B. 5/4.2.1).

Vorwort

Vor Ihnen liegt der achte und wahrscheinlich letzte eigenständige Bericht über meine Tätigkeit als Datenschutzaufsichtsbehörde im nicht-öffentlichen Bereich. Im Mai nächsten Jahres wird die für öffentliche und nicht-öffentliche Stellen gleichermaßen geltende Datenschutz-Grundverordnung in Kraft treten und damit die bisher bestehende starke Trennung beider Bereiche weitgehend aufheben. Lediglich dort, wo die Datenschutz-Grundverordnung entsprechende Öffnungsklauseln enthält, wird es noch spezielle Regelungen für den jeweiligen Bereich geben. Für den nicht-öffentlichen Bereich sind diese im Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU) vom 30. Juni 2017 (BGBl. I S. 2097) enthalten. Ich beabsichtige daher, zukünftig nur noch einen einheitlichen Tätigkeitsbericht zu erstellen, im Gegensatz zur derzeitigen Verfahrensweise dann allerdings jährlich (Art. 59 DS-GVO).

Auf meine mehr als unzureichende Personalausstattung habe ich in den letzten Jahren immer wieder hingewiesen. Leider hat sich diesbezüglich auch im Berichtszeitraum nur wenig getan. Nach wie vor vermisse ich ein deutliches Bekenntnis der politischen Entscheidungsträger zur Sicherstellung einer adäquaten Datenschutzaufsicht im Freistaat Sachsen. Leidtragende sind einerseits die Betroffenen, deren Eingaben nicht zeitnah bearbeitet werden können bzw. die mangels unzureichender anlassfreier Kontrolltätigkeit (vermeidbar) überhaupt erst Datenschutzverstößen ausgesetzt worden sind. Andererseits kann ich deshalb aber auch nicht auf die Unternehmen in einem Maße, wie ich es gern würde, beratend (und im Sinne der Betroffenen präventiv) zugehen.

Es ist absehbar, dass spätestens mit dem Inkrafttreten der Datenschutz-Grundverordnung wegen der damit verbundenen zusätzlichen Aufgaben eine signifikante Aufstockung meines Personalbestandes unumgänglich ist, andernfalls werde ich nicht in der Lage sein, die an mich durch die Datenschutz-Grundverordnung gestellten Anforderungen ordnungsgemäß zu erfüllen. Dies betrifft insbesondere enge Fristvorgaben, z. B. im Rahmen der vielfältigen Abstimmungen auf nationaler und europäischer Ebene. Dabei geht es aber nicht nur um die Bearbeitung konkreter Sachverhalte. Vielmehr werden zukünftig noch stärker als bislang weitreichende Entscheidungen zur Auslegung und Anwendung der Datenschutz-Grundverordnung bindend auf europäischer Ebene getroffen werden. Ohne entsprechendes neues Personal kann ich diese Abstimmungsprozesse auf der Arbeitsebene – wenn überhaupt – zwar mitverfolgen, nicht jedoch im Sinne der Betroffenen und Unternehmen im Freistaat Sachsen inhaltlich mitgestalten. Anders als Datenschutzaufsichtsbehörden in anderen Bundesländern kann ich mich deshalb auch kaum adäquat auf die mit der Datenschutz-Grundverordnung eintretende vollkommene neue Gesetzeslage vorbereiten und insbesondere auch nicht die meiner Aufsicht unterstehenden Unternehmen bereits jetzt intensiv beraten.

Im Rahmen einer Abordnung eines Sachbearbeiters ist mir für zwei Jahre befristet lediglich eine temporäre Verstärkung zugestanden worden. Auf diese Weise konnte ich zumindest sicherstellen, dass sich die Tendenz der stetigen Vergrößerung der offenen Aufsichtsverfahren bzw. damit verbunden die Verlängerung der Bearbeitungszeiten nicht weiter fortsetzt (vgl. Pkt. 4); allerdings ist es mir vor diesem Hintergrund auch nicht gelungen, die Bearbeitungsrückstände spürbar zu verringern. Ebenso wenig habe ich meine anlassfreie Kontrolltätigkeit intensivieren können. Die wenigen im Berichtszeitraum durchgeführten Regelkontrollen (vgl. Pkt. 3.1) werden meinem Anspruch einer effektiven, glaubhaft und überzeugend agierenden sowie vor allem auch präventiv wirkenden Aufsichtsbehörde nicht gerecht. Lediglich für die Verfolgung von Ordnungswidrigkeiten habe ich eine einzige Stelle zusätzlich bekommen, was angesichts des erheblich gestiegenen Arbeitsaufwandes in diesem Bereich (vgl. Pkt. 13.1) auch bitter nötig war. So musste ich jedenfalls kaum noch Verfahren wegen überlanger Verfahrensdauer einstellen.

Bewährt haben sich die im Mai 2015 in das Sächsische Datenschutzgesetz aufgenommenen Regelungen zur Kostenerhebung im Rahmen der Aufsichtstätigkeit nach dem Bundesdatenschutzgesetz (vgl. 7/10.3). Im Berichtszeitraum habe ich auf diese Weise für den Landeshaushalt Einnahmen in Höhe von mehr als 27.000 € erzielen können (vgl. Pkt. 12.3). Anders als bei Ordnungswidrigkeiten haben sich die verantwortlichen Stellen nur in ganz wenigen Fällen gegen diese Kostenerhebungen gewehrt. Dabei darf aber auch nicht übersehen werden, dass auch die Kostenerhebung für mich mit einem zusätzlichen, nicht unerheblichen Aufwand verbunden ist. Die verantwortlichen Stellen sind vor der Kostenerhebung anzuhören; die danach zu erlassenden Bescheide sind entsprechend zu begründen und ggf. mit Ausführungen zu den festgestellten Datenschutzverstößen zu versehen (§ 40 Abs. 2 Satz 1 SächsDSG). Die sich u. U. anschließenden Klageverfahren binden weitere Ressourcen. Einen Stellenausgleich für diese zusätzliche Aufgabe habe ich nicht erhalten; das dadurch gebundene Personal fehlt mir dann natürlich im Rahmen meiner Aufsichtstätigkeit.

Datenschutzverstöße können für die verantwortlichen Stellen also – selbst wenn kein Bußgeldverfahren eingeleitet wird – schnell auch einmal teuer werden. Je aufwändiger sich die Aufsichtstätigkeit gestaltet und umso unkooperativer sich eine verantwortliche Stelle gegenüber der Aufsichtsbehörde verhält, desto höher fallen auch die Kosten bei Feststellung eines Datenschutzverstoßes aus. Auch die Durchführung örtlicher Kontrollen – im Berichtszeitraum war das immerhin 122-mal der Fall – führt zu einer Kostenerhöhung, da nach Nr. 1b der Anlage zu § 40 SächsDSG in diesen Fällen erhöhte Gebührensätze zur Anwendung kommen. Einen insoweit besonders herausragenden Fall habe ich unter Pkt. 8.2.1 beschrieben. In einem sich sehr lange, letztlich über vier Jahre hinziehenden Aufsichtsverfahren hat ein Unternehmen schließlich in der Summe mehr

als 70.000 € an Buß- und Zwangsgeldern sowie Verwaltungskosten bezahlt, bis ich dieses Verfahren endlich guten Gewissens abschließen konnte.

Man kann den Vorwurf erheben, dass das Instrumentarium der Aufsichtsbehörden nicht darauf ausgelegt ist, schnell und effektiv Erfolge zu erzielen. Dies ist aber der Tribut, der berechtigterweise an die Gewährleistung eines rechtsstaatlichen Verfahrens zu zollen ist. Der Beispielfall zeigt nichtsdestoweniger, dass man dennoch – mit einigem Aufwand zwar – mit den zur Verfügung stehenden Kontrollinstrumenten zum Ziel kommen kann, auch wenn man öfter mal ausgebremst wird. Klar ist, dass die verantwortliche Stelle es – durch entsprechend kooperatives Verhalten – weitgehend selbst in der Hand hat, welche Kosten ihr im Rahmen eines Aufsichtsverfahrens auferlegt werden, zumal es mir § 40 Abs. 4 Satz 1 SächsDSG erlaubt, über die Befreiung oder Ermäßigung von Kosten selbst zu entscheiden.

Den Spitzenplatz bei den Eingaben nimmt schon seit Jahren die Videoüberwachung ein. Diese Tatsache verdeutlicht einerseits die große Sensibilität der Bevölkerung gegen derartige Überwachungsmaßnahmen, andererseits zeigt dies aber auch, dass seitens der Betreiber ohne Rücksicht auf datenschutzrechtliche Vorschriften (zu) große Erwartungen in eine Videoüberwachung gesetzt werden. Dass diese Erwartungen oftmals nicht erfüllt werden, weil die Aufnahmen von zu geringer Auflösung und Qualität sind oder die Täter sich natürlich darauf einstellen und im Zuge der Dunkelheit agieren bzw. sich entsprechend vermummen, wird meist verschwiegen. Mit etwas Glück werden – eher selten – auch Täter überführt; das eigentliche Ziel, Diebstähle, Überfälle, Einbrüche, Sachbeschädigungen und andere Straftaten zu verhindern, wird aber regelmäßig nicht erreicht, denn dazu müssten die Monitore ständig beobachtet werden. Den damit verbundenen Personalaufwand wollen die meisten Betreiber aus Kostengründen aber gerade vermeiden. Insoweit werden Videoüberwachungsmaßnahmen vom Nutzen her also deutlich überbewertet. Unterbewertet bzw. zu wenig beachtet hingegen werden der Überwachungsdruck für die Betroffenen, die damit ggf. verbundene Verhaltens- und Leistungskontrolle sowie die möglichen Folgen für die Betroffenen, wenn sie zufällig zur falschen Zeit am falschen Ort gewesen sind und im Zuge der nachträglichen Aufklärung von Vorfällen dann fälschlicherweise in den Blickpunkt der Ermittlungen geraten.

Das Videoüberwachungsverbesserungsgesetz vom 28. April 2017 (BGBl. I S. 968) zeigt, dass auch der Bundesgesetzgeber diesem Fehlschluss erlegen ist. Er hat der Tatsache, dass Eingaben zur Videoüberwachung bei allen Aufsichtsbehörden zumindest einen vorderen Platz belegen und folglich mitnichten von einer allgemeinen Akzeptanz der Videoüberwachung ausgegangen werden kann, zu wenig Aufmerksamkeit gewidmet. Zur (behaupteten) Terrorabwehr jedenfalls ist eine erweiterte Videoüberwachung durch Private sicherlich nicht geeignet – kein Selbstmordattentäter wird sich durch eine Videokamera

beeindrucken und von seinem Vorhaben abbringen lassen –, ganz abgesehen davon, dass der Schutz der Bevölkerung eine ureigene Aufgabe des Staates ist. Ich gehe davon aus, dass dieses Gesetz nicht lange Bestand haben wird. Inzwischen hat die Piratenpartei am 28. Juni 2017 auch schon Verfassungsbeschwerde gegen das Videoüberwachungsverbesserungsgesetz beim Bundesverfassungsgericht in Karlsruhe eingereicht.

Der Anteil der festgestellten Datenschutzverstöße an der Gesamtzahl der durchgeführten Anlasskontrollen ist mit ca. 38 % auf einen Rekordwert gestiegen, d. h. bei deutlich mehr als jeder dritten Kontrolle habe ich einen Verstoß gegen datenschutzrechtliche Vorschriften feststellen müssen. Im Umkehrschluss bedeutet das aber zugleich, dass meine Kontrollen in etwa 62 % aller Fälle beanstandungsfrei verlaufen sind, d. h. dass sich die betreffenden verantwortlichen Stellen – jedenfalls was den jeweils vorgeworfenen Datenschutzverstoß betrifft – entsprechend datenschutzkonform verhalten haben. Die Schlussfolgerung, dass es deshalb bei diesen Stellen auch insgesamt bestens um den Datenschutz bestellt ist, kann daraus natürlich nicht gezogen werden. Als diesbezügliches Indiz habe ich es aber gewertet, wenn die jeweilige Stelle einen Datenschutzbeauftragten bestellt hatte. Gleichwohl gab es aber auch etliche Fälle, in denen ich – gewissermaßen als Nebenerkenntnis – (als weiteren Verstoß) die Nichtbestellung eines Datenschutzbeauftragten feststellen musste (vgl. Pkt. 8.16.1).

Aber auch bei den Beschwerdeführern habe ich mitunter feststellen müssen, dass sie – auch wenn sie mit ihrer konkreten Beschwerde Recht hatten – jedenfalls für sich selbst noch nicht die notwendigen Konsequenzen gezogen hatten. Wer sich bei mir per E-Mail über mangelnden Datenschutz im Internet, beispielsweise über den Rechnungsversand via E-Mail mit vollständiger Bankverbindung (Pkt. 8.2.3), beschwert, sollte dies möglichst nicht von einem Googlemail- bzw. Gmail-Account aus tun.

Der vorliegende Bericht enthält in bewährter Weise neben allgemeinen überblicksmäßigen Ausführungen auch wieder zahlreiche Darstellungen interessanter Einzelfälle aus meiner Aufsichtstätigkeit (Pkt. 8), insbesondere aus meiner Kontroll- und Beratungspraxis. Natürlich habe ich auch die bereits in den vorangegangenen Berichten enthaltenen Statistiken zu meiner Tätigkeit als Aufsichts- und OWiG-Verwaltungsbehörde fortgeführt.

1 Datenschutzaufsicht im nicht-öffentlichen Bereich

Als Sächsischem Datenschutzbeauftragten obliegt mir auch 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. § 15 OWiZuVO) übertragen, d. h. ich bin auch für die Verfolgung von Ordnungswidrigkeiten nach den §§ 43 BDSG, 16 Abs. 2 Nr. 2 bis 5 TMG und 130 OWiG 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.

- **Stellungnahmen zu Unterlassungsklagen** (§ 12a UKlaG)
  Werden personenbezogene Daten eines Verbrauchers zu Zwecken der Werbung, der Markt- und Meinungsforschung, des Betreibens einer Auskunftei, des Erstellens von Persönlichkeits- und Nutzungsprofilen, des Adresshandels, des sonstigen Datenhandels oder zu vergleichbaren kommerziellen Zwecken erhoben, verarbeitet oder genutzt und ist dazu bei dem zuständigen Gericht eine zivilrechtliche Verbandsklage anhängig, hat mich das Gericht vor einer Entscheidung anzuhören.

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 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

- Erlass förmlicher und damit vollstreckbarer **Duldungsanordnungen**, gegebenenfalls auch verbunden mit der Verhängung von Zwangsgeldern, zur Durchsetzung der Betretungs- und Besichtigungsrechte der Aufsichtsbehörde (§ 38 Abs. 4 Sätze 1, 2 und 4 BDSG)

- Durchführung von **Ordnungswidrigkeitenverfahren** nach dem Bundesdatenschutzgesetz, den datenschutzrechtlichen Tatbeständen des Telemediengesetzes sowie nach § 130 OWiG (§ 15 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 – dies sind in erster Linie Wirtschaftsauskunfteien, Adresshändler sowie Markt- und Meinungsforschungsinstitute. Zum anderen unterliegen auch solche Unternehmen der Meldepflicht, 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 2017 lagen insgesamt 36 Registermeldungen von 23 Unternehmen vor, die

- in 7 Fällen Verfahren von Handels- und Wirtschaftsauskunfteien,

- in 23 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.

Ich habe darauf hinzuweisen, dass ein Registereintrag weder die Gewähr bietet, dass das betreffende Unternehmen datenschutzkonform arbeitet bzw. dass es bereits einer Kontrolle durch die Aufsichtsbehörde unterzogen worden ist, noch stellt er 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 hatte ich kein solches Verlangen zu verzeichnen.

3 Regelaufsicht

3.1 Überblick

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

Im Berichtszeitraum habe ich – wenn auch nur in geringem und bei Weitem nicht ausreichendem Umfang – wieder einige anlassfreie Kontrollen durchführen können. Nach wie vor sehe ich hier jedoch ein erhebliches Kontrolldefizit. Das mir zur Verfügung stehende Personal reicht insbesondere leider auch weiterhin nicht aus, um mich – wie die Aufsichtsbehörden der anderen Bundesländer – an konzertierten bundesweiten Kontrollaktionen zu beteiligen. Gerade solche gemeinsamen Kontrollaktionen betrachte ich aber als sehr wertvoll und zielführend, da sie unter Zugrundelegung abgestimmter Prüfkonzepte durchgeführt werden, eine weitgehend einheitliche Bewertung über Ländergrenzen hinweg ermöglichen und daher auch für die kontrollierten Unternehmen bzw. Branchen in besonderem Maße aufschlussreich und nutzbringend sind.

Die durch mich durchgeführten Regelkontrollen betrafen ein Aktenvernichtungsunternehmen, fünf für das elektronisch geführte Grundbuch abrufberechtigte Unternehmen aus der Immobilienbranche (vgl. Pkt. 3.3) sowie 127 Firmen, die ich in Bezug auf eine Übermittlung personenbezogener Daten in die USA (Stichwort: Safe Harbor, vgl. Pkt. 3.2) angeschrieben habe.

Berichtszeitraum	2001 2002	2003 2004	2005 2006	2007 2008	2009 2010	01.01.11 31.03.13	01.04.13 31.03.15	**01.04.15 31.03.17**
Anzahl Regelkontrollen	104	110	45	55	2	7	0	**133**

Auch wenn der Vergleich in quantitativer Hinsicht gegenüber den vorangegangenen Berichtszeiträumen eine deutliche Steigerung ergibt, darf nicht übersehen werden, dass 127 der 133 angegebenen Kontrollen lediglich als Fragebogenaktion ausgestaltet waren und mit der Problematik der Datenübermittlung in die USA letztendlich nur einen kleinen Ausschnitt der Datenverarbeitung zum Gegenstand hatten. Insoweit bleibt es mein Ziel, den Bereich der Regelkontrollen deutlich auszubauen und dabei die Datenverarbeitung nicht-öffentlicher Stellen sowohl intensiver als auch extensiver, insbesondere auch verstärkt im Rahmen örtlicher Kontrollen, zu prüfen. Voraussetzung dafür ist nach wie vor eine deutliche Erhöhung meiner personellen Ressourcen, welche aber zuallererst eine

– bislang leider nicht erkennbare – deutliche Positionierung der politischen Entscheidungsträger zugunsten des Datenschutzes voraussetzt.

3.2 Safe Harbor

Für sehr viele Unternehmen sind Datentransfers in die USA alltäglicher Teil ihrer Arbeit geworden, nicht zuletzt durch die Nutzung von Cloud-Dienstleistungen und sozialen Netzwerken. Die Unternehmen tragen dabei als übermittelnde Stelle die Verantwortung für die Zulässigkeit der Datenübermittlungen in die USA (§ 4b Abs. 5 BDSG).

Der Europäische Gerichtshof hat mit Urteil vom 6. Oktober 2015 (Az. C-362/14) entschieden, dass Datenübermittlungen in die USA nicht länger auf die sog. Safe Harbor-Entscheidung der Europäischen Kommission (Entscheidung vom 26. Juli 2000 – 2000/520/EG) gestützt werden können und damit datenschutzwidrig sind, wenn sie auf dieser Grundlage weiterhin erfolgen (vgl. dazu auch Pkt. 7). Das Urteil des Europäischen Gerichtshofes hat dabei nicht zuletzt wegen der darin enthaltenen grundsätzlichen Aussagen zum Umfang des durch die Charta der Grundrechte der Europäischen Union gewährleisteten Rechts auf Achtung des Privat- und Familienlebens (Art. 7) und des Schutzes personenbezogener Daten (Art. 8) sowie des Rechts auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht (Art. 47) über den entschiedenen Einzelfall hinaus Bedeutung für Datentransfers in die USA.

Um belastbare Informationen zu haben, wie Unternehmen mit Sitz im Freistaat Sachsen mit Datenübermittlungen in die USA verfahren und welche Umstellungen sie nach Erlass des Safe Harbor-Urteils des EuGH bereits vorgenommen haben, habe ich im Februar 2016 127 ausgewählte sächsische Unternehmen um Auskunft gebeten, ob und auf welcher Rechtsgrundlage sie Daten in die USA übermitteln. Ziel war dabei auch, die Unternehmen für Fragen des internationalen Datentransfers zu sensibilisieren. Die Auswertung ergab, dass etwa die Hälfte der angeschriebenen Unternehmen Daten in die USA übermittelt hatte, ca. ein Viertel der angeschriebenen Unternehmen stützte die Datentransfers dabei auf die aufgehobene Safe Harbor-Entscheidung. Die Aufsichtsbehörden anderer Bundesländer führten ähnliche Abfragen durch. Zudem starteten zehn Bundesländer im November 2016 eine koordinierte Prüfung des internationalen Datenverkehrs, an der ich mich aufgrund meiner beschränkten personellen Ressourcen jedoch nicht beteiligen konnte.

3.3 Automatisierte Abrufe aus dem elektronisch geführten Grundbuch

Unternehmen können unter bestimmten Voraussetzungen am automatisierten Verfahren zum Datenabruf aus dem elektronischen Grundbuch teilnehmen, benötigen hierfür aber von der Leitstelle für Informationstechnologie der sächsischen Justiz eine Genehmigung. Die spätere Kontrolle der Einhaltung der dabei zu beachtenden datenschutzrechtlichen Regelungen, insbesondere der einzelfallbezogenen Abrufberechtigung, obliegt dann mir als zuständiger Datenschutzaufsichtsbehörde (§ 38 Abs. 1 Satz 1 BDSG). § 83 Abs. 1 Satz 3 GBV gibt dazu vor, dass das Grundbuchamt die Abrufprotokolle für eine stichprobenartige Überprüfung durch die aufsichtführenden Stellen bereitzuhalten hat.

Nachdem das Regierungspräsidium Dresden als seinerzeit zuständige Datenschutzaufsichtsbehörde bereits 2005/2006 einige solcher (anlassfreien) Kontrollen durchgeführt hatte (vgl. dazu 3/3.2), habe ich mich im Berichtszeitraum wieder dieser Aufgabe zuwenden müssen, dabei aber infolge der unverändert prekären Personalsituation zunächst nur fünf – alle aus der Immobilienbranche – der 106 im Freistaat aktuell zum automatisierten Abrufverfahren zugelassenen Unternehmen einer diesbezüglichen Kontrolle unterziehen können.

Regelmäßig prüfe ich bei solchen Kontrollen auch die Einhaltung allgemeingültiger datenschutzrechtlicher Anforderungen wie die Verpflichtung auf das Datengeheimnis oder die Bestellung eines betrieblichen Datenschutzbeauftragten; Schwerpunkt ist aber natürlich die stichprobenhafte Überprüfung der Zulässigkeit der Abrufe aus dem elektronischen Grundbuch. Die abrufberechtigten Stellen müssen bei diesen Kontrollen für ca. fünf bis zehn Prozent der im Kontrollzeitraum getätigten Abrufe ihre Abrufberechtigung anhand konkreter, einzelfallbezogener Unterlagen, z. B. Vollmachten der Eigentümer oder entsprechende Grundbucheintragungen, nachweisen. Bei den Überprüfungen wird insbesondere auch darauf geachtet, dass Abrufe aller berechtigten Mitarbeiter – dies ist an den Bearbeiterkennzeichen erkennbar – und alle aus irgendeinem Grund ungewöhnlichen Abrufe (z. B. hinsichtlich der Abrufzeit) mit abgedeckt werden.

Diesbezügliche Datenschutzverstöße, d. h. unberechtigte Datenabrufe, habe ich bei den fünf im Berichtszeitraum durchgeführten Kontrollen nicht feststellen müssen. In einem Fall ist allerdings deutlich geworden, dass das betreffende Unternehmen weder seiner Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten nachgekommen war noch seine Mitarbeiter auf das Datengeheimnis verpflichtet hatte. Auch ein Verfahrensverzeichnis war nicht vorhanden. Nach meinem Kontrollbesuch sind diese Mängel aber dann umgehend behoben worden.

Die von mir zum Zweck der Stichprobenkontrolle von der Leitstelle für Informationstechnologie der sächsischen Justiz abgeforderten Abrufprotokolle werden von mir gemäß § 83 Abs. 3 Satz 3 GBV spätestens ein Jahr nach Eingang vernichtet, es sei denn, ich benötige sie für weitere bereits eingeleitete Prüfungen oder bei bereits durchgeführten Prüfungen für die Ahndung unzulässiger Datenabrufe.

4 Anlassaufsicht

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).

Während Regelkontrollen (anlassfreie Kontrollen) ohne konkreten Anhaltspunkt für eine Datenschutzverletzung durchgeführt werden, beruhen Anlasskontrollen regelmäßig auf solchen Anhaltspunkten, die beispielsweise aus Hinweisen Dritter, Presse- oder Internetveröffentlichungen oder aus bereits durchgeführten Überprüfungen resultieren können. Der mit Abstand größte Teil der durchgeführten Anlasskontrollen hat seinen Ursprung aber natürlich in entsprechend substantiiert vorgetragenen Eingaben Betroffener.

Im Berichtszeitraum bin ich in insgesamt 840 Fällen Anhaltspunkten für einen Datenschutzverstoß nachgegangen, 91 Fälle resultierten dabei noch aus dem letzten Berichtszeitraum. Hinsichtlich der neu bearbeiteten Sachverhalte (749 Fälle) ist damit gegenüber dem letzten Berichtszeitraum ein geringfügiger Rückgang zu verzeichnen, die Anzahl der zu bearbeitenden Vorgänge bewegte sich infolge der durch den akuten Personalmangel verursachten Bearbeitungsrückstände aus den Vorjahren aber auf einem vergleichbaren Niveau. Hinzu kommen zahlreiche telefonische Anfragen, die ich immer dann zahlenmäßig nicht separat erfasst habe, wenn ich diese sofort, d. h. ohne Schriftverkehr, beantworten konnte.

Anlasskontrollen führe ich im Regelfall im schriftlichen Verfahren durch, daneben kontrolliere ich die verantwortlichen Stellen in vielen Fällen aber auch vor Ort. So habe ich im Berichtszeitraum – wie auch schon im letzten Berichtszeitraum – in wiederum 122 Fällen örtliche Überprüfungen bei insgesamt 106 verantwortlichen Stellen durchgeführt. Örtliche Überprüfungen sind immer – schon wegen des Reiseaufwandes und der (aus Beweis- und Sicherheitsgründen) Bindung von im Regelfall mindestens zwei Bediensteten – mit einem erheblichen Mehraufwand verbunden. Ich versuche zwar immer mehrere Kontrollen – etwa in Großstädten – terminlich miteinander zu verbinden, jedoch bietet sich das gerade in den Randzonen des Freistaates nicht immer an, zuweilen steht auch die Dringlichkeit einer Angelegenheit solch einer Terminkombination entgegen. Zudem kann ich im Interesse einer zügigen Bearbeitung einer Eingabe nicht immer auf einen örtlich naheliegenden weiteren Aufsichtsfall warten.

Nicht zuletzt auch deshalb ist es mir leider nicht gelungen, die Bearbeitungsrückstände aus dem letzten Berichtszeitraum entscheidend zu verringern. Dies wird – was ich leider

nur immer wiederholen kann – nur möglich werden, wenn meine Personalausstattung entsprechend verbessert wird. Die hohe Anzahl der offenen Verfahren ist das Spiegelbild der hohen Arbeitsbelastung meiner Mitarbeiter im nicht-öffentlichen Bereich; für die Betroffenen spürbar wird dies in erster Linie durch überdurchschnittlich lange Bearbeitungszeiten und damit verbunden auch dadurch, dass Datenschutzverstöße nicht zeitnah festgestellt und unterbunden werden können; die Zahl der Betroffenen sich also ggf. sogar noch erhöht.

		2007 2008	2009 2010	01.01.11 31.03.13	*01.04.11* *31.03.13*	01.04.13 31.03.15	**01.04.15** **31.03.17**
Neueingänge		410	648	904	*803**	807	**749**
zzgl. Übernahme Vorjahr		15	29	14	*14*	26	**91**
anhängige Sachverhalte gesamt		425	677	918	*817**	833	**840**
davon	mit örtlichen Kontrollen	51	68	162	*87**	98	**106**
	Verstöße	87	152	324	*288**	259	**292**
	keine Zuständigkeit	57	160	180	*160**	124	**150**
	noch in Bearbeitung	29	14	26	*26*	91	**79**

* Vergleichswerte (Zweijahreszeitraum), rechnerisch ermittelt!

Die vorstehende Tabelle fasst den Umfang meiner anlassbedingten Kontrolltätigkeit im Berichtszeitraum zusammen und stellt deren Entwicklung im Vergleich zu den Vorjahren dar.

Den Schwerpunkt meiner anlassbedingten Kontrolltätigkeit bilden unverändert Videoüberwachungsfälle, deren absolute Anzahl erneut gestiegen ist. Um etwa ein Drittel angestiegen sind die Beschwerden über die Nichtgewährung bzw. die nicht vollständige Gewährung von Betroffenenrechten, hier insbesondere des Auskunftsrechts (§ 34 BDSG). Im Bereich Arbeitnehmerdatenschutz hatte ich sogar ein um 50 % erhöhtes, sehr breit gefächertes Eingabeaufkommen zu verzeichnen. Etwas zurückgegangen sind Eingaben in Bezug auf das Internet (E-Commerce, Social-Web, Internetdienstleistungen, Werbemails); gestiegen ist hingegen die Anzahl der Beschwerden betreffend die Wohnungswirtschaft – Schwerpunkt waren hier vor allem Mieterfragebögen und Personalausweiskopien.

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

1. Videoüberwachung 154 Fälle
2. Betroffenenrechte 108 Fälle

3.	Beschäftigtendatenschutz	75 Fälle
4.	Internet	53 Fälle
5.	Wohnungswirtschaft	26 Fälle
6.	Gesundheitswesen	23 Fälle
7.	Datenschutzbeauftragter	16 Fälle
8.	Kreditwirtschaft	15 Fälle
9.	Vereine und Verbände	14 Fälle
	Werbung	14 Fälle
10.	Rechtsanwälte	13 Fälle
11.	Versicherungswirtschaft	9 Fälle
12.	Sozialeinrichtungen / freie Sozialträger	8 Fälle
13.	Energiewirtschaft	7 Fälle
	Hotels, Gastronomie	7 Fälle

Bei deutlich mehr als jeder dritten Kontrolle (ca. 38 %) habe ich im Ergebnis einen Verstoß gegen datenschutzrechtliche Vorschriften feststellen müssen. Die bereichsspezifische Auswertung zeigt dabei eine weitgehende Übereinstimmung mit den durchgeführten Kontrollen:

1.	Videoüberwachung	70 Verstöße	(53 %)
2.	Betroffenenrechte	53 Verstöße	(49 %)
3.	Datenschutzbeauftragter	31 Verstöße	(---)
4.	Beschäftigtendatenschutz	24 Verstöße	(32 %)
5.	Datengeheimnis	21 Verstöße	(---)
6.	Internet	19 Verstöße	(36 %)
7.	Wohnungswirtschaft	16 Verstöße	(62 %)

Die bezüglich der betrieblichen Datenschutzbeauftragten festgestellten Verstöße betrafen fast ausnahmslos die Bestellungspflicht. Deren Anzahl (31) liegt deutlich höher als die der mit diesem Fokus durchgeführten Anlasskontrollen (16), was schlichtweg darin begründet liegt, dass es sich dabei zumeist um Nebenerkenntnisse aus mit einem anderen Schwerpunkt durchgeführten Kontrollen gehandelt hat (vgl. Pkt. 8.16.1). Gleiches gilt auch für die – von mir regelmäßig mit abgefragte – Verpflichtung auf das Datengeheimnis (vgl. Pkt. 8.17.1).

Soweit es sich bei den festgestellten Datenschutzverstößen um allgemein interessierende Fallgestaltungen handelt, die in den vorangegangenen Tätigkeitsberichten noch nicht thematisiert worden sind, werden diese unter Pkt. 8 näher beschrieben.

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 136 Fällen – und damit nur geringfügig weniger als im letzten Berichtszeitraum – Beratungsanliegen an mich herangetragen worden. In vier Fällen habe ich die verantwortlichen Stellen kostenpflichtig vor Ort beraten; darüber hinaus habe ich auch einer Rechtsanwaltskanzlei für eine schriftliche Beratung die mir entstandenen Kosten in Rechnung gestellt (vgl. dazu auch Pkt. 12.3).

Die nachfolgende Übersicht stellt die Entwicklung des Beratungsanfalles in den letzten Jahren dar:

Berichtszeitraum	2007 2008	2009 2010	01.01.11 31.03.13	*01.04.11* *31.03.13*	01.04.13 31.03.15	**01.04.15** **31.03.17**
Beratungsfälle	34	87	122	*108**	146	**136**

* Vergleichswert (Zweijahreszeitraum), rechnerisch ermittelt!

Telefonische Anfragen, die auch sofort durch telefonische Beratung erledigt werden konnten, sind in diesen Zahlen nicht enthalten – hierüber wurde keine Statistik geführt.

Auch bei den Beratungen bildeten Zulässigkeitsfragen in Bezug auf (geplante) Videoüberwachungen den absoluten Schwerpunkt im Berichtszeitraum. Diesbezüglich erreichten mich 28 Anfragen, so auch zur frühzeitigen Klärung der Zulässigkeit des Kamerabetriebs in einem in Privateigentum befindlichen, nichtsdestoweniger aber öffentlich gewidmeten Gebäudedurchgang (Pkt. 8.1.2). Aus dem Gesundheitsbereich sind – überwie-

gend von Krankenhäusern – 17 Beratungsanliegen an mich herangetragen worden; besonders erwähnenswert sind insoweit die Beratungen zu Videoüberwachungen in der Psychiatrie (Pkt. 8.1.7), zum Videodolmetschen (Pkt. 8.1.8), zur Wunddokumentation mittels Fotografie (Pkt. 8.4.1) sowie zur Nutzung externer Abrechnungsstellen durch Ergotherapeuten (Pkt. 8.4.6). In 13 Fällen haben sich Unternehmer oder deren Datenschutzbeauftragte mit Fragen rund um die Bestellung, Fachkunde und Tätigkeit betrieblicher Datenschutzbeauftragter an mich gewandt. In elf Fällen nutzten Vereine ihr Beratungsrecht, so etwa zur Frage der Datenlöschung bei Vereinsaustritt (Pkt. 8.7.2). Zum Thema Beschäftigtendatenschutz hatte ich zehn sehr breitgefächerte Beratungsanfragen zu verzeichnen: Hier ging es beispielsweise um Fragen der Mitarbeiterüberwachung bzw. Kontrollbefugnisse des Arbeitgebers und um die Nutzung von GPS-Trackern. Achtmal hatte ich Anfragen freier Träger im Sozialbereich zu beantworten, u. a. zur Weitergabe von Informationen über Zahlungsrückstände beim Wechsel der KiTa (Pkt. 8.9.3) und zu Aufbewahrungsfristen für Fallakten (Pkt. 8.9.5). In Bezug auf die verbleibenden Beratungsfälle waren keine besonderen Schwerpunkte feststellbar.

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 der Aufsichtsbehörde dazu entsprechende Vertragsklauseln oder verbindliche Unternehmensregelungen vorzulegen. Im Berichtszeitraum sind an mich jedoch keine derartigen Anträge gestellt worden.

Werden die von der Europäischen Kommission festgelegten Standardvertragsklauseln verwendet, ist eine Genehmigung der Datenübermittlungen durch die Aufsichtsbehörde nicht mehr erforderlich. Derzeit gibt es drei derartige Standardvertragsklauseln (siehe *http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm*):

- Standardvertragsklauseln für die Datenübermittlung (2001/497/EG)
- Alternative Standardvertragsklauseln für die Datenübermittlung (nicht anwendbar für Beschäftigtendaten) (2004/915/EG)
- Standardvertragsklauseln für Auftragsdatenverarbeitung (2010/87/EU)

Bei einer Reihe von Staaten hat die Europäische Kommission bereits formell festgestellt, dass dort ein im Sinne des § 4b BDSG angemessenes Datenschutzniveau gegeben ist. Zu diesen Ländern zählen Andorra, Argentinien, die Färöer, Guernsey, Israel, die Isle of Man, die Vogtei Jersey, Kanada (mit Einschränkungen), Neuseeland, die Schweiz, Uruguay sowie die USA (jetzt: Privacy Shield, s. u.), vgl. dazu *http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.* Bei einer Übermittlung in diese Länder bzw. an die den jeweiligen Regelungen unterfallenden Stellen (Kanada, USA) ist ebenso wie bei der Verwendung der Standardvertragsklauseln keine Genehmigung durch die Aufsichtsbehörde erforderlich. Im Vergleich zum vorangegangenen Berichtszeitraum sind keine Angemessenheitsentscheidungen zu weiteren Ländern getroffen worden; allerdings haben sich Änderungen in Bezug auf die USA ergeben:

Nachdem der Europäische Gerichtshof in seinem Urteil vom 6. Oktober 2015 in der Rechtssache C-362/14 die (Safe Harbor-)Entscheidung 2000/520/EG für ungültig erklärt hatte, hat die Europäische Kommission am 12. Juli 2016 unter Aktenzeichen C(2016) 4176 einen neuen Angemessenheitsbeschluss gefasst, der den Anforderungen von Art. 25 der Richtlinie 95/46/EG in der Auslegung durch den Gerichtshof gerecht werden soll und unter dem Namen Privacy Shield (EU-US-Datenschutzschild) bekannt geworden ist. Allerdings lassen die rechtlichen Bedenken, die der Europäische Gerichtshof in seinem Urteil formuliert hat, auch Zweifel an der Wirksamkeit des Privacy Shield sowie der anderen Übermittlungsinstrumente wie Standardvertragsklauseln und verbindliche Unternehmensregeln (BCR) aufkommen. Aufgrund dieser rechtlichen Unsicherheiten erscheinen daher – in den Fällen, in denen dies der Sache nach möglich ist, z. B. bei der Nutzung von Cloud-Dienstleistungen – in erster Linie technische Maßnahmen, die den Inhalt der Daten wirksam gegen den Zugriff Dritter schützen, bei Datenübermittlungen in die USA empfehlenswert.

Das Privacy Shield beruht auf einem System der Selbstzertifizierung, wonach sich amerikanische Organisationen zu einem Katalog von Datenschutzgrundsätzen verpflichten, die vom Handelsministerium der USA herausgegeben wurden und im Anhang des o. g. Beschlusses enthalten sind. Er erfasst sowohl die für die Datenverarbeitung Verantwortlichen als auch die Auftragsdatenverarbeiter in den USA mit der Maßgabe, dass sich die Auftragsdatenverarbeiter vertraglich verpflichten, nur auf Weisung des Verantwortlichen in der EU zu handeln und Letzteren dabei zu unterstützen, Privatpersonen die Wahrnehmung ihrer Rechte zu erleichtern.

Unbeschadet der Einhaltung innerstaatlicher Vorschriften auf der sogenannten ersten Stufe, insbesondere zur Zulässigkeit der Datenverarbeitung nach den §§ 4, 28 ff. BDSG, hat der Beschluss zum Privacy Shield also die Wirkung, dass die Übermittlung von Daten von einem für die Verarbeitung Verantwortlichen in der EU an Organisationen in den USA, die sich durch Selbstzertifizierung beim Handelsministerium zur Einhaltung der Grundsätze verpflichtet haben, auf der sogenannten zweiten Stufe zulässig ist.

Die Liste der US-Organisationen, die sich beim US-Handelsministerium durch Selbstzertifizierung zu den Grundsätzen des Privacy Shield bekannt haben, kann unter folgendem Link abgerufen werden: *https://www.privacyshield.gov/list*

Für Unternehmen hat die Art. 29-Gruppe weitergehende Informationen unter dem Link *http://ec.europa.eu/newsroom/document.cfm?doc_id=40933* in Form von FAQ (WP 245) zum Abruf bereitgestellt.

Die Europäische Kommission hat zudem einen Leitfaden für Bürgerinnen und Bürger herausgegeben, in dem die Rechte Betroffener unter dem Privacy Shield dargestellt werden, abrufbar unter:
http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_de.pdf

8 Ausgewählte Sachverhalte

8.1 Videoüberwachung

8.1.1 Dashcams

Auch in diesem Berichtszeitraum musste ich mich mit der Thematik Dashcams intensiver auseinandersetzen (siehe bereits 7/8.1.1). Mich erreichten diesbezüglich mehrere Hinweise. Offensichtlich ist bei Weitem noch nicht allen Besitzern dieser On-Board-Videokameras bewusst, dass deren Einsatz im öffentlichen Straßenverkehr gegen Datenschutzrecht verstößt.

Zur Erinnerung: Der Düsseldorfer Kreis hatte sich zu dieser Problematik bereits mit Beschluss vom 25./26. Februar 2014 (7/14.4.2) geäußert und festgestellt, dass der Einsatz solcher Kameras datenschutzrechtlich generell unzulässig ist - jedenfalls sofern dieser nicht ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. Hierzu hat der Europäische Gerichtshof mit Urteil vom 11. Dezember 2014 (Az. C-212/13, Rdnr. 29 ff., juris) entschieden, dass, soweit sich eine Videoüberwachung auch nur teilweise auf den öffentlichen Raum erstreckt und dadurch auf einen Bereich außerhalb der privaten Sphäre desjenigen gerichtet ist, der die Daten auf diese Weise verarbeitet, sie nicht als eine ausschließlich persönliche oder familiäre Tätigkeit angesehen werden kann.

Neben dem Verwaltungsgericht Ansbach (Urteil vom 12. August 2014 – AN 4 K 13.01634, juris) hat nun auch das Verwaltungsgericht Göttingen (Beschluss vom 12. Oktober 2016 – 1 B 171/16, juris) bestätigt, dass der Einsatz von Dashcams durch Private im öffentlichen Straßenverkehr datenschutzwidrig ist.

Datenschutzwidrig ist dabei grundsätzlich nicht nur das Speichern der Videoaufnahmen (unbefugte Datenverarbeitung), sondern bereits das ständige Beobachten des öffentlichen Verkehrsraums ohne Aufzeichnungen (unbefugte Datenerhebung): Gemäß § 6b Abs. 3 Satz 1 BDSG, der von „erhobenen Daten“ spricht, ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) im Sinne des § 6b Abs. 1 BDSG als Datenerhebung anzusehen. Ein Beobachten und damit eine Datenerhebung liegen damit bereits vor, wenn die Videokamera im Hintergrund mitläuft und die Möglichkeit besteht, dass der Fahrer oder ein Beifahrer Bilder ansieht und auswertet, indem er z. B. in den Aufzeichnungsmodus wechselt, weil er einen potentiellen Verkehrssünder entdeckt. Für das Vorliegen einer Datenerhebung ist irrelevant, ob die Bilder (dauerhaft) aufgezeichnet werden (sollen) (vgl. Scholz in Simitis, BDSG, 8. Auflage, § 6b Rdnr. 64 f.).

Die Datenerhebung und – im Fall der Speicherung von Aufnahmen – die Datenverarbeitung beurteile ich als unbefugt. Datenerhebungen und Datenverarbeitungen sind gemäß

§ 4 Abs. 1 BDSG grundsätzlich verboten, es sei denn, sie werden durch eine Rechtsvorschrift zugelassen. Eine solche Befugnisnorm ist vorliegend nicht gegeben. Die Zulässigkeit der Videoüberwachung öffentlich zugänglicher Räume beurteilt sich ausschließlich nach § 6b BDSG als lex specialis. Dessen Voraussetzungen für eine zulässige Videoüberwachung sind nicht erfüllt.

Die Videoüberwachung erfolgt nicht in Wahrnehmung des Hausrechts im Sinne des § 6b Abs. 1 Nr. 2, Abs. 3 BDSG. Denn das Hausrecht endet an der Grundstücksgrenze und kann nicht die Videoüberwachung öffentlicher Verkehrsbereiche durch den Betreiber der Dashcam rechtfertigen.

Soweit der Besitzer der Dashcam mit deren Betrieb sein Eigentum schützen und Beweise sichern will, überwiegen die schutzwürdigen Interessen der unbeteiligten, sich verkehrsgerecht verhaltenden Passanten (§ 6b Abs. 1 Nr. 3, Abs. 3 BDSG), nicht anlasslos und heimlich auf öffentlichem Grund überwacht zu werden. Der Betreiber der Dashcam greift mit der heimlichen Videoüberwachung in schwerwiegender Weise in das Recht auf informationelle Selbstbestimmung der anderen Verkehrsteilnehmer ein (vgl. die eingangs erwähnten Entscheidungen der Verwaltungsgerichte Ansbach und Göttingen sowie Scholz, a. a. O., § 6b BDSG, Rdnr. 96). Die anderen Verkehrsteilnehmer sind auf die Nutzung von Gehweg und Straße angewiesen und werden – ohne hierfür einen Grund gegeben zu haben – unter Generalverdacht gestellt und mittels Videokamera überwacht.

Ich nehme insofern auch auf den bereits erwähnten Beschluss des Düsseldorfer Kreises vom 25./26. Februar 2014 Bezug, in dem es hierzu heißt:

„Das informationelle Selbstbestimmungsrecht umfasst das Recht des Einzelnen, sich in der Öffentlichkeit frei zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. … Das Interesse des Autofahrers, für den eher theoretischen Fall eines Verkehrsunfalls Videoaufnahmen als Beweismittel zur Hand zu haben, kann diesen gravierenden Eingriff in das Persönlichkeitsrecht der Verkehrsteilnehmer nicht rechtfertigen. Da selbst die Polizei Videokameras zur Verfolgung von Straftaten und Ordnungswidrigkeiten nur auf der Grundlage spezifischer Regelungen und ausschließlich dann einsetzen darf, wenn gegen die betroffene Person ein entsprechender Anfangsverdacht besteht, können erst recht sonstige Stellen nicht für sich beanspruchen, den öffentlichen Verkehrsraum anlass- und schrankenlos mittels Kameras zu überwachen.“

Die Speicherung der Videoaufnahmen birgt ein erhebliches Missbrauchspotential, da diese über das Internet praktisch grenzenlos verbreitet werden können. Der Betreiber der Dashcam allein hat es in der Hand zu entscheiden, ob und wie lange er ohne Wissen der anderen Verkehrsteilnehmer Aufnahmen anfertigt, dauerhaft speichert und was er mit diesen macht.

Ich höre in diesem Zusammenhang von Betreibern der Dashcams oft das Argument, dass Zivil- und Strafgerichte Aufzeichnungen, die mit Dashcams angefertigt wurden, als Beweismittel anerkennen. Allerdings lassen diese Entscheidungen die datenschutzrechtliche Zulässigkeit des Einsatzes der Dashcams regelmäßig offen und setzten sich allein mit der Frage auseinander, ob aus einer datenschutzrechtlichen Unzulässigkeit des Betriebs der Dashcams ein sogenanntes Beweisverwertungsverbot im konkreten Zivil- oder Strafverfahren folgt. Ein Beweisverwertungsverbot würde bedeuten, dass die datenschutzrechtlich unzulässigen Videoaufnahmen nicht als Beweismittel herangezogen werden dürften, d. h. als nicht existent behandelt werden müssten. Ob ein Beweisverwertungsverbot eingreift, lässt sich nicht pauschal bejahen oder verneinen. Vielmehr hängt dies vom jeweiligen Einzelfall ab und bedarf einer umfassenden Gesamtwürdigung aller konkreten Umstände – einer unter vielen ist dabei der Datenschutzverstoß.

Häufig beklagen sich die Besitzer von Dashcams bei mir auch darüber, dass die Hersteller nicht auf die datenschutzrechtliche Unzulässigkeit des Betriebs solcher Kameras hinweisen. Tatsächlich ist es misslich, dass viele Hersteller von Dashcams (z. B. in der Bedienungsanleitung) nicht oder nur unzureichend darauf hinweisen, dass die Nutzung der Dashcams im öffentlichen Straßenverkehr datenschutzrechtlich unzulässig ist. Allerdings ist es primär eine zivil- und keine datenschutzrechtliche Frage, ob die Hersteller eine entsprechende Hinweispflicht trifft oder nicht. Datenschutzrechtlich bleibt derjenige, der eine Dashcam im öffentlichen Straßenverkehr einsetzt, als verantwortliche Stelle für die Einhaltung der Vorschriften des Bundesdatenschutzgesetzes verantwortlich.

Ich begrüße daher sehr, dass sich die weit überwiegende Anzahl derjenigen, die Dashcams in ihren Fahrzeugen einsetzten, nach meinem entsprechenden Hinweis auf die Rechtslage sofort bereit erklärten, die Dashcams dauerhaft zu demontieren. Hierdurch wird eine kostenpflichtige datenschutzrechtliche Anordnung gemäß § 38 Abs. 5 Satz 1 BDSG entbehrlich. Zudem fallen dann in der Regel (wenn kein weiterer Schriftverkehr erforderlich ist) auch keine Kosten für meine Kontrolltätigkeit an, weil ich in diesen Fällen von der Erhebung von Gebühren und Auslagen aus Billigkeitserwägungen absehe (§ 40 Abs. 1 Satz 1 i. V. m. Abs. 4 Satz 1 SächsDSG).

Abschließend der Hinweis, dass der datenschutzwidrige Betrieb von Videoüberwachungsanlagen als unbefugte Erhebung und Verarbeitung von personenbezogenen Daten von mir als Ordnungswidrigkeit verfolgt (§ 43 Abs. 2 Nr. 1 BDSG) und mit einer Geldbuße bis zu 300.000 € (§ 43 Abs. 3 Satz 1 BDSG) geahndet werden kann. Von der Möglichkeit, Ordnungswidrigkeitenverfahren einzuleiten, habe ich in einigen Fällen auch Gebrauch gemacht.

8.1.2 Öffentlich gewidmeter Gebäudedurchgang in Privatbesitz

Im Zusammenhang mit der durch öffentliche Mittel geförderten Sanierung eines Wohn- und Geschäftshauses hatte eine Kommune mit den Eigentümern vereinbart, dass aus Gründen der Verkehrssicherheit durch dieses Gebäude zukünftig eine Passage als Verbindungsweg führen sollte. Nach Fertigstellung sollte diese Passage dann gewidmet und auf diese Weise öffentlicher Gehweg werden. Kurz vor dem Abschluss der Baumaßnahme teilten die Eigentümer dann mit, dass sie beabsichtigten, an den beiden Eingängen der Passage jeweils eine Videokamera zu installieren, um Verschmutzungen und Beschädigungen des Gebäudekörpers zu dokumentieren, die Verursacher zu ermitteln und anschließend zur Rechenschaft zu ziehen. Da die Kommune gegen eine solche Videoüberwachung eines öffentlichen Gehweges durch eine Privatperson datenschutzrechtliche Bedenken geltend machte, wandte man sich – letztendlich gemeinsam – an mich.

In der Tat wirft die geplante Videoüberwachung einer öffentlichen Passage durch einen privaten Eigentümer als verantwortliche Stelle eine Reihe datenschutzschutzrechtlicher Fragen auf und ist alles andere als unproblematisch zu betrachten. Dabei war insbesondere auch zu berücksichtigen, dass sich in der Passage auch der Hauseingang zu den in diesem Gebäude errichteten Mietwohnungen befindet.

Die datenschutzrechtliche Bewertung hat dabei auf der Grundlage von § 6b Abs. 1 Nr. 3 und Abs. 3 BDSG zu erfolgen. Nach dieser Vorschrift ist eine Videobeobachtung öffentlich zugänglicher Räume nur zulässig, soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Die weitere Verarbeitung (Speicherung) oder Nutzung der Videodaten erfordert eine nochmalige Abwägung nach den bereits genannten Kriterien.

Der von den Eigentümern angeführte Schutz ihres Eigentums gegen Beschädigungen des Baukörpers, also die diesbezügliche Prävention einerseits und die Beweissicherung im Schadensfall andererseits, war grundsätzlich als berechtigtes Interesse zu werten. Das Risiko entsprechender Beschädigungen hatten diese mit einschlägigen eigenen Erfahrungen sowie den baulichen Besonderheiten des Durchgangs (Mauerversatz) auch nachvollziehbar begründet.

Dem entgegen standen jedoch die schutzwürdigen Interessen der Passanten, im Zuge der Nutzung der Passage nicht von Privatpersonen beobachtet und diesbezüglichen Aufzeichnungen ausgesetzt sein zu müssen, ohne deren weitere Nutzung in irgendeiner Weise beeinflussen zu können. Mit der zunächst geplanten Komplettüberwachung der Passage wäre in erheblicher Weise in die Individualsphäre der Passanten eingegriffen worden. Ein

Durchqueren der Passage wäre schlichtweg unmöglich gewesen, ohne dass dies mittels Videoaufzeichnungen dokumentiert worden wäre. Die Individualsphäre schützt das Selbstbestimmungsrecht und bewahrt die persönliche Eigenart der Menschen in ihren Beziehungen zur Umwelt, d. h. ihrem öffentlichen, wirtschaftlichen, beruflichen Wirken. Nach der Rechtsprechung des Bundesgerichtshofs (Urteil vom 25. April 1995 – VI ZR 272/94, juris) haben Privatleute von notwehrähnlichen Situationen abgesehen nicht das Recht, durch Videoaufzeichnungen Passanten auf öffentlichen Wegen zu erfassen. Das verfassungsmäßige Recht auf informationelle Selbstbestimmung verbürgt insoweit das Recht des Einzelnen, sich insbesondere in der Öffentlichkeit frei und ungezwungen bewegen zu dürfen, ohne befürchten zu müssen, ungewollt zum Gegenstand einer Videoüberwachung gemacht zu werden.

Dies gilt in gleicher Weise für die zukünftigen Bewohner des Gebäudes. Der Hauseingang zu den im Gebäude einzurichtenden Wohnungen befand sich direkt im Durchgang. Das Amtsgericht München hat entschieden, dass die Überwachung eines Hauseingangs durch eine Kamera – und zwar unabhängig davon, ob eine Speicherung der Bilder erfolgt – einen erheblichen Eingriff in das Persönlichkeitsrecht des Mieters darstellt (Urteil vom 16. Oktober 2009 – 423 C 34037/08, juris). Das allgemeine Persönlichkeitsrecht umfasse auch die Freiheit von unerwünschter Kontrolle und Überwachung durch Dritte. Dies beinhalte für den Mieter einer Wohnung nicht nur die Freiheit, die eigene Wohnung zu verlassen und zu betreten, ohne dass dies überwacht wird. Es beinhalte auch das Recht, ungestört und unüberwacht Besuch zu empfangen.

Vor diesem Hintergrund führten die nach § 6b Abs. 1 Nr. 3 und Abs. 3 BDSG vorzunehmenden Abwägungen zwischen dem Interesse der Betreiber am Schutz ihres Eigentums und dem Persönlichkeitsrecht der Betroffenen im Fall der beabsichtigten Komplettüberwachung zu einem deutlichen Überwiegen der schutzwürdigen Interessen der Passanten, den Durchgang passieren zu können, ohne dass dies stets mittels Videoaufzeichnungen dokumentiert wird. Insoweit stellte die bestehende Umgehungsmöglichkeit entlang öffentlicher Straßen auch keine ins Gewicht fallende Alternative dar, da sie in besonderem Maße gefahrengeneigt und aufwändig war (fehlender Bürgersteig bzw. mehrere Straßenquerungen). Eben aus diesem Grund war ja die Passage auch gebaut worden.

Die beschriebene Abwägung konnte allerdings dann zugunsten des Überwachungsinteresses der Eigentümer ausgehen, wenn sie die Überwachung auf den insoweit besonders kritischen Bereich der im Durchgang liegenden Gebäudeecke beschränkten. Dabei müsste einerseits sichergestellt sein, dass der innenliegende Hauseingang nicht mit überwacht wird, und die zu installierende Kamera müsste andererseits so eingestellt werden, dass Passanten dann nicht erfasst werden, wenn sie sich normal in der Mitte des Durchgangs bewegen. Dem Stand der Technik entsprechende Kameras bieten hierfür die Möglichkeit

der Einstellung so genannter Privatzonen, d. h. es können Teile des tatsächlichen Erfassungsbereiches geschwärzt oder verpixelt und die Videoüberwachung damit auf die wirklich relevanten Bereiche beschränkt werden.

In Bezug auf die Speicherdauer von Videoaufzeichnungen gibt § 6b Abs. 5 BDSG vor, dass diese unverzüglich zu löschen sind, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. Vor diesem Hintergrund bestanden gegen die von den Eigentümern vorgesehene fortlaufende Überschreibung der Videoaufnahmen innerhalb von 24 Stunden keine Einwände. Es versteht sich von selbst, dass als Beweismittel nach einem Vorfall gesicherte Videoaufzeichnungen dessen ungeachtet bis zur Klärung des betreffenden Vorfalls aufbewahrt werden können.

Nach § 6b Abs. 2 BDSG besteht die Verpflichtung, den Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen, d. h. den videoüberwachten Bereich entsprechend zu kennzeichnen. Praktisch bedeutet dies, dass an beiden Eingängen der Passage entsprechende Hinweisschilder anzubringen sind, aus denen insbesondere auch hervorgehen muss, wer konkret für den Betrieb der Videoüberwachung verantwortlich und wie er zu erreichen (Anschrift) ist.

8.1.3 Öffentlicher Grünstreifen vor einem Privatgrundstück

Nachdem bereits in der regionalen Presse über Videokameras, die von einem privaten Grundstück aus auf öffentliche Verkehrsbereiche – zumindest – gerichtet waren, berichtet worden war, gelangte der Fall auch an mich.

Das betreffende Grundstück war von einer Mauer umgeben, daran schlossen sich ein etwa drei Meter breiter, mit jungen Bäumen bepflanzter Grünstreifen und schließlich ein unbefestigter öffentlicher Weg an. Auf zwei Gebäuden waren je eine Videokamera installiert, die offensichtlich auch Bereiche außerhalb der Grundstücksgrenze erfassten und durch die sich – jedenfalls nach Aktenlage – insbesondere einige Nachbarn in ihrem Persönlichkeitsrecht beeinträchtigt fühlten.

Der Grundstückseigentümer erläuterte mir, dass er seit mehr als zwei Jahren zunächst vollkommen uneigennützig, später dann auf der Grundlage eines mit der Kommune abgeschlossenen Pflegevertrages, die Pflege der Rasenfläche und der darauf gepflanzten Jungbäume übernommen und dabei auch eigene finanzielle Mittel eingesetzt, beispielsweise auf eigene Kosten Hochborde zum Schutz gegen das Überfahren der Grünfläche gesetzt hatte. In dieser Zeit habe er immer wieder mit mutwilligen Zerstörungen der Grünfläche kämpfen müssen: Bordsteine seien mit der Spitzhacke zerhackt, Wiese und Bäume wiederholt mit Gift besprüht, Müll auf die Rasenfläche platziert, Bäume abgesägt und die Grasfläche mit schwerem Gerät überfahren worden. Dazu legte er mir umfangreiche

Unterlagen (Pflegevertrag, Presseveröffentlichungen, Strafanzeigen) vor, die den Sachverhalt vollumfänglich bestätigten. Sofort nach Installation der Kameras seien bestimmte Nachbarn auf den Plan getreten und hätten lauthals gegen die Videokameras gewettert – der aufmerksame Leser denkt sich seinen Teil.

Die mir zudem übergebenen Screenshots belegten, dass sich der Erfassungsbereich der beiden Videokameras in der Tat auf den Grünstreifen beschränkte. Darüber hinausgehende Bereiche, insbesondere der Wirtschaftsweg, waren ausgeblendet worden. Da es sich bei dem überwachten Bereich zudem um eine Grünfläche handelte, die üblicherweise nicht von Passanten betreten wird, insbesondere auch nicht dazu bestimmt ist, habe ich die schutzwürdigen Interessen eventuell Betroffener als nur geringfügig tangiert betrachtet. An dem berechtigten Überwachungsinteresse des Betreibers und der Erforderlichkeit der Videoüberwachung habe ich unter den gegebenen Umständen keine Zweifel gehegt, sodass ich hier zu dem Abwägungsergebnis gelangt bin, dass die Videoüberwachung in der praktizierten Form zulässig ist.

8.1.4 Öffentlicher Verkehrsraum bei außergewöhnlichen Gefährdungssituationen

Grundsätzlich dürfen Private den öffentlichen Verkehrsbereich vor ihrem Grundstück nicht mittels Videokameras überwachen, selbst wenn es in der Vergangenheit zu Sachbeschädigungen (Graffitis) oder Einbrüchen kam (siehe 7/8.1.4.)

Ich hatte die Frage zu entscheiden, ob es ausnahmsweise zulässig ist, dass Private Teilbereiche des öffentlichen Fußwegs vor ihrem Grundstück mittels Videokameras überwachen dürfen, wenn es in der Vergangenheit zu erheblichen Straftaten gekommen war. Da in den konkreten Fällen eine Gefährdungseinschätzung der Sicherheitsbehörden für das jeweilige Objekt vorlag, die weitere schwerwiegende Straftaten zum Nachteil der verantwortlichen Stellen befürchten ließ, habe ich im Ergebnis der nach § 6b Abs. 1 Nr. 3, Abs. 3 BDSG durchzuführenden umfassenden Interessenabwägung die Videoüberwachung eines schmalen Streifens des öffentlichen Gehwegs ausnahmsweise für datenschutzrechtlich vertretbar erachtet.

8.1.5 Treppenhäuser, Hauseingänge

Die Unzulässigkeit der Videoüberwachung von Hauseingängen war schon Gegenstand unter 3/4.2.1.3. Die Thematik ist weiterhin aktuell, wie mehrere Kontrollen zeigten. Die Betreiber der Videokameras, meist Eigentümer oder Vermieter, aber auch Gewerbemieter, begründen die Notwendigkeit der Videoüberwachungsanlagen meist damit, dass auf diese Weise Straftaten verhindert oder aufgeklärt werden sollen. Teilweise wird auch dahingehend argumentiert, dass die Wohnungen schlechter vermietbar seien, wenn keine

Videokameras installiert wären. Allerdings zeigen Eingaben von Mietern, dass es keinesfalls so ist, dass es diesen egal ist, ob sie videoüberwacht werden oder nicht.

Gesetzliche Grundlagen für die Videoüberwachung

Soweit Kameras öffentlich zugängliche Bereiche (z. B. Gehweg, Straße, Grünflächen und Spielplätze auf dem Gelände, den Eingangsbereich vor der Haustür, den Abstellplatz von Müllcontainern, Fahrradständer außerhalb des Hauses, die außen angebrachten Briefkästen) erfassen, ist ihr Einsatz an § 6b BDSG zu messen. Gemäß § 6b Abs. 1 Nr. 3 und 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 (z. B. Mieter, Besucher, Handwerker, Postbote) überwiegen.

Hinsichtlich der nicht öffentlich zugänglichen Bereiche (z. B. verschlossen gehaltene Hausflure, Treppenhäuser, Aufzüge, Waschmaschinen- und Trockenräume sowie Fahrradkeller) richtet sich die Zulässigkeit der Videoüberwachung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Danach ist das Erheben, Speichern und Nutzen personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass schutzwürdige Interessen der Betroffenen am Ausschluss der Verarbeitung oder Nutzung überwiegen.

Beide Vorschriften setzen folglich voraus, dass die verantwortliche Stelle mit der Videoüberwachung berechtigte Interessen verfolgt und dass die Videoüberwachung geeignet, erforderlich und verhältnismäßig ist. Die Verhinderung von Straftaten bzw. der Eigentumsschutz (präventive Zwecke) sowie die Aufklärung von Schadensfällen (repressive Zwecke) stellen dabei berechtigte Interessen des Vermieters, Eigentümers oder Gewerbemieters dar. In beiden Fällen ist eine umfassende Interessenabwägung vorzunehmen, wobei grundsätzlich die durch das Recht auf informationelle Selbstbestimmung geschützte Privatsphäre der von der Videoüberwachung Betroffenen bei einer Videoüberwachung nicht öffentlich zugänglicher Bereiche eine größere Bedeutung hat als im öffentlich zugänglichen Raum.

Man kann schon daran Zweifel haben, ob die Videoüberwachung geeignet ist, Diebstähle und Sachbeschädigungen zu verhindern. Denn es müsste schon ständig jemand vor dem Monitor sitzen und sich die Videobilder live ansehen, um dann direkt und hoffentlich noch rechtzeitig einschreiten zu können, um den Täter abzuwehren. Tatsächlich werden die Videoaufnahmen herangezogen, um die Straftat aufzuklären, was jedoch in der Regel nur gelingt, wenn der Täter gut erkennbar und (polizei-)bekannt ist.

Des Weiteren habe ich erhebliche Bedenken, ob die im Hausflur oder in Treppenhäusern angebrachten Videokameras erforderlich sind, d. h., ob es nicht gleich wirksame Mittel gibt, um insbesondere die typischen Straftaten zu verhindern. Gleich abschreckend wie funktionierende Kameras wirken z. B. Hinweisschilder in Verbindung mit Attrappen.

Wenn es darum geht, im Hausflur abgestellte Gegenstände von Mietern (z. B. Fahrräder, Kinderwagen) zu schützen, kommt anstatt einer Rund-um-die-Uhr-Videoüberwachung des Hausflurs auch die Aufforderung an die Mieter in Betracht, ihr Eigentum in einen abschließbaren Keller- oder Fahrradraum zu stellen oder in ihrer Gewerbeeinheit zu lagern. Vermieter sind grundsätzlich nicht verpflichtet, das im Hausflur abgestellte Eigentum ihrer Mieter vor Verlust zu schützen, hierfür sind in erster Linie die Mieter selbst verantwortlich. Wenn die Mieter darauf verzichten, ihr Eigentum durch Abstellen in einen abschließbaren Keller- oder Fahrradraum angemessen zu schützen, tragen allein die Mieter das Verlustrisiko. Auch aus brandschutzrechtlichen Gründen dürfte das Zustellen von Fluchtwegen mit Gegenständen bedenklich sein.

Als Alternative zu einer umfassenden Videoüberwachung hat der Vermieter bzw. Eigentümer zudem zu prüfen, ob Eingangs- und Kellertüren nicht dauerhaft verschlossen bleiben können und eine Gegensprechanlage angeschafft werden soll. Wohnungseinbrüche lassen sich in erster Linie und wesentlich effektiver als durch eine Videoüberwachung des Hausflurs oder der Treppenhäuser durch sicherheitstechnische Maßnahmen (entsprechende Schlösser, verstärkte Türen, Alarmanlagen) verhindern.

Im Regelfall ist die Videoüberwachung jedenfalls unverhältnismäßig: Die schutzwürdigen Belange der Betroffenen überwiegen das Interesse der Betreiber von Videoüberwachungsanlagen, insbesondere wenn die Kameras den gesamten Hausflur von der Hauseingangstür bis zum Treppenaufgang komplett erfassen. Denn dann lässt sich ggf. über mehrere Tage (auch per Fernzugriff über das Internet) beobachten und kontrollieren, wer wann mit wem das Haus betritt und verlässt. Dies stellt einen erheblichen Eingriff in das Persönlichkeitsrecht der Mieter dar. Diese können sich der Videoüberwachung in der Regel nicht entziehen, weil der Hausflur der einzige reguläre Zugang zu ihrer Wohnung und zu den Briefkästen ist. Bereits die Möglichkeit, dass der Vermieter, Eigentümer oder Gewerbemieter jederzeit kontrollieren kann, welcher Mieter wann welchen Besuch empfängt, kommt oder geht, setzt die Mieter einem erheblichen Überwachungs- und Anpassungsdruck aus. Gespeicherte Videoaufnahmen beinhalten zusätzlich ein erhebliches Missbrauchspotential.

Nicht vergessen werden darf bei der umfassenden Interessenabwägung auch, dass die Aufklärung und Verfolgung von Straftaten den staatlichen Ermittlungsbehörden obliegt, die sich dazu auch nur der Mittel bedienen dürfen, die die Strafprozessordnung vorsieht.

Die Videoüberwachung gehört bei den in Betracht kommenden Straftaten regelmäßig nicht dazu.

Einwilligung der Mieter

Eine Reihe von Vermietern versucht daher die Videoüberwachung auf Einwilligungserklärungen der Mieter zu stützen. Eine solche Einwilligung ist gemäß § 4a Abs. 1 BDSG jedoch nur wirksam, wenn sie auf der freien Entscheidung der Mieter beruht. Diese sind auf den vorgesehenen Zweck der Videoüberwachung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen (z. B. Mietvertragsabschluss) schriftlich erteilt werden, ist sie besonders hervorzuheben.

Zweifel bestehen in der Regel an der erforderlichen Freiwilligkeit der entsprechenden Erklärungen der Mieter. Freiwilligkeit bedeutet, dass sich die von der Videoüberwachung Betroffenen nicht in einer Situation befinden dürfen, die sie faktisch dazu zwingt, sich mit dem Zugriff auf ihre Daten einverstanden zu erklären. Derartige Situationen sind typischerweise gegeben, wenn ein Abhängigkeits- oder Über-/Unterverhältnis besteht (Simitis in Simitis, BDSG, 8. Auflage, § 4a Rdnr. 62) oder die Einwilligung unter Ausnutzung einer wirtschaftlichen Machtposition verlangt wurde (Gola/Schomerus, BDSG, 12. Auflage, § 4a Rdnr. 19). Diese Voraussetzungen sind bei Wohnungsmietverträgen regelmäßig erfüllt: Es droht die Kündigung oder der Nichtabschluss des Mietvertrags, wenn – wie dies häufig der Fall sein wird (prekäre Wohnungssituation) – der Vermieter in einer stärkeren Position ist. Die Mieter haben dann aufgrund des Machtungleichgewichts praktisch keine echte Alternative, als sich mit der Videoüberwachung einverstanden zu erklären.

Häufig ist die Einwilligungserklärung auch deshalb unwirksam, weil die Mieter u. a. nicht umfassend über den Zweck der Videoüberwachung, Zugriffsrechte, Auswertungsmöglichkeiten, Speicher- und Löschfristen informiert wurden.

Für den Vermieter ist eine Einwilligungslösung auch darüber hinaus mit erheblichen Risiken verbunden. Denn die Mieter haben jederzeit das Recht, ihre Einwilligungen mit Wirkung für die Zukunft zu widerrufen. Es reicht der Widerruf einer Mietvertragspartei und schnell erweist sich die Videoüberwachungsanlage – wenn sich die Videoüberwachung nicht ausnahmsweise auf eine gesetzliche Rechtsgrundlage stützen lässt – als teure Fehlinvestition. Zudem berücksichtigt die Einwilligungslösung nicht, dass z. B. auch

Besucher des Hauses, der Postbote und Handwerker weder in die Videoüberwachung eingewilligt haben noch sich dieser wirksam entziehen können (ohne ggf. arbeitsrechtliche Konsequenzen oder soziale Nachteile zu gegenwärtigen).

8.1.6 Notfallaufnahme

Ein privates Krankenhaus hatte alle Behandlungszimmer in der Notfallaufnahme mit Videokameras ausgestattet, deren Bilder in das Arzt-/Schwesternzimmer der Notfallaufnahme übertragen wurden. Begründet wurde die Videoüberwachung damit, dass die Notfallaufnahme von vielen Menschen mit meist akuten und unklaren Beschwerden aufgesucht wird. Um auch Patienten mit einer geringen Behandlungspriorität die Möglichkeit zu geben, ungestört von Mitpatienten zu warten, wurden die Patienten schnellstmöglich in einen der Untersuchungsräume gebeten. Das Krankenhaus argumentierte, dass die Videobeobachtung im Untersuchungsraum notwendig sei, weil sich der Gesundheitszustand der länger wartenden Patienten akut verschlechtern bzw. eine lebensbedrohliche Situation entstehen könne. Ältere Patienten fühlten sich oft mit der Bedienung der Rufanlage überfordert; suchtkranke bzw. alkoholisierte Patienten könnten aggressiv werden; Simulanten könnten leichter identifiziert werden. Die Videoüberwachung diene einer kontinuierlichen Gewährleistung der Patientensicherheit, zumal die Untersuchungsräume dezentral gelegen und damit vom Arzt-/Schwesternzimmer schwer einsehbar seien. Aufgrund der Eingabe war bekannt, dass die Videokameras auch während der Behandlung liefen.

Die Videoüberwachung war datenschutzrechtlich unzulässig: Ohne Einwilligung der Betroffenen dürfen Patientendaten (zu denen auch derartige Videoaufnahmen gehören) nur dann erhoben werden, soweit dies zur Erfüllung der Aufgaben des Krankenhauses oder im Rahmen des krankenhausärztlichen Behandlungsverhältnisses erforderlich ist (§ 28 Abs. 6 und Abs. 7 BDSG). Dies bedeutet, dass eine Videobeobachtung ohne ausdrückliche, informierte, schriftliche Einwilligung der Patienten (§ 4a BDSG) nur insoweit erlaubt ist, als dies zwingend medizinisch erforderlich ist. Die Videobeobachtung selbst ist regelmäßig keine unmittelbare Maßnahme der Heilbehandlung, sondern allenfalls insoweit medizinisch erforderlich, wie der Patient überwachungsbedürftig ist.

Das bedeutet: Bei Prüfung der datenschutzrechtlichen Zulässigkeit der Videoüberwachung ist ein strenger Maßstab an Zweckverfolgung, Erforderlichkeit und Verhältnismäßigkeit anzulegen, denn bei Einsatz der Videotechnik werden besondere Arten von personenbezogenen Daten (§ 3 Abs. 9 BDSG) erhoben. Videoüberwachung im Krankenhaus kann immer nur in Ausnahmefällen gerechtfertigt sein.

Im konkreten Fall bestanden bereits Zweifel an der Geeignetheit der Videoüberwachung, nämlich die Patientensicherheit zu gewährleisten, d. h. eine sofortige Reaktion des medizinischen Personals in plötzlich auftretenden Notsituationen zu erreichen. Hierzu hätte (was nicht der Fall war) qualifiziertes Personal eine Vielzahl von Bildübertragungen permanent im Auge behalten und daraus die zutreffenden medizinischen Schlüsse ziehen müssen. Insofern war zweifelhaft, ob man anhand der Videoaufnahmen (aus der Ferne) erkennen kann, ob sich der Gesundheitszustand eines sitzenden oder ggf. bereits liegenden Patienten akut verschlechtert, er z. B. ohnmächtig wird. Auch stärkere Schmerzen wird man kaum – sofern keine grundsätzlich unzulässige Tonübertragung erfolgt – auf diese Weise feststellen können. Während der Behandlung hätten die Videokameras zudem ausgeschaltet werden müssen. Auch war eine Speicherung der Videoaufnahmen für die dargelegten Zwecke überflüssig: Denn eine Überwachung der in den Behandlungszimmern wartenden Patienten mittels Videokameras, um Notsituationen rechtzeitig erkennen und hierauf reagieren zu können, kann nur zeitlich unmittelbar und nicht nachträglich anhand einer Auswertung der gespeicherten Aufnahmen erfolgen.

Darüber hinaus war die Videoüberwachung auch nicht erforderlich. Eine Sitzwache oder regelmäßige Kontrollen durch medizinisches Personal sind nämlich zur Zweckerreichung gleich geeignete, aber im Hinblick auf das Grundrecht auf informationelle Selbstbestimmung der Patienten deutlich mildere Mittel. Fehlendes Personal für eine örtliche Dauerüberwachung (Sitzwache) oder regelmäßige Kontrollbesuche bei den in den Behandlungsräumen wartenden Patienten rechtfertigen ebenso wenig wie haftungsrechtliche Gründe eine Beobachtung mit optoelektronischen Mitteln.

Letztlich ist die Videobeobachtung von Behandlungszimmern wegen der verhaltenslenkenden Wirkung und des potentiellen Überwachungsdrucks als schwerwiegender Eingriff in das informationelle Selbstbestimmungsrecht des betroffenen Patienten zu werten und daher unverhältnismäßig. Bei Behandlungszimmern handelt es sich um besonders sensible Bereiche. Im konkreten Fall war auch zu berücksichtigen, dass die Patienten bei der geschilderten Organisation der Notfallaufnahme gar keine andere Wahl hatten, als sich in einen videoüberwachten Behandlungsraum zu begeben, weil sie sonst im Wartezimmer höchst wahrscheinlich vergessen worden wären.

Im Ergebnis war ein weiteres aufsichtsbehördliches Einschreiten jedoch nicht notwendig: Das Krankenhaus hatte auf die Beschwerde eines Patienten noch vor meinem Tätigwerden reagiert und die Videoüberwachung der Notfallaufnahme eingestellt.

8.1.7 Psychiatrie

Bei zwei Beratungsanfragen ging es darum, dass private psychiatrische Krankenhäuser beabsichtigten, auf (geschlossenen) Stationen, insbesondere in Patientenzimmern, aber auch im Raucherzimmer, in Treppenhäusern und im eingefriedeten Außenbereich Videokameras zu installieren. Die Videobilder sollten nicht aufgezeichnet, sondern lediglich auf einen Monitor im Arzt-/Schwesternzimmer live übertragen werden (reines Monitoring-System). Die Videokameras sollten jederzeit separat ein- und ausgeschaltet werden können. Verhindert werden sollte mit der Videobeobachtung in erster Linie fremd- und selbstgefährdendes Verhalten der Patienten.

Gesetzliche Rechtsgrundlagen für die Videoüberwachung im Krankenhaus

Ohne wirksame Einwilligung der Betroffenen (oder ggf. deren gesetzlicher Vertreter/ Betreuer) dürfen Patientendaten, zu denen auch Bildaufnahmen gehören, als besondere personenbezogene Daten nur dann erhoben werden, soweit dies zur Erfüllung der Aufgaben des Krankenhauses oder im Rahmen des krankenhausärztlichen Behandlungsverhältnisses erforderlich ist (§ 28 Abs. 6 und Abs. 7 BDSG bzw. § 33 Abs. 2 SächsKHG). Dies bedeutet, dass eine Videobeobachtung ohne ausdrückliche, informierte, schriftliche Einwilligung der Patienten (§ 4a BDSG bzw. § 33 Abs. 2 SächsKHG) nur insoweit erlaubt ist, als dies zwingend medizinisch erforderlich ist. Dabei kann die Videobeobachtung bei überwachungsbedürftigen Patienten grundsätzlich medizinisch notwendig sein.

Die Videoüberwachung muss allerdings geeignet sein, um den mit ihr verfolgten Zweck auch zu erreichen. Sie ist zudem im datenschutzrechtlichen Sinne nur dann erforderlich, wenn es kein milderes Mittel zur Erreichung des angestrebten zulässigen Zwecks gibt. D. h., die Videoüberwachung muss unter den zur Verfolgung eines legitimen Zwecks (hier Erhöhung der Patientensicherheit) zur Verfügung stehenden geeigneten Maßnahmen diejenige sein, die das Grundrecht des Betroffenen auf informationelle Selbstbestimmung und ggf. seiner Menschenwürde am wenigsten beeinträchtigt. Insofern bestehen grundsätzliche Bedenken. Denn um die Sicherheit der Patienten zu erhöhen, indem selbst- oder fremdgefährdendes Verhalten möglichst frühzeitig erkannt und durch Personal Schlimmeres verhindert werden kann, wäre es notwendig, dass ständig ausreichend qualifiziertes Personal vor dem Monitor sitzt und im Ernstfall unverzüglich Alarm schlägt. Dies dürfte in der Realität jedoch selten der Fall sein. Davon abgesehen gibt es mildere Mittel, mit denen sich die Patientensicherheit gleichermaßen erhöhen lässt. Denn anstatt ständig vor dem Monitor zu sitzen, könnte dieser Mitarbeiter auch regelmäßig in die Patientenzimmer sehen, in den Raucherraum schauen und durch das Treppenhaus und den Außenbereich laufen.

Darüber hinaus muss die Videoüberwachung verhältnismäßig sein, was eine Abwägung der Interessen des Krankenhauses an der Videoüberwachung mit den (verfassungs-)rechtlich geschützten Positionen der Patienten, aber auch der Mitarbeiter (§ 32 Abs. 1 BDSG) und Besucher (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG) unter Würdigung aller Umstände des Einzelfalls bedingt. Eine dauerhafte Videobeobachtung ist wegen der verhaltenslenkenden Wirkung und des Kontroll- und Einschüchterungspotenzials auch in anderen Fällen immer als besonders schwerwiegender Eingriff in das informationelle Selbstbestimmungsrecht der hiervon Betroffenen zu werten. Die Patientenzimmer stellen für die Patienten für die Dauer ihres Aufenthalts auf der geschlossenen Station auch Rückzugs- und Ruheraum dar. Die Beobachtung mittels Videokamera erfasst den höchstpersönlichen Lebensbereich des Patienten (siehe § 201a StGB).

Der empfundene Überwachungsdruck, den Kameras selbst dann auslösen, wenn sie nicht eingeschaltet sind, ist – je nach Krankheitsbild – bei Menschen, die stationärer psychiatrischer Behandlung bedürfen, unter Umständen sogar noch deutlich gesteigert. Erst recht gilt dies, wenn der betreffende Patient den Raum nicht verlassen und sich der Videobeobachtung nicht einmal vorübergehend entziehen kann. Aber auch in den übrigen Fällen muss den Patienten ein kamerafreier Rückzugsraum verbleiben, was – wenn bereits die Patientenzimmer mit Videokameras ausgestattet sind – gegen eine Videoüberwachung von Raucherzimmer und Außenbereich spricht, die in erster Linie dem geselligen Miteinander und der Entspannung dienen sollen. Fehlendes Personal für eine örtliche Dauerüberwachung (1:1-Betreuung) oder für regelmäßige Kontrollbesuche bei den Patienten rechtfertigen ebenso wenig wie haftungsrechtliche Gründe eine Beobachtung mit optoelektronischen Mitteln. Die Videoüberwachung im psychiatrischen Krankenhaus kann deshalb nur in Ausnahmefällen gesetzlich gerechtfertigt sein.

Zu beachten ist außerdem, dass die Videoüberwachung nicht zu einer dauerhaften Überwachung von Beschäftigten führen darf (§ 32 Abs. 1 BDSG). Im Falle einer 1:1-Betreuung, d. h. wenn sich neben dem Patienten auch ständig oder überwiegend ein Mitarbeiter in den Patientenzimmern aufhält, wäre die Videobeobachtung unzulässig. Eine wirksame Einwilligung im Arbeitsverhältnis scheidet wegen des bestehenden Über- und Unterordnungsverhältnisses regelmäßig aus.

Als Maßnahme des technischen Datenschutzes ist sicherzustellen, dass die Videokameras in den Patientenzimmern nicht die Bäder erfassen und dass die Monitore nicht für Unbefugte zugänglich und einsehbar sind. Tonaufnahmen und die Möglichkeit der Speicherung von Bildaufnahmen sind bauartbedingt oder technisch in jedem Fall irreversibel auszuschließen. Die Kameras müssen zudem jederzeit ohne Schwierigkeiten einzeln an- und abschaltbar sein. Anlass, Anordnung, Umfang und Dauer der Maßnahmen sind umfas-

send zu dokumentieren. Der Einsatz der Videoüberwachung muss auf einer dokumentierten ärztlichen Gefahreneinschätzung beruhen und sich auf das zeitlich Erforderliche beschränken. Die betroffenen Patienten sowie ggf. ihre gesetzlichen Vertreter/Betreuer sind über die Videoüberwachung und ihre Zwecke zu informieren.

Einwilligungslösung

Soweit danach die Voraussetzungen des § 28 Abs. 7 BDSG bzw. § 33 Abs. 2 SächsKHG (bzw. hinsichtlich eventueller Besucher des § 28 Abs. 1 Nr. 2 BDSG bzw. § 33 Abs. 2 SächsKHG) nicht vorliegen, kann die Videoüberwachung nur auf der Grundlage einer wirksamen Einwilligung erfolgen. Gemäß § 4a Abs. 1 Satz 1 BDSG ist die Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Die Einwilligung muss informiert erfolgen, d. h. der Betroffene muss über den Zweck der Videoüberwachung aufgeklärt werden (§ 4a Abs. 1 Satz 2 BDSG bzw. § 33 Abs. 2 SächsKHG). Die Einwilligung ist grundsätzlich schriftlich zu erteilen (§ 4a Abs. 1 Satz 3 BDSG bzw. § 33 Abs. 2 Satz 1 SächsKHG) und sie sollte grundsätzlich nicht mit anderen Erklärungen gemeinsam erfolgen (§ 4a Abs. 1 Satz 4 BDSG). Der Patient ist darauf hinzuweisen, dass ihm wegen der Verweigerung der Einwilligung keine Nachteile entstehen (§ 33 Abs. 2 Satz 4 SächsKHG). Ratsam ist es auch, den Patienten auf die Möglichkeit hinzuweisen, dass er seine Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. Im Falle von Gesundheitsdaten muss sich die Einwilligung auch ausdrücklich auf die Erhebung dieser besonderen Arten von personenbezogenen Daten beziehen (§ 4a Abs. 3 BDSG).

Zweifelhaft kann bei psychisch Kranken sein, ob die Einwilligung freiwillig erfolgt. Im datenschutzrechtlichen Kontext spricht man von einer freien Entscheidung nur dann, wenn die Betroffenen (hier Patienten) sich nicht in einer Lage befinden, die sie faktisch dazu zwingt, sich mit der Videoüberwachung einverstanden zu erklären (Simitis in Simitis, BDSG, 8. Auflage, § 4a Rdnr. 62). Die Patienten müssen eine echte Wahl haben, ob sie der Videoüberwachung zustimmen oder ob sie sie ablehnen, ohne dadurch einen Nachteil zu erleiden (Taeger in Taeger/Gabel, BDSG, 2. Auflage, § 4a Rdnr. 52). Diese Voraussetzungen dürften am ehesten erfüllt sein, wenn Patienten auch auf einem separaten Einwilligungsformular echte Alternativen eingeräumt werden: z. B ❒ Ja, ich bin mit einer Videoüberwachung meines Patientenzimmers einverstanden. ❒ Nein, ich bin mit einer Videoüberwachung meines Patientenzimmers nicht einverstanden.

Kritisch ist darüber hinaus die Frage, ob psychisch kranke Patienten überhaupt einwilligungsfähig sind, d. h. über die nötige Einsichtsfähigkeit verfügen, selbst über die Verwendung ihrer personenbezogenen Daten unter den konkreten Bedingungen einer geschlossenen psychiatrischen Station zu entscheiden. In der betreuungsrechtlichen Literatur und

Rechtsprechung wird auf die natürliche Einsichts- und Steuerungsfähigkeit des Patienten in Bezug auf die konkrete Einwilligungserklärung abgestellt, wobei deren Vorliegen regelmäßig durch einen medizinischen Sachverständigen festzustellen wäre. Datenschutzrechtlich wird vertreten, dass minderjährige Patienten, die in der Lage sind, Notwendigkeit und Tragweite einer ärztlichen Behandlung zu beurteilen, sodass diese nicht ohne ihr Einverständnis vorgenommen werden darf, auch selbst darüber bestimmen können müssen, wie ihre Gesundheitsdaten verwendet werden (Simitis, a. a. O., § 4a Rdnr. 23 m. w. N.).

Vor diesem Hintergrund halte ich auch die Annahme einer wirksamen Einwilligung psychisch Kranker, soweit ihre Einwilligungsfähigkeit etwa im Hinblick auf ärztliche Behandlungsmaßnahmen konkret feststeht, nicht für generell ausgeschlossen. Ob und unter welchen Voraussetzungen ein Betreuer im Falle der Einwilligungsunfähigkeit des Patienten in die Videoüberwachung einwilligen kann, ist in erster Linie eine betreuungsrechtliche Frage und überschreitet damit meinen Zuständigkeitsbereich.

Die Einwilligungslösung ist allerdings mit dem Risiko verbunden, dass das Krankenhaus im Beschwerdefall nachweisen können muss, dass der konkrete Patient bei der Erklärung einwilligungsfähig war. Zudem ist sicherzustellen, dass immer dann, wenn der Patient seine Einwilligung widerruft oder für den Fall, dass später Einwilligungsunfähigkeit eintritt, und er mit seinem sogenannten natürlichen Willen zum Ausdruck bringt, dass er die Videoüberwachung ablehnt, die Videokamera unverzüglich ausgeschaltet wird.

Praktisch ausgeschlossen erscheint es, die Videoüberwachung der Treppenhäuser, des Raucherzimmers und der eingefriedeten Außenbereiche wegen der damit verbundenen Unwägbarkeiten auf die Einwilligungslösung zu stützen. Denn es werden nicht nur Patienten erfasst, die sich wirksam mit der Videoüberwachung einverstanden erklärt haben, sondern auch solche, die nicht einwilligungsfähig sind oder die der Videoüberwachung widersprochen haben. Ggf. sind auch Besucher von der Videoüberwachung betroffen. Es ist außerdem vorstellbar, dass sich Patienten mit der Videoüberwachung auch nur partiell einverstanden erklären, d. h. diese in ihrem Zimmer akzeptieren, aber nicht in den anderen Räumen und im Außenbereich.

Auch für die Einwilligungslösung gilt, dass die Videoüberwachung auf das absolut Notwendige zu beschränken und durch technisch-organisatorische Maßnahmen des Datenschutzes (§ 9 BDSG) zu flankieren ist.

Im Ergebnis bleibt festzuhalten, dass die Videoüberwachung in einem psychiatrischen Krankenhaus mit rechtlichen Risiken und tatsächlichen Schwierigkeiten verbunden ist.

Sie kann zu erheblichen Fehlinvestitionen führen, wenn sich im Nachhinein herausstellt, dass sie unzulässig ist.

8.1.8 Videodolmetschen im Krankenhaus

Im Zuge der Flüchtlingskrise sah sich ein sächsisches Krankenhaus in erhöhtem Maße mit der Problematik der Erstuntersuchung von Flüchtlingen konfrontiert. Als besonderes Problem für eine zügige und effektive Abwicklung der Untersuchungen wurden dabei die bestehenden Sprachbarrieren detektiert. Dem Krankenhaus war es praktisch nicht möglich, ständig für alle Herkunftsländer fachkundige Dolmetscher vorzuhalten bzw. kurzfristig bereitzustellen, um eine entsprechende Befragung der Flüchtlinge nach aktuellen Beschwerden und eventuellen Vorerkrankungen durchführen zu können.

Als Ausweg bot sich die Zusammenarbeit mit einer österreichischen Übersetzungsfirma an, die für die meisten der benötigten Sprachen Dolmetscher online bereitstellen konnte. Die Übersetzungsdienstleistungen sollten auf der Grundlage einer Videoverbindung erbracht werden; mit der Anforderung würde eine Verbindung vom Krankenhaus zum Übersetzungsdienst aufgebaut. Für den Zeitraum der Übersetzung bliebe die Verbindung bestehen; eine elektronische Aufzeichnung von Gesprächsinhalten sollte weder beim Krankenhaus noch beim Übersetzungsdienst erfolgen.

Grundsätzlich ist eine Nutzung derartiger Übersetzungsdienstleistungen entweder auf der Grundlage von § 33 Abs. 10 SächsKHG oder aber auf der Basis individueller Einwilligungen möglich. § 33 Abs. 10 SächsKHG schied dabei im Beispielfall praktisch allerdings aus, da es sich bei dem Übersetzungsdienst um eine österreichische Firma handelte und vom Krankenhaus nicht sichergestellt werden konnte, dass deren Mitarbeiter die § 203 StGB entsprechende Schweigepflicht einhalten.

Demnach verblieb also nur eine individuelle Einwilligung, die wegen des Einsatzes im Krankenhausumfeld als Schweigepflichtentbindung auszugestalten war. § 4a BDSG fordert diesbezüglich eine vorherige schriftliche Erklärung. Zwar kann wegen besonderer Umstände auch eine andere Form – hier die mündliche Einwilligung zu Beginn der Videoverbindung – angemessen sein, jedoch würde wohl auch bereits damit ein Verstoß gegen die Schweigepflicht nach § 203 StGB im Raum stehen. Ich habe dem Krankenhaus daher empfohlen, schriftliche Schweigepflichtentbindungen in den benötigten Sprachen vorzubereiten und diese den Betroffenen vor Beginn der Videoschaltung zur Unterschrift vorzulegen. Bei minderjährigen Kindern ist die Einwilligung durch die Eltern und je nach Einsichtsfähigkeit zusätzlich durch die Kinder zu erteilen.

Dass es sich beim Videodolmetschen um eine Verarbeitung und Nutzung besonderer Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) handelt, steht außer Frage. Eine

Vorabkontrolle ist aber wegen der vorher eingeholten Einwilligungen nicht erforderlich (§ 4d Abs. 5 Satz 2 BDSG).

Für die vertraglichen Vereinbarungen mit dem Auftragnehmer habe ich dem Krankenhaus trotz der einzuholenden individuellen Einwilligungen empfohlen, die Vorgaben zur Auftragsdatenverarbeitung (§ 11 Abs. 2 Satz 2 BDSG) zugrunde zu legen.

8.1.9 Logopädiepraxis

In meinem 4. TB habe ich mich unter den Punkten 3.2 und 4.2.1.7 ausführlich zur Zulässigkeit einer Videoüberwachung in Zahnarztpraxen geäußert. Die dortigen Ausführungen sind ohne weiteres auch auf andere Arztpraxen übertragbar. Auch im hier zu beschreibenden Fall kommt es letztendlich nicht darauf an, dass es sich um eine Logopädiepraxis handelt.

Die betreffende Praxis hatte sich im Obergeschoss eines Gewerbeobjektes eingemietet. Im Erdgeschoss befand sich eine Frühförder- und Beratungsstelle eines freien Trägers der Jugendhilfe. Beide Einrichtungen nutzten einen gemeinsamen Eingangsbereich, den der Betreiber der Logopädiepraxis mit einer Videokamera überwachte. Von der Videoüberwachung betroffen waren somit insbesondere auch die Mitarbeiter und das Klientel der Beratungsstelle.

Als Begründung für die Installation der Videokamera führte der Praxisinhaber verschiedene Zwischenfälle im Erdgeschoss des betreffenden Gebäudes an. So sei es dort zu körperlichen Auseinandersetzungen Dritter gekommen, Kinder und Erwachsene hätten randaliert, Kinder seien Roller gefahren und es hätten sich unbefugt Personen dort aufgehalten. Aus diesen Vorfällen leitete er ein besonderes Schutzbedürfnis auch für seine Patienten und sein Inventar ab. Dies war für mich aber vor allem schon deswegen nicht nachvollziehbar, weil sich seine Praxisräume im Obergeschoss des Gebäudes befanden und er selbst auch nur Mieter, nicht etwa Eigentümer war. Ich habe den Betrieb dieser Kamera daher als unzulässig bewertet; die Videoüberwachung des Eingangsbereiches im Erdgeschoss war für die vom Inhaber der Logopädiepraxis verfolgten Zwecke nicht erforderlich. Zudem waren schutzwürdige Interessen der Betroffenen verletzt, nicht zuletzt deshalb, weil auch ein großer Personenkreis mit in die Überwachung einbezogen worden war, der zu der Logopädie in keinerlei Beziehung stand, d. h. deren Praxisräume überhaupt nicht aufsuchen wollte, sondern vielmehr der Beratungsstelle im Erdgeschoss zuzurechnen war.

Wie häufig bei datenschutzrechtlichen Kontrollen, gab es bei der Prüfung des vorstehend beschriebenen Sachverhaltes auch einen Zufallsfund. Der Logopäde hatte nämlich im Flur seiner Praxisräume im Obergeschoss noch eine weitere Kamera in Betrieb.

Die Begründung für deren Einsatz unterschied sich im Prinzip nicht von der für die Kamera im Erdgeschoss. An dieser Stelle war daher schon fraglich, wie mit dieser Kamera im Obergeschoss Zwischenfälle im Erdgeschoss verhindert werden sollten. Entsprechende Vorfälle in den Praxisräumen hatte der Logopäde nicht benannt. Im Ergebnis fehlte es auch bezüglich dieser Kamera an der Erforderlichkeit zur Zweckerreichung, zudem waren auch hier schutzwürdige Interessen der Mitarbeiter und Patienten verletzt. Mit der Kamera zeichnete der Praxisinhaber jedes Durchqueren des Flures durch seine Mitarbeiter auf und erzeugte dadurch einen entsprechenden Überwachungsdruck. Auch seine Patienten mussten die Wartezeit vor einer Behandlung (Sitz-/Wartebereich im Gang) offensichtlich unter ständiger Beobachtung einer Videokamera verbringen. Soweit er tatsächlich entsprechende Risiken für seine Mitarbeiter, Patienten und Praxisräume hätte belegen können, stellte sich die Frage, warum eine Überwachung des unmittelbaren Praxiszugangs (oberer Treppenbereich) nicht ausreichend sein sollte. In diesem Zusammenhang zu prüfen gewesen wäre auch eine Beschränkung der Überwachung auf die Schließzeiten sowie als alternative (vorrangige) Maßnahme ein verbesserter Zutrittsschutz. Soweit er seinen Patienten den Zutritt nur über einen Türöffner gewähren würde, könnte er wesentlich wirksamer ausschließen, dass sich unbefugte Personen in seinen Praxisräumen aufhalten.

Im Ergebnis meines Tätigwerdens sind schließlich beide Kameras demontiert worden.

8.1.10 Freibad: Liegewiese und Imbissstand

Der Pächter eines im kommunalen Eigentum stehenden Freibades hatte mehrere Kameras installiert, die insbesondere auch die Liegewiese sowie den im Freibad befindlichen Imbissstand erfassten. Zur Begründung führte er zwei mehrere Jahre zurückliegende Einbrüche sowie eine Brandstiftung an; darüber hinaus würde er die Kameras zur Steuerung des Imbiss- und Einlassbetriebes sowie zur Ausrichtung des Kundenservices am Besucheraufkommen nutzen. Da er nicht ständig im Bad anwesend sei, könne er sich auf diese Weise immer über die aktuelle Frequentierung des Bades informieren und die Servicepersonalstärke entsprechend anpassen.

Im Tagbetrieb sind zwar keine Bilder aufgezeichnet worden; ich habe den Betrieb dieser Kameras aber dennoch als unzulässig bewertet.

§ 6b Abs. 1 Nr. 3 BDSG erlaubt die Beobachtung öffentlich zugänglicher Bereiche, soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Die vom Pächter angeführten Interessen

- Steuerung des Imbiss- und Einlassbetriebes und
- Ausrichtung des Kundenservices an den Kameradaten

waren zwar als berechtigt anzuerkennen, jedoch ist eine Videobeobachtung dazu nicht erforderlich gewesen. Als weniger in das Persönlichkeitsrecht der Badbesucher eingreifende Maßnahmen haben alternative Meldewege (z. B. telefonisch durch das vor Ort tätige Personal) bestanden. Zudem standen einer Videobeobachtung unabhängig davon auch schutzwürdige Betroffeneninteressen entgegen. Freibäder dienen der individuellen Freizeitgestaltung, was sich in einem lockeren ungezwungenen Umgang miteinander manifestiert. Die Besucher vertrauen dabei auf die besondere Privatheit des in der Regel besonders einladend und für eine längere Verweildauer konzipierten Umfeldes der jeweiligen Freizeiteinrichtung. An solchen Orten sind die einer Videobeobachtung entgegenstehenden Betroffeneninteressen besonders schutzwürdig, zumal sie selbst für eine Videobeobachtung keinerlei Anlass gegeben haben. Die Badegäste haben ein schutzwürdiges Interesse daran, dass ihr Verhalten während ihres Aufenthalts im Bad nicht permanent beobachtet und möglicherweise auch aufgezeichnet wird – sie erhalten schließlich keine Information darüber, dass nur beobachtet wird bzw. sind insoweit dem Belieben des Badbetreibers ausgeliefert. Unter dem Druck der offensichtlichen Überwachung, deren tatsächlicher Umfang für sie also nicht ersichtlich ist, werden sie ihr Verhalten bewusst oder unbewusst darauf einstellen und sind damit in der freien Entfaltung ihrer Persönlichkeit und somit auch in ihrer Erholung beeinträchtigt.

Der mit einer Aufzeichnung verbundene Kamerabetrieb während der Schließzeiten des Bades diente dem Gebäudeschutz, insbesondere auch im Hinblick auf den separaten Imbissstand, und begegnete keinen datenschutzrechtlichen Bedenken.

8.1.11 Lebensmittelherstellung / IFS Food

Unternehmen der Lebensmittelbranche, die Produktionsbereiche praktisch lückenlos mit Videokameras überwachen, berufen sich hierzu gern auf die Vorgaben des IFS Food. Dieser Branchenstandard soll der Auditierung von Unternehmen dienen, die Lebensmittel verarbeiten oder lose Lebensmittelprodukte verpacken. Mittels Videoüberwachung der Mitarbeiter sollen dabei u. a. Verstöße gegen Hygienevorschriften verhindert und aufgeklärt werden. In einem Fall hatte ein lebensmittelproduzierendes Unternehmen annähernd 50 Videokameras installiert, um so seine Produktionsräume fast flächendeckend zu erfassen.

Die Zulässigkeit der Videoüberwachung von Produktionsbereichen, in denen Arbeitnehmer eingesetzt werden, richtet sich ausschließlich nach § 32 BDSG (BAG, Urteil vom 22. September 2016 – 2 AZR 848/15, juris). Grundsätzlich kann eine Videoüberwachung

nach § 32 Abs. 1 Satz 1 BDSG in Betracht kommen, um Produktionsabläufe im Lebensmittelbereich zu verfolgen oder den Zutritt unberechtigter Personen zu sensiblen Bereichen zu verhindern. Diese präventiven Zwecke lassen sich jedoch nur dann erreichen, wenn das Unternehmen die Kameras live im Auge behält, um sofort reagieren zu können (Live Monitoring). Auch dann ist die Videoüberwachung jedoch auf ein Minimum zu beschränken; Beschäftigte sind soweit wie möglich auszublenden. Unzulässig wäre es, mittels Videokameras einen ordnungsgemäßen Dienstablauf sicherzustellen und Verfehlungen zu verhindern, anstatt entsprechendes Personal einzustellen.

Nach der Rechtsprechung des Bundesarbeitsgerichts (Beschluss vom 29. Juni 2004 – 1 ABR 21/03, Beschluss vom 14. Dezember 2004 – 1 ABR 34/03 sowie Beschluss vom 26. August 2008 – 1 ABR 16/07, juris) ist eine dauerhafte, verdachtsunabhängige Videoüberwachung der Belegschaft unverhältnismäßig und stellt deshalb einen ungerechtfertigten Eingriff in das durch das Grundgesetz geschützte allgemeine Persönlichkeitsrecht der Arbeitnehmer dar. Auch wenn nicht ständig jemand vor den Monitoren sitzt, werden die Beschäftigten durch die bloße Möglichkeit der jederzeitigen Videoüberwachung ihres Arbeitsplatzes einem unzumutbaren Überwachungs- und Anpassungsdruck ausgesetzt. Denn sie können ja nicht wissen, ob sie gerade beobachtet werden oder nicht. Eine solche Videoüberwachung kann nur bei besonderen, konkret darzulegenden Sicherheitsinteressen eines Unternehmens ausnahmsweise gerechtfertigt sein.

Derartige Sicherheitsinteressen lassen sich nicht allein aus den Vorgaben des IFS Food (Version 6 vom April 2014) herleiten, um die Notwendigkeit der flächendeckenden Videoüberwachung der Produktionshallen sowie der Wareneingangs- und -ausgangsbereiche zu rechtfertigen. Zunächst stellen weder der IFS Food noch der Leitfaden zur Umsetzung der Anforderungen an den Produktschutz (Food Defense) verbindliche Regelungen im Sinne des § 4 Abs. 1 BDSG dar, die eine Videoüberwachung fordern. Vielmehr handelt es sich um eine reine Selbstverpflichtung der beteiligten Handelspartner:

„*Der IFS Food Standard ist ein von der GFSI (Global Food Safety Initiative) anerkannter Standard für die Auditierung von Lebensmittelherstellern. Der Schwerpunkt liegt hierbei auf Lebensmittelsicherheit und der Qualität der Verfahren und Produkte. Der Standard gilt für die Verarbeiter von Lebensmitteln ebenso wie für Unternehmen, in denen unverpackte Lebensmittel verpackt werden.*“

Quelle: https://www.ifs-certification.com/index.php/de/standards/23-ifs-food-de

Darüber hinaus werden darin Videokameras lediglich als eine von mehreren Möglichkeiten benannt, Schwachstellen aufzudecken und zu begegnen. Wichtig ist in diesem

Zusammenhang auch die Feststellung, dass der Leitfaden den Fokus auf eine Minimierung der Risiken eines unberechtigten Zutritts zu Lager- und Produktionsstätten richtet. Es gibt jedoch einige lebensmittelproduzierende Unternehmen, die die Videoüberwachung und Videoaufzeichnung gerade nicht auf diese Bereiche beschränken, sondern allumfassend die Produktion überwachen. Auch die Bestimmungen der Lebensmittelhygiene, insbesondere die Implementierung eines HACCP-Systems (Konzept zur Gefahrenanalyse kritischer Lenkungspunkte), verlangen keine dauerhafte und flächendeckende Videoüberwachung der Produktionsstätte und Produktionsabläufe.

Die Unternehmen müssen vielmehr auf der Grundlage eines schriftlichen Sicherheits- und Betriebskonzepts zur Videoüberwachungsanlage darlegen, warum der Einsatz jeder einzelnen Videokamera aus Gründen der Lebensmittelhygiene oder Produktsicherheit geeignet und zwingend erforderlich ist und andere Mittel (Kontrollen durch Schichtleiter, Stichproben, mehr Personal) nicht gleichermaßen wirksam sind. Zudem muss die Videoüberwachung technisch so ausgestaltet werden, dass eine dauerhafte Beobachtung der Beschäftigten ausgeschlossen ist (z. B. durch Verpixelung, Privacy-Filter, Ausblendungen der Dauerarbeitsplätze).

Das eingangs erwähnte Unternehmen konnte nicht ansatzweise darlegen, wie es die einzelnen Produktionsprozesse durch die Videobeobachtung konkret sichern wollte. Aus diesem Grund hielt ich die Videoüberwachung bereits für ungeeignet, diesen präventiven Zweck zu erreichen; im Übrigen für nicht erforderlich.

Das Unternehmen konnte auch auf Nachfrage nicht erläutern, wie es Hygieneprobleme mittels der in den Produktionsbereichen installierten Videokameras verhindern wollte: Es beobachtete niemand die Produktionsprozesse am Monitor in Echtzeit, um ggf. sofort zur Prozesssicherung korrigierend einschreiten zu können. Man war dennoch überzeugt, dass die Vielzahl der Kameras helfen würde, aufgetretene Probleme in den Griff zu bekommen. Auch wenn das Unternehmen beteuerte, nicht das Ziel zu verfolgen, die Mitarbeiter permanent zu überwachen, übte es doch mit der Installation der Videokameras einen erheblichen und letztlich auch beabsichtigten Anpassungs- und Überwachungsdruck auf die Mitarbeiter aus. Dies war unverhältnismäßig und auch nicht erforderlich. Erfolgversprechender lassen sich Hygienevorschriften nämlich durch Schulungen und die direkte, persönliche Kontrolle und unmittelbare Ansprache der Mitarbeiter vor Ort umsetzen. Dass die Videoüberwachung billiger ist als Personal, ist übrigens kein ausschlaggebendes Argument.

Soweit Videokameras auch betrieben werden, um Verstöße der Mitarbeiter gegen Produktions- und Hygienevorschriften nachträglich aufklären zu können (d. h. Videoauf-

zeichnungen erfolgen), müssen vorab konkret entsprechende Anhaltspunkte für entsprechendes, nicht nur einmaliges Fehlverhalten bestimmter Mitarbeiter in der Vergangenheit dokumentiert werden (§ 32 Abs. 1 Satz 2 BDSG). Nur befürchtete Verfehlungen der Arbeitnehmer können die dauerhafte Videoüberwachung und die Speicherung der Videoaufnahmen nicht rechtfertigen. Denn anderenfalls werden die Arbeitnehmer ohne Anlass unter Generalverdacht gestellt.

Letzteres war bei dem bereits erwähnten Unternehmen der Fall, weshalb ich den Einsatz der Videokameras auch insofern als datenschutzwidrig beurteilt habe. Die gespeicherten Videoaufnahmen sollten im Nachgang gesichtet und ausgewertet werden, um Verstöße der Mitarbeiter gegen Hygienevorschriften ahnden zu können. Das Unternehmen vermutete eine mangelnde Personalhygiene, ohne konkrete Verstöße einzelner Mitarbeiter belegen zu können. Aufgezeichnet und späterer Auswertung zugänglich gemacht wurden fast ausschließlich Verhaltensweisen und Lebensäußerungen ohne lebensmittelhygienische Relevanz, wie die Verrichtung der Arbeit, mögliche Unterbrechungen und jegliche Form der Kommunikation mit anderen Arbeitnehmern in den Produktionsräumen. Betroffen von der Videoüberwachung waren dabei weit überwiegend Mitarbeiter, denen gegenüber kein Verdacht des Verstoßes gegen Hygienevorschriften bestand. Es ist unzulässig, allgemein einen ordnungsgemäßen Dienstablauf durch ausufernde, nicht auf einen bestimmten Zeitraum oder Anlass begrenzte Videoüberwachung sicherzustellen. Die Vielzahl oder gar Gesamtheit sich regelkonform verhaltender Arbeitnehmer musste schwerwiegende Eingriffe in ihr Persönlichkeitsrecht hinnehmen, um einige wenige Mitarbeiter abzuschrecken, die mutmaßlich gegen Hygienevorschriften verstießen (in diesem Sinne BAG, Beschluss vom 29. Juni 2004 – 1 ABR 21/03, Rdnr. 23, juris).

Im Ergebnis meiner Kontrolltätigkeit erklärte sich das Unternehmen bereit, die Mehrzahl der Videokameras dauerhaft außer Betrieb zu nehmen.

8.1.12 Bäckereifilialen

Mit der Videoüberwachung in den Produktionsräumen von Bäckereien (Backstuben) habe ich mich bereits in 6/8.1.6 befasst.

Nach einer entsprechenden Eingabe habe ich mich nunmehr auch mit der Zulässigkeit von Videokameras in den Verkaufsräumen auseinandersetzen müssen.

Eine Großbäckerei hatte 34 seiner 69 Filialen mit jeweils einer Videokamera ausgerüstet und beabsichtigte dies auch für alle übrigen Filialen. Zur Rechtfertigung wurden in erster Linie präventive Zwecke (Schutz vor Einbrüchen und Überfällen) benannt, darüber hinaus aber auch die diesbezügliche Beweissicherung sowie die schnelle Reaktion auf bzw. die Bewertung von Alarmen der zusätzlich installierten Einbruchmeldeanlagen. Die

Kameras waren an der Decke befestigt und in Richtung der Verkaufstheke, mithin auf das Verkaufspersonal, gerichtet.

Für die datenschutzrechtliche Bewertung war zunächst § 32 BDSG heranzuziehen; alternativ kam auch § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Betracht.

Gemäß § 32 Abs. 1 Satz 1 BDSG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigtenverhältnisses erhoben und verarbeitet werden, wenn dies für dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten gemäß § 32 Abs. 1 Satz 2 BDSG nur dann erhoben und verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Videoüberwachung zur Aufdeckung erforderlich ist und schützenswerte Interessen der Arbeitnehmer nicht entgegenstehen. Dass Anhaltspunkte für ein strafbares Verhalten Beschäftigter vorliegen, hatte die Großbäckerei nicht vorgetragen. Auch ein aus § 32 Abs. 1 Satz 1 BDSG aus der Natur des Arbeitsverhältnisses selbst abzuleitendes Erfordernis war unter Berücksichtigung der benannten Überwachungsziele nicht festzustellen.

Damit verblieb lediglich eine Interessenabwägung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Wenn man berücksichtigt, dass die Geschäftsführer auf meine Frage nach der Gefährdungslage (während der Öffnungszeiten) lediglich einen länger zurückliegenden Überfall in einer Filiale anführen konnten und im Übrigen die präventive Ausrichtung der Videoüberwachung in den Vordergrund stellten, kam man nicht umhin, bereits die Erforderlichkeit der Videoüberwachung der Filialen – jedenfalls während der Öffnungszeiten – in Frage zu stellen. Sie mag zwar zur Zweckerreichung geeignet gewesen sein, jedoch war sie vor dem Hintergrund, dass keine besondere Gefährdungslage bestand, unverhältnismäßig und es gab mildere Mittel, hier die bloße Existenz der Kamera im Sinne einer Attrappe, um die gewünschten Abschreckungseffekte zu erzielen. Wenn überhaupt hätte man eine Erforderlichkeit allenfalls für den unmittelbaren Kassenbereich anerkennen können.

In jedem Fall standen einer solchen Dauerüberwachung aber schutzwürdige Interessen der Filialmitarbeiter entgegen. Eine dauerhafte Überwachung am Arbeitsplatz erfasst – anders als etwa die Kameras in Bahnhöfen, Tankstellen, Kaufhäusern – 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; die Eingriffsintensität ist damit besonders hoch. Zudem ist der überwachte

Personenkreis dem Arbeitgeber von vornherein bekannt; der Überwachungsdruck ist daher für die betroffenen Mitarbeiter besonders groß (BAG, Beschluss vom 29. Juni 2004 – 1 ABR 21/03, juris). 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, Beschluss vom 14. Dezember 2004 – 1 ABR 34/03, juris).

Dies bedeutete, dass die Videoüberwachung in den Filialen in der praktizierten Form unzulässig und damit rechtswidrig war. Den Interessen der Mitarbeiter in jeder Weise gerecht werden würde eine Abschaltung der Kameras während der Öffnungszeiten. Dies dürfte durch eine Zeitsteuerung vergleichsweise einfach zu realisieren sein. In den übrigen Zeiten könnte die Videoüberwachung in vollem Umfang aufrechterhalten werden. Alternativ käme das Ausblenden (Schwärzen) aller Bereiche außerhalb der unmittelbaren Kassenumgebung in Betracht. Auch in diesem Fall könnte die Videoüberwachung außerhalb der Öffnungszeiten wie bisher praktiziert werden. Es war auch denkbar, dass die Mitarbeiter die Videokameras tagsüber im Fall eines besonderen Vorkommnisses selbst aktivieren können, etwa über einen Alarmknopf.

Auf den von den Bäckereivertretern schließlich nachgeschobenen Zweck, dass die Überwachung auch der Aufklärung und Verhütung von Warenverlusten durch Eigentumsdelikte der Kunden dienten, habe ich entgegnet, dass es in Bäckereifilialen mit den zum Kunden hin geschlossenen Theken üblicherweise an frei zugänglichen, durch das Personal nicht überschaubaren Warenpräsentationen fehlt, sodass Ladendiebstähle eher unwahrscheinlich sind und daher nicht zur Begründung einer Videoüberwachung herangezogen werden können.

Soweit im Übrigen im Einzelfall eine konkrete Raubüberfall-Gefährdung für eine einzelne Filiale nachgewiesen werden kann, wäre eine Videoüberwachung damit ggf. für diese und nur für diese Filiale begründbar. Es ist keineswegs so, dass Bäckereifilialen generell einem hohen Überfallrisiko ausgesetzt sind. In einem solchen Fall würde es auch ausreichen, wenn die Eingangstür von innen überwacht und – im Hinblick auf die verfolgten präventiven Zwecke – das Ladengeschäft außen deutlich als videoüberwacht gekennzeichnet wird. Für diesen Zweck nicht erforderlich ist jedoch die Videoüberwachung des Thekenbereiches.

Davon unabhängig müssen in jedem Fall die Mitarbeiter über die Zeiten und den Umfang (überwachte Bereiche) der Videoüberwachung ausführlich informiert werden. Anders

lässt sich dem allein durch die Existenz und Ausrichtung der Kamera bedingten Überwachungsdruck nicht begegnen.

8.1.13 Werkhallen / Produktionsstätten

Mich erreichten mehrere Eingaben, die sich mit der Zulässigkeit von Videoüberwachungsanlagen in Werkhallen und Produktionsstätten befassten. Dabei musste ich feststellen, dass die verantwortlichen Stellen Videokameras häufig anschaffen, ohne sich vorher mit den Grundlagen für einen rechtmäßigen Betrieb auseinanderzusetzen oder Alternativen zu einer Videoüberwachung zu prüfen. Im besten Fall vertraut man der Fachfirma, wobei man übersieht, dass diese – anders als der betriebliche Datenschutzbeauftragte oder Datenschutzberater – in erster Linie eigene (wirtschaftliche) Interessen verfolgt. Nur wenigen Unternehmen scheint bekannt zu sein, dass ich auch einen Beratungsauftrag habe (§ 38 Abs. 1 Satz 2 BDSG).

Mancher Unternehmer musste im Aufsichtsverfahren feststellen, dass die angeschafften Videokameras für seine Zwecke ungeeignet waren, weil sie sich nicht datenschutzgerecht konfigurieren ließen. Vermeintlich billige Lösungen können sich dann im Nachhinein als Fehlinvestition herausstellen; dazu kommen die Kosten für meine Kontrolltätigkeit, wenn ich – was regelmäßig der Fall ist – Datenschutzverstöße beim Betrieb der Videoüberwachungsanlage feststellen muss.

In vielen Fällen hatten die Unternehmen keine Vorabkontrolle durchgeführt (§ 4d Abs. 5 BDSG) und kein Sicherheits- oder Betriebskonzept (und kein Verfahrensverzeichnis, § 4g Abs. 2 bzw. Abs. 2a BDSG) für ihre Videoüberwachungsanlage, was sich rächt, wenn es zu Beschwerden und meiner Kontrolle kommt. Erst dann machen sich die Verantwortlichen – erstmalig – Gedanken, wozu sie die Videokameras eigentlich genau brauchen, dass und warum die Videokameras rund um die Uhr laufen und Mitarbeiter bei der Arbeit überwachen, ob und warum die Aufnahmen an mobile Endgeräte oder auf Monitore vor Ort übertragen werden, wer im Unternehmen Zugriff auf die Videobilder und ggf. Videoaufzeichnungen haben muss, wo (lokal, Cloud) und wie lange die Aufnahmen gespeichert werden.

Falls es eine schriftliche Information der Mitarbeiter gibt, ist diese häufig lückenhaft und wenig transparent. Eine solche schriftliche Information der Mitarbeiter hilft nicht nur, berechtigte Vorbehalte und Ängste gegen die Videoüberwachung abzubauen. Sie spielt auch im Rahmen der zur Beurteilung der Zulässigkeit der Videoüberwachung vorzunehmenden umfassenden Interessenabwägung eine wichtige Rolle. In die schriftliche Information ist mindestens aufzunehmen, für welchen konkreten Zweck die Videoüberwachung erfolgt, einschließlich der Festlegung, dass sie als Mittel allgemeiner Leistungs-

und Verhaltenskontrollen der Mitarbeiter nicht verwendet werden darf, ob und ggf. für welche Dauer die Videoaufnahmen gespeichert werden, dass keine Tonaufnahmen erfolgen, wer berechtigt ist, in welchem Umfang und unter welchen Voraussetzungen die Videoaufnahmen einzusehen, einschließlich der Pflicht zur restriktiven Vergabe der Zugriffsrechte sowie welche Einsichts- und Auskunftsrechte die Mitarbeiter haben.

Klarstellen möchte ich, dass die schriftliche Information der Mitarbeiter, auch wenn sie diese gegenzeichnen (müssen), nicht als Einwilligung in die Videoüberwachung verstanden werden kann. Eine datenschutzrechtlich wirksame Einwilligung setzt nämlich voraus, dass diese freiwillig erfolgt, d. h. sie muss auf der freien Entscheidung des Betroffenen beruhen (§ 4a Abs. 1 Satz 1 BDSG). Daran fehlt es in diesen Fällen regelmäßig aufgrund des im Arbeitsverhältnis bestehenden Über-/Unterordnungsverhältnisses zwischen Arbeitgeber und Arbeitnehmer. Die Arbeitnehmer haben keine andere Wahl als die Videoüberwachung zu akzeptieren, weil sie befürchten, anderenfalls ihren Arbeitsplatz zu verlieren.

Als Rechtsgrundlage für die Videoüberwachung kommt, da sich in Werkhallen und Produktionsstätten hauptsächlich Mitarbeiter aufhalten, nur § 32 Abs. 1 BDSG in Betracht (BAG, Urteil vom 22. September 2016 – 2 AZR 848/15, juris). Nach § 32 Abs. 1 Satz 1 BDSG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Das heißt, die Videoüberwachung muss geeignet sein, die konkret damit verfolgten Zwecke zu erreichen. Sie muss erforderlich sein, d. h. zur Videoüberwachung darf es keine gleich wirksamen Alternativen geben und sie muss verhältnismäßig sein.

Einige Unternehmer haben Videokameras als preiswertes Mittel entdeckt, ihre Mitarbeiter von der Ferne aus bei der Arbeit zu beobachten und zu überwachen, um so die Arbeitsmoral zu steigern und die Arbeitszeit zu kontrollieren. Ihnen ist bewusst, dass sie so einen erheblichen Anpassungs- und Überwachungsdruck auf ihre Mitarbeiter ausüben. Andere Unternehmer möchten mit der Videoüberwachung ihrer Mitarbeiter die Einhaltung von Unfallverhütungs- oder Sicherheitsvorschriften durchsetzen und berufen sich insofern auf Anforderungen von Berufsgenossenschaften, Zertifizierungsstellen (siehe zum IFS Food Pkt. 8.1.11) bzw. ihrer Auftraggeber sowie Vorgaben bei der zollrechtlichen Direktabwicklung.

Bat ich die Unternehmer darum, durch entsprechende Bescheide oder Schreiben zu belegen, dass die installierten Videokameras durch andere Behörden oder die Auftraggeber der Unternehmen bzw. Zertifizierungsstellen verlangt werden, stellte ich regelmäßig fest, dass es solche Forderungen nicht gab. Videokameras werden als ein mögliches, aber nicht

zwingendes Mittel dargestellt, um z. B. Unfälle zu vermeiden oder Industriesabotage zu verhindern. Im letztgenannten Fall sehen die Bestimmungen, auf die sich die Unternehmen berufen, lediglich vor, dass Maßnahmen getroffen werden, um unberechtigte Zutritte Dritter zum Betriebsgelände zu verhindern bzw. dass die Tore und Türen zu Fertigungsbereichen gesichert werden. Welche Maßnahmen der Unternehmer wählt, bleibt ihm überlassen. Gleiches galt im Hinblick auf die Anforderungen der Berufsgenossenschaften, die Alternativen zur Videoüberwachung aufzeigten.

Die vorgenannten Zwecke und auch die angesprochene Verhaltenskontrolle der Mitarbeiter lassen sich im Übrigen nur durch ein sogenanntes Live Monitoring erreichen, d. h. es müsste permanent ein Mitarbeiter (z. B. Sicherheitsdienst oder Pförtner) die Videobilder ansehen, um bei Fehlverhalten unmittelbar korrigierend eingreifen zu können. Dies war bei den von mir zu beurteilenden Eingaben nicht der Fall. Gespeicherte Aufnahmen, auch wenn diese später ausgewertet werden, könnten allenfalls hilfreich sein, um im Nachhinein Schadensfälle aufzuklären.

Darüber hinaus bedarf es einer Videoüberwachung nicht, wenn sich eine Zugangskontrolle auch auf andere Weise (Pförtner, automatisiertes Zutrittskontrollsystem, Alarmanlage) gewährleisten lässt. Qualität und Quantität der Arbeitsleistung lassen sich durch qualifiziertes Führungspersonal (Vorarbeiter, Schichtleiter etc.) wesentlich effektiver und erfolgversprechender gewährleisten, sodass die Videoüberwachung auch nicht erforderlich ist. Die Arbeitszeit lässt sich mittels elektronischer Arbeitszeiterfassungssysteme kontrollieren. Kostengründe sind dabei kein durchgreifendes Argument.

In jedem Fall ist eine solche Videoüberwachung jedoch unverhältnismäßig. Dies gilt insbesondere, wenn die Videokameras (auch) Arbeitsplätze erfassen, an denen die Mitarbeiter dauerhaft oder die weit überwiegende Zeit über ihre Arbeitsleistung erbringen müssen, sich also praktisch der Videoüberwachung allenfalls kurz entziehen können. Die dauerhafte und verdachtsunabhängige Videoüberwachung stellt einen schwerwiegenden Eingriff in das Persönlichkeitsrecht der Mitarbeiter dar, der nicht durch die Verfolgung ebenfalls verfassungsrechtlich geschützter Rechtspositionen der Unternehmen (Berufs- und Eigentumsfreiheit) aufgewogen wird (vgl. BAG, Beschluss vom 29. Juni 2004 – 1 ABR 21/03, Beschluss vom 14. Dezember 2004 – 1 ABR 34/03 sowie Beschluss vom 26. August 2008 – 1 ABR 16/07, juris). Denn die Installation der Videokameras führt – was die Unternehmen auch einräumen – zu einem Überwachungsdruck und damit zu einer Verhaltensänderung der Mitarbeiter.

Auch wenn sich in den von mir zu entscheidenden Fällen niemand permanent die Videobilder ansah (was jedoch möglich gewesen wäre), waren die Beschäftigten in den Pro-

duktionshallen durch die bloße Möglichkeit der jederzeitigen und dauerhaften Videoüberwachung ihres Arbeitsplatzes einem unzumutbaren Überwachungs- und Anpassungsdruck ausgesetzt. Denn sie konnten ja nicht wissen, ob sie gerade beobachtet werden oder nicht. Eine solche Videoüberwachung kann nur bei besonderen, konkret darzulegenden Sicherheitsinteressen eines Unternehmens ausnahmsweise gerechtfertigt sein. Diese Voraussetzungen lagen in allen Fällen offenkundig nicht vor. Es ist unverhältnismäßig, mittels Videokameras einen ordnungsgemäßen Dienstablauf sicherzustellen und Verfehlungen zu verhindern, anstatt entsprechendes Personal einzustellen.

Soweit Videokameras für die Zutrittskontrolle ausnahmsweise erforderlich sind, wären sie nach den Grundsätzen der Datenvermeidung und Datensparsamkeit (§ 3a BDSG) so auszurichten, dass sie auf die jeweiligen Tore bzw. Türen dauerhaft fokussiert sind und Randbereiche, in denen sich Mitarbeiter dauerhaft oder auch nur zeitweilig aufhalten, ausgeblendet oder geschwärzt werden. Die Videoüberwachung ist immer auf das Minimum (wie z. B. großflächige Übersichtsaufnahmen, keine Speicherung) zu beschränken. Beschäftigte sind so weit wie möglich auszublenden; ihnen müssen beobachtungsfreie Rückzugsräume bleiben.

Unternehmer, die mit der Videoüberwachung (auch) bezweckten, Straftaten von Mitarbeitern aufzuklären, scheiterten regelmäßig an den Voraussetzungen des § 32 Abs. 1 Satz 2 BDSG. Es ist nämlich unzulässig, mittels der (dann meist auch noch flächendeckenden und lückenlosen) Videoüberwachung Mitarbeiter unter Generalverdacht zu stellen. Mittels Videokamera beobachtet werden nämlich fast ausschließlich alltägliche Verhaltensweisen, wie die Verrichtung der Arbeit, mögliche Unterbrechungen und jegliche Form der Kommunikation mit anderen Arbeitnehmern (in diesem Sinne BAG, Beschluss vom 29. Juni.2004 – 1 ABR 21/03, Rdnr. 23, juris). Gemäß § 32 Abs. 1 Satz 2 BDSG sind derartige Eingriffe in das allgemeine Persönlichkeitsrecht der Arbeitnehmer nur zulässig, wenn der zu dokumentierende konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung besteht und die Auswertung der mittels Videokamera erhobenen Daten praktisch das einzig mögliche Mittel zur Aufklärung darstellt. Der Verdacht muss sich auf eine konkrete Person oder zumindest auf eine räumlich-funktional abgrenzbare Personengruppe beziehen. Die tatsächlichen Verdachtsmomente sind schriftlich oder elektronisch zu dokumentieren. Die Datenerhebung, -verarbeitung und -nutzung muss zur Aufdeckung erforderlich sein: Das bedeutet, dass keine ebenso effektiven, den Arbeitnehmer weniger belastenden Möglichkeiten zur Aufklärung der Straftaten zur Verfügung stehen dürfen. Die Videoüberwachung ist zudem nur zeitlich eng begrenzt zulässig.

Gerade Unternehmen, die ihren Sitz in abgelegenen Gewerbegebieten haben, betrieben die Videoüberwachung auch, um ihr Eigentum zu schützen bzw. Straftaten aufzuklären.

Soweit die Videoüberwachung in den Werkhallen ausschließlich außerhalb der Arbeitszeiten der Mitarbeiter erfolgt (was durch technische Maßnahmen [z. B. Verknüpfung mit einer Alarmanlage oder mittels Riegelkontaktschalter] sicherzustellen ist) oder sich auf den Außenbereich des Werkgeländes beschränkt (ohne die Pausen- oder Raucherecke und öffentliche Verkehrsbereiche zu erfassen), bestehen, wenn die Speicherdauer auf maximal 72 Stunden begrenzt wird, keine grundsätzlichen datenschutzrechtlichen Bedenken: Das Unternehmen verfolgt legitime Interessen im Sinne des § 28 Abs. 1 Nr. 2 BDSG, schutzwürdige Interessen der Betroffenen überwiegen nicht.

In allen Fällen konnte ich die Unternehmen letztlich davon überzeugen, die Videokameras entweder außer Betrieb zu nehmen oder - wenn die eingesetzte Technik dies ermöglichte - datenschutzkonform zu konfigurieren.

8.1.14 Videokameras gegen Geschirrdiebstahl

Ich erhielt den Hinweis, dass ein Unternehmer die Betriebskantine, in der er seinen Mitarbeitern kostenlose Mahlzeiten anbot, mittels Videokamera überwachte. Auf meine Nachfrage teilte mir der Unternehmer mit, dass er mit der Videoüberwachung die unerlaubte Mitnahme von Gegenständen und Speisen durch seine Mitarbeiter verhindern und aufklären wolle.

Als Rechtsgrundlage für die Videoüberwachung kam, da diese in nicht für die Allgemeinheit bestimmten Räumen stattfand und ausschließlich Arbeitnehmer davon betroffen waren, ausschließlich § 32 Abs. 1 BDSG in Betracht (BAG, Urteil vom 22. September 2016 – 2 AZR 848/15, juris). Allerdings waren die Voraussetzungen der Vorschrift nicht erfüllt:

§ 32 Abs. 1 Satz 2 BDSG sieht vor, dass zur Aufdeckung von Straftaten personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden dürfen, 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.

Anders als von der Vorschrift vorgesehen, hatte der Arbeitgeber keinen konkreten Verdacht gegen einen oder mehrere der mehr als 50 Beschäftigten, sondern setzte alle Mitarbeiter einem Generalverdacht aus. Nur wenn es einen durch Tatsachen unterlegten konkreten Verdacht gegen einen oder mehrere bestimmte Mitarbeiter gegeben hätte, hätte

die Videoüberwachung zur Aufklärung von Straftaten im Beschäftigungsverhältnis unter Umständen zulässig sein können.

Hinsichtlich der mit der Videokamera ebenfalls verfolgten präventiven Zwecke (Abschreckung) kam § 32 Abs. 1 Satz 1 BDSG als Rechtsgrundlage in Betracht. Allerdings war die Videoüberwachung nicht erforderlich, d. h. nicht das mildeste Mittel. Denn der Diebstahl von Geschirr und Speisen lässt sich genauso gut durch mehr Personal in der Betriebskantine verhindern. Zudem war die konkrete Videoüberwachung unverhältnismäßig. Die verfassungsrechtlich geschützten Rechte der betroffenen Arbeitnehmer (allgemeines Persönlichkeitsrecht, Recht auf informationelle Selbstbestimmung) überwogen die Eigentumsinteressen des Unternehmers deutlich. Bei der vorzunehmenden umfassenden Interessenabwägung ist von Bedeutung, wie intensiv die Videoüberwachung ihrer Art und Dauer nach ist, welche Umstände und Inhalte von Verhalten und Kommunikation erfasst werden können, welche Nachteile den Betroffenen aus der Maßnahme drohen und in welcher Zahl unverdächtige Dritte mitbetroffen sind.

Bei der praktizierten Videoüberwachung handelte es sich insoweit um einen erheblichen Eingriff in das allgemeine Persönlichkeitsrecht der betroffenen Arbeitnehmer. Die Videoüberwachung war nicht auf einen überschaubaren Zeitraum begrenzt, sondern wurde permanent durchgeführt. Diese Arbeitnehmer wurden, wenn sie die Kantine besuchten, einem erheblichen Überwachungsdruck ausgesetzt, denn sie wussten, dass sie dort gefilmt wurden und der Unternehmer die Aufnahmen auch täglich auswertete. Dadurch entstand bewusst oder unbewusst ein Druck, sich möglichst unauffällig zu benehmen, um nicht später in irgendeiner Weise Gesprächsobjekt zu werden und Vorhaltungen ausgesetzt zu sein (vgl. zum Ganzen BAG, Beschluss vom 14. Dezember 2004 – 1 ABR 34/03, Rdnr. 15 ff., juris). Oder die Arbeitnehmer entschieden sich, die Kantine zukünftig zu meiden (mit der Folge, dann auf eine warme Mahlzeit verzichten zu müssen).

Eingriffsintensivierend wirkte sich aus, dass die Kantine während der Pausenzeiten besucht wird und es sich damit typischerweise um einen Ort handelt, an dem sich Mitarbeiter erholen und entspannen sollen. Die Videokamera erfasste dort in erster Linie Verhaltensweisen ohne jede strafrechtliche Relevanz und ganz überwiegend Personen, die unverdächtig waren. Demgegenüber handelt es sich bei den Verlusten an Geschirr und Speisen in der Kantine um einen verhältnismäßig geringen Eingriff in die verfassungsrechtlich geschützten Rechtspositionen des Unternehmers, auch wenn nicht verkannt wird, dass sich die Verluste im Laufe der Zeit aufsummieren können.

Im Ergebnis erklärte sich der Unternehmer bereit, die Videokamera zu entfernen, teilte mir jedoch zugleich noch mit, dass er auch die kostenlose Verpflegung eingestellt habe.

8.1.15 Versteckte Videokameras in der Gastronomie

Bei einer Kontrolle stellte ich fest, dass in einer Gaststätte Lautsprecher montiert waren, in denen sich – für die Gäste nicht erkennbar – Videokameras befanden, mit denen das Geschehen im Gastraum auch während der Öffnungszeiten beobachtet und aufgezeichnet wurde. Abgesehen davon, dass diese heimliche und anlasslose Videoüberwachung der Gäste weder erforderlich noch verhältnismäßig war (siehe 4/4.2.1.9), verstieß der Betreiber auch noch gegen § 90 Abs. 1 Satz 1 TKG. § 90 Abs. 1 Satz 1 TKG verbietet, sonstige Telekommunikationsanlagen (§ 3 Nr. 23 TKG) zu besitzen, die mit Gegenständen des täglichen Gebrauchs verkleidet sind und auf Grund dieser Umstände oder auf Grund ihrer Funktionsweise in besonderer Weise geeignet und dazu bestimmt sind, das Bild eines anderen von diesem unbemerkt aufzunehmen. Wer gegen dieses Verbot verstößt, kann gemäß § 148 Abs. 1 Nr. 2a TKG mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft werden, siehe dazu auch die diesbezügliche Pressemitteilung der Bundesnetzagentur (Anlage 1). Auf meinen Hinweis hin entfernte der Wirt diese Videokameras.

8.1.16 Dokumentation des Baufortschritts

Baustellenkameras erfreuen sich – zumeist als Marketinginstrument – zunehmender Beliebtheit. In erster Linie geht es dabei immer um die Dokumentation des Baufortschritts durch oder in Verantwortung des Bauherrn. Interessierten Personen soll die Möglichkeit eröffnet werden, sich ein Bild über den aktuellen Stand sie interessierender Bauarbeiten zu machen. Ein solches Interesse kann aus unterschiedlichen Gründen bestehen – so kann es sein, dass es um ein Bauvorhaben im Wohnungsbereich geht und der Betrachter bereits einen Miet- oder Kaufvertrag abgeschlossen hat; es ist aber beispielsweise auch denkbar, dass ein besonderes Interesse der Allgemeinheit am Fortgang der Bauarbeiten bei besonderen Gesellschaftsbauten besteht. Im Regelfall werden die dabei aufgenommenen Videos oder Bilder von einer Webcam aufgenommen und dann der Öffentlichkeit über das Internet zugänglich gemacht. In eher seltenen Fällen werden die Bilder ohne Veröffentlichung gespeichert, um daraus später einen Zeitrafferfilm zu erzeugen.

Datenschutzrechtlich relevant sind solche Kameras immer dann, wenn sie tatsächlich auch Personen erfassen und diese auch bestimmbar sind. Dies können unbeteiligte Dritte in der unmittelbaren Umgebung sein, aber auch und vor allem die auf der Baustelle tätigen Arbeiter.

Soweit auch an die Baustelle angrenzende Verkehrsbereiche von der Kamera erfasst werden und die Videoaufnahmen von einer Qualität sind, die eine Identifizierung von Verkehrsteilnehmern möglich machen, sind solche Videoaufnahmen unzulässig. Der

Kamerabetreiber kann sich weder auf sein (Baustellen-)Hausrecht (§ 6b Abs. 1 Nr. 2 BDSG) noch auf berechtigte Interessen (§ 6b Abs. 1 Nr. 3 BDSG) berufen. Für die Dokumentation des Baufortschritts ist es überhaupt ohne Bedeutung, was sich auf den an die Baustelle angrenzenden Flächen abspielt. Dies gilt auch für nicht öffentlich zugängliche Nachbargrundstücke (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG). Zudem stehen einer insoweit heimlichen Videoüberwachung überwiegende schutzwürdige Interessen der hiervon betroffenen Verkehrsteilnehmer entgegen, die in beiden Fällen entsprechend zu berücksichtigen sind und gleichfalls zu einer Unzulässigkeit des Kamerabetriebs führen. Derartige Bereiche sind folglich aus dem Erfassungsbereich herauszunehmen (Einrichtung von Privatzonen durch Verpixelungen oder Schwärzungen).

Soweit sich der Betrieb einer solchen Kamera auch auf einen ggf. vorangestellten Gebäudeabriss erstreckt, ist zu berücksichtigen, dass dadurch plötzlich auch angrenzende Flächen neben oder hinter dem verschwundenen Gebäude in den Fokus der Kamera gelangen können. In diesem Fall gelten die vorstehenden Aussagen natürlich analog.

In Bezug auf die auf der Baustelle tätigen Arbeiter liegen die Voraussetzungen für eine Datenschutzrelevanz deutlich niedriger. Eine Personenbeziehbarkeit ist hier – anders als in den angrenzenden Verkehrsbereichen – auch dann anzunehmen, wenn die Auflösung der Webcam aus der bildlichen Darstellung heraus allein noch keine Identifizierung ermöglicht. Während für einen Außenstehenden beispielsweise nur eine mehr oder weniger große Anzahl (gelb-)behelmter Arbeiter auf der Baustelle zugange ist, können deren Arbeitgeber, Kollegen oder andere Personen mit entsprechendem Hintergrundwissen diese Personen anhand ihrer konkreten Tätigkeit (z. B. Kranführer) oder ihres Tätigkeitsortes (z. B. Gerüst) sehr wohl konkret bestimmen und zwar auch dann, wenn keine Gesichter erkennbar sind. Damit gewinnt die Überwachungsproblematik an dieser Stelle besondere Bedeutung. Solange und soweit man die Arbeiter auf der Baustelle mehr oder weniger kontinuierlich über die Webcam beobachten kann, ist deren Betrieb daher gleichfalls unzulässig. Die datenschutzrechtliche Beurteilung erfolgt in diesem Fall auf der Grundlage des § 28 Abs. 1 Satz 1 Nr. 2 BDSG – mit dem Ergebnis, dass das schutzwürdige Interesse der Arbeiter, während ihrer gesamten Arbeitszeit nicht dauerhaft von Dritten, ggf. sogar von ihrem Arbeitgeber, beobachtet und überwacht zu werden, klar das – wie dargelegt – bloße Marketinginteresse des Bauherrn überwiegt. Die Vorschriften des § 6b BDSG sind in diesem Fall ebenso wenig einschlägig wie die des § 32 BDSG, denn einerseits stellt die Baustelle keinen öffentlich zugänglichen Bereich dar, andererseits sind die auf der Baustelle tätigen Personen (in aller Regel) keine Beschäftigten des Bauherren als Kamerabetreiber. Da die Bauarbeiter im Übrigen während ihrer Tätigkeit gezwungen sind, sich ständig im Erfassungsbereich der Kamera zu bewegen, können sie auch nicht als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit gemäß § 23

Abs. 1 Nr. 2 KunstUrhG gesehen und die Veröffentlichung auf diese Weise gerechtfertigt werden.

Abhilfe kann in solchen Fällen nur der Wechsel von Video- auf Einzelbildaufnahmen schaffen. Dabei ist der zeitliche Abstand der Einzelbilder von wesentlicher Bedeutung. Dieser muss so groß gewählt werden, dass die Erstellung eines Bewegungs- und Arbeitsprofils der Bauarbeiter praktisch unmöglich ist. Soweit die Aufnahmen nicht auf (Tages-)Zeiten von Baupausen beschränkt werden können, sollte der zeitliche Abstand nicht unter zwei, besser noch vier Stunden liegen. Die Sichtbarmachung des Baufortschritts wird dadurch sicher nicht gefährdet. Soll im Übrigen ein Zeitrafferfilm erstellt werden, d. h. müssen alle Aufnahmen gespeichert werden, sollte dies auch ein Gebot des Umfangs des letztendlich zu verarbeitenden Datenvolumens sein.

8.1.17 Videoaufzeichnung zu Schulungszwecken bei Showaufgüssen in einer Sauna

In einem Freibad mit einem angeschlossenen Erlebnissaunabereich hatte der Betreiber für eine Sauna als besondere Attraktion Showaufgüsse arrangiert. Diese Showaufgüsse waren mit Kostümen, Aufgussdüften, verschiedenen Wedeltechniken, Musik und einer Lichtshow hochwertig inszeniert und sollten zu besonderen Anlässen, wie beispielsweise Silvester, die Attraktivität der Sauna bzw. der Freizeiteinrichtung insgesamt entsprechend erhöhen. Um insbesondere bei diesbezüglichen Premieren später eine Fehlerkorrektur beim Zusammenspiel der Showkomponenten durchführen und Anhaltspunkte zur Verbesserung der Shows erhalten zu können, waren einige dieser Showaufgüsse mittels Videokamera aufgezeichnet worden. Am Eingang zu dieser Sauna war wie an allen anderen Saunen auch ein festes Schild montiert, auf dem die Besonderheiten dieser Sauna näher beschrieben waren und auf denen auch darauf hingewiesen wurde, dass in Ausnahmefällen einzelne Aufgüsse zu Schulungszwecken gefilmt werden können. Zudem war mir mitgeteilt worden, dass dies unmittelbar vor dem Aufguss auch immer vom Aufgießer bekanntgegeben werde. Die Saunabesucher hätten dann die Möglichkeit, sich umzusetzen, sich mit einem Handtuch zu bekleiden oder aber die Sauna zu verlassen. Es werde immer nur das Gesamtgeschehen aufgezeichnet.

Schulungszwecke können Videoaufnahmen in Saunen aber nicht rechtfertigen.

§ 6b Abs. 1 Nr. 3 sowie Abs. 3 BDSG regeln, dass Videoaufnahmen in allgemein zugänglichen Bereichen – und dazu zählen auch Saunen in Freizeiteinrichtungen – nur zulässig sind, wenn dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Im konkreten Fall fehlte es zunächst schon an der Erforderlichkeit einer Videoaufzeichnung. Es gibt in jedem Fall mildere Mittel, das Zusammenwirken der Aufgusskomponenten zu überprüfen, diesbezügliche Fehler zu korrigieren, Verbesserungen zu prüfen und das eigene Personal zu schulen, als Videoaufnahmen im laufenden Badebetrieb. Im einfachsten Fall werden das Zusammenwirken der Aufgusskomponenten bei leerer Sauna getestet und für den Abschlusstest Freiwillige aus dem eigenen Personalbestand rekrutiert. Die ordnungsgemäße Durchführung der Showaufgüsse kann im Einzelfall auch dadurch überwacht werden, dass dem – ggf. noch unerfahrenen – Aufgießer eine Begleitung zur Seite gestellt wird oder sich eine solche Kontrollperson selbst unter die Saunagäste begibt. Allein die vorliegend fehlende Erforderlichkeit führt schon zur Unzulässigkeit der Videoaufzeichnung.

Unabhängig davon sehe ich in jedem Fall auch schutzwürdige Interessen der Betroffenen verletzt. Der Aufenthalt in einer Sauna erfolgt üblicherweise unbekleidet oder nur mit einem Handtuch bedeckt – dem Interesse der Saunabesucher, dabei nicht Gegenstand von Videoaufzeichnungen zu werden, deren nachfolgende Verwendung sich vollkommen ihrem Einfluss entzieht, kommt dabei besonderes Gewicht zu. Vor diesem Hintergrund ist – abgesehen von einer ausdrücklichen Einwilligung nach § 4a BDSG – im Grunde genommen keine Konstellation vorstellbar, in der zulässiger Weise Videoaufnahmen angefertigt werden könnten. Unbeachtlich ist insoweit, dass auf dem – vergleichsweise viel Text enthaltenden – Informationsschild am Eingang der Sauna auf die bloße Möglichkeit von Videoaufzeichnungen hingewiesen wurde. Dies genügt weder den Anforderungen des § 4a BDSG, noch konnte auf diese Weise sichergestellt werden, dass sich auch tatsächlich jeder Saunabesucher (z. B. ausländische Bürger, Sehbehinderte, Minderjährige etc.) dieser Tatsache bewusst waren. Aus den Hinweisen wurde auch nicht deutlich, wann konkret mit solchen Videoaufzeichnungen zu rechnen ist. Sind aber die Gäste erst einmal in der Sauna, kommt eine entsprechende Information regelmäßig zu spät.

Auch in Bezug auf die Mitarbeiter ist die Erstellung von Videoaufzeichnungen datenschutzrechtlich unzulässig gewesen. Nach § 32 Abs. 1 Satz 1 BDSG dürfen personenbezogene Daten der Beschäftigten, zu denen auch Videoaufnahmen gehören, 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 bestand hier aber nicht. Der alternativ zur Anwendung kommende § 28 Abs. 1 Satz 1 Nr. 2 BDSG erfordert ähnlich wie § 6b BDSG eine Abwägung zwischen den berechtigten Interessen des Arbeitgebers und dem schutzwürdigen Arbeitnehmerinteresse am Ausschluss der Erstellung von Videoaufzeichnungen für Schulungszwecke. Auch diese Abwägung scheitert bereits an der fehlenden Erforderlichkeit der Videoaufzeichnung für die hier verfolgten Zwecke.

Wegen des Überwachungscharakters der Videoaufzeichnung bzw. der damit verbundenen Leistungs- und Verhaltenskontrolle ist im Übrigen zudem auch hier von einer Videoaufzeichnung entgegenstehendem überwiegendem Arbeitnehmerinteresse auszugehen. Zugleich schließt dies die Möglichkeit der Rechtfertigung der Videoaufzeichnung durch eine Einwilligung aus, denn eine ggf. eingeholte Einwilligung wäre unter diesen Umständen nicht tatsächlich freiwillig und damit unwirksam (§ 4a Abs. 1 Satz 1 BDSG). Arbeitnehmer würden sich vielmehr regelmäßig gezwungen sehen, in dieser Frage nicht gegen ihren Arbeitgeber zu intervenieren.

8.2 Internet

8.2.1 Ein besonders langwieriger Fall

Bereits im März 2012 erreichte mich eine eher banale Eingabe zu einer unzulässigen werblichen Ansprache durch einen Internethändler. Zu diesem Zeitpunkt ahnte ich noch nicht, dass sich dieser Fall zu dem bisher langwierigsten Aufsichtsfall meiner Behörde entwickeln würde und dass ich in diesem fast das gesamte mir zur Verfügung stehende aufsichtsrechtliche Instrumentarium zur Anwendung bringen würde.

Der eigentliche Sachverhalt konnte recht schnell geklärt und Anfang Mai 2012 mit der Feststellung eines diesbezüglichen Datenschutzverstoßes abgeschlossen werden. Der Kunde hatte über den Amazon-Marketplace einen Artikel des betreffenden Händlers erworben; anschließend war ihm von diesem Händler entgegen den Amazon-Teilnahmebedingungen und auch noch nach gemäß § 28 Abs. 4 BDSG erhobenem Widerspruch postalische Werbung zugesandt worden.

Die Krux bei der Sache war aber die, dass ich mich entschlossen hatte, diese Eingabe im Rahmen einer örtlichen Kontrolle des Händlers zu bearbeiten. Bei dieser örtlichen Kontrolle habe ich eine ganze Reihe weiterer datenschutzrechtlicher Mängel feststellen müssen, u. a.

- die unterlassene Bestellung eines Datenschutzbeauftragten,
- die nicht erfolgte Verpflichtung auf das Datengeheimnis,
- fehlende Auftragsdatenverarbeitungsverträge mit mehreren Dienstleistern,
- keine Unterrichtung über das Widerspruchsrecht in den Werbesendungen,
- werbliche Kundenansprache entgegen der eigenen Datenschutzerklärung,
- ungesicherte Weitergabe von Kundendaten an die Dienstleister.

Im Weiteren gestaltete sich die Kommunikation mit der verantwortlichen Stelle sehr schwierig und auch zeitaufwändig. Auskunftsaufforderungen wurde nur selten recht-

zeitig, oft erst nach Erlass eines Heranziehungsbescheides und Festsetzung eines Zwangsgeldes, nachgekommen und auch inhaltlich hinterließ die Geschäftsführung nicht den Eindruck, dass sie verstanden hatte, worum es beim Datenschutz im Allgemeinen wie auch bei den festgestellten Datenschutzmängeln, insbesondere der Auftragsdatenverarbeitung, im Speziellen eigentlich ging. So waren beispielsweise meine an den Händler als verantwortliche Stelle gerichteten Aufforderungen zum Abschluss rechtskonformer Auftragsdatenverarbeitungsverträge durch die Geschäftsführung einfach als zusätzliche Bedingung aller zukünftig zu erteilenden Aufträge an die Dienstleister weitergereicht worden. Die Geschäftsführung hatte also schlichtweg lange nicht begriffen oder nicht begreifen wollen, dass sie als verantwortliche Stelle selbst in der Pflicht ist, die gesetzlichen Vorgaben des § 11 BDSG umzusetzen. Leider bewirkte auch die nachgeholte Bestellung eines betrieblichen Datenschutzbeauftragten wegen der diesbezüglichen Dominanz der Geschäftsführung hier nur sehr wenig.

Alles in allem habe ich diese Angelegenheit aber schließlich nach

- zwei örtlichen Kontrollen,
- vier Heranziehungsbescheiden,
- fünf Zwangsgeldfestsetzungen,
- einer Anordnung und
- sieben Bußgeldbescheiden

und daraus resultierend Zahlungseingängen in Höhe von insgesamt mehr als 70.000 € nach mehr als vier Jahren im April 2016 doch noch erfolgreich, d. h. mit der Feststellung, dass alle von mir zu Beginn des Aufsichtsvorgangs festgestellten Datenschutzmängel durch die verantwortliche Stelle abgestellt worden sind, abschließen können.

8.2.2 E-Mail-Adressen in Gästebüchern

Ich wurde darauf hingewiesen, dass ein Parkplatzbetreiber die E-Mail-Adressen derjenigen Personen, die im Gästebuch seines Internetauftritts einen Eintrag tätigen, veröffentlicht. Neben der Bewertung des Parkplatzes gebe es im Gästebuch ein Feld „E-Mail“. Wenn man dies anklicke, erscheine die E-Mail-Adresse des Kommentargebers.

Die auf der betreffenden Internetseite für jedermann bestehende Möglichkeit, anderen Personen, die im Gästebuch einen Eintrag getätigt haben, direkt eine Antwort an ihre dort hinterlegten E-Mail-Adressen zu senden und dazu – bzw. auch ohne eine solche Absicht – deren E-Mail-Adressen auszulesen, verstieß gegen die Vorgaben des Telemediengesetzes:

§ 12 Abs. 1 TMG bestimmt, dass personenbezogene Daten zur Bereitstellung von Telemedien (hier des Gästebuches) nur erhoben und verwendet werden dürfen, soweit das Telemediengesetz oder eine andere sich ausdrücklich auf Telemedien beziehende Rechtsvorschrift dies erlaubt oder der Nutzer eingewilligt hat. Eine Einwilligung des Nutzers wurde bei Benutzung des Gästebuches aber nicht eingeholt; die Nutzer wurden noch nicht einmal auf die Bekanntgabe ihrer E-Mail-Adresse hingewiesen. Eine andere Regelung des Telemediengesetzes, die eine solche Bekanntgabe erlauben könnte, war nicht ersichtlich. Stattdessen gibt § 14 Abs. 1 TMG vor, dass personenbezogene Daten eines Nutzers nur erhoben und verwendet werden dürfen, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind. Danach war schon nicht ersichtlich, weshalb die E-Mail-Adresse bei der Erstellung eines Eintrags ins Gästebuch überhaupt erhoben wurde. Nach § 13 Abs. 4 Satz 1 Nr. 3 TMG hat der Diensteanbieter zudem durch technische und organisatorische Vorkehrungen sicherzustellen, dass der Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann.

Ich habe den Parkplatzbetreiber daher aufgefordert, diese konkrete Antwortfunktion seines Gästebuches umgehend zu deaktivieren. Für das Führen eines Gästebuches auf einer Webseite ist es nicht erforderlich, jedem beliebigen Leser die E-Mail-Adressen der Nutzer bekanntzugeben, die sich in dem Gästebuch eingetragen haben.

8.2.3 Rechnungsversand via E-Mail mit vollständiger Bankverbindung

Ein Kunde eines Internetunternehmens hatte sich mit der Mitteilung an mich gewandt, wonach das Unternehmen seine monatliche Abrechnung als Anhang (im PDF-Format) einer (unverschlüsselten) E-Mail verschickt und darin jedes Mal die vollständige Bankverbindung des Kunden angibt, von der aus der Bankeinzug erfolgen soll.

Es stand außer Frage, dass durchgreifende Argumente gegen eine Erforderlichkeit der vollumfänglichen Angabe der zu belastenden Bankverbindung beim Rechnungsversand bestehen. Um einem Kunden bei der Rechnungslegung regelmäßig noch einmal in Erinnerung zu rufen, von welchem seiner Konten der fällige Betrag abgebucht wird – nichts anderes wird mit der Angabe der Bankverbindung an dieser Stelle bezweckt –, muss nicht die komplette Bankverbindung angegeben werden. Hierfür genügen der Name oder der BIC des Kreditinstituts bzw. eine Teilangabe der IBAN. Kontodaten genießen zudem eine besondere Schutzwürdigkeit, der im Hinblick auf die Übertragungssicherheit (Vertraulichkeit als Bestandteil der Weitergabekontrolle gemäß Nr. 4 der Anlage zu § 9 BDSG) mit einem unverschlüsselten E-Mail-Versand nicht adäquat entsprochen wird. Als technisch trivialste Abhilfe bot sich hier eine Teilmaskierung der IBAN an. Unbedenklich ist

z. B. die Darstellung der letzten vier IBAN-Ziffern als „xxxx“, wie man das auch von Lastschriftbelegen im Einzelhandel kennt (vgl. dazu Pkt. 8.5.8). Auch andere Varianten sind vorstellbar.

Das Unternehmen hat meinen Handlungsvorschlag auf kooperative Weise aufgegriffen und verzichtet seither auf die Angabe der vollständigen Bankverbindung.

8.2.4 Werbung auf E-Mail-Adressen aus Kontaktformularen

Ein Betroffener hatte sich über das Kontaktformular eines Internetreiseanbieters über einen Mitbewerber beschwert. Einige Minuten nach Absenden seiner Nachricht hatte er zwei Werbe-E-Mails dieses Reiseanbieters in seinem Postfach. Der Betroffene stand in keiner Geschäftsbeziehung zu dieser Firma; eine solche hatte auch noch nie bestanden.

Diese werbliche Ansprache ist unzulässig gewesen. Die alleinige Nutzung eines Kontaktformulars berechtigt einen Reiseanbieter nicht, den Absender anschließend sofort in seinen Verteiler für Werbemails zu übernehmen. Dem steht die Vorschrift des § 28 Abs. 3 Satz 6 BDSG unter besonderer Beachtung der Regelungen des § 7 Abs. 2 Nr. 3, Abs. 3 UWG entgegen. Schutzwürdige Interessen eines Betroffenen stehen einer Datennutzung für Werbezwecke dann entgegen, wenn der Reiseanbieter eine E-Mail-Adresse unter Missachtung wettbewerbsrechtlicher Vorschriften nutzt. Vorliegend hatte der Reiseanbieter die E-Mail-Adresse des Betroffenen eben gerade nicht im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung, sondern infolge einer davon unabhängigen Nutzung des elektronischen Kontaktformulars erhalten und konnte sich daher nicht auf die Ausnahmeregelung des § 7 Abs. 3 UWG berufen, insbesondere waren die Voraussetzungen des § 7 Abs. 3 Nr. 1 und 2 UWG nicht erfüllt.

8.2.5 Veröffentlichung von Informationen zu Privatinsolvenzen

Insolvenzdaten werden nach § 9 Abs. 1 InsO auf der Internetseite *www.insolvenzbekanntmachungen.de* im Internet amtlich bekannt gegeben. Gemäß § 2 Abs. 1 Nr. 3 InsoBekV ist dabei für diese amtliche Veröffentlichung sicherzustellen, dass die Insolvenzdaten nur innerhalb der ersten zwei Wochen der öffentlichen Bekanntmachung ungehindert für jedermann abrufbar und insoweit allgemein zugänglich sind.

In 6/8.9.4 habe ich ausführlich erläutert, dass darüber hinaus auch die Veröffentlichung von Insolvenzdaten durch private Anbieter über den in der Insolvenz-Internet-Bekanntmachungsverordnung vorgesehenen Zeitraum hinaus wegen Verstoßes gegen § 29 Abs. 2 Satz 1 BDSG unzulässig ist.

Im Berichtszeitraum habe ich diesbezüglich eine Reihe von Eingaben zu verschiedenen, Insolvenzdaten zum Abruf bereithaltenden Internetportalen, beispielsweise

- *privatinsolvenzportal.net*
- *insolvenzen-deutschland.com*
- *insolvenzen.to*

erhalten. Diese Portale haben oder hatten ihren Sitz ausnahmslos außerhalb meines Zuständigkeitsbereiches, regelmäßig im Ausland, z. B. auf den Philippinen oder im Königreich Tonga. Zumeist ist es auch so, dass diese Webseiten meist nur begrenzte Zeit aufrufbar sind und häufig die Domain wechseln.

Als für den Freistaat Sachsen zuständige Datenschutzaufsichtsbehörde habe ich – wie auch die anderen deutschen Aufsichtsbehörden – in diesen Fällen leider keine Handlungsmöglichkeiten.

Einziger Ansatzpunkt ist insoweit, dass die betreffenden Seiten von den Betroffenen häufig über eine Google-Suche aufgefunden werden und die Ergebnisse auch nach einer Löschung oder wenn das Portal selbst nicht mehr erreichbar ist noch bei Google angezeigt werden.

Die Betroffenen haben in diesem Fall zumindest die Möglichkeit, im Hinblick auf diese Suchergebnisse einen Löschantrag bei Google zu stellen. Unter der URL

https://support.google.com/legal/contact/lr_eudpa?product=websearch

können Betroffene ein von Google dafür bereitgestelltes Formular ausfüllen. Sie erhalten dann per E-Mail eine Eingangsbetätigung sowie Hinweise zum weiteren Ablauf. Nach meinen Informationen gibt Google derartigen Anträgen im Allgemeinen auch statt.

Sollte Google die Löschung der Einträge im Einzelfall ablehnen, können Betroffene sich an die für Google zuständige Datenschutzaufsichtsbehörde, den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, wenden. Für die weitere Bearbeitung sind dazu der konkrete Suchbegriff (Namen), der entsprechende Link, die geführte Kommunikation sowie die Google-Bearbeitungsnummer mitzuteilen.

8.3 Arbeitnehmerdatenschutz

8.3.1 Beurteilungsplattform in kanadischer Cloud

Ein Unternehmen, dessen Muttergesellschaft ein internationaler Technikkonzern mit Sitz in einem außereuropäischen Staat ist, nutzte für sein Beurteilungswesen eine Datenbankanwendung eines kanadischen Anbieters. Die Mitarbeiter und Vorgesetzten waren gehalten, mittels der Beurteilungssoftware regelmäßig eine Selbst- bzw. Fremdeinschätzung vorzunehmen. Die Software ermöglichte es den Vorgesetzten, softwareunterstützt kurz- oder mittelfristige Ziele zu vereinbaren und diese nach Ablauf der vereinbarten Frist auch zu kontrollieren. Für die Mitarbeiter und Vorgesetzten wurden zunächst personalisierte Profile angelegt, die im Verlauf des Aufsichtsverfahrens auf Personalnummern umgestellt wurden. Die Daten sollen erst drei Jahre nach Beendigung des Arbeitsverhältnisses in der Datenbank gelöscht werden.

Gespeichert wurden die Daten bei dem kanadischen Softwareanbieter auf der Grundlage eines Lizenz- und Servicevertrags, der neben der Nutzung der Software auch die Inanspruchnahme von Service- und Cloud-Dienstleistungen (On-Demand-Hosting-Services) umfasste. Die Daten sollten grundsätzlich auf Servern in Kanada verarbeitet werden, wobei der kanadische Anbieter jedoch einen Zugriff und eine Übermittlung der in der Datenbank gespeicherten Kundendaten an Stellen auch außerhalb von Kanada ausdrücklich nicht ausschloss. Regelmäßige Backups wurden für die Dauer von einem Jahr durch den kanadischen Dienstleister vorgehalten.

Das Unternehmen hatte mit dem Softwareanbieter keinerlei vertragliche Regelungen entsprechend § 11 Abs. 2 BDSG getroffen, die insbesondere sicherstellten, dass der kanadische Datenbankanbieter einem Löschungs-, Sperrungs- oder Berichtigungsverlangen unverzüglich nachzukommen hatte. Eine Löschung oder Sperrung der Daten aus der Webanwendung heraus war nicht möglich.

Ich habe den Einsatz der Datenbankanwendung als datenschutzrechtlich unzulässig beurteilt:

Vorliegen personenbezogener Daten

Das Unternehmen vertrat die Auffassung, dass es sich bei den auf Veranlassung ihres Arbeitgebers von den Mitarbeitern und deren Vorgesetzten in die Datenbank eingegebenen Daten nicht um personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG handele, da der kanadische Cloud-Anbieter ja nicht wisse, welcher Mitarbeiter sich hinter der jeweiligen Personalnummer verberge. Dem widersprach ich: Personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten

oder bestimmbaren natürlichen Person. Auch pseudonymisierte Daten im Sinne des § 3 Abs. 6a BDSG bleiben personenbezogene Daten, solange eine Re-Identifizierbarkeit des Betroffenen lediglich erschwert, aber nicht unmöglich wird. Entscheidend für die Frage der Re-Identifizierbarkeit ist dabei die Kenntnis des Arbeitgebers als verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG, d. h. als diejenige Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

Das Unternehmen besaß zweifellos die notwendigen Zusatzinformationen um zu wissen, welchem Mitarbeiter welche Personalnummer zugeordnet ist. D. h., den Geschäftsführern und mindestens den Vorgesetzten sowie den Personalverantwortlichen war ohne weiteres eine Zuordnung der unter der Personalnummer in der Datenbankanwendung vorgenommenen Selbst- und Fremdeinschätzungen zu einem namentlich bekannten Mitarbeiter möglich. Anders hätte die Nutzung der Beurteilungsdatenbank auch keinen Sinn gemacht.

Selbst wenn man bei der Frage der Re-Identifizierbarkeit nicht das Zusatzwissen der verantwortlichen Stelle für entscheidend halten würde, war dem kanadischen Datenbankanbieter eine Zuordnung der einzelnen Profile in der Datenbank zu einzelnen Mitarbeitern möglich. Für die Frage, ob personenbezogene Daten erhoben und verarbeitet werden, kommt es – wie sich aus § 3 Abs. 6 und Abs. 6a BDSG ergibt – entscheidend darauf an, ob eine Re-Identifizierbarkeit aufgrund des damit einhergehenden unverhältnismäßigen Aufwands praktisch ausgeschlossen ist. Nicht entscheidend ist, ob dieser Aufwand tatsächlich betrieben wird, sondern ob entsprechende Risiken bestehen.

Dies war hier der Fall: Denn der Cloud-Dienstleister konnte nicht zuletzt im Rahmen der vertraglich vereinbarten Servicedienstleistungen im Rahmen der Fernwartung Zugriff auf Daten haben, die ihm eine Zuordnung der Personalnummer zu bestimmten Mitarbeitern hätten ermöglichen können (vgl. § 11 Abs. 5 BDSG). Die in den Selbst- und Fremdeinschätzungen hinterlegten sehr individuellen und persönlichen Informationen zur privaten und beruflichen Situation des jeweiligen Mitarbeiters ermöglichten es einem Dritten mit einem gewissen, keinesfalls unverhältnismäßigen Aufwand die hinter den Personalnummern stehenden Personen zu identifizieren. Bei meiner Beurteilung spielte dabei auch eine Rolle, dass bei dem Unternehmen weniger als 50 Mitarbeiter beschäftigt waren, die in Gruppen mit einem entsprechenden Vorgesetzten aufgeteilt wurden, wobei sich diese Aufteilung auch in der Datenbank wiederfand. Nicht zuletzt ging auch der kanadische Datenbankanbieter davon aus, dass es sich bei den in der Cloud gespeicherten Daten um personenbezogene Mitarbeiterdaten handelt.

Unzulässigkeit der Datenverarbeitung (Übermittlung nach und Speicherung in Kanada) auf der sogenannten 1. Stufe

Die Erhebung und Verarbeitung dieser personenbezogenen Beschäftigtendaten erfolgte ohne rechtlichen Grund. Die Datenerhebung, -verarbeitung und -nutzung ist gemäß § 4 Abs. 1 BDSG grundsätzlich verboten. Es lagen weder wirksame Einwilligungen der Mitarbeiter vor, noch ergab sich die Zulässigkeit aus dem Gesetz, insbesondere nicht aus § 32 Abs. 1 Satz 1 BDSG oder § 28 Abs. 1 Satz 1 Nr. 2 BDSG.

Zwar war der kanadische Datenbankanbieter – auch wenn kein Auftragsdatenverarbeitungsvertrag im Sinne des § 11 Abs. 2 BDSG geschlossen wurde – materiell-rechtlich Auftragsdatenverarbeiter im Sinne des § 11 Abs. 1 Satz 1 BDSG. Cloud-Dienstleistungen sind nämlich nach ganz herrschender Ansicht als Auftragsdatenverarbeitung zu qualifizieren (Petri in Simitis, BDSG, 8. Auflage, § 11 Rdnr. 30; Gola/Schomerus, BDSG, 12. Auflage, § 11 Rdnr. 8). Dies entsprach auch dem Selbstverständnis des kanadischen Datenbankanbieters, der seine datenschutzrechtliche Verantwortlichkeit ausdrücklich ausschloss, auch wenn das Unternehmen zeitweilig eine abweichende Auffassung vertrat.

Allerdings bestimmt § 3 Abs. 8 Satz 3 BDSG, dass bei einem Auftragsdatenverarbeiter, der seinen Sitz weder in der Europäischen Union noch dem Europäischen Wirtschaftsraum hat, die Privilegierung des § 3 Abs. 8 Satz 3 BDSG entfällt und folglich auf der sogenannten 1. Stufe – neben den Bestimmungen des § 11 BDSG – auch eine Rechtsgrundlage für die Datenverarbeitung (Übermittlung und Speicherung) durch ein in einem Drittstaat ansässiges Unternehmen vorhanden sein muss. Dies war hier nicht der Fall.

Nach § 32 Abs. 1 Satz 1 BDSG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies u. a. nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Erforderlich bedeutet dabei, dass die Datenerhebung und -verarbeitung geeignet und zugleich das relativ mildeste Mittel sein muss, um den unternehmerischen Interessen bei der Durchführung des Beschäftigungsverhältnisses Rechnung zu tragen. Die berechtigten und verfassungsrechtlich geschützten Interessen des Unternehmens müssen umfassend mit dem Recht der Arbeitnehmer auf informationelle Selbstbestimmung abgewogen werden (Seifert in Simitis, BDSG, 8. Auflage, § 32 Rdnr. 11).

Die Datenerhebung und Datenverarbeitung mittels Datenbankanwendung war bereits nicht im Sinne des § 32 Abs. 1 Satz 1 BDSG erforderlich, denn das bis zu deren Einführung im Unternehmen praktizierte Beurteilungswesen mittels Vorgesetztengesprächs oder handschriftlich auszufüllender Beurteilungsbögen war gleichermaßen geeignet, um die mit der Beurteilungssoftware verfolgten Ziele der Personalentwicklung zu erreichen.

Aber auch wenn man ein datenbankgestütztes Beurteilungswesen aufgrund der softwareseitigen Auswertungs- und Berichtsmöglichkeiten sowie Fristenverwaltung grundsätzlich für besser geeignet hielte, vermochten die verfassungsrechtlich geschützten Rechtspositionen des Unternehmens nicht den mit der Datenerhebung und Datenverarbeitung in Kanada verbundenen schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung der Mitarbeiter aufzuwiegen.

Zwar handelte es sich bei den nach Kanada übermittelten Daten um pseudonyme und damit weniger schutzbedürftige personenbezogene Mitarbeiterdaten. Allerdings war das Vertragsverhältnis weitgehend ungeregelt, insbesondere im Hinblick auf Kontroll- und Weisungsrechte des Arbeitgeberunternehmens. Dieses war deshalb insbesondere hinsichtlich der Löschung, Sperrung oder Berichtigung von Mitarbeiterdaten vollständig vom guten Willen des Datenbankanbieters abhängig, was erhebliche Risiken für das Recht auf informationelle Selbstbestimmung der Mitarbeiter bedeutete. Zudem war es weder für den Arbeitgeber, noch die betroffenen Arbeitnehmer oder die Aufsichtsbehörde nachprüfbar, ob z. B. eine behauptete Löschung tatsächlich erfolgt war. Potenziert wurden die Risiken für die Mitarbeiter auch dadurch, dass die Daten in der Datenbank und damit in Kanada für die Dauer von drei Jahren nach ihrem Ausscheiden gespeichert bleiben sollten.

Der Eingriff in das informationelle Selbstbestimmungsrecht der Mitarbeiter war auch deshalb schwerwiegend, weil ihr Arbeitgeber keine valide Kenntnis über die von dem kanadischen Datenbankbetreiber getroffenen Maßnahmen des technisch-organisatorischen Datenschutzes hatte und diesen auch mangels vertraglicher Vereinbarung nicht nachprüfen konnte. Die auf den Servern in Kanada gespeicherten Mitarbeiterdaten waren einem Zugriff Dritter ausgesetzt, ohne dass der kanadische Datenbankanbieter seinen Vertragspartner oder die betroffenen Arbeitnehmer hiervon hätte informieren müssen.

Durch die Übermittlung der Daten an den kanadischen Datenbankanbieter war es für die betroffenen Arbeitnehmer kaum noch nachvollziehbar und kontrollierbar, was mit ihren personenbezogenen Daten geschieht und ob und in welcher Weise diese vor dem Zugriff Unbefugter gesichert sind. Transparente Informationen ihres Arbeitgebers hierzu fehlten komplett.

Des Weiteren war bei der Gesamtabwägung zu berücksichtigen, dass das kanadische Datenschutzrecht PIPEDA und damit auch die Entscheidung der Europäischen Kommission vom 20. Dezember 2001 (2002/2/EG) zur Angemessenheit des kanadischen Datenschutzniveaus für Beschäftigtendaten nicht gelten. Die nach Kanada übermittelten Beschäftigtendaten sind damit deutlich erhöhten Missbrauchsrisiken ausgesetzt.

Angesichts der Schwere des Eingriffs in das informationelle Selbstbestimmungsrecht seiner Arbeitnehmer mussten die wirtschaftlichen Interessen des Unternehmens an der Nutzung der Cloud-Dienstleistungen zurücktreten. Das Unternehmen hatte insofern auch nicht geltend gemacht, dass die lizensierte Software ausschließlich auf Servern des Datenbankanbieters in Kanada genutzt werden konnte. Als milderes Mittel kam daher der Betrieb der lizensierten Software auf einem eignen oder z. B. dem Server eines Auftragsdatenverarbeiters mit Sitz innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums in Betracht.

Unzulässigkeit der Datenverarbeitung (Übermittlung nach und Speicherung in Kanada) auf der sogenannten 2. Stufe

Die Übermittlung der Beschäftigtendaten nach Kanada war zudem nach § 4b Abs. 2 Satz 2 BDSG unzulässig.

Danach hat die Übermittlung an Stellen in einem Drittstaat, d. h. einem Staat außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums, zu unterbleiben, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn ein angemessenes Datenschutzniveau nicht festgestellt werden kann; es sei denn, dass ein Ausnahmetatbestand nach § 4c Abs. 1 oder Abs. 2 BDSG eingreift.

Die Angemessenheit des Schutzniveaus bestimmt sich dabei nach § 4b Abs. 3 BDSG, d. h. sie ist unter Berücksichtigung aller Umstände zu beurteilen, insbesondere anhand der für den betreffenden Empfängerstaat geltenden Rechtsnormen sowie der Rechtspraxis. In Anwendung dieser Grundsätze gewährleistet Kanada für die Beschäftigtendaten von Mitarbeitern privater Unternehmen kein dem europäischen Datenschutzniveau äquivalentes.

In diesem Zusammenhang ist zunächst zu berücksichtigen, dass Kanada einer der sogenannten Five-Eyes-Staaten ist, deren Geheimdienste weitgehend einschränkungslos auch auf Inhaltsdaten von elektronisch gespeicherten Daten zugreifen können, ohne dass sich die Betroffenen wirksam dagegen wehren können. Abgesehen davon hat die Europäische Kommission in ihrer Entscheidung vom 20. Dezember 2001 (2002/2/EG) entschieden, dass Kanada nur insofern als ein Land angesehen wird, das ein angemessenes Datenschutzniveau garantiert, als die übermittelten Daten dem kanadischen Datenschutzrecht PIPEDA unterliegen. Beschäftigtendaten von Privatunternehmen sind vom Anwendungsbereich des PIPEDA jedoch ausgenommen.

Die Datenübermittlung nach Kanada ließ sich auch nicht nach § 4c Abs. 1 oder Abs. 2 Satz 1 BDSG rechtfertigen. Die Ausnahmetatbestände des § 4c Abs. 1 BDSG lagen offenkundig nicht vor. EU-Standardvertragsklauseln im Sinne des § 4c Abs. 2 Satz 1 BDSG schloss das Unternehmen trotz mehrfacher Hinweise nicht ab.

Nachdem das Unternehmen nicht bereit war, innerhalb angemessener Frist datenschutzkonforme Zustände herzustellen, erließ ich eine datenschutzrechtliche Anordnung nach § 38 Abs. 5 Satz 1 BDSG, mit der ich dem Unternehmen aufgab, die Software entweder ohne Inanspruchnahme der Cloud-Dienstleistungen zu nutzen oder bei weiterer Inanspruchnahme der Cloud-Dienstleistungen eine dem kanadischen Datenbankanbieter nicht zugängliche Form einer Datenverschlüsselung einzurichten. Diese Anordnung wurde bestandskräftig. Das Unternehmen nutzt mittlerweile einen Server mit Standort innerhalb der europäischen Union und hat auch einen Auftragsdatenvertrag gemäß § 11 Abs. 2 BDSG abgeschlossen.

8.3.2 Aushang einer Kündigung am Schwarzen Brett

Ein Betroffener, dem fristlos gekündigt worden war, bat mich um Hilfe, nachdem sein Arbeitgeber am „Schwarzen Brett“ ein Schreiben ausgehangen hatte, in dem die anderen Mitarbeiter u. a. darüber informiert wurden, dass dem Betroffenen fristlos gekündigt wurde und ihm verboten wird, sich in den Geschäftsräumen aufzuhalten. Des Weiteren befand sich auf der Information der handschriftliche Zusatz, dass die Hintergründe der Kündigung in einer Dienstberatung ausgewertet werden sollten.

Ich habe dem Arbeitgeber mitgeteilt, dass diese Veröffentlichung datenschutzrechtlich unzulässig ist. Gemäß § 32 Abs. 1 Satz 1 BDSG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies u. a. für die Beendigung des Beschäftigungsverhältnisses erforderlich ist. Die Veröffentlichung und auch die angekündigte Mitteilung der Hintergründe der fristlosen Kündigung in einer Dienstberatung erfüllen diese Voraussetzungen offenkundig nicht. Es geht die anderen Mitarbeiter (mit Ausnahme der Personalsachbearbeiter und des Vorgesetzten) schlichtweg nichts an, warum ihrem Kollegen fristlos gekündigt wurde. Gleiches gilt für das erteilte Hausverbot, das sich auch auf weniger öffentlichkeitsheischende Art und Weise durchsetzen lässt (z. B. Abnahme des Schlüssels; mündliche Information des Pförtners). Besonders brisant wäre es, wenn Publikumsverkehr bestünde: Dann würde die Tatsache der Kündigung in unzulässiger Weise an Dritte übermittelt, ohne dass hierfür auch nur ansatzweise berechtigte Interessen des Arbeitgebers ersichtlich sind.

Auf meine Aufforderung hat der Arbeitgeber den Aushang entfernt und mir bestätigt, dass die Gründe für die fristlose Kündigung nicht in einer Betriebsversammlung thematisiert werden.

8.3.3 Namentliche Bekanntgabe von Mitarbeitern mit größeren krankheitsbedingten Fehlzeiten

Aufgrund zweier Eingaben musste ich mich erneut mit dieser Thematik auseinandersetzen (siehe schon 5/4.3.3.4). So veranlasste der Vorstand eines Vereins, dass über den elektronischen Newsletter an die Mitglieder und Mitarbeiter des Vereins ein Bericht versandt wurde, in dem sich ein Hinweis auf die Dauer der Arbeitsunfähigkeit ausgewählter, namentlich benannter Mitarbeiter befand. Ein anderer Arbeitgeber gab im Rahmen eines Projektleiter-Meetings in einer Präsentation mehrere Mitarbeiter namentlich bekannt, die jeweils mehr als 50 Krankheitstage aufwiesen. Diese Präsentation wurde anschließend mit dem Protokoll per E-Mail an die Teilnehmer des Meetings sowie weitere Personen versandt.

Im letztgenannten Fall handelte es sich, da der Krankenstand nur Betriebsangehörigen mitgeteilt wurde, um eine Nutzung personenbezogener Daten. Im Falle des Vereins lag hingegen eine Datenübermittlung vor, da die Vereinsmitglieder im Verhältnis zum Verein als Dritte anzusehen sind (§ 3 Abs. 8 Satz 2 BDSG). Diese Unterscheidung spielt insofern eine Rolle, als nur die unbefugte Datenübermittlung, nicht jedoch die unbefugte Datennutzung bußgeldbewehrt ist (§ 43 Abs. 2 Nr. 1 BDSG).

Ich habe die Bekanntgabe der Arbeitsunfähigkeit in beiden Fällen für unzulässig erachtet. Personenbezogene Daten eines Arbeitnehmers dürfen nach § 32 Abs. 1 Satz 1 BDSG nur für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Aus den insoweit für die Bewertung heranzuziehenden § 28 Abs. 6 BDSG (Erhebung, Verarbeitung und Nutzung besonderer Arten personenbezogener Daten für eigene Geschäftszwecke) oder § 84 Abs. 2 SGB IX (betriebliches Eingliederungsmanagement) ergibt sich keine Befugnis, die Mitglieder des Vereins bzw. die Projektleiter personenbezogen über die Zahl der bisherigen Krankheitstage einzelner Mitarbeiter zu unterrichten.

Bei der Tatsache, dass und wie lange ein Mitarbeiter krankgeschrieben war, handelt es sich um besonders schutzwürdige personenbezogene Daten im Sinne des § 3 Abs. 9 BDSG. Deren Verarbeitung ist ohne Einwilligung des Betroffenen nur unter engen, im Einzelnen aufgezählten Voraussetzungen zulässig: u. a. zum Schutz lebenswichtiger Inte-

ressen, wenn der Betroffene aus physischen oder rechtlichen Gründen an einer Einwilligung gehindert ist (§ 28 Abs. 6 Nr. 1 BDSG), wenn es sich um offenkundig von dem Betroffenen öffentlich gemachte Daten handelt (§ 28 Abs. 6 Nr. 2 BDSG) oder zur Geltendmachung rechtlicher Ansprüche (§ 28 Abs. 6 Nr. 3 BDSG).

Diese Voraussetzungen lagen in beiden Fällen nicht vor. Insbesondere kann sich ein Arbeitgeber nicht auf § 28 Abs. 6 Nr. 2 BDSG mit der Begründung berufen, dass die Arbeitnehmer ihre krankheitsbedingten Fehlzeiten durch automatische Abwesenheitsnotizen im E-Mail-Programm öffentlich bekannt gemacht haben. Denn auf diese Weise konnte der Empfänger allenfalls wissen, dass der Mitarbeiter häufiger abwesend war, nicht jedoch aus welchem Grund und schon gar nicht, seit wann und wie lange in der Summe. Der Verein konnte zudem nicht geltend machen, dass die Versendung des Krankenstands der Angestellten des Vereins über den Newsletter erfolgte, um rechtliche Ansprüche der Vereinsmitglieder gegenüber dem Vorstand wegen unzureichender Organisation der Verwaltungsabläufe abzuwehren. Hierfür war die Bekanntgabe der Tatsache der Krankschreibung bestimmter Angestellter des Vereins offensichtlich nicht erforderlich. Abgesehen davon überwiegt das schutzwürdige Interesse der Angestellten, dass ihr Krankenstand nicht in einem vereinsinternen elektronischen Newsletter veröffentlicht wird, dessen Weiterverbreitung nicht kontrollierbar ist.

Tatsächlich beriefen sich beide Arbeitgeber letztlich sinngemäß darauf, dass Zwecke der Personalplanung (hohe Arbeitsbelastung der übrigen Mitarbeiter) die Bekanntgabe der Fehlzeiten erfordert hätten; ein insoweit einschlägiger Zulässigkeitstatbestand ist § 28 Abs. 6 BDSG jedoch nicht zu entnehmen. Die Norm geht insofern auch dem allgemeinen Zulässigkeitstatbestand des § 28 Abs. 1 und Abs. 2 BDSG vor.

Der Verein bereinigte auf meinen Hinweis den Bericht mit den krankheitsbedingten Fehlzeiten, der in dem versandten Newsletter verlinkt war.

8.3.4 Zugriff auf E-Mail-Postfächer im Abwesenheitsfall

Ich war über einen nicht rechtskonformen Umgang mit Passwörtern in einer sächsischen Firma unterrichtet worden: Die individuellen Passwörter der Mitarbeiter wären im Unternehmen allgemein bekannt; in Abwesenheitszeiten (z. B. bei Urlaub, Krankheit) würde regelmäßig auf die E-Mail-Postfächer der betreffenden Mitarbeiter zugegriffen.

Ganz so krass stellte sich die betriebliche Praxis dann aber doch nicht dar. Tatsächlich bestand in diesem Unternehmen aber wegen der besonderen Serviceorientierung die Vorgabe, dass bei geplanter Abwesenheit eines Mitarbeiters eine automatische Weiterleitung an seinen Vertreter – eine Privatnutzung des E-Mail-Systems war nicht erlaubt – einzu-

richten ist. Bei längeren ungeplanten Abwesenheiten sei es in der Vergangenheit tatsächlich so gewesen, dass in dringenden Fällen der Mitarbeiter gebeten worden sei, einem Kollegen seines Vertrauens sein Passwort bekanntzugeben, um den Zugriff auf wichtige E-Mails zu ermöglichen und so den Geschäftsbetrieb aufrechterhalten zu können.

Mit Erhalt meines Schreibens sind diese Regelungen bzw. Verfahrensweisen sofort ausgesetzt worden. Ich habe dem Geschäftsführer auf dessen Bitte folgende rechtskonforme Alternativen aufgezeigt:

Für den Fall einer planmäßigen Abwesenheit von Mitarbeitern stellt das Setzen einer Abwesenheitsnotiz gegenüber einer E-Mail-Weiterleitung das mildere Mittel dar. Dabei ist einerseits zu berücksichtigen, dass ein Mitarbeiter auch bei untersagter Privatnutzung des E-Mail-Systems nicht verhindern kann, dass ihm als privat einzustufende E-Mails zugesandt werden. Andererseits ist davon auszugehen, dass auch die E-Mail-Absender regelmäßig davon ausgehen, dass ihre E-Mails ausschließlich dem jeweiligen Adressaten zugestellt werden. Dies kann sich sowohl in deren Schreibstil als auch in zusätzlich in den jeweiligen E-Mails enthaltenen Informationen mit Privatbezug widerspiegeln. Eine solche Abwesenheitsnotiz sollte die Informationen enthalten, bis wann der Adressat nicht erreichbar ist, dass die E-Mails bis dahin nicht gelesen werden und an wen sich der Absender vertretungsweise wenden kann.

Im Fall einer unvorhergesehenen längeren Abwesenheit eines Mitarbeiters kann dieser eine solche Abwesenheitsnotiz naturgemäß nicht setzen. In diesem Fall kann die nachträgliche Einrichtung einer E-Mail-Weiterleitung wie auch die Sichtung der bis dahin auf diesem Account eingegangenen E-Mails zulässig sein. Allerdings sollte hierfür nicht das bisher vom betroffenen Mitarbeiter genutzte Passwort in Erfahrung gebracht werden, da aus diesem Passwort auch Rückschlüsse auf dessen generelle Vorgehensweise bei der Passwortwahl gezogen werden können. Stattdessen ist in solchen Ausnahmefällen – also falls ein dringendes betriebliches Bedürfnis besteht und ein möglicherweise bestehender Betriebsrat einbezogen worden ist – das Passwort durch den Systemadministrator zurückzusetzen und ein neues temporäres Passwort zu vergeben. Soweit möglich ist der Betroffene noch vorher, spätestens jedoch bei seiner Rückkehr darüber zu informieren. Bei Rückkehr ist das Passwort durch den Mitarbeiter sofort wieder zu ändern. In solchen Fällen ist darauf zu achten, dass E-Mails vom jeweiligen Vertreter bzw. Vorgesetzten immer dann nicht weiter inhaltlich zur Kenntnis genommen werden, wenn bzw. sobald ihr privater Charakter erkannt worden ist.

8.3.5 Outsourcing von Personalverwaltungsaufgaben

Ich hatte mich aufgrund von Eingaben betroffener Mitarbeiter mit der Frage auseinanderzusetzen, unter welchen Voraussetzungen die Auslagerung von Personalverwaltungsaufgaben innerhalb eines Konzerns datenschutzrechtlich zulässig ist. In den konkreten Fällen übernahm eine Konzerntochter aufgrund entsprechender Anweisungen der Konzernmutter für alle anderen Konzerntöchter Aufgaben, die zuvor deren eigene Personalsachbearbeiter wahrgenommen hatten.

Zunächst ist festzuhalten, dass das Bundesdatenschutzgesetz kein Konzernprivileg kennt. Bei konzernangehörigen Unternehmen handelt es sich um eigenständige juristische Personen, die damit verantwortliche Stellen im Sinne des § 3 Abs. 7 BDSG sein können. Die Mitarbeiter sind auch nicht als Mitarbeiter des Konzerns anzusehen, vielmehr ist Arbeitgeber ausschließlich die jeweilige Konzerntochter, mit der der Arbeitsvertrag geschlossen wurde. Wenn also die personalverwaltende Konzerntochter für andere Konzernunternehmen Aufgaben der Personalverwaltung erledigt, erhebt, verarbeitet und nutzt sie personenbezogene Daten fremder Arbeitnehmer. Weil die Personaldaten nicht beim eigentlichen Arbeitgeber gespeichert werden, führt dies bei den betroffenen Arbeitnehmern zu berechtigten Nachfragen.

Für die datenschutzrechtliche Beurteilung ist es dabei im vorliegenden Kontext nicht ausschlaggebend, ob der Arbeitgeber seine Arbeitnehmer anweist, der personalverwaltenden Konzerntochter selbst Personaldaten mitzuteilen oder ob der Arbeitgeber diese selbst bei seinen Arbeitnehmern erhebt und anschließend an die personalverwaltende Konzerntochter übermittelt.

Entscheidend für die rechtliche Beurteilung ist aber, ob die personalverwaltende Konzerntochter im Verhältnis zum Arbeitgeber als Dritter oder als Auftragsdatenverarbeiter anzusehen ist. Denn wenn eine Personalverwaltung durch Mitarbeiter anderer Unternehmen nicht als Auftragsdatenverarbeitung im Sinne des § 11 BDSG qualifiziert werden kann, liegt eine Datenübermittlung an Dritte vor (§ 3 Abs. 8 Satz 2, Abs. 4 Satz 2 Nr. 3 BDSG), die nur dann zulässig ist, wenn die betroffenen Mitarbeiter wirksam einwilligen (§ 4a BDSG) oder eine Norm, insbesondere des Bundesdatenschutzgesetz diese erlauben. Anderenfalls ist sie verboten (§ 4 Abs. 1 BDSG).

Ob die personalverwaltende Konzerntochter Auftragsdatenverarbeiter oder Dritter und damit verantwortliche Stelle ist, lässt sich nicht pauschal beantworten, sondern nur anhand des konkreten Einzelfalls entscheiden (vgl. Petri in Simitis, BDSG, 8. Auflage, § 11 Rdnrn. 20 ff.). Anhaltspunkt für eine Auftragsdatenverarbeitung ist z. B., ob die personalverwaltende Stelle als weisungsgebundenes Werkzeug des Arbeitgebers agiert und nur

einzelne Hilfstätigkeiten übernimmt. Wird die Aufgabe der Personalverwaltung komplett von einer Konzerntochter für alle anderen Konzernunternehmen übernommen, agiert diese weisungsfrei und im übergeordneten Konzerninteresse, liegt ein Fall der sogenannten Funktionsübertragung vor: Dann ist die personalverwaltende Konzerntochter als Dritter anzusehen.

In einem Fall qualifizierte ich auf der Grundlage dieser Kriterien das Rechtsverhältnis zwischen den beteiligten Konzerntöchtern als *Funktionsübertragung*: Das Unternehmen hatte die Personalverwaltung vollständig auf ein Schwesterunternehmen ausgegliedert und gab an, dass die dort beschäftigten Personalsachbearbeiter nur ihren Vorgesetzten, nicht jedoch der Geschäftsführung des Unternehmens verantwortlich sind. Die Personalsachbearbeiter des Schwesterunternehmens hatten sogar die Befugnis, Arbeitsverträge abzuschließen und Kündigungen auszusprechen. Dass zwischen den Schwesterunternehmen ein Auftragsdatenverarbeitungsvertrag abgeschlossen wurde, war insofern irrelevant. Denn auch in diesem stand, dass der „Auftragnehmer" sämtliche Aufgaben der Personalsachbearbeitung/-verwaltung für den „Auftraggeber" übernahm, weil der „Auftraggeber" den Bereich Personalverwaltung ausgegliedert hat.

Die Funktionsübertragung schloss materiell eine Auftragsdatenverarbeitung im Sinne des § 11 Abs. 1 BDSG aus, es handelte sich vielmehr um eine Datenübermittlung zwischen den Schwesterunternehmen. Diese beurteilte ich im Ergebnis als datenschutzwidrig, weil sie sich weder auf § 32 Abs. 1 Satz 1 BDSG noch auf § 28 Abs. 1 Nr. 2 BDSG (wenn man diese Vorschrift überhaupt für anwendbar hält) stützen konnte.

Gemäß § 32 Satz 1 BDSG ist die Datenerhebung und -verarbeitung im Beschäftigungsverhältnis nur dann zulässig, wenn sie für die Durchführung des Arbeitsverhältnisses erforderlich ist. Reine Zweckmäßigkeitserwägungen, die für eine Auslagerung der Personalverwaltung sprechen können, genügen nicht, weil diese Aufgaben genauso gut wie in der Vergangenheit durch eigene Mitarbeiter des Unternehmens hätten erledigt werden können. Finanzielle Erwägungen der Konzernmutter spielen insofern keine Rolle.

Im Rahmen der gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG vorzunehmenden Interessenabwägung überwogen die schutzwürdigen Interessen der Arbeitnehmer am Ausschluss der Datenerhebungen, -verarbeitungen und -nutzungen durch die personalverwaltende Konzerntochter die berechtigten Interessen des ausgliedernden Unternehmens. Denn die Erhebung, Übermittlung und Nutzung von personenbezogenen Daten der Mitarbeiter erfolgte innerhalb des Konzerns völlig ungeregelt. Ein konzerninternes Datenschutzkonzept für den Austausch von Beschäftigtendaten existierte nicht. Auch der Auftragsdatenverarbeitungsvertrag enthielt keinerlei konkretisierende Regelungen zum Verarbeitungszweck, einschließlich Zweckbindung sowie Angaben zur Gewährleistung und

Durchsetzung von Rechten der betroffenen Arbeitnehmer gegenüber den beteiligten Konzerngesellschaften.

Für die vorzunehmende Gesamtabwägung sind schlüssige konzerninterne Datenschutzkonzepte jedoch von überragender und entscheidender Bedeutung und in global agierenden Konzernen auch die Regel. Möglicherweise nicht zuletzt deshalb, weil Datenübermittlungen, die sich nicht durch eine Rechtsnorm legitimieren lassen, als unbefugte Verarbeitung von personenbezogenen Daten gemäß § 43 Abs. 2 Nr. 1 BDSG mit einer Geldbuße in Höhe von bis zu 300.000 € geahndet werden können (§ 43 Abs. 3 BDSG). Die betriebliche Datenschutzbeauftragte des Unternehmens teilte mir mit, dass ein solches Datenschutzkonzept unter Berücksichtigung der Vorgaben der Datenschutz-Grundverordnung erarbeitet wird, wovon ich mich überzeugen werde.

In einem anderen Fall lag hingegen tatsächlich eine *Auftragsdatenverarbeitung* vor, denn die Arbeitgebergesellschaft behielt sich vertraglich umfassende Weisungsrechte vor, inhaltliche Entscheidungsbefugnisse hatte das Schwesterunternehmen nicht. Das Schwesterunternehmen übernahm lediglich die räumliche Ablage der in Papier geführten Personalakten, es erfasste Arbeits-, Urlaubs- und Krankheitstage der Mitarbeiter und übergab Lohnunterlagen an das Steuerbüro.

Die Konzernunternehmen waren nicht als Dritte anzusehen (§ 3 Abs. 8 Satz 3 BDSG), so dass auch keine Datenverarbeitung in Form der Datenübermittlung vorlag, die ansonsten einer besonderen Rechtsgrundlage bedurft hätte. Der vorgelegte schriftliche Auftragsdatenverarbeitungsvertrag erfüllte die Anforderungen des § 11 Abs. 2 BDSG.

Allerdings hatte sich auch wegen der räumlichen Nähe zwischen den Schwesterunternehmen die Praxis etabliert, dass die Geschäftsführerin des einen Unternehmens die Personalleiterin des anderen Unternehmens beratend bei personellen Entscheidungen sowie zur Unterstützung bei Vorstellungsgesprächen hinzuzog. Insofern wurde der Rahmen der in der Vereinbarung über die Auftragsdatenverarbeitung definierten Datenerhebung und Datenverarbeitung überschritten. Zudem handelte die Personalleiterin diesbezüglich nicht nur als weisungsgebundenes Werkzeug, sondern die Geschäftsführerin nutzte bewusst das Know-how der Personalabteilung des Schwesterunternehmens. Man teilte sich insofern letztlich die Entscheidungsverantwortung.

Diese Datenverarbeitung in Form der Datenübermittlung ist nur zulässig, soweit sie für die Begründung, Durchführung und Beendigung des Arbeitsverhältnisses gemäß § 32 Abs. 1 Satz 2 BDSG erforderlich ist.

Hinsichtlich der Begründung von Arbeitsverhältnissen ist anerkannt, dass sich der potentielle Arbeitgeber zur Durchführung von Eignungstests externer Dienstleister bedienen

darf (Seifert in Simitis, BDSG, 8. Auflage, § 32 Rdnr. 54). Allerdings sind die Bewerber ausdrücklich vorab darauf hinzuweisen, dass und warum an dem Auswahlgespräch ein Dritter teilnimmt. Gemäß § 28 Abs. 5 Satz 3 BDSG hätte die Geschäftsführerin das Schwesterunternehmen – am besten schriftlich – darauf hinweisen müssen, dass die personenbezogenen Daten, die der Personalleiterin z. B. für die Vorbereitung der Auswahlgespräche übermittelt werden, grundsätzlich nicht für andere Zwecke genutzt werden dürfen. Zudem muss sichergestellt werden, dass das Schwesterunternehmen Daten abgelehnter Bewerber unverzüglich nach Abschluss des Bewerbungsverfahrens löscht.

Als datenschutzrechtlich unzulässig erachtete ich jedoch die Praxis, dass die Geschäftsführerin die Personalleiterin des Schwesterunternehmens beratend bei personellen Einzelfallentscheidungen heranzog. Ohne Zweifel hätte die Geschäftsführerin im Hinblick auf anstehende Personalentscheidungen nicht bei der Personalabteilung irgendeines anderen Unternehmens unter Preisgabe personenbezogener Daten ihrer Arbeitnehmer Rat gesucht. Ein Konzernprivileg existiert nicht. Soweit die Geschäftsführerin nicht nur abstrakte Sachverhalte schilderte (wobei ausgeschlossen sein musste, dass die Personalleiterin des Schwesterunternehmens aufgrund der überschaubaren Mitarbeiterzahl diese identifizieren konnte), handelt es sich um eine Datenübermittlung (§ 3 Abs. 4 Satz 2 Nr. 3a BDSG). Diese ist nicht für die Durchführung des Arbeitsverhältnisses erforderlich (§ 32 Abs. 1 Satz 1 BDSG). Die Datenübermittlung konnte auch nicht auf § 28 Abs. 1 Nr. 2 BDSG gestützt werden, denn die schutzwürdigen Interessen der Arbeitnehmer an dem Ausschluss der Übermittlung überwogen. Denn in erster Linie oblag es der Geschäftsführerin, im Unternehmen den erforderlichen Sachverstand vorzuhalten, um Personalentscheidungen eigenverantwortlich treffen zu können (Einstellung einer Personalreferentin, Fortbildungsmaßnahmen, Beratung durch einen Rechtsanwalt, der besonderen standesrechtlichen Verschwiegenheitspflichten unterworfen ist). Die Arbeitnehmer mussten den in der Datenübermittlung an das Schwesterunternehmen liegenden, erheblichen Eingriff in ihr Recht auf informationelle Selbstbestimmung nicht hinnehmen. Zu berücksichtigen war hierbei auch, dass es sich bei den diskutierten Sachverhalten um besonders sensible personenbezogene Daten handeln konnte (z. B. im Zusammenhang mit krankheits- oder verhaltensbedingten Kündigungen, Abmahnungen, Beurteilungen). Gründe der Kostenersparnis vermochten diesen Eingriff nicht zu legitimieren.

8.3.6 Biometrisches Zeiterfassungs- und Ortungssystem

Ein Unternehmen führte ein biometrisches Zeiterfassungssystem ein. Die Mitarbeiter erhielten mobile Endgeräte mit Kamerafunktion (Smartphone, Tablet), auf denen eine App installiert war. Des Weiteren wurde den Mitarbeitern ein Kärtchen mit einem QR-Code ausgehändigt, der Namen und Vornamen des Mitarbeiters widerspiegelte. Die Mitarbeiter

wurden verpflichtet, Beginn und Ende der Arbeitszeit bzw. Pausen dergestalt zu dokumentieren, dass sie mittels des mobilen Endgeräts ein Foto von sich mit dem QR-Code anfertigten. Das Foto nebst QR-Code sowie die Zeit- und Ortsangaben wurden dann an den Dienstleister übermittelt, der einen Server mit Standort in den Niederlanden nutzte. Die Identifikation der Mitarbeiter erfolgte nach Vortrag des Unternehmens „manuell" anhand der mit Hilfe der App angefertigten Fotos durch eine Personalsachbearbeiterin des Arbeitgeberunternehmens. Die Lichtbilder der Mitarbeiter sollten jeweils bis zum 15. des Monats, der auf den Monat folgt, in dem sie übermittelt wurden, gespeichert werden¸ die übrigen Daten für die Dauer von zehn Jahren. Einen Auftragsdatenverarbeitungsvertrag mit dem Dienstleister hatte das Unternehmen nicht geschlossen.

Die Einführung dieses Zeiterfassungssystems begründete das Unternehmen damit, dass Manipulationen bei der Zeiterfassung (z. B. durch Einstempeln durch einen anderen Mitarbeiter) verhindert werden sollten. Zudem sollten die erfassten Orts- und Zeitangaben dazu dienen, Leistungen des Unternehmens gegenüber seinen Auftraggebern abzurechnen. Erreicht werden sollte auf diese Weise auch eine verbesserte Auslastung und Auftragsabwicklung sowie eine Optimierung der Personalplanung. Das Unternehmen räumte ein, dass das System eine gewisse Leistungssteigerung der Mitarbeiter erzeugt hatte, was man als positiven Nebeneffekt empfand. Das Unternehmen vertrat die Auffassung, dass die Verwendung des biometrischen Zeiterfassungssystems zulässig sei, weil die Mitarbeiter wirksam schriftlich in die Nutzung eingewilligt hätten: Sie seien durch die jeweiligen Vorgesetzten aufgeklärt worden und hätten die Möglichkeit gehabt, den Einsatz des Zeiterfassungssystems zu verweigern, ohne dass hieraus Konsequenzen erwachsen wären. Tatsächlich stellte sich heraus, dass lediglich die Anfertigung der Fotos zur Disposition der Mitarbeiter gestellt wurde.

Diese biometrische Zeiterfassung war datenschutzrechtlich unzulässig. Auf eine wirksame Einwilligung konnten Datenerhebung und Datenverarbeitung nicht gestützt werden. Denn nach meiner Einschätzung mangelte es aufgrund des im Arbeitsverhältnis bestehenden Über-/Unterordnungsverhältnisses an der erforderlichen Freiwilligkeit der Einwilligungserklärung im Sinne des § 4a BDSG. Echte Alternativen zum Gebrauch des biometrischen Zeiterfassungssystems hat das Unternehmen den Mitarbeitern nämlich nicht eröffnet. Dies ergab sich auch aus dem Inhalt der für alle Mitarbeiter verbindlichen Arbeitsordnung des Unternehmens.

Eine gesetzliche Rechtsgrundlage für den Einsatz des biometrischen Zeiterfassungssystems existierte nicht: Die Datenerhebung und Datenverarbeitung im Arbeitsverhältnis ist zulässig, wenn sie für dessen Durchführung erforderlich ist (§ 32 Abs. 1 Satz 1 BDSG). Des Weiteren ist eine Datenerhebung und Datenverarbeitung zulässig, wenn sie zur Wahrung der berechtigten Interessen des Unternehmens erforderlich ist und kein Grund zu der

Annahme besteht, dass das schutzwürdige Interesse der betroffenen Arbeitnehmer an dem Ausschluss der Datenerhebung und Datenverarbeitung überwiegt (§ 28 Abs. 1 Nr. 2 BDSG).

Ein zulässiger Zweck, der mit dem Einsatz des Zeiterfassungs- und Ortungssystems verfolgt wird, allein genügte folglich nicht. Vielmehr muss das Recht auf unternehmerische Freiheit mit dem Recht auf informationelle Selbstbestimmung der Arbeitnehmer umfassend abgewogen werden. Hinsichtlich der Datenerhebung und Datenspeicherung spielen dabei die besonderen Gefahren des Zeiterfassungs- und Ortungssystems (z. B. als Mittel zur Erstellung von Bewegungsprofilen und einer lückenlosen Überwachung der Arbeitnehmer) eine Rolle. Mildere Mittel, mit dem sich der angestrebte Zweck gleichermaßen erreichen lässt, dürfen nicht verfügbar sein.

Verhindert bzw. aufgeklärt werden sollten mit Hilfe der biometrischen Komponente in erster Linie Manipulationen, d. h. Arbeitszeitbetrug der Mitarbeiter. Letztlich ging es dem Unternehmen damit um eine allgemeine, d. h. anlasslose Verhaltens- und Leistungskontrolle der Mitarbeiter. Eine solche setzt die Mitarbeiter jedoch einem Generalverdacht aus und stellt einen schwerwiegenden Eingriff in deren Recht auf informationelle Selbstbestimmung dar.

Unter Heranziehung der Wertungen des § 32 Abs. 1 Satz 2 BDSG sind derartige Eingriffe in das allgemeine Persönlichkeitsrecht der Arbeitnehmer nur zulässig, wenn der zu dokumentierende konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung besteht und die Auswertung der mittels des Zeiterfassungs- und Ortungssystems erhobenen Daten praktisch das einzig mögliche Mittel zur Aufklärung darstellt. Der Verdacht muss sich auf eine konkrete Person oder zumindest auf eine räumlich-funktional abgrenzbare Personengruppe beziehen. Die tatsächlichen Verdachtsmomente gegenüber bestimmten Mitarbeitern wären schriftlich oder elektronisch zu dokumentieren. Die Datenerhebung, -verarbeitung und -nutzung muss zur Aufdeckung dieses konkreten Arbeitszeitbetrugs erforderlich sein: Das bedeutet, dass keine ebenso effektiven, den Arbeitnehmer weniger belastenden Möglichkeiten zur Aufklärung zur Verfügung stehen dürfen. Und nicht zuletzt muss die Maßnahme verhältnismäßig sein (vgl. z. B. LArbG Köln, Urteil vom 29. September 2014 – 2 Sa 181/14, juris). Diese Voraussetzungen lagen offenkundig nicht vor, vielmehr wurde den Mitarbeitern mehr oder weniger pauschal unterstellt, Arbeitszeiten abzurechnen, die nicht angefallen sind: Dies sollte durch die Anfertigung der Lichtbilder in Verbindung mit der Erfassung der Zeit- und Standortdaten verhindert werden.

Soweit das Unternehmen die durch das biometrische Zeiterfassungs- und Ortungssystem erfassten Daten auch zur Abrechnung von Aufträgen (Rechnungsstellung gegenüber

Auftraggebern) verwendet hat, verfolgte es im Sinne des § 28 Abs. 1 Satz 1 Nr. 2 BDSG berechtigte Interessen. Allerdings hatte ich Zweifel an der Eignung des eingesetzten Systems zur Erreichung des angegebenen, damit verfolgten Zwecks (Nachweis im Streitfall). Zudem überwogen die schutzwürdigen Belange der Arbeitnehmer. Es war nicht nachvollziehbar, in welcher Form die von den Mitarbeitern erhobenen Daten (Zeiterfassung, Ortsdaten etc.) in die Abrechnung einflossen und von Auftraggebern des Unternehmens gefordert und anerkannt wurden. Als milderes Mittel kamen Aufschriebe der eingesetzten Mitarbeiter in Betracht. In beiden Fällen muss das Unternehmen nämlich letztlich darauf vertrauen, dass die Angaben korrekt sind. Denn die mittels des biometrischen Zeiterfassungs- und Ortungssystems erfasste Anwesenheit der Mitarbeiter an dem Einsatzort belegt nicht, dass der Mitarbeiter dort auch gearbeitet hat. Allerdings ist der Eingriff in das informationelle Selbstbestimmungsrecht der Mitarbeiter bei einem elektronischen Zeiterfassungssystem, zumal einem webbasierten ungleich schwerer.

Nicht zuletzt wegen der Speicherdauer und der technischen Ausgestaltung des Systems (Speicherung in der Cloud, fehlende umfassende Systemdokumentation; keine Vorabkontrolle) und der vom Unternehmen nicht ausgeschlossenen Möglichkeit die Daten auch für Zwecke der allgemeinen Verhaltens- und Leistungskontrolle einzusetzen, kam ich zu dem Schluss, dass die schutzwürdigen Belange der Arbeitnehmer auch bei Verzicht auf die Anfertigung von Fotos überwogen. Zudem hatte das Unternehmen auch keinen Auftragsdatenverarbeitungsvertrag gemäß § 11 Abs. 2 BDSG mit dem Dienstleister geschlossen.

Ich wies das Unternehmen zudem darauf hin, dass es vor der Inbetriebnahme des Zeiterfassungs- und Ortungssystems eine Vorabkontrolle hätte durchführen müssen. Nach § 4d Abs. 5 BDSG ist eine Vorabkontrolle immer dann durchzuführen, wenn automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen. Dies war hier der Fall. Denn das eingesetzte Zeiterfassungs- und Ortungssystem ermöglichte eine Rundumüberwachung der Mitarbeiter, einschließlich potentiell möglicher umfassender Leistungs- und Verhaltenskontrollen und barg daher erhebliche Gefahren für die informationelle Selbstbestimmung der Mitarbeiter. Insbesondere ermöglichten es die Geräte, Bewegungsprofile der Mitarbeiter zu erstellen, die Arbeits- und Pausenzeiten und die Standorte während der gesamten Arbeitszeit zu erfassen. Die Verpflichtung entfiel auch nicht deshalb, weil das System für die Durchführung der Arbeitsverhältnisse erforderlich gewesen wäre (Petri in Simitis, BDSG, 8. Auflage, § 4d Rdnr. 34).

Nachdem ich das Unternehmen zu der Absicht angehört hatte, zur Beseitigung der festgestellten datenschutzrechtlichen Verstöße eine aufsichtsbehördliche Anordnung gemäß

§ 38 Abs. 5 Satz 1 BDSG zu erlassen, stellte es die Nutzung des biometrischen Zeiterfassungs- und Ortungssystems ein.

Zum Abschluss eine klarstellende Anmerkung: Eine Arbeitszeiterfassung mit elektronischen Mitteln ist datenschutzrechtlich (ohne Verwendung biometrischer Merkmale der Arbeitnehmer) nach § 32 Abs. 1 Satz 1 BDSG nicht generell ausgeschlossen. Auch kann der Arbeitgeber grundsätzlich ein berechtigtes Interesse daran haben zu wissen, wo sich sein Mitarbeiter, der im Außendienst tätig ist, befindet (Disposition). Allerdings lässt sich damit grundsätzlich nur die Datenerhebung (Live Tracking), nicht jedoch die Datenspeicherung, insbesondere nicht für die Dauer von zehn Jahren rechtfertigen. Denn eine Disposition aktueller Aufträge lässt sich auf der Grundlage gespeicherter und damit überholter Datensätze nicht realisieren.

8.4 Gesundheitswesen

8.4.1 Wunddokumentation per Foto im Krankenhaus

Ein privates Krankenhaus fragte mich nach der Zulässigkeit der Anfertigung von Fotodokumentationen von Wunden bei im Krankenhaus stationär behandelten Patienten, insbesondere nach der Notwendigkeit einer hierfür einzuholenden gesonderten Einwilligung des Patienten.

Die ärztliche Dokumentationspflicht wird durch unterschiedliche Rechtsvorschriften geregelt, siehe § 10 BO der Sächsischen Landesärztekammer und § 57 BMV-Ä. Schließlich wird die Dokumentationspflicht seit Inkrafttreten des Patientenrechtegesetzes in § 630f BGB geregelt, wonach der Behandelnde verpflichtet ist, zum Zweck der Dokumentation in unmittelbarem zeitlichen Zusammenhang mit der Behandlung eine Patientenakte in Papierform oder elektronisch zu führen. Der Behandelnde ist zudem verpflichtet, in der Patientenakte sämtliche aus fachlicher Sicht für die derzeitige und künftige Behandlung wesentlichen Maßnahmen und deren Ergebnisse aufzuzeichnen, insbesondere die Anamnese, Diagnosen, Untersuchungen, Untersuchungsergebnisse, Befunde, Therapien und ihre Wirkungen, Eingriffe und ihre Wirkungen, Einwilligungen und Aufklärungen. Arztbriefe sind in die Patientenakte aufzunehmen.

Die ärztliche Dokumentation dient der Therapiesicherung und der Rechenschaftslegung sowie der Beweissicherung (mit der in § 630h BGB normierten Beweislastumkehr).

Wann ein Behandlungsinhalt als wesentlich zu qualifizieren ist, hängt meiner Auffassung nach in erster Linie von medizinischen Gesichtspunkten und von den Umständen des Einzelfalls ab. Soweit aus fachlichen Gründen eine Fotodokumentation angezeigt ist, halte

ich eine solche eben im Hinblick auf die bestehende Dokumentationspflicht für zulässig. Denn zu § 630f BGB führt die Gesetzesbegründung (BT-Drs. 17/10488) Folgendes aus:

„*Der Behandelnde kann die dokumentationspflichtige Maßnahme sowohl in Papier- als auch in elektronischer Form vermerken oder z. B. auch ein Video von einem operativen Eingriff erstellen und elektronisch speichern.*“

Soweit daher selbst Videoaufzeichnungen unter die Dokumentation fallen sollen, halte ich das Fertigen von Bildern ebenfalls für zulässig.

Aufgrund gesetzlicher Erlaubnisnorm bedarf es, soweit aus fachlicher Sicht eine entsprechende bildliche Dokumentation ansteht, nicht – noch zusätzlich – der Einwilligung des Patienten.

8.4.2 Weitergabe von Daten möglicher Organ- oder Gewebespender zwischen Kliniken

Ein Petent, dessen Angehöriger kurz zuvor in einer Klinik verstorben war, wandte sich an mich, nachdem er von einer anderen Klinik die Anfrage erhielt, ob er mit einer Transplantation der Organe des Verstorbenen einverstanden sei. Der Petent empfand das Vorgehen der beiden Kliniken als taktlos. Er wollte wissen, ob die Klinik, in der der Angehörige verstorben war, die Kontaktdaten des Petenten ohne dessen Zustimmung weitergeben durfte. Ein Organspenderausweis lag nicht vor.

Die beteiligten Kliniken haben sich datenschutzkonform verhalten; für die Weitergabe der Informationen bedurfte es keiner Einwilligung. Die Übermittlung war datenschutzrechtlich zulässig. Rechtsgrundlage hierfür ist § 7 TPG. Danach sind Erhebung und Verwendung personenbezogener Daten eines möglichen Organ- oder Gewebespenders, eines nächsten Angehörigen und die Übermittlung dieser Daten zwischen den beteiligten Kliniken zulässig, soweit dies u. a. zur Klärung erforderlich ist, ob eine Organ- oder Gewebeentnahme nach den §§ 3 Abs. 1 und 2, 4 Abs. 1 bis 3 sowie 9 Abs. 3 Satz 2 TPG zulässig ist. Gemäß § 4 Abs. 1 bis 3 TPG sind dabei die nächsten Angehörigen, zu denen der Petent zählte, dazu berufen, über die Organtransplantation zu entscheiden, wenn kein Organspenderausweis vorliegt.

8.4.3 Private Gutachtertätigkeit eines angestellten Klinikarztes

Ein Unternehmen, dessen Geschäftstätigkeit die ambulante medizinische Rehabilitation von Suchtkranken umfasste, beschäftigte einen angestellten Arzt als medizinischen Leiter. Dieser Arzt betrieb außerdem als Selbständiger eine Praxis in einem anderen Ort sowie unter seiner Privatanschrift ein Gutachterbüro. Im Rahmen dieser selbständigen

Tätigkeit wurde der Arzt von Sozialgerichten als Sachverständiger hinzugezogen. Die zur Erstellung der Sachverständigengutachten erforderliche Exploration der Patienten erfolgte jedoch nicht nur in seiner Praxis, sondern auch in den Räumlichkeiten der medizinischen Einrichtung, seinem Arbeitgeber.

Ein Patient, der von dem Arzt in den Räumlichkeiten der medizinischen Einrichtung im Auftrag eines Sozialgerichts begutachtet wurde, wandte sich an mich, weil er befürchtete, dass seine Gesundheitsdaten von dem Arzt unbefugt an Mitarbeiter der medizinischen Einrichtung weitergegeben wurden. Den Termin zur Begutachtung hatte der Patient mit einer Mitarbeiterin der medizinischen Einrichtung unter einer Handynummer vereinbaren müssen. Er sorgte sich auch, dass das Gutachten auf Rechnern der medizinischen Einrichtung gespeichert wurde und damit Dritten zugänglich war.

Der Arzt ist, wenn er als selbständiger Gutachter außerhalb seiner Kliniktätigkeit agiert, gemäß § 3 Abs. 7 BDSG verantwortliche Stelle. Denn er erhebt im Rahmen der Exploration personenbezogene Daten über die zu Begutachtenden (§ 3 Abs. 3 BDSG), genauer gesagt Gesundheitsdaten und damit besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG). Wenn er im Rahmen der Exploration Personal der medizinischen Einrichtung einsetzt oder Gutachten (ungesichert) auf deren Rechnern speichert, liegt darin eine Datenübermittlung an Dritte (§ 3 Abs. 4 Satz 2 Nr. 3 BDSG). Diese ist nur zulässig, soweit sie gesetzlich erlaubt oder angeordnet wird oder der Betroffene (hier der zu Begutachtende) wirksam (§ 4a BDSG) eingewilligt hat (§§ 4 Abs. 1, 28 Abs. 6 und 7 BDSG). Etwas anderes würde nur dann gelten, wenn ein Auftragsdatenverarbeitungsverhältnis im Sinne des § 11 BDSG mit der medizinischen Einrichtung besteht oder die Mitarbeiter der medizinischen Einrichtung auch bei dem Arzt selbst angestellt sind (§ 3 Abs. 8 Satz 2 und 3 BDSG).

Entsprechendes gilt natürlich auch für die medizinische Einrichtung: Diese darf nicht einfach zulassen oder dulden, dass der angestellte Arzt ohne weiteres, insbesondere ohne Einwilligung der zu Begutachtenden, Zugriff auf ihre Patientenakten oder elektronisch gespeicherte Datenbestände nimmt, um diese im Rahmen seiner selbständigen Sachverständigentätigkeit zu nutzen. Eine Person, die berufliche Aufgaben sowohl innerhalb als auch außerhalb der verantwortlichen Stelle wahrnimmt, muss die Funktionskreise strikt trennen (vgl. hierzu Dammann in Simitis, BDSG, 8. Auflage, § 3 Rdnrn. 156 und 237; Gola/Schomerus, BDSG, 12. Auflage, § 3 Rdnr. 54). Wegen der unterschiedlichen Verantwortlichkeiten (einerseits die medizinische Einrichtung, andererseits der Arzt als selbständiger Gutachter) müssen Datenerhebung und Datenverarbeitung voneinander getrennt erfolgen, was durch entsprechende technisch-organisatorische Maßnahmen sicherzustellen ist (§ 9 BDSG).

Eine unbefugte Datenübermittlung und ggf. Schweigepflichtverletzung läge im Übrigen auch vor, wenn dienstliche Telefonate über einen Privatanschluss geführt werden und Dritte auf diese Weise Kenntnis von Patientendaten erlangen. Auch bei Nutzung privater Räumlichkeiten muss durch entsprechende bauliche und technische Vorkehrungen sichergestellt werden, dass die Gesundheitsdaten vor dem Zugriff von Familienangehörigen oder Dritten sicher sind.

Im konkreten Fall habe ich den betroffenen Arzt und die medizinische Einrichtung um Auskunft gebeten und mich von den Maßnahmen des technisch-organisatorischen Datenschutzes in der medizinischen Einrichtung vor Ort überzeugt. Der Arzt nutzte in seiner Funktion als selbständiger Sachverständiger die Räumlichkeiten der medizinischen Einrichtung auf vertraglicher Grundlage; die Patientenakten wurden sowohl in Papier- als auch in elektronischer Form getrennt und zugriffssicher voneinander aufbewahrt. Die von dem Arzt im Rahmen seiner selbständigen Sachverständigentätigkeit hinzugezogene Mitarbeiterin der medizinischen Einrichtung hatte mit ihm einen Vertrag abgeschlossen. Dass sie damit praktisch einen Doppelhut aufhat, war datenschutzrechtlich nicht zu beanstanden, solange sie die Erkenntnisse, die sie aus dem einen Arbeitsverhältnis erhält, nicht für die andere Tätigkeit (oder sonst) nutzt. Man bestätigte mir zudem, dass es sich bei der von dem Petenten beanstandeten Handynummer um einen dienstlichen Anschluss handelte.

Im Ergebnis konnte ich damit zum Zeitpunkt der Kontrolle keine datenschutzrechtlichen Verstöße (mehr) feststellen.

8.4.4 Aufbewahrung von Beschwerdeschreiben in Patientenakten

Eine Petentin wandte sich an mich, weil sie vermutete, dass ein privates Krankenhaus ein Beschwerdeschreiben zu ihrer Krankenakte genommen hatte, weswegen sie Nachteile bei weiteren Behandlungen befürchtete. Auf eine entsprechende Bitte, das Schreiben zu vernichten, soll das Krankenhaus nicht reagiert haben.

Die Aufbewahrung einer ggf. auszugsweisen Kopie des Beschwerdeschreibens in der Patientenakte wäre nur unter den Voraussetzungen des § 630f Abs. 2 BGB zulässig. Danach ist der Behandelnde verpflichtet, in der Patientenakte sämtliche aus fachlicher Sicht für die derzeitige und künftige Behandlung wesentlichen Maßnahmen und deren Ergebnisse aufzuzeichnen, insbesondere die Anamnese, Diagnosen, Untersuchungen, Untersuchungsergebnisse, Befunde, Therapien und ihre Wirkungen, Eingriffe und ihre Wirkungen, Einwilligungen und Aufklärungen. Arztbriefe sind ebenfalls in die Patientenakte aufzunehmen.

Soweit diese Voraussetzungen – wovon ich aufgrund der Mitteilung des Krankenhauses ausgehen musste – nicht vorliegen, darf das Beschwerdeschreiben ausschließlich in der Verwaltungsakte, die getrennt von der Patientenakte zu führen ist, aufbewahrt werden. Ob die Aufbewahrung des Beschwerdeschreibens in der Verwaltungsakte zu Recht erfolgt, beurteilt sich in erster Linie anhand von § 28 Abs. 6 Nr. 3 BDSG. Danach ist die Speicherung zulässig, wenn dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und eine Abwägung ergibt, dass das Interesse der Patientin an einer Vernichtung des Schreibens nicht überwiegt.

Allerdings sind personenbezogene Daten, die für eigene Zwecke des Krankenhauses zulässigerweise erhoben und gespeichert wurden, zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist (§ 35 Abs. 2 Satz 2 Nr. 3 BDSG). An die Stelle der Löschung tritt die Sperrung, wenn einer Löschung gesetzliche oder vertragliche Aufbewahrungsfristen entgegenstehen (§ 35 Abs. 3 Nr. 1 BDSG) oder Grund zu der Annahme besteht, dass eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigen würde (§ 35 Abs. 3 Nr. 2 BDSG).

Das Beschwerdeschreiben sollte – wie in anderen Fällen auch – für die Dauer von drei Jahren in der Verwaltungsakte verbleiben, wobei sich das Krankenhaus an der regelmäßigen Verjährungsfrist für Ansprüche aus dem Behandlungsvertrag orientierte (§ 195 BGB). Bei der Verjährungsfrist handelt es sich jedoch nicht um eine gesetzliche Aufbewahrungsfrist im Sinne des § 35 Abs. 3 Nr. 1 BDSG. Vielmehr sind im Rahmen des § 35 Abs. 2 Nr. 3 BDSG die konkreten Umstände des Einzelfalls zu bewerten. Dabei spielt auch eine Rolle, ob konkret mit der Geltendmachung zivilrechtlicher Ansprüche durch den Patienten zu rechnen ist. Auf diese Anforderungen habe ich das Krankenhaus ausdrücklich hingewiesen. Im konkreten Fall erschienen mögliche Rechtsstreitigkeiten nicht ausgeschlossen, sodass es wohl auch im Interesse der Patientin lag, dass das Krankenhaus zumindest für eine gewisse Dauer auf das Beschwerdeschreiben zurückgreifen konnte. Da ich den Inhalt des Beschwerdeschreibens nicht kannte, war mir diesbezüglich aber keine abschließende Beurteilung möglich.

Wäre ein Beschwerdeschreiben (ausnahmsweise) nach den oben dargestellten Kriterien Teil der Patientenakte geworden, hätte das Krankenhaus es nach § 630f Abs. 3 BGB für die Dauer von zehn Jahren ab dem Ende der Behandlung aufbewahren müssen; ggf. wäre darauf aber ebenfalls ein Sperrvermerk anzubringen gewesen (§ 35 Abs. 2 Satz 2 Nr. 3, Abs. 3 Nr. 1 BDSG).

Vorliegend trafen diese Voraussetzungen jedoch nicht zu. Die Kopie des Beschwerdeschreibens wurde daher aus der Patientenakte entfernt. Das Krankenhaus nahm den Vorgang außerdem zum Anlass, die Verfahrensanweisung zum Umgang mit Beschwerden

entsprechend zu überarbeiten und zu ergänzen sowie seine Mitarbeiter diesbezüglich noch einmal zu sensibilisieren.

8.4.5 Herausgabe von Behandlungsunterlagen an Krankenkassen

Ein Krankenhaus in privater Trägerschaft gab mir folgenden Sachverhalt zur Kenntnis:

Krankenkassen wenden sich immer wieder an Krankenhäuser und weisen in diesem Zusammenhang darauf hin, dass Versicherte Unzufriedenheit mit der Behandlung, entweder in dem angeschriebenen oder aber in einem anderen Krankenhaus geäußert hätten. Es sei vom Versicherten die Vermutung einer fehlerhaften Behandlung geäußert und die Krankenkasse um Unterstützung bei der Klärung des Sachverhaltes gebeten worden. Die Einschätzung, ob tatsächlich ein Behandlungsfehler vorlag, soll dann mittels einer Begutachtung durch den Medizinischen Dienst der Krankenversicherung erfolgen. Hierzu werden die Krankenhäuser von den Krankenversicherungen gebeten, Behandlungsunterlagen über den Patienten zur Verfügung zu stellen, beispielsweise Befunde, Epikrisen, OP-Berichte, Aufklärungen. Diese Unterlagen sollen dann direkt an den zuständigen Sachbearbeiter der jeweiligen Krankenkasse übermittelt werden. Die Krankenkassen legen in der Regel eine Erklärung ihrer jeweiligen Versicherten über die Entbindung von der ärztlichen Schweigepflicht vor, die überwiegend eine konkrete Krankheit bzw. Behandlung sowie einen entsprechenden Behandlungszeitraum benennen.

Strittig ist, ob die Krankenkassen von den Krankenhäusern auf der Grundlage von § 66 SGB V tatsächlich die Herausgabe der sensiblen Informationen über das Behandlungsgeschehen ihrer Versicherten verlangen können.

Nach § 66 SGB V sollen die Krankenkassen die Versicherten bei der Verfolgung von Schadensersatzansprüchen unterstützen, die bei der Inanspruchnahme von Versicherungsleistungen aus Behandlungsfehlern entstanden sind. Voraussetzung ist dabei, dass die Schadensersatzansprüche nicht nach § 116 SGB X auf die Krankenkassen übergehen. Vorher war es in das Ermessen der Krankenkasse gestellt, ob sie die Behandlungsfehleranfragen bearbeiten oder nicht. Die unterschiedliche Handhabung hat offensichtlich den Gesetzgeber (BT-Drs. 17/10488, S. 32) veranlasst, die Ansprüche der Versicherten in diesem Punkt zu unterstreichen. Das heißt, sie sind nun grundsätzlich zur Unterstützung verpflichtet, es sei denn, es sprechen besondere Gründe dagegen.

Wie die Unterstützungsleistung genau aussehen muss, ist im Gesetz nicht geregelt. Allerdings wird in der Gesetzesbegründung wie auch in der Kommentarliteratur ausdrücklich erwähnt, dass dies etwa durch Unterstützungsleistungen, mit denen die Beweisführung der Versicherten erleichtert wird, geschehen kann.

Im Hinblick auf diese Unterstützungsobliegenheit der Krankenkasse normiert § 284 Abs. 1 Nr. 5 SGB V ausdrücklich eine entsprechende Datenerhebungsbefugnis der Krankenkasse. So ist die Krankenkasse nicht gehalten, nur mit Beweismitteln zu unterstützen, die ihr – bereits – bekannt sind und sich in ihren Akten befinden. So führt auch das Hessische LSG in seinem Urteil vom 4. Mai 2015 (L 1 KR 381/13, juris) ausdrücklich aus:

„*Unterstützungsleistungen beschränken sich demnach regelmäßig auf die Verschaffung von Auskünften über die vom Arzt gestellten Diagnosen, die angewandte Therapie, die Namen der Behandler, die Anforderung ärztlicher Unterlagen einschließlich Röntgenaufnahmen etc. von der Behandlung und die Begutachtung durch den Medizinischen Dienst der Krankenversicherung nach § 275 Abs. 3 Nr. 4 SGB V. ... Dem hat die Krankenkasse vorliegend entsprochen und den Sozialmedizinischen Dienst ein Gutachten nach Beiziehung der relevanten medizinischen Unterlagen erstellen lassen und im Anschluss daran dem Kläger alle Unterlagen zur Verfügung gestellt.*“

Im Ergebnis halte ich daher die Krankenkasse für berechtigt, in Fällen des § 66 SGB V selbst Unterlagen beim betreffenden Behandler – hier dem Krankenhaus – abzufragen.

8.4.6 Nutzung externer Abrechnungsstellen durch Ergotherapeuten

Darf ein Ergotherapeut ein externes Abrechnungszentrum in Anspruch nehmen, ohne die Einwilligung des Patienten einzuholen? Diese Frage stellte mir ein gesetzlich krankenversicherter Petent, nachdem er eine Rechnung über noch ausstehende Zuzahlungen (§ 61 SGB V) von einem Abrechnungszentrum erhalten hatte. Ich habe zu dieser Frage wie folgt Stellung genommen:

Die Weitergabe von Patientendaten gesetzlich Versicherter an Abrechnungsstellen ist aufgrund einer Entscheidung des Bundessozialgerichts seinerzeit groß thematisiert worden. Das Bundessozialgericht hatte mit Urteil vom 10. Dezember 2008 (B 6 KA 37/07 R, juris) festgestellt, dass die Weitergabe von Patientendaten der im Krankenhaus behandelten gesetzlich krankenversicherten Patienten an private Dienstleistungsunternehmen nach den derzeitigen Bestimmungen selbst dann nicht zulässig ist, wenn der Patient zuvor eine schriftliche Einwilligungserklärung unterzeichnet hat.

Wie das Bundessozialgericht in seinen Entscheidungsgründen ausführt, existieren nur sehr wenige gesetzlich geregelte Fälle, in denen die Zwischenschaltung Dritter in den Abrechnungsweg ausnahmsweise zugelassen ist:

- für Apotheken gemäß § 300 Abs. 2 SGB V;
- für Leistungserbringer im Bereich der Heil- und Hilfsmittel und sonstige Leistungserbringer gemäß § 302 Abs. 2 Satz 2 ff. SGB V.

Zu den sonstigen Leistungserbringern zählen auch Ergotherapeuten (Michels in: Becker/ Kingreen, Kommentar zum SGB V, 2008, Rdnr. 1 zu § 302). Dies gilt meiner Auffassung nach auch für die Abrechnung gesetzlich normierter Zuzahlungen.

Zur Abrechnung gegenüber den Kostenträgern dürfen entsprechende Leistungserbringer daher auch Rechenzentren in Anspruch nehmen. Da dies gesetzlich ausdrücklich normiert ist, bedarf es für die Zulässigkeit der Übermittlung nicht zusätzlich noch einer Einwilligung der Patienten.

Die Regelung des § 302 Abs. 2 Satz 2 SGB V sieht keine Pflicht vor, den gesetzlich Versicherten über die Tatsache, dass sein Ergotherapeut ein privates Rechenzentrum eingeschaltet hat, zu unterrichten.

Die Regelung des SGB V bezieht sich allerdings ausschließlich auf die Abrechnung in der GKV. Sollten in einer Praxis auch Privatpatienten behandelt werden und auch diese Abrechnungen durch ein privates Rechenzentrum abrechnen lassen, kann dies nicht auf § 302 SGB V gestützt werden. In diesen Fällen ist insoweit eine – informierte – Einwilligung des betreffenden Privatpatienten notwendig. Ich stütze diese auf § 28 Abs. 6 BDSG. In diesem Fall muss der betreffende Privatpatient bei Einholung der schriftlichen Einwilligung (§ 4a Abs. 1 Satz 3 sowie Abs. 3 BDSG) auch darüber aufgeklärt werden, dass sein Leistungserbringer über ein privates Rechenzentrum abrechnet und um welches Rechenzentrum es sich handelt.

8.4.7 Bestellbestätigungen durch Versandapotheken

In einer Eingabe zum Versand von Bestellbestätigungen per E-Mail durch eine Versandapotheke ging es um die Problematik, dass in der Bestellbestätigung die Bestellung insgesamt noch einmal wiederholt und auf diese Weise besondere Arten personenbezogener Daten (Gesundheitsdaten gemäß § 3 Abs. 9 BDSG) unverschlüsselt über das Internet übertragen werden.

Es ist allgemein bekannt, dass der unverschlüsselte Versand von E-Mails vergleichbar mit dem Versand einer Postkarte ist. Alle an der Datenübertragung beteiligten Stellen können problemlos mitlesen, wann konkrete Kunden welche Bestellungen ausgelöst haben und dadurch auch Rückschlüsse auf deren Gesundheitszustand ziehen. Während der Inhaber der betreffenden Versandapotheke die Registrierung neuer Kunden und auch den eigentlichen Bestellprozess offensichtlich über eine SSL-Verschlüsselung seines Webshops ausreichend abgesichert hatte, konterkarierte er diese Maßnahmen anschließend selbst, indem er die Bestellbestätigungen völlig ungesichert über das Internet versandte. Dies stand im Widerspruch zu den Vorgaben der Nr. 4 der Anlage zu § 9 BDSG,

wonach zu gewährleisten ist, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Letztendlich stand damit sogar eine Verletzung der Schweigepflicht nach § 203 StGB im Raum. Auch § 13 Abs. 4 Nr. 3 TMG gibt einem Dienstanbieter technische und organisatorische Vorkehrungen auf, damit seine Kunden die angebotenen Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen können. Es nutzt Kunden wenig, wenn zwar der Bestellprozess verschlüsselt abgewickelt wird, wenig später aber der Inhalt der Bestellung vollkommen ungeschützt über das Internet übertragen und damit die vorgenommenen Bestellungen Dritten wieder zugänglich gemacht werden. In der Konsequenz bedeutet dies, dass unverschlüsselte E-Mails jedenfalls dann (vgl. § 9 Satz 2 BDSG) nicht als Kommunikationsmittel zwischen Apotheke und Kunde verwendet werden dürfen, wenn die Nachrichten (auch) besondere Arten personenbezogener Daten enthalten.

Eine mögliche Lösung besteht darin, dass den Kunden in den Bestätigungsmails nur noch ein Link auf Ihre Bestellung mitgeteilt und dass ein Zugriff auf die Bestelldaten über diesen Link nur über eine verschlüsselte Verbindung unter vorheriger Abfrage der Login-Daten, insbesondere eines Passwortes, möglich ist.

8.4.8 Neuer bundeseinheitlicher Blut- und Plasmaspenderfragebogen

Mich erreichten Eingaben zur datenschutzrechtlichen Zulässigkeit des neuen einheitlichen Blut- und Plasmaspenderfragebogens (Anlage 2). Die Kritik betraf dabei in erster Linie die Frage 16, die wie folgt lautet:

Einheitlicher Blut- und Plasmaspenderfragebogen (Version 2) – Stand 13.01.2015

16.	Über den Sexualverkehr können Infektionen, wie z.B. HIV oder Hepatitis, übertragen werden. Direkt nach der Ansteckung mit HIV und/oder Hepatitis kann ein Spender ohne es zu wissen infiziert sein und durch sein Blut den Empfänger der Spende anstecken. Leider können Labortests eine Infektion zum Teil erst bis zu 4 Monate nach der Ansteckung nachweisen. Daher schützen Sie mit Ihrer ehrlichen Antwort die Empfänger Ihrer Spende.		
	Hatten Sie in den letzten 4 Monaten Sexualverkehr • mit einer neuen Partnerin / einem neuen Partner? • mit einer Person, die eine schwere Infektionskrankheit (z.B. AIDS oder Hepatitis) hat oder haben könnte? • für den Sie Geld oder andere Leistungen (Unterkunft, Drogen) bezahlt haben? • **Nur für Frauen:** mit einem bisexuellen Mann?	□ ja	□ nein
	• Haben Sie schon einmal Geld oder andere Leistungen für Sexualverkehr erhalten? • **Nur für Männer**: Hatten Sie schon einmal Sexualverkehr mit einem anderen Mann?	□ ja	□ nein

Die rechtliche Grundlage für diese Datenerhebung und Datenspeicherung findet sich in § 11 TFG, wonach jede Spendeentnahme und die damit verbundenen Maßnahmen für die im Transfusionsgesetz geregelten Zwecke, für Zwecke der ärztlichen Behandlung der spendenden Person und für Zwecke der Risikoerfassung nach dem Arzneimittelgesetz zu protokollieren sind (Absatz 1), weshalb die Spendeeinrichtungen auch die dafür relevanten personenbezogenen Daten der Spender erheben, verarbeiten und nutzen dürfen (Absatz 2).

Gemäß § 5 Abs. 1 TFG dürfen nur Personen zur Spendeentnahme zugelassen werden, die unter der Verantwortung einer ärztlichen Person nach dem Stand der medizinischen Wissenschaft und Technik für tauglich befunden worden sind und die Tauglichkeit durch eine ärztliche Person festgestellt worden ist. Die Zulassung zur Spendeentnahme soll nicht erfolgen, soweit und solange die spendewillige Person nach Richtlinien der Bundesärztekammer von der Spendeentnahme auszuschließen oder zurückzustellen ist. Das Transfusionsgesetz sieht in § 12a Abs. 1 i. V. m. § 12 Abs. 1 Nr. 2 vor, dass die Bundesärztekammer im Einvernehmen mit der zuständigen Bundesoberbehörde, dem Paul-Ehrlich-Institut, und nach Anhörung von Sachverständigen unter Berücksichtigung der Empfehlungen der europäischen Union, des Europarates und der Weltgesundheitsorganisation zu Blut und Blutbestandteilen in Richtlinien den allgemein anerkannten Stand der medizinischen Wissenschaft und Technik insbesondere für die Auswahl der spendenden Personen und die Durchführung der Auswahl erlässt. Auf Grundlage dieser Ermächtigung wurde die sogenannte Hämotherapie-Richtlinie vom 4. Mai 2010 erlassen, aus der sich damit ergibt, welche Fragen durch die Spendeeinrichtungen zulässigerweise gestellt werden dürfen und müssen.

In der Hämotherapie-Richtlinie steht unter Ziffer 2.2, dass vor jeder Spende zu prüfen ist, ob ein Ausschlusskriterium vorliegt. Hierzu heißt es unter Ziffer 2.2.1 – Kriterium für einen Dauerausschluss:

„Personen, deren Sexualverhalten ein gegenüber der Allgemeinbevölkerung deutlich erhöhtes Übertragungsrisiko für durch Blut übertragbare schwere Infektionskrankheiten, wie HBV, HCV oder HIV bergen:

heterosexuelle Personen mit sexuellem Risikoverhalten, z. B. Geschlechtsverkehr mit häufig wechselnden Partnern,

Männer, die Sexualverkehr mit Männern haben (MSM),

männliche und weibliche Prostituierte.“

Ziffer 2.2.2 bestimmt zeitlich begrenzte Rückstellungskriterien, u. a. nach Ziffer 2.2.2.2 – Exposition mit dem Risiko, eine übertragbare Infektion zu erwerben:

„nach intimem Kontakt mit Personen, die einer Gruppe mit erhöhtem Infektionsrisiko für HBV, HCV und/oder HIV angehören (s. oben) für 4 Monate,“

Die als zu weitgehend empfundenen Fragen unter Ziffer 16 des neuen einheitlichen Blut- und Plasmaspenderfragebogens sind vor diesem Hintergrund datenschutzrechtlich nicht zu beanstanden, da sie einzig der transfusionsmedizinischen und arzneimittelrechtlichen

Risikoerfassung und Risikobewertung dienen und damit auf gesetzlicher Grundlage erfolgen.

Der Blutspende-Ausschluss von Personen, deren Sexualverhalten ein deutlich erhöhtes Risiko für die Übertragung schwerer Infektionskrankheiten durch gespendetes Blut birgt, ist ein langjähriger Grundsatz in der Hämotherapie-Richtlinie. Allerdings wurden die bisherigen Fragen von der Personengruppe der homosexuellen Männer als Diskriminierung empfunden, zudem gab es fachliche Kritik an der Art und Weise, wie bislang gefragt wurde. Im Zuge der vom Arbeitskreis Blut im Juni 2010 beschlossenen Einführung eines bundeseinheitlichen Blutspenderfragebogens, der ein Höchstmaß an Sicherheit gewährleisten soll, wurden daher auch diese Fragestellungen überarbeitet und dabei versucht, mit Ziffer 16 eine möglichst neutrale Fragestellung zu finden. Die Einschätzung der medizinischen Expertengruppe, dass mit der neu gewählten Formulierung potentielle transfusionsrelevante Risiken, die mit jedem neuen Sexualpartner des Spenders für diejenigen verbunden sind, die Spenderblut benötigen, sicherer als bislang erfasst werden können, ist dabei durch mich aufgrund meiner auf den Datenschutz beschränkten Zuständigkeit nicht zu hinterfragen.

8.4.9 Verarbeitung von Daten von der Blutspende ausgeschlossener oder zeitweilig zurückgestellter Spender

Ein Petent entschloss sich aufgrund von Informationen im Internet zu einer Blutspende, wobei er davon ausging, dass er als Spender in Betracht kommt. Nachdem er den Spenderfragebogen ausgefüllt, die Einverständniserklärung zur Datenerhebung und -verarbeitung unterzeichnet sowie die Voruntersuchung (Messung von Blutdruck und Hämoglobinwert) absolviert hatte, wurde er zur ärztlichen Untersuchung gebeten. Dort teilte man ihm mit, dass er aufgrund einer mehr als ein Jahr zurückliegenden Krebsbehandlung nicht zur Blutspende zugelassen wird. Der abgelehnte Spender forderte daraufhin von der Blutspendeeinrichtung, dass sie seine personenbezogenen Daten vollständig löscht. Da sich die Blutspendeeinrichtung weigerte, bat mich der Petent um Hilfe. Er fühlte sich kriminalisiert und fürchtete einem ständigen Datenabgleich zu unterliegen, obwohl es nicht zu einer Spende gekommen war.

§ 11 Abs. 1 Satz 1 TFG bestimmt, dass jede Spendeentnahme und die damit verbundenen Maßnahmen nicht nur für die im Transfusionsgesetz enthaltenen Zwecke (1. Alt.) und zum Zweck der ärztlichen Behandlung der spendenden Person (2. Alt.), sondern auch für Zwecke der Risikoerfassung nach dem Arzneimittelgesetz (3. Alt.) zu protokollieren sind. Insofern hat die Blutspendeeinrichtung bei Arzneimitteln, die bei Menschen angewendet werden, ein sogenanntes Pharmakonvigilanz-System einzurichten, das es ihr ermöglicht,

Risiken zu erkennen, zu vermeiden und zu minimieren (§ 63b Abs. 1 und Abs. 2 Nr. 1 AMG). Bei Blutzubereitungen handelt es sich dabei um Arzneimittel (§ 4 Abs. 2 AMG).

Im Rahmen dieser Risikovermeidung bzw. Risikovorsorge nach dem Arzneimittelgesetz, auf die § 11 Abs. 1 TFG ausdrücklich Bezug nimmt, spielen bei Blutzubereitungen die Kriterien, nach denen Spendewillige von der Spende auszuschließen sind, eine entscheidende Rolle. Die Ausschluss- oder Zurückstellungskriterien sind in der Hämotherapie-Richtlinie der Bundesärztekammer geregelt (§ 5 Abs. 1 Satz 2 i. V. m. §§ 12a Abs. 1, 12 Abs. 1 Nr. 2 TFG). Gesetzlicher Zweck dieser Vorschriften ist es sicherzustellen, dass nur zur Blutspende taugliche Spender ausgewählt und zugelassen werden. Der Spendedienst ist gesetzlich verpflichtet, vor der Spende zu prüfen, ob entsprechende dauerhafte oder zeitweilige Ausschlussgründe bei dem Spendewilligen vorliegen (§ 5 Abs. 1 Satz 1 TFG).

Bei einem Spendewilligen, der sich erstmals zu einer Spende entschließt, müssen die entsprechenden Gesundheitsdaten zunächst erhoben und gespeichert werden. Bei weiteren Spendeversuchen kann der Blutspendedienst auf die auch zu diesem Zweck bereits gespeicherten Daten des Spendewilligen zurückgreifen. Dies ist in § 11 Abs. 2 Satz 1 TFG ausdrücklich vorgesehen: Spendeeinrichtungen dürfen personenbezogene Daten der spendewilligen und spendenden Personen erheben, verarbeiten und nutzen, soweit das für die in Absatz 1 genannten Zwecke erforderlich ist. Genutzt („abgerufen“) werden die Daten, wenn sich der dauerhaft oder zeitweilig ausgeschlossene Spendewillige erneut zu einer Spende meldet. Sollte der Spendewillige dagegen von weiteren Spendeversuchen absehen, werden seine Daten lediglich für die gesetzlich vorgesehene Dauer gespeichert und unterliegen damit keinem ständigen Datenabgleich.

Im Falle eines abgelehnten Erstspenders, bei dem es tatsächlich nicht zu einer Spende gekommen ist, beträgt die Speicherdauer dabei regelmäßig 15 Jahre bzw. im Falle der §§ 8 und 9 Abs. 1 TFG regelmäßig 20 Jahre (§ 11 Abs. 1 Satz 2 TFG).

8.4.10 Gesundheitliche Fragebogenaktion eines Verbands

Mich erreichte die Anfrage eines Sportlers, dessen Übungsleiter im Auftrag eines Landesverbands eine Fragebogenaktion zum Thema Gesundheit durchführte. Den Sportlern wurde dabei eine Information ausgehändigt, in der besonders darauf hingewiesen wurde, dass die Anonymität der Befragung gewahrt werde. Der Sportler wunderte sich über diese Aussage, denn der Übungsleiter führte eine Liste, in der jedem Sportler eine Nummer zugewiesen wurde, die auch auf den Fragebögen vermerkt wurde. Der Sportler befürchtete nicht zu Unrecht, dass nicht nur die ausgefüllten Fragebögen, sondern eines Tages

auch die Listen an den Landesverband gelangen und so seine Anonymität gerade nicht gewahrt wird.

Zunächst hatte der Sportler Recht: Die Datenerhebung, Datenverarbeitung und Datennutzung durch den Landesverband erfolgte nicht anonym, sondern lediglich in pseudonymer Form: Weil die Übungsleiter eine Liste mit den Nummern der Fragebögen und den dazu gehörenden Namen der Sportler führten, war eine Zuordnung der im Rahmen der Fragebogenaktion erhobenen personenbezogenen Gesundheitsdaten zu einzelnen Sportlern und damit deren Reidentifizierung unter bestimmten Voraussetzungen auch durch den Verband möglich (§ 3 Abs. 6a BDSG).

Im Ergebnis meiner Prüfung musste ich feststellen, dass die Fragebogenaktion insgesamt datenschutzwidrig war. Ich wies den Landesverband darauf hin, dass gemäß § 4 Abs. 1 BDSG die Erhebung, Verarbeitung und Nutzung personenbezogener Daten (wozu auch pseudonyme Daten gehören) nur zulässig sind, soweit dies durch Gesetz erlaubt wird oder der Betroffene wirksam im Sinne des § 4a Abs. 1 BDSG eingewilligt hat. § 28 Abs. 6 BDSG betont dabei für Gesundheitsdaten den unbedingten Vorrang der Einwilligung der Betroffenen, indem er auf das Einwilligungserfordernis des § 4a Abs. 3 BDSG verweist.

Eine gesetzliche Ausnahme, d. h. eine Datenerhebung, Datenverarbeitung und Datennutzung ohne wirksame Einwilligung war nicht ersichtlich. Insbesondere konnte sich der Verband hinsichtlich der Erhebung, Verarbeitung und Nutzung pseudonymer Gesundheitsdaten nicht auf § 28 Abs. 6 Nr. 4 BDSG berufen, wonach die Erhebung, Verarbeitung und Nutzung von Gesundheitsdaten zulässig ist, wenn sie zur Durchführung der wissenschaftlichen Forschung erforderlich ist. Der Landesverband war keine Forschungseinrichtung; für Drittforschung wäre § 28 Abs. 6 Nr. 4 BDSG nicht einschlägig gewesen.

Der Verband, ein eingetragener Verein, vertrat insofern die Auffassung, dass die Übungsleiter Mitglieder des Verbands sind und daraus per se die datenschutzrechtliche Zulässigkeit ihrer Einbindung in die Fragebogenaktion folge. Dem widersprach ich. Denn dem Verein als verantwortliche Stelle im Sinne des § 3 Abs. 7 BDSG zugerechnet werden lediglich der Vorstand, unselbständige Untergliederungen und angestellte Mitglieder sowie Auftragsdatenverarbeiter. Nur insofern handelt es sich um eine Nutzung der Gesundheitsdaten innerhalb der verantwortlichen Stelle (§ 3 Abs. 8 Satz 3 BDSG). Selbständige Organisationen des Vereins und alle Mitglieder, die keine Funktionsträger, Auftragsdatenverarbeiter oder Angestellte sind, sind hingegen im Verhältnis zum Verein datenschutzrechtlich Dritte (§ 3 Abs. 8 Satz 2 BDSG). Jegliche Datenerhebung und Datenverarbeitung (wozu auch die Datenübermittlung zählt) durch oder an diese Dritten müssen deshalb nach § 28 BDSG zulässig sein, wenn sie nicht auf eine wirksame Einwilligung gestützt werden können.

Eine wirksame Einwilligung der Sportler lag jedoch nicht vor. Gemäß § 4a Abs. 1 BDSG ist die Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Der Betroffene ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung hinzuweisen. Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen (§ 4a Abs. 3 BDSG). Die Einwilligung in die Erhebung, Verarbeitung und Verwendung von Gesundheitsdaten muss folglich freiwillig und informiert sein. Anderenfalls ist sie unwirksam. Empfehlenswert ist es, Hinweise auf das Auskunftsrecht und zu Aufbewahrungs- bzw. Löschungsfristen zu geben. Zweckmäßig ist auch der Hinweis darauf, dass die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen werden kann. Die Einwilligung muss zudem gemäß § 4a Abs. 1 Satz 3 BDSG in Schriftform vorliegen. Schriftform bedeutet, dass die Betroffenen die Einwilligungen unterschreiben müssen (§ 126 Abs. 1 BGB).

Im Hinblick auf die Fragebogenaktion bedeutet das Folgendes:

Die betroffenen Sportler hätten unterrichtet werden müssen, dass sie nicht verpflichtet sind, an der Fragebogenaktion teilzunehmen und ihre Gesundheitsdaten preiszugeben. Sie hätten in geeigneter Weise über die Bedeutung und Konsequenzen der Einwilligung aufgeklärt werden müssen, was nicht der Fall war. Dazu hätte insbesondere gehört, dass die Sportler über die Daten besitzende/n und verarbeitende/n Stelle/n (hier: Übungsleiter, der Verband, ggf. weitere Dritte) und den oder die genauen Verwendungszweck/e der Daten ausführlich und aussagekräftig informiert werden. Die Sportler hätten des Weiteren darauf hingewiesen werden müssen, in welchem Umfang (Inhalt der Datensätze, Datenkategorien, schutzwürdige Daten im Sinne des § 3 Abs. 9 BDSG) und in welcher Weise (z. B. in pseudonymisierter oder anonymisierter Form) ihre Daten für welche Dauer gespeichert werden sowie wer in welchem Umfang Zugriff auf die Daten haben soll. Die Sportler hätten insofern darüber informiert werden müssen, ob und durch wen in wessen Auftrag die Daten aus den Fragebögen elektronisch weiterverarbeitet werden und was nach Übertrag der Daten aus den Fragebögen mit den Fragebögen passiert (Vernichtung, weitere Aufbewahrung). Sofern die Daten (etwa im Rahmen der Evaluierung) an Dritte übermittelt werden, müssen die Sportler wissen, an wen die Übermittlung zu welchem Zweck und in welcher Form erfolgen soll. Es muss für sie auch klar ersichtlich sein, wann ihre Reidentifizierung durch wen erfolgen kann und soll.

Die Information genügte diesen Anforderungen nicht; sie war fehler- und lückenhaft, so dass ich die Einwilligungen als unwirksam beurteilte.

Darüber hinaus musste ich feststellen, dass der Verband mit den Übungsleitern keinen schriftlichen Auftragsdatenverarbeitungsvertrag geschlossen hatte. Der Verband ließ

durch die Übungsleiter, die keine Beschäftigten des Verbands waren, personenbezogene Gesundheitsdaten, wenn auch pseudonymisiert, erheben und speichern. Die Übungsleiter taten dies dabei nicht im eigenen Interesse und für eigene Zwecke, sondern für den Verband im Auftrag, so dass sie als Auftragsdatenverarbeiter anzusehen waren (§§ 3 Abs. 8 Sätze 2 und 3, 11 Abs. 1 BDSG).

Der Verband war deshalb als Auftraggeber gemäß § 11 Abs. 2 BDSG verpflichtet, mit den Übungsleitern schriftlich einen Vertrag abzuschließen, der die Vorgaben des § 11 Abs. 2 BDSG erfüllt. In dem Vertrag hätte bezogen auf die Fragebogenaktion insbesondere geregelt werden müssen, wie die Übungsleiter mit den Listen, den Einwilligungen und den Fragebögen umzugehen haben, wo diese aufzubewahren sind und wer darauf zugreifen darf (ggf. unter welchen Voraussetzungen) und in welchen Fällen eine Reidentifizierung der Sportler durch wen erfolgen darf. Die bloße Verpflichtung der Übungsleiter auf das Datengeheimnis erfüllt die Voraussetzungen des § 11 Abs. 2 BDSG nicht.

Letztlich erfordert eine Fragebogenaktion, zumal wenn Gesundheitsdaten betroffen sind, ein schriftliches Datenschutzkonzept, das die Zwecke der Datenerhebung, -verarbeitung und -nutzung, die Datenflüsse und die Rolle der an der Fragebogenaktion Beteiligten konkret definiert, insbesondere im Einzelnen Maßnahmen des technisch-organisatorischen Datenschutzes (§ 9 BDSG) vorsieht und dessen Umsetzung in der Praxis gewährleistet ist. Anderenfalls ist die Erhebung und Verarbeitung der personenbezogenen Gesundheitsdaten der Teilnehmer auch im Falle wirksamer Einwilligungen datenschutzrechtlich unzulässig.

Nachdem ich dem Verband zum beabsichtigten Erlass einer aufsichtsbehördlichen Anordnung anhörte, stoppte dieser die Fragebogenaktion und sorgte für die datenschutzgerechte Vernichtung der Fragebögen und der bei den Übungsleitern aufbewahrten Zuordnungslisten.

8.5 Handel, Gewerbe, Dienstleistungen

8.5.1 Auskunftspflicht gegenüber OWi-Behörden oder polizeilichen Ermittlungsbeamten

Mich erreichte eine Anfrage, ob eine private Stelle in einem Bußgeldverfahren gegenüber der Verwaltungsbehörde als Bußgeldstelle zur Auskunft verpflichtet ist (vgl. dazu auch Pkt. 13.2).

Geschäftsführer oder namentlich bekannte Mitarbeiter privater Unternehmen sind als Zeugen verpflichtet, gegenüber der Ordnungswidrigkeitenbehörde Angaben zu machen.

Diese Zeugnispflicht ist im Bußgeldverfahren auch zwangsweise durchsetzbar (§ 161a Abs. 1 Satz 1 und Abs. 2 StPO i. V. m. § 46 Abs. 1 und 2 OWiG): Weigert sich ein Zeuge zu erscheinen oder auszusagen, ohne hierzu berechtigt zu sein, kann die Ordnungswidrigkeitenbehörde gegen diesen ein Ordnungsgeld verhängen (§§ 51 bzw. 70 i. V. m. 161a Abs. 2 StPO, 46 Abs. 1 und 2 OWiG). Die Ordnungswidrigkeitenbehörde hat im Bußgeldverfahren die Rechte und Pflichten der Staatsanwaltschaft (§ 46 Abs. 2 OWiG), d. h. sie kann selbst ermitteln (Zeugen vernehmen) oder die Polizeibehörden als Ermittlungsbeamte damit beauftragen.

Anders zu beurteilen ist die Rechtslage, wenn es um Auskunftsverlangen von Polizeibeamten in anhängigen Bußgeld- bzw. staatsanwaltlichen Ermittlungsverfahren geht. Eine Auskunftspflicht bestand insofern bislang nicht. Nach Inkrafttreten des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens zum 21. August 2017 (BGBl. I S. 3202) sind Zeugen nun jedoch verpflichtet, einer Vorladung der Polizei Folge zu leisten und (vorbehaltlich etwaiger Zeugnis- oder Auskunftsverweigerungsrechte) auszusagen, wenn dem ein Auftrag der Staatsanwaltschaft (§ 163 Abs. 3 Satz 1 StPO n. F.) bzw. der Ordnungswidrigkeitenbehörde (§ 46 Abs. 1 und Abs. 2 OWiG) zugrunde liegt.

Auch wenn es (noch) keinen Vernehmungsauftrag der Staatsanwaltschaft gibt, bedeutet dies nicht, dass die privaten Unternehmen der Polizei keine Auskunft erteilen dürften. Das Recht zur Auskunftserteilung bestimmt sich vielmehr anhand der Bestimmung des § 28 Abs. 2 BDSG. Danach ist die Übermittlung von Daten für einen anderen Zweck (hier: Strafverfolgung bzw. Verfolgung von Ordnungswidrigkeiten durch die Polizei) zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle (Nr. 1) oder berechtigter Interessen eines Dritten oder zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten (Nr. 2) erforderlich ist und jeweils kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat.

Letztlich muss die verantwortliche Stelle eine umfassende Abwägung vornehmen. Insofern verbietet es sich in der Regel, „auf Zuruf“ am Telefon z. B. Kundendaten an die Polizei herauszugeben. Die Anforderung sollte schriftlich erfolgen und wenigstens das Aktenzeichen des polizeilichen/staatsanwaltschaftlichen Vorgangs enthalten sowie Auskunft darüber geben, ob es sich um ein Ermittlungsverfahren oder einen Vorgang zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit handelt. Die private Stelle muss in der Lage sein, ihren Auskunfts- und Dokumentationspflichten nachkommen zu können.

Andererseits hat die private Stelle keinen umfassenden Anspruch auf Erläuterung, warum die Polizeibeamten die Auskunft benötigen, etwa dazu, ob der Kunde, dessen Daten angefordert werden, Zeuge oder Beschuldigter ist. Denn insoweit hat der Kunde auch ein schützenswertes Interesse daran, dass die Polizei diese Tatsache seinem Vertragspartner nicht offenbart.

8.5.2 Aushang von Werksverboten

Von einem Hinweisgeber, der wiederholt beruflich in einem sächsischen Industriebetrieb tätig gewesen war, hatte ich die Information erhalten, dass sich dort am Werkseingang für alle einsehbare DIN-A4-Aushänge mit Haus- bzw. Werksverboten befänden. In den Aushängen seien Personen mit Vorname, Name, Firma und Personalausweisnummer benannt.

Im Rahmen eines Kontrollbesuches konnte ich mich von der Richtigkeit dieser Mitteilung überzeugen. Zum Kontrollzeitpunkt war jedenfalls ein vom Niederlassungsleiter sowie der Logistikleiterin unterzeichnetes Hausverbot am Werkseingang (Pförtnerhäuschen) so ausgehangen, dass jeder, der diesen Bereich passierte, dieses Hausverbot zur Kenntnis nehmen konnte. Nach den Ausführungen der Unternehmensvertreter handelte es sich dabei um eine ständige Praxis in dieser Niederlassung, d. h. soweit entsprechende Hausverbote ausgesprochen werden, würden diese auch regelmäßig zum Aushang gebracht. Im Allgemeinen handele es sich dabei um Mitarbeiter von Speditionen, die sich trotz Belehrung und Einweisung innerhalb des Betriebsgeländes (wiederholt) nicht regelkonform verhalten hätten.

Der Aushang ausgesprochener Hausverbote stellte einen Verstoß gegen § 28 Abs. 1 Satz 1 Nr. 2 BDSG dar und war damit unzulässig (vgl. auch 7/8.5.5).

Mit dem Aushang eines Hausverbots werden Daten zur Person des Betroffenen den Mitarbeitern, Besuchern, Lieferanten sowie sonstigen Geschäftspartnern bekanntgegeben und somit im datenschutzrechtlichen Sinne an einen unbestimmten Personenkreis übermittelt. Nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist dies nur dann zulässig, wenn es zur Wahrung berechtigter Interessen erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Veröffentlichung überwiegt. Diese Voraussetzungen waren vorliegend nicht erfüllt.

Zur Durchsetzung des Hausrechts genügt es, wenn lediglich der Betroffene persönlich (bzw. über seine Spedition als seinem Arbeitgeber) über das Hausverbot informiert wird und im Übrigen darüber hinaus noch die Mitarbeiter des Einlasskontrolldienstes davon in Kenntnis gesetzt werden. Die Information weiterer Personen, die weder an der Einlasskontrolle beteiligt noch überhaupt zur Durchsetzung des Hausrechts befugt oder zu der in

diesem Zusammenhang erforderlichen Identifikation Dritter berufen sind, war dazu nicht erforderlich, mithin also auch der Aushang des Hausverbots unzulässig. Wegen der mit dem Aushang des Hausverbots zudem verbundenen Prangerwirkung und des großen Empfängerkreises ohne jegliches berechtigte Informationsinteresse war darüber hinaus auch von überwiegenden schutzwürdigen Interessen des Betroffenen auszugehen.

Die vorstehende Bewertung bezieht sich ausschließlich auf den Aushang des Hausverbots. Ob Hausverbote berechtigterweise ausgesprochen werden, habe ich nicht zu beurteilen.

Die Vertreter des Unternehmens sind meiner Argumentation gefolgt und haben den betreffenden Aushang noch während meines Kontrollbesuches abgenommen. Ich habe die Zusage erhalten, dass zukünftig keine Hausverbote mehr zum Aushang gebracht werden, stattdessen werde man die diesbezüglichen Informationen ausschließlich dem Einlasskontrolldienst zukommen lassen.

8.5.3 Personalausweisfotografien durch Sicherheitsdienst

Im Treppenhaus und im Aufzug eines Einkaufszentrums waren mit einem Edding-Stift vorgenommene Schmierereien festgestellt worden. Der dort tätige Sicherheitsdienst hatte daraufhin einige Tage später eine Jugendliche in der Erwartung angesprochen, diese könne Hinweise zum Täter geben. Diese Erwartung entsprang der Auswertung der Aufzeichnungen einer vor dem Aufzug befindlichen Überwachungskamera, die – zwar ohne Tatbezug – auf eine Gruppe von Jugendlichen als Tätergruppe hindeutete, zu der auch diese Jugendliche gehört hatte. Die Betroffene gab wohl an, den Täter zu kennen und zur Selbstbezichtigung bewegen zu können und durfte daraufhin das Haus wieder verlassen. Am Tag danach hat die Jugendliche dann gemeinsam mit ihren Freunden den Täter auch wirklich zum Sicherheitsdienst gebracht. Die Mitarbeiter des Sicherheitsdienstes hätten daraufhin mitgeteilt, dass sich die Angelegenheit für sie und ihre Freunde damit erledigt habe, sie die Angelegenheit jedoch der Polizei übergeben würden. Zu diesem Zweck fotografierte einer der Mitarbeiter die Personalausweise der Jugendlichen noch mit dem Handy ab. Der Vater der Jugendlichen wandte sich daraufhin an mich, um die Rechtmäßigkeit dieses Vorgehens zu prüfen.

Nachdem ich – wohl wegen eines Personalwechsels beim Sicherheitsdienst – einige Mühe hatte, den betreffenden Sicherheitsdienst zu kontaktieren und eine Stellungnahme zu erhalten, räumte der (inzwischen neue) Leiter des Sicherheitsdienstes mir gegenüber dann ein diesbezügliches Fehlverhalten der damaligen Mitarbeiter ein. Statt die Personalausweise abzufotografieren und auf diese Weise eine Vielzahl nicht benötigter Daten zu erfassen, hätten diese die zur Identitätsfeststellung notwendigen Angaben – und nur

diese – schriftlich erfassen können und müssen. Die grundsätzliche Befugnis für die diesbezügliche Datenerhebung habe ich wegen der den Jugendlichen zukommenden Zeugenfunktion nicht in Frage gestellt (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG).

Der Leiter des Sicherheitsdienstes hat mir zugesichert, dass er dafür Sorge tragen werde, dass sich derartige Vorfälle unter seiner Verantwortung nicht wiederholen. Die Fotoaufnahmen der Personaldokumente seien bereits vernichtet worden; die beiden für den Vorgang verantwortlichen Mitarbeiter hätten das Unternehmen inzwischen wieder verlassen.

8.5.4 Schufa-Abfrage für private Zwecke

Eine von einer Inkasso- und Ermittlungsgesellschaft über sie eingeholte Schufa-Auskunft hatte eine Betroffene veranlasst, sich an mich zu wenden. Dabei stellte sich zunächst heraus, dass die Schufa-Auskunft von der Inkasso- und Ermittlungsgesellschaft nicht im eigenen Namen, sondern im Auftrag einer anderen Firma gestellt worden war. Die Betroffene teilte mir mit, zu der Auftrag gebenden Firma in keiner vertraglichen Beziehung zu stehen, allerdings sei ihr deren Geschäftsführerin schon persönlich bekannt.

Auf meine Nachfrage hat die Geschäftsführerin eingeräumt, dass sie das von ihr geführte Unternehmen beauftragt habe, für sich als Privatperson eine Schufa-Auskunft über die Betroffene einzuholen. Sie begründete dies damit, dass die Betroffene ihren Verpflichtungen aus einem Immobilienkaufvertrag nicht nachgekommen sei und sie daher ihr gegenüber Schadensersatzansprüche geltend machen wolle. Den Kaufvertrag hatte sie allerdings als Privatperson abgeschlossen und darin war sogar ausdrücklich vermerkt, dass die Vertragspartner den vorliegenden Vertrag nicht in Ausübung einer gewerblichen oder selbständigen beruflichen Tätigkeit abschließen.

Ich habe diese Schufa-Abfrage als unzulässig bewertet.

Ob die Schadensersatzansprüche der Geschäftsführerin berechtigt waren, hatte ich nicht zu beurteilen. Dies konnte jedoch dahinstehen, denn diese hatte ihre Forderung der Betroffenen gegenüber als Privatperson und nicht im Namen des von ihr geführten Unternehmens geltend gemacht. Die Schufa-Abfrage hatte die Geschäftsführerin nichtsdestoweniger im Namen ihres Unternehmens beauftragt und dabei gegenüber der Inkasso- und Ermittlungsgesellschaft sogar ausdrücklich erklärt, dass eine Forderung gegen die Betroffene bestünde. Tatsächlich hatte die Firma aber gar keine Forderung an die Betroffene und als Privatperson wäre die Geschäftsführerin im Übrigen überhaupt nicht zu einer solchen Schufa-Abfrage berechtigt gewesen.

Mit der im Rahmen der Schufa-Abfrage erfolgten Erhebung, Verarbeitung und Nutzung personenbezogener Daten hat die Geschäftsführerin gegen § 28 Abs. 1 BDSG verstoßen,

denn das von ihr geführte Unternehmen hatte weder ein rechtsgeschäftliches oder rechtsgeschäftsähnliches Schuldverhältnis mit der Betroffenen (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG), noch konnte das Unternehmen für sich berechtigte Interessen (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG) geltend machen. Vielmehr diente die Abfrage bei der Schufa einzig dazu, der Geschäftsführerin privat Informationen über die Betroffene zu beschaffen.

8.5.5 Herausgabe von Hotelbuchungsdaten an Familienangehörige

Eine Familie mit Kindern verbrachte ihren Urlaub in einem Hotel im Erzgebirge. Die Eltern des Familienvaters wollten ihn und vor allem die Enkel dort überraschen. Obwohl sie ihren Sohn als Vorsorgebevollmächtigten in ihren Vorsorgeausweisen eingetragen hatten, verweigerte das Hotelpersonal eine Auskunft über seinen Aufenthalt.

Das Verhalten des Hotelpersonals war meinerseits nicht zu beanstanden. Denn die Weitergabe der dem Hotel vorliegenden Informationen über den Aufenthalt des Sohnes als Hotelgast wäre hier allenfalls unter den Voraussetzungen des § 28 Abs. 2 Nr. 2a BDSG zulässig gewesen. Demnach hätte zum einen die Weitergabe dieser Informationen zur Wahrung der berechtigten Interessen der Eltern erforderlich sein müssen. Dafür bestanden hier keine Anhaltspunkte. Insbesondere lag keine notfallähnliche Situation vor, die ein unverzügliches Aufsuchen des Sohnes in seiner Funktion als Vorsorgebevollmächtigten erfordert und das Hotel insoweit zu einer entsprechenden Mithilfe ermächtigt (keinesfalls jedoch verpflichtet) hätte.

Zum anderen hätte auch kein Grund zu der Annahme bestehen dürfen, dass der Sohn ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. Auch und gerade dies war in der gegebenen Situation kaum sicher auszuschließen. Dem Hotelpersonal war die familiäre Situation im Einzelnen nicht bekannt, sodass es gar nicht beurteilen konnte, ob ein solcher Überraschungsbesuch vom Sohn unter den konkreten Umständen tatsächlich gewollt und erwünscht war, zumal man derartige Besuche üblicherweise im Vorfeld innerhalb der Familie abspricht und dabei die notwendigen Daten bereits austauscht.

8.5.6 Ablehnung eines Feuerwerks unter Verweis auf Referenzfälle

Ein Brautpaar wollte auf dem Gelände eines denkmalgeschützten Schlosses anlässlich seiner Hochzeit ein Feuerwerk abbrennen lassen. Der von dem Brautpaar ausgesuchte Feuerwerker erhielt jedoch keine Genehmigung durch die (private) Schlossverwaltung. Bei der Begründung verwies die Schlossverwaltung auf einen vorgelagerten vergleichbaren Fall, bei dem ebenfalls keine Genehmigung erteilt worden war. Zum Beweis hatte sie das entsprechende Ablehnungsschreiben per E-Mail beigefügt.

Dieses Ablehnungsschreiben enthielt allerdings zahlreiche personenbezogene Daten der seinerzeit beteiligten Akteure. Für diese Übermittlung personenbezogener Daten gab es keine rechtliche Grundlage. Es lag weder eine Einwilligung der betroffenen Personen vor, noch konnte sich die Schlossverwaltung auf § 28 Abs. 1 Satz 1 Nr. 1 oder 2 BDSG (Datenerhebung und Speicherung für eigene Geschäftszwecke) oder eine andere gesetzliche Grundlage stützen. Die Schlossverwaltung versicherte mir, den Vorgang zum Anlass zu nehmen, künftig im Umgang mit personenbezogenen Daten die notwendige Sorgfalt walten zu lassen und seine Mitarbeiter entsprechend zu belehren.

8.5.7 Personalausweiskopien bei Goldankauf

Ich erhielt einen Hinweis, wonach ein Unternehmen, das mit Edelmetallen handelt, in unzulässiger Weise Personalausweiskopien von Kunden anfordert oder auch selbst anfertigt und aufbewahrt.

Da die Anfertigung von Personalausweiskopien nur unter engen Voraussetzungen zulässig ist, bat ich das Unternehmen um eine Stellungnahme. Das Unternehmen legte mir gegenüber dar, dass es keinen Ankauf von Edelmetallen ohne Identifizierung des Kunden tätigen dürfe und hierfür in der Regel Personalausweiskopien gefertigt und aufbewahrt würden.

Ich teilte dem Unternehmen daraufhin mit, dass gegen eine Identifizierung von Personen mittels Personalausweis zunächst einmal keine Bedenken bestehen. § 20 Abs. 1 PAuswG regelt, dass der Inhaber den Ausweis auch bei nicht-öffentlichen Stellen als Identitätsnachweis und Legitimationspapier verwenden kann, d. h. der Ausweisinhaber kann den Ausweis bei Bedarf vorlegen und damit seine Identität entsprechend nachweisen.

Eine Befugnis zur Anfertigung von Personalausweiskopien kann aus dieser Norm jedoch nicht abgeleitet werden. Für eine Identifizierung unter Anwesenden, also im direkten Kundenkontakt, reicht es aus, wenn die zur Identifikation erforderlichen Angaben (Name, Vorname, Anschrift, ggf. Geburtsdatum) auf der Grundlage von § 28 Abs. 1 Satz 1 Nr. 1 BDSG notiert und durch Einsichtnahme in den Personalausweises verifiziert werden sowie ein entsprechender Vermerk (z. B. „Personalausweis hat vorgelegen“) angefertigt wird.

Eine Ausnahme bilden lediglich Geschäfte mit Transaktionen im Wert von 15.000 € und mehr. In diesen Fällen (vgl. § 3 Abs. 2 Nr. 2 GwG) ist gemäß § 3 Abs. 1 Nr. 1 GwG eine Identifizierung des Vertragspartners vorgeschrieben. Dazu hat sich der Händler anhand eines gültigen amtlichen Lichtbildausweises zu vergewissern, dass die von seinem Kunden angegebenen Identifizierungsdaten zutreffend sind (§ 4 Abs. 4 Satz 1 Nr. 1 GwG).

Hierüber sind entsprechende Aufzeichnungen anzufertigen, dies kann auch durch Anfertigung und Aufbewahrung einer Ausweiskopie erfolgen (§ 8 Abs. 1 Satz 3 GwG).

Im Fall des Fehlens eines direkten Kundenkontaktes – nach Angabe des Händlers ließen manche Kunden die zum Ankauf bestimmten Waren auch per Post anliefern – kann eine Ausweiskopie unter bestimmten Voraussetzungen dennoch zulässig sein. Aus der Vorgabe des § 20 Abs. 2 PAuswG, wonach der Ausweis außer zum elektronischen Identitätsnachweis weder zum automatisierten Abruf noch zur automatisierten Speicherung personenbezogener Daten verwendet werden darf, folgt, dass Ausweise nicht gescannt und anschließend elektronisch übermittelt werden dürfen, auch nicht durch den Ausweisinhaber selbst (vgl. VG Hannover, Urteil vom 28. November 2013 – 10 A 5342/11, juris). Damit sind also ausschließlich Papierkopien zulässig, wobei

- die Kopien als solche erkennbar sein müssen,
- Daten, insbesondere die auf dem Ausweis aufgedruckte Zugangs- und Seriennummer, die nicht zur Identifizierung benötigt werden, (durch den Ausweisinhaber) zu schwärzen sind (zumindest ist dieser darauf hinzuweisen), und
- die Kopie (durch den Händler) unverzüglich zu vernichten ist, sobald der mit der Kopie verfolgte Zweck, also die Identifizierung, erreicht ist.

Das Unternehmen teilte mir daraufhin mit, dass es seine Arbeitsabläufe nach diesen Vorgaben überprüft und entsprechend geändert hat.

8.5.8 Vollständige IBAN auf Kassenbelegen

Eine Betroffene wandte sich an mich mit dem Anliegen, dass bei Zahlungsvorgängen mit EC-Geldkarten im Einzelhandel die IBAN-Nummer vollständig lesbar auf der Einkaufsquittung abgedruckt wird. Dies hatte die Betroffene auch bereits mehrfach erfolglos in dem betreffenden Geschäft beanstandet.

Im Rahmen der Prüfung des Anliegens der Betroffenen bin ich zu dem Ergebnis gelangt, dass das Abdrucken einer vollständig lesbaren IBAN-Nummer auf einer Einkaufsquittung nicht beanstandungsfähig ist, auch wenn dies aus datenschutzrechtlicher Sicht natürlich keinen Idealzustand darstellt. Dies begründet sich vornehmlich damit, dass die Einkaufsquittung allein dem Kunden als Betroffenen ausgehändigt wird. Damit verfügt schlussendlich allein der Betroffene über die Einkaufsquittung und es obliegt allein seiner Verantwortung, was mit dieser und den darauf abgedruckten personenbezogenen Daten passieren soll.

Dem Unternehmen habe ich dennoch empfohlen, das Abdrucken der vollständigen IBAN bzw. der PAN-Nummer auf der Einkaufsquittung zu überdenken, da es sich hierbei um

die Angabe sensibler Kontodaten handelt. Es ist im Einzelhandel durchaus üblich und unter Datenschutzgesichtspunkten zu empfehlen, Konto- bzw. Kartendaten auf Kassenbons bzw. Lastschriftbelegen zu verfremden, d. h. einige Ziffern durch entsprechende Platzhalter (z. B. „X“ oder „#“) zu ersetzen. Für den Kunden bleibt dabei erkenn- und nachvollziehbar, welche Karte (welchen Kontos) er zur Bezahlung genutzt hat; Dritte hingegen können mit dieser Angabe nichts anfangen.

8.6 Sparkassen / Banken

8.6.1 Abfrage personenbezogener Daten von Familienangehörigen bei Verwaltungsratsmitgliedern einer Sparkasse

Ein Mitglied des Verwaltungsrates einer Sparkasse wandte sich an mich mit der Bitte um Prüfung, ob ein Auskunftsersuchen der Sparkasse ihm gegenüber aufgrund seiner Wahl als Verwaltungsratsmitglied rechtmäßig ist. Im Konkreten hatte die Sparkasse das Verwaltungsratsmitglied mittels eines Fragebogens u. a. um Angaben zum Familienstand gebeten sowie Namen, Geburtsdaten und berufliche Tätigkeiten von Familienangehörigen erfragt.

Die Sparkasse verwies mir gegenüber dazu auf das im Zuge der Umsetzung des Bilanzrechtsmodernisierungsgesetzes geänderte Handelsgesetzbuch. § 285 Nr. 21 HGB lege fest, dass die im Fragebogen enthaltenen Angaben zu nahe stehenden Personen eines Verwaltungsratsmitgliedes im Anhang des Jahresabschlusses enthalten sein müssten. Eine Pflicht zur Benachrichtigung der betroffenen Dritten bestehe aufgrund der Verankerung im europäischen Recht in diesem Fall gemäß § 33 BDSG nicht.

Dieser Auffassung habe ich nicht folgen können; das Auskunftsersuchen der Sparkasse war in dieser Form unzulässig.

Nach § 285 Nr. 21 HGB sind im Anhang zum Jahresabschluss Geschäftsbeziehungen mit Personen in Schlüsselpositionen – wie dem Verwaltungsrat – und diesem nahe stehenden Personen, also auch Familienangehörigen, zwingend allein dann und ohne Personenbezug (ohne namentliche Nennung) anzugeben,

a) soweit die Geschäftsbeziehungen für die Beurteilung der Finanzlage wesentlich sind und
b) sie nicht marktüblichen Bedingungen entsprechen.

Hieraus folgt datenschutzrechtlich, dass zur Erstellung des Jahresabschlusses auf Grundlage von § 28 Abs. 1 Satz 1 Nr. 1 BDSG die Angaben,

a) ob ein Verwaltungsratsmitglied ledig, verheiratet, geschieden oder verwitwet ist,

b) wie sein Ehegatte oder Lebenspartner heißt, wo er wohnt, wann er Geburtstag hat, wo er geboren ist und in welchem Beruf er arbeitet sowie
c) die Namen, Geburtsdaten und Tätigkeiten von Kindern

im Sinne eines Erfordernisses allenfalls dann abgefragt, also erhoben werden dürfen, wenn die Berichtspflicht auch tatsächlich besteht. Der entsprechende Fragebogen war daher so zu gestalten, dass diese Angaben nur dann erfragt werden, wenn ein Verwaltungsratsmitglied – nach bestem Wissen und Gewissen – die hinreichend bestimmt zu fassende Vorfrage, ob ihm nahe stehende Personen neben dem originären Bankgeschäft sonstige Vertrags- und Geschäftsbeziehungen mit der Sparkasse unterhalten,

a) die über ein jährliches Kostenvolumen einer zu definierenden Wesentlichkeitsgrenze hinausgehen und
b) deren Bedingungen nicht marktüblich sind,

mit „Ja“ beantwortet hat. Ansonsten besteht kein Erhebungserfordernis.

Soweit unter Beachtung der vorstehenden Ausführungen eine Befugnis zur Erhebung der Daten Dritter besteht, sind Dritte gleichwohl zu benachrichtigen, denn für einen Ausschluss nach § 33 Abs. 2 Nr. 4 BDSG fehlt es hierfür an der erforderlichen Normenklarheit: § 285 Nr. 21 HGB regelt insoweit nicht ausdrücklich – im Sinne einer transparenten, unmittelbaren Ermächtigung – das Recht zur Datenverarbeitung.

Die Sparkasse hat den Fragebogen daraufhin entsprechend angepasst.

8.7 Vereine / Verbände

8.7.1 Öffentliche Aushänge in Gartenvereinen

Unverändert ein Dauerthema sind öffentliche Aushänge in Garten- und anderen Vereinen. Obwohl ich mich dazu – in Bezug auf Sportvereine – bereits in meinem 7. TB unter den Punkten 8.7.3 und 8.7.4 geäußert habe, möchte ich dies daher hier nochmals thematisieren.

In der konkreten Angelegenheit wandte sich eine Betroffene an mich mit der Bitte um Prüfung, ob es zulässig ist, offene Beitragsforderungen des Gartenvereins gegenüber Vereinsmitgliedern durch Aushang am „Schwarzen Brett“ mit namentlicher Nennung öffentlich bekannt zu machen.

Ein solcher Aushang ist nicht zulässig.

Aushänge eines Gartenvereins am „Schwarzen Brett“ bzw. im Schaukasten stellen datenschutzrechtlich zunächst eine Übermittlung an die Gemeinschaft der Vereinsmitglieder dar. Ist der Ort des Aushangs auch anderen Personen (z. B. Gästen oder Spaziergängern) zugänglich, wovon gerade in Kleingartenanlagen regelmäßig auszugehen ist, liegt auch eine Übermittlung an vereinsfremde Personen vor.

Wenn keine Einwilligung der betroffenen Vereinsmitglieder vorliegt, dass bestimmte Angaben zur Person mittels Aushang vereinsöffentlich oder gar darüberhinausgehend allgemein bekannt gemacht werden dürfen, ist eine Übermittlung nach § 28 Abs. 1 Satz 1 Nr. 1. bzw. Nr. 2 BDSG nur dann zulässig, wenn die Veröffentlichung der Mitgliederdaten aus einem (persönlichkeitsrechtlich verhältnismäßigem) Gemeinschaftsakt des Vereins (Mitgliederbeschluss oder Regelung in der Satzung) gerechtfertigt werden kann oder der Zweckbestimmung des Vereins im Sinne der Mitgliedschaftsrechte und -pflichten entspricht oder (sonst) zumindest ein weitergehendes Interesse des Vereins an der Mitteilung besteht, dem kein schutzwürdiges Interesse des Betroffenen entgegensteht (7/8.7.3). Typische zulässige Aushänge eines Gartenvereins sind hiernach beispielsweise Aushänge zu neuen Vorstandsmitgliedern und Ehrungen.

Weder satzungsrechtlich regelbar noch im Sinne eines berechtigten Vereinsinteresses gestattet bzw. aus dem Mitgliedschaftsverhältnis ableitbar ist jedoch eine allgemeine Befugnis, säumige Vereinsmitglieder als solche öffentlich namhaft zu machen. Abgesehen von der fehlenden Erforderlichkeit einer solchen Veröffentlichung überwiegt das Persönlichkeitsrecht der Betroffenen in diesem Fall grundsätzlich jedes Mitteilungsinteresse des Vereins, denn mit dem öffentlichen Anprangern vermeintlicher oder tatsächlicher Außenstände als Mittel der Beitreibung oder Präventionsmaßnahme zur Verbesserung der allgemeinen Zahlungsmoral soll ein sozialer Druck jenseits der Grenzen gesetzlich erlaubter Instrumente zum Einzug finanzieller Forderungen aufgebaut bzw. genutzt werden.

8.7.2 Datenlöschung bei Vereinsaustritt

Einem Verein ging es um die Verfahrensweise zur Datenlöschung bei Beendigung einer Mitgliedschaft. Diesbezüglich gäbe es gegensätzliche Vorschriften und auch in Publikationen der Datenschutzaufsichtsbehörden würden widersprüchliche Auffassungen vertreten. Einerseits werde gefordert, dass die Daten eines Mitgliedes nach dem Vereinsaustritt zu löschen seien, andererseits werde auf die 10-jährige Aufbewahrungsfrist des Steuerrechts verwiesen. Es gäbe außerdem ein berechtigtes Interesse des Vereins, seine Geschichte zu bewahren. Mit der von den Aufsichtsbehörden im Muster für eine Datenschutzerklärung vorgeschlagenen Formulierung „Beim Austritt werden Name, Adresse und Geburtsjahr des Mitglieds aus der Mitgliedsliste gelöscht.“ könne man dies aber nicht erreichen. Vom Mitglied bliebe nichts, wenn dessen Name gelöscht werde.

Ich habe keinen Widerspruch zwischen der Forderung nach Löschung von Mitgliederdaten bei Austritt aus dem Verein und den steuerrechtlichen Aufbewahrungsfristen gesehen. Bei der Mitgliederdatenbank einerseits und der – für die Buchhaltung relevanten – Beitragsverwaltung andererseits handelt es sich um separate Anwendungen mit getrennten Dateien bzw. Datenbeständen. Während ich in Bezug auf die Mitgliederdatenbank keinen Hinderungsgrund sehe, die Daten eines ausgeschiedenen Mitglieds dem laufenden Geschäftsgang zu entziehen, d. h. diese Daten dort sofort bzw. nach einer festzulegenden Übergangszeit – in diesem Fall muss eine entsprechende Kennzeichnung des betreffenden Datensatzes als „inaktiv“ erfolgen – zu löschen, können und müssen die Daten der Beitragsabrechnung natürlich gemäß den gesetzlichen Fristen weiter aufbewahrt werden, dürfen dabei aber für keine anderen Zwecke mehr genutzt werden (Sperrung gemäß § 35 Abs. 3 Nr. 1, Abs. 8 BDSG).

Das Vereinsinteresse an der Wahrung seiner Geschichte kann ich – jedenfalls in Bezug auf bestimmte Funktionsträger bzw. bei einer bestimmten Ausrichtung eines Vereins (z. B. Förderverein) auch für alle Mitglieder – nachvollziehen. Um archivmäßig zu dokumentieren, welche Personen zu welchen Zeiten Vereinsmitglieder gewesen sind und das Anliegen des Vereins entsprechend unterstützt haben, ist es jedoch nicht erforderlich, deren gesamte Mitgliederdaten zu archivieren. Meines Erachtens reicht eine listenmäßige oder sonst strukturierte Erfassung mit Namen, Mitgliedsnummer, ggf. Funktion, Mitgliedszeiten und Wohnort (im Zeitraum der Mitgliedschaft) aus. Weder das Geburtsdatum noch die Bankverbindung ist für diese Zwecke erforderlich, auch sind insoweit entgegenstehende schutzwürdige Betroffeneninteressen (vgl. § 28 Abs. 1 Satz 1 Nr. 2 BDSG) zu berücksichtigen. Dies gilt auch für die erfassten Kontaktdaten (Anschrift, Telefon, Fax, E-Mail), zumal sich diese auch vergleichsweise häufig ändern und damit ohnehin ihre Bedeutung verlieren.

8.7.3 Tonaufzeichnungen von Vorstandssitzungen zur Protokollerstellung

Ein Vereinsvorstand hat mich um Auskunft gebeten, unter welchen Voraussetzungen Tonaufzeichnungen von Vorstandssitzungen und Besprechungen zum Zweck der (Erleichterung der) Protokollerstellung zulässig sind und welche Löschfristen hierfür gelten.

Ich habe dem Verein hierzu folgende Auskunft gegeben:

Tonaufzeichnungen von Vorstandssitzungen sind dann zulässig, wenn eine der folgenden drei Voraussetzungen vorliegt:

a) Es haben alle Sitzungsteilnehmer gemäß § 4a BDSG eingewilligt.

b) Es gibt eine diesbezügliche Regelung in der Vereinssatzung oder einen entsprechenden Vorstandsbeschluss. Die Tonaufzeichnung ist dann gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG zulässig. Auf eine Einwilligung kommt es in dem Fall nicht mehr an.

c) Es wird vor jeder Sitzung die Absicht zur Tonaufzeichnung bekanntgegeben und abgefragt, ob hiergegen Einwände bestehen. Nur dann, wenn niemand Einwände erhebt, ist die Tonaufzeichnung gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG (Interessenabwägung) zulässig. Dies sollte im Sitzungsprotokoll auch so dokumentiert werden.

Die Frist für die Löschung der Tonaufzeichnungen bemisst sich nach § 35 BDSG. Nach § 35 Abs. 2 Nr. 3 BDSG sind sie zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Dies ist vorliegend dann der Fall, wenn das Protokoll in seiner genehmigten endgültigen Fassung vorliegt.

8.8 Wohnungswirtschaft

8.8.1 Mieterselbstauskünfte

Insbesondere in den sächsischen Ballungszentren wird es für Wohnungssuchende zunehmend schwerer, geeigneten, vor allen Dingen bezahlbaren, Wohnraum zu finden. Um ihre Chance zu wahren, können es sich Mietinteressenten kaum leisten, unzulässige Fragen der Vermieterseite ihnen gegenüber zu hinterfragen oder unbeantwortet zu lassen. Umso wichtiger ist es daher, dass von der Vermieterseite her nur zulässige Fragen gestellt werden. Eine gute Hilfestellung bietet hier die in 7/14.2.1 wiedergegebene Orientierungshilfe des Düsseldorfer Kreises zur „Einholung von Selbstauskünften bei Mietinteressenten“. Dieses Dokument halte ich auch auf meiner Webseite *(http://www.datenschutz.sachsen.de)* unter Nichtöffentlicher Bereich / Informationen / Arbeitshilfen zum Download bereit.

Im Berichtszeitraum haben mich zu dieser Thematik zahlreiche Beschwerden erreicht. Von Mietinteressenten sind mir dazu die ihnen vorgelegten Selbstauskunftsvordrucke von Vermietern bzw. in deren Auftrag tätigen Hausverwaltungen mit der Bitte um Prüfung übersandt worden.

Bei meinen Prüfungen habe ich in diesen Mieterselbstauskunftsbögen regelmäßig unzulässige Fragestellungen feststellen müssen. Am häufigsten betraf dies die Abfrage der Staatsangehörigkeit und der Personalausweis- bzw. Passnummer. Gleichfalls unzulässig waren Fragen nach der Dauer des bestehenden Arbeitsverhältnisses, zum regelmäßigen Spielen von Musikinstrumenten sowie die immer noch anzutreffende Forderung nach Übergabe einer Personalausweiskopie.

In Bezug auf die Forderung einer Vorvermieter- bzw. Mietschuldenfreiheitsbescheinigung wurde bislang die Auffassung vertreten, dass die Frage nach früheren bzw. aktuellen Vermietern grundsätzlich unzulässig ist, weil diese eine dem Direkterhebungsgrundsatz widersprechende Datenerhebung beim Vorvermieter ermöglicht bzw. darstellt.

Nachdem der BGH aber mit Urteil vom 9. April 2014 (VIII ZR 107/13, juris) entschieden hat, dass Fragen nach der Person und Anschrift des Vorvermieters, der Dauer des vorangegangenen Mietverhältnisses und der Erfüllung der mietvertraglichen Pflichten grundsätzlich geeignet sind, sich über die Bonität und Zuverlässigkeit des potentiellen Mieters ein gewisses Bild zu machen und es sich dabei auch nicht um Fragen handelt, die den persönlichen oder intimen Lebensbereich des Mieters betreffen und aus diesem Grund unzulässig sein könnten, kann dies in dieser Absolutheit nicht mehr aufrechterhalten werden.

Festzuhalten ist zunächst, dass die bloße Abfrage dieser Daten noch keinen Verstoß gegen das Direkterhebungsprinzip darstellt, denn damit ist noch keine Datenerhebung des neuen Vermieters beim alten Vermieter verbunden. Begnügt sich der neue Vermieter ohne weitere Nachfragen mit diesen Informationen, wird dagegen nichts einzuwenden sein; im Übrigen werden die gegen eine Rückfrage beim alten Vermieter bestehenden Bedenken allerdings aufrechterhalten.

Verlangt der neue Vermieter hingegen eine Mietschuldenfreiheitsbestätigung, so sollte dies nur als freiwillige Option möglich sein, da ein Vermieter jedenfalls nicht zur Ausstellung einer solchen Bescheinigung verpflichtet ist. Ein Mieter hat nach früherer Rechtsprechung des BGH (Urteil vom 30. September 2009 – VIII ZR 238/08, juris) keinen Anspruch gegen seinen bisherigen Vermieter auf Ausstellung einer Mietschuldenfreiheitsbescheinigung. Dies führe allerdings nicht dazu, dass der neue Vermieter vor Abschluss eines Mietvertrages eine diesbezügliche Bescheinigung vom Mietinteressenten nicht (zumindest) erbitten könne (BGH, Urteil vom 9. April 2014 – VIII ZR 107/13, juris).

Eine vor diesem Hintergrund adäquate Lösung könnte daher darin bestehen, dass eine Mietschuldenfreiheitsbestätigung nur erbeten werden kann, wenn dem Mieter in diesem Zusammenhang freigestellt wird, seine Zuverlässigkeit und Bonität in Mietangelegenheiten auch auf anderem Wege, z. B. über den alten Mietvertrag und Kontoauszüge (alles teilgeschwärzt), aus denen sich die regelmäßige Mietzahlung ergibt, nachzuweisen.

8.8.2 Datenübermittlung vom Vermieter an Pflegedienst bei altersgerechtem Wohnen

Mich erreichten mehrere Eingaben, weil die Mieter eines Seniorenwohnheims nach einem Eigentümerwechsel die Aufforderung erhielten, mit dem dort ansässigen Pflegedienst Betreuungs- und Serviceverträge abzuschließen oder sich eine neue Wohnung zu suchen. Das Schreiben, das neben Namen und Anschrift der Mieter auch das Einzugsdatum enthielt, war dabei nicht nur von dem Objektverwalter des Eigentümers, sondern auch vom Pflegedienst und einem Servicedienstleister sowie einem Mitglied des Mieterrats unterzeichnet.

Die Mietverträge der betroffenen Altmieter waren (anders als die Neuverträge) nicht an die Bedingung geknüpft, dass auch Betreuungs- und Serviceverträge abzuschließen sind, d. h. der Mietvertrag mit den Betreuungs- und Serviceverträgen stehen und fallen sollte. Eine Rechtsgrundlage für die Datenübermittlung vom Vermieter an den Pflegedienst, den Servicedienstleister und den Vertreter des Mieterrats war insofern nicht gegeben: Die Datenübermittlung war nicht zur Durchführung des Mietvertrags im Sinne des § 28 Abs. 1 Satz 1 Nr. 1 und Abs. 2 BDSG erforderlich. Sie war auch nicht gemäß § 28 Abs. 1 Satz 1 Nr. 2 und Abs. 2 BDSG zulässig, denn das Interesse der Altmieter überwog, frei und unbeeinflusst darüber entscheiden zu können, ob sie sich an den jeweiligen Pflegedienst und Servicedienstleister wenden möchten oder nicht. Eine wirksame schriftliche Einwilligung (§ 4a Abs. 1 BDSG) der Altmieter lag ebenfalls nicht vor.

Der Vermieter teilte mir auf meine Nachfrage jedoch – unwiderlegbar – mit, dass es sich bei dem Schreiben um eine Serienbriefvorlage gehandelt habe, wobei den Unterzeichnern nicht bekannt war, an welche Mieter der Serienbrief versandt werden würde. Die unterschriebene letzte Seite des Serienbriefs sei dann als Kopie in der jeweiligen Reinschrift verwendet worden. Insofern konnte ich auch keinen datenschutzrechtlichen Verstoß feststellen.

8.8.3 Weitergabe der Telefonnummer eines Mieters an Reparaturfirmen zwecks Terminabstimmung

Offensichtlich um einem Handwerksunternehmen die Arbeit zu erleichtern, teilte ein Beschäftigter einer Hausverwaltung diesem die (nicht öffentlich bekannte) Mobiltelefonnummer einer Mieterin mit. Diese hatte den Handwerker nicht beauftragt, stattdessen handelte es sich um eine Kontrollmaßnahme seitens des Vermieters in den Räumen der Mieterin. Nachdem der Handwerker sodann die Mieterin telefonisch zur Terminvereinbarung kontaktiert hatte, wandte sich diese mit der Frage nach der rechtlichen Zulässigkeit dieser Vorgehensweise an mich.

Die Hausverwaltung hat das eigenmächtige Handeln eines Beschäftigten eingeräumt; es sei wohl irrtümlich von einer Übermittlungsbefugnis im Mietvertrag ausgegangen worden.

Aufgrund der Umstände schied eine Übermittlungsbefugnis nach 28 Abs. 1 Satz 1 Nr. 1 BDSG allerdings aus – die Kontrollmaßnahme war durch die Mieterin zwar zu dulden, jedoch war der Eigentümer bzw. die Hausverwaltung zunächst einmal selbst in der Pflicht, eine Terminabstimmung mit der Mieterin vorzunehmen. Aus dem Mietvertrag konnte keine Befugnis abgeleitet werden, die – in anderweitigem Zusammenhang durch die Mieterin mitgeteilte – Telefonnummer, an das Handwerksunternehmen zur eigenständigen Vereinbarung eines Betretungstermins weiterzugeben. Der Zulässigkeitstatbestand des § 28 Abs. 1 Satz 1 Nr. 2 BDSG erfordert eine Interessenabwägung zwischen erleichterter Koordinierung der Wartungs- bzw. Kontrollmaßnahmen durch die Hausverwaltung auf der einen und den Schutz der Privatsphäre der Mieterin auf der anderen Seite. Diese Abwägung erfolgte vorliegend unter offenbar unzureichender Kenntnis des geltenden Rechts und führte zu einem falschen Ergebnis. Mieter müssen sich darauf verlassen können, dass die Hausverwaltung ihre privaten Telefonnummern nur zu den vereinbarten Zwecken nutzt oder an Dritte übermittelt. Für alle übrigen Zwecke sind vorab Einwilligungen einzuholen bzw. ist deren Verweigerung zu respektieren.

8.8.4 Veröffentlichung von Fotos von zum Verkauf stehender vermieteter Wohnungen

Eine vermietete Wohnung sollte über einen Makler verkauft werden. Der Makler veröffentlichte dafür das Exposé mit Fotos der Wohnung im Internet. Die Mieter der Wohnung beschwerten sich bei mir über die Veröffentlichung der Fotos, da auf den Fotos die Inneneinrichtung ihrer Wohnung zu sehen war und sie der Veröffentlichung ausdrücklich widersprochen hatten. Zwar hatten sie der Anfertigung von Fotos zugestimmt, aber ausdrücklich nur für die Erstellung eines Gutachtens für interne Zwecke. Obwohl der Makler diese Bilder nach der schriftlichen Untersagung durch die Mieter aus dem Internet zunächst entfernt und sich bei den Mietern entschuldigt hatte, tauchten die Bilder nach einigen Monaten überraschender Weise erneut im Internet auf.

Fotos der Inneneinrichtung einer Wohnung stellen Angaben über persönliche Verhältnisse natürlicher Personen dar. Die Beschreibung der Lage im Exposé ließ es zusammen mit den Abbildungen des Wohnhauses und insbesondere des Balkons zumindest für Ortskundige zu, auf die konkrete Wohnung und damit auf die Identität der damaligen Mieter zu schließen. Insofern handelt es sich um personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG.

Gemäß § 4 Abs. 1 BDSG sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder andere Rechtsvorschriften dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Eine Einwilligung der Betroffenen lag nicht vor. Als Grundlage wäre allenfalls noch § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Betracht gekommen, jedoch nur, wenn die Veröffentlichung der Fotos für den Verkauf zwingend erforderlich gewesen wäre und das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Veröffentlichung nicht überwogen hätte. Davon konnte vorliegend nicht ausgegangen werden. In seiner Stellungnahme hierzu versicherte der Makler mir dann jedoch ausdrücklich, dass es sich bei der nochmaligen Veröffentlichung um ein Versehen gehandelt habe. Dies war insofern auch glaubhaft, da die Wohnung zu dem Zeitpunkt bereits verkauft war. Den Vorgang konnte ich damit abschließen.

8.8.5 Veröffentlichung der Privatanschriften von Genossenschaftsvertretern im Internet

Eine Wohnungsgenossenschaft hatte Namen und Adressen der gewählten Genossenschaftsvertreter in ihrer Mitglieder- und Mieterzeitschrift und diese wiederum auch im Internet veröffentlicht. Einer der betroffenen Genossenschaftsvertreter teilte mir mit, dass viele Vertreter eine Veröffentlichung im Internet nicht wünschten. Er selbst hatte der Veröffentlichung im Internet gegenüber der Genossenschaft ausdrücklich nicht zugestimmt, indem er den diesbezüglichen Passus in der Einwilligungserklärung gestrichen hatte. Die Genossenschaft hatte ihm jedoch mitgeteilt, an der Veröffentlichung dennoch festhalten zu wollen. Sie sehe darin keinen datenschutzrechtlichen Verstoß. Sie stützte sich dabei zunächst auf § 43a Abs. 6 GenG, alternativ auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG.

Ich habe den Sachverhalt geprüft und bin zu dem Ergebnis gekommen, dass keine der beiden Vorschriften eine Veröffentlichung im Internet rechtfertigen kann.

§ 43a Abs. 6 GenG besagt lediglich, dass eine Liste mit den Namen und Anschriften der Vertreter in den Geschäftsräumen der Genossenschaft und ihren Niederlassungen für mindestens zwei Wochen auszulegen ist. Nur die Bekanntmachung der Auslegung ist, im Unterschied zur Auslegung der Namen und Anschriften selbst, in einem öffentlichen Blatt vorzunehmen. Darüber hinausgehende Regelungen zur Veröffentlichung von Namen und Anschriften der gewählten Genossenschaftsvertreter, so auch zu einer Veröffentlichung im Internet, enthält § 43a GenG dagegen nicht.

§ 28 Abs. 1 Satz 1 Nr. 2 BDSG wäre als Rechtsgrundlage nur dann in Betracht gekommen, wenn eine Veröffentlichung im Internet erforderlich gewesen wäre und dabei kein Grund zu der Annahme bestanden hätte, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Auch wenn im

Ergebnis dieser Abwägung eine Veröffentlichung der Vertreterdaten z. B. in einem Printmedium der Genossenschaft als zulässig angesehen werden könnte, kann daraus nicht zugleich von einer Zulässigkeit der Veröffentlichung im Internet ausgegangen werden. Denn im Gegensatz zur Veröffentlichung der Daten in gedruckten, von der Natur der Sache her einem begrenzten, interessierten Kreis zugänglichen Publikationen und Verzeichnissen, stellt die Bereitstellung im Internet – trotz seiner zum Alltag gehörenden Informationsfunktion – sich als Veröffentlichung in einer von jedermann global abrufbaren, virtuellen Zeitung dar, wobei diese Daten mit anderen im Internet anzutreffenden Daten über die betroffene Person problemlos verknüpft und losgelöst von dem Zweck der ursprünglichen Veröffentlichung verwendet werden können (Gola/Schomerus, BDSG 12. Auflage, Rdnr. 21 zu § 28). Die Veröffentlichung der Vertreterdaten im Internet stellte also einen stärkeren Eingriff in die Persönlichkeitsrechte der Betroffenen dar mit der Folge, dass sowohl von erheblichen schutzwürdigen Interessen der Betroffenen auszugehen als auch bei der Prüfung der Erforderlichkeit ein besonders strenger Maßstab anzulegen war.

Die Genossenschaft verteidigte in ihrer Stellungnahme zwar ihren Standpunkt der Zulässigkeit ihres bisherigen Vorgehens. Im Ergebnis konnte dennoch eine, wie ich meine, gute, datenschutzkonforme Lösung gefunden werden. Die Genossenschaft nahm die beiden Seiten mit den Namen und Anschriften der gewählten Genossenschaftsvertreter aus der Internetveröffentlichung heraus und kündigte an, zukünftig nur noch eine Bekanntgabe über das Intranet vornehmen zu wollen. Zusätzlich sei beabsichtigt, auf der Website der Genossenschaft einen gut sichtbaren Hinweis für die Genossenschaftsmitglieder zu platzieren, dass die Liste mit den betreffenden Daten jederzeit über die Genossenschaft abgefordert werden kann.

8.8.6 Werbung an WEG-Mitglieder nach Verkauf einer Wohnung

Bei der bereits in 7/8.9.1 behandelten Thematik hat es sich offensichtlich nicht um einen Einzelfall gehandelt. Grund genug, dieses Thema noch einmal aufzugreifen.

Wiederum war ein Immobilienmakler mit dem Verkauf einer Wohnung beauftragt worden und hatte in diesem Zusammenhang Kenntnis der Anschriften aller WEG-Mitglieder erlangt. Diesbezüglich sind mir zwei Fallkonstellationen bekannt geworden. In dem Fall aus dem 7. TB hatte der Makler auf der Grundlage einer Eigentümervollmacht Einsicht in das Grundbuch genommen und bei dieser Gelegenheit dort die Adressdaten der Miteigentümer erhoben; in dem aktuellen Fall hat er die Adressdaten direkt über den Eigentümer in Erfahrung gebracht, dessen Wohnung er verkaufen sollte. In beiden Fällen ist schon die Datenerhebung rechtswidrig gewesen, denn die Kenntnis der Adressdaten

der Miteigentümer ist für die Abwicklung des Verkaufs einer Eigentumswohnung nicht erforderlich.

In beiden Fällen hatte sich der Makler nach erfolgreichem Verkauf der Wohnung an alle Wohnungseigentümer gewandt, sie über den Eigentümerwechsel informiert und ihnen für den Fall einer Verkaufsabsicht seine Dienste angeboten.

Im aktuellen Fall versuchte sich der Makler mir gegenüber zunächst damit zu rechtfertigen, dass es sich nicht um Werbe-, sondern um Informationsschreiben gehandelt habe.

Der Begriff der Werbung ist im Bundesdatenschutzgesetz nicht definiert. Stattdessen ist dafür die EU-Richtlinie 2006/114/EG über irreführende und vergleichende Werbung heranzuziehen: Nach Art. 2 lit. a der Richtlinie ist unter „Werbung“ jede Äußerung bei der Ausübung eines Handels, Gewerbes, Handwerks oder freien Berufs mit dem Ziel, den Absatz von Waren oder die Erbringung von Dienstleistungen, einschließlich unbeweglicher Sachen, Rechte und Verpflichtungen, zu fördern, zu verstehen. Für die Annahme des Werbecharakters reicht es also aus, dass das Schreiben unmittelbar oder mittelbar dem Ziel dient, die Erbringung von Dienstleistungen des eigenen Unternehmens zu fördern. Der Werbecharakter ergibt sich dabei allein schon aus in der in solchen Schreiben regelmäßig enthaltenen positiven Selbstdarstellung des Unternehmens (vgl. dazu auch BGH, Urteil vom 9. Juni 2005 – I ZR 279/02, Rdnr. 32 [dort zum Werbecharakter eines Gewinnspiels], juris).

Davon abgesehen war und ist es nicht die Aufgabe eines Maklers, die verbleibenden WEG-Mitglieder über den Verkauf einer Wohnung zu informieren. Eine solche Information ist allein eine Obliegenheit der von der WEG beauftragten Hausverwaltung.

Darüber hinaus hatte sich der Makler auch auf das Listenprivileg des § 28 Abs. 3 Satz 2 BDSG berufen, dabei aber übersehen, dass dies voraussetzt, dass er die genutzten Daten im Rahmen eines Vertragsverhältnisses direkt bei den Betroffenen oder aus allgemein zugänglichen Adress-, Rufnummern-, Branchen- oder vergleichbaren Verhältnissen erhoben hat (§ 28 Abs. 3 Satz 2 Nr. 1 BDSG). Dies war vorliegend aber nicht der Fall, er hatte diese Daten stattdessen von einem Miteigentümer abgefragt.

Die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten der Miteigentümer für Werbezwecke ist daher rechtswidrig gewesen.

8.8.7 Schwärzung der IBAN auf Überweisungsbelegen

Ein Wohnungsverwalter hatte im Rahmen der Einladung zu einer außerordentlichen Eigentümerversammlung personenbezogene Bankverbindungsdaten der Beiratsvorsitzenden allen Eigentümern zur Kenntnis gebracht. Konkret handelte es sich dabei um einen Nachweis der Internetüberweisung, die die Beiratsvorsitzende zur Beitragszahlung für eine Vermögenshaftpflichtversicherung für den Beirat getätigt hatte. Dieser Nachweis war allen Einladungen zu der außerordentlichen Mitgliederversammlung beigefügt.

Mir ist weder eine Vorschrift bekannt, die die Wohnungsverwaltung zu dieser Datenübermittlung ermächtigt haben könnte, noch erschloss sich mir überhaupt die Erforderlichkeit der damit verbundenen Unterrichtung aller WEG-Mitglieder über die konkrete Bankverbindung der Beiratsvorsitzenden. Die betreffende Datenweitergabe ist unzulässig und somit rechtswidrig gewesen (§§ 4, 28 Abs. 1 BDSG).

Ich stelle dabei nicht in Abrede, dass es zur Vorbereitung und Durchführung der außerordentlichen Eigentümerversammlung notwendig war, der Gemeinschaft vor der Beschlussfassung die Versicherungsunterlagen und auch den Zahlungsnachweis vorzulegen. Nicht erforderlich war es jedoch, auf diese Weise allen Miteigentümern auch die Bankverbindung der Beiratsvorsitzenden bekanntzugeben. Diese eine Angabe hätte ohne weiteres geschwärzt werden können, ohne dass dadurch die Glaubhaftigkeit des Zahlungsnachweises in irgendeiner Weise in Frage zu stellen gewesen wäre.

Die Hausverwaltung hatte mir daraufhin einen nochmaligen Versand des Zahlungsnachweises mit geschwärzter IBAN in Verbindung mit der Bitte, ihr den ungeschwärzten Zahlungsnachweis wieder zurückzusenden bzw. ihr die Vernichtung zu bestätigen, zugesagt. Auf diese Weise wäre gewährleistet gewesen, dass die Eigentümer weiterhin über vollständige Unterlagen verfügen, ohne dabei auch unzulässiger Weise Angaben zur Bankverbindung eines Miteigentümers in ihrem Besitz zu haben.

Leider ging auch diese Aktion gründlich schief. Auf den mir vorgelegten Überweisungsbeleg war die IBAN der Beiratsvorsitzenden wiederum nicht geschwärzt; stattdessen fehlte auf diesen Zahlungsbelegen die – an dieser Stelle unkritische – IBAN der Versicherung als Zahlungsempfänger.

Es bedurfte daher eines weiteren Schreibens zur nochmaligen Korrektur des missglückten Belegversandes. Ich gehe daher davon aus, dass diese Angelegenheit nachhaltigen Eindruck bei der Hausverwaltung hinterlassen hat und eine Wiederholungsgefahr insoweit nicht besteht. Der Betroffenen habe ich nahegelegt, nicht erforderliche Daten zukünftig gleich selbst in den an die Wohnungsverwaltung weiterzugebenden Unterlagen zu schwärzen.

8.8.8 Wiederverwendung von Fehldrucken

Eine Mieterin hatte von der von ihrem Vermieter beauftragten Hausverwaltung eine Zahlungsaufforderung erhalten. Auf der Rückseite ihres eigenen Kontoblattes fand sie allerdings eine Saldo-Liste des Hausverwalters mit den Namen aller Mieter verschiedener Objekte, die ihm noch Geld schuldeten, einschließlich der Höhe des Zahlungsrückstandes.

Die Überprüfung des Sachverhaltes hat dann ergeben, dass irrtümlich einseitig bereits bedrucktes Papier in den Drucker eingelegt worden war. Wie das konkret passieren konnte, war dabei leider nicht mehr aufzuklären, jedenfalls sei das aber keine gängige Arbeitsweise gewesen. Unbestritten war aber, dass auf diese Weise unbefugt personenbezogene Daten an die Mieterin übermittelt worden sind (Verstoß gegen § 28 Abs. 1 Satz 1 Nr. 1 BDSG).

Nach § 38 Abs. 1 Satz 6 BDSG bin ich befugt, bei Feststellung eines Datenschutzverstoßes die Betroffenen, hier die übrigen in der Liste offener Salden aufgeführten Mieter, hierüber zu unterrichten. Ich habe der Hausverwaltung angeboten, davon abzusehen, wenn sie mir – unter Vorlage geeigneter Nachweise – zeitnah bestätigt, dass sie dies bereits selbst getan hat. Die Hausverwaltung ist diesem Vorschlag gefolgt.

8.9 Schulen / Kindertagesstätten / Sozialeinrichtungen

8.9.1 Datenschutzrecht für Privatschulen

Im Berichtszeitraum wurde die Frage aufgeworfen, welche Datenschutzvorschriften für Privatschulen in Sachsen (Schulen in freier Trägerschaft) zur Anwendung kommen, insbesondere wie es sich mit der Anwendung der Verwaltungsvorschrift über den Datenschutz beim Umgang mit personenbezogenen Daten an Schulen (VwV Schuldatenschutz) verhält.

Die Anfrage habe ich dahingehend beantwortet, dass prüfungsrechtliche Maßnahmen und Entscheidungen einschließlich der Erteilung von Zeugnissen als hoheitlicher Akt einzustufen sind. Die Privatschule handelt insoweit als Beliehener, sodass für diesen Bereich gemäß § 2 Abs. 1 Satz 2 SächsDSG das Sächsische Datenschutzgesetz Anwendung findet. Alle anderen Maßnahmen einer Privatschule im Verhältnis zu ihren Schülern, deren Eltern und ihren Beschäftigten sind allein privatrechtlicher Natur. Insoweit handelt eine Privatschule als nicht-öffentliche Stelle, sodass diesbezüglich das Bundesdatenschutzgesetz Anwendung findet. Die VwV Schuldatenschutz findet auf Privatschulen keine Anwendung. Der Anwendungsbereich bezieht sich auf öffentliche Schulen im Freistaat Sachsen. Auf Privatschulen wird insoweit nicht ausdrücklich verwiesen.

8.9.2 Stundenplananzeige über Monitor

Ein Lehrer wandte sich an mich und beanstandete, dass über im Schulgebäude angebrachte Monitore für jeden, insbesondere auch für Besucher und Bewerber, neben dem Stundenplan auch der vollständige Name der die jeweiligen Unterrichtstunden durchführenden Lehrkräfte sichtbar war. Der Betroffene hatte der Veröffentlichung seines Vornamens gegenüber der Schulleitung schriftlich widersprochen; diese an der Praxis jedoch festgehalten.

Nach Prüfung des Anliegens habe ich dem Betroffenen mitgeteilt, dass ich die Schule grundsätzlich für befugt halte, unter automatisierter Verarbeitung von Beschäftigtendaten eine elektronische Stundenplananzeigetafel zu betreiben, die im Unterrichtsgebäude – auch wenn dieses über die Schülerschaft und Kollegen hinaus Dritten gegenüber allgemein zugänglich ist – Auskunft über die jeweiligen Unterrichtsorte, -zeiten und -inhalte verbunden mit der Person des Lehrenden gibt, da dies im Sinne eines geregelten Schulbetriebs erforderlich sein kann. Zweifel hatte ich dessen ungeachtet an der Nennung des vollständigen Vornamens; bei gleichen Nachnamen kann auch eine Abkürzung des Vornamens eine Personenunterscheidung ermöglichen. Insoweit konnte hier zwar von einem Verarbeitungsübermaß gesprochen werden, allerdings bewegte sich dieses allenfalls im Bagatellbereich, d. h. die Persönlichkeitsrechtsverletzung war in Anbetracht der Maßstäbe der Rechtsprechung zu öffentlichen Lehrerbewertungsportalen lediglich marginal.

8.9.3 Weitergabe von Informationen über Zahlungsrückstände bei Wechsel der KiTa

Die Leiterin einer Kindertagesstätte bat mich um Auskunft, ob es zulässig sei, die Leitung einer anderen Kindertagesstätte über ausstehende Elternbeiträge zu informieren, wenn das betreffende Kind in diese Kindertagesstätte wechselt.

Ich habe der Leiterin der Kindertagesstätte mitgeteilt, dass eine solche Informationsweitergabe nicht zulässig ist.

Bei Kindertagesstätten in freier Trägerschaft richtet sich die Zulässigkeit des Datenverarbeitungshandelns nach § 28 BDSG. Gemäß § 28 Abs. 1 Satz 1 BDSG ist die Übermittlung personenbezogener Daten zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist. Dass die Übermittlung von Informationen zu Beitragsrückständen für die Durchführung bzw. Beendigung des Kindertagesstättenvertrags erforderlich sein könnte, ist weder ersichtlich, noch wurde dies vorgetragen. Da auch sonst keine gesetzliche Übermittlungsbefugnis ersichtlich ist und eine Einwilligung nicht vorliegt, scheidet eine Übermittlung dieser Daten aus.

8.9.4 Offenbarungs- und Ausforschungsverbot im Zusammenhang mit Adoptionen

Von einem freien Träger der Jugendhilfe wurde ich auf folgende Problematik hingewiesen:

Der Jugendhilfeträger war Vormund zweier Kinder, die sich in der Adoptionsvermittlung befanden. Diese Kinder waren in einer Bereitschaftspflege untergebracht; aus dieser wurden sie in die Adoptionspflege entlassen. Die Adoption sollte als sogenannte Inkognito-Adoption erfolgen.

Beide Kinder waren zunächst über die Pflegemutter gesetzlich krankenversichert und sollten nunmehr über die Adoptiveltern versichert werden. Im Zuge der Abmeldung der Kinder von der Krankenversicherung hatte diese einen Nachweis über das (Fort-)Bestehen einer Absicherung im Krankheitsfall gefordert.

Pflegekinder sind nach Maßgabe des § 10 Abs. 1 Satz 1 i. V. m. Abs. 4 Satz 1 SGB V über die Pflegeeltern familienversichert. Mit Beendigung des Pflegschaftsverhältnisses endet die Eigenschaft als Kind im Sinne der vorgenannten Regelungen, sodass die Voraussetzungen der Familienversicherung entfallen, die Familienversicherung mithin endet. Bei Personen, deren Familienversicherung endet, setzt sich gemäß § 188 Abs. 4 Satz 1 SGB V die Versicherung als freiwillige Mitgliedschaft fort, wenn nicht das Mitglied innerhalb von zwei Wochen nach einem entsprechenden Hinweis der Krankenkasse seinen Austritt erklärt. Dieser Austritt wird jedoch nur dann wirksam, wenn das Bestehen eines anderweitigen Anspruchs auf Absicherung im Krankheitsfall nachgewiesen wird.

Das Offenbarungs- und Ausforschungsverbot des § 1758 Abs. 1 BGB verbietet das Offenbaren und Ausforschen von Tatsachen, die geeignet sind, die Annahme (als Kind) und ihre Umstände aufzudecken, ohne Zustimmung des Annehmenden und auch des Kindes, es sei denn, besondere Gründe des öffentlichen Interesses erfordern dies. In diesem Zusammenhang wird davon ausgegangen, dass die Offenbarung bzw. Ausforschung bereits dann zulässig ist, wenn sie für die Gesetzesanwendung erforderlich ist (vgl. Heiderhoff in jurisPK, 7. Auflage, Rdnr. 10 zu § 1758 BGB). § 188 Abs. 4 SGB V will sicherstellen, dass keine Person ohne hinreichenden Krankenversicherungsschutz ist und verlangt daher als Voraussetzung für die Wirksamkeit des Austritts aus der Krankenversicherung die Vorlage eines Nachweises über einen anderweitigen Schutz. Die Anwendung dieser Regelung erfordert eine Offenbarung bestimmter Daten.

Mit Blick auf die Schutzrichtung beider Regelungen stellt sich jedoch die Frage, welchen Umfang ein solcher Nachweis haben muss. Aufgrund des Gesetzeszwecks des § 188 Abs. 4 SGB V wird aus dem Nachweis hervorgehen müssen, dass diejenigen Personen,

deren Versicherung endet, anderweitig versichert sind. Es ist daher zu prüfen, ob der Nachname zwingend auf der Bescheinigung angegeben werden muss oder ob andere Angaben (Vorname, Geburtsdatum und Geburtsort) eine hinreichend sichere Identifizierung zulassen. So könnte die Identität des Annehmenden geschützt werden, zumal diese für die Frage, ob für die betroffenen Kinder hinreichender Krankenversicherungsschutz besteht, ohne Relevanz ist.

Soweit sich der Nachweis alternativ auch auf den Nachnamen des Kindes erstrecken und somit zugleich die Person des Annehmenden preisgeben würde, wäre sicherzustellen, dass keine dauerhafte Speicherung dieses Nachweises erfolgt, denn zur Feststellung eines hinreichenden Krankenversicherungsschutzes dürften eine Einsichtnahme in den Nachweis und ein hierzu gefertigter Aktenvermerk ausreichend sein.

8.9.5 Aufbewahrungsfristen für Fallakten bei freien Trägern der Jugendhilfe

Ein Verein als Betreiber einer Sozialeinrichtung fragte mich nach den Fristen für die Aufbewahrung seiner Fallakten.

Zunächst ist festzuhalten, dass in Bezug auf die Aufbewahrung von Fallakten bei einem freien Träger der Jugendhilfe keine speziellen landesrechtlichen Vorgaben bestehen. Auch aus den bundesgesetzlichen Regelungen des SGB VIII und des SGB X ergeben sich keine konkreten Aufbewahrungsfristen.

Die gesetzlichen Normen der Datenschutzbestimmungen des SGB VIII und SGB X gelten aufgrund der Verweisung auf § 35 SGB I zudem nur für die öffentlichen Leistungsträger und dort bezeichneten Stellen. Freie Träger der Jugendhilfe und andere Anbieter, die auf dem Gebiet der Jugendhilfe tätig sind, sind deshalb nicht unmittelbar durch die gesetzlichen Vorschriften zur Einhaltung des Datenschutzes verpflichtet. Dieses gilt wegen Art. 140 GG i. V. m. Art. 137 WRV auch für kirchliche Organisationen, obwohl diese als Körperschaften des öffentlichen Rechts eingerichtet sind. Dennoch muss vor dem Hintergrund, dass Jugendhilfeleistungen häufig durch freie Träger erbracht werden, auch innerhalb dieser Organisationen natürlich sichergestellt sein, dass ein effektiver Datenschutz gewährleistet ist.

Für die freien Träger statuiert allerdings § 61 Abs. 3 SGB VIII die Verpflichtung der öffentlichen Träger, die Einhaltung der Datenschutzbestimmungen bei der Einschaltung freier Träger sicherzustellen. Gesetzlich sind aber weder die Form noch der Umfang normiert, wie dieses zu geschehen hat. Praktisch kann dies nur durch eine Vereinbarung mit dem freien Träger erfolgen. Dabei ist aber zu beachten, dass eine pauschale Selbstverpflichtung („Wir beachten den Datenschutz!“) keinesfalls ausreichend sein kann.

Um die Sicherstellung eines umfassenden Datenschutzes gewährleisten zu können, sollte das Jugendamt als örtlicher Träger der öffentlichen Jugendhilfe den freien Träger insbesondere auch über Methoden aufklären, wie die Datenschutzbestimmungen praktisch umzusetzen sind. Ich rege daher bei derartigen Anfragen an, sich mit dem zuständigen Jugendamt in Verbindung zu setzen und dieses im Hinblick auf § 61 Abs. 3 SGB VIII aufzufordern mitzuteilen, inwieweit dort eine Aufbewahrung abgeschlossener Fallakten für zulässig erachtet wird. Im Übrigen steht meiner Auffassung nach einem analogen Rückgriff auf die Bestimmungen in § 147 AO und § 257 HGB bzw. § 10 BO der Sächsischen Landesärztekammer, die eine Aufbewahrung noch für die Dauer von zehn Jahren nach der Beendigung verlangen, nichts entgegen. Soweit eine darüber hinausgehende Aufbewahrungsfrist im Einzelfall aus Sicht des betroffenen Mitarbeiters nach seiner Einschätzung geboten erscheint (vgl. hierzu § 35 Abs. 3 BDSG), sollte anhand des jeweiligen Einzelfalls eine darüber hinausgehende Aufbewahrungsdauer festgelegt und dies dann allerdings auch dokumentiert werden.

Im Hinblick auf § 199 Abs. 2 BGB bestehen gegen eine Aufbewahrung von entsprechenden Dokumentationen in der dort festgelegten Frist keine Bedenken, wenn diese Aufzeichnungen gegebenenfalls zu Beweismittelzwecken in Haftungsfällen in Betracht kommen, um im Falle von Streitigkeiten alle durchgeführten Maßnahmen belegen zu können.

Für steuerlich relevante Unterlagen sind zudem die spezialgesetzlichen Regelungen in der Abgabenordnung zu beachten.

8.9.6 Einwilligung in die Veröffentlichung von Fotos eines Kindes durch ein Elternteil

Im Rahmen eines Babyschwimmkurses wurden Fotos der Kinder angefertigt und veröffentlicht. Zuvor hatte die Kindsmutter dies auf einem vor Ort ausliegenden Unterschriftenblatt unterschrieben.

Auf dem Blatt war der Hinweis enthalten, dass der Unterzeichner dem Fotografen mit seiner Unterschrift das Recht zur unentgeltlichen Online- und Offlinepublikation der von ihm gemachten Fotos einräumt und sich mit der redaktionellen Bearbeitung, Weiterverwendung und Nutzung für Werbezwecke in sämtlichen Medien einverstanden erklärt. Der Kindsvater, der sich an mich gewandt hatte, war der Auffassung, dass die Einwilligung seiner Frau allein für die Veröffentlichung der Fotos nicht ausgereicht habe, da auch seine Zustimmung erforderlich gewesen sei.

Ausgehend von dem vorstehend dargestellten Sachverhalt ergibt sich folgende rechtliche Bewertung:

Gemäß § 4 Abs. 1 BDSG ist eine Datenverarbeitung zulässig, wenn der Betroffene bzw. bei Kindern, deren gesetzliche Vertreter in die Datenverarbeitung einwilligen. § 4a BDSG regelt die Anforderungen an die Einwilligung des Betroffenen. Diese muss nach dessen Abs. 1 Satz 1 auf der freien Entscheidung des Betroffenen beruhen. Gemäß § 4a Abs. 1 Satz 2 BDSG ist es darüber hinaus erforderlich, dass auf den vorgesehenen Zweck hingewiesen wird. Gemäß § 4a Abs. 1 Satz 3 BDSG bedarf die Einwilligung in der Regel der Schriftform, d. h. es ist eine eigenhändige Unterschrift erforderlich.

Gemäß § 1629 Abs. 1 Satz 2 BGB vertreten die Eltern bei gemeinschaftlicher elterlicher Sorge das Kind grundsätzlich gemeinschaftlich. Haben beide Eltern das Sorgerecht, müssen grundsätzlich auch beide Eltern unterschreiben. Die Eltern können sich allerdings in Sorgerechtsangelegenheiten gegenseitig bevollmächtigen. Haben sich die Eltern in einer Sorgerechtsangelegenheit geeinigt, so kann ein Elternteil die danach erforderliche Erklärung auch für den anderen Elternteil abgeben. Bei zusammenlebenden Elternteilen wird man sich im Allgemeinen auf eine solche (stillschweigende) Ermächtigung ungefragt verlassen dürfen. Nach diesen Grundsätzen reicht bei Einigkeit der Eltern eine Unterschrift aus. Dies vorausgeschickt erachtete ich die Vorgehensweise des Fotografen als zulässig.

Auf dem ausliegenden Formular hatte die Kindsmutter ihre Einwilligung in die Veröffentlichung der Fotos des Kindes erteilt. Es war nicht erkennbar, dass diese Einwilligung nicht auf deren freier Entscheidung beruht hätte. Den Hinweis auf die geplante Veröffentlichung in Online- und Offlinemedien bzw. den Hinweis auf die geplante Nutzung in Werbemedien habe ich als ausreichend erachtet.

Auf den vom Petenten erfolgten Widerruf der von seiner Frau erteilten Einwilligung wurden die Fotos des Kindes gelöscht, sodass in diesem Zusammenhang kein weiterer Veranlassungsbedarf für meine Behörde bestand.

8.10 Energie- und Versorgungswirtschaft

8.10.1 Altpapiertonne mit Chip

Abfallentsorger versehen ihre Abfalltonnen inzwischen oftmals mit Chips. Soweit damit personenbezogene Daten erhoben werden, die für Zwecke der Entgeltberechnung erforderlich sind, bestehen dagegen in der Regel keine datenschutzrechtlichen Bedenken. Nun erhielt ich jedoch den Hinweis einer betroffenen Person, dass ein Entsorgungsunternehmen auch seine blauen Tonnen mit Chips versehen habe. Da diese Tonnen der Altpapiersammlung dienen, für deren Nutzung keine Entgelte erhoben werden, stellte sich hier die Frage der Rechtmäßigkeit einer möglichen Datenerhebung.

In seiner Stellungnahme legte das Entsorgungsunternehmen dann jedoch dar, dass mit dem Chip lediglich eine Inventarisierung der Tonnen und auch Tourenoptimierungen erfolgten. Zwar würden keine Namen erfasst, jedoch sei es für die genannten Zwecke zumindest erforderlich, die Grundstücksadressen der Tonnenstandorte im eingesetzten Behälterverwaltungsprogramm zu hinterlegen.

Das Entsorgungsunternehmen sei vertraglich gegenüber dem Landkreis verpflichtet, für die Abrechnung seiner Leistungen eine Kalkulation zur Ermittlung von Selbstkostenfestpreisen vorzulegen. In dieser Kalkulation dürfen nur betriebsnotwendige Kosten angesetzt werden. Dies betrifft sowohl die Anzahl der einsetzten Papiertonnen als auch die Anzahl der notwendigen Sammelfahrzeuge. Datengrundlage für die Tourenoptimierung sei im Wesentlichen die Anzahl der geleerten Behälter.

Gegen diese Art der Datenverarbeitung habe ich keine Einwände erhoben. Da die Grundstücksadressen ohne weiteres mit den Grundstückseigentümern in Beziehung gebracht werden können, handelt es sich zwar um personenbezogene (genauer um personenbeziehbare) Daten, jedoch begegnet deren Verarbeitung insoweit, d. h. unter den mir dargelegten Rahmenbedingungen, keinen Bedenken; die Zulässigkeit ergibt sich aus § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Eine Übersicht über die Behälterstandorte ist im Übrigen auch schon vor Einführung der Chips geführt worden und auch die Anzahl der geleerten Behälter musste aus den gleichen Gründen schon vorher – manuell – ermittelt werden.

8.10.2 Ausgabekarten für Gelbe Säcke

Aufgrund mehrerer Eingaben musste ich mich mit der Praxis eines Abfallentsorgers befassen, der Dienstleister der Dualen System Deutschland GmbH war und Gelbe Säcke nur gegen Abgabe einer ausgefüllten sogenannten Sackausgabekarte an die Endverbraucher verteilen ließ. Jeder Haushalt bekam dabei in der Regel eine Sackausgabekarte zur Verfügung gestellt. Zur Verteilung der Gelben Säcke bediente sich das Unternehmen dann privater und öffentlicher Stellen: Diese gaben gegen Vorlage der ausgefüllten Sackausgabekarte eine der Personenzahl des Haushalts entsprechende Anzahl an Rollen Gelber Säcke aus. Sie bewahrten zudem die ausgefüllten Sackausgabekarten – ohne zugrunde liegende vertragliche Regelung – auf, um diese später an den Abfallentsorger zu übergeben. Mittels der Sackausgabekarten wurden nicht nur Name und Anschrift der Endkunden, sondern auch die Anzahl der im jeweiligen Haushalt lebenden Personen abgefragt, um so die Menge an Gelben Säcken zu ermitteln, die die Sackausgabestellen verteilen durften. Der Abfallentsorger begründete dies damit, dass nur so einem Missbrauch der Gelben Säcke durch die Endkunden (z. B. zur Beseitigung von Laub) begegnet werden könne.

Ich beurteilte diese Praxis nicht nur aufgrund des Fehlens schriftlicher Auftragsdatenverarbeitungsverträge zwischen dem Abfallentsorger und den Sackausgabestellen für datenschutzwidrig.

Nach § 6 Abs. 3 Satz 1 VerpackV ist die unentgeltliche und regelmäßige Abholung gebrauchter, restentleerter Verkaufsverpackungen beim privaten Endverbraucher oder in dessen Nähe in ausreichender Weise einschränkungslos zu gewährleisten. Sie darf also nicht an Bedingungen, insbesondere eine Datenpreisgabe, geknüpft werden. Insoweit besteht also weder im Sinne von § 28 Abs. 1 Satz 1 Nr. 1 noch § 28 Abs. 1 Satz 1 Nr. 2 BDSG eine rechtlich anerkennenswerte Befugnis des Entsorgers zur Datenerhebung und Datenspeicherung. Das Risiko der Zweckentfremdung der Abholsäcke war allein dem Entsorgungsmodell des Unternehmens geschuldet, das jedoch vom Dualen System frei wählbar ist und andernorts auch ohne eine vergleichbare Datenverarbeitung auskommt. Insofern waren die Datenerhebung und Datenspeicherung mittels der Sackausgabekarten auch nicht erforderlich.

Vertretbar wäre es allenfalls gewesen, wenn Privathaushalte ihren erstmaligen Grund- und einen weitergehenden einmaligen Mehrbedarf an Gelben Säcken gegen Abhol-Wertmarken erhielten, die den Haushalten zu Beginn des Jahres als unadressierte und damit verarbeitungsfreie Postwurfsendung mit der Tagespost oder über Zeitungen zugestellt werden. Sollten einzelne Endkunden darüber hinaus einen weiteren Mehrbedarf geltend machen, halte ich die mit einer Zusendung (Internet- und/oder Telefonbestellung) verbundene Erhebung und Verarbeitung der Daten des Bestellers, also Name, Adresse und Bestellanliegen, für zulässig, soweit diese Daten ausschließlich in Abwicklung des Bestell- und Versandvorgangs verarbeitet und sodann gelöscht werden. Die Haushaltsgröße darf nicht erfragt werden, da dem Abfallentsorger insoweit die rechtliche Ermächtigung für Plausibilitätskontrollen fehlt. Nach meiner Kenntnis wird andernorts der Zweckentfremdung dadurch begegnet, dass je Mehrbedarfs-Bestellung immer nur eine Rolle angefordert werden kann.

Das Unternehmen erklärte sich mir gegenüber zunächst bereit, zukünftig auf personenbezogene Sackausgabekarten zu verzichten und das System auf Abholwertmarken umzustellen. Nachdem es jedoch – wie erneute Eingaben von Bürgern der betroffenen Gemeinden zeigten – auch nach einer angemessenen Frist die geschilderte Praxis unverändert fortsetzte, habe ich gemäß § 38 Abs. 1 Satz 6 BDSG Anzeige bei der zuständigen Ordnungswidrigkeitenbehörde erstattet.

8.11 Freizeiteinrichtungen

8.11.1 Kletterhalle: Speicherung von Nutzungs- und Konsumdaten

Die Nutzerin einer Kletterhalle wandte sich an mich und trug vor, dass der Betreiber über Jahre hinweg in einer Kundendatenbank nicht nur speicherte, wann sie die Kletterhalle oder den Wellnessbereich besucht, sondern auch, was sie dort jeweils konsumiert oder gekauft hatte. Die Nutzerin gab an, dass sie die Eintritte und Waren stets bar bezahlt hatte und fragte sich, ob der Betreiber diese Bargeschäfte – ohne ihr ausdrückliches schriftliches Einverständnis – elektronisch erfassen und speichern durfte.

Auf mein Auskunftsersuchen teilte mir der Betreiber der Kletterhalle mit, dass er die Daten auch bar bezahlter Geschäftsvorfälle für die Dauer von zehn Jahren erfasste und speicherte, weil buchhalterische Erfordernisse und steuerliche Vorschriften ein kundenbezogenes Erfassen sämtlicher verkaufter Produkte und Dienstleistungen im Kassensystem gebieten. Das Kassensystem sähe einen Workflow vor, bei dem Kunden zunächst eingecheckt und danach die von ihnen bezahlten Produkte und Dienstleistungen erfasst werden. Zudem sei Klettern ein gefahrgeneigter Sport: Die Kletterhalle müsse anhand der Buchungshistorie individuelle Risiken, die sich aus den Fähigkeiten der jeweiligen Kunden ergeben, beurteilen und entsprechend des Risikoprofils des Kunden Dienstleistungen anbieten können; im Schadensfall müsse man auf die Daten zu Nachweiszwecken zurückgreifen können. Jeder Neukunde müsse eine schriftliche Erklärung vorlegen, dass er die Benutzerordnung, die Allgemeinen Geschäftsbedingungen und die Datenschutzerklärung anerkenne. Der Betreiber der Kletterhalle war insofern auch der Ansicht, dass die Datenerhebungen und Datenverarbeitungen auf der Grundlage wirksamer Einwilligungen der Kunden erfolgten.

Wirksame, d. h. informierte schriftliche *Einwilligungen* der Kunden im Sinne des § 4a BDSG konnte ich allerdings zum Zeitpunkt der Kontrolle nicht feststellen. Der Hinweis auf die Einbeziehung der Allgemeinen Geschäftsbedingungen der Kletterhalle war datenschutzrechtlich unerheblich, da gemäß der darin enthaltenen Datenschutzerklärung die personenbezogenen Daten der Kunden ausschließlich zur Abwicklung des Vertrags verwendet werden sollten. Die Kunden konnten daraus weder erkennen, dass sämtliche auch bar abgewickelten Geschäftsvorfälle für die Dauer von zehn Jahren als individuelle Kundenhistorie gespeichert wurden, noch was der Betreiber mit diesen Daten tat. Die Datenschutzerklärung schloss dies vielmehr aus. Zudem ist die zivilrechtliche Wirksamkeit derartiger Klauseln zu Datenverarbeitungen zweifelhaft (siehe Urteil des LG Koblenz vom 19. Dezember 2013 – 3 O 205/13, juris).

Die 10-jährige Speicherung der *kletterunspezifischen Geschäftsvorfälle* (z. B. konsumierte Getränke, Speisen, Wellnessbereich, Verkäufe) hielt ich für datenschutzwidrig,

denn sie ließen sich nicht auf § 28 Abs. 1 Satz 1 Nr. 1 oder Nr. 2 BDSG stützen. Weder waren sie zur Durchführung des rechtsgeschäftlichen Schuldverhältnisses mit den Kunden (dieses war mit der Bezahlung und Übergabe der Ware erledigt; Gewährleistungsansprüche konnten auf der Grundlage des Kassenbons abgewickelt werden) noch zur Wahrnehmung berechtigter Interessen des Betreibers der Kletterhalle erforderlich. Außerdem überwog das schutzwürdige Interesse der Kunden an dem Ausschluss der Verarbeitung und Nutzung. Die eingesetzte Software hatte Funktionalitäten, die es dem Betreiber der Kletterhalle ermöglichten, anhand der über Jahre hinweg erfassten Konsumentendaten Profile der Kunden zu erstellen und auszuwerten, ohne dass die Kunden hiervon überhaupt Kenntnis hatten. Dies beurteilte ich – nicht zuletzt wegen des erheblichen Missbrauchspotentials solcher elektronischer Datensammlungen, auf die auch alle Mitarbeiter zugreifen konnten – als einen schwerwiegenden Eingriff in das Recht der Kunden auf informationelle Selbstbestimmung, der nicht durch überwiegende berechtigte Interessen der Kletterhalle gerechtfertigt werden konnte.

Entgegen der Ansicht des Betreibers der Kletterhalle gebieten es die Grundsätze ordnungsgemäßer Buchführung oder steuerliche Vorschriften nicht, namentlich in einer Datenbank des Kassensystems erfassten Kunden einzelne, bar bezahlte Geschäftsvorfälle, wie konsumierte Getränke und Speisen sowie Verkäufe zuzuordnen. Denn anderenfalls müsste jeder Gastronom, jedes Kaufhaus oder jedes Schwimmbad an der Kasse nach den Personalien der Kunden fragen. Der Betreiber der Kletterhalle berief sich insofern auf die Rechtsprechung des Bundesfinanzhofs (Urteil vom 16. Dezember 2014 – X R 42/13, juris), woraus entsprechende Pflichten resultieren würden.

Entgegen der Ansicht des Betreibers der Kletterhalle ergab sich aus dem Urteil des Bundesfinanzhofs jedoch keine gesetzliche Pflicht zu der von der Kletterhalle praktizierten kundenbezogenen Einzelaufzeichnung der baren Geschäftsvorfälle. Nur dann, wenn sich der Steuerpflichtige – freiwillig – dafür entscheidet, ein entsprechendes Kassensystem einzusetzen, kann er sich gegenüber der Finanzverwaltung bei einer Steuerprüfung nicht mehr auf die Unzumutbarkeit der Aufzeichnungsverpflichtung berufen (d. h., er ist verpflichtet, die Datenbestände für zehn Jahre vorzuhalten und zugänglich zu machen). Insofern hinderte mich die Rechtsprechung des Bundesfinanzhofs daran, von dem Betreiber (trotz der datenschutzrechtlichen Unzulässigkeit der Erhebung und Verarbeitung der Kundendaten) für die zurückliegenden Geschäftsjahre eine Löschung des Datenbestands zu verlangen. Ich konnte von der Kletterhalle nur verlangen, die betroffenen Datenbestände gemäß § 35 Abs. 3 Nr. 1 BDSG zu sperren.

Zur Notwendigkeit, *kletterspezifische Geschäftsvorfälle* (Eintritte, Kurse) längerfristig speichern zu müssen, berief sich der Betreiber der Kletterhalle darauf, dass er so bei eventuellen Schadensfällen einen Nachweis über erfolgte Belehrungen zur Nutzung der

Kletterhalle erbringen und anhand der Häufigkeit der Besuche die jeweiligen Fähigkeiten der Anspruchssteller belegen könne.

Die bloßen Buchungen der Klettereintritte auf den jeweiligen Kunden besagen jedoch nichts darüber aus, ob die Kunden über die Kletterregeln belehrt wurden, sodass die Datenverarbeitungen zur Zweckerreichung insoweit bereits ungeeignet waren. Dementsprechend trug der Betreiber auch ergänzend vor, dass jeder Kunde, bevor er erstmals Leistungen in der Klettersporthalle in Anspruch nahm, mittels Unterschrift sein Einverständnis zu den im Rahmen der Benutzerordnung aufgestellten Kletterregeln gab.

Wenn diese Einwilligungen in die Benutzerordnung schriftlich eingeholt und aufbewahrt werden, ist eine ergänzende elektronische Speicherung der danach in Anspruch genommenen Kletterdienstleistungen für den angegebenen Zweck (Nachweis der Erfüllung der Verkehrssicherungspflicht) jedoch nicht erforderlich. Diese Belehrungen und Bestätigungen können dabei regelmäßig schriftlich wiederholt werden. Ausschließlich diese Dokumente, nicht jedoch die in dem Kassensystem vorgehaltenen Geschäftsvorfälle, nämlich dass bestimmte Kletterdienstleistungen später erneut von diesem Kunden gebucht und bezahlt wurden, vermögen hinsichtlich der Frage, ob die Kletterhalle ihrer Verkehrssicherungspflicht im konkreten Schadensfall nachgekommen ist, weiterzuhelfen. Insofern reicht es folglich aus, wenn der Betreiber der Kletterhalle einen Nachweis über erfolgte Belehrungen und die Anerkennung der Benutzerordnung kundenspezifisch für die Dauer von maximal drei Jahren nach Abschluss des jeweiligen Geschäftsjahrs (§ 195 BGB) speichert.

Zustimmen konnte ich dem Betreiber der Kletterhalle jedoch insofern, als sich anhand der individualisierten Buchung der Klettereintritte und besuchten Kurse im Schadensfall nachweisen ließ, welche Fähigkeiten der verunfallte Kunde hatte. Insofern lag ein berechtigtes Interesse der Kletterhalle an entsprechenden Datenverarbeitungen vor (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG); diese waren jedoch aufgrund der Ausgestaltung der Zugriffsrechte und der Speicherdauer von zehn Jahren unverhältnismäßig.

Im Verlauf des Aufsichtsverfahrens überarbeitete der Betreiber die Sicherheitserklärung und die Allgemeinen Geschäftsbedingungen der Kletterhalle einschließlich der Datenschutzerklärung. Ich wies ihn darauf hin, dass diese vor allem im Hinblick auf die Datenkategorien, die Datenverarbeitungszwecke und die Speicherfristen sowie den Auskunftsanspruch der Kunden nach § 34 BDSG konkreter gefasst werden musste.

Trotz der erheblichen Risiken, die mit einer *Einwilligungslösung* verbunden sind, beharrte der Betreiber darauf, die Datenerhebung, -verarbeitung und -nutzung auf Einwilligungen seiner Kunden zu stützen. Die Einwilligung kann jederzeit mit Wirkung für die

Zukunft widerrufen werden, mit der Folge, dass die Kletterhalle dann wohl die Geschäftsbeziehung mit dem Kunden partiell beenden muss. Ich wies darauf hin, dass eine wirksame, informierte Einwilligung voraussetzt, dass die Kunden wissen, worin sie einwilligen sollen. D. h. der Betreiber muss im Einzelnen in einer schriftlichen Information definieren, welche Daten (Personalien, Anschrift, Geburtsdatum, Telefonnummer, E-Mail-Adresse, Eintritte, Getränke, Speisen, Wellnessbereich, Einkäufe von Sportartikeln) er zu welchen Zwecken wie lange speichert, wo er die Daten speichert und wer darauf Zugriff hat und an wen die Daten weitergegeben werden. Soll die datenschutzrechtliche Einwilligung in Verbindung mit anderen Erklärungen abgegeben werden, muss sie drucktechnisch abgehoben werden (§ 4a Abs. 1 Satz 4 BDSG). Bedenken im Hinblick auf die datenschutzrechtliche Wirksamkeit der Einwilligungserklärung bestanden auch, weil der Betreiber seinen Kunden suggerierte, dass diese jederzeit die Löschung der erhobenen personenbezogenen Daten verlangen können, was nicht der Fall ist, weil er dadurch steuerrechtliche Aufbewahrungsfristen verletzen würde.

Nach Ankündigung einer datenschutzrechtlichen Anordnung gemäß § 38 Abs. 5 Satz 1 BDSG und Gesprächen mit dem Entwickler der Kassensoftware wird diese zeitnah angepasst, um einen datenschutzkonformen Einsatz in der Kletterhalle zu gewährleisten. Prämisse der Anpassungen war, dass die zugrundeliegenden Buchungen personenbezogen für steuerliche Prüfungen weiterhin zur Verfügung stehen, jedoch die Zugriffsrechte (Anzeige) entsprechend der datenschutzrechtlichen Anforderung des § 35 Abs. 2 Satz 2 Nr. 3, Abs. 2 Nr. 1 und Nr. 2 BDSG begrenzt werden (Sperrung im Sinne des § 3 Abs. 4 Satz 2 Nr. 4 BDSG). Die Datensätze/Buchungen bleiben dabei an sich unverändert; nur der Zugriff ist beschränkt auf die in § 35 Abs. 8 BDSG aufgeführten Fälle. Im Übrigen waren die berechtigten Interessen des Betreibers der Kletterhalle und der Kunden umfassend abzuwägen (§ 28 Abs. 1 BDSG) mit folgendem Ergebnis:

Aufgrund der Gefahrgeneigtheit der Kletterdienstleistungen und des berechtigten Interesses des Betreibers der Kletterhalle überprüfen zu können, ob die Angaben des Kunden zu seinen Kletterkenntnissen und Kletterfähigkeiten plausibel sind, bestand die Notwendigkeit, für kletterspezifische Buchungsvorgänge einerseits, und sonstige angebotene Leistungen (insbesondere Wellnessbereich, Verkauf von Getränken, Speisen und sonstigen Waren) andererseits, unterschiedliche Fristen festzulegen, nach denen bestimmte Buchungsvorgänge nicht mehr personenbezogen angezeigt werden. In der kundenbezogenen Buchungshistorie werden kletterspezifische Leistungen nicht mehr angezeigt, wenn sie älter als 24 Monate; die kletterunspezifischen Leistungen, wenn sie älter als sechs Monate (= reguläre Verjährungsfrist der Mängelrechte bei Kaufverträgen gemäß § 438 Abs. 1 Nr. 3 BGB) sind. Buchungen im Kassenbestand werden nach sechs Monaten

nicht mehr angezeigt. In der Transaktionsstatistik werden Buchungen, die in einem Geschäftsjahr anfallen, nur für die Dauer von drei Jahren nach Abschluss dieses Geschäftsjahrs (= regelmäßige Verjährungsfrist gemäß § 195 BGB) personenbezogen angezeigt. Die Zugriffsrechte werden im Einzelnen durch Festlegung von Benutzerkategorien definiert.

Von der Umsetzung dieser Vorgaben werde ich mich im Rahmen einer Nachkontrolle überzeugen.

8.12 Verkehrs- und Beförderungswesen

8.12.1 Benennung des Arztes auf Freifahrtbescheinigungen

Ein Verkehrsunternehmen stellte an Personen, die ein Fahrrad als orthopädisches Hilfsmittel zur Fortbewegung benötigten, Bescheinigungen zur unentgeltlichen Fahrradmitnahme aus. Bei der Antragstellung mussten diese Personen einen entsprechenden Nachweis erbringen. Das Unternehmen hatte daher auf den Bescheinigungen eine Textzeile „ärztliche Bescheinigung ausgestellt:“ vorgesehen, hinter der die namentliche Nennung des Arztes erfolgte.

Ein betroffener Fahrgast wandte sich an mich mit der Bitte um Prüfung dieser Praxis. Er fühlte sich in seiner Privatsphäre verletzt, da so jeder Kontrolleur sehen könne, bei welchem Arzt er in Behandlung ist.

Die genannte Praxis wäre nur auf Basis von Einwilligungen der Betroffenen (Arzt und Fahrgast) gemäß § 4a BDSG oder einer anderen Rechtsgrundlage zulässig gewesen. Beides war hier jedoch nicht gegeben. Es lagen weder entsprechende Einwilligungen vor noch waren die grundsätzlich in Betracht kommenden Vorschriften des § 28 Abs. 1 Nr. 1 und 2 BDSG (Datenerhebung und Speicherung für eigene Geschäftszwecke) anwendbar. Denn hierfür fehlte es bereits erkennbar an der Erforderlichkeit der namentlichen Nennung des Arztes auf der Bescheinigung.

Das Unternehmen nahm den Fall zum Anlass, seine bisherige Praxis zu überprüfen. Im Ergebnis nahm es von der Nennung des Arztes auf den Bescheinigungen Abstand und teilte mir mit, auch alle bereits ausgestellten Bescheinigungen im Nachgang entsprechend ändern bzw. austauschen zu wollen.

8.13 Rechtsanwälte

8.13.1 Übermittlung von Schriftsätzen per E-Mail

Auch Rechtsanwälte, mit denen ich es in meiner Aufsichtspraxis recht häufig zu tun habe, stehen unter Zeit- und Kostendruck und versuchen daher gelegentlich die Kommunikation mit meiner Behörde unkonventionell per E-Mail abzuwickeln.

Ich betrachte den unverschlüsselten E-Mail-Versand von Schriftsätzen vor dem Hintergrund des § 203 StGB insbesondere bei Rechtsanwälten als eine absolut ungeeignete Kommunikationsform. § 203 StGB schützt die Individualinteressen Betroffener in besonderer Weise dadurch, dass er Geheimnisträgern wie Rechtsanwälten, denen Betroffene im Rahmen der Mandatserteilung regelmäßig Geheimnisse anvertrauen, für den Fall der Verletzung ihrer Geheimhaltungs- und Verschwiegenheitspflichten entsprechende Strafen androht. Soweit und solange sich also Rechtsanwälte nicht nur mit allgemeinen Fragestellungen oder Anliegen an die Aufsichtsbehörde wenden, sondern die Aufsichtsbehörde in Ausübung eines konkreten Mandats eines Betroffenen kontaktieren und dabei mandantenbezogene bzw. mandantenbeziehbare Äußerungen und Stellungnahmen tätigen, ist wegen des hohen Schutzbedarfes der Kommunikationsinhalte in jedem Fall eine Verschlüsselung des E-Mail-Verkehrs erforderlich.

Der unverschlüsselte E-Mail-Versand widerspricht auch den Vorgaben der Nr. 4 der Anlage zu § 9 BDSG, wonach zu gewährleisten ist, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Satz 3 der Anlage zu § 9 BDSG ist insoweit zu entnehmen, dass dies auch durch Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren realisierbar ist.

Ich gehe daher davon aus bzw. fordere dies gegebenenfalls, dass Rechtsanwälte ihre E-Mails zukünftig verschlüsseln oder aber ihre Schriftsätze per Fax und/oder Briefpost versenden. Für Ersteres habe ich einen Zugang für mit PGP verschlüsselte E-Mails eröffnet (vgl. § 2 Abs. 1 Sätze 1 und 3 SächsEGovG). Zu beachten ist dabei, dass auch die – unverschlüsselte – Angabe des Betreffs keine personenbezogenen Daten enthalten darf.

Es wird beobachtet werden müssen, ob und in welcher Weise der elektronische Rechtsverkehr von und mit Behörden bzw. von und mit Rechtsanwälten zukünftig noch konkreter geregelt wird.

8.13.2 Offene Lagerung von Handakten

Im Berichtszeitraum besonders erwähnenswert sind zwei Fälle, in denen Rechtsanwälte recht sorglos mit Mandantenunterlagen umgingen. In einem Fall lagerte ein Rechtsanwalt Handakten in unverschlossenen Aktenschränken, die sich in den Geschäftsräumen eines befreundeten Unternehmers in Bereichen befanden, die dessen Angestellten zugänglich waren. In einem weiteren Fall stellte ein Rechtsanwalt während der Dauer eines sich über mehrere Tage hinziehenden Umzugs Handakten in unverschlossenen Kisten in den Hausflur und den Fahrstuhl eines Mehrfamilienhauses.

Auch in solchen Fällen bin ich zu einer Kontrolle befugt, denn die Subsidiaritätsklausel des § 1 Abs. 3 Satz 1 BDSG greift nicht: Trotz der anwaltlichen Verschwiegenheitspflichten verdrängen die Vorschriften der Bundesrechtsanwaltsordnung nicht allgemein das Bundesdatenschutzgesetz. Denn die Vorschriften des Bundesdatenschutzgesetzes sind nicht mit denen der Bundesrechtsanwaltsordnung identisch, schützen sie doch über die Vertraulichkeit des Verhältnisses Mandant und Rechtsanwalt hinaus auch die personenbezogenen Daten der am Mandatsverhältnis unbeteiligten Dritten. Dies gilt insbesondere auch dann, wenn sich die Aufsichtsverfahren – wie hier – ausschließlich auf Fragen des technisch-organisatorischen Datenschutzes in einer Rechtsanwaltskanzlei beschränkt.

Beide Rechtsanwälte hatten mit ihrem Verhalten die in den Handakten enthaltenen personenbezogenen Daten unbefugt verarbeitet (und damit den Bußgeldtatbestand des § 43 Abs. 2 Nr. 1 BDSG verwirklicht). Denn sie haben diese personenbezogenen Daten Dritten, nämlich einerseits dem Unternehmer und dessen Mitarbeitern andererseits den Mietern und deren Besuchern, durch die offene Lagerung im Sinne des § 3 Abs. 4 Satz 1 und Satz 2 Nr. 3a BDSG übermittelt. Danach ist Übermitteln das Bekanntgeben gespeicherter personenbezogener Daten an einen Dritten in der Weise, das die Daten an den Dritten weitergegeben werden. „Weitergeben“ ist nach dem Gesetzeszweck jede finale Handlung, durch die die in den Akten enthaltenen Informationen in den Bereich eines Dritten gelangen. Weitergegeben sind die personenbezogenen Daten dabei in dem Moment, in dem Dritte die Möglichkeit haben, unabhängig vom Weitergebenden die Informationen zur Kenntnis zu nehmen. Ob sie dies tatsächlich tun, ist unerheblich (vgl. Dammann in Simitis, BDSG, 8. Auflage, § 3 Rdnr. 146 m. w. N.).

Beide Rechtsanwälte haben den datenschutzwidrigen Zustand unverzüglich abgestellt, weshalb ich auch von einer Ordnungswidrigkeitenanzeige abgesehen habe.

8.14 Unternehmensübergänge

8.14.1 Übertragung von Kundendatenbanken im Wege eines Asset Deals

Im Zuge von Unternehmensinsolvenzen oder Unternehmensumstrukturierungen stellt sich die Frage, wie die in Datenbanken gesammelten personenbezogenen Kundendaten (Personalien, Anschriften, E-Mail-Adressen, Telefonnummern, Buchungshistorie, laufende Geschäftsvorfälle, Bankdaten) datenschutzgerecht übertragen werden können. In den an mich herangetragenen Fällen waren diese Kundendatenbanken ein bzw. das entscheidende vermögenswerte Gut der Unternehmen und sollten an eine Erwerbergesellschaft bzw. die neu gegründete Tochtergesellschaft durch Veräußerung der Kundendatenbank, d. h. im Wege eines Asset Deals übertragen werden.

Die beteiligten Unternehmen (meist Gesellschaften) sind im Verhältnis zueinander Dritte (§ 3 Abs. 8 Satz 2 und 3 BDSG). Datenschutzrechtlich handelt es sich deshalb bei der Veräußerung der Kundendatenbank um eine Datenverarbeitung: auf Seiten des Veräußerers in Form der Datenübermittlung (§ 3 Abs. 4 Satz 2 Nr. 3 BDSG), auf Seiten des Erwerbers in Form des Speicherns (§ 3 Abs. 4 Satz 2 Nr. 1 BDSG) verbunden mit einer Datennutzung (§ 3 Abs. 5 BDSG). Anders wäre es nur dann, wenn die Kundendatenbank bei der (insolventen) Gesellschaft verbleibt und nur deren Gesellschafter wechseln (Share Deal).

Um datenschutzkonform zu sein, bedürfen diese Datenverarbeitungen einer gesetzlichen Rechtsgrundlage oder die betroffenen Kunden müssen, bevor der Erwerber Zugriff auf die Kundendatenbank erhält, wirksam hierin einwilligen (§ 4 Abs. 1 BDSG). Insbesondere Insolvenzverwalter wollen die Einholung von Einwilligungen der Kunden jedoch gern vermeiden. Dabei spielen wirtschaftliche Erwägungen eine entscheidende Rolle, weil es für die Veräußerer und Erwerber kaum kalkulierbar ist, ob die Kunden auf die entsprechenden Informationsschreiben überhaupt reagieren und falls ja, ob sie zustimmen. Dieses Risiko wirkt sich dementsprechend auf den Kaufpreis aus. Hinzu kommen praktische Erwägungen, wie man eine solche Einwilligungslösung technisch ohne großen finanziellen Aufwand umsetzen kann.

Einwilligungslösung

Ich halte die Einwilligungslösung, was ich den betroffenen Unternehmen auch mitgeteilt habe, aus datenschutzrechtlicher Sicht grundsätzlich für vorzugswürdig: Nur sie gewährleistet letztlich, dass die Kunden – umfassend informiert – selbst darüber entscheiden können, ob sie die Vertragsbeziehung mit einem neuen Anbieter fortsetzen oder letztlich von der Inanspruchnahme der angebotenen Leistungen (wegen Wegfall des Verkäuferunternehmens) zukünftig absehen wollen. Sie bietet den beteiligten Unternehmen auch

Rechtssicherheit, weil auf diese Weise die Zulässigkeit der Verwendung der Kundendaten durch den Erwerber für Werbezwecke (§ 7 Abs. 3 UWG) eindeutig geklärt werden kann.

Ein Unternehmen, das Geschäfte per Onlineshop abwickelte, und seine Firmengruppe restrukturierte, schloss sich meiner Auffassung auch an. Es informierte seine Kunden im Zuge neuer Bestellvorgänge umfassend und holte entsprechende elektronische Einwilligungserklärungen ein. Aufgrund der Tatsache, dass den Kunden bekannt war, dass der Bestellvorgang grundsätzlich per Internet oder telefonisch abgewickelt wurde, hielt ich die ansonsten gemäß § 4a Abs. 1 Satz 3 BDSG erforderliche Schriftform (§§ 126, 126a BGB) aufgrund der Gesamtumstände für entbehrlich. Ich empfahl dem Unternehmen, die auf elektronischem Wege erteilten Einwilligungen in Anlehnung an die Bestimmungen des § 28 Abs. 3a BDSG zu protokollieren und sicherzustellen, dass die Kunden deren Inhalt jederzeit abrufen und die Einwilligung mit Wirkung für die Zukunft widerrufen können. Bei mündlichen Einwilligungserklärungen der Kunden im Rahmen telefonischer Bestellungen verpflichtete sich das Unternehmen, den Inhalt der mündlich erteilten Einwilligung dem Kunden in Anlehnung an § 28 Abs. 3a Satz 1 BDSG schriftlich zu bestätigen und den Auftrag erst danach abzuwickeln, d. h. die Kundendaten an die neu gegründete Gesellschaft zu übertragen. Das Unternehmen sicherte zu, durch entsprechende vertragliche und technisch-organisatorische Maßnahmen sicherzustellen, dass die Datenbestände auch tatsächlich bis zur erteilten Einwilligung getrennt gespeichert wurden und kein Zugriff durch die neue Gesellschaft möglich war.

Gesetzliche Rechtsgrundlage für die Übertragung der Datenbank – Widerspruchsrecht der Kunden

In anderen Fällen wollte der Veräußerer wegen der geschilderten wirtschaftlichen Risiken nicht auf die Einwilligungslösung zurückgreifen. Die Frage war daher, ob die Übertragung der Kundendatenbank nach § 28 Abs. 1 Satz 1 Nr. 2, Abs. 2 Nr. 1 BDSG datenschutzrechtlich zulässig ist, weil der Veräußerer das berechtigte Interesse verfolgt, bei der Veräußerung der Kundendatenbank möglichst hohe Gewinne zu erzielen oder weil anderenfalls eine Umstrukturierung des Unternehmens scheitert. Die Verfolgung berechtigter Interessen allein genügt jedoch nicht, sondern die Datenübermittlung ist nur dann zulässig, wenn kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Kunden die Interessen des Unternehmens überwiegt. Erforderlich ist damit immer eine umfassende, auf den konkreten Einzelfall bezogene Interessenabwägung.

Eine Veräußerung der Kundendatenbank ohne eine vorherige Information der Kunden stellt einen erheblichen Eingriff in deren allgemeines Persönlichkeitsrecht bzw. Recht auf

informationelle Selbstbestimmung dar und wäre in jedem Fall unverhältnismäßig und datenschutzwidrig.

Das Argument, das mir entgegengehalten wurde, dass die Endkunden ein positives Interesse an der Datenübermittlung an einen (solventen) Käufer haben, der dieselben oder ähnliche Leistungen erbringt, verkennt, dass die Endkunden sich vielleicht bewusst für diesen Vertragspartner entschieden hatten und gerade nicht für den Erwerber, an den jetzt ihre personenbezogenen Daten übertragen werden sollen. Der Wechsel des Vertragspartners hat aus den unterschiedlichsten Gründen nicht für jeden Endkunden positive Effekte oder ist diesem – wie es häufig heißt – auch nicht egal. Denn weder der Veräußerer noch dessen Kunden können wissen, was der Erwerber mit den erworbenen Datenbeständen machen wird. Man kann auch nicht unterstellen, dass alle Kunden, die einmal eine bestimmte Leistung (eines Onlineshops) in Anspruch genommen haben, automatisch auch für die Zukunft ein Interesse daran haben. Vielleicht sind sie aufgrund der Gesamtumstände auch froh, dass die Vertragsbeziehung ein Ende hat.

Bei der umfassenden Interessenabwägung ist auch zu berücksichtigen, dass es einen Unterschied macht, ob die gesamte Kundendatenbank übertragen wird oder nur bestimmte Datenkategorien. Kontodaten sind missbrauchsanfälliger und damit schutzwürdiger als Anschriften, E-Mail-Adressen und Telefonnummern. Buchungshistorien sind datenschutzrechtlich sensibler, weil damit die Bildung von Profilen möglich ist. Im Ergebnis halte ich daher eine differenzierte Lösung für angebracht:

- Kontodaten und Zahlungsinformationsdaten dürfen ohne wirksame vorherige Einwilligung der Kunden dem Erwerber nicht zugänglich gemacht werden (Opt-In). Kommt es zu weiteren Geschäften mit dem Erwerber, kann dieser diese Informationen bei der Abwicklung ohne weiteres erfragen.
- Abhängig von den Umständen des jeweiligen Veräußerungsgeschäfts halte ich eine Übermittlung der Buchungshistorie ohne Einwilligung der Kunden hingegen nicht grundsätzlich für unzulässig, wenn die Kunden umfassend informiert werden und diesen rechtzeitig vor der Übertragung mit angemessener Frist ein Widerspruchsrecht eingeräumt wird (Opt-Out).
- Hinsichtlich der übrigen, grundsätzlich weniger sensiblen Kundendaten (Anschrift, E-Mail-Adresse, Telefonnummern) habe ich gegen eine Widerspruchslösung ebenfalls keine Bedenken.

Steht fest, dass Kunden die Informationen über ihr Widerspruchsrecht nicht erhalten haben (z. B. E-Mails oder Post ist unzustellbar), sind diese Datenbestände wie solche zu

behandeln, bei denen Kunden ausdrücklich einer Weitergabe an den Erwerber widersprochen haben. Die Mitteilung, mit der die Kunden über das Widerspruchsrecht informiert werden, muss transparent und umfassend sein und insbesondere deutlich machen, welche Nutzerdaten übertragen werden sollen. Der Versand der Informationen ist rechtssicher zu dokumentieren (siehe oben).

Letztlich sind die technisch-organisatorischen Maßnahmen, die der Veräußerer bei einer Widerspruchslösung ergreifen muss, um eine datenschutzgerechte Trennung und Übertragung der bereinigten Datenbestände zu gewährleisten, mit einem Aufwand verbunden, der kaum geringer ist als im Falle der Einwilligungslösung. Die Widerspruchslösung ist auch mit rechtlichen Unsicherheiten verbunden: Veräußerer und Erwerber gehen jedenfalls in all den Fällen erhebliche Risiken ein, in denen der Nachweis nicht gelingt, dass den Kunden die Information über das Widerspruchsrecht zugegangen ist.

Abschließend der Hinweis, dass die Widerspruchslösung auch nicht gilt, soweit es um die Frage der Zulässigkeit von Werbung geht. Eine Verwendung von E-Mail-Adressen und Telefonnummern der Kunden durch den Erwerber für Werbezwecke muss sich an den Bestimmungen des Gesetzes gegen den unlauteren Wettbewerb messen lassen, d. h. sie wäre grundsätzlich ohne ausdrückliche Werbeeinwilligung des Kunden rechtswidrig.

8.15 Religionsgemeinschaften

8.15.1 Kontrollzuständigkeit bei kirchennahen Stellen

Im Oktober 2014 hat sich das Bundesverfassungsgericht (Beschluss vom 22. Oktober 2014 – 2 BvR 661/12, juris) zu der – deswegen bedeutsamen Frage, weil sich danach meine Aufsichtsbefugnis richtet – Thematik geäußert, inwieweit privatwirtschaftliche Bereiche der Kirchen deren Selbstverwaltung unterfallen. Träger des kirchlichen Selbstbestimmungsrechts sind nach dieser Entscheidung nicht nur die Kirchen selbst, sondern alle ihr zugeordneten Institutionen, Gesellschaften, Organisationen und Einrichtungen, wenn und soweit sie nach dem glaubensdefinierten Selbstverständnis der Kirchen entsprechend ihrem Zweck oder ihrer Aufgabe berufen sind, Auftrag und Sendung der Kirchen wahrzunehmen und zu erfüllen. Dies gilt unbeschadet der Rechtsform der einzelnen Einrichtung auch dann, wenn der kirchliche Träger sich privatrechtlicher Organisationsformen bedient. Die Kirchen können die jedermann offen stehenden privatautonomen Gestaltungsformen nutzen, Dienstverhältnisse begründen und nach ihrem Selbstverständnis ausgestalten. Allein ganz überwiegend der Gewinnerzielung dienende Organisationen und Einrichtungen können das Privileg der Selbstbestimmung nicht in Anspruch nehmen, da bei ihnen der enge Konnex zum glaubensdefinierten Selbstverständnis aufgehoben ist.

Gemessen hieran handelt es sich etwa bei durch privatrechtlich organisierten Stellen, betriebenen Verlagen, Online-Shops oder sonstigen Unternehmungen im Allgemeinen um mittelbare kirchliche bzw. kirchennahe Einrichtungen, die wegen des in Art. 137 Abs. 3 Satz 1 WRV (anwendbar über Art. 140 GG) verfassungsrechtlich verbrieften kirchlichen Selbstverwaltungsrechts eigenem Datenschutzrecht und der datenschutzrechtlichen Selbstkontrolle unterliegen. Demgemäß ist mir eine Kontrolle dieser Stellen von Verfassungs wegen entzogen. Ich vermag Petenten daher in diesen Fällen nur an die Datenschutzbeauftragten der jeweiligen Religionsgemeinschaft zu verweisen.

8.16 Betrieblicher Datenschutzbeauftragter

8.16.1 Unterlassene Bestellungen

Wenn ich mich im Rahmen meiner anlassbedingten Aufsichtstätigkeit an eine verantwortliche Stelle wende, frage ich regelmäßig auch ab, ob ein betrieblicher Datenschutzbeauftragter bestellt ist. Zudem bitte ich um Auskunft, wie viele Mitarbeiter insgesamt bei diesem Unternehmen beschäftigt sind und wie viele davon tätigkeitsbedingt (auch) mit personenbezogenen Daten umgehen (§ 4f Abs. 1 Satz 4 BDSG). Nach wie vor stelle ich dabei sehr häufig – quasi als Nebenerkenntnis (vgl. dazu auch Pkt. 8.17.1) – Verstöße gegen die Bestellungspflicht fest. Die betreffenden Unternehmen müssen dann mit der Einleitung eines Ordnungswidrigkeitenverfahrens rechnen.

Oft wird dies allerdings erst nach entsprechendem Nachfassen deutlich, denn zunächst wird mir zumeist nur eine kleine Anzahl von Mitarbeitern genannt, die personenbezogene Daten verarbeiten. Die Unternehmen beziehen diese Frage häufig nur auf die reine Personaldatenverarbeitung und übersehen dabei, dass auch an vielen anderen Stellen im Unternehmen personenbezogene Daten erhoben, verarbeitet und genutzt werden, so etwa von Kunden, Lieferanten, Geschäftspartnern oder Gesellschaftern. Um derartige Fehlverständnisse des Datenschutzrechts zu erkennen, ist zunächst ein Abgleich der angegebenen Mitarbeiterzahl mit der Gesamtbeschäftigtenzahl hilfreich, sodann frage ich noch ab, wie viele Mitarbeiter überhaupt in der Verwaltung des Unternehmens tätig sind bzw. lasse mir eine funktionsbezogene Mitarbeiterübersicht vorlegen. Denn 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).

8.16.2 Bekanntgabe der Kontaktdaten des Datenschutzbeauftragten

Aus der Belegschaft eines Unternehmens war mir mitgeteilt worden, dass dort nicht bekannt und auch nicht in Erfahrung zu bringen sei, wer aktuell als betrieblicher Datenschutzbeauftragter bestellt und wie er zu erreichen ist. Noch nicht einmal der Betriebsrat sei in der Lage, diese Person zu benennen.

Nach § 4f Abs. 5 Satz 2 BDSG können sich Betroffene – und dazu gehören auch und vor allem die Mitarbeiter – jederzeit an den betrieblichen Datenschutzbeauftragten wenden. Wenn ein Geschäftsführer seiner Belegschaft allerdings keinerlei Informationen über die Person des betrieblichen Datenschutzbeauftragten zur Verfügung stellt, untergräbt er dieses Anrufungsrecht. Den Betroffenen ist auch nicht zuzumuten, sich über die Geschäftsführung oder andere Leitungspersonen an den betrieblichen Datenschutzbeauftragten zu wenden, denn dies wiederum läuft den nach § 4f Abs. 4 BDSG bestehenden Verschwiegenheitspflichten des betrieblichen Datenschutzbeauftragten zuwider. § 4f Abs. 5 Satz 2 BDSG gewährleistet also nicht nur den Zugang zum Beauftragten, sondern schließt auch Umwege aus, die den Betroffenen die Möglichkeit nehmen könnte, den Beauftragten ebenso schnell wie vertraulich anzurufen (vgl. Simitis, BDSG, 8. Auflage, Rdnr. 161 zu § 4f). Nicht zuletzt nährt eine mangelnde Kommunikation der Kontaktdetails des betrieblichen Datenschutzbeauftragten auch Zweifel an dessen Zuverlässigkeit, denn sie suggeriert, dass dieser nicht wirklich gewillt ist, seinen diesbezüglichen Aufgaben nachzukommen.

Es ist auch nicht Aufgabe des Betriebsrats, dafür zu sorgen, dass innerhalb des Unternehmens bekanntgemacht wird, wer als betrieblicher Datenschutzbeauftragter bestellt worden und wie er zu erreichen ist.

Ich habe daher an das Unternehmen die Forderung herangetragen, umgehend geeignete Maßnahmen zu treffen, die eine diesbezügliche Information der Belegschaft bewirken. Der Geschäftsführer hat dafür zu sorgen, dass diese Information allen Mitarbeitern jederzeit zur Verfügung steht, beispielsweise durch Veröffentlichung im Intranet, am Schwarzen Brett oder im innerbetrieblichen Telefonbuch.

8.17 Technische und organisatorische Maßnahmen

8.17.1 Verpflichtung auf das Datengeheimnis

Auch die Kontrolle der vorgenommenen Verpflichtung auf das Datengeheimnis ist regelmäßiger Bestandteil meiner Anlasskontrollen. Immer wieder stelle ich dabei entsprechende Mängel fest. So die Voraussetzungen für die Bestellung eines betrieblichen Datenschutzbeauftragten erfüllt sind, korrespondieren unterlassene Verpflichtungen auf das

Datengeheimnis zumeist auch mit einem Verstoß gegen die Bestellungspflicht (vgl. Pkt. 8.16.1).

Gemäß § 5 BDSG ist es den bei der Datenverarbeitung beschäftigten Personen untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Die genannten Personen sind bei Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten.

Das Datengeheimnis geht somit weit über eine bloße Verschwiegenheitspflicht hinaus, da es das gesetzliche Verbot jedweder unbefugten Verarbeitung und Nutzung enthält, d. h. ein Verstoß impliziert nicht notwendigerweise auch einen Bruch bestehender Verschwiegenheitspflichten. Die von verantwortlichen Stellen häufig in die Arbeitsverträge eingestellte Verschwiegenheitsklausel reicht demnach nicht aus, um den Anforderungen des § 5 BDSG zu entsprechen. Unter das dem Datengeheimnis zugrunde liegende Verbot fallen beispielsweise auch Auswertungen für private Zwecke sowie unbefugte Zugriffe (Einsichtnahmen), Datenveränderungen (Manipulationen) oder auch Löschungen.

Auch wenn § 5 BDSG keine schriftliche Verpflichtung fordert, ist jeder Unternehmer gut beraten, wenn er eine solche einholt. Dies erleichtert einerseits den gegebenenfalls gegenüber der Aufsichtsbehörde erforderlichen Nachweis der vorgenommenen Verpflichtung, andererseits sichert sich der Unternehmer damit gegenüber individuellem Fehlverhalten seiner Mitarbeiter ab. Das Original der Erklärung sollte zu den Personalunterlagen genommen werden, der Verpflichtete eine Kopie erhalten.

Ein Muster einer solchen Verpflichtungserklärung halte ich auf meiner Website zum Abruf bereit.

8.18 Kurioses aus der Aufsichtstätigkeit

Beschwerden über einen E-Mail-Versand mit offenem Verteiler kommen immer wieder vor (siehe dazu auch 7/8.2.4); die Ursache ist meist in individuellem Fehlverhalten eines Mitarbeiters zu finden. Fast schon amüsant war die diesbezügliche Einlassung eines allein arbeitenden Versicherungsmaklers, der mitteilte, dass der Versand versehentlich und ihm unerklärlich – trotz vorheriger Belehrung bzw. Verbots – durch seinen 8-jährigen Sohn ausgelöst worden sei, der einen abrupten durchfallbedingten Toilettengang seines Vaters ausgenutzt habe, um an dessen Laptop „herumzudrücken“. Schließlich teilte er noch mit: *„Wir haben versucht den Verteiler zu löschen, wir denken es hat geklappt.“* – Ob er mit „wir“ wohl seinen Sohn und sich gemeint hat? Und ob es geklappt hat? Jedenfalls habe ich diesbezüglich keine weiteren Eingaben erhalten.

Auch die Nichterfüllung der Auskunftsverpflichtungen nach § 34 BDSG beschäftigt mich regelmäßig. Einem Petenten war es offensichtlich zu aufwändig, immer wieder neu bei einer verantwortlichen Stelle nachzufragen, daher versuchte er es mit einem Dauerauftrag bzw. einer Art Auskunfts-Abo: *„Da der Anspruch auf Auskunft einmal je Kalenderjahr besteht, fordere ich Sie auf, mir zukünftig in jedem Jahr, beginnend mit diesem, Auskunft bis zum 23.12. des Jahres zu erteilen."* – Klingt praktisch, ist aber leider so nicht vom Gesetz gedeckt. Überdies: Dass der Betroffene seiner wiederkehrenden Auskunftsforderung mit einem gleichzeitig gestellten Löschungsantrag selbst die Grundlage entzogen hatte, war ihm nicht aufgefallen.

Warum wegwerfen, was noch funktioniert? Über die zweckfremde Verwendung einer Babyfon-Kamera habe ich schon in 7/8.3.7 berichtet. Offensichtlich macht das Beispiel Schule – Babyfon-Kameras werden jetzt auch zur Überwachung von Hauseingängen durch Mieter eingesetzt: Nachdem sich Mitmieter über eine Kamera außen am Küchenfenster einer Wohnungseinheit beschwert hatten, habe ich mich dieser Angelegenheit angenommen. Der – anwaltlich vertretene – Mieter ließ daraufhin erklären, dass er diese Kamera immer dann am Küchenfenster platziere, wenn er ein Paket erwarte. Er treibe regelmäßig im Keller Sport und höre dann das Klingeln an der Haustür nicht. So könne er sehen, wenn der Paketbote an der Hauseingangstür steht. – Wie praktisch, da kann er auch gleich die Pakete für seine Nachbarn mit annehmen, und dass das Training auf einem Hometrainer kurzweiliger ist, wenn man dabei auf einen Monitor schaut, das kennt man ja aus dem Fitnessstudio!

9 Informationspflicht 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 46 solcher Meldungen eingegangen. Gegenüber dem vorherigen Berichtszeitraum (24) stellt dies praktisch eine Verdoppelung dar. In elf Fällen habe ich nach entsprechender Prüfung eine Meldepflicht verneint, weil entweder meine Zuständigkeit nicht gegeben war oder aber die Voraussetzungen des § 42a BDSG nicht erfüllt gewesen sind, insbesondere die Kenntnisnahme Dritter nicht angenommen werden konnte oder keine schwerwiegende Beeinträchtigung für die Rechte oder schutzwürdigen Interessen der Betroffenen drohte.

In 35 Fällen hat eine Meldepflicht bestanden:

- Fehlversand einer Abtretungserklärung zur Risikolebensversicherung infolge Adressatenverwechslung durch einen Finanzdienstleister (Gesundheits- und Kontodaten)
- Fehlversand von Dokumenten per Telefax infolge Zahlendrehers durch ein Krankenhaus an eine Ärztin (zwei Meldungen) (Gesundheitsdaten)
- Fehlversand eines Tilgungsplanes infolge Anlagenverwechslung durch einen Finanzdienstleister (Kontodaten)
- Fehlversand von Kontoauszügen infolge Irrtums über Verfügungsberechtigung durch ein Kreditinstitut (Kontodaten)
- Fehlversand eines Fragebogens zum Gesundheitszustand infolge Verwechslung der Kundennummer durch eine Versicherung (Gesundheitsdaten)
- Fehlversand einer SEPA-Lastschrift-Vorabinformation (Pre-Notification) infolge Anlagenverwechslung durch ein Unternehmen (zwei Meldungen) (Kontodaten)
- Fehlversand einer SEPA-Lastschrift-Vorabinformation (Pre-Notification) infolge Adressatenverwechslung (falsche Hausnummer) durch ein Unternehmen (Kontodaten)
- unbefugte Übermittlung einer Kontoübersicht an Verbundunternehmen durch ein Kreditinstitut (Kontodaten)
- zeitweise Aufhebung der Zugriffsbeschränkung auf ein Netzlaufwerk mit Personaldaten in einem Unternehmen (Daten über Verdacht strafbarer Handlungen)

- Kreditkartendatenabgriff bei einem Katalog- und Onlinehändler (Kreditkartendaten)
- Fehlversand von Dokumenten infolge Adressverwechslung durch Finanzdienstleister oder Kreditinstitute (fünf Meldungen) (Kontodaten)
- Weitergabe eines Überweisungsbelegs als Zahlungsnachweis an WEG-Mitglieder durch den Verwalter (Kontodaten)
- Fehlversand einer Rechnung in eine Online-Postbox infolge Softwarefehlers durch ein Unternehmen (Kontodaten)
- fehlerhafte Zuordnung von Patientenunterlagen in einer Krankenakte mit anschließender Übermittlung an einen falschen Patienten durch ein Krankenhaus (Gesundheitsdaten)
- Diebstahl von Versicherungsunterlagen aus einem PKW eines Außendienstmitarbeiters (Gesundheits-, Bank- und Kreditkartendaten)
- mögliche Kenntnisnahme eines festgefahrenen Überweisungsvorgangs auf einem Überweisungsterminal (Bankdaten)
- Diebstahl von Festplatte, PC und Digitalkamera mit Patientendaten aus einer Klinik bzw. Praxis (zwei Meldungen) (Gesundheitsdaten)
- Diebstahl von PC und Festplatten bei einem Sportverein (Bank- und Kreditkartendaten)
- Hackerangriff auf den Server eines Vertriebsunternehmens (Bankdaten)
- Fehlversand von Vertragsunterlagen infolge Adressverwechslung durch eine Versicherung (zwei Meldungen) (Bankdaten)
- Beschädigung eines Briefumschlages durch äußere Umstände bei einem Zustelldienst (Daten, die einem Berufsgeheimnis unterliegen)
- zeitweise Aufhebung der Zugriffsbeschränkung auf einen Server einer Vermögensberatung (Gesundheits- und Bankdaten sowie Daten, die einem Berufsgeheimnis unterliegen)
- fehlerhafte Datenzuordnung in einem Online-Portal (Bankdaten)
- Fehlversand von Versicherungsunterlagen per E-Mail infolge Adressverwechslung einer Vermögensberatung (Bankdaten)
- Fehlkuvertierung von Schreiben eines Labors (Gesundheitsdaten)
- Fehlkuvertierung von Schreiben eines Personaldienstleisters (Gesundheitsdaten)
- Diebstahl eines PC aus Apotheke (Gesundheitsdaten)

In Bezug auf die betroffenen Datenarten liegt der Schwerpunkt der Meldungen bei Bank- und Gesundheitsdaten.

Hinsichtlich der verantwortlichen Stellen ist auch im aktuellen Berichtszeitraum kein besonderer Schwerpunkt erkennbar. Korrespondierend zu den in erster Linie betroffenen

Daten handelt es sich bei den meldepflichtigen Stellen vor allem um Unternehmen aus der Versicherungs- und Gesundheitsbranche sowie um Kreditinstitute.

Auffällig häufig liegt die Ursache im Fehlversand von Unterlagen. Dies wiederum beruht zum Großteil auf Adressverwechslungen, fehlerhaften Zuordnungen von Anlagen, Fehlkuvertierungen oder auf simplen Zahlendrehern. Insoweit hilft die stetige Sensibilisierung hinsichtlich solcher Fehlerquellen und die Einführung und aktive Wahrnehmung von Kontrollhandlungen, da zumeist ein Einzelfallversagen vorliegt.

Eine weitere wesentliche Fallgruppe für Meldungen nach § 42a BDSG sind nach wie vor der Diebstahl technischer Geräte wie Festplatten oder Computer. In der Regel wäre eine Kenntnisnahme der darauf gespeicherten Daten durch eine wirksame Verschlüsselung vermeidbar gewesen.

In allen der Aufsichtsbehörde gemeldeten Fällen sind die Betroffenen letztendlich ordnungsgemäß benachrichtigt und auch ausreichende Maßnahmen zur Verhinderung einer Wiederholung und zur Minimierung eines möglichen Schadens getroffen worden.

10 Stellungnahmen zu Unterlassungsklagen

Am 23. Februar 2016 trat das Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts in Kraft. Hierdurch wurde u. a. das Unterlassungsklagengesetz geändert und gibt nunmehr Verbraucherschutzorganisationen die Möglichkeit, gegen Datenschutzverstöße auf Unterlassung und Beseitigung zu klagen.

Im Rahmen der Änderungen des Unterlassungsklagengesetzes wurde dort der § 12a – Anhörung der Datenschutzbehörden in Verfahren über Ansprüche nach § 2 – eingefügt. Hiernach hat das Gericht vor einer Entscheidung in einem Verfahren über einen Anspruch nach § 2, das eine Zuwiderhandlung gegen ein Verbraucherschutzgesetz nach § 2 Abs. 2 Satz 1 Nr. 11 zum Gegenstand hat, die zuständige inländische Datenschutzbehörde zu hören. Satz 1 ist nicht anzuwenden, wenn über einen Antrag auf Erlass einer einstweiligen Verfügung ohne mündliche Verhandlung entschieden wird. Die Regelung orientiert sich an § 8 Abs. 2 UKlaG, wonach bei der gerichtlichen Überprüfung von Allgemeinen Geschäftsbedingungen eine Anhörung der Bundesanstalt für Finanzdienstleistungsaufsicht zu erfolgen hat. Ob und wie die zuständige Datenschutzbehörde dieses Anhörungsrecht wahrnimmt, steht in derem Ermessen. Ziel der Anhörung ist die Vermeidung unterschiedlicher datenschutzrechtlicher Beurteilungen des streitgegenständlichen Sachverhalts. Gleichwohl ist es nicht ausgeschlossen, dass das Gericht schlussendlich zu einem anderen Ergebnis als die angehörte Datenschutzbehörde kommt.

Im Berichtszeitraum gingen im Rahmen von Verbandsklagen nach dem Unterlassungsklagengesetz zwei gerichtliche Anhörungsgesuche bei mir ein.

In dem einen Verfahren gegen einen privaten Kabelnetzbetreiber war aus datenschutzrechtlicher Sicht zu beurteilen, ob personenbezogene Daten auf Grundlage der nachfolgenden Klausel genutzt und verarbeitet werden dürfen:

„Ich stimme hiermit der Nutzung und/oder Übermittlung meiner Daten an Dritte zu Werbe- und Marktforschungszwecken im Auftrag der Gesellschaft zu und erkläre mich einverstanden, per Telefon, Brief und/oder E-Mail im Rahmen von Marketingaktionen über Produktveränderungen informiert zu werden. Ich bin berechtigt, mein Einverständnis jederzeit mit sofortiger Wirkung gegenüber der Gesellschaft zu widerrufen.“

Im Rahmen der Stellungnahme habe ich folgende Beurteilung abgegeben:

Eine Einwilligung ist nach § 4a Abs. 1 Satz 1 BDSG nur wirksam, wenn sie auf einer freien Entscheidung des Betroffenen beruht, was wiederum voraussetzt, dass der Betroffene wissen muss, worin er einwilligt. Es bedarf also einer sogenannten informierten

Einwilligung. Dies setzt zunächst einmal voraus, dass der Betroffene wissen muss, welche personenbezogenen Daten der Einwilligung unterliegen. Eine Einwilligungsklausel, die lediglich allgemein von „meinen Daten“ spricht, erfüllt diese Anforderung nicht. Es bedarf vielmehr entweder einer Aufzählung der betreffenden Datenarten oder einer entsprechenden Bezugnahme, d. h. für den Betroffenen müssen die der Einwilligung konkret unterfallenden Daten klar erkennbar sein. Die hier verwendete Formulierung ließ eine solche Konkretisierung aber gerade nicht zu. Des Weiteren muss der Betroffene über den Zweck der Verarbeitung und Nutzung und mindestens auch über die Kategorien von Datenempfängern informiert werden. Auch dies konnte der zu bewertenden Klausel nicht klar und deutlich entnommen werden. Es blieb insoweit vollkommen offen, ob die Daten lediglich an verbundene Unternehmen oder an beliebige Dritte weitergegeben werden sollen und ob sich die Werbezwecke auch auf vertragsfremde Leistungen und Produkte beziehen. Die betreffende Einwilligungsklausel kam daher als Erlaubnistatbestand für die beabsichtigte Verarbeitung und Nutzung nicht in Betracht, d. h. eine Verarbeitung oder Nutzung personenbezogener Daten auf Grundlage dieser Klausel war unzulässig (§ 4 Abs. 1 BDSG).

In dem anderen Verfahren ging es um die Frage der rechtlichen Zulässigkeit eines Bonusprogramms eines Kreditinstituts. Infolge des nur eingeschränkt bekannten Sachverhalts stellte sich die datenschutzrechtliche Bewertung an dieser Stelle jedoch als problematisch dar. Diesbezüglich ist zu berücksichtigen, dass Anhörungen nach § 12a UKlaG im Rahmen eines zivilgerichtlichen Verfahrens und somit allein auf Grundlage des Parteivorbringens erfolgen. Es gilt der sogenannte Beibringungsgrundsatz, wobei der zugrundeliegende Sachverhalt oftmals auch streitig ist. Im Rahmen meiner Stellungnahme konnte ich daher in diesem Fall nur eingeschränkt eine Bewertung vornehmen. Festzuhalten war insoweit jedenfalls, dass ein Kreditinstitut, welches die im Rahmen des Zahlungsdienstvertrags erhobenen Daten zu einem eigenständigen Nutzer-Account zur Durchführung eines Bonusprogramms zusammenführt, hierdurch auch eine eigenständige Datenverarbeitung vornimmt. Insoweit bedarf das Anlegen und Unterhalten eines solchen Nutzer-Accounts im Rahmen des Bonusprogramms einer datenschutzrechtlichen Rechtfertigung im Sinne des § 4 Abs. 1 BDSG, sei es in Form einer Einwilligung oder unter den Voraussetzungen des § 28 Abs. 1 BDSG.

11 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 nunmehr achten Tätigkeitsbericht zum Datenschutz im nicht-öffentlichen Bereich erfülle ich meine Verpflichtung, die Öffentlichkeit alle zwei Jahre über die Tätigkeit der Aufsichtsbehörde zu informieren. Der Bericht kann – ebenso wie alle vorangegangenen Berichte – per Download von meinem Internetauftritt *(http://www.datenschutz.sachsen.de)* bezogen bzw. als Druckexemplar bei mir abgerufen werden. Darüber hinaus halte ich im Internet weitere Informationen zu aktuellen Datenschutzthemen wie bundesweit abgestimmte Orientierungshilfen oder Anwendungshinweise zur Unterstützung der Tätigkeit der verantwortlichen Stellen und ihrer Datenschutzbeauftragten zum Abruf bereit.

Den auch im Berichtszeitraum an mich gerichteten zahlreichen Anfragen wegen einer Referententätigkeit bei verschiedenen Fach- und Fortbildungsveranstaltungen konnte ich wegen der bereits seit Jahren äußerst angespannten Personalsituation leider nur in sehr geringem Umfang entsprechen. Ich bedauere dies ausdrücklich, muss aber zur Kenntnis nehmen, dass die mir aktuell zugestandenen personellen Ressourcen die Wahrnehmung derartiger Aufgaben unverändert einfach nicht zulassen.

Auch in Bezug auf die vierteljährlich stattfindenden GDD-Erfa-Kreise musste ich mein Engagement aus diesem Grund leider zurückfahren. Anders als in früheren Berichtszeiträumen konnte ich nur noch vereinzelt an diesen Tagungen teilnehmen. Das ist sehr bedauerlich, da der Austausch mit den auf diesen Veranstaltungen anwesenden betrieblichen Datenschutzbeauftragten für beide Seiten immer sehr gewinnbringend gewesen ist.

12 Durchsetzung der Rechte und Befugnisse der Aufsichtsbehörde

12.1 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 waren für mich wiederum ein wirksames Mittel, um von verantwortlichen Stellen, die im Regelfall mindestens zwei aufsichtsbehördliche Schreiben ignoriert oder die Auskunftserteilung aktiv verweigert haben, die zur Aufgabenerfüllung erforderlichen Auskünfte zu erhalten. Mit Einführung einer Gebührenordnung im Mai 2015 (vgl. dazu 7/10.3 sowie Pkt. 12.3 des vorliegenden TB) sind auch die mit dem Erlass eines solchen Bescheides verbundenen Gebühren mit mindestens 150 € (vgl. Nr. 2 der Anlage zu § 40 SächsDSG) deutlich gestiegen, was wohl auch als Grund dafür angesehen werden muss, dass deutlich weniger Zwangsgeldfestsetzungen erforderlich gewesen sind. Offensichtlich waren die Kosten des Heranziehungsbescheides schon ausreichend hoch, um die verantwortlichen Stellen zur Auskunftserteilung zu bewegen.

Berichtszeitraum		2007 2008	2009 2010	01.01.11 31.03.13	01.04.13 31.03.15	**01.04.15 31.03.17**
Förmliche Heranziehungen		4	7	31	20	**18**
davon	mit einmaliger Zwangsgeldfestsetzung	1	4	6	9	**4**
	mit zweimaliger Zwangsgeldfestsetzung	0	0	0	3	**0**
	mit dreimaliger Zwangsgeldfestsetzung	1	0	0	0	**0**
	Klage gegen den Heranziehungsbescheid	0	0	2	1	**4**

In vier der 18 förmlichen Verfahren zur Auskunftsheranziehung haben die verantwortlichen Stellen Rechtsmittel eingelegt, d. h. Klage erhoben. In einem Fall hat sich die Klage gegen die Zwangsgeldfestsetzung gerichtet; in den drei anderen Fällen gegen die Auskunftsforderung. Drei Klageverfahren sind inzwischen bereits zu meinen Gunsten abgeschlossen worden. Im vierten Verfahren steht die Entscheidung in der Hauptsache noch aus, allerdings ist der gleichzeitig eingereichte Antrag auf Wiederherstellung der

aufschiebenden Wirkung – ich hatte die sofortige Vollziehbarkeit angeordnet – bereits abgelehnt worden und zwar sowohl durch das Verwaltungsgericht als auch das Oberverwaltungsgericht.

Auch mit der Zahlung eines Zwangsgeldes erlischt die Auskunftspflicht der verantwortlichen Stelle nicht. Auch können nach § 19 Abs. 5 SächsVwVG Zwangsmittel wiederholt und so lange angedroht werden, bis die verantwortliche Stelle ihrer Verpflichtung nachgekommen ist. Das Zwangsverfahren wird aber eingestellt, sobald die geforderten Auskünfte erteilt worden sind. Die Gesamtsumme der im Berichtszeitraum festgesetzten Zwangsgelder beträgt 3.000 €.

Der Erlass eines Bescheides zur Festsetzung eines Zwangsgeldes hat zumeist auch die Einleitung eines Ordnungswidrigkeitenverfahrens wegen Verstoßes gegen die Auskunftspflicht nach § 38 Abs. 3 Satz 1 BDSG (vgl. § 43 Abs. 1 Nr. 10 BDSG) zur Folge.

12.2 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).

Die von der Aufsichtsbehörde mit der Kontrolle beauftragten Personen sind befugt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben erforderlich ist, während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. Sie können geschäftliche Unterlagen, insbesondere die Übersicht nach § 4g Abs. 2 Satz 1 sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme, einsehen. Der Auskunftspflichtige hat diese Maßnahmen zu dulden (§ 38 Abs. 4 Sätze 1, 2 und 4 BDSG).

Im Berichtszeitraum habe ich insgesamt sechs Anordnungen erlassen müssen, drei davon betrafen Maßnahmen zur Beseitigung festgestellter Datenschutzverstöße (§ 38 Abs. 5

BDSG), die anderen bezogen sich auf die Duldung einer aufsichtsbehördlichen Kontrollmaßnahme (§ 38 Abs. 4 BDSG). Alle Anordnungen sind bestandskräftig geworden; Zwangsgeldfestsetzungen sind insoweit nicht notwendig geworden.

Die Anordnungen zur Beseitigung von Datenschutzmängeln betrafen

- die Ausrichtung des auch für Kunden einsehbaren Kontrollmonitors einer Videoüberwachungsanlage in einem Einzelhandelsgeschäft,
- die Nutzung einer auf kanadischen Servern laufenden Software zur individuellen Zieldefinition und Leistungsbeurteilung von Mitarbeitern und
- die Videoüberwachung in einem Biergarten.

Gleich in mehreren Fällen ist es vorgekommen, dass ich ungeachtet einer frühzeitigen Kontrollankündigung keine auskunftsfähigen und auch auskunftsbefugten Ansprechpartner vor Ort angetroffen habe. Um dies bei den dadurch notwendig gewordenen Folgeterminen zu vermeiden, habe ich dann jeweils vorher auf der Grundlage von § 38 Abs. 4 BDSG eine kostenpflichtige – sofort vollziehbare – Duldungsanordnung erlassen, mit der ich der verantwortlichen Stelle zum einen aufgegeben habe, das Betreten der betreffenden Geschäftsräume durch Bedienstete meiner Behörde zum Kontrolltermin zu dulden, insbesondere den Zugang zu ermöglichen. Zum anderen betraf die Anordnung auch die Duldung von Prüfungsmaßnahmen der betreffenden Datenverarbeitungsanlage durch meine Bediensteten, insbesondere das Bereithalten darauf bezogener technischer Unterlagen und Dokumentationen (u. a. Bedienungsanleitungen, Verfahrensverzeichnis gemäß § 4g Abs. 2 Satz 1 BDSG) sowie die Einsichtnahme in diese Unterlagen wie auch in Datenverarbeitungsprogramme und Datenverarbeitungsanlagen, auch soweit diese durch Passwörter gesichert waren.

12.3 Einführung einer Gebührenordnung

Mit Wirkung vom 9. Mai 2015 wurde das Sächsische Datenschutzgesetz um eine Regelung erweitert, die mich ermächtigt, entsprechend dem Verwaltungsaufwand für bestimmte Amtshandlungen und sonstige öffentlich-rechtliche Leistungen nach dem Bundesdatenschutzgesetz Kosten zu erheben (vgl. dazu auch 7/10.3).

Nach dieser Regelung (§ 40 SächsDSG) darf ich von nicht-öffentlichen Stellen insbesondere dann einen Kostenausgleich verlangen, wenn ich bei meiner Prüfung Datenschutzverstöße festgestellt habe. Auch datenschutzrechtliche Beratungen nicht-öffentlicher Stellen sind im Regelfall kostenpflichtig. Lediglich Kontrollen und Beratungen einfacher Art sowie die Beratung von Stellen ohne Gewinnerzielungsabsicht bleiben kostenfrei. Für

Anordnungen, Untersagungen, Abberufungen von Datenschutzbeauftragten sowie bestimmte Prüfungen, Verfahren oder Genehmigungen sind spezielle Kostensätze festgelegt.

Auf der Grundlage dieser Gebührenregelung habe ich im Berichtszeitraum Einnahmen in Höhe von mehr als 27.000 € erzielen können. Diese Einnahmen stammen aus:

- 72 Mängelfeststellungen bei Datenschutzkontrollen (§ 38 Abs. 1 Satz 1 BDSG),
- 18 Registervorgängen (§ 38 Abs. 2 Satz 1 BDSG),
- 5 Beratungen (§ 38 Abs. 1 Satz 2 BDSG),
- 15 Heranziehungsbescheiden (§ 38 Abs. 3 Satz 1 BDSG) sowie
- 6 Anordnungen (§ 38 Abs. 4, 5 BDSG).

Ich kann feststellen, dass die Akzeptanz meiner Kostenbescheide deutlich höher ist als beim Erlass von Bußgeldbescheiden. In lediglich zwei Fällen haben verantwortliche Stellen bislang in Bezug auf die Kostenerhebung Klage erhoben. Gerichtliche Entscheidungen liegen mir in diesen Verfahren noch nicht vor.

13 Ordnungswidrigkeitenverfahren

13.1 Durchgeführte Ordnungswidrigkeitenverfahren

Als Verwaltungsbehörde nach § 36 Abs. 2 OWiG (§ 15 OWiZuVO) bin ich für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 43 BDSG, § 16 Abs. 2 Nr. 2 bis 5 TMG sowie § 130 OWiG zuständig.

Im Berichtszeitraum sind insgesamt 124 Bußgeldverfahren bei mir anhängig gewesen; 22 davon stammten noch aus den Vorjahren (vgl. 7/11.2).

In 47 Fällen habe ich die vorgeworfenen Datenschutzverstöße mit einem Bußgeldbescheid abgeschlossen; in zwei weiteren Fällen habe ich lediglich eine Verwarnung ausgesprochen und dies mit einem Verwarnungsgeld in der maximal möglichen Höhe von 55 Euro verbunden. Die Anzahl der als Ordnungswidrigkeit geahndeten Datenschutzverstöße entspricht also trotz der gestiegenen Gesamtzahl der bearbeiteten Verfahren (zufällig) exakt dem vorangegangenen Berichtszeitraums. 63 Verfahren habe ich wieder eingestellt und neun Verfahren aus Zuständigkeitsgründen an andere Behörden abgegeben. Die abgegebenen Verfahren betrafen überwiegend Verstöße gegen die Impressumspflicht im Telemedienbereich (§ 16 Abs. 2 Nr. 1 TMG), für die ich keine Verfolgungszuständigkeit habe.

Trotz der gestiegenen Gesamtverfahrenszahl habe ich die Zahl offener Verfahren deutlich reduzieren können; zum Ende des Berichtszeitraums waren anders als in den Vorjahren nur noch drei Verfahren in Bearbeitung.

Berichtszeitraum		2007 2008	2009 2010	01.01.11 31.03.13	01.04.13 31.03.15	**01.04.15 31.03.17**
Einleitung		16	24	79	88	**102**
zzgl. Übernahme Vorjahr		3	2	3	29	**22**
anhängig gesamt		19	26	82	117	**124**
davon	mit Bußgeld	7	14	36	49	**47**
	mit Verwarnungsgeld	0	0	1	0	**2**
	eingestellt	10	9	16	41	**63**
	unzuständig	0	0	0	5	**9**
	noch in Bearbeitung	2	3	29	22	**3**
Bußgeldsumme in Euro		13.450	24.800	54.095	353.572	**174.226**

Die vorstehende Übersicht zeigt, dass sich die Höhe der festgesetzten Bußgelder gegenüber dem vorangegangenen Berichtszeitraum in etwa halbiert hat, dennoch aber immer noch deutlich höher liegt als in den noch weiter davor liegenden Jahren. Tatsächlich habe

ich im Berichtszeitraum im Gegensatz zum 7. TB auch keine Bußgelder festsetzen müssen, mit denen ich den für formale Datenschutzverstöße bestehenden Bußgeldrahmen vollständig ausgeschöpft habe. Die im Berichtszeitraum nichtsdestoweniger herausragenden Bußgelder betrafen folgende formalen Verstöße:

- Missachtung der Auskunftspflicht gegenüber der Aufsichtsbehörde (1-mal 10.000 €),
- Missachtung der Pflicht zur Bestellung eines Datenschutzbeauftragten (4-mal 10.000 €),
- Nichtbefolgung einer datenschutzrechtlichen Anordnung (1-mal 16.000 €) sowie
- Missachtung der Pflicht zur Erteilung schriftlicher Auftragsdatenverarbeitungsaufträge (1-mal 18.000 €).

Aus dem Bereich des § 43 Abs. 1 BDSG (formale Rechtsverstöße) sind in der Summe (34 Fälle) folgende Sachverhalte mit Buß- bzw. Verwarnungsgeldern belegt worden:

- Nichtbeachtung der Meldepflichten nach § 4d BDSG (fünf Fälle)
- unterlassene Bestellung eines Datenschutzbeauftragten (§ 4f Abs. 1 BDSG) (zehn Fälle)
- Missachtung der Auskunftspflichten gegenüber der Aufsichtsbehörde (§ 38 Abs. 3 BDSG) (sechs Fälle)

Diesbezüglich in negativer Hinsicht besonders erwähnenswert sind zwei Unternehmer, die der Aufsichtsbehörde die geforderten Auskünfte zwar fristgemäß, jedoch falsch erteilt hatten. In einem Fall ging es um die Erfassungsbereiche von Videokameras und die Vorlage entsprechender Screenshots: Für deren Erstellung hatte der Geschäftsinhaber die Ausrichtung der Kameras lediglich temporär verändert, anschließend aber den ursprünglichen Zustand wiederhergestellt. Im Zuge einer nachfolgenden unangemeldeten örtlichen Kontrolle war das dann aber aufgefallen. In dem anderen Fall hatte ein Geschäftsführer der Aufsichtsbehörde per E-Mail die elektronische Fassung eines Auftragsdatenverarbeitungsvertrages (ohne Unterschriften) vorgelegt und wahrheitswidrig behauptet, dieser Vertrag sei schon vor geraumer Zeit abgeschlossen worden. In beiden Fällen sind neben der Falschauskunft auch die zugrundeliegenden Datenschutzverstöße (unzulässige Videoüberwachung, fehlender Auftragsdatenverarbeitungsvertrag) als Ordnungswidrigkeit geahndet worden.

- Nichtbefolgung einer datenschutzrechtlichen Anordnung (ein Fall)
- in Werbeschreiben unterlassene Unterrichtungen über das Widerspruchsrecht (§ 28 Abs. 4 Satz 2 BDSG) (vier Fälle)

- unterlassene oder nicht rechtzeitige Erteilung von Auskünften an den Betroffenen (§ 34 Abs. 1 BDSG) (vier Fälle)
- Verstoß gegen die inhaltlichen Vorgaben bei Auftragsdatenverarbeitungsverträgen (§ 11 Abs. 2 Satz 2 BDSG) (vier Fälle)

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

- Videoaufzeichnung des öffentlichen Verkehrsraumes mit einer im Dauerbetrieb befindlichen Klingelkamera und Veröffentlichung von Videosequenzen im Internet
- Videoüberwachung des öffentlichen Verkehrsraumes mittels an einem Wohngebäude angebrachten Videokameras (Vermieter)
- Videoüberwachung des öffentlichen Verkehrsraumes mittels einer am Fenster einer Wohnung angebrachten Kamera (Mieter)
- Videoüberwachung des öffentlichen Verkehrsraums vor einer Spielhalle
- Videoüberwachung im Sozialraum einer Tankstelle
- Einsatz von Dashcams mit Audioaufnahmen in einem Taxibetrieb
- Betrieb einer Dashcam, sowohl im fahrenden als auch im geparkten Wohnmobil
- Übermittlung von Namen und Telefonnummern von zu kündigenden Mitarbeitern an einen potentiellen neuen Arbeitgeber
- Entsorgung von Rechtsanwaltsakten in eine normale Altpapiertonne
- Erhebung personenbezogener Daten bei der Ausgabe gelber Säcke
- Verarbeitung der Daten von Mitgliedern einer WEG für Werbezwecke durch einen Immobilienmakler
- Nutzung von Adressdaten von Anlegern zum Zwecke anwaltlicher Werbung
- GPS-Tracker am Privat-PKW einer Nachbarin
- privat motivierter Zugriff auf Kundendatensätze durch Call-Center-Agenten
- Aufsichtspflichtverletzung bei der Gewährleistung der Systemsicherheit (frei zugänglicher FTP-Server)

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 und Personenvereinigungen festgesetzte Geldbußen. Die im Berichtszeitraum bestandskräftig mit einem Bußgeldbescheid abgeschlossenen Verfahren haben in 28 Fällen zu solch einem Gewerbezentralregistereintrag geführt.

13.2 Wahrnehmung besonderer Ermittlungsbefugnisse

Anders als im verwaltungsrechtlichen Aufsichtsverfahren habe ich als Verfolgungsbehörde nach dem Ordnungswidrigkeitengesetz zunächst keine besonderen Betretungs-, Besichtigungs- oder Prüfrechte. Soweit mir eine mögliche Ordnungswidrigkeit – mit entsprechenden Unterlagen, Informationen und eventuellen Zeugen – nicht aus dem Aufsichtsbereich meiner Behörde angezeigt wird, stellt sich daher regelmäßig die Frage, wie ich die Aufklärung des Sachverhalts weiter voranbringen und geeignete Beweismittel erlangen kann. Im Gegensatz zum Aufsichtsverfahren unterliegt der (im Ordnungswidrigkeitenverfahren als Betroffener bezeichnete) für die Datenverarbeitungshandlung Verantwortliche insoweit grundsätzlich keinen Duldungspflichten. Er ist auch nicht verpflichtet, an der Aufklärung des Sachverhalts mitzuwirken. Er kann mir also das Betreten seiner Geschäftsräume ebenso verwehren, wie er mir auch nicht Einsicht in geschäftliche Unterlagen gewähren, Prüfungshandlungen an Datenverarbeitungsanlagen dulden und Auskünfte erteilen muss.

Nach § 46 Abs. 2 OWiG habe ich als Verfolgungsbehörde im Bußgeldverfahren im Wesentlichen aber dieselben Rechte und Pflichten wie die Staatsanwaltschaft bei der Verfolgung von Straftaten; auch gelten für das Bußgeldverfahren bis auf Ausnahmen sinngemäß die Vorschriften der allgemeinen Gesetze über das Strafverfahren, namentlich der Strafprozessordnung (§ 46 Abs. 1 OWiG).

Als insoweit auch für mich probates Mittel haben sich dabei Zeugenvernehmungen herausgestellt. Während ich mich im Aufsichtsverfahren nur an die verantwortliche Stelle und die mit deren Leitung beauftragten Personen wenden kann, weil nur diese der Auskunftspflicht nach § 38 Abs. 3 BDSG unterliegen, kann ich als Verfolgungsbehörde auch Mitarbeiter der verantwortlichen Stellen vernehmen. Als Zeugen haben diese – soweit sie sich dadurch nicht selbst oder Angehörige belasten (§§ 52 Abs. 1, 55 Abs. 1 StPO) – auch kein Auskunfts- bzw. Zeugnisverweigerungsrecht. Die Angaben eines Zeugen zur Person und zur Sache müssen dabei in jedem Fall auch der Wahrheit entsprechen (§ 57 Abs. 1 StPO). Ich entscheide jeweils von Fall zu Fall, ob ich als Zeugen in Frage kommende Personen lediglich schriftlich vernehme oder zur mündlichen Vernehmung in meine Behörde vorlade. Das Erscheinen eines Zeugen und seine Aussage vor der Verwaltungsbehörde sind im Bußgeldverfahren auch zwangsweise durchsetzbar (§ 161a Abs. 1 Satz 1 StPO).

Einem Zeugen, der ohne genügende Entschuldigung nicht erscheint, können die durch seine Säumnis entstandenen Kosten und ein Ordnungsgeld bis zu 1.000 € auferlegt werden (§§ 51 Abs. 1, 161a Abs. 2 StPO).

Im Berichtszeitraum habe ich innerhalb eines Verfahrens in vier Fällen davon Gebrauch gemacht. Die vier Zeugen waren nicht zu ihrer Vernehmung erschienen und hatten angeführt, dass sie als Angestellte des Betroffenen ein umfassendes Auskunftsverweigerungsrecht für sich geltend machen würden und unter diesen Umständen ein persönliches Erscheinen bei mir für nicht erforderlich hielten. Allerdings konnten diese Zeugen sich schon nach Aktenlage nicht auf ein solches umfassendes Auskunftsverweigerungsrecht nach § 55 StPO berufen, sondern wären allenfalls befugt gewesen, einzelne Fragen nicht zu beantworten. Selbst ein Zeuge, der sich zu Recht auf ein umfassendes Auskunftsverweigerungsrecht beruft, kann damit sein Ausbleiben beim Vernehmungstermin nicht wirksam im Sinne des § 51 Abs. 2 StPO entschuldigen, sondern muss erscheinen.

In Bezug auf die fehlenden Betretungs-, Prüfungs- und Besichtigungsrechte verbleibt mir – soweit der Betroffene diese nicht freiwillig gewährt – nur der Rückgriff auf einen richterlichen Durchsuchungsbeschluss. Dabei ist es aber keinesfalls so, dass ich standardmäßig auf diese Ermittlungsmöglichkeit zurückgreife, insbesondere bei Bagatellordnungswidrigkeiten verzichte ich darauf regelmäßig, ebenso in Fällen, in denen nicht zu erwarten ist, dass überhaupt noch gerichtsverwertbare Beweismittel aufgefunden werden können oder eine Ahndung nicht mehr angezeigt ist, etwa weil der Betroffene bereits Kenntnis von den laufenden Ermittlungen erhalten und entsprechend reagiert, d. h. die im Fokus der Ermittlungen stehende Datenverarbeitungshandlung, beispielsweise eine rechtswidrige Videoüberwachung, eingestellt und die Kamera entfernt hat. Zudem ist eine Durchsuchung immer nur das ultimo ratio der möglichen Ermittlungsmaßnahmen – zuvor müssen alle anderen Aufklärungsmöglichkeiten ausgeschöpft sein.

Eine Durchsuchung und – damit verbunden – eine Beschlagnahme müssen immer auch in angemessenem Verhältnis zu Umfang und Dauer des datenschutzrechtlichen Verstoßes, zur Stärke des Tatverdachts und zur Höhe der zu erwartenden Geldbuße stehen. Besonders wenn sich der Tatvorwurf gegen Privatpersonen richtet – und das ist gerade bei rechtswidrigen Videoüberwachungen, seien es nun fest installierte Kameras oder auch Dashcams, leider häufig und zunehmend der Fall –, handelt es sich bei dem einer Durchsuchung immanenten Eingriff in den grundrechtlich besonders geschützten Wohnbereich des Betroffenen regelmäßig um einen schwerwiegenden Eingriff in dessen Privatsphäre. Dieser Eingriff muss dann immer sehr sorgfältig abgewogen werden mit der Schwere und Art der Tat und dem Kreis der von der Tat Betroffenen.

Im Berichtszeitraum habe ich beim zuständigen Ermittlungsrichter in vier Fällen einen Durchsuchungsbeschluss beantragt und auch erhalten. Die eigentliche Durchsuchung führe ich dann regelmäßig mit Unterstützung der örtlichen, diesbezüglich entsprechend routinierten Polizei durch. Alle vier Fälle betrafen dabei den Vorwurf rechtswidriger Videoüberwachungen, zum Teil auch von Privatpersonen.

14 Strafanträge

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

Als Straftat nach dem Bundesdatenschutzgesetz verfolgbar sind 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).

Im Berichtszeitraum habe ich auf Grundlage dieser Antragsbefugnis in einem Fall einen Strafantrag gestellt. Der Strafantrag betraf dabei die – in Bereicherungsabsicht erfolgte – Beantragung von Kurzzeitkennzeichen unter Missbrauch der Personalien unbeteiligter Personen.

15 Zusammenarbeit mit anderen Aufsichtsbehörden

Die Zusammenarbeit mit den Datenschutzaufsichtsbehörden der anderen Bundesländer sowie mit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit spielte sich im Wesentlichen im Rahmen der Datenschutzkonferenz (vgl. dazu meinen parallel erscheinenden 18. Tätigkeitsbericht für den öffentlichen Bereich), dem Düsseldorfer Kreis sowie den diesbezüglichen Arbeitsgruppen und Arbeitskreisen ab.

Der Düsseldorfer Kreis selbst tagt zweimal im Jahr; auf diesen Tagungen stimmen die Aufsichtsbehörden ihre Rechtsauffassungen in grundsätzlichen oder sonst besonders wichtigen datenschutzrechtlichen, ausschließlich den nicht-öffentlichen Bereich betreffenden Fragen sowie in diesbezüglichen länderübergreifenden Sachverhalten untereinander ab; zwischen den Tagungen geschieht dies bei Notwendigkeit auch im schriftlichen Verfahren. Ich bin regelmäßiger Teilnehmer dieses Gremiums; die im Berichtszeitraum gefassten Beschlüsse sind unter Pkt. 16 dieses Berichts abgedruckt.

Unterhalb des Düsseldorfer Kreises gibt es eine Reihe von spezialisierten Arbeitsgruppen, in denen auf Arbeitsebene Erfahrungen aus der Aufsichts- und Sanktionspraxis ausgetauscht, allgemein interessierende datenschutzrechtliche Fragestellungen untereinander sowie entweder regelmäßig oder auf besondere Einladung hin auch mit Vertretern der Wirtschaft, insbesondere mit Wirtschaftsverbänden, diskutiert und Beschlüsse für den Düsseldorfer Kreis vorbereitet werden. Im Berichtszeitraum war meine Behörde in allen dem Düsseldorfer Kreis zugeordneten Arbeitsgruppen

- Auskunfteien
- Internationaler Datenverkehr
- Kreditwirtschaft
- Sanktionen
- Versicherungswirtschaft
- Videoüberwachung
- Werbung und Adresshandel (Ad-hoc AG)

sowie auch in den sich mit Querschnittsthemen zwischen öffentlichem und nicht-öffentlichem Bereich befassenden Arbeitskreisen der Datenschutzkonferenz

- Beschäftigtendatenschutz
- (Tele-)Medien
- Technik
- Verkehr
- Zertifizierung (Ad-hoc AG)

vertreten und hat darüber hinaus auch an den jährlich durchgeführten Workshops der Datenschutzaufsichtsbehörden teilgenommen. In den Workshops werden einerseits Themen diskutiert, die keiner der fachspezifischen Arbeitsgruppen bzw. Arbeitskreise zuzuordnen sind, andererseits dienen diese Treffen dem Austausch praktischer Kontrollerfahrungen. 2015 fand der Workshop beim Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit und 2016 beim Hessischen Datenschutzbeauftragten statt.

Nach wie vor verfolge ich das Ziel, gemeinsam mit den Aufsichtsbehörden anderer Bundesländer abgestimmte anlasslose Prüfungen durchzuführen. Derartige Projekte laufen bundesweit bereits seit geraumer Zeit und haben sich zweifelsfrei bewährt (vgl. Pkt. 3.1). Mit den mir zur Verfügung stehenden, deutlich zu knapp bemessenen Personalressourcen bin ich dazu derzeit jedoch nicht in der Lage.

16 Beschlüsse des Düsseldorfer Kreises

16.1 Beschlüsse vom 15./16. September 2015

16.1.1 Orientierungshilfe „Videoüberwachung in öffentlichen Verkehrsmitteln“

Datenschutzgerechter Einsatz von optisch-elektronischen Einrichtungen in Verkehrsmitteln des öffentlichen Personennahverkehrs und des länderübergreifenden schienengebundenen Regionalverkehrs

Stand: 16. September 2015

1. Vorbemerkung

Die Datenschutzbeauftragten des Bundes und der Länder sowie die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich hatten unter Beteiligung des Verbandes Deutscher Verkehrsunternehmen (VDV) im Jahre 2001 Empfehlungen zur Videoüberwachung in öffentlichen Verkehrsmitteln abgestimmt.

Unter Berücksichtigung der Erfahrungen aus der Anwendungspraxis sowie auch der technischen Entwicklungen auf dem Gebiet der Videoüberwachungstechnik der letzten Jahre halten die Aufsichtsbehörden eine Fortschreibung dieser Empfehlungen nunmehr für geboten. Zudem wurde der Anwendungsbereich der ursprünglich nur für den öffentlichen Personennahverkehr (ÖPNV) geltenden Orientierungshilfe auf den länderübergreifenden schienengebundenen Regionalverkehr (SPNV) erweitert.

Im Spannungsfeld zwischen den berechtigten Interessen der Verkehrsunternehmen an einer Videoüberwachung und dem informationellen Selbstbestimmungsrecht ihrer Fahrgäste und Beschäftigten soll dieses Dokument eine datenschutzrechtliche Orientierung für den zulässigen Einsatz von Videoüberwachungseinrichtungen in öffentlichen Verkehrsmitteln geben.

2. Zulässigkeit der Videoüberwachung

Maßgebliche Vorschrift für die Prüfung der Zulässigkeit von Videoüberwachungsanlagen in öffentlichen Verkehrsmitteln ist § 6b des Bundesdatenschutzgesetzes (BDSG), sofern der Verkehrsbetrieb nicht öffentlich-rechtlich betrieben wird und deshalb die Zulässigkeit des Kameraeinsatzes nach Maßgabe des jeweiligen Landesdatenschutzgesetzes zu beurteilen ist.

Soweit Kameras auch Arbeitsplätze von Beschäftigten der Verkehrsunternehmen in öffentlichen Verkehrsmitteln miterfassen (z. B. Fahrerarbeitsplätze), findet neben dieser

Vorschrift ggf. auch § 32 BDSG Anwendung. Zweckmäßig ist auch der Abschluss einer Betriebsvereinbarung.

2.1 Videoüberwachung in Fahrgastbereichen

Nach § 6b Abs. 1 BDSG ist das Beobachten öffentlich zugänglicher Räume, zu denen auch die Fahrgastbereiche in öffentlichen Verkehrsmitteln gehören, mit optisch-elektronischen Einrichtungen nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der davon betroffenen Personen überwiegen.

2.1.1 Wahrnehmung des Hausrechts oder berechtigter Interessen

Eine Videoüberwachung in öffentlichen Verkehrsmitteln kann zur Wahrnehmung des Hausrechts oder berechtigter Interessen insbesondere zur Verhinderung oder Verfolgung von Gewalt gegen Personen und Beförderungseinrichtungen sowie zur technischen Fahrgastsicherheit in Betracht kommen.

Eine Videobeobachtung (sog. Monitoring) kann erfolgen, um Personen davon abzuhalten, Rechtsverstöße zu begehen (z. B. Gewalt gegen Beschäftigte, Sachbeschädigungen an Beförderungseinrichtungen). Dieser Überwachungszweck wird auf direkte Weise erreicht, wenn das Geschehen in Echtzeit durch interventionsbereites Personal beobachtet und dadurch im Notfall ein schnelles Eingreifen möglich wird.

Ist die Videoüberwachung als reine Aufzeichnungslösung ausgestaltet (sog. Black-Box-Lösung), so kann sie eingesetzt werden, um etwa die Aufklärung von Straftaten oder die Durchsetzung von Schadensersatzansprüchen zu ermöglichen (Beweissicherung). Voraussetzung ist, dass eine Gefahrenlage schlüssig dargelegt werden kann bzw. dass Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit Straftaten zu rechnen ist. Insoweit sind konkrete Tatsachen zu fordern, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen oder besondere Vorkommnisse (z. B. Missbrauch von Notbrems- oder Notrufeinrichtungen) in der Vergangenheit. Ratsam ist es daher, entsprechende Ereignisse sorgfältig zu dokumentieren (Datum, Art und Ort des Vorfalls, Schadenshöhe) oder etwaige Strafanzeigen aufzubewahren.

2.1.2 Erforderlichkeit der Videoüberwachung

Vor dem Einsatz einer Videoüberwachung in öffentlichen Verkehrsmitteln ist stets einzelfallbezogen zu prüfen, ob sie für den verfolgten Zweck tatsächlich erforderlich ist. Die

Erforderlichkeit einer Videoüberwachung kann nur dann bejaht werden, wenn die Überwachung geeignet ist, das festgelegte Ziel zu erreichen, und es hierfür kein milderes, in die Rechte der Betroffenen weniger einschneidendes Mittel gibt.

Wenn der Zweck ausschließlich in der Beobachtung des Geschehens in Echtzeit zur direkten Intervention besteht, ist nur eine Monitoring-Lösung geeignet; eine reine Black-Box-Ausgestaltung der Videoüberwachung eignet sich wiederum zur Aufklärung von Straftaten.

Vor dem Einsatz einer Videoüberwachungsanlage müssen sich die Verkehrsunternehmen insbesondere mit zumutbaren alternativen Methoden auseinandersetzen, die in das informationelle Selbstbestimmungsrecht der Fahrgäste weniger eingreifen.

So kann der regelmäßige Einsatz von Personal dem Schutzbedürfnis der Fahrgäste ebenso gut Rechnung tragen wie der Einsatz von Überwachungskameras. Auch die Verwendung besonders widerstandsfähiger Sitze/Sitzbezüge sowie eine spezielle Oberflächenbeschichtung können Vandalismusschäden vorbeugen. Zudem kann eine nur temporäre Videoüberwachung (z. B. nur zu bestimmten Tages- bzw. Nachtzeiten) oder der Kameraeinsatz nur auf besonders gefährdeten Linien oder beschränkt auf schlecht einsehbare Fahrgastbereiche ausreichen. Denkbar ist es, zu Zeiten oder auf Linien, in denen eine permanente Videoüberwachung nicht erforderlich ist, die Möglichkeit einer anlassbezogenen Aktivierung der Videoüberwachung durch einen Notfallschalter für den Fahrzeugführenden oder das Begleitpersonal vorzusehen.

Nicht erforderlich ist eine Videoüberwachung zur Abwehr von Haftungsansprüchen gegen das Verkehrsunternehmen. Der Einsatz von Kameras kann nicht damit begründet werden, dass die Aufzeichnungen benötigt werden, um (unberechtigte) Ansprüche von Fahrgästen wegen Sturzverletzungen oder Beschädigungen persönlicher Gegenstände infolge (angeblich) starker Bremsungen o. Ä. abzuwehren. Zunächst ist der Betroffene in der Pflicht, seine Schadensersatzansprüche zu begründen und den Nachweis zu erbringen, dass sein Sturz unter den gegebenen Umständen für ihn unvermeidbar war und durch das Verkehrsunternehmen verursacht worden ist. Videoaufnahmen zum Beweis des Gegenteils bedarf es daher nicht.

Schließlich ist eine Videoüberwachung allein zur Steigerung des subjektiven Sicherheitsgefühls der Fahrgäste unter dem Gesichtspunkt der Erforderlichkeit nicht geboten.

Ist unter Berücksichtigung dieser Kriterien die Erforderlichkeit einer Videoüberwachung insgesamt oder im vorgesehenen Umfang zu verneinen, so ist der Einsatz von Videokameras unzulässig, ohne dass es noch auf die Frage ankommt, ob ihr schutzwürdige Interessen der Betroffenen entgegenstehen.

2.1.3 Beachtung der schutzwürdigen Interessen der Betroffenen

Auch wenn eine Videoüberwachung zur Wahrnehmung des Hausrechts oder berechtigter Interessen im Einzelfall erforderlich sein sollte, darf sie nur in Betrieb genommen werden, wenn schutzwürdige Interessen der Betroffenen nicht überwiegen.

Vorzunehmen ist eine Abwägung zwischen den berechtigten Interessen der Verkehrsunternehmen und dem informationellen Selbstbestimmungsrecht der von einer Videoüberwachung betroffenen Fahrgäste. Dabei darf die Intensität der Grundrechtsbeschränkung aufgrund der Überwachungsmaßnahme nicht außer Verhältnis zu dem Gewicht des Überwachungsinteresses stehen. Bei der Abwägung sind die Gesamtumstände jedes Einzelfalls maßgeblich. Entscheidend ist insbesondere die Eingriffsintensität der jeweiligen Maßnahme. Diese wird durch Art und Umfang der erfassten Informationen (Informationsgehalt und Informationsdichte), durch Anlass und Umstände der Erhebung (zeitliches und räumliches Ausmaß des Videoeinsatzes), durch den betroffenen Personenkreis und die Art und den Umfang der Verwertung der erhobenen Daten bestimmt.

So stellt eine zeitlich und räumlich lückenlose Überwachung des Fahrgastraumes, der sich die Fahrgäste nicht entziehen können, einen intensiveren Eingriff dar als eine nur zeitweilige Beobachtung, die nur Teilbereiche des Raumes erfasst. Dasselbe gilt hinsichtlich der typischen Aufenthaltsdauer der Fahrgäste im Verkehrsmittel: je länger der Beförderungsvorgang andauert, desto intensiver ist der von einer Videoüberwachung ausgehende Eingriff in das Recht auf informationelle Selbstbestimmung der Fahrgäste. Die informationelle Selbstbestimmung wird zudem besonders intensiv bei der Überwachung von Bereichen betroffen, in denen Menschen typischerweise miteinander kommunizieren. Hinzu kommt, dass die Fahrgäste häufig auf die Nutzung öffentlicher Verkehrsmittel angewiesen sind und nur bedingt auf andere Verkehrsmittel ausweichen können. Zudem wird durch eine Videoüberwachung in öffentlichen Verkehrsmitteln eine Vielzahl von Personen betroffen, die durch ihr Verhalten keinerlei Anlass für eine solche Überwachungsmaßnahme bieten.

Eine Videoüberwachung in öffentlichen Verkehrsmitteln kann daher nur zum Schutz von Rechtsgütern erheblichen Gewichts gerechtfertigt sein.

Vor dem Einsatz einer Videoüberwachung in öffentlichen Verkehrsmitteln ist im Rahmen einer abwägenden Einzelfallprüfung nach Strecken, Tageszeiten und Fahrzeugbereichen zu differenzieren und gemäß § 6b BDSG entsprechend zu beschränken. Maßstab für eine Differenzierung können beispielsweise die Anzahl von Vorkommnissen, Schadenshöhe sowie Art von Ereignissen in der Vergangenheit (Sachbeschädigung, Missbrauch von

Notrufeinrichtungen etc.) sein. Eine generelle, zeitlich und räumlich durchgängige Videoüberwachung des gesamten Fahrgastbereichs ist daher nach § 6b BDSG in aller Regel unverhältnismäßig und somit unzulässig. Bei der Beschaffung einer Videoüberwachungseinrichtung sollte darauf geachtet werden, dass die technischen Möglichkeiten für eine Differenzierung bestehen.

Da sich die Intensität des von einer Videoüberwachung ausgehenden Eingriffs in das informationelle Selbstbestimmungsrecht der Fahrgäste durch eine längere Aufenthaltsdauer in überwachten Bereichen deutlich erhöht, kann auf längeren Strecken – wie beispielsweise dem länderübergreifenden Bahnbetrieb – eine Videoüberwachung nur auf Streckenabschnitten mit häufigen und schwerwiegenden Eingriffen in Rechtsgüter erheblichen Gewichts in Betracht kommen. Nur geringfügige oder vereinzelt auftretende Beeinträchtigungen dieser Rechtsgüter können dort keine Videoüberwachung der Fahrgastbereiche rechtfertigen. Eine solche kann aufgrund ihrer hohen Eingriffsintensität auf längeren Streckenabschnitten allenfalls in Ausnahmefällen erfolgen.

2.2 Videoüberwachung von Beschäftigten

Sofern in öffentlichen Verkehrsmitteln auch Arbeitsplätze von Beschäftigten von optisch-elektronischen Einrichtungen erfasst werden (z. B. der zum Zutritt für Fahrgäste hin offene Fahrerplatz in Bussen), ist Folgendes zu beachten:

In Fällen, in denen die Erfassung der Arbeitsplätze der Beschäftigten lediglich eine Nebenfolge der zulässigen Überwachung des Publikumsverkehrs darstellt, ist das Einrichten von sog. Privatzonen, d. h. das dauerhafte Ausblenden von Bereichen, in denen sich nur die Beschäftigten aufhalten, erforderlich. Vorzugsweise ist die Kamera jedoch so zu installieren, dass sich kein ständiger Arbeitsplatz im Erfassungsbereich befindet.

Wird ausschließlich der Fahrerarbeitsplatz (z. B. der durch eine Tür vom Fahrgastraum getrennte Fahrzeugführerstand) durch Kameras erfasst, richtet sich die datenschutzrechtliche Zulässigkeit einer solchen Maßnahme nach § 32 BDSG. Das Erheben, Verarbeiten oder Nutzen personenbezogener Daten der Beschäftigten durch eine Videoüberwachungsanlage kann allerdings in der Regel nicht auf § 32 Abs. 1 Satz 1 BDSG gestützt werden. Denkbar ist zwar eine offene Videoüberwachung zur Erfüllung der Schutzpflicht des Arbeitgebers gegenüber seinen Beschäftigten, wenn eine Videoüberwachung in besonders gefahrträchtigen Arbeitsbereichen erforderlich ist. Davon kann bei einem abgeschlossenen Fahrerarbeitsplatz jedoch in aller Regel nicht ausgegangen werden. Selbst wenn in Ausnahmefällen hier eine Videoüberwachung in Betracht kommen sollte, ist der Erfassungsbereich der Kamera auf den sicherheitsrelevanten Bereich zu beschränken und der Beschäftigte ist auszublenden.

Im Übrigen dürfen personenbezogene Daten eines Beschäftigten insbesondere mittels Videoüberwachung nur zur Aufdeckung einer Straftat nach Maßgabe des § 32 Abs. 1 Satz 2 BDSG erhoben, verarbeitet oder genutzt werden. Erforderlich sind hier zu dokumentierende tatsächliche Anhaltspunkte, die den Verdacht begründen, dass der Beschäftigte 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. Liegen diese Voraussetzungen vor, ist eine Videoüberwachung gleichwohl nur für einen befristeten Zeitraum zulässig, sofern diese Maßnahme das einzige Mittel zur Überführung eines der Begehung von Straftaten konkret verdächtigten Beschäftigen darstellt. Eine dauerhafte Videoüberwachung von Beschäftigten ohne konkreten Verdacht ist hingegen datenschutzwidrig. Insbesondere dürfen Kameras nicht zur Kontrolle von Arbeitsleistungen, Sorgfalt und Effizienz verwendet werden.

Vor diesem Hintergrund muss das Verkehrsunternehmen nicht zuletzt auch dafür Sorge tragen, dass mittels der in den Fahrzeugen installierten Kameras keine Überwachung des in den Betriebshöfen mit der Reinigung, Reparatur und Wartung beauftragten technischen Personals erfolgen kann. Dies kann beispielsweise durch den Einbau diesbezüglicher Werkstattschalter oder die Kopplung des Kamerabetriebs an die Eingabe einer Linienkennung erreicht werden.

3. Maßnahmen vor Einrichtung einer Videoüberwachung

Die Verantwortung für eine datenschutzgerechte Videoüberwachung liegt auch dann beim Verkehrsunternehmen, wenn es Fahrzeuge mit eingebauter Videoüberwachungstechnik, die von anderer Seite, z. B. von der die Verkehrsleistung beauftragenden lokalen Nahverkehrsgesellschaft (LNVG) zur Verfügung gestellt worden sind, verwendet. Daher obliegt es auch dem Verkehrsunternehmen, vor der Inbetriebnahme von Videoüberwachungskameras den damit verfolgten Zweck in einer Verfahrensbeschreibung festzulegen.

3.1 Betrieblicher Datenschutzbeauftragter

Der oder die betriebliche Datenschutzbeauftragte des Verkehrsunternehmens ist über die geplante Einrichtung einer Videoüberwachung rechtzeitig zu unterrichten, da hier die Zuständigkeit für die Durchführung der Vorabkontrolle liegt (§ 4d Abs. 5 und 6 BDSG). Er oder sie trägt außerdem dafür Sorge, dass eine Beschreibung des Verfahrens „Videoüberwachung“ mit den Angaben nach § 4e Satz 1 Nrn. 1 bis 8 BDSG auf Antrag jedermann in geeigneter Weise verfügbar gemacht wird.

3.2 Information der Fahrgäste

An jedem Fahrzeug, das videoüberwacht wird, müssen Hinweisschilder / Piktogramme / Displays außen die Videoüberwachung kenntlich machen (vgl. § 6b Abs. 2 BDSG).

Der Hinweis ist so anzubringen, dass der Fahrgast ihn beim Eintritt in den überwachten Bereich im normalen Blickwinkel hat und nicht erst von ihm gesucht werden muss, auch bei geöffneten Türen. Der Betroffene muss einschätzen können, welcher Bereich von einer Kamera erfasst wird, damit er in die Lage versetzt wird, gegebenenfalls der Überwachung auszuweichen oder sein Verhalten anzupassen.

Durch geeignete Maßnahmen muss die verantwortliche Stelle mit Anschrift erkennbar sein. Entscheidend ist dabei, dass für den Betroffenen problemlos feststellbar ist, an wen er sich bezüglich der Wahrung seiner Rechte wenden kann. Daher ist die verantwortliche Stelle mit ihren Kontaktdaten explizit zu nennen.

3.3 Dienstanweisung

Erforderlich ist eine Dienstanweisung, in der alle mit der Videoüberwachung zusammenhängenden Fragen und Probleme geregelt werden.

In der Dienstanweisung müssen unter anderem auch die zu benutzenden Datenträger, auf denen die Speicherung der Bilddaten erfolgen soll, festgelegt werden. Außerdem müssen die besonderen Gründe festgelegt werden, aufgrund derer die Beweis sichernden Bilder der Aufzeichnung entnommen und auf einen neuen Datenträger übertragen werden dürfen sowie wann die Aufzeichnung zu löschen ist. Die Beschäftigten, die Zugang zu den Aufzeichnungen haben, müssen mit ihrer Funktionsbezeichnung (nicht namentlich) bestimmt werden. Schließlich soll die verantwortliche Person bestimmt sein, die eine zu Beweiszwecken identifizierte Person zu benachrichtigen hat (§ 6b Abs. 4 BDSG).

3.4 Mitbestimmung durch die Betriebs- / Personalvertretung

Bei der Videoüberwachung von Beschäftigten handelt es sich regelmäßig um eine Maßnahme, die zur Überwachung des Verhaltens und der Leistung der Beschäftigten geeignet ist. Ihre Einführung und Anwendung unterliegt gemäß § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) der Mitbestimmung durch den Betriebsrat. In einer Betriebsvereinbarung sollte deshalb darauf hingewirkt werden, dass die Datenerhebung und die Auswertung in so engen Grenzen gehalten werden wie möglich. Dabei werden folgende Punkte als Bestandteil einer Betriebsvereinbarung festzulegen sein:

- Gegenstand der Datenerhebung, -verarbeitung oder -nutzung
- Art und Umfang der erhobenen, verarbeiteten oder genutzten Daten
- Zweckbeschreibung
- Datenvermeidung- und Datensparsamkeit
- Empfängerin und/oder Empfänger der Daten
- Rechte der Betroffenen
- Löschungsfristen
- Beschreibung der technischen und organisatorischen Maßnahmen (Anlage zu § 9 Abs. 1 BDSG), insbesondere Erstellung eines Berechtigungskonzepts.

Eine solche Betriebsvereinbarung wird dazu beitragen, die Erfüllung der gemeinsamen Aufgaben von Arbeitgeberin bzw. Arbeitgeber und Betriebsrat sicherzustellen, die freie Entfaltung der Persönlichkeit der im Betrieb Beschäftigten zu schützen und zu fördern (§ 75 Abs. 2 BetrVG).

In Unternehmen ohne Betriebsrat sollten Arbeitgeberinnen und Arbeitgeber Regelungen in Dienstanweisungen treffen.

4. Durchführung einer zulässigen Videoüberwachung

4.1 Löschungspflicht

Bei der nicht anlassbezogenen Aufzeichnung in einer Black-Box erfolgt – sofern kein Vorkommnis festgestellt wird – die Löschung der Aufzeichnung ohne Kenntnisnahme der aufgezeichneten Bilder unverzüglich.

Die Frist beginnt spätestens, wenn sich das Verkehrsmittel nicht mehr im täglich festgelegten Einsatz befindet und eine Überprüfung etwaiger Vorkommnisse durch eine verantwortliche Person möglich ist. Die Löschung soll daher im Regelfall nach 48 Stunden erfolgen. In begründeten Einzelfällen kann eine längere Speicherfrist angenommen werden, wenn beispielsweise das Verkehrsmittel nicht innerhalb dieser Frist zu einem Ort zurückkehren kann, an dem festgestellte und aufgezeichnete Vorfälle gesondert gesichert werden können.

Im Falle einer anlassbezogenen Aufzeichnung (ob mit oder ohne Historie) erfolgt die Löschung unverzüglich nach Prüfung der Bilder zum Zwecke der Beweissicherung; hierzu geeignete Bilder werden auf einem neuen Datenträger gespeichert und die Übrigen unverzüglich gelöscht.

4.2 Unterrichtungspflicht

Werden die Kameraaufnahmen einer bestimmten Person zugeordnet, ist diese Person darüber zu unterrichten (§ 6b Abs. 4 BDSG). Zweck dieser Regelung ist es, der identifizierten Person die Überprüfung der Rechtmäßigkeit der Datenverarbeitung und die Verfolgung ihrer Rechte zu ermöglichen. Inhaltlich geht die Unterrichtungspflicht über die Hinweispflicht hinaus. Die Unterrichtung hat über die Art der Daten, die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Identität der verarbeitenden Stelle zu erfolgen.

4.3 Übermittlung von Videosequenzen an Polizei und Staatsanwaltschaft

Nach § 6b Abs. 3 Satz 2 BDSG können gespeicherte Videoaufnahmen zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten an Polizei oder Staatsanwaltschaft herausgegeben werden.

Können bzw. müssen angeforderte Videosequenzen zulässigerweise an Polizei oder Staatsanwaltschaft herausgegeben werden, so müssen der Grund der Übermittlung, Art und Umfang der übermittelten Videodaten, Speichermedium sowie der Zeitpunkt der Übergabe und der Name der die Daten im Empfang nehmenden Person dokumentiert werden (vgl. Anlage zu § 9 BDSG).

4.4 Ausschreibungen

In Ausschreibungen, insbesondere durch die Verkehrsgesellschaften der Länder als Aufgabenträger für den schienengebundenen Personennahverkehr (SPNV), sind die Grundsätze dieser Orientierungshilfe zu beachten. Ausschreibungen, die z. B. pauschal eine „möglichst umfassende“ Videoüberwachung fordern, entsprechen diesen Grundsätzen nicht und richten sich auf Videoüberwachungsmaßnahmen, die mit § 6b BDSG nicht zu vereinbaren sind.

4.5 Überprüfung der Rechtmäßigkeitsvoraussetzungen

Verkehrsunternehmen, die in ihren Fahrzeugen eine Videoüberwachungsanlage betreiben, sind verpflichtet, die rechtlichen Voraussetzungen für deren Betrieb in regelmäßigen Abständen zu überprüfen. Insbesondere die Frage der Erforderlichkeit der Maßnahme ist zu evaluieren. Lassen sich zum Beispiel nach Ablauf eines Jahres, in dem die Kameras in Betrieb waren, keine Tatsachen (mehr) feststellen, welche die Annahme rechtfertigen, dass das überwachte Objekt gefährdet ist, oder wurde der mit der Überwachung angestrebte Zweck nicht erreicht, darf die Videoüberwachungsanlage nicht weiter betrieben werden. Das Ergebnis der Überprüfung sollte dokumentiert werden.

16.1.2 Videoüberwachung in Schwimmbädern – Zusatz zur Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ vom 19.2.2014

Stand 10. August 2015

Da der Besuch von Schwimmbädern auch mit einigen Risiken verbunden sein kann, greifen viele Betreiber zum Hilfsmittel der Videoüberwachung, sei es, beispielsweise, um den Aufbruch von Spinden oder die unsachgemäße Benutzung der Rutsche zu verhindern. Schwimmbäder, die sich in öffentlicher Trägerschaft befinden, sind nach dem geltenden Landesrecht zu prüfen.

Ansonsten findet das Bundesdatenschutzgesetz (BDSG) Anwendung, weshalb die in der Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ des Düsseldorfer Kreises (OH Videoüberwachung) beschriebenen Grundsätze für diese Schwimmbäder anwendbar sind.

Der Großteil der in Schwimmbädern befindlichen Kameras überwacht Bereiche, die für die Kunden zugänglich sind. Für diese öffentlich zugänglichen Räume beurteilt sich die datenschutzrechtliche Zulässigkeit nach § 6b BDSG.

Da sich die Schwimmbadbesucher im Schwimmbad zum Zweck der Freizeitgestaltung aufhalten, genießen sie besonderen Schutz (vgl. OH Videoüberwachung) und die Prüfung des Vorliegens der gesetzlichen Voraussetzungen bedarf besonderer Sorgfalt. Nach § 6b BDSG muss die Videoüberwachung zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich sein und es dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Unabhängig von der Frage eines berechtigten Interesses oder der befugten Hausrechtsausübung ist eine Videoüberwachung jedenfalls nicht erforderlich zur Verhinderung des unberechtigten Zutritts zu Bereichen, für die ein zusätzliches Entgelt (z. B. zum Saunabereich) zu entrichten ist. Dies kann durch andere geeignete Maßnahmen, wie hohe Drehkreuze oder Schranken ohne unverhältnismäßigen Aufwand verhindert werden.

Besonderes Augenmerk ist auf das erforderliche Maß der Überwachung zu richten: Sofern die übrigen Voraussetzungen vorliegen, ist der Aufnahmebereich der Kamera ausschließlich auf den Bereich (z. B. Kassenautomaten) zu richten, den der Zweck der Videoüberwachung betrifft. Zur Sicherung von Beweisen im Falle von Einbrüchen reicht eine Videoaufzeichnung außerhalb der Öffnungszeiten.

Zur Abwehr von den mit dem Baden verbundenen Gefahren ist eine Videoaufzeichnung nicht erforderlich. Im Ausnahmefall kann eine reine Beobachtung („verlängertes Auge“) zulässig sein, wenn sie der Unterstützung der Badeaufsicht an besonders gefährlichen oder unübersichtlichen Orten dient. Die Gefährlichkeit dieser Stellen muss sich aufgrund objektiver Anhaltspunkte ergeben, beispielsweise, weil es bereits konkrete Vorfälle gegeben hat oder Erfahrungswerte für eine erhöhte Gefährlichkeit (wie z. B. bei Sprungtürmen, Rutschen, Kinderbecken) sprechen. Nicht ausreichend ist die allgemein erhöhte Unfallgefahr wegen des Aufenthalts im Wasser. Der Einsatz von Videoüberwachungstechnik kann kein Ersatz für Aufsicht durch Personal sein!

Eine Videoaufzeichnung ausschließlich zum Ausschluss des Haftungsrisikos gegenüber Ansprüchen von Badegästen ist aufgrund der überwiegenden schutzwürdigen Interessen der von der Videoüberwachung Betroffenen unzulässig. Es ist nicht verhältnismäßig, einen derartigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung für eine große Zahl von Personen hinzunehmen, nur, damit das Schwimmbad im Zweifel die Möglichkeit hat, seine Haftung auszuschließen. Eine Haftung unterliegt zudem der Beweispflicht des Geschädigten. Die Rechtsprechung fordert keinen Nachweis der hinreichenden Wahrnehmung der Verkehrssicherungspflicht mit Videoaufzeichnungen.[1]

Schutzwürdige Interessen der Betroffenen überwiegen immer, wenn die Intimsphäre des Betroffenen berührt ist, weswegen eine Videoüberwachung von Personen in Sanitärräumen, Umkleidekabinen oder Umkleidebereichen und in der Sauna generell unzulässig ist.

Eine Videoüberwachung kann im Einzelfall zur Sicherung von Beweismitteln bei nachgewiesenen Spindaufbrüchen zulässig sein, sofern nicht gleichzeitig Bänke/Ablageflächen oder Umkleidebereiche erfasst werden. Voraussetzung ist, dass den Badegästen eine echte Wahlmöglichkeit eingeräumt wird, in welchen Bereich sie sich begeben. Dabei sind Bereiche, die videoüberwacht werden, von solchen, in denen keine Überwachung stattfindet, erkennbar zu trennen, beispielsweise durch farbige Markierung des Fußbodens.

Unverhältnismäßig und damit nicht zulässig ist jedenfalls die Videoüberwachung aufgrund von Bagatellschäden (z. B. Beschädigung von Haartrocknern).

[1] OLG Koblenz, Beschluss vom 07.05.2010, Az.: 8 U 810/09: Der Betreiber genügt seiner Verkehrssicherungspflicht, wenn durch Hinweisschilder mit ausformulierten Warnhinweisen oder mit Piktogrammen auf die Problempunkte eindeutig hingewiesen wird; LG Münster, Urteil vom 17.05.2006, Az.: 12 O 639/04: Der Betreiber eines Schwimmbads genügt seiner Verkehrssicherungspflicht, wenn er einen Bademeister bereitstellt, der sein Augenmerk auch - wenn auch nicht ununterbrochen - auf die besonderen Schwimmbadeinrichtungen (hier: ins Nichtschwimmerbecken führende Kinderrutsche) richtet.

Darüber hinaus sind die in der OH Videoüberwachung unter Ziffer 2.2 benannten Maßnahmen (z. B. Verfahrensverzeichnis, Vorabkontrolle, Hinweisbeschilderung) zu beachten. Dazu gehört auch, Bildschirme so zu positionieren, dass sie nicht für Dritte einsehbar sind.

16.1.3 Nutzung von Kameradrohnen durch Private

In jedem Elektronikmarkt sind sie mittlerweile zu finden: Drohnen mit Kameraausstattung zu einem erschwinglichen Preis. Drohnen kommen als unbemannte Luftfahrzeuge nicht nur in Krisengebieten oder in der Landwirtschaft zum Einsatz, sondern werden immer häufiger auch von Privaten für die Freizeitbeschäftigung gekauft und im nachbarschaftlichen Umfeld eingesetzt. Da können durchaus Begehrlichkeiten aufkommen: ein unbeobachteter Blick in den Garten des Nachbarn, auf die Sonnenterrasse oder in sonstige nicht einfach zugängliche Orte.

Der potentiell überwachbare Bereich wird nur von den technischen Gegebenheiten des eingesetzten Geräts begrenzt. Mauern, Zäune oder sonstige Abtrennungen, die Dritten das Betreten des so geschützten Bereichs oder den Einblick in diesen erschweren oder unmöglich machen sollen, stellen im Rahmen des Drohneneinsatzes kein Hindernis mehr dar. Darüber hinaus ist es für Betroffene auch regelmäßig nicht ohne weiteres möglich, den für den Drohneneinsatz Verantwortlichen zu erkennen. Aus diesen Gründen kann der Einsatz von mit Videokameras ausgerüsteten Drohnen im Vergleich zum Einsatz stationärer Videoüberwachungsmaßnahmen mit einem ungleich größeren Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen verbunden sein.

Auch wenn der Betrieb von Drohnen durch Privatpersonen zu Zwecken des Sports oder der Freizeitgestaltung mit Ausnahme von § 16 Abs. 1 Nr. 1 LuftVO keiner luftverkehrsrechtlichen Erlaubnis der zuständigen Landesluftfahrtbehörde bedarf und im Hinblick auf § 1 Abs. 2 Nr. 3 des Bundesdatenschutzgesetzes (BDSG) außerhalb des datenschutzrechtlichen Regelungsregimes erfolgen kann, sind Verwendungen von Drohnen mit Videotechnik denkbar, die in den Anwendungsbereich des BDSG fallen. In solchen Fällen sind Drohnen nur im Rahmen von datenschutzrechtlichen Erlaubnisnormen zu betreiben, wobei deren Voraussetzungen in der Mehrzahl der Fälle wegen des regelmäßigen Überwiegens von Interessen Betroffener nicht gegeben sind. Dies ist insbesondere dann der Fall, wenn die Aufnahmen für eine Veröffentlichung im Internet stattfinden oder ein zielgerichteter Drohneneinsatz zur kontinuierlichen Beobachtung öffentlich zugänglicher Räume im Sinne des § 6b BDSG erfolgt. Wenn solche Drohnen innerhalb des Anwendungsbereiches des BDSG betrieben werden und hierbei unbefugt Daten erhoben oder verarbeitet werden, kann die zuständige Behörde hierfür ein Bußgeld von bis zu 300.000 Euro verhängen.

Jedoch sind auch außerhalb des Anwendungsbereiches des BDSG rechtliche Rahmenbedingungen zu beachten. So sind auch hier das Recht am eigenen Bild, das Grundrecht der Betroffenen auf informationelle Selbstbestimmung im Besonderen sowie das Persönlichkeitsrecht im Allgemeinen zu wahren.

Dem mit dem Drohneneinsatz verbundenen Eingriff in das allgemeine Persönlichkeitsrecht Betroffener kann neben den Möglichkeiten der zuständigen Aufsichts- oder Bußgeldbehörde auch zivilrechtlich begegnet werden. Vor allem dann, wenn die Verletzung des allgemeinen Persönlichkeitsrechts in einem Eindringen in geschützte Bereiche, wie beispielsweise das befriedete und blickgeschützte Grundstück, besteht oder eine zielgerichtete Beobachtung erkennbar stattfindet. Dem Betroffenen kann in solchen Fällen ein Abwehranspruch aus § 823 in Verbindung mit § 1004 Abs. 1 des Bürgerlichen Gesetzbuches (BGB) analog zustehen. Auch das Kunsturhebergesetz (KUG), welches das Recht am eigenen Bild – als besondere Ausprägung des allgemeinen Persönlichkeitsrechts – schützt, kann tangiert sein (§§ 22, 23 KUG), sofern eine Verbreitung oder Veröffentlichung der Aufzeichnungen erfolgt.

Die Strafverfolgungsbehörden können eingeschaltet werden, wenn durch den Drohneneinsatz die Verwirklichung von Straftatbeständen droht, wie beispielsweise bei der Anfertigung von Bildaufnahmen höchstpersönlicher Lebensbereiche (§ 201a des Strafgesetzbuches (StGB)), mithin Bereiche der Intimsphäre (im Einzelnen dazu: Bundestagsdrucksache 15/2466, S. 5.) oder der Aufzeichnung des nichtöffentlich gesprochenen Wortes (§ 201 StGB).

Der Düsseldorfer Kreis fordert daher Drohnenbetreiber auf, grundsätzlich niemanden ohne seine Einwilligung zu filmen und die Privatsphäre anderer zu achten. Private Nutzer dürfen Drohnen mit Foto- oder Videoausrüstung nur in solchen Bereichen einsetzen, in denen eine Verletzung von Rechten Dritter ausgeschlossen werden kann.

16.1.4 Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste

Die Orientierungshilfe richtet sich an die Anbieter von Smart-TV-Diensten und -Produkten. Hierzu zählen insbesondere Gerätehersteller, Portalbetreiber, App-Anbieter, Anbieter von Empfehlungsdiensten und Anbieter von HbbTV-Angeboten. Die Orientierungshilfe gibt einen Überblick über die datenschutzrechtliche Bewertung durch die Aufsichtsbehörden.

Stand: September 2015, Version 1.0

Inhaltsverzeichnis

1. Einleitung

Fernsehgeräte der ersten Generation waren reine Empfangsgeräte. Programme wurden zunächst terrestrisch, später über Kabel und Satellit ausgestrahlt. Sendeschemata, Zusatz- oder Hintergrundinformationen zu dem Programm konnte das Fernsehpublikum durch Zeitungen oder Zeitschriften zur Kenntnis nehmen. Reaktionen zum Programm erfolgten auf getrennten Kommunikationswegen wie Brief, Telefon oder E-Mail. Parallel dazu entwickelte sich das Internet mit der Möglichkeit der unmittelbaren Kommunikation in alle Richtungen. Die rasant fortschreitende Konvergenz der Medien führt dazu, dass das Fernsehen, der Hörfunk und die Kommunikation über das Internet zusammenwachsen und der Markt insofern darauf reagiert, als – von der Fernsehseite aus betrachtet – mittlerweile fast ausschließlich Geräte angeboten werden, die diese Funktionalitäten zusammenführen.

Da nach der Verbindung eines „smarten“ Fernsehgerätes mit dem Internet nicht mehr nur (Rundfunk-)Signale empfangen werden, sondern vielmehr ein Rückkanal zu den jeweiligen Diensteanbietern existiert, stellen sich aus datenschutzrechtlicher Sicht zahlreiche Fragen, insbesondere, wann und welche personenbezogenen Daten bei Nutzung der unterschiedlichen Angebote fließen, wer diese Daten zu welchen Zwecken erhält, ob eine Erlaubnis für das Erheben und die weitere Verwendung der Daten existiert, ob die Datenschutzgrundsätze eingehalten werden und inwieweit technisch-organisatorische Maßnahmen dem jeweiligen Schutzbedarf entsprechen.

Diese Orientierungshilfe richtet sich an die Anbieter von Smart-TV-Diensten, insbesondere Gerätehersteller, Portalbetreiber, App-Anbieter, Anbieter von Empfehlungsdiensten und von HbbTV-Angeboten. Sie enthält nach Beschreibung der relevanten Begriffe (Kapitel 2) einen kurzen Überblick über die Struktur der Smart-TV-Nutzung einschließlich der beteiligten Anbieter (Kapitel 3), der gesetzlichen Grundlagen für die jeweilige Kommunikation (Kapitel 4 bis 6) und daraus folgend eine Darstellung der konkreten datenschutzrechtlichen und technisch-organisatorischen Anforderungen an Smart-TV-Dienste (Kapitel 7).

2. Begriffsbestimmungen

2.1 Auftragsdatenverarbeiter

Nimmt eine andere Stelle Datenverarbeitungen im Auftrag des eigentlichen Diensteanbieters bzw. der eigentlichen verantwortlichen Stelle und somit streng weisungsgebunden vor, so werden diese Datenverarbeitungen dem Auftraggeber zugerechnet. Den Auftraggeber treffen vielfältige Sorgfalts- und Kontrollverpflichtungen, die in § 11 Bundesdatenschutzgesetz (BDSG) dargestellt und geregelt sind. Dem Auftragnehmer ist es untersagt,

personenbezogene Daten für andere Zwecke als diejenigen der verantwortlichen Stelle zu erheben und zu verwenden. Obwohl er verpflichtet ist, die Weisungen des Auftraggebers zu befolgen, obliegt es ihm, den Auftraggeber unverzüglich darauf hinzuweisen, wenn und soweit eine Weisung gegen Datenschutzbestimmungen verstößt.

Kein Auftragsdatenverarbeitungsverhältnis i. S. d. § 11 BDSG liegt jedoch vor, wenn ganze Funktionalitäten ausgelagert werden und eine andere Stelle personenbezogene Daten in eigener Verantwortung erhebt und verwendet. Dann ist die andere Stelle als Dritter tätig und unterliegt deshalb den datenschutzrechtlichen Anforderungen in eigener Verantwortung.

2.2 HbbTV

Die Abkürzung HbbTV steht für Hybrid Broadcasting Broadband TV und bedeutet, dass sowohl das Rundfunksignal (Broadcasting) als auch das Breitbandinternet (Broadband) genutzt werden, um dem Fernsehzuschauer neben der Rundfunksendung auch zahlreiche weitere Zusatzinformationen anzubieten. Dabei wird mittels des Rundfunksignals entweder der (erste) Inhalt einer HbbTV-HTML-Seite oder eine HTTP-URL mitgeliefert, anhand derer ein Smart-TV eine spezielle HbbTV-HTML-Seite über das Internet von einem Server des Fernsehsenders laden kann.

Derzeit werden über HbbTV z. B. Zusatzinformationen zum TV-Programm durch die Sender zur Verfügung gestellt, ein Zugriff auf Mediatheken und soziale Netzwerke ermöglicht und elektronische Programmzeitschriften sowie sonstige Seiten zum Aufruf angeboten. Ferner ist denkbar, z. B. Merchandising-Artikel zu einem Spielfilm parallel über HbbTV anzubieten oder Zuschauerumfragen in Echtzeit zu schalten. Darüber hinaus könnte über HbbTV die Schaltung von interessenbezogener Werbung (nicht nur durch die Sender, sondern auch durch Dritte) bei direkter Möglichkeit zur Reichweitenmessung und Nutzungsanalyse erfolgen.

2.3 Lineares Verfahren/Karussellverfahren

Das Rundfunksignal enthält für die Bereitstellung von HbbTV-Inhalten eine Datentabelle (Application Information Table – AIT), anhand deren Einträge der Transportweg des HbbTV-Contents (z. B. der Startseite) definiert wird. Ist hierfür das „DSMCC Object Carousel“ eingetragen, werden darstellbare Inhalte über das lineare Rundfunksignal ausgeliefert. In diesem Fall ist es im Vergleich zu dem Broadband-Verfahren, das Inhalte der Startseite über den Internet-Rückkanal lädt, nicht notwendig, dass Nutzungsdaten vor dem Drücken des Red Buttons (siehe 2.5) übertragen werden. Sollen dynamische oder personalisierte Inhalte nach Drücken des Red Buttons angeboten werden, könnte über das

lineare Verfahren der Inhalt der verkleinerten Darstellung der HbbTV-Startseite (bestehend z. B. aus HTML, CSS und Grafikdateien) ausgeliefert werden; die anderen (dynamischen) Inhalte könnten dann in der HbbTV-Anwendung gekapselt und damit erst bei Erkennen des Events, das mit dem Drücken des Red Buttons zusammenhängt, aktiviert werden und über den Internet-Rückkanal könnten sodann weitere Inhalte geladen werden.

2.4 Personenbezogene Daten

Personenbezogene Daten sind gem. § 3 Abs. 1 BDSG „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“. Hiernach gelten alle Informationen, die einen Rückschluss auf eine Person erlauben, mindestens als bestimmbar, damit aber auch als personenbezogen und datenschutzrelevant. Bei der Frage, ob eine Bestimmtheit oder Bestimmbarkeit einer natürlichen Person gegeben ist, sind alle Mittel zu berücksichtigen, die vernünftigerweise entweder von der datenverarbeitenden Stelle oder einem Dritten eingesetzt werden können, um die betreffende Person zu bestimmen[1]. Gerade im Online-Umfeld bedarf es hierbei nicht zwingend einer Individualisierung mittels des bürgerlichen Namens, vielmehr genügt es, wenn eine Person „singularisiert“, d. h. als Individuum herausgehoben wird[2].

Speziell im Zusammenhang mit Smart-TV-Diensten stehende personenbezogene Daten sind u.a.

- **die IP-Adresse** des Nutzers, die – bei dynamischen IP-Adressen in Verbindung mit der Zeitangabe – nach Ansicht der Datenschutzaufsichtsbehörden ein personenbezogenes Datum und auch bei Smart-TV-Diensten für die Internetkommunikation notwendig ist und
- **Geräte-IDs[3]**, die dauerhaft mit dem Gerät verbunden sind und regelmäßig einer Person zugeordnet werden können (z. B. bei Registrierung).

Dass unter Umständen mehrere Personen ein Fernsehgerät nutzen, führt nicht dazu, dass bei den genannten Informationen nicht mehr von einem Personenbezug auszugehen ist. Dem Diensteanbieter ist (zunächst) nicht bekannt, ob sich hinter einer IP-Adresse oder Geräte-ID wie der MAC-Adresse oder der Seriennummer nur ein Nutzer der Smart-TV-Dienste oder mehrere Personen verbergen, welche die Dienste über die gleiche Kennung in Anspruch nehmen. Da dies nicht erkennbar ist und auch nicht ausgeschlossen werden kann, gehen die Datenschutzbehörden in Europa davon aus, dass ein einzelner Nutzer

[1] Vgl. Art. 2 a) Richtlinie 95/46/EG und Erwägungsgrund 26; Stellungnahme 4/2007 zum Begriff „personenbezogener Daten“ der Artikel 29-Gruppe (WP 136, S.17).
[2] WP 136, S. 16.
[3] Vgl. WP 136, S.16, WP 202, Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten, S.10; „Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter“ des Düsseldorfer Kreises vom Juni 2014, S.5.

jedenfalls hinter einem relevanten, hohen Prozentsatz der Kennungen steckt.[4] Daher ist der Gesamtbestand der Daten als personenbezogen zu behandeln. Darüber hinaus ist es auch möglich, bei Heranziehung des Nutzungsverhaltens Unterscheidungen zu tätigen (z. B. kann anhand der gesehenen Sendungen das Geschlecht und ggf. das Alter eingeschätzt werden) und so die jeweils konkrete Person zu individualisieren. Bei einigen Geräten lassen sich außerdem Profile für die einzelnen Nutzer einrichten, wobei dann in der Regel personalisierte IDs verwendet werden, die zweifellos als personenbezogene Daten einzustufen sind.

Neben den dargestellten „speziellen" Daten können mittels der Smart-TV-Dienste zahlreiche weitere Arten personenbezogener Daten erhoben und verwendet werden, wie z. B.:

- **Audiodaten** mit Stimmaufnahmen
- **Foto- und Filmaufnahmen** einer Person
- **Informationen über die Smart-TV-Dienste-Nutzung**, d. h. Auskunft darüber, welche Funktionalität und welches Angebot vom Nutzer in Anspruch genommen wurden
- **Fernsehverhalten**, d. h. Informationen zu den angesehenen Fernsehinhalten (Fernsehprogramm, Zeitpunkt und Dauer)
- **Registrierungsdaten**, z. B. Name, E-Mail-Adresse, Heimatregion
- **Zahlungsdaten**, z. B. Bankverbindungen, Kreditkartendaten

2.5 Red Button

Ist ein HbbTV-Angebot verfügbar, wird dies dem Nutzer derzeit anhand eines kleinen Ausschnittes der HbbTV-Startseite am (unteren) Bildschirmrand angezeigt. Zugleich wird er aufgefordert, für die Inanspruchnahme des HbbTV-Angebots die rote Taste, den sog. Red Button, auf der Fernbedienung zu drücken, um die Startseite im Vollbildmodus aufrufen zu können.

2.6 Smart-TV

Smart-TV (= intelligenter Fernseher), auch Hybrid-TV genannt, ist die Bezeichnung für Fernsehgeräte mit Computer-Zusatzfunktionen und insbesondere Internet-Fähigkeit. Sogenannte smarte Fernsehgeräte verfügen neben der TV-Funktion u. a. über Zusatzschnittstellen wie z. B. USB und WLAN und meist über die HbbTV-Funktionalität (vgl. Definition HbbTV). Dadurch ist es mit diesen Geräten möglich, nicht nur Fernsehprogramme zu empfangen, sondern auch im Internet zu surfen, Filme in Echtzeit oder aus Online-

[4] vgl. WP 136, S. 20.

Videotheken abzurufen und über manche Geräte Videotelefonate zu führen. Darüber hinaus können diese Geräte, wie manche „normale“ Geräte bisher auch schon, auf Video-, Musik- und Bilddateien zugreifen, die auf einem PC oder USB-Stick gespeichert sind.

2.7 Telemedien

Telemedien sind nach § 1 Abs. 1 Telemediengesetz (TMG) alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 Telekommunikationsgesetz (TKG), die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 TKG oder Rundfunk nach § 2 des Rundfunkstaatsvertrages (RStV) sind.

Bei einer elektronisch im Wege der Telekommunikation erbrachten Dienstleistung, bei der Inhalte bereitgestellt werden, handelt es sich um einen elektronischen Informations- und Telekommunikationsdienst im o. g. Sinne.[5] Keine direkte Anwendung findet das TMG allerdings, wenn es sich dabei um Dienste handelt, die ganz in der Übertragung von Signalen (ohne Inhaltsangebot) liegen, wenn eine Individualkommunikation zwischen dem TK-Diensteanbieter (oder Dritten) und TK-Kunden, in deren Rahmen der TK-Diensteanbieter (oder Dritte) gegenüber TK-Kunden eine Inhaltsleistung erbringen[6] im Raum steht oder wenn ein linearer Informations- und Kommunikationsdienst angeboten wird, der eine für die Allgemeinheit und zum zeitgleichen Empfang bestimmte Veranstaltung und Verbreitung von Angeboten in Bewegtbild oder Ton entlang eines Sendeplans unter Benutzung elektromagnetischer Schwingungen (Rundfunk)[7] darstellt.

In der Regel ist somit dann von einem Telemediendienst auszugehen, wenn

- Inhalte (wie Bilder, Töne, Zeichen) online übertragen werden,
- die übertragende Stelle selbst nicht nur als neutraler Übermittler, sondern (auch) als Inhaltsanbieter tätig ist,
- die Inhaltsleistung zeitlich von der Übertragung trennbar ist und
- es sich nicht um einen linearen Dienst handelt, der nur anhand eines bestimmten Sendeplans zeitgleich von der Allgemeinheit empfangen werden kann.

2.8 Verantwortliche Stelle und Betroffene, Diensteanbieter und Nutzer

Verantwortliche Stelle ist nach der Definition in § 3 Abs. 7 BDSG jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

[5] Ricke, in: Spindler/Schuster, Recht der elektronischen Medien, 3. Auflage 2015, § 1 TMG Rn. 4.
[6] Vgl. BT-Drs. 16/3078, 13.
[7] Gem. § 47 RStV gelten bei Vorliegen eines Rundfunkdienstes die Vorschriften des TMG jedoch entsprechend.

Als **Betroffenen** definiert das BDSG jede natürliche Person, die durch personenbezogene Daten, d. h. Einzelangaben über persönliche oder sachliche Verhältnisse bestimmt oder bestimmbar gemacht werden kann (§ 3 Abs. 1 BDSG).

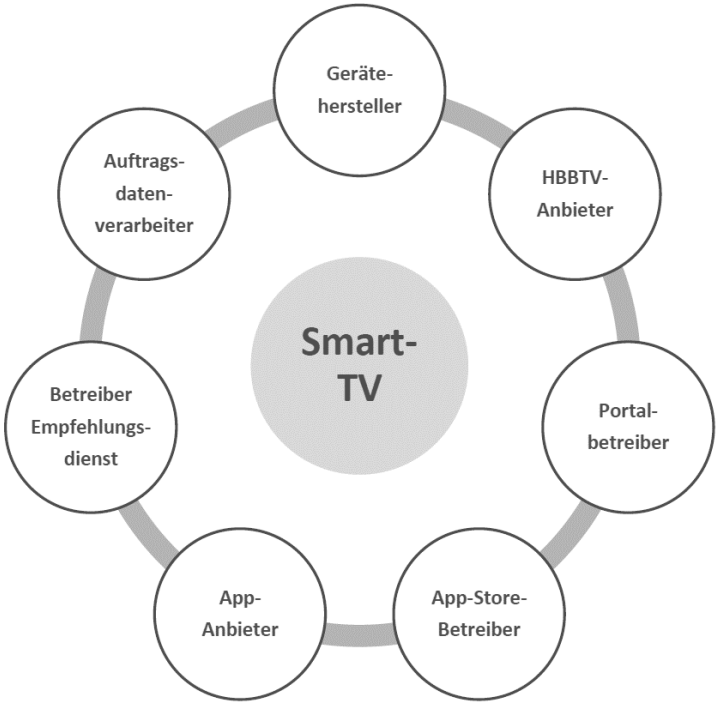
Diensteanbieter ist gemäß § 2 Nr. 1 TMG jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt; bei audiovisuellen Mediendiensten auf Abruf ist Diensteanbieter jede natürliche oder juristische Person, die die Auswahl und Gestaltung der angebotenen Inhalte wirksam kontrolliert. Im Bereich der Smart-TV-Nutzung ist hier vor allem zu denken an Anbieter von HbbTV-Angeboten, Anbieter von Web-Diensten, die über das Smart-TV-Gerät abrufbar sind, sowie Betreiber von Smart-TV-Plattformen, die den Zugang zu Web-Diensten ermöglichen.

Nutzer ist jede natürliche oder juristische Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen (§ 2 Nr. 3 TMG).

Diese unterschiedlichen Begrifflichkeiten leiten sich aus den unterschiedlichen Rechtsgrundlagen, dem BDSG und dem TMG her. Im Folgenden werden die Stellen, die mit personenbezogenen Daten umgehen (verantwortliche Stellen und Diensteanbieter) als Anbieter und die natürlichen Personen, mit deren personenbezogenen Daten umgegangen wird (Betroffene und Nutzer) als Nutzer bezeichnet (es sei denn, eine Differenzierung ist aus Gründen der Klarheit gefordert).

3. Anbieter in Zusammenhang mit Smart-TV

Smart-TV-Nutzung setzt sich, wie in der folgenden Grafik dargestellt, aus vielen verschiedenen Diensten zusammen. Dabei ist zu berücksichtigen, dass die Entwicklung von Geschäftsmodellen im Zusammenhang mit Smart-TV ebenso wie die technische Entwicklung sehr dynamisch ist und diese Grafik deshalb nur eine Momentaufnahme darstellt, die sich aus den Erkenntnissen der technischen Überprüfung durch das Bayerische Landesamt für Datenschutzaufsicht in eigener örtlicher Zuständigkeit und unter Mitwirkung der für die verschiedenen Hersteller von Smart-TV örtlich zuständigen Aufsichtsbehörden in den Monaten Dezember 2014 und Januar 2015 ergeben haben.



Da die datenschutzrechtlichen Grundlagen für die Beziehung zwischen dem Nutzer und den jeweiligen Anbietern von Smart-TV-Diensten unterschiedlich sind, ist es erforderlich, zunächst konkret festzustellen, wer welche Dienste in welcher Verantwortlichkeit anbietet, um dann prüfen zu können, welche gesetzlichen Grundlagen für den jeweiligen Dienst und den damit zusammenhängenden Datenumgang bestehen. Im Folgenden werden deshalb zunächst die in der obigen Grafik benannten Akteure näher dargestellt und bereits nach ihrer jeweiligen Verantwortlichkeit eingestuft. Welche Anforderungen einen Akteur in der Regel treffen und welche Empfehlungen die Aufsichtsbehörden für den konkreten Akteur aussprechen, wird nach einem allgemeinen datenschutzrechtlichen Überblick in Kapitel 7 näher erläutert.

Die folgende Aufzählung benennt die Akteure nach Funktionen getrennt; jedoch ist es nicht unüblich, dass eine Stelle auch mehrere Funktionen wahrnimmt (z. B. Gerätehersteller ist auch Portalbetreiber).

3.1 Gerätehersteller

Gerätehersteller produzieren nicht nur das Gerät, sondern führen bei der Nutzung des Gerätes als Smart-TV, d. h. nachdem das Gerät mit dem Internet verbunden wurde, häufig zumindest Update-Checks durch und spielen bei Bedarf neue Updates ein. Zudem erstellen sie oftmals Statistiken über die Bedienung des Gerätes, um z. B. die Benutzerfreundlichkeit verbessern zu können. Gerätehersteller sind für eine damit verbundene Erhebung und Verwendung personenbezogener Daten (z. B. Geräte-ID, IP-Adresse) verantwortliche Stelle. Gerätehersteller, die Telemedien anbieten, agieren zugleich als Telemedien-Diensteanbieter.

3.2 HbbTV-Anbieter

Soweit (Programm-)Anbieter Fernseh- und Hörfunkprogramme anbieten, ist dieser Vorgang nicht Gegenstand dieser Orientierungshilfe. Bietet der Sender selbst oder ein von ihm beauftragtes Unternehmen (vgl. Kapitel 2.1) daneben HbbTV-Zusatzangebote an, ist der Sender jedoch (auch) Telemedienanbieter und verantwortliche Stelle für den mit dem Zusatzangebot verbundenen Datenumgang. Mögliche weitere Konstellation ist, dass eine Gesellschaft, z. B. die für Multimedia-Inhalte zuständige Gesellschaft, die zu der gleichen Unternehmensgruppe wie die Sendergesellschaft gehört, das HbbTV-Angebot in eigener datenschutzrechtlicher Verantwortlichkeit bereitstellt. In diesem Fall ist die (Multimedia-)Gesellschaft selbst Diensteanbieter und verantwortliche Stelle für den Datenumgang im Zusammenhang mit dem HbbTV-Angebot.

3.3 Portalbetreiber

Einige Smart-TVs bieten einen Zugang zu einem eigenen oder einem von dritter Stelle betriebenen Smart-TV-Portal an, über das z. B. vorinstallierte Apps (auch in Form von Verlinkungen) genutzt werden können oder auf App-Stores zugegriffen werden kann. In einigen Fällen ist eine Registrierung des Nutzers erforderlich, um das Portal nutzen zu können. Zudem werden zum Teil Nutzungsanalysen durchgeführt. Über die TV-Plattformen können u. U. zusätzlich weitere Akteure, wie z. B. ein App-Store-Betreiber oder App-Anbieter angesprochen werden. Die Betreiber des Portals agieren als verantwortliche Stelle und Diensteanbieter, soweit sie selbst in eigener Verantwortung personenbezogene Daten erheben und verwenden.

3.4 App-Store-Betreiber

Neben den vorinstallierten Apps wird dem Nutzer bei vielen Plattformen die Möglichkeit gegeben, selbst Apps über einen App-Store zu installieren. Wird der App-Store nicht von dem Portalbetreiber selbst betrieben, handelt es sich bei dem App-Store-Betreiber um einen weiteren Akteur, der jedenfalls im Falle einer Registrierung und Nutzung des App-Stores personenbezogene Daten zu eigenen Zwecken erhebt und verwendet. In diesem Fall ist der App-Store-Betreiber verantwortliche Stelle und Diensteanbieter.

3.5 App-Anbieter

Handelt es sich bei den (vorinstallierten oder im Nachhinein heruntergeladenen) Apps um „Fremd-Anwendungen“, also nicht solche des Portalbetreibers, ist der jeweilige App-Anbieter als eigen-ständiger Diensteanbieter und verantwortliche Stelle einzustufen.

Ebenfalls sind App-Anbieter auch diejenigen Stellen, die Smartphone- oder Tablet-Apps für eine Kommunikation mit dem Smart-TV anbieten (z. B. Fernaufnahmefunktion, Second Screen). Oft werden diese Apps von den Geräteherstellern selbst entwickelt und angeboten.

3.6 Betreiber von Personalisierungsdiensten (Empfehlungsdienste)

Häufig werden dem Nutzer Empfehlungsdienste angeboten, die auf Basis des jeweiligen Nutzerverhaltens Vorschläge für weitere Angebote oder Fernsehsendungen machen, die den Vorlieben des Nutzers entsprechen. Die Vorlieben des Nutzers werden dabei ermittelt, indem z. B. bei der Bedienung des – online betriebenen – elektronischen Programmführers (EPG) erfasst wird, welche Sendungen ein Nutzer aus diesem heraus anklickt, aufnimmt, vormerkt etc. oder aber indem analysiert wird, welche Inhalte von einem externen Speichermedium aus auf das Gerät eingespielt oder wie welche Smart-TV-Dienste genutzt werden. Der Betreiber eines Empfehlungsdienstes ist als verantwortliche Stelle und Diensteanbieter einzustufen.

3.7 Auftragsdatenverarbeiter

In vielen Fällen werden Dienstleister eingeschaltet, um bestimmte Datenverarbeitungen im Auftrag durchzuführen (= Auftragsdatenverarbeitung, vgl. Definition in Kapitel 2.1). Neben der Wartung und Pflege von Software kommen z. B. Dienstleister, die Nutzungsanalysen durchführen, in Betracht. Das weisungsgebundene Handeln wird dem Auftraggeber (= verantwortliche Stelle) zugerechnet.

4. Anwendbares Datenschutzrecht

4.1 Deutsches Datenschutzrecht

Das Bundesdatenschutzgesetz gilt als allgemeine Rechtsgrundlage bei Umgang mit personenbezogenen Daten durch Stellen mit Sitz in der Bundesrepublik Deutschland (BRD) oder eine Tätigkeit im Rahmen einer Niederlassung in der BRD ausgeführt wird, soweit nicht andere Vorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind. Im Zusammenhang mit der Smart-TV-Nutzung enthält das Telemediengesetz in den §§ 11 ff. datenschutzrechtliche Regelungen, die als bereichsspezifische Rechtsvorschriften den allgemeinen Datenschutzregelungen im BDSG vorgehen.

Gem. § 1 Abs. 1 Satz 1 TMG gilt das TMG „für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes (TKG), die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3

Nr. 25 des TKG oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind (Telemedien).“ Welche Dienste als Telemedien eingestuft werden können, wurde bereits unter Kapitel 2.7 dargestellt.

Da im Zusammenhang mit Smart-TV-Angeboten regelmäßig Inhalte elektronisch übertragen werden (Webseiten, Apps etc.) und somit Telemediendienste vorliegen, sind vorwiegend das TMG und ergänzend das BDSG als allgemeines Gesetz zu beachten.[8]

4.2 Internationaler Datenverkehr

Soweit ein Anbieter, der nicht in einem Mitgliedstaat der Europäischen Union (EU) oder einem Vertragsstaat des Europäischen Wirtschaftsraumes (EWR) belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, findet das Bundesdatenschutzgesetz Anwendung (§ 1 Abs. 5 Satz 2 BDSG). Soweit ein in einem anderen Mitgliedstaat der EU oder im EWR-Bereich gelegener Anbieter personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt und dies nicht durch eine Niederlassung dieses Anbieters im Inland erfolgt, findet das Bundesdatenschutzgesetz keine Anwendung (§ 1 Abs. 5 Satz 1 BDSG), sondern das Recht des jeweiligen Mitgliedstaats der Europäischen Union oder des Vertragsstaats im EWR.[9]

Da das Telemediengesetz insoweit keine eigenen innergemeinschaftlichen Kollisionsvermeidungsnormen enthält, ist für die Anwendbarkeit dieser bereichsspezifischen datenschutzrechtlichen Regelungen auf die kollisionsrechtlichen Regelungen des Bundesdatenschutzgesetzes abzustellen. Soweit also grundsätzlich das BDSG zur Anwendung käme, im vorgelegten Fall aber aus Gründen der Subsidiarität nicht einschlägig ist, treten die bereichsspezifischen Regelungen des Telemediengesetzes an die Stelle der Vorschriften des Bundesdatenschutzgesetzes.

5. Datenschutzrechtliche Rahmenbedingungen für Smart-TV

Sowohl nach den Vorschriften des Bundesdatenschutzgesetzes als auch des Telemediengesetzes gilt der Grundsatz, dass personenbezogene Daten nur erhoben und verwendet[10] werden dürfen, soweit dies durch das Bundesdatenschutzgesetz, das Telemediengesetz oder eine andere einschlägige Rechtsvorschrift erlaubt ist oder der Nutzer eingewilligt hat (sog. Verbot mit Erlaubnisvorbehalt, vgl. § 4 Abs. 1 BDSG und § 12 Abs. 1 TMG).

[8] Vgl. auch die gemeinsame Position des Düsseldorfer Kreises und der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten „Smartes Fernsehen nur mit smarten Datenschutz“ vom Mai 2014, Ziffer 2.

[9] Weitere Ausführungen zum anwendbaren Recht finden sich in der Stellungnahme der Art. 29 Gruppe 8/2010 zum anwendbaren Recht, abrufbar unter ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_de.pdf.

[10] Der Begriff „Verwenden“ personenbezogener Daten findet sich in den §§ 11 ff. TMG. Er umfasst das Verarbeiten und Nutzen personenbezogener Daten i. S. d. § 3 Abs. 4 und Abs. 5 BDSG. Entsprechend wird dieser Begriff vorliegend einheitlich (sowohl im Anwendungsbereich des BDSG als auch des TMG) verwendet.

Wenn nicht eine dieser Voraussetzungen vorliegt, ist der Umgang mit personenbezogenen Daten durch Anbieter von Smart-TV-Diensten datenschutzrechtlich unzulässig, kann durch die zuständige Datenschutzaufsichtsbehörde unterbunden und gegebenenfalls mit einem Bußgeld geahndet werden.

5.1 Erlaubnistatbestände

Bei der Nutzung von Smart-TV-Diensten stehen der Umgang mit Bestandsdaten (vgl. § 14 TMG) und Nutzungsdaten (vgl. § 15 TMG) im Fokus. Hiervon zu unterscheiden sind Inhaltsdaten. Für diese Daten gelten in der Regel die allgemeinen Datenschutzgesetze (im nicht-öffentlichen Bereich das BDSG).

5.1.1 Erlaubnistatbestände aus dem TMG

Die datenschutzrechtlichen Regelungen des Telemediengesetzes finden sich in den §§ 11 ff. In diesen Regelungen wird die Erhebung und Verwendung der Bestands- und Nutzungsdaten sowohl durch öffentliche als auch durch nicht-öffentliche Stellen (§ 1 Abs. 1 Satz 2 TMG) behandelt. Der Anwendungsbereich des TMG ist eröffnet, soweit es sich bei dem angebotenen Dienst um einen Telemediendienst gem. § 1 Abs. 1 TMG handelt.

5.1.1.1 Bestandsdaten

Gem. § 14 Abs. 1 TMG darf ein Diensteanbieter personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind (Bestandsdaten). Welche personenbezogenen Daten konkret für diese Zwecke erforderlich sind, wird durch den jeweiligen Nutzungsvertrag bestimmt, der zwischen Anbieter und Nutzer abgeschlossen wird. Zu den Bestandsdaten können insbesondere Name, Anschrift, Rufnummer, Registrierungs- und Zahlungsdaten zählen.

Beispiel:
Kann sich ein Nutzer in einem Online-Portal registrieren, um eine Bewertung zu einer TV-Sendung o. Ä. abzugeben, handelt es sich bei den Registrierungsdaten um Bestandsdaten.

5.1.1.2 Nutzungsdaten

Nutzungsdaten sind gem. § 15 Abs. 1 TMG die personenbezogenen Daten, die erforderlich sind, um die Inanspruchnahme von Telemedien zu ermöglichen und mit dem Nutzer abzurechnen.

Das TMG definiert nicht abschließend folgende Daten als Nutzungsdaten:

- Merkmale zur Identifikation des Nutzers
- Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung
- Angaben über die vom Nutzer in Anspruch genommenen Telemedien

Zu den Nutzungsdaten zählen somit alle personenbezogenen Daten, die notwendigerweise zur Nutzung des Dienstes durch den Diensteanbieter erhoben und verwendet werden müssen, wie z. B. nach Auffassung der Datenschutzbehörden die IP-Adresse oder – soweit im Einzelfall erforderlich – eindeutige Kennnummern. Die Erforderlichkeit misst sich hierbei an Sinn und Zweck des jeweiligen Dienstes. Für die Erbringung des Dienstes ist dann die Erhebung und Verwendung dieser Nutzungsdaten zulässig.

Beispiel:
Ein Smart-TV lädt aus dem Internet über das HTTP-Protokoll Daten zur Erbringung eines Dienstes, zum Beispiel zur Erbringung des HbbTV-Angebotes oder zur Nutzung einer App. In diesem Zusammenhang werden z. B. die IP-Adresse, ein Zeitstempel und weitere Nutzungsdaten, die für die Erbringung des Dienstes technisch notwendig sind, zulässigerweise an den Anbieter übertragen.

§ 15 Abs. 3 TMG gestattet dem Diensteanbieter die Erstellung von Nutzungsprofilen auf der Basis von Nutzungsdaten für Zwecke der Werbung, der Marktforschung und zur bedarfsgerechten Gestaltung von Telemedien bei Verwendung von Pseudonymen, soweit der Nutzer nicht widerspricht.

Der Nutzer muss vom Diensteanbieter auf die Erstellung eines solchen Nutzungsprofils und die Möglichkeit, der Verwendung seiner Nutzungsdaten zu diesem Zweck widersprechen zu können, hingewiesen werden. Dies muss zumindest in der Datenschutzerklärung (vgl. Kapitel 5.2.1) geschehen. Die Widerspruchsmöglichkeit muss effektiv und angemessen sein. Es sollte daher eine direkte Opt-Out-Möglichkeit (Link, Möglichkeit des Auskreuzens) für den Nutzer vorgehalten werden, die mit möglichst einem Klick aktiviert werden kann und dazu führt, dass der Datenfluss unterbrochen wird. Die Möglichkeit, per E-Mail oder postalisch einer Nutzungsprofilerstellung gem. § 15 Abs. 3 TMG zu widersprechen, genügt nicht, da bei einem Widerspruch per E-Mail oder per Post eine Zuordnung aufgrund des Medienbruches im Allgemeinen nicht erfolgen kann. Der Widerspruch gegen die automatisierte Nutzungsprofilbildung unter Pseudonym kann im Regelfall auf technischer Ebene effektiv umgesetzt werden (z. B. Opt-Out-Cookie). Widerspricht der Nutzer der Profilbildung unter Pseudonym, so sind etwa vorhandene Profildaten zu löschen oder wirksam gem. § 3 Abs. 6 BDSG zu anonymisieren.

Die Regelungen des § 15 Abs. 3 TMG berechtigen nur den Diensteanbieter selbst oder seine Auftragnehmer zur Erstellung pseudonymer Nutzerprofile zu Werbezwecken. Eine Verwendung von Nutzungsdaten durch Dritte kann nicht auf diese Regelungen gestützt werden. Zum Zwecke der Marktforschung anderer Diensteanbieter dürfen jedoch anonymisierte Nutzungsdaten übermittelt werden (§ 15 Abs. 5 Satz 3 TMG).

Eindeutige Gerätekennungen oder auch die IP-Adresse stellen kein Pseudonym dar[11]. Diese Daten dürfen nicht in das Nutzungsprofil einfließen, da die Zusammenführung pseudonymer Nutzungs-profile mit Daten über den Träger des Pseudonyms unzulässig ist (Verstoß gegen § 15 Abs. 3 Satz 3 TMG, § 13 Abs. 4 Nr. 6 TMG).

Im Zusammenhang mit der Nutzung von Smart-TV-Diensten wird die soeben dargestellte Erlaubnis zur Erstellung von Nutzungsprofilen auf der Basis von Nutzungsdaten für Zwecke der Werbung, der Marktforschung und zur bedarfsgerechten Gestaltung von Telemedien bei Verwendung von Pseudonymen insbesondere in den folgenden Konstellationen genutzt:

- **Reichweitenmessung**

  Eine Nutzungsprofilerstellung unter Pseudonym gem. § 15 Abs. 3 TMG findet insbesondere zur Reichweitenmessung statt. Mittels einer Reichweitenmessung kann ein Diensteanbieter feststellen, in welchem Umfang und auf welche Weise sein Angebot genutzt wird. So kann er z. B. feststellen, wie viele Nutzer einen bestimmten Sender ansehen, wie viele davon den Red Button drücken und welche Angebote sie wie oft innerhalb der HbbTV-Plattform ansehen und nutzen.

  Auf die Voraussetzungen für die „Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten“ hat der Düsseldorfer Kreis mit Beschluss vom 26./27. November 2009 hingewiesen.[12] Diese folgenden Voraussetzungen sind auch bei einem Einsatz im Zusammenhang mit der Nutzung von Smart-TV-Diensten einzuhalten:

  - Anonymisierung der IP-Adresse (z. B. durch Kürzen oder Überschreiben der IP-Adresse),
  - Vorhalten einer Widerspruchsmöglichkeit und wirksame Umsetzung von Widersprüchen,
  - keine Zusammenführung des Pseudonyms mit Daten über Träger des Pseudonyms,

[11] Vgl. auch die gemeinsame Position des Düsseldorfer Kreises und der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten „Smartes Fernsehen nur mit smarten Datenschutz“ vom Mai 2014, Ziffer 2.

[12] Beschluss „Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten" vom 26./27. November 2009, abrufbar unter www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/Nov09Reichweitenmessung.html.

- Unterrichtung über Erstellung pseudonymer Nutzungsprofile und über die Widerspruchsmöglichkeit und
- soweit ein Dienstleister eingesetzt wird, Abschluss eines Auftragsdatenverarbeitungsvertrages gem. § 11 BDSG.

- **Werbefinanzierte Dienste**

Viele Dienste können „kostenfrei“ genutzt werden. In Wahrheit werden diese Angebote vielfach durch eine Verarbeitung von Nutzungsdaten zu Werbezwecken finanziert. Dazu kann beispielsweise auch ausgewertet werden, wie Nutzer ein HbbTV-Angebot bedienen, um ihnen möglichst passgenaue Werbung zu präsentieren. Datenschutzrechtlich ist das nur zulässig, wenn die oben genannten Voraussetzungen des § 15 Abs. 3 TMG eingehalten werden oder ein anderer Erlaubnistatbestand für den Umgang mit personenbezogenen Daten vorliegt.

Soweit Nutzungsdaten durch Diensteanbieter für die Abrechnung kostenpflichtiger Angebote verwendet werden, handelt es sich um Abrechnungsdaten, deren Verwendung in den §§ 15 Abs. 2, 4 ff. TMG geregelt wird. Der Diensteanbieter darf diese Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus verwenden, wenn sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind.

5.1.2 Erlaubnistatbestände aus dem BDSG

Soweit es nicht um eine Datenerhebung und -verwendung auf der Anwendungsebene, sondern um eine Datenerhebung und -verwendung auf der Inhaltsebene geht, findet grundsätzlich das Bundesdatenschutzgesetz Anwendung. Ein Datenumgang auf der Inhaltsebene ist dann anzunehmen, wenn online Daten zwischen dem Nutzer und dem Anbieter ausgetauscht werden, um ein Vertrags- oder Leistungsverhältnis zu begründen, das selbst keinen Telemediendienst darstellt („Offline-Vertrag“). Zwar werden die Daten unter Anwendung des Smart-TV-Dienstes eingegeben und übermittelt, ermöglicht wird jedoch eine Verwendung außerhalb des Anwendungsbereichs des TMG. Bei der Erhebung und Verwendung personenbezogener Daten durch nicht-öffentliche Stellen sind die §§ 27 ff. BDSG anzuwenden. Darüber hinaus können im konkreten Einzelfall spezielle Datenschutzregelungen vorrangig anzuwenden sein.

Beispiel:
Im Rahmen eines HbbTV-Angebotes kann der zu einem Menü in einer gerade ausgestrahlten Kochsendung passende Wein bestellt werden. Die dann in das Bestellformular eingegebenen Daten sind nicht erforderlich für die Begründung, inhaltliche Ausgestaltung oder Änderung des „Telemedien-Vertragsverhältnisses“, aber für die „Offline-Erfüllung“ des dann geschlossenen Kaufvertrages.

5.1.3 Einwilligung

Existiert kein gesetzlicher Erlaubnistatbestand, sind Erhebung und Verwendung personenbezogener Daten nur mit einer wirksamen Einwilligung des Nutzers möglich.

Soweit eine Einwilligung in Betracht kommt, sind die Voraussetzungen für eine wirksame Einwilligung – je nachdem, ob das TMG Anwendung findet oder nicht – in § 4a BDSG und § 13 Abs. 2, 3 TMG geregelt.

Während § 4a BDSG neben der Freiwilligkeit und Informiertheit der Einwilligung grundsätzlich die Schriftform fordert, erlaubt und regelt das Telemediengesetz für Telemedien die Einholung einer elektronischen Einwilligung. Eine Einwilligung kann gegenüber dem Anbieter elektronisch erklärt werden, wenn die Vorgaben des § 13 Abs. 2 und Abs. 3 TMG eingehalten werden. Hiernach ist erforderlich, dass

- der Nutzer seine Einwilligung bewusst und eindeutig erklärt hat (z. B. durch Ankreuzen einer vorformulierten Einwilligung),
- die Einwilligung protokolliert wird,
- der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und
- der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. Hierauf ist der Nutzer bereits vor Erteilung der Einwilligung hinzuweisen.

Die freiwillige Einwilligung muss vor der Datenverarbeitung durch den Nutzer abgegeben worden sein. In diesem Zusammenhang ist insbesondere auch zu beachten, dass gemäß § 12 Abs. 3 TMG i. V. m. § 28 Abs. 3b BDSG das Kopplungsverbot gilt, d. h. die verantwortliche Stelle darf den Abschluss eines Vertrages nicht von einer Einwilligung des Nutzers in die werbliche Nutzung seiner Daten abhängig machen, wenn dem Nutzer ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Hiervon ist auszugehen, wenn ein vergleichbarer gleichwertiger Dienst von einem anderen Anbieter nicht bezogen werden kann.[13]

Wenn ein Datenumgang in Klauseln geregelt wird, die gem. §§ 305 ff. Bürgerliches Gesetzbuch (BGB) nicht wirksam sind, fehlt die Rechtsgrundlage für den dort geregelten Datenumgang.

[13] Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, 3. Auflage 2015, § 28 BDSG, Rn. 17 ff.

5.2 Informationspflichten

5.2.1 Datenschutzerklärung

Ein Telemedienanbieter hat gemäß § 13 Abs. 1 Satz 1 TMG den Nutzer „zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten [außerhalb der EU bzw. des EWR] (...) in allgemein verständlicher Form zu unterrichten“. Nach Satz 3 des § 13 Abs. 1 TMG muss der Inhalt der Unterrichtung für den Nutzer auch jederzeit abrufbar sein. Zudem ist der Nutzer zu Beginn eines automatisierten Verfahrens, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, hierüber zu informieren (vgl. § 13 Abs. 1 Satz 2 TMG). Letztere Unterrichtungspflicht zielt insbesondere auf den Einsatz von Cookies ab, betrifft jedoch nicht nur diese.

5.2.1.1 Hinweise zu Nutzungsbeginn und jederzeit

Jeder Anbieter von Telemedien ist nach § 13 Abs.1 TMG dafür verantwortlich, dass sich der Nutzer zu Beginn des Nutzungsvorgangs und jederzeit über den Umgang mit seinen personenbezogenen Daten und die Erhebung und Verwendung in einem automatisierten Verfahren, welches die Verwendung personenbezogener Daten vorbereitet, informieren kann. Aus dieser Anforderung erwächst die Verpflichtung, die Datenschutzhinweise derart zu verankern, dass der Nutzer zwangsläufig und so frühzeitig wie möglich mit diesen in Berührung gelangt. Deshalb muss die Information in einer Erklärung, die als „Datenschutzerklärung“, „Hinweise zum Datenschutz“ o. Ä. bezeichnet und ohne Umwege erreichbar ist, erfolgen. Eine Information, die im Impressum oder den Allgemeinen Geschäftsbedingungen (AGB) erfolgt, genügt nicht den Anforderungen an die Transparenz. Die Datenschutzhinweise müssen sich auf den konkret und aktuell angebotenen Dienst beziehen. Nicht ausreichend ist es, wenn gesetzliche Normen wiedergegeben oder allgemeine Floskeln zur Wichtigkeit des Datenschutzrechts angezeigt werden. Auch sind zukünftig geplante oder ggf. in anderen Staaten stattfindende Datenumgänge nicht abstrakt in den Informationen darzustellen. Selbst wenn die Ausführungen entsprechend gekennzeichnet sind, wirkt dies der erforderlichen allgemeinen inhaltlichen Verständlichkeit entgegen. Die Information muss den gegenwärtigen Zustand abbilden und für den Nutzer relevant sein (d. h. keine allgemeine Darstellung der Praxis in anderen Rechtsordnungen auf der obersten Ebene). Soweit ein Dienst Änderungen erfährt, die dazu führen, dass weitere, andere oder weniger personenbezogene Daten erhoben und verwendet werden, ist die Datenschutzerklärung zu aktualisieren, so dass der Nutzer weiterhin über den konkreten und aktuellen Datenumgang bei der Nutzung des Dienstes informiert wird.

Zu beachten ist insbesondere auch, dass nicht sonstige Textbausteine, die häufig für herkömmliche Webseiten erstellt werden, genutzt werden, da eine Abweichung zwischen Smart-TV-Diensten und herkömmlichen Webseiten bei den Einstellungsmöglichkeiten für den Nutzer besteht. Während bei gängigen Internetbrowsern gezielt Einstellungen zur Privatsphäre und zum Datenschutz vorgenommen werden können, wie z. B. das Löschen von Tracking-Cookies, ist es dem Nutzer bei Smart-TV-Geräten über Betriebssystemmittel regelmäßig noch nicht möglich, derartige Maßnahmen zu ergreifen. Werden diese allerdings in der Datenschutzerklärung unter Bezugnahme auf die Webseite dargestellt, so ist dies irreführend, weil sie auf die Nutzung des konkreten Angebots keine Anwendung finden.

5.2.1.2 Kontaktmöglichkeiten

Um dem Nutzer die unkomplizierte Wahrnehmung seiner Nutzerrechte zu ermöglichen, sollten Anbieter eine einfache Kontaktmöglichkeit (z. B. postalische Adresse, E-Mail Adresse) zu ihnen bzw. einer bei ihnen für datenschutzrechtliche Fragen zuständigen Stelle in der Datenschutzerklärung angeben.[14] Dies ist insbesondere dann hilfreich, wenn mehrere Anbieter an der Erbringung von Diensten beteiligt sind und dem Nutzer nicht ohne weiteres ersichtlich ist, welche Stelle für welche Datenverarbeitungsvorgänge verantwortlich ist. Dies kann sich regelmäßig gerade erst aus der transparenten Darstellung in der Datenschutzerklärung ergeben.

5.2.2 Unterrichtungspflicht der verantwortlichen Stelle

Gem. § 4 Abs. 3 Satz 1 BDSG ist die betroffene Person, bei der personenbezogene Daten erhoben werden, von der verantwortlichen Stelle grundsätzlich über die Identität der verantwortlichen Stelle (Nr. 1), die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung (Nr. 2) und die Kategorien von Empfängern zu informieren. Werden personenbezogene Daten ohne Kenntnis des Nutzers zu eigenen Zwecken gespeichert, ist der Nutzer grundsätzlich über die Speicherung, die Art der Daten, die Zweckbestimmung des Datenumgangs und die Identität der verantwortlichen Stelle zu benachrichtigen (vgl. § 33 BDSG). Soweit eine verantwortliche Stelle zugleich Diensteanbieter ist, kann die Information im Rahmen der Datenschutzerklärung gegeben werden, ansonsten bedarf es einer sonstigen Information des Nutzers. Sinn und Zweck der Information ist, dass sich ein Nutzer frei entscheiden können muss, ob er mit dem Datenumgang einverstanden ist. Hieraus folgt, dass die Information bereits vor der Erhebung, Verarbeitung und Nutzung erfolgen muss.

[14] Zwar kann aus dem Impressum gem. §§ 5 f. TMG entnommen werden, wer Diensteanbieter ist, empfehlenswert ist es jedoch, wenn darüber hinaus ein Kontakt für datenschutzrechtliche Fragestellungen in der Datenschutzerklärung angegeben wird.

5.3 Nutzerrechte

Jeder Nutzer, dessen personenbezogene Daten erhoben und verwendet werden, hat gem. § 34 BDSG (ggf. i. V. m. § 13 Abs. 7 TMG) das Recht, Auskunft über die durch die verantwortliche Stelle zu seiner Person gespeicherten Daten zu verlangen. Gemäß § 35 BDSG kann er die Berichtigung, Löschung und Sperrung von Daten verlangen. Diese Ansprüche bestehen auch bei Nutzung eines Smart-TV-Angebotes. Smart-TV-Dienste-anbieter sollten deshalb wie sonstige verantwortliche Stellen bei der Verarbeitung von Nutzerdaten (Bestands-, Nutzungs- und Inhaltsdaten) auf entsprechende Anfragen von Nutzern vorbereitet sein, um bei Bedarf zeitnah reagieren zu können. Wenn ein Anbieter seiner Auskunftspflicht nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig nachkommt, kann dies mit einem Bußgeld geahndet werden.

5.4 Datenschutzrechtliche Grundsätze

Selbstverständlich gelten im Zusammenhang mit dem Angebot von Smart-TV-Diensten die sich aus den Vorschriften des BDSG und auch des TMG ergebenden datenschutzrechtlichen Grundsätze. Hierzu zählen u. a.:

5.4.1 Grundsatz der Direkterhebung

Gem. § 4 Abs. 2 Satz 1 BDSG sind personenbezogene Daten grundsätzlich beim Betroffenen zu erheben. Ausnahmen bestehen nach § 4 Abs. 2 Satz 2 BDSG nur dann, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt, der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder wenn die Erhebung beim Nutzer einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte für die Beeinträchtigung eines überwiegend schutzwürdigen Interesses des Nutzers besteht. Der Nutzer soll wissen, wer welche Daten zu welchen Zwecken über ihn erhebt, verarbeitet und nutzt. Die personenbezogenen Daten müssen somit nicht nur bei ihm direkt, sondern auch mit seiner Kenntnis oder unter seiner Mitwirkung erlangt werden. Findet eine Datenerhebung heimlich statt, so wird der Grundsatz der Direkterhebung verletzt, soweit nicht eine der im Gesetz genannten Ausnahmen greift.

Im Rahmen eines Online-Angebotes ist es daher notwendig, den Nutzer konkret über die Erhebung und Verwendung seiner personenbezogenen Daten zu informieren (vgl. 5.2) und die gegebenenfalls erforderliche Einwilligung einzuholen.

5.4.2 Grundsatz der Datenvermeidung und der Datensparsamkeit

Nach den in § 3a BDSG normierten Grundsätzen der Datenvermeidung und Datensparsamkeit sollten so wenig personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden.

Diese Grundsätze sind bereits frühzeitig, möglichst bei der Entwicklung eines Verfahrens oder Diensteangebots zu beachten. Die Angebote sind daher so zu entwickeln und zu betreiben, dass von Beginn an so wenig personenbezogene Daten wie möglich erhoben und verwendet werden („Privacy by design“) und standardmäßig die datenschutzfreundlichste Voreinstellung vorgenommen wird („Privacy by default“).

Der Aufruf der Web-Dienste und die damit einhergehende wechselseitige Kommunikation mit den Anbietern von Smart-TV-Diensten dürfen deshalb erst stattfinden, wenn diese durch die Nutzer selbst initiiert werden, er also einen Dienst in Anspruch nehmen möchte und deshalb die Daten überhaupt benötigt werden. Ohne eine Inanspruchnahme durch den Nutzer bedarf es keines Datenumganges. Die Datenerhebung und -verwendung kann somit vermieden werden (konkret im Zusammenhang mit HbbTV-Angeboten, vgl. Kapitel 7.2).

Auch wenn die verantwortliche Stelle auf die Implementierung datenschutzfreundlicher Voreinstellungen hinzuwirken hat, ist es wünschenswert, dass Entwickler von Verfahren und Produkten diese bereits so herstellen, dass Datenflüsse nicht ohne weiteres ausgelöst werden.

Das Gebot der Datensparsamkeit und der Datenvermeidung verlangt z. B., dass Gerätehersteller Funktionalitäten wie Mikrofon (für Spracherkennung) und Kamera (für Gestensteuerung) so einbinden müssen, dass diese erst durch den Nutzer aktiviert werden und darüber hinaus, dass auf dem Gerät gespeicherte Daten der Kontrolle der Nutzer unterliegen, also z. B. Cookies verwaltet werden können[15].

5.4.3 Grundsatz der Zweckbindung

Jeder Umgang mit personenbezogenen Daten muss einen bestimmten, legitimen Zweck verfolgen. Eine Datensammlung ohne einen konkret festgelegten Zweck ist genauso wenig zulässig wie die Änderung eines früher festgelegten Zwecks und Verwendung der bis dahin gesammelten Daten für einen neuen Zweck, ohne dass auch für diesen Datenumgang eine Erlaubnis existiert. Soweit der verfolgte Zweck wegfällt, sind die personenbezogenen Daten grundsätzlich zu löschen. Im Falle gesetzlicher Verpflichtungen zur

[15] Vgl. auch die gemeinsame Position des Düsseldorfer Kreises und der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten „Smartes Fernsehen nur mit smarten Datenschutz“ vom Mai 2014, Ziffer 3.

weiteren Aufbewahrung (etwa nach Vorgaben der Abgabenordnung oder des Handelsgesetzbuches) sind die Daten zu sperren und dazu von den aktuellen Produktivdaten zu trennen.

5.4.4 Grundsatz der Erforderlichkeit

Der Grundsatz der Erforderlichkeit bedeutet, dass nur die für einen konkreten Zweck erforderlichen personenbezogenen Daten erhoben und verwendet werden dürfen. Sofern Möglichkeiten bestehen, personenbezogene Daten durch Verarbeitungsschritte so zu verändern, dass der Informationsgehalt auf das erforderliche Mindestmaß begrenzt wird, sind diese umzusetzen.

5.4.5 Grundsatz der anonymen und pseudonymen Nutzung

Soweit es dem Diensteanbieter technisch möglich und zumutbar ist, hat er die Nutzung von Telemedien und ihre Bezahlung gem. § 13 Abs. 6 TMG anonym oder unter Pseudonym zu ermöglichen. Über diese Möglichkeit ist der Nutzer zu informieren. Dem Nutzenden muss z. B. bei Apps zur Nutzung sozialer Netzwerke jedenfalls die Möglichkeit gegeben werden, unter einem Pseudonym zu agieren.

6. Technische und organisatorische Maßnahmen

Zusätzlich zu den in den vorigen Kapiteln genannten datenschutzrechtlichen Anforderungen haben die Anbieter von Smart-TV-Diensten die technischen und organisatorischen Anforderungen, die sich aus § 9 BDSG und der Anlage zu § 9 BDSG sowie aus § 13 Abs. 4 TMG ergeben, einzuhalten. Insbesondere betrifft dies die folgenden Anforderungen:

6.1 Regelmäßige Sicherheitsupdates

Die verantwortlichen Stellen für die Smart-TV-Geräte müssen dafür Sorge tragen, dass regelmäßige Sicherheitsupdates angeboten werden. Stehen für ein (älteres) Gerät keine Patches mehr zur Verfügung, sollte dies dem Nutzer bei Einschalten des Gerätes bzw. vor Nutzung eines Dienstes mitgeteilt werden. Die Updates müssen auch Komponenten von Drittanbietern, die durch die verantwortliche Stelle genutzt werden, umfassen (z. B. Browser-Engine, Bibliothek für Videowiedergabe,…).

6.2 IT-Sicherheitsarchitektur

Bei Smart-TVs besteht, wie bei anderen mit dem Internet verbundenen Geräten (PCs, Smartphones,…) auch, die Gefahr, dass einzelne Anwendungen (App, Webseite, HbbTV-Seite) oder Medien (MP3, Filme) durch Unbefugte derart manipuliert werden, dass diese

einen Zugriff auf andere Bereiche des Gerätes (z. B. Kamera, Mikrophon, Cookie-Datenbank, Passwörter, DNS-Einstellungen,…) erlangen. Aus diesem Grund ist es notwendig, dass geeignete IT-Sicherheitsarchitekturen Anwendung finden, beispielsweise unterschiedliche Benutzerrechte auf Systemebene für einzelne Anwendungen oder Sandboxing-Verfahren.

6.3 Verschlüsselung nach dem Stand der Technik

Bei Nutzung des Smart-TV werden sämtliche Inhalte, wie z. B. Geräteupdates, Grafiken, Nachrichten, HbbTV-Inhalte oder Empfehlungsdienste meist über das HTTP-Protokoll übertragen. Werden dabei auch personenbezogene Daten übertragen, müssen diese nach dem Stand der Technik verschlüsselt werden (Anlage zu § 9 BDSG). Als Orientierung können die Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) herangezogen werden. Zum Zeitpunkt der Erstellung der Orientierungshilfe sind aber mindestens folgende Anforderungen umzusetzen:

- HTTPS
- Perfect Forward Secrecy
- kein SSL2/SSL3
- mindestens 2048-Bit beim X.509 Zertifikat
- keine RC4-Verschlüsselung
- kein SHA1-Hashverfahren

Darüber hinaus müssen vorhandene Sicherheitsprobleme, die sich aus der Implementierung des TLS-Protokolls ergeben können, zeitnah durch Updates behoben werden (z. B. Heartbleed-Lücke).

Die Smart-TV-Hersteller müssen die HTTPS-Verschlüsselung derart implementieren, dass keine Man-In-The-Middle Attacken durch ungenügende Prüfung der Serverzertifikate möglich sind.

7. Konkrete Anforderungen an Anbieter von Smart-TV-Diensten

Adressat datenschutzrechtlicher Vorgaben für den Umgang mit personenbezogenen Daten und somit verantwortlich für die Umsetzung der datenschutzrechtlichen Anforderungen ist jeweils der Diensteanbieter bzw. die verantwortliche Stelle. Um die datenschutzrechtlichen Verantwortlichkeiten auseinanderhalten zu können, ist strikt zwischen den verschiedenen Anbietern von Smart-TV-Diensten und deren jeweiliger Verantwortlichkeit zu unterscheiden. Nur auf diese Weise können die Rechte und Pflichten der einzelnen Anbieter bestimmt werden.

Im Folgenden werden die einzelnen Akteure nochmals (vgl. bereits Kapitel 3) benannt und die gesetzlichen Anforderungen („muss“) und Empfehlungen („sollte“) der Aufsichtsbehörden bezogen auf den jeweiligen Akteur dargestellt. Da dies jedoch nur schematisch geschehen kann, wird darauf hingewiesen, dass die Darstellung der rechtlichen Pflichten und Empfehlungen nicht abschließend ist. Soweit ein Akteur mehrere Funktionen wahrnimmt (z. B. Gerätehersteller ist auch Portalbetreiber) muss er die Vorgaben und Empfehlungen der entsprechenden Abschnitte kumuliert beachten.

7.1 Gerätehersteller

Wie bereits unter Kapitel 3.1 dargestellt, agiert ein Gerätehersteller, der lediglich das Gerät und ggf. Software-Updates zur Verfügung stellt, dann als verantwortliche Stelle, wenn er im Rahmen der Software-Updates personenbezogene Daten, wie z. B. die IP-Adresse erhebt und verwendet. Bietet der Gerätehersteller Telemediendienste an, so agiert er als Telemedienanbieter, womit er den datenschutzrechtlichen Vorgaben des TMG unterliegt.

7.1.1 Information des Nutzers

Der Gerätehersteller muss den Nutzer über den Umgang mit dessen personenbezogenen Daten informieren. Die Informationspflicht der verantwortlichen Stelle erwächst i. d. R. aus § 4 Abs.3 BDSG (vgl. Kapitel 5.2.2.1). Im Rahmen dieser Information sollte der Nutzer auch darüber informiert werden, wann er das Angebot des Geräteherstellers verlässt und damit Nutzerdaten durch eine andere verantwortliche Stelle erhoben werden. Dabei wird jedoch nicht gefordert, dass vor jeder Weiterleitung ein Pop-Up erscheint; vielmehr genügt eine einmalige, aktive Information des Nutzers (z. B. bei der Einrichtung des Gerätes), die jederzeit aktiv durch den Nutzer wieder aufgerufen werden kann. Dies kann z. B. der Fall sein, wenn der Portalbetreiber nicht mit dem Gerätehersteller identisch ist. Zwar muss der Portalbetreiber den Nutzer über seine Identität und den Datenumgang informieren (vgl. Kapitel 7.3.2). Durch den Hinweis seitens des Geräteherstellers wird der Nutzer jedoch bereits im Vorfeld darauf hingewiesen, dass er im Begriff ist, das Angebot des Geräteherstellers zu verlassen. Der Nutzer kann sich bereits, bevor personenbezogene Daten durch den Portalbetreiber erhoben werden, für oder gegen eine Nutzung durch den Portalbetreiber entscheiden.

Soweit der Gerätehersteller selbst zugleich Anbieter von Telemedien ist, ist er verpflichtet, den Nutzer im Rahmen einer Datenschutzerklärung gem. § 13 Abs.1 TMG über Art, Umfang und Zweck des Datenumgangs zu informieren (vgl. Kapitel 5.2.1). Zudem muss dem Nutzer dann die Weitervermittlung zu einem anderen Anbieter angezeigt werden (vgl. § 13 Abs. 5 TMG).

7.1.2 Software-Update

Hinsichtlich eines möglichen Software-Updates ist der Nutzer bei der Einrichtung des Gerätes durch eine Information (welche in der Firmware enthalten ist) darauf hinzuweisen, dass regelmäßig neue Software-Updates durch den Gerätehersteller zur Verfügung gestellt werden. Der Nutzer sollte gebeten werden, auszuwählen, ob er

1. manuell die Prüfung und Installation neuer Updates durchführen möchte,
2. automatisch neue Updates ohne Interaktion installieren möchte oder
3. eine Benachrichtigung wünscht, sobald ein neues Update zur Verfügung gestellt wird.

Entscheidet sich der Nutzer für die Option 1., liegt es in seiner Sphäre, wann er eine Überprüfung anstößt, ob ein Software-Update zur Verfügung steht und damit Datenflüsse (z. B. IP-Adresse) auslöst. Bei den Optionen 2. und 3. hingegen findet in regelmäßigen Abständen ein Abruf des aktuell installierten Softwarestandes statt. Ist eine aktuellere Software verfügbar, wird diese dann automatisch oder nach Bestätigung des Nutzers installiert. In allen drei Fällen sollte der Nutzer über die Datenflüsse und die Neuerungen, die mit einem Update einhergehen werden (Option 1. und 3.) bzw. einher gingen (Option 2), wie z. B. Aktualisierung der Software oder Schließen von Sicherheitslücken, informiert werden.

Soweit personenbezogene Daten für die Abfrage des Software-Standes, die Zusendung von Informationen und das Einspielen des Software-Updates erforderlich sind, dürfen diese im gesetzlich erlaubten Umfang erhoben und verwendet werden.

7.1.3 Analyse des Nutzerverhaltens

Einige Gerätehersteller analysieren das Verhalten der Nutzer bei der Bedienung, aber auch bei der Einrichtung des Gerätes, um z. B. die Menü-Führung bei der Einrichtung des Gerätes verbessern zu können. Da bei einer solchen Analyse zumindest die IP-Adresse an den Gerätehersteller fließt, bedarf es einer Erlaubnis für die Erhebung und ggf. Verwendung der personenbezogenen Daten. Eine Erlaubnis aus dem Gesetz ist jedoch nicht ersichtlich, so dass es einer Einwilligung des Nutzers bedarf, um das Nutzerverhalten erheben und analysieren zu dürfen.

7.1.4 Umgang mit Gerätekennungen

7.1.4.1 Erheben und Nutzen von Gerätekennungen

Erhebt und verwendet der Gerätehersteller eindeutige Gerätekennungen, bedarf er hierfür entweder einer Erlaubnis aus dem Gesetz oder einer Einwilligung des Nutzers (vgl. Ziffer

5.1). Für die Einstufung einer eindeutigen Gerätekennung als personenbezogenes Datum spielt es zunächst keine Rolle, ob Gerätekennungen fest lokal auf dem Gerät hinterlegt sind (z. B. MAC-Adresse, Seriennummer) oder durch den Hersteller bei einem erstmaligem Start des Gerätes vergeben werden (z. B. im Rahmen von Cloud-Diensten) – vielmehr muss eine Person bestimmbar sein (vgl. hierzu Kapitel 2.4). Ob und welche Rechtsgrundlage im Einzelfall greift, hängt von dem konkreten Zweck ab, zu dem die Gerätekennung benötigt wird. Ist die Erhebung und Verwendung einer eindeutigen Gerätekennung nicht erforderlich, sondern werden hierdurch z. B. lediglich künftige Servicedienste durch eine erleichterte nachträgliche Zusammenführung von Gerätedaten mit einem konkreten Nutzer möglich, ist eine Erforderlichkeit zunächst[16] nicht erkennbar und es bedarf einer Einwilligung des Nutzers.

7.1.4.2 Deaktivierung von Schnittstellen

Der HbbTV-Standard definiert eine minimale Unterstützung von verschiedenen Standards, die für ein einheitliches Funktionieren von HbbTV-Inhalten sorgen sollen. Ein expliziter Zugriff auf eindeutige Gerätekennungen ist nicht Teil des Standards. Da diese von Seiten der HbbTV-Anbieter aber möglicherweise zur Realisierung von gerätebezogenen Trackingverfahren verwendet werden könnten, sollte ein Hersteller den Zugriff (evtl. auch bei Verwendung von Drittanbieterbibliotheken) auf diese Schnittstellen überprüfen und eindeutige Gerätekennungen mit einem leeren Wert (Nullstring) ersetzen. So sollte beispielsweise sichergestellt sein, dass die Implementierung einer der HbbTV-Standards, der OIPF, „Volume 5 - Declarative Application Environment“ einen Zugriff über die Netzwerkschnittstelle auf die MAC-Adresse nicht umsetzt.

7.1.5 Verwaltung von Cookies

Wie im „klassischen“ Internet werden für die Realisierung von HbbTV-Inhalten häufig Cookies eingesetzt. Diese können es technisch ermöglichen, eine eindeutige Kennung auf dem Smart-TV des HbbTV-Nutzers abzulegen. Aus diesem Grund sollten[17] bei Smart-TV-Geräten, so wie bei den meisten Browsern auf PCs auch, Standardfunktionalitäten zur Verwaltung von Cookies vorhanden sein:

1. Anzeige aller Cookies, die von den HbbTV-Anbietern (und Dritten, die in den HbbTV-Seiten eingebunden sind) gesetzt werden

[16] Selbst wenn eine Erforderlichkeit für die Wiedererkennung eines Gerätes für die inhaltliche Ausgestaltung des Vertragsverhältnisses besteht, ist dazu regelmäßig nicht zwingend die eindeutige Geräteerkennung erforderlich; vielmehr kann ein sonstiges, zufällig vergebenes Identifizierungsmerkmal verwendet werden.

[17] Vgl. auch die gemeinsame Position des Düsseldorfer Kreises und der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten „Smartes Fernsehen nur mit smarten Datenschutz“ vom Mai 2014, Ziffer 3.

2. Grundsätzliches Blockieren von Cookies, insbesondere von Dritten, sogenannten Third-Party-Cookies, da damit ein webseitenübergreifendes Tracking möglich ist.
3. Möglichkeit zum Löschen aller Cookies eines HbbTV-Angebots bei Wechsel des Senders oder bei Ausschalten des Gerätes (auch auf Standby).

Zusätzlich zu den „klassischen“ Cookies, den sogenannten HTTP-Cookies, ist es bei Verwendung von HTML5 auch möglich, dessen Speichertechniken als Cookie-Ersatz zu gebrauchen. Es soll dem Nutzer möglich sein, diese Art der Cookies genauso wie die HTTP-Cookies zu verwalten (Anzeige, Verhinderung, Löschung).

7.1.6 Red Button ohne Autostart-Funktion

Ist eine HbbTV-URL im linearen Rundfunksignal vorhanden, wird die darin referenzierte HbbTV-Seite automatisch über das Internet geladen. Diese Art der Autostartfunktion wird bei den meisten HbbTV-Inhalten eingesetzt. Einige wenige Gerätehersteller bieten jedoch ihre Geräte bereits (von vornherein bzw. nachdem ein Nutzer dies aktiv in den Einstellungen auswählt) derart an, dass vor dem Laden von HbbTV-Angeboten und der damit einhergehenden wechselseitigen Kommunikation zunächst nur eine Information erscheint, dass ein solches Angebot verfügbar ist. Erst wenn der Nutzer aktiv den Red Button klickt, wird eine Internetverbindung aufgebaut und das jeweilige Angebot geladen. Mit einem zweiten Aktivieren des Red Buttons gelangt der Nutzer dann in das jeweilige HbbTV-Angebot. Zudem stellen einige Gerätehersteller die Auswahl der HbbTV-Angebote zur Disposition, d. h. der Nutzer selbst kann senderbezogen im Menü auswählen, welche konkreten HbbTV-Angebote ihn interessieren und ggf. automatisch geladen werden sollen und bei welchen nicht einmal eine Verfügbarkeits-Information über das vorhandene Angebot erfolgen soll. Auch wenn diesbezüglich derzeit keine datenschutzrechtliche Verantwortung der Gerätehersteller besteht, den Datenfluss zu unterbinden, sind diese Voreinstellungen bzw. Einstellungsmöglichkeiten vor dem Hintergrund des Grundsatzes der Datenvermeidung und der Datensparsamkeit besonders positiv hervorzuheben. Da diese datenschutzfreundliche Funktion noch nicht Bestandteil des HbbTV-Standards ist, sollte diese bei einer zukünftigen Erweiterung mit hinzugenommen werden.

Die Gerätehersteller sollten es deshalb als Option für den Nutzer ermöglichen, dass bei Erkennen eines HbbTV-Inhaltes im linearen Signal z. B. ein standarisierter Red Button bzw. anderweitiges Zeichen eingeblendet wird, das unabhängig von der HbbTV-Seite ist und nicht über das Internet geladen wird. Erst nach Information der Nutzer über die Bedeutung dieses Zeichens und nach aktivem Drücken des Red Buttons sollte die HbbTV-Seite, die dann senderspezifisch ist, über das Internet geladen werden. Diese Funktion

entspricht einem Privacy-by-Design-Ansatz und sollte als Voreinstellung aktiv sein (Privacy-by-Default), soweit Hersteller bzw. Programmanbieter eine entsprechende Funktionalität nicht durch andere, ebenso wirksame Maßnahmen sicherstellen.

7.1.7 Technische Prüftransparenz

Eine starke Verschlüsselung ist für die Wahrung der Vertraulichkeit und Integrität der bei Smart-TV übermittelten Daten sinnvoll und für personenbezogene Daten zwingend notwendig. Zur Überprüfung der übertragenen Inhalte eines Smart-TV-Gerätes sollten aber sichere Mechanismen zur Verfügung gestellt werden, die Prüfern und technisch interessierten Nutzern einen Einblick in die eigenen Daten des eigenen Smart-TV-Gerätes innerhalb des eigenen (Labor-)Netzes an die beteiligten Server ermöglichen. Diesbezüglich wären mehrere technische Verfahren möglich:

- Es könnte, wie es bei Smartphones üblich ist, für einen Smart-TV-Nutzer möglich sein, dass eigene selbstsignierte **Zertifikate** dem Gerät bekannt gemacht werden (z. B. über USB-Stick im Servicemenü). Sollte dies von einem Gerätehersteller aus Sicherheitsgründen nicht gewünscht sein, so wäre auch eine Erzeugung des selbstsignierten Serverzertifikates des eigenen Smart-TV durch das eigene Gerät vorstellbar, dass vom Smart-TV auf einen Analyserechner heruntergeladen werden kann. Dieser Vorgang könnte in Laborumgebungen, die von Fachmedien, interessierten Nutzern, der IT-Sicherheitsforschung, den Verbraucherschützern und Datenschutzaufsichtsbehörden durchgeführten Man-In-The-Middle-Analysen im eigenen Netz in die Lage versetzen, eine technische Prüftransparenz der eigenen Smart-TV-Daten herzustellen. Erhöhte Sicherheitsrisiken erstehen durch dieses Verfahren kaum, da nur der HTTPS-Datenverkehr des eigenen Testgeräts entschlüsselt werden kann. Sollten sicherheitsrelevante Informationen (z. B. Authentifizierungstokens des Backends) Bestandteil des Datenverkehrs sein, könnten diese durch eine zusätzliche Verschlüsselung geschützt werden.
- Eine vorinstallierte Anwendung des Smart-TV-Herstellers, die als **Netzwerkmonitor**[18] fungiert, könnte einem Nutzer nach Aktivierung alle http-basierten Internetverbindungen seines Smart-TV-Gerätes mit Dritten anzeigen. Für jeden Aufruf müsste dann ein Zeitstempel, der Empfangsserver (IP-Adresse und Domainname), der http-Header sowie HTTP-Requests und HTTP-Responses anzeigt werden. Auch Inhalte von HTTPS-Verbindungen könnten so dargestellt werden, da der Netzwerkmonitor die eigenen Daten auf dem eigenen Gerät vor der Verschlüsselung darstellt.

[18] Im Jahr 2015 bietet zum Beispiel der Browser Firefox die „Netzwerkanalyse“ für eine dynamische Analyse von Web-Content an.

7.1.8 Umgang mit Kameras und Mikrofonen

Enthält ein Smart-TV-Gerät Kameras oder Mikrofone, besteht ein besonderes Risiko, dass im Falle eines unbefugten Zugriffs auf diese Gerätebestandteile der Nutzer in seiner Privat- oder sogar Intimsphäre verletzt wird. Aus diesem Grund sollen besondere Sicherheitsmechanismen vorhanden sein, die das Missbrauchsrisiko deutlich minimieren oder Missbrauch zumindest aufdecken:

- Es sollte möglich sein, die Nutzung von Kameras und Mikrofonen über eine Geräteeinstellung dauerhaft abzuschalten.
- Vor Installation bzw. Start von Anwendungen, die Zugriff auf Kameras oder Mikrofone einfordern, sollte die Zustimmung des Nutzers eingeholt werden.
- Es sollte über ein Gerätemenü möglich sein, die Liste der Anwendungen, die Zugriff auf Kameras oder Mikrofone haben, zu verwalten.
- Bei aktiver Aufnahme sollte der Nutzer über ein visuelles Symbol darüber informiert werden, z. B. durch ein gut sichtbares LED-Signal neben der Kameralinse oder dem Mikrofonausschnitt. Hinweissignale müssen derart aktiviert werden, dass sie von einer kompromittierten Anwendung nicht ausgeschaltet werden können (z. B. über „Verdrahtung“ auf Hardwareebene).
- Vertrauensfördernd für den Nutzer wäre die Bereitstellung von Möglichkeiten, kritische Bereiche wie Kameralinse oder Mikrofonausschnitt mechanisch zu deaktivieren oder abzudecken, z. B. mit einer verschiebbaren Klappe. Solche klar erkennbaren Schutzvorrichtungen können durch Software-Manipulation nicht überlistet werden und Nutzern so das ggf. unbestimmte Gefühl des Beobachtet oder Belauschtwerdens nehmen. Versehen z. B. mit dem Hersteller-Logo könnten Abdeckungen sogar als prägendes Design-Element für ein Smart-TV-Gerät ausgestaltet werden.

7.2 HbbTV-Anbieter

7.2.1 Zulässiger Datenumgang

Wird eine HbbTV-URL mit dem Rundfunksignal versandt und die entsprechende Seite unmittelbar und ohne Tätigwerden des Nutzers von dem Server des HbbTV-Anbieters unter Eröffnung eines Rückkanals für die Übertragung von Online-Inhalten, bei denen zumindest[19] – technisch bedingt – das personenbezogene Datum IP-Adresse übertragen und verwendet wird, abgerufen, so ist für diesen Datenverarbeitungsschritt eine Rechtsgrundlage nicht erkennbar.

[19] Im Rahmen einer Reichweitenmessung bzw. zum Zweck interessensbasierter Werbung könnten auch weitere Nutzungsdaten betroffen sein.

Weder willigt der Nutzer in diesen Datenumgang ein, noch ist eine Erlaubnis aus dem Gesetz einschlägig. Insbesondere kann § 15 Abs. 1 TMG nicht greifen, da allein aufgrund der Nutzung eines Smart-TV-Gerätes und dem Einschalten eines Senders, der HbbTV-Inhalte anbietet, noch nicht von der „Inanspruchnahme von Telemedien“ im Sinne des § 15 Abs. 1 TMG durch den Fernsehzuschauer und damit noch nicht von einem Anbieter-Nutzer-Verhältnis ausgegangen werden kann.[20] Ein solches ist jedoch für die Eröffnung des Anwendungsbereichs des Telemediengesetzes elementar. So spricht z. B. § 11 Abs. 2 TMG davon, dass Nutzer jede natürliche Person ist, die Telemedien nutzt, und § 14 Abs. 1 stellt auf die Begründung eines Vertragsverhältnisses ab. Daher genügt als Voraussetzung für die Anwendbarkeit des § 15 Abs. 1 TMG weder die Einrichtung eines Internet-anschlusses noch die Herstellung einer Verbindung mit dem Internet, sondern es ist ein aktives Aufrufen des Telemediendienstes erforderlich.

Der Aufruf der Web-Dienste und die damit einhergehende wechselseitige Kommunikation mit den Anbietern von Smart-TV-Diensten dürfen deshalb erst stattfinden, wenn diese durch die Nutzer selbst initiiert werden, z. B. durch die aktive Entscheidung, den Red Button bei HbbTV zu aktivieren und damit den Abruf eines Telemediendienstes bewusst zu veranlassen. Dies könnte durch eine Auswahl der HBBTV-Fernsehsender in einem Menü des Smart-TV oder durch ein Opt-In-Cookie des HBBTV-Angebots, das durch auf eine mit dem linearen Karussellverfahren ausgelieferte HBBTV-Startseite ausgewertet wird, realisiert werden. Das bloße Verbinden des Gerätes mit dem Internet ist dagegen nicht als bewusste Inanspruchnahme von Telemedien zu bewerten, da dies nicht zwingend dahingehend verstanden werden kann, dass eine Nutzung des HbbTV-Angebotes beim Empfang des Fernsehprogramms ohne weiteren Zwischenschritt gewünscht ist. Eine Erlaubnis für die Erhebung der IP-Adresse bzw. weiterer Nutzungsdaten ist dann nicht gegeben. Die standardmäßige Voreinstellung der HbbTV-Nutzung und die damit zusammenhängende wechselseitige Kommunikation bei Einschalten des Gerätes und Auswahl eines Senders widersprechen dem.

HbbTV-Anbieter als für die Datenerhebung und -verwendung (zumindest der IP-Adresse) verantwortliche Stellen müssen Sorge dafür tragen, dass eine Kommunikation mit ihrem Server erst stattfindet, wenn der Nutzer aktiv den Red Button auf seiner Fernbedienung drückt. Dies kann über das lineare Verfahren (auch Karussellverfahren genannt, siehe Kapitel 2.3) realisiert werden, bei dem die HbbTV-HTML-Startseite mittels des Rundfunksignals übertragen wird. In diesem Moment wird noch kein Rückkanal eröffnet. Erst bei der Aktivierung des Red Buttons wird die volle Startseite aus dem Internet geladen und damit eine Internetverbindung aufgebaut.

[20] Eine Rechtsgrundlage aus dem BDSG ist ebenfalls nicht ersichtlich.

Sollte der HbbTV-Standard derart angepasst werden, dass ein Gerät so eingestellt werden kann, dass die HbbTV-Startseite erst nach Drücken des Red Buttons geladen wird (siehe Kapitel 7.1.6), dann kann die HbbTV-Startseite auch über das Internet geladen werden.

Im Ergebnis müssen die HbbTV-Anbieter als verantwortliche Stellen, ggf. in Kooperation mit den Geräteherstellern es dem Nutzer ermöglichen, anonym – d. h. ohne dass personenbezogene Daten wie IP-Adressen und/oder Nutzungsdaten beim Einsatz von Verfahren zur Reichweitenmessung an den HbbTV-Anbieter fließen – Fernsehen zu können.[21]

7.2.2 Datenschutzerklärung

Der HbbTV-Anbieter muss als Telemedienanbieter gem. § 13 Abs. 1 TMG eine Datenschutzerklärung vorhalten, die zu Beginn des Nutzungsvorganges und jederzeit auffindbar ist (vgl. Kapitel 5.2.1). Dass eine Datenschutzerklärung existiert und abrufbar ist, sollte dem Nutzer bereits über die Startseite deutlich gemacht werden. D. h., die über das Rundfunksignal ausgelieferte Startseite sollte bereits signalisieren, dass der Nutzer beim Aufruf des Vollbildes (Drücken des Red Buttons) Zugang zu einer Datenschutzerklärung erhält. Diese Datenschutzerklärung muss im HbbTV-Angebot unmittelbar aufzufinden sein und auch jederzeit von jeder weiteren Seite aufgerufen werden können.

7.2.3 Nutzungsprofilbildung

Eine Nutzungsprofilbildung ist nur dann zulässig, wenn der Nutzer wirksam eingewilligt hat oder diese gem. § 15 Abs. 3 TMG zum Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung des Telemedienangebotes unter Pseudonym erfolgt und dem Nutzer eine wirksame Widerspruchsmöglichkeit angeboten wird (vgl. Kapitel 5.1.1.2). Über die Erstellung eines Nutzungsprofils und die Möglichkeit zu widersprechen, ist der Nutzer im Rahmen der Datenschutzerklärung (vgl. Kapitel 7.2.2) zu informieren.

Vor einem aktiven Aufruf des HbbTV-Angebotes ist auch die Erhebung von Nutzungsdaten zu Zwecken der Nutzungsprofilbildung nur auf der Grundlage einer informierten, ausdrücklichen und freiwilligen Einwilligung zulässig.

7.3 App-Store-Betreiber/ Portalbetreiber

7.3.1 Datenerhebung nur im erforderlichen Umfang

App-Store-Betreiber dürfen lediglich personenbezogene Daten erheben und verwenden, wenn hierfür eine Rechtsgrundlage oder eine Einwilligung des Nutzers gegeben ist.

[21] Vgl. auch die gemeinsame Position des Düsseldorfer Kreises und der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten „Smartes Fernsehen nur mit smartem Datenschutz“ vom Mai 2014, Ziffer 1.

Grundsätzlich nicht erhoben werden dürfen daher Informationen darüber, welche App von welchem Nutzer installiert und gestartet wird, es sei denn, dies ist für die Durchführung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Verhältnisses zwischen dem Nutzer und dem App-Store-Betreiber bzw. für die Erbringung des Dienstes erforderlich. Regelmäßig nicht erforderlich ist die Erhebung von Geräte-IDs.

7.3.2 Datenschutzerklärung

Der App-Store Betreiber muss als Telemedienanbieter gem. § 13 Abs. 1 TMG eine Datenschutzerklärung vorhalten, die zu Beginn des Nutzungsvorganges und jederzeit auffindbar ist (vgl. Kapitel 5.2.1). Der Nutzer muss somit unmittelbar, nachdem er aktiv den App-Store aufgerufen hat, die Möglichkeit erhalten, sich über den Umgang mit seinen personenbezogenen Daten informieren zu können.

7.3.3 Nutzungsprofilbildung

Ein Nutzungsprofil unter Pseudonym zu Zwecken der Werbung, der Marktforschung oder der bedarfsgerechten Gestaltung des Telemediendienstes (App-Store) darf nur unter Einhaltung der Vorgaben des § 15 Abs. 3 TMG (vgl. Kapitel 5.1.1.2) erfolgen. Hierbei ist dem Nutzer eine wirksame Widerspruchsmöglichkeit und eine Information über die Nutzungsprofilbildung und die Möglichkeit, zu widersprechen, zur Verfügung zu stellen.

Geht eine Profilerstellung über den Anwendungsbereich des § 15 Abs. 3 TMG hinaus, bedarf es einer Einwilligung.

7.4 App-Anbieter

App-Anbieter unterliegen als Anbieter von Telemedien zahlreichen datenschutzrechtlichen Anforderungen, welche bereits in einer eigenen Orientierungshilfe, der „Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter“ des Düsseldorfer Kreises vom 16. Juni 2014 veröffentlicht wurden.[22] Auch wenn dort unter Kapitel 1 dargestellt wird, dass Besonderheiten von Apps, die für spezielle Endgeräte wie z. B. Smart-TVs entwickelt und angeboten werden, nicht berücksichtigt würden, kann das Dokument als Orientierung dienen. Besonderheiten bei Smart-TV-Apps sind jeweils im Einzelfall zu untersuchen und zu bewerten. Klassische Besonderheiten sind den Aufsichtsbehörden derzeit nicht bekannt.

[22] Die „Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter“ ist z. B. unter der URL http://www.lda.bayern.de/MobileApplikationen/index.html abrufbar.

7.5 Betreiber von Personalisierungsdiensten (Empfehlungsdienste)

7.5.1 Profilbildung für personalisiertes Angebot

Betreiber von Empfehlungsdiensten erheben regelmäßig Nutzungsdaten, um dem entsprechenden Nutzer Empfehlungen entsprechend seiner Interessen (Fernsehgewohnheiten, App-Nutzung) geben zu können. Nutzungsdaten dieser Dienste zu Empfehlungszwecken dürfen nur dann erhoben und verwendet werden, wenn die Voraussetzungen des § 15 Abs. 3 TMG eingehalten werden (vgl. Kapitel 5.1.1.2). Da derartige Nutzungsprofile gem. § 15 Abs. 3 Satz 3 und § 13 Abs. 4 Satz 1 Nr. 6 TMG nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden dürfen, ist eine Zusammenführung mit Registrierungsdaten, eindeutigen Geräte-IDs oder auch der IP-Adresse ohne Einwilligung des Nutzers unzulässig.

7.5.2 Anonyme oder pseudonyme Nutzung

Soweit sich ein Nutzer für einen Empfehlungsdienst registrieren kann, ist dem Nutzer gem. § 13 Abs. 6 TMG grundsätzlich eine Nutzung unter Pseudonym zu ermöglichen (vgl. Kapitel 5.4.5).

7.5.3 Datenschutzerklärung

Der Betreiber von Personalisierungsdiensten muss als Telemedienanbieter gem. § 13 Abs. 1 TMG eine Datenschutzerklärung vorhalten, die zu Beginn des Nutzungsvorganges und jederzeit leicht auffindbar ist (vgl. Kapitel 5.2.1).

7.6 Auftragsdatenverarbeiter

Auftragsdatenverarbeiter (vgl. Kapitel 2.1) können in die verschiedensten Datenumgänge eingebunden werden, indem ihnen bestimmte Datenverarbeitungs-Aufgaben übertragen werden. Der Auftragsdatenverarbeiter darf gem. § 11 Abs. 3 BDSG nur im Rahmen der Weisungen des Auftraggebers mit personenbezogenen Daten umgehen. Gem. § 11 Abs. 4 BDSG treffen den Auftragnehmer nur bestimmte Verpflichtungen aus dem BDSG. Die Verantwortlichkeit für den Datenumgang im Rahmen der Auftragsdatenverarbeitung liegt jedoch bei dem Auftraggeber.

8 Handlungsmöglichkeiten und -verpflichtungen der Datenschutzaufsichtsbehörden

8.1 App-Anbieter

Datenschutzaufsichtsbehörden haben gemäß § 38 Abs. 1 Satz 2 BDSG die Aufgabe, verantwortliche Stellen mit Rücksicht auf deren typische Bedürfnisse zu beraten und zu

unterstützen. Dies bedeutet, dass Anbieter von Smart-TV-Diensten sich von ihrer zuständigen Datenschutzaufsichtsbehörde u. a. dazu beraten lassen können, ob die Gestaltung ihres Beitrags zu der Smart-TV-Nutzung datenschutzkonform ist. Umfang und Intensität der Prüfung hängen dabei allerdings von den personellen Ressourcen und der Prioritätensetzung der Aufsichtsbehörde ab. Die Verantwortung bleibt bei den Diensteanbietern.

8.2 Anordnung nach § 38 Abs. 3 und 5 BDSG

Datenschutzaufsichtsbehörden haben gemäß § 38 Abs. 3 BDSG das Recht (und gelegentlich auch die Pflicht), von verantwortlichen Stellen und damit auch von Anbietern von Smart-TV-Diensten die für die Erfüllung der Aufgaben der Aufsichtsbehörde erforderlichen Auskünfte, das heißt in diesem Zusammenhang insbesondere Auskünfte über die erhobenen personenbezogenen Daten der Smart-TV-Nutzer und die Verwendung dieser Daten, zu verlangen. Wenn Aufsichtsbehörden Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technische und organisatorische Mängel feststellen, können sie gemäß § 38 Abs. 5 BDSG Maßnahmen zur Beseitigung dieser Verstöße anordnen und bei schwerwiegenden Verstößen oder Mängeln die Nutzung oder den Einsatz einzelner Verfahren untersagen.

8.3 Bußgeldverfahren

Datenschutzrechtliche Bußgeldtatbestände sind insbesondere in § 16 TMG und § 43 BDSG enthalten. Verstöße können mit einer Geldbuße bis zu 50.000 Euro, zum Teil sogar bis zu 300.000 Euro geahndet werden.

So handeln Anbieter, die die nach § 38 Abs. 3 BDSG erbetene Auskunft vorsätzlich oder fahrlässig nicht, nicht vollständig oder nicht rechtzeitig erteilen, oder vollziehbaren Anordnungen zur Beseitigung festgestellter Verstöße oder der Untersagung der Nutzung oder des Einsatzes einzelner Verfahren nach § 38 Abs. 5 BDSG zuwiderhandeln, ordnungswidrig und können mit einem Bußgeld bestraft werden.

Anlage: Gemeinsame Position

Mai 2014

Gemeinsame Position
der

Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis)

Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten

---

Smartes Fernsehen nur mit smartem Datenschutz

Moderne Fernsehgeräte (Smart-TV) bieten neben dem Empfang des Fernsehsignals u. a. die Möglichkeit, Internet-Dienste aufzurufen. Den Zuschauern ist es somit möglich, simultan zum laufenden TV-Programm zusätzliche Web-Inhalte durch die Sender auf dem Bildschirm anzeigen zu lassen (etwa durch den HbbTV-Standard). Auch Endgerätehersteller bieten über eigene Web-Plattformen für Smart-TV-Geräte verschiedenste Internet-Dienste an. Für die Zuschauer ist aufgrund der Verzahnung der Online- mit der TV-Welt oft nicht mehr erkennbar, ob sie gerade das TV-Programm oder einen Internet-Dienst nutzen. Überdies können sie vielfach nicht erkennen, um welchen Dienst es sich handelt.

Durch die Online-Verbindung entsteht – anders als beim bisherigen Fernsehen – ein Rückkanal vom Zuschauer zum Fernsehsender, zum Endgerätehersteller oder zu sonstigen Dritten. Das individuelle Nutzungsverhalten kann über diesen Rückkanal erfasst und ausgewertet werden.

Fernsehen ist ein maßgebliches Medium der Informationsvermittlung und notwendige Bedingung für eine freie Meinungsbildung. Das Recht auf freien Informationszugang ist verfassungsrechtlich geschützt und Grundbedingung der freiheitlich demokratischen Grundordnung. Die Wahrnehmung dieses Rechts würde durch die umfassende Erfassung, Auswertung und Nutzung des Nutzungsverhaltens empfindlich beeinträchtigt.

Aus datenschutzrechtlicher Sicht sind die folgenden Anforderungen zu beachten:

1. Die anonyme Nutzung von **Fernsehangeboten** muss auch bei Smart-TV-Nutzung gewährleistet sein. Eine Profilbildung über das individuelle Fernsehverhalten ist ohne informierte und ausdrückliche Einwilligung der Zuschauer unzulässig.

2. Soweit Web- oder HbbTV-Dienste über Smart-TV-Geräte genutzt werden, unterliegen diese als **Telemedien** den datenschutzrechtlichen Anforderungen des Telemediengesetzes. Endgerätehersteller, Sender sowie alle sonstigen Anbieter von Telemedien müssen entweder eine entsprechende Einwilligung der Betroffenen einholen oder zumindest die folgenden rechtlichen Vorgaben beachten:

   - Auch personenbeziehbare Daten der Nutzer dürfen nur verwendet werden, sofern dies zur Erbringung der Dienste oder zu Abrechnungszwecken erforderlich ist.
   - Spätestens bei Beginn der Nutzung müssen die Nutzer erkennbar und umfassend über die Datenerhebung und –verwendung informiert werden.
   - Anbieter von Telemedien dürfen nur dann Nutzungsprofile erstellen und analysieren, sofern hierzu Pseudonyme verwendet werden und die betroffene Nutzerin oder der betroffene Nutzer dem nicht widersprochen hat. Derartige Widersprüche sind wirksam umzusetzen, insbesondere im Gerät hinterlegte Merkmale (z.B. Cookies) sind dann zu löschen. Auf das Widerspruchsrecht sind die Nutzer hinzuweisen. IP-Adressen und Gerätekennungen sind keine Pseudonyme im Sinne des Telemediengesetzes.
   - Verantwortliche Stellen haben sicherzustellen, dass Nutzungsprofildaten nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

3. Beachtung des Prinzips „privacy by default“: Die Grundeinstellungen der Smart-TV-Geräte und Web-Dienste sind durch die Hersteller und Anbieter derart zu gestalten, dass dem Prinzip der anonymen Nutzung des Fernsehens hinreichend Rechnung getragen wird. Der Aufruf der Web-Dienste und die damit einhergehende wechselseitige Kommunikation mit Endgerätehersteller, Sender oder sonstigen Anbietern per Internet dürfen erst nach umfassender Information durch die Nutzer selbst initiiert werden, z. B. die Red-Button-Aktivierung bei HbbTV. Die auf den Geräten gespeicherten Daten müssen der Kontrolle durch die Nutzer unterliegen. Insbesondere muss die Möglichkeit bestehen, Cookies zu verwalten.

4. Smart-TV-Geräte, die HbbTV- Angebote der Sender sowie sonstige Web-Dienste müssen über sicherheitstechnische Mechanismen verfügen, die die Geräte und den Datenverkehr vor dem Zugriff unbefugter Dritter schützen.

Diese Position wird von der Konferenz der Direktoren der Landesanstalten für Medien unterstützt.

16.2 Beschluss vom 8./9. März 2016

16.2.1 Orientierungshilfe zur datenschutzrechtlichen Einwilligungserklärung in Formularen

Stand: März 2016

Diese Orientierungshilfe enthält Hinweise zur datenschutzgerechten Formulierung und Gestaltung von schriftlichen Einwilligungserklärungen nach § 4a Bundesdatenschutzgesetz (BDSG) und elektronischen Texten nach § 13 Abs. 2 und Abs. 3 des Telemediengesetzes (TMG). Einwilligungen in Übermittlungen in Drittstaaten werden von dieser Orientierungshilfe nicht erfasst. Ergänzend sind gegebenenfalls die gesetzlichen Regelungen zu Allgemeinen Geschäftsbedingungen zu beachten.

In der täglichen Praxis der Datenschutzaufsichtsbehörden fällt immer wieder auf, dass in Antragsvordrucken von Firmen, Versicherungen, Banken, und anderen neben den vom Leistungsanbieter fest vorgegebenen Vertragsbedingungen die eventuell dazu ergänzend vorgesehenen datenschutzrechtlichen Einwilligungserklärungen nicht den Erfordernissen des § 4a BDSG entsprechen oder aber als „Einwilligungen“ bezeichnete Texte vielmehr in Wirklichkeit als unabdingbare Vertragserklärungen bzw. allgemein geltende Geschäftsbedingungen einzustufen sind. Muss eine (AGB-rechtlich zulässige) Erklärung abgegeben bzw. Vertragsbedingung akzeptiert werden, um einen Vertrag abzuschließen, hat die betroffene Person also gar keine freie Wahlmöglichkeit, so handelt es sich nicht um eine datenschutzrechtliche Einwilligung nach § 4a BDSG, sondern um ein Vertragsangebot, das angenommen oder abgelehnt werden kann. Die mögliche Erlaubnis für den Datenumgang ergibt sich dann nicht aus § 4a BDSG, sondern aus § 28 Abs. 1 Satz 1 Nr. 1 BDSG.

1. Überschriften

Bereits die Überschriften bringen häufig nicht klar genug zum Ausdruck, ob hier vom Antragsteller oder Kunden neben seiner hauptsächlichen Erklärung, beispielsweise dem Versicherungsantrag oder seiner Teilnahmeerklärung, noch zusätzlich eine datenschutzrechtliche Einwilligung abverlangt wird. Dies soll anhand einiger **Negativbeispiele** für Überschriften aufgezeigt werden:

- Datenschutzerklärung
- Datenschutz
- Datenschutzklausel
- Hinweis zum Datenschutz

- Erklärung zum Datenschutz
- Erklärung zur Datenverarbeitung

Im Gegensatz dazu weisen folgende dem § 4a BDSG entsprechende Positivbeispiele für Überschriften den Unterzeichnenden darauf hin, dass er mit Unterzeichnung eine datenschutzrechtliche Einwilligung abgibt:

- Einwilligungserklärung Datenschutz
- Datenschutzrechtliche Einwilligungserklärung
- Datenschutzrechtliche Einwilligungsklausel
- Einwilligungserklärung nach dem Bundesdatenschutzgesetz

2. Eindeutigkeit

Auch die Erklärung selbst ist zuweilen nicht eindeutig genug vorformuliert. So reicht es nicht aus, wenn sie mit den Worten beginnt: „Mir ist bekannt, dass ...“. Hier ist dem Kunden nicht bewusst, dass er eine zusätzliche Erklärung abgibt.

Die notwendige Klarheit besteht nur, wenn die Formulierung den Erklärungscharakter eindeutig zum Ausdruck bringt, wie es in folgenden Positivbeispielen aufgezeigt wird:

- Ich willige ein, dass ...
- Ich bin einverstanden, dass ...
- Mit der Unterschrift geben Sie Ihre Einwilligung, dass ...
- Durch Ihre Unterschrift wird die vorstehende Einwilligungserklärung mit den auf der Rückseite abgedruckten näheren Erläuterungen zur Datenverarbeitung und Datennutzung für … (*Zweck*) Bestandteil des Antrages.

Weiter muss es sich um eine bewusste Erklärung der betreffenden Person selbst handeln (opt-in). Schon von der verantwortlichen Stelle im Sinne einer Zustimmung vorangekreuzte Einwilligungstexte oder nur mit einer Streich-/Abwahl-Möglichkeit versehene „vorgegebene Zustimmungen“ (opt-out) genügen dem grundsätzlich nicht.

3. Freiwilligkeit

Eine wirksame datenschutzrechtliche Einwilligung im Sinne von § 4a BDSG liegt nur dann vor, wenn diese freiwillig abgegeben werden und auch jederzeit widerrufen werden kann. Eine unter Druck oder Zwang abgegebene datenschutzrechtliche Einwilligung ist unwirksam.

4. Hervorhebung

In zahlreichen vorformulierten Einwilligungserklärungen fehlt es an der gemäß § 4a Abs. 1 Satz 4 BDSG und – bei Einwilligung in Werbung – gemäß § 28 Abs. 3a Satz 2 BDSG erforderlichen besonderen Hervorhebung gegenüber anderen Textpassagen, zum Beispiel durch

- Fettdruck, Schriftart oder Schriftgröße,
- farbliche Gestaltung der Schrift oder des Hintergrundes oder
- eine Umrahmung der Erklärung.

5. Platzierung

Die datenschutzrechtliche Einwilligungserklärung gehört als besondere beziehungsweise zusätzliche Willensäußerung der betroffenen Person in hervorgehobener Form (siehe unter Ziffer 4) grundsätzlich insgesamt auf das eigentliche Antragsformular und dort in aller Regel unmittelbar vor die Unterschrift, die dann sowohl die Hauptsacheerklärung (beispielsweise den Versicherungsantrag) als auch die datenschutzrechtliche Einwilligungserklärung abdeckt.

Denkbar ist aber auch bei längeren Einwilligungstexten eine besonders hervorzuhebende aussagekräftige Kurzfassung mit den wesentlichen Inhalten der datenschutzrechtlichen Einwilligungserklärung bei der Unterschrift mit einem Hinweis auf den beispielsweise auf der Rückseite oder auf einer Anlage enthaltenen erläuternden Text (siehe letztes Positivbeispiel unter Ziffer 2.).

Besonders datenschutzfreundlich – und in einzelnen Fallkonstellationen zwingend erforderlich (beispielsweise bei der beabsichtigten Übermittlung von Gesundheitsdaten) – ist es, wenn im Formular für die datenschutzrechtliche Einwilligung eine gesonderte Unterschrift vorgesehen ist.

Jedenfalls ist zur Sicherstellung der Eindeutigkeit und Freiwilligkeit (siehe Ziffern 2 und 3) erforderlich, dass die Einwilligungserklärung für ihre Gültigkeit ausdrücklich angenommen werden muss (beispielsweise durch ein Ankreuzen).

6. Trennung

In manchen Formularen werden die Datenschutzhinweise und -informationen nach § 4 Abs. 3 BDSG zu unabdingbaren Vertragsinhalten beziehungsweise allgemein geltenden Geschäftsbedingungen mit einer auf freiwilliger Basis abgefragten datenschutzrecht-

lichen Einwilligungserklärung nach § 4a BDSG vermischt. Unter der Überschrift „Datenschutzhinweise“ beginnt der Text mit Hinweisen und geht dann im weiteren Verlauf unvermittelt in eine Einwilligungserklärung über.

Dem Betroffenen wird hier nicht deutlich genug vor Augen geführt, dass er eine datenschutzrechtliche Einwilligungserklärung abgeben soll. Die reinen Informationen über Datenverarbeitung auf der Grundlage von Gesetz beziehungsweise Vertrag auf der einen Seite und die freiwillige datenschutzrechtliche Einwilligungserklärung auf der anderen Seite müssen textlich getrennt dargestellt werden. Eine mangelnde Trennung kann dazu führen, dass die Einwilligung als solche nicht erkannt wird und deshalb unwirksam sein kann.

7. Klare Zuordnung

Die ansonsten korrekt gestaltete datenschutzrechtliche Einwilligungserklärung soll nicht mit Datenverwendungen aufgebläht werden, die gar nicht einwilligungsbedürftig sind, da sie bereits auf Grund eines Gesetzes oder einer sonstigen Rechtsvorschrift zulässig sind.

Es ist vielmehr eine klare Zuordnung zur Einwilligung einerseits und zu den Datenschutzinformationen nach § 4 Abs. 3 BDSG andererseits vorzunehmen.
Ist es rechtlich strittig, ob eine Datenverwendung einer Einwilligung bedarf, bestehen keine Bedenken, sie unter Beachtung der oben genannten Formvorschriften „vorsichtshalber“ in die Einwilligungserklärung mit einzubeziehen.

8. Einwilligung bei besonderen Arten personenbezogener Daten

Soweit sich die Einwilligung auf besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) beziehen soll, ist bei der formularmäßigen Gestaltung der Erklärung § 4a Abs. 3 BDSG zu beachten, das heißt die Einwilligung muss ausdrücklich auch für diese besonderen Arten personenbezogener Daten erklärt werden.

9. Inhalt von Einwilligungen

Der Text der Einwilligungserklärung muss die betroffene Person klar und allgemein verständlich über die zu verarbeitenden Daten und den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung der Daten durch die verantwortliche Stelle informieren, und muss, soweit nach den Umständen des Einzelfalls erforderlich, auf eventuelle Folgen der Verweigerung der Einwilligung hinweisen (§ 4a Abs. 1 Satz 2 BDSG).
Auf die grundsätzlich gegebene Widerrufsmöglichkeit der Einwilligung ist hinzuweisen; im Bereich der Telemedien ist ein solcher Hinweis durch § 13 Abs. 3 TMG sogar ausdrücklich vorgeschrieben (siehe bei Nr. 10).

Wenn im Rahmen der Verarbeitung auch Datenübermittlungen an Dritte in Betracht kommen, sind die Datenübermittlungen mit deren Zweckbestimmung und die Empfänger der Daten transparent zu erläutern.

Eine undifferenzierte, nicht mehr überschaubare Darstellung einer großen Anzahl genannter Datenempfänger kann den Transparenzanforderungen widersprechen und nach der zivilrechtlichen Rechtsprechung zu einer Unwirksamkeit der Einwilligung führen.

10. Einwilligung bei Telemedienangeboten

Wird eine Einwilligung elektronisch im Rahmen eines Telemedienangebotes eingeholt (beispielsweise auf einer Webseite), so sind gemäß § 13 Abs. 2 und Abs. 3 TMG einige Besonderheiten zu beachten:

Danach muss der Diensteanbieter sicherstellen, dass

- der Nutzer die Einwilligung bewusst und eindeutig erteilt hat,
- die Einwilligung protokolliert wird,
- der Nutzer den Inhalt der Einwilligung jederzeit abrufen und
- mit Wirkung für die Zukunft widerrufen kann.

Der Nutzer muss zudem vor Erklärung der Einwilligung auf sein jederzeitiges Widerrufsrecht hingewiesen werden, wobei diese Information für den Nutzer jederzeit abrufbar sein muss. Diese Unterrichtung kann beispielsweise in der Datenschutzerklärung erfolgen.

11. Werbeeinwilligungen

Hierzu wird auf die ergänzenden Regelungen in § 28 Abs. 3a und 3b BDSG hingewiesen. Siehe insoweit auch die Ziffern 2 und 4 der Anwendungshinweise der Datenschutzaufsichtsbehörden zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für werbliche Zwecke, https://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/Anwendungshinweise_Werbung.pdf.

16.3 Beschluss vom 13./14. September 2016

16.3.1 Fortgeltung bisher erteilter Einwilligungen unter der Datenschutz-Grundverordnung

Bisher erteilte Einwilligungen gelten fort, sofern sie der Art nach den Bedingungen der Datenschutz-Grundverordnung entsprechen (Erwägungsgrund 171, Satz 3 Datenschutz-Grundverordnung).

Bisher rechtswirksame Einwilligungen erfüllen grundsätzlich diese Bedingungen.

Informationspflichten nach Artikel 13 Datenschutz-Grundverordnung müssen dafür nicht erfüllt sein, da sie keine Bedingungen im Sinne des genannten Erwägungsgrundes sind.

Besondere Beachtung verdienen allerdings die folgenden Bedingungen der Datenschutz-Grundverordnung; sind diese Bedingungen nicht erfüllt, gelten bisher erteilte Einwilligungen nicht fort:

- Freiwilligkeit („Kopplungsverbot“, Artikel 7 Absatz 4 in Verbindung mit Erwägungsgrund 43 Datenschutz-Grundverordnung),
- Altersgrenze: 16 Jahre (soweit im nationalen Recht nichts anderes bestimmt wird; Schutz des Kindeswohls, Artikel 8 Absatz 1 in Verbindung mit Erwägungsgrund 38 Datenschutz-Grundverordnung).

Anlagen

Anlage 1 – Pressemitteilung der Bundesnetzagentur

Bundesnetzagentur

Pressemitteilung

HAUSANSCHRIFT
Tulpenfeld 4
53113 Bonn

TEL +49 228 14–9921
FAX +49 228 14–8975

pressestelle@bnetza.de
www.bundesnetzagentur.de

Bonn, 25. April 2016

Bundesnetzagentur sagt verbotenen Spionagekameras den Kampf an

Homann: „Gerade in der heutigen Zeit ist dem Schutz der Privatsphäre besondere Aufmerksamkeit zu schenken“

Die Bundesnetzagentur ist in den letzten Wochen gegen mehr als 70 Fälle von verbotenen Spionagekameras vorgegangen.

Hierbei handelte es sich zum großen Teil um WLAN-fähige Kameras, die einen anderen Gegenstand vortäuschten oder mit Gegenständen des täglichen Gebrauchs verkleidet waren.

„Besonders beliebt ist es nach unseren Erkenntnissen, diese Kameras in Uhren, Rauchmeldern oder Lampen zu verstecken,“ so Jochen Homann, Präsident der Bundesnetzagentur. „Aber auch Pop-Art-Blumen oder Powerbanks dienen als Verkleidung. Der Phantasie sind hierbei offenbar keine Grenzen gesetzt.“

Nach § 90 Telekommunikationsgesetz (TKG) ist es verboten, Sendeanlagen zu besitzen, zu vertreiben oder herzustellen die mit Gegenständen des täglichen Gebrauchs verkleidet sind und auf Grund dieser Umstände in besonderer Weise geeignet und dazu bestimmt sind, das Bild eines anderen von diesem unbemerkt aufzunehmen.

„Diese Kameras ermöglichen eine unbemerkte Fernüberwachung und gefährden dadurch ein unbeschwertes Privatleben. Wir gehen daher entschlossen gegen alle Beteiligten wie Hersteller, Verkäufer und Käufer dieser Kameras vor,“ betonte Homann.

Gerade im Internet sind derartige Kameras auf den unterschiedlichsten Verkaufsplattformen zu finden. Wird die Bundesnetzagentur durch eigene Recherche oder Hinweise auf solche Angebote aufmerksam, werden zunächst die Plattformbetreiber zur Löschung des Angebotes aufgefordert, um den weiteren Verkauf sofort zu unterbinden. Anschließend werden die Verkäufer im Rahmen eines Verwaltungsverfahrens kontaktiert, damit diese künftig den Vertrieb unterlassen und die Käufer der Gegenstände benennen. Von den Verkäufern und Käufern wird die Vernichtung der Gegenstände verlangt. Hierüber ist ein Nachweis, etwa in Form einer Bescheinigung einer Abfallwirtschaftsstation, beizubringen.

Häufig zeigen sich die Käufer und Verkäufer einsichtig und sind kooperativ.

Anlage 2 – Einheitlicher Blut- und Plasmaspenderfragebogen

Einheitlicher Blut- und Plasmaspenderfragebogen (Version 2) – Stand 13.01.2015

Fragen zu Ihrem allgemeinen Gesundheitszustand			
1.	• Fühlen Sie sich **krank** oder sind Sie **krankgeschrieben**? • Haben Sie heute schon gegessen und getrunken? * • Wiegen Sie mindestens 50kg? *	□ ja □ ja □ ja	□ nein □ nein □ nein
2.	Hatten Sie in der letzten Woche • einen unkomplizierten Infekt (z. B. Schnupfen, Erkältung, Harnwegsinfekt) ohne Fieber, • eine zahnärztliche Behandlung oder professionelle Zahnreinigung, • eine Verletzung oder einen kleinen operativen Eingriff?	 □ ja □ ja □ ja	 □ nein □ nein □ nein
3.	Hatten Sie in den letzten 4 Wochen Durchfall, anhaltende Bauchschmerzen, Erbrechen, eine Entzündung oder Fieber?	□ ja	□ nein
4.	Waren Sie in den letzten 4 Monaten im Krankenhaus, beim Arzt oder beim Heilpraktiker?	□ ja	□ nein
5.	Haben oder hatten Sie eine oder mehrere der folgenden Erkrankungen (ggf. unterstreichen): • Herz- oder Gefäßerkrankung (z. B. Thrombose, Herzrhythmusstörung, Schlaganfall, Herzinfarkt), • Nervenerkrankung (z.B. Epilepsie), • Erkrankung von Haut, Blut, Lunge (z. B. Asthma), Leber, Niere, Magen oder Darm; chronische Erkrankungen wie Allergien, Zuckerkrankheit, • Tumor (z.B. Krebs)?	 □ ja □ ja □ ja □ ja	 □ nein □ nein □ nein □ nein
6.	• Ist Ihnen schon einmal gesagt worden, dass Sie kein Blut spenden dürfen? • Hat es bei einer früheren Blutentnahme/Blutspende Komplikationen gegeben? • Spenden Sie auch in anderen Blutspende-Einrichtungen?	□ ja □ ja □ ja	□ nein □ nein □ nein
7.	Konsumieren Sie Medikamente oder Rauschmittel missbräuchlich?	□ ja	□ nein
8.	Werden Sie in den nächsten 12 Stunden Tätigkeiten in Beruf oder Hobby ausüben, die Sie oder andere gefährden könnten (z. B. Personenbeförderung, Tätigkeit mit Absturzgefahr oder erheblicher körperlicher Belastung)	□ ja	□ nein
9.	• Sind Sie schwanger oder stillen Sie? • Waren Sie **jemals** schwanger? • Wenn ja, wann zuletzt?	□ ja □ ja	□ nein □ nein
Fragen zu Infektionskrankheiten, die durch Blut übertragen werden können			
10.	Wurde bei Ihnen jemals • eine Leberentzündung („Gelbsucht"), z. B. Hepatitis A, Hepatitis B oder Hepatitis C festgestellt? • eine Infektion mit HIV (AIDS) oder HTLV nachgewiesen?	 □ ja □ ja	 □ nein □ nein
11.	• Hatten Sie in den letzten 4 Monaten eine Akupunktur? • Haben Sie sich in den letzten 4 Monaten tätowieren lassen oder einer anderen Maßnahme unterzogen, die Haut oder Schleimhaut verletzt wie Piercing, Ohrlochstechen, Botoxspritzen, permanentes Make-up, Body Modification?	□ ja □ ja	□ nein □ nein
12.	Haben Sie in den letzten 4 Monaten mit einer Person in einem Haushalt gelebt, bei der eine Leberentzündung (Hepatitis) festgestellt wurde?	□ ja	□ nein
13.	Sind Sie in den letzten 4 Monaten in Berührung mit Blut einer anderen Person gekommen, z.B. über die Schleimhaut (auch Auge) oder durch eine Verletzung mit einem Instrument (z.B. Injektionsnadel)?	□ ja	□ nein
14.	Haben Sie innerhalb der letzten 2 Jahre eine Blutübertragung (rote Blutkörperchen, Blutplättchen, Blutplasma - auch Eigenblut) erhalten?	□ ja	□ nein
15.	Hatten Sie in den letzten 4 Monaten eine Operation, eine Gewebetransplantation, eine Endoskopie (z. B. Magen-, Blasen-, Darm- oder Gelenkspiegelung), eine Katheteranwendung oder wurde Ihnen Gewebe entnommen (Biopsie)?	□ ja	□ nein

16.	Über den Sexualverkehr können Infektionen, wie z.B. HIV oder Hepatitis, übertragen werden. Direkt nach der Ansteckung mit HIV und/oder Hepatitis kann ein Spender ohne es zu wissen infiziert sein und durch sein Blut den Empfänger der Spende anstecken. Leider können Labortests eine Infektion zum Teil erst bis zu 4 Monate nach der Ansteckung nachweisen. Daher schützen Sie mit Ihrer ehrlichen Antwort die Empfänger Ihrer Spende.		
	Hatten Sie in den letzten 4 Monaten Sexualverkehr • mit einer neuen Partnerin / einem neuen Partner? • mit einer Person, die eine schwere Infektionskrankheit (z.B. AIDS oder Hepatitis) hat oder haben könnte? • für den Sie Geld oder andere Leistungen (Unterkunft, Drogen) bezahlt haben? • **Nur für Frauen:** mit einem bisexuellen Mann?	□ ja	□ nein
	• Haben Sie schon einmal Geld oder andere Leistungen für Sexualverkehr erhalten? • **Nur für Männer**: Hatten Sie schon einmal Sexualverkehr mit einem anderen Mann?	□ ja	□ nein
17.	Haben Sie schon einmal Drogen gespritzt, oder geschnupft?	□ ja	□ nein
18.	Waren Sie innerhalb der letzten 4 Monate in Haft?	□ ja	□ nein
19.	Haben Sie in den letzten 4 Monaten Spritzen erhalten, die nicht vom Arzt verschrieben wurden (z.B. Muskelaufbaupräparate)?	□ ja	□ nein
20.	• Haben Sie jemals Frischzellen, bzw. Gewebe (Transplantate) oder Gewebeextrakte von Tieren erhalten?	□ ja	□ nein
	• Sind Sie in den letzten 12 Monaten nach Tierkontakt gegen Tollwut geimpft worden?	□ ja	□ nein
	• Erhielten Sie in den letzten 12 Monaten tierisches Serum (z.B. gegen Schlangenbisse)?	□ ja	□ nein
21.	• Sind Sie außerhalb Europas geboren?	□ ja	□ nein
	• Haben Sie jemals länger als 6 Monate außerhalb Europas gelebt? Wenn ja, wo? ..... Wann?	□ ja	□ nein
	• Waren Sie in den letzten 6 Monaten, auch kurzfristig, im Ausland? wo?	□ ja	□ nein
22.	Wurde bei Ihnen jemals eine Malaria festgestellt?	□ ja	□ nein
23.	Haben oder hatten Sie eine Tuberkulose, Osteomyelitis, Syphilis, Rheumatisches Fieber, Toxoplasmose, Salmonelleninfektion (Typhus- oder Paratyphus), Q-Fieber?	□ ja	□ nein
24.	Wurde bei Ihnen jemals eine der folgenden seltenen Erkrankungen festgestellt: Chagas-Krankheit (Trypanosomiasis), Brucellose, Babesiose, Leishmaniose, Lepra, Melioidose, Rückfallfieber, Hasenpest (Tularämie), Fleckfieber oder andere Rickettsiosen?	□ ja	□ nein
Fragen zu möglichen Rückständen von Arzneimitteln im Blut			
25.	Haben Sie innerhalb der letzten 4 Wochen Tabletten o.a. Medikamente eingenommen, wie z.B. Antibiotika, Schmerzmittel (auch Aspirin, ASS), Mittel gegen Bluthochdruck oder andere? Wenn ja, welche?	□ ja	□ nein
26.	Haben Sie jemals Tabletten zur Behandlung von Schuppenflechte oder schwerer Akne eingenommen (z.B. Tigason©, Neo-Tigason©, Roaccutan©)?	□ ja	□ nein
27.	Wurden Sie in den letzten 4 Wochen geimpft? Wenn ja, gegen welche Erkrankungen?	□ ja	□ nein
Fragen nach übertragbaren Hirnerkrankungen			
28.	Wurde bei Ihnen oder einem Ihrer Blutsverwandten die Creutzfeldt-Jakob-Krankheit oder eine ähnliche Erkrankung festgestellt oder bestand jemals ein Verdacht auf eine dieser Erkrankungen?	□ ja	□ nein
29.	• Wurden Sie vor 1986 mit Hormonen der Hirnanhangdrüse, z.B. wegen Wachstumsstörungen, Unfruchtbarkeit, Endometriose behandelt?	□ ja	□ nein
	• Haben Sie jemals Hornhaut -, Hirnhaut - oder andere Transplantate erhalten?	□ ja	□ nein
30.	• Haben Sie sich in der Zeit zwischen dem 01.01.1980 und 31.12.1996 insgesamt länger als 6 Monate im Vereinigten Königreich Großbritannien und Nordirland aufgehalten?	□ ja	□ nein
	• Sind Sie im Vereinigten Königreich Großbritannien und Nordirland nach dem 01.01.1980 operiert worden oder haben Sie dort eine Blutübertragung (rote Blutkörperchen, Blutplättchen, Blutplasma) erhalten?	□ ja	□ nein

* Aufnahme der Fragen in den Spenderfragebogen ist nicht verpflichtend.
Die gelb hinterlegten Zusatzangaben des Spenders müssen nicht auf einem selbst auszufüllenden Fragebogen dokumentiert werden, sondern können auch im Gespräch mit dem ärztlichen Spendepersonal erfragt und dokumentiert werden.

Stichwortverzeichnis