Sächsischer Landtag
6. Wahlperiode

DRUCKSACHE 6/2563

Schutz des Persönlichkeitsrechts im nicht-öffentlichen Bereich

7. Tätigkeitsbericht

des

Sächsischen Datenschutzbeauftragten

Berichtszeitraum: 1. April 2013 bis 31. März 2015

Dem Sächsischen Landtag

vorgelegt zum 31. März 2015

gemäß § 30 des Sächsischen Datenschutzgesetzes

Eingegangen am: 24. September 2015 Ausgegeben am: 24. September 2015

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
AEntG	Arbeitnehmer-Entsendegesetz
AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
AGG	Allgemeines Gleichbehandlungsgesetz
AO	Abgabenordnung
Aufl.	Auflage
Az.	Aktenzeichen
BAG	Bundesarbeitsgericht
BCC	Blind Carbon Copy (Blindkopie-Empfänger)
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BZRG	Bundeszentralregistergesetz
CC	Carbon Copy (Kopie-Empfänger)
DSK	Konferenz der Datenschutzbeauftragten des Bundes und der Länder
EC	Electronic Cash
EG	Europäische Gemeinschaft
EMRK	Europäische Menschenrechtskonvention
Erfa-Kreis	Erfahrungsaustausch-Kreis
EU	Europäische Union
EuGH	Europäischer Gerichtshof
GastG	Gaststättengesetz
GDD	Gesellschaft für Datenschutz und Datensicherung e. V.
GewO	Gewerbeordnung
GG	Grundgesetz

GmbH	Gesellschaft mit beschränkter Haftung
GPS	Global Positioning System
GVG	Gerichtsverfassungsgesetz
GwG	Geldwäschegesetz
HGB	Handelsgesetzbuch
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
IP	Internet Protocol (Internetprotokoll)
KG	Kammergericht
KiTa	Kindertagesstätte
KunstUrhG	Kunsturheberrechtsgesetz
KWG	Kreditwesengesetz
LDA	Bayerisches Landesamt für Datenschutzaufsicht (Ansbach)
LG	Landgericht
LSA	Lichtsignalanlage
LSG	Landessozialgericht
MiLoG	Mindestlohngesetz
NJW	Neue Juristische Wochenschrift
OLG	Oberlandesgericht
OWiG	Ordnungswidrigkeitengesetz
OWiZuVO	Ordnungswidrigkeiten-Zuständigkeitsverordnung
PAuswG	Personalausweisgesetz
PGP	Pretty Good Privacy (Verschlüsselungsverfahren)
PIN	Persönliche Identifikationsnummer
Pkw	Personenkraftwagen
RDG	Rechtsdienstleistungsgesetz
Rdnr.	Randnummer
RL	Richtlinie
RR	Rechtsprechungsreport
RStV	Rundfunkstaatsvertrag
SächsDSG	Sächsisches Datenschutzgesetz
SächsGVBl.	Sächsisches Gesetz- und Verordnungsblatt

SächsMG	Sächsisches Meldegesetz
SächsVwVG	Sächsisches Verwaltungsvollstreckungsgesetz
SächsWaldG	Sächsisches Waldgesetz
SD-Karte	Secure Digital Memory Card (sichere digitale Speicherkarte)
SEPA	Single Euro Payments Area (Einheitlicher Euro-Zahlungsverkehrsraum)
SGB	Sozialgesetzbuch
SSL	Secure Sockets Layer (Verschlüsselungsmethode)
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TB	Tätigkeitsbericht
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
UWG	Gesetz gegen den unlauteren Wettbewerb
VG	Verwaltungsgericht
VwVfG	Verwaltungsverfahrensgesetz
WEG	Wohnungseigentümergemeinschaft / Wohneigentumsgesetz
WoFG	Wohnraumförderungsgesetz
ZAG	Zahlungsdiensteaufsichtsgesetz
ZPO	Zivilprozessordnung

Vorwort

Nach der Umstellung des Berichtszeitraums im Jahr 2013 kehre ich mit meinem siebenten Tätigkeitsbericht wieder zu dem gewohnten Zweijahresrhythmus zurück und berichte nunmehr - im Gleichklang mit dem öffentlichen Bereich - über meine Aufsichtstätigkeit im Zeitraum vom 1. April 2013 bis zum 31. März 2015.

Ich habe in den letzten Jahren immer wieder auf meine vollkommen unzureichende Personalausstattung hingewiesen und vor deren Folgen gewarnt. Bereits in der Vergangenheit musste ich bekanntlich - anders als die meisten anderen Datenschutzaufsichtsbehörden - erhebliche Abstriche bei meiner Aufsichts-, Kontroll- und Ahndungstätigkeit machen. Weil meine Mitarbeiter mit der Bearbeitung der ständig wachsenden Anzahl der Eingaben und Beratungswünsche mehr als ausgelastet waren, musste ich insbesondere meine anlassfreie Kontrolltätigkeit ganz erheblich einschränken und habe nunmehr den absoluten Tiefpunkt erreicht: Im Berichtszeitraum habe ich keine einzige anlassfreie Kontrolle durchführen können. Zum Vergleich: In den Jahren 2003/2004 (Berichtszeitraum des 2. TB) sind durch das seinerzeit noch zuständige Sächsische Staatsministerium des Innern bzw. eigentlich durch die dem Ministerium nachgeordneten Regierungspräsidien insgesamt noch 110 (!) Regelkontrollen durchgeführt worden. Zugegebenermaßen war das Beschwerde- und Beratungsaufkommen in dieser Zeit bei Weitem nicht so hoch wie heute, allerdings verdeutlichen diese Zahlen eindrucksvoll das im Datenschutz aktuell in Sachsen bestehende Vollzugsdefizit. Man muss kein Hellseher sein, um zu erkennen, dass der insoweit durch die Personalausstattung praktisch vorgegebene Verzicht auf die in erster Linie mit präventiver Zielsetzung durchgeführten Regelkontrollen natürlich auch zu einem letztendlich vergrößerten Anstieg der Eingaben und damit der anlassbedingten Tätigkeit führt. Wie man so schön sagt, beißt sich die Katze also in den Schwanz. Es bleibt abzuwarten, ob die mir nun nach langem Ringen bei den diesjährigen Haushaltsverhandlungen zugestandenen Personalverstärkungen tatsächlich im notwendigen Umfang und der benötigten Qualität kommen und zu einer Entlastung meiner Mitarbeiter führen werden. Derzeit jedenfalls überschreitet das anstehende Arbeitspensum deutlich das Limit meiner Mitarbeiter. Dies wird - bei erstmals nur geringfügig weiter gestiegenen Beschwerdeaufkommen (vgl. Pkt. 4), jedoch wiederum erheblich angestiegenen Beratungswünschen (Zunahme um 41 % - vgl. Pkt. 5) - daran deutlich, dass sich die Bearbeitungszeiten gerade bei den Eingaben deutlich verlängert haben. So waren zum Stichtag dieses Tätigkeitsberichtes (31. März 2015) noch sage und schreibe 91 anlassbedingte Aufsichtsfälle in Bearbeitung - in den Vorjahren waren dies nie mehr als 30 Fälle gewesen. Bearbeitungszeiten von einem Jahr kommen durchaus vor. Im Bereich der Ordnungswidrigkeiten musste ich erheblich mehr Verfahren als sonst - wegen überlanger Verfahrensdauer - einstellen (vgl. Pkt. 11.2).

Hinzu kommt, dass auch die Auseinandersetzungen mit der Staatsanwaltschaft in der Frage meiner Unabhängigkeit bei der Ahndung von Datenschutzverstößen erhebliche Ressourcen gebunden haben. Darüber hinaus habe ich im Bereich der Ordnungswidrigkeiten auch neue zusätzliche Verfolgungszuständigkeiten erhalten (vgl. Pkt. 11.1).

Zukünftig werde ich daher (auch deshalb) die verantwortlichen Stellen an den Kosten meiner Aufsichtstätigkeit beteiligen müssen. Mit Wirkung vom 9. Mai 2015 wurde in § 40 SächsDSG eine Regelung aufgenommen, die mich ermächtigt, entsprechend dem Verwaltungsaufwand für bestimmte Amtshandlungen und sonstige öffentlich-rechtliche Leistungen nach dem Bundesdatenschutzgesetz Kosten zu erheben (vgl. dazu Pkt. 10.3).

Trotz der unverändert schlechten Rahmenbedingungen habe ich im Berichtszeitraum wiederum zahlreiche Veränderungen zugunsten des Datenschutzes bei den verantwortlichen Stellen bewirken können. Auch die Tatsache, dass ich nur bei etwa jeder dritten Kontrolle im Ergebnis einen Verstoß gegen datenschutzrechtliche Vorschriften habe feststellen müssen, zeugt davon, dass es um den Datenschutz im nicht-öffentlichen Bereich im Freistaat Sachsen nicht so schlecht bestellt ist, wie das die stete Zunahme der anlassbedingten Kontrollfälle möglicherweise suggeriert. Im Umkehrschluss bedeutet das zwar auch, dass die Eingaben in der Mehrzahl der Fälle unbegründet waren, jedoch möchte ich an dieser Stelle ausdrücklich dazu ermutigen, sich auch in Zweifelsfällen an mich zu wenden. In Zeiten, in denen viele Menschen insbesondere im Internet sehr freizügig mit ihren Daten umgehen, begrüße ich es, wenn sich Bürger bei mir melden und auf mögliche datenschutzrechtliche Probleme hinweisen, auch wenn sich der Verdacht eines Datenschutzverstoßes dann am Ende doch nicht bestätigt. Dies zeugt zweifellos von einer in großen Teilen der Bevölkerung vorhandenen Sensibilität für datenschutzrechtliche Fragen. Soweit Eingaben bzw. Hinweise nicht in offensichtlich missbräuchlicher Schädigungsabsicht erfolgen, muss auch niemand damit rechnen, als Hinweisgeber oder Beschwerdeführer der verantwortlichen Stelle gegenüber offengelegt zu werden.

Dem vorliegenden Bericht können Sie neben allgemeinen Ausführungen zu meiner Tätigkeit als Aufsichts- und OWiG-Verwaltungsbehörde entnehmen, welche (neuen) datenschutzrechtlichen Sachverhalte im Berichtszeitraum an mich herangetragen worden sind und wie ich diese bewertet habe.

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 § 43 BDSG sowie seit Mitte 2014 auch von datenschutzrechtlichen Ordnungswidrigkeiten nach dem Telemediengesetz und nach § 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.

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

- 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 2015 lagen insgesamt 34 Registermeldungen von 28 Unternehmen vor, die

- in 9 Fällen Verfahren von Handels- und Wirtschaftsauskunfteien,

- in 19 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 lediglich ein solches Verlangen zu verzeichnen.

3 Regelaufsicht

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

Regel- bzw. anlassfreie Kontrollen sind reine Routineüberprüfungen. Die Erfahrungen aus früheren Jahren (s. u.) zeigen, dass man dabei - wenn auch mit einigem Aufwand - eine erhebliche Wirkung erzielen kann. Dies gilt umso mehr, wenn man solche Kontrollen auf bestimmte Branchen konzentriert, nach einem einheitlichen Muster bei einer Vielzahl von Unternehmen durchführt und die Überprüfungen vorher auch ankündigt. Man erreicht auf diese Weise bei weitaus mehr Unternehmen Verbesserungen in der Datenschutzorganisation als dann tatsächlich kontrolliert werden. Vor der eigentlichen Kontrolle muss zunächst jeder damit rechnen, dass auch er unter den kontrollierten Unternehmen ist, und später sprechen sich die Ergebnisse, Bewertungen und ggf. auch die repressiven Maßnahmen der Aufsichtsbehörde natürlich herum. Auch Aufsichtsbehörden anderer Bundesländer haben mir das mehrfach bestätigt.

Praktisch bin ich jedoch in personeller Hinsicht auch weiterhin nicht zu solchen Kontrollaktionen in der Lage. Meine personellen Ressourcen sind vollständig durch die ständig im Umfang steigende Anlassaufsicht (vgl. Pkt. 4) gebunden. Im Berichtszeitraum habe ich daher erstmals keine einzige anlassfreie Kontrolle durchführen können:

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

Ohne zusätzliches Personal werde ich leider auch zukünftig nicht mehr im Bereich der Regelkontrollen tätig sein können.

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).

Anlasskontrollen der Aufsichtsbehörde setzen - wie die Bezeichnung schon sagt - Anhaltspunkte für eine Datenschutzverletzung voraus. Sie beschränken sich dabei nicht auf die Bearbeitung von Eingaben, sondern erstrecken sich darüber hinaus auch auf Sachverhalte, die mir durch Hinweisgeber, also Personen, die von einem Vorgang nicht selbst datenschutzrechtlich betroffen sind, oder eigene Ermittlungen bei anderen Stellen oder auch durch Presse- oder Internetveröffentlichungen bekanntgeworden sind. So habe ich im Berichtszeitraum - allerdings nur dank der Unterstützung zweier Praktikanten - meine bereits 2012 begonnenen Überprüfungen der Einhaltung der Kennzeichnungspflicht von Videoüberwachungen in Geschäften von Einkaufszentren fortsetzen können. Die Ergebnisse unterscheiden sich nicht wesentlich von denen aus dem Jahr 2012 (vgl. 6. TB, Pkt. 8.1.3), sodass in diesem Tätigkeitsbericht auf eine nochmalige Auseinandersetzung mit dieser Thematik verzichtet wird.

Im Berichtszeitraum bin ich in insgesamt 833 Fällen Anhaltspunkten für einen Datenschutzverstoß nachgegangen, 26 Fälle resultierten dabei noch aus dem letzten Berichtszeitraum. Hinsichtlich der neu bearbeiteten Sachverhalte (807 Fälle) ist damit gegenüber dem letzten Berichtszeitraum scheinbar ein Rückgang festzustellen, tatsächlich bewegt sich die Zahl aber in etwa auf einem vergleichbaren Niveau, denn der letzte Berichtszeitraum war wegen der Änderung in § 30 Abs. 1 Satz 1 SächsDSG bekanntlich um drei Monate länger als der übliche Zweijahreszeitraum. Auf Zweijahreszeiträume bezogen unterscheiden sich die Fallzahlen hingen nur gering: 6. TB: 803 neue Fälle; 7. TB: 807 neue Fälle.

Die zahlreichen telefonischen Anfragen, die ich auch sofort telefonisch beantworten konnte, habe ich anzahlmäßig nicht erfasst.

Im Regelfall führe ich Anlasskontrollen unverändert im schriftlichen Verfahren durch, daneben kontrolliere ich die verantwortlichen Stellen - insbesondere bei der Prüfung von Videoüberwachungsanlagen - in vielen Fällen aber auch vor Ort. So habe ich im Berichtszeitraum in 122 Fällen örtliche Überprüfungen bei insgesamt 98 verantwortlichen Stellen durchgeführt. Örtliche Überprüfungen sind immer - schon wegen des Reiseaufwandes

und der Bindung mindestens zweier Bediensteter - mit einem nicht unerheblichen Mehraufwand verbunden; dazu kommen solche Fälle, in denen meine Mitarbeiter auch außerhalb ihrer regulären Arbeitszeit tätig werden müssen, etwa bei unangekündigten Kontrollen in den frühen Morgenstunden (Kontrolle von mit GPS ausgerüsteten Firmenfahrzeugen vor deren täglichen Einsatz) oder den späten Abendstunden (Videoüberwachung eines Weihnachtsmarktes nach dessen Schließung), sodass ich wegen meiner bekanntlich äußerst begrenzten personellen Ressourcen nur noch eingeschränkt von dieser Kontrollform Gebrauch machen kann. Ich muss daher in Kauf nehmen, dass ich datenschutzrechtliche Sachverhalte aus diesem Grund nicht immer in dem Umfang aufklären kann, wie ich mir und wie sich das auch die Betroffenen wünschen, und dass dadurch auch die Zahl der Zufallsfunde, also zufällig entdeckter Datenschutzmängel, entsprechend sinkt.

Aus der nachfolgenden Tabelle ergeben sich weitere Einblicke in meine anlassbedingte Kontrolltätigkeit, auch in Bezug auf die Entwicklung gegenüber den Vorjahren:

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

* Vergleichswerte (Zweijahreszeitraum), rechnerisch ermittelt!

Am auffälligsten ist der hohe Anstieg der noch in Bearbeitung befindlichen Vorgänge auf das 3,5-fache des Wertes aus dem letzten Berichtszeitraum. Dieser Wert zeigt die hohe Arbeitsbelastung meiner Behörde und verdeutlicht, dass die mir zur Verfügung stehenden personellen Ressourcen inzwischen nicht einmal mehr ausreichen, um die Eingaben in einer für die Petenten akzeptablen Zeit abschließend zu bearbeiten.

Den absoluten Schwerpunkt meiner anlassbedingten Kontrolltätigkeit haben nun - man muss schon sagen erwartungsgemäß - Videoüberwachungsfälle übernommen, dicht gefolgt von Eingaben betreffend den Umgang mit personenbezogenen Daten im Internet, wobei hier Beschwerden über unerwünschte E-Mail-Werbung ca. 50 % der diesbezüglichen Aufsichtsvorgänge bildeten. Darüber hinaus sehr häufig haben mich Eingaben zur Nichtgewährung von Betroffenenrechten, insbesondere des Rechts auf Auskunft (§ 34 BDSG), sowie zur Thematik des Arbeitnehmerdatenschutzes erreicht.

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

1.	Videoüberwachung	146 Fälle
2.	Internet	127 Fälle
	davon Werbemails (Newsletter)	*61 Fälle*
3.	Rechte des Betroffenen	74 Fälle
4.	Beschäftigtendatenschutz	50 Fälle
5.	Personalausweisdaten	20 Fälle
	Datensicherheit	20 Fälle
6.	Wohnungswirtschaft	19 Fälle
	Datenschutzbeauftragter	19 Fälle
7.	Gesundheitswesen	18 Fälle
8.	Kreditwirtschaft	15 Fälle
9.	Betriebs- und Unternehmensänderungen	14 Fälle
10.	Parteien	13 Fälle
11.	Freie Träger im Sozialbereich	11 Fälle
	Rechtsanwälte	11 Fälle
12.	Versicherungswirtschaft	10 Fälle
	Energiewirtschaft	10 Fälle
13.	Werbung	9 Fälle
	Einzelhandel	9 Fälle
14.	Bildungswesen	7 Fälle
15.	Sport- und Freizeiteinrichtungen	6 Fälle
	Auskunfteien	6 Fälle
	Auftragsdatenverarbeitung	6 Fälle
16.	Dienstleistungssektor	5 Fälle

Bei etwa jeder dritten Kontrolle (ca. 29 %) habe ich im Ergebnis einen Verstoß gegen datenschutzrechtliche Vorschriften feststellen müssen. Damit ist ein leichter Rückgang gegenüber dem vorhergehenden Berichtszeitraum (ca. 36 %) zu verzeichnen. Die bereichsspezifische Auswertung zeigt dabei eine weitgehende Übereinstimmung mit der der durchgeführten Kontrollen:

1.	Umgang mit Daten im Internet	64 Verstöße	(50 %)
	davon Werbemails (Newsletter)	*44 Verstöße*	*(85 %)*
2.	Videoüberwachung	55 Verstöße	(38 %)
3.	Rechte des Betroffenen	22 Verstöße	(30 %)
4.	Betrieblicher Datenschutzbeauftragter	17 Verstöße	(90 %)
5.	Datensicherheit	14 Verstöße	(70 %)
6.	Beschäftigtendatenschutz	13 Verstöße	(26 %)
7.	Personalausweisdaten	12 Verstöße	(60 %)

Die bezüglich der betrieblichen Datenschutzbeauftragten festgestellten Verstöße betrafen fast ausnahmslos die Bestellungspflicht. Zumeist hatten sich Betroffene aber nicht deswegen an mich gewandt, vielmehr handelte es sich um Nebenerkenntnisse aus meiner diesbezüglichen Kontrolltätigkeit. Es verwundert sicher niemanden, dass Unternehmen, bei denen ich beispielsweise unzulässige Datenverarbeitungen feststellen oder die Gewährung von Betroffenenrechten anmahnen musste, in vielen Fällen auch keinen Datenschutzbeauftragten bestellt hatten.

Im Bereich der Videoüberwachung ist es nach wie vor ein Problem, dass für die Betroffenen der tatsächliche Erfassungsbereich der Videokameras nicht erkennbar ist und sie daher eine unzulässige Überwachung ihrer Person befürchten (müssen). Im Falle von Kameraattrappen mag der Überwachungsdruck auch so gewollt sein; in anderen Fällen habe ich feststellen können, dass durchaus wirksame Maßnahmen zur Begrenzung der Videoüberwachung, etwa in Form von Schwärzungen von Teilbereichen des Erfassungsbereiches der Kameras, getroffen worden waren. Bei beiden Fallgestaltungen hat also kein datenschutzrechtlicher Verstoß vorgelegen. Ich kann den Betroffenen dann nur mitteilen, dass kein datenschutzrechtlicher Verstoß vorgelegen hat (vgl. dazu auch 6. TB, Pkt. 8.1.8); den verantwortlichen Stellen kann ich allenfalls empfehlen, ihre Kameras bzw. ihre Kameraattrappen so auszuwählen bzw. so auszurichten, dass gar nicht erst der Eindruck einer unzulässigen Überwachung entsteht. Ich werde also damit leben müssen, dass auch die Bearbeitung von letztendlich unbegründeten Beschwerden zur Videoüberwachung einen wesentlichen Teil meiner Aufsichtstätigkeit bilden wird. Zumindest im Fall der Kameraattrappen hat es der Gesetzgeber aber in der Hand, dies entsprechend zu ändern und den Geltungsbereich des Bundesdatenschutzgesetzes entsprechend zu erweitern.

Der unzulässige Umgang mit Personalausweisen ist weiterhin ständiger Inhalt meiner Aufsichtstätigkeit. Immer wieder erhalte ich Hinweise darauf, dass unzulässiger Weise Personalausweiskopien angefertigt (vgl. Pkt. 8.2.8 und 8.9.5) oder Personalausweise als Pfandobjekt (vgl. Pkt. 8.5.6) einbehalten werden.

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 146 Fällen Beratungsanliegen an mich herangetragen worden. Im vorangegangenen Tätigkeitsbericht waren es noch 122 Beratungsfälle, dies allerdings - wegen der Änderung in § 30 Abs. 1 Satz 1 SächsDSG - bezogen auf einen um drei Monate längeren Berichtszeitraum. Dies entspricht einer absoluten Steigerung um 36 % bzw. bezogen auf einen Zweijahreszeitraum einer relativen Steigerung von sogar 41 %.

Die nachfolgende Übersicht verdeutlicht den stetigen Anstieg der Beratungsfälle in den letzten Jahren:

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

* Vergleichswert (Zweijahreszeitraum), rechnerisch ermittelt!

Der Schwerpunkt meiner Beratungstätigkeit lag im Berichtszeitraum wiederum in Fragen rund um die Bestellung, Fachkunde und Tätigkeit betrieblicher Datenschutzbeauftragter (25 Anfragen). Sehr oft um Beratung ersucht wurde aber auch zu Fragen der Videoüberwachung (22 Fälle), hier in erster Linie aus dem Bereich der Vermieter und Immobilienbesitzer, sowie zu Problemstellungen im Beschäftigtendatenschutz (12 Beratungsanliegen). In acht Fällen nutzten Vereine ihr Beratungsrecht; in ebenso vielen Fällen ließen sich Unternehmen zu Fragen der Auftragsdatenverarbeitung von mir beraten. Jeweils fünf

Anfragen kamen aus dem Bereich der Wohnungswirtschaft, des E-Commerce, des Gesundheitswesens sowie der freien Träger im Sozialbereich.

In 20 Fällen habe ich eine Beratung abgelehnt (vgl. dazu Pkt. 5.2.2 in meinem 5. TB).

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

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 allerdings 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:

- 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)

Die Texte der betreffenden Kommissionsentscheidungen und der dazugehörigen Standardvertragsklauseln sind in deutscher Sprache über die EU-Rechtsdatenbank *http://eur-lex.europa.eu* abrufbar. Dazu sind in das dort angebotene Suchformular das Jahr und die Dokumentennummer (oben in Klammern angegeben) einzutragen; als Dokumentenart ist „Beschluss/Entscheidung“ auszuwählen.

Bei einer Reihe von Staaten hat die Europäische Kommission bereits formell festgestellt, dass dort ein im Sinne des § 4b BDSG angemessenes Datenschutzniveau gegeben ist. Dazu gehören bislang (keine Veränderungen gegenüber dem vorhergehenden Berichtszeitraum) Andorra, Argentinien, die Färöer, Guernsey, Israel, die Isle of Man, die Vogtei Jersey, Kanada (mit Einschränkungen), Neuseeland, die Schweiz, Uruguay sowie die USA (Safe Harbor), vgl. dazu *http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm*. Bei einer Übermittlung in diese Länder bzw. an die den jeweiligen Regelungen unterfallenden Stellen (Kanada, USA) ist gleichfalls keine Genehmigung durch die Aufsichtsbehörde erforderlich.

8 Ausgewählte Sachverhalte

8.1 Videoüberwachung

8.1.1 Dashcams

Mit Dashcams habe ich mich schon in meinem 6. TB, dort gleichfalls unter Pkt. 8.1.1, auseinandergesetzt.

Inzwischen haben die Beschwerden zu diesem Thema deutlich zugenommen. Dashcams werden nicht nur von privaten Fahrzeugführern, sondern insbesondere auch gern von Bus- und Taxiunternehmen eingesetzt (s. dazu weiter unten!).

Der Düsseldorfer Kreis hatte sich zu dieser Problematik in Bezug auf Taxiunternehmen bereits in seinem Beschluss vom 26./27. Februar 2013 (vgl. 6. TB, Pkt. 13.7.1) geäußert und festgestellt, dass die Ausstattung von Taxis mit „Unfallkameras“ unzulässig ist. Ein weiterer Beschluss vom 25./26. Februar 2014 (vgl. Pkt. 14.4.2) greift diese Thematik - ohne Beschränkung auf Taxiunternehmen - nochmals auf und stellt klar, dass der Einsatz solcher Kameras datenschutzrechtlich generell - jedenfalls sofern dieser nicht ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt - unzulässig ist.

Inzwischen hat sich auch die Rechtsprechung schon mit Dashcams befasst:

Auch wenn der Bescheid des Bayerischen Landesamtes für Datenschutzaufsicht zur Untersagung des Einsatzes einer Dashcam vor dem VG Ansbach aus formalen Gründen keinen Bestand hatte, hat das Gericht doch festgestellt, dass der permanente Einsatz einer Dashcam zu dem vom Kläger verfolgten Zweck der Verwendung in verkehrsrechtlichen Streitigkeiten, insbesondere bei Unfällen, nach dem Bundesdatenschutzgesetz unzulässig ist. Mit einer Dashcam würden auch personenbezogene Daten verarbeitet, da es natürlich möglich sei, von der Kamera erfasste Personen zu identifizieren. Die vorzunehmende Abwägung zwischen den o. g. Interessen des Betreibers und den schutzwürdigen Interessen der Betroffenen, nicht ohne ihr Wissen von Dashcams beliebiger Fahrzeuge erfasst zu werden, falle gegen den Einsatz solcher On-Board-Kameras aus. Maßgeblich dafür sei, dass das Bundesdatenschutzgesetz heimliche Aufnahmen unbeteiligter Dritter grundsätzlich nicht zulasse und derartige Aufnahmen daher einen erheblichen Eingriff in das Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung der Betroffenen darstellen. Der verantwortlichen Stelle wurde aufgegeben, die bereits angefertigten Videoaufzeichnungen zu löschen (VG Ansbach, Urteil vom 12. August 2014, AN 4 K 13.01634, in: juris).

Das AG München (Beschluss vom 13. August 2014, 345 C 5551/14, in: juris) hat entschieden, dass mit Hilfe einer auf dem Armaturenbrett oder an der Windschutzscheibe

von Fahrzeugen angebrachten Dashcam angefertigte fortwährende Aufzeichnungen im Zivilprozess nicht als Beweismittel verwertet werden können. Die permanente, anlasslose Überwachung des Straßenverkehrs durch eine im Pkw installierte Autokamera verstoße gegen § 6b Abs. 1 Nr. 3 BDSG sowie gegen § 22 Satz 1 KunstUrhG und verletze den Beklagten in seinem Recht auf informationelle Selbstbestimmung als Ausfluss des allgemeinen Persönlichkeitsrechts nach Art. 2 Abs. 1 GG, Art. 1 Abs.1 GG. Mit Verweis auf eine Entscheidung des BVerfG (Beschluss vom 11. August 2009, 2 BvR 941/08, in: juris), wonach allein das allgemeine Interesse an einer funktionstüchtigen Straf- und Zivilrechtspflege nicht ausreiche, um im Rahmen der Abwägung stets von einem gleichen oder gar höheren Gewicht ausgehen zu können, als es dem Persönlichkeitsrecht zukomme, und daher weitere Aspekte hinzutreten müssten, die ergeben, dass das Interesse an der Beweiserhebung trotz der Persönlichkeitsbeeinträchtigung schutzwürdig ist, genügt dem AG München angesichts der im Straßenverkehr generell bestehenden Gefahr, in einen Unfall verwickelt zu werden, die bloße Möglichkeit, dass eine Beweisführung notwendig werden könnte, nicht zur Rechtfertigung der damit verbundenen Persönlichkeitsrechtsbeeinträchtigungen der übrigen Verkehrsteilnehmer.

Auch das LG Heilbronn (Urteil vom 3. Februar 2015, I 3 S 19/14, in: juris) hat in gleicher Weise entschieden, dass Aufzeichnungen einer in einem Pkw installierten Dashcam im Zivilprozess nicht als Beweismittel zum Hergang eines Unfalls verwertet werden können.

Vor diesem Hintergrund kann ich Fahrzeugbetreibern nur raten, auf den Einsatz von Dashcams zu verzichten: Eine Verwertung im Zivilrechtsverfahren ist ausgeschlossen; wegen der Erstellung der Aufzeichnungen droht zudem ein datenschutzrechtliches Bußgeldverfahren.

Auf zwei Kontrollfälle möchte ich noch gesondert eingehen:

1. Ein Busunternehmer hatte in seinen Fahrzeugen Dashcams installiert, die im Falle der Erschütterung des Fahrzeugs das Verkehrsgeschehen als Videosequenz mit Datum, Uhrzeit, Geschwindigkeit und Geolokation (GPS-Ortung) mit einer Laufzeit von fünfzehn Sekunden vor der Erschütterung und fünf Sekunden nach der Erschütterung auf einer SD-Karte dauerhaft aufzeichnen, wobei die Empfindlichkeit des die Speicherung auslösenden Erschütterungssensors in neun Stufen frei einstellbar war.

   Da das Gerät jedoch Erschütterungen als Auslöser der vorbezeichneten Speicherung nicht vorhersehen kann, wurden Bildsequenzen notwendiger Weise auch darüber hinaus - zumindest im Wege einer Zwischenspeicherung für 15 Sekunden - im datenschutzrechtlichen Sinne erhoben und verarbeitet; sie verfielen - im Wege einer automatisierten Löschung - lediglich ohne nachträgliches Ereignis (Erschütterung) nach

kurzer Zeit. Gleichwohl handelte es sich insoweit bereits um eine Erhebung und Verarbeitung personenbezogener Daten.

Fahrzeugerschütterungen, die im Wesentlichen allein auf die jeweilige Fahrbahnbeschaffenheit zurückzuführen sind, sind im Straßenverkehr keine zuverlässigen Indikatoren besonders unfallträchtiger Ereignisse, sondern typische Verkehrsparameter, die ständig wiederkehrend eintreten, ohne mit einer Unfallsituation im Zusammenhang zu stehen. Ausdruck der Unzuverlässigkeit der Zuordnung zu einem Unfallereignis ist gerade die frei wählbare Einstellung der Sensorempfindlichkeit, die nicht auf fundierten (objektiven) technischen oder wissenschaftlichen Erkenntnissen von Verkehrsgutachtern beruht, sondern es der subjektiven Einschätzung bzw. dem Belieben des Gerätebetreibers überlässt, präventiv viele oder wenige permanente Sequenzen dauerhaft zu speichern. Von einem bloßen „Unfalldatenschreiber“ konnte hier daher keine Rede sein. In Anbetracht einer Aufzeichnung, die gerade auf regelmäßigen, verkehrstypischen Ereignissen beruhte und deshalb auf eine anlasslose permanente bildliche Erhebung und Verarbeitung normalen Verkehrsgeschehens hinauslief, bin ich daher von einer Unvereinbarkeit dieser Videobeobachtungsanlage mit geltendem Recht ausgegangen. Letzteres auch deshalb, weil jeder vermeintlich ereignisbezogenen Speicherung eine anlasslose Erhebung und Verarbeitung vorausging, also gleichwohl eine Dauerüberwachung in Rede stand.

Der Betrieb dieser Dashcams hat wegen der damit verbundenen - anlasslosen - Aufenthalts- und Verhaltenskontrolle der Beschäftigten (GPS-Ortung, vgl. dazu auch Pkt. 8.3.4) auch gegen die Bestimmungen von § 32 Abs. 1 Satz 1 BDSG bzw. § 28 Abs. 1 Satz 1 Nr. 2 BDSG verstoßen.

Nachdem ich dem Unternehmer in Anbetracht dessen eine Untersagungsanordnung in Aussicht gestellt hatte, hat dieser die Speicherkarten aus den Geräten entfernt und die Nutzung vollständig eingestellt.

2. Eine öffentliche Personenfahndung der Polizei in einer Tageszeitung mit Fotos aus dem Innenraum sowie der unmittelbaren Umgebung eines Taxis hat mich zu einem Taxiunternehmer geführt, der - natürlich mit dem Hinweis, dass dies in der Branche absolut üblich sei - seine Fahrzeuge gleichfalls mit Dashcams ausgerüstet hatte. An den Beginn meiner Kontrolle stellte ich die Besichtigung eines Fahrzeugs verbunden mit der Bitte einer kurzen Probefahrt, der der Taxiunternehmer auch persönlich nachkam. Anschließend erfolgte eine Auswertung der Videoaufzeichnungen am PC, bei der sich ein ziemlich unerwartetes Ergebnis zeigte:

Es gab drei Arten von Aufzeichnungen, zwei davon waren anlassbezogen (automatische Auslösung über den G-Sensor (Schocksensor) bzw. manuelle Auslösung durch den Fahrer) und eine anlassfreie (Regel-)Aufzeichnung. Beim Betrachten einzelner Videosequenzen waren meine Mitarbeiter dann schon sehr überrascht, als sie feststellen mussten, dass die Aufzeichnungen nicht nur gestochen scharfe Außen- (gesamter Straßenraum einschließlich Gehwege) und Innenaufnahmen enthielten, sondern darüber hinaus auch noch Audiosequenzen aus dem Innenraum zu hören waren. Da meine Mitarbeiter (wie natürlich auch die Taxikunden) weder durch entsprechende Kennzeichnungen noch durch mündlich gegebene Informationen darauf hingewiesen worden waren, informierten sie unmittelbar darauf die Polizei, gaben den festgestellten Sachverhalt zu Protokoll und stellten als unmittelbar von der heimlichen Tonaufzeichnung Betroffene in eigenem Namen Strafantrag wegen Verletzung der Vertraulichkeit des Wortes (§ 201 Abs. 1 Nr. 1 StGB, vgl. auch Pkt. 12).

Bereits zu Beginn der Auswertung hatte der Unternehmer behauptet, dass den Fahrern der Kameraeinsatz freigestellt sei. Die Kameras könnten ganz einfach durch Kappen der Stromversorgung außer Betrieb genommen werden. Auf konkrete Nachfrage (im Hinblick auf die Einwilligungsproblematik im Arbeitsverhältnis) war er jedoch nicht bereit, konkrete Mitarbeiter zu benennen, die davon tatsächlich und folgenlos Gebrauch gemacht hätten. Stattdessen führte er im weiteren Gespräch aus, in solchen Fällen (Unfälle, keine Videos als Beweismittel) die Fahrer gegebenenfalls in Regress nehmen zu wollen. Von Freiwilligkeit konnte damit keine Rede mehr sein, zumal man den Fahrern ohnehin nur in Bezug auf die Erhebung ihrer eigenen Fahr-, Audio- und Videodaten, mithin nur bei Leerfahrten, überhaupt eine solche Entscheidungsbefugnis hätte einräumen können. Wenn es um die Erhebung der Daten von Fahrgästen oder anderen Verkehrsteilnehmern geht, kann es - abgesehen von der Bedienung eines Notfalltasters - nicht mehr dem Belieben eines angestellten Taxifahrers unterfallen, ob eine Videoaufzeichnung durchgeführt wird oder nicht.

Im Hinblick auf eine auch hier im Raum stehende Untersagungsanordnung habe ich dann unerwartete Hilfe von der Straßenverkehrsbehörde erhalten. Diese ist zugleich auch die Aufsichts- und Genehmigungsbehörde nach dem Personenbeförderungsgesetz für den gewerblichen Personenverkehr. Im Rahmen einer Routinekontrolle hatte auch die Straßenverkehrsbehörde den - unzulässigen - Einsatz der Dashcams festgestellt und nicht nur mich informiert, sondern den Fortbestand der Beförderungsgenehmigung von der Abgabe einer Erklärung des Unternehmers abhängig gemacht, dass ab sofort keine Dashcams in den Fahrzeugen des Taxiunternehmens mehr zum Einsatz kommen. Diese Erklärung hat der Unternehmer dann - wenn auch unter Protest - unterzeichnet und nachweislich auch seine Fahrer in diesem Sinne belehrt.

8.1.2 Wildkameras

Zur Videoüberwachung in der freien Natur, insbesondere in Wäldern (Wildkameras) sind bei mir bislang nur sehr wenige Anfragen eingegangen, konkrete Beschwerden noch keine. Dies mag daran liegen, dass Wildkameras äußerlich so gestaltet sind, dass sie sich sehr gut der Umgebung anpassen und praktisch nicht auffallen, d. h. nur bei genauer Kenntnis des Montageortes erkennbar sind. Kein Jäger oder sonstiger Betreiber möchte schließlich den Diebstahl oder die Zerstörung seiner Kamera riskieren. Bezeichnender Weise betrifft die einzige Beschwerde, bei der ich in der Vergangenheit den Einsatz einer Wildkamera festgestellt habe, den nachbarschaftlichen Bereich, d. h. den „zweckfremden" Einsatz im Wohnumfeld. Gleichwohl gehe ich davon aus, dass auch in Sachsen vielerorts Wildkameras betrieben werden. Derartige Kameras sind bereits seit Längerem in verschiedenen Ausführungen preiswert am Markt erhältlich und werden sogar schon von Lebensmitteldiscountern im Rahmen ihrer regelmäßigen Verkaufsaktionen angeboten.

Nach § 11 Abs. 1 SächsWaldG darf - unter Beachtung der Einschränkungen von § 11 Abs. 3 SächsWaldG - jeder den Wald zum Zwecke der Erholung betreten. Soweit ein solches Betretungsrecht besteht, handelt es sich um öffentlich zugängliche Räume im Sinne von § 6b BDSG. Nach § 6b Abs. 1 Nr. 3 BDSG ist eine Videoüberwachung zulässig, soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. (Werden Wildkameras durch sächsische öffentliche Stellen betrieben, gilt stattdessen § 33 SächsDSG - vgl. dazu Pkt. 12.1 meines 17. TB zum Schutz des Persönlichkeitsrechts im öffentlichen Bereich.)

Im Regelfall wird die somit vorzunehmende Interessenabwägung zugunsten der Waldbesucher (Wanderer, Spaziergänger, Pilzsucher, Geocacher etc.) ausfallen, der Betrieb von Wildkameras also unzulässig sein. Das Interesse der Waldbesucher, sich unbeobachtet in der freien Natur - nicht etwa nur auf Waldwegen - zu bewegen und zu erholen, überwiegt regelmäßig das Interesse der Jäger an der Effizienzsteigerung der Jagd durch den Einsatz von Wildkameras.

Etwas anderes kann ausnahmsweise an für Jäger besonders bedeutsamen und von Waldbesuchern im Regelfall kaum aufgesuchten Stellen gelten. Dies bedarf jeweils einer Bewertung im Einzelfall, wobei dann der Gewährleistung der in § 6b Abs. 2 BDSG geforderten Transparenz besondere Bedeutung zukommt. Der Betreiber muss die überwachten Bereiche entsprechend kennzeichnen und insbesondere die verantwortliche Stelle genau bezeichnen. Der Betrieb von Wildkameras muss dann zudem nach § 4d Abs. 1 BDSG bei mir gemeldet werden, es sei denn, der Betreiber hat einen Datenschutzbeauftragten bestellt (§ 4d Abs. 2 BDSG).

8.1.3 Kameradrohnen

Immer wieder erreichen mich auch Anfragen zum Einsatz von Kameradrohnen. Zum Schutz der Privatsphäre und des Grundrechts auf informationelle Selbstbestimmung gilt für sie - ungeachtet anderer, wie etwa luftverkehrsrechtlicher Vorgaben - Folgendes:

1. Gezielte Aufnahmen fremder Grundstücke, insbesondere geschützter Bereiche wie des Wohnungsinneren oder sonst allgemein den Blicken anderer verborgener Bereiche, z. B. des Gartens oder der Terrasse, sind immer eine verbotene Besitzstörung, der sich die Betroffenen zivilrechtlich erwehren können (§ 1004 BGB). Zudem sind Bildaufnahmen des höchstpersönlichen Lebensbereiches strafbar und werden von den Strafverfolgungsbehörden auf Antrag verfolgt (§§ 201a, 205 StGB). Ebenso strafbar ist, neben Bild- auch solche Audioaufnahmen zu tätigen, die nicht-öffentliche Gespräche aufzeichnen (§ 201 StGB).

2. Der EuGH hat am 11. Dezember 2014 (Rechtssache C-212/13) entschieden, dass jede Videobeobachtung, auch die mit einer Drohne, die nicht ausschließlich auf die private Sphäre (z. B. das Grundstück oder Familienangehörige) des Betreibers gerichtet ist, etwa, weil sie (auch) öffentlich zugängliche Bereiche erfasst, in den Anwendungsbereich der Europäischen Datenschutzrichtlinie und damit in den des Bundesdatenschutzgesetzes fällt; sie ist somit nur unter den dort geregelten Voraussetzungen zulässig und von mir aufsichtlich prüfbar (vgl. dazu auch Pkt. 8.1.4). Im Fall des rechtswidrigen Gebrauchs drohen Untersagungen und empfindliche Bußgelder bis zu 300.000 Euro (§§ 38 Abs. 5 Satz 1 und 43 Abs. 2 Nr. 1, Abs. 3 BDSG).

   In Anwendung von § 6b Abs. 1 Nr. 3 BDSG, der eine Abwägung mit den schutzwürdigen Interessen Betroffener gebietet, halte ich den nicht-gewerblichen Einsatz von Drohnen durch Privatpersonen in öffentlich-zugänglichen Bereichen, die keine besondere Persönlichkeitsrechtsrelevanz haben, jedenfalls für eigene spielerische oder dokumentarische Zwecke insoweit für zulässig, wie erkennbar ist, dass Dritte und deren Lebensumstände nicht Ziel der Beobachtung, sondern nur deren zufälliges „Beiwerk“ sind. Solange die Beobachtung vor Ort offen erfolgt und der Betreiber Betroffenen auf Verlangen bereitwillig Auskunft zu seiner Person und den Zwecken seines Tuns gibt, sehe ich zudem die Voraussetzungen von § 6b Abs. 2 BDSG als weitgehend erfüllt an. Eine Veröffentlichung der Filmsequenzen - beispielsweise im Internet - richtet sich nach den Bestimmungen des Kunsturheberrechtsgesetzes. Im Bereich des beruflichen und gewerblichen Einsatzes kann die Interessenabwägung indes weit enger ausfallen. Dies ist aber auch hier eine Frage des Einzelfalls.

8.1.4 Einfamilienhäuser

Die im vorangegangen Punkt bereits erwähnte Entscheidung des EuGH vom 11. Dezember 2014 (Rechtssache C-212/13) betraf im Ausgangspunkt den Fall eines tschechischen Bürgers, der am Haus seiner Familie eine Überwachungskamera angebracht hatte, die den Eingang des Hauses, den öffentlichen Straßenraum sowie den Eingang des gegenüberliegenden Hauses aufzeichnete. Mit Hilfe der Kamera war es ihm bzw. letztendlich der Polizei gelungen, zwei Verdächtige zu identifizieren, die eine Fensterscheibe seines Hauses mittels einer Schleuder beschossen und zerstört hatten.

Einer der Verdächtigen beanstandete dann jedoch zunächst erfolgreich beim tschechischen Amt für den Schutz personenbezogener Daten die Rechtmäßigkeit der Verarbeitung der von der Überwachungskamera aufgezeichneten Daten. Tatsächlich stellte das Amt dann auch fest, dass der Betrieb der Kamera gegen die tschechischen Datenschutzvorschriften verstoßen habe, und verhängte eine Geldbuße gegen den Betreiber. Die Daten des Verdächtigen habe er ohne dessen Einwilligung im öffentlichen Verkehrsraum aufgezeichnet.

Gegen diese Entscheidung ist dann wiederum der Kamerabetreiber vorgegangen. Das daraufhin mit dem Rechtsstreit weiter befasste Oberste Verwaltungsgericht der Tschechischen Republik hat dem Europäischen Gerichtshof in diesem Zusammenhang die Frage vorgelegt, ob eine Videoaufzeichnung von Personen im öffentlichen Straßenraum, die der Betreiber vorgenommen hatte, um sein Leben, seine Gesundheit und sein Eigentum zu schützen, eine Datenverarbeitung darstellt, die nicht von der Richtlinie erfasst wird, weil die Aufzeichnung von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wurde.

Dies hat der Europäische Gerichtshof verneint. Die Ausnahme, die in der Richtlinie für die Datenverarbeitung vorgesehen ist, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen wird, sei eng auszulegen. Eine Videoüberwachung, die sich auf den öffentlichen Raum erstreckt und dadurch auf einen Bereich außerhalb der privaten Sphäre desjenigen gerichtet ist, der die Daten verarbeitet, könne nicht als eine ausschließlich persönliche oder familiäre Tätigkeit angesehen werden. Die Europäische Datenschutzrichtlinie ist also auf die Videoaufzeichnung des öffentlichen Verkehrsraums mit an einem Einfamilienhaus angebrachten Überwachungskameras anwendbar.

Im konkreten Einzelfall des tschechischen Bürgers müssen nun die dortigen Gerichte weiter entscheiden, ob die Videoüberwachung des öffentlichen Verkehrsraumes nach geltendem Datenschutzrecht zulässig war oder nicht. Der Europäische Gerichtshof hat

nur die Frage der Anwendbarkeit des europäischen Datenschutzrechts und des darauf aufbauenden nationalen Datenschutzrechts beantwortet.

Die Entscheidung des Europäischen Gerichtshofs bindet in gleicher Weise auch andere nationale Gerichte und Aufsichtsbehörden, die mit einem ähnlichen Problem befasst werden.

Vor diesem Hintergrund kann ich meine im 4. TB, Pkt. 4.2.1.2 (3. Abs.), geäußerte Auffassung, dass dann, wenn Privatpersonen zu präventiven Zwecken ihr selbstgenutztes Wohneigentum, insbesondere ihren Hauseingang oder ihre Garageneinfahrt bzw. ihr Grundstück mit Videokameras überwachen und dabei auch angrenzende öffentlich zugängliche Bereiche (z. B. Gehweg, Straße) mit erfassen, dies ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt, womit hier der Anwendungsbereich (vgl. § 1 Abs. 2 Nr. 3 BDSG) des Bundesdatenschutzgesetzes insgesamt, auch des § 6b, nicht eröffnet ist, nicht länger aufrechterhalten.

Die Rechtmäßigkeit einer Videoüberwachung öffentlich zugänglicher Räume, die Private zum Schutz ihres Eigentums vornehmen, bestimmt sich demnach also nach § 6b BDSG.

Soweit als Zulässigkeitstatbestand § 6b Abs. 1 Nr. 2 BDSG herangezogen werden soll, ist zu berücksichtigen, dass die Befugnisse des Hausrechtsinhabers grundsätzlich an der Grundstücksgrenze enden und daher darüber hinaus keine Videoüberwachung rechtfertigen können.

Damit verbleibt nur noch § 6b Abs. 1 Nr. 3 BDSG, d. h. eine Abwägung der berechtigten Betreiberinteressen mit den einer Überwachung entgegenstehenden schutzwürdigen Interessen Betroffener (Fahrzeugführer, Passanten). Eine Ausdehnung der Videoüberwachung auf öffentliche Geh- oder Radwege oder auch Straßen wird dabei im Allgemeinen aber nur dann überhaupt in Betracht kommen, wenn diese Verkehrsbereiche unmittelbar an das zu schützende Gebäude angrenzen.

Eine Überwachung an das eigene Grundstück angrenzender öffentlicher Verkehrsbereiche wird dessen ungeachtet nur im absoluten Ausnahmefall, d. h. wenn schwerwiegenden Beeinträchtigungen der Rechte des Betreibers, etwa Angriffen auf seine Person oder seine unmittelbare Wohnsphäre, nicht in anderer Weise zumutbar begegnet werden könnte, als zulässig erachtet werden können. Nach der Rechtsprechung des Bundesgerichtshofs (Urteil vom 25. April 1995, VI ZR 272/94, in: 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 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. Die sich daraus ergebenden schutzwürdigen Interessen der Betroffenen überwiegen das Betreiberinteresse an einer präventiven Überwachung seines Eigentums einerseits sowie der Beweissicherung im Fall von Sachbeschädigungen und Diebstählen andererseits.

Zieht man das Urteil des AG Berlin-Mitte vom 18. Dezember 2003 (16 C 427/02, in: juris) hinzu, so kann sich eine Zulässigkeit allenfalls bezüglich eines schmalen Streifens entlang der Gebäudeaußenwand ergeben.

Auch das LG München hat in seinem Urteil vom 21. Oktober 2011 (20 O 19879/10, in: juris) festgestellt, dass die Herstellung von Abbildungen von Privatpersonen auf öffentlichen Straßen und Plätzen durch Videokameras grundsätzlich einen unzulässigen Eingriff in das allgemeine Persönlichkeitsrecht darstellt. Nur soweit aus technischen Gründen unvermeidbar ein Teil des öffentlichen Verkehrsraums miterfasst wird, kann im Einzelfall das allgemeine Persönlichkeitsrecht von zufällig miterfassten Passanten wegen des überwiegenden Interesses des Eigentümers am Schutz seines Eigentums zurücktreten. Dazu müssen zuvor aber mögliche Maßnahmen zur Beschränkung des Erfassungsbereiches, beispielsweise durch entsprechende Ausrichtung der Kameras und Schwärzung oder Verpixelung irrelevanter Bereiche, ausgeschöpft sein.

8.1.5 Sichtbarkeit von Überwachungskameras

Die Anfrage eines Lebensmitteldiscounters, ob - bei entsprechender Kennzeichnung - eine Videoüberwachung mittels versteckt angebrachter Videoüberwachungstechnik möglich und zulässig sei, habe ich wie folgt beantwortet:

Verkaufsbereiche von Lebensmitteldiscountern sind öffentlich zugängliche Räume, so dass für dort durchgeführte Videoüberwachungen die Vorschriften des § 6b BDSG zur Anwendung kommen. Absatz 2 dieser Vorschrift besagt dabei, dass der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen sind. Gesetzlich gefordert ist also nicht die Sichtbarkeit der eingesetzten Videokameras, sondern die Kennzeichnung der überwachten Bereiche. Dies wird regelmäßig durch entsprechende Hinweisschilder realisiert, die so angebracht sein müssen, dass sie vor Betreten des überwachten Discounters zur Kenntnis genommen werden können.

8.1.6 Offene Kontrollmonitore

In mit Videoüberwachungskameras ausgerüsteten Einzelhandelsgeschäften begegnet mir gelegentlich die Praxis, dass die Kamerabilder auf in den Verkaufsraum gerichteten Monitoren wiedergegeben werden, dies entweder dauerhaft oder auch als Wechselbilder verschiedener Kameras.

Der Betrieb von für jedermann sichtbaren Kontrollmonitoren in Einzelhandelsgeschäften ist unzulässig.

Mit dem Betrieb dieser Monitore werden personenbezogene Daten der Kunden und Mitarbeiter an andere (den Monitor betrachtende) Kunden übermittelt. Hierzu bedarf es eines Erlaubnistatbestandes im Bundesdatenschutzgesetz. § 6b Abs. 3 BDSG regelt diesbezüglich, dass die Verarbeitung oder Nutzung von mit Videokameras erhobenen Daten zulässig ist, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Die mir von den verantwortlichen Stellen genannten präventiven Zwecke können eine Erforderlichkeit einer solchen Datenübermittlung nicht begründen. Dazu sind die im Eingangsbereich anzubringenden Hinweise auf die Videoüberwachung vollkommen ausreichend. Es steht den verantwortlichen Stellen frei, diese so groß und auffällig zu gestalten sowie an solchen Stellen anzubringen, dass diese von ihren Kunden in keinem Fall übersehen werden können. Darüber hinaus geht auch von den zumeist offen angebrachten Videokameras eine entsprechend präventive Wirkung aus. Mithin fehlt es bezüglich des offenen Monitorbetriebes an der Erforderlichkeit zur Zweckerreichung, so dass der Betrieb der Monitore in dieser Form schon allein aus diesem Grund unzulässig ist.

Unabhängig davon stehen einer Bekanntgabe der Überwachungsbilder an die Kunden aber auch deren schutzwürdige Interessen entgegen. Diese (wie auch die im Geschäft tätigen Mitarbeiter) müssen es nicht hinnehmen, während ihres Aufenthalts im Verkaufsraum bzw. ihrer dortigen beruflichen Tätigkeit einer ständigen Beobachtung durch Dritte, zu denen kein direkter Sichtkontakt besteht, zu unterliegen. Letztendlich wird auf diese Weise eine Videoüberwachung der Kunden und Beschäftigten untereinander ermöglicht. Es steht außer Frage, dass dies schutzwürdige Interessen der Betroffenen verletzt.

In einer bundesweiten Arbeitsgruppe zu Fragen der Videoüberwachung haben sich die Vertreter der Aufsichtsbehörden in dieser Frage dahingehend abgestimmt, dass das Anbringen von allgemein sichtbaren Überwachungsmonitoren nur unter folgenden Voraussetzungen zulässig ist:

1. Der Monitor überträgt keine Wechselbilder.
2. Gezeigt wird nur der Bereich, welcher gerade durch den Kunden durchschritten wird. Andere Bereiche innerhalb des Geschäfts dürfen auf dem Monitor nicht zu sehen sein.
3. Es existieren zusätzliche Hinweisschilder.
4. Eine Aufzeichnung findet nicht statt.

8.1.7 Weihnachtsmärkte

Die für die Durchführung eines Weihnachtsmarktes zuständige städtische Gesellschaft hatte eine Sicherheitsfirma mit der Nachtbewachung des Weihnachtsmarktes beauftragt. Der Auftrag schloss den Einsatz von Überwachungskameras, insbesondere auch die Bildaufzeichnung ein. Den Hintergrund für den Kameraeinsatz bildeten - in den Nachtstunden erfolgte - Sachbeschädigungen und Diebstähle auf den Weihnachtsmärkten der vorangegangenen Jahre. Der Kamerabetrieb lag dabei in der alleinigen Verantwortung der Sicherheitsfirma.

Gegen eine solche, sich auf die Nachtstunden beschränkende und der Vermeidung bzw. Aufklärung von Diebstählen und Sachbeschädigungen dienende Videoüberwachung habe ich aus datenschutzrechtlicher Sicht keine grundsätzlichen Einwände. Sichergestellt werden muss dabei aber im Besonderen eine Information aller Standbetreiber über die Betriebszeiten der Videoüberwachungsanlage, da sich deren Mitarbeiter ggf. auch während der Schließzeiten des Marktes berechtigterweise auf dem Veranstaltungsgelände aufhalten können.

Keinesfalls zulässig gewesen wäre eine Videoüberwachung während des Marktbetriebes. Da die Verkaufsstände in dieser Zeit allesamt besetzt sind, ist mit Einbrüchen nicht zu rechnen, d. h. es fehlt insoweit schon am Vorliegen eines berechtigten Interesses (§ 6b Abs. 1 Nr. 3 BDSG). Davon unabhängig bestanden Anhaltspunkte für überwiegende schutzwürdige Betroffeneninteressen, denn Weihnachtsmärkte sind - ähnlich wie Gaststätten (vgl. 4. TB, Pkt. 4.2.1.9) - ein Paradebeispiel für öffentliche Räume, in denen Menschen zielgerichtet zur Erholung verweilen, ihre Bekanntschaften pflegen, ungezwungen miteinander kommunizieren und dazu gern auch ein oder mehrere Tassen Glühwein o. Ä. zu sich nehmen. An solchen Orten sind die einer Videoüberwachung entgegenstehenden Betroffeneninteressen besonders schutzwürdig. Die Marktbesucher haben ein schutzwürdiges Interesse daran, dass ihr - ggf. stimmungsgeladenes - Verhalten während ihres Aufenthalts auf dem Markt nicht permanent beobachtet, aufgezeichnet und nachfolgend für eine - für sie - unbestimmte Zeit vorgehalten wird, ohne dass sie die weitere Verwendung bzw. auch Löschung in irgendeiner Form kontrollieren oder beeinflussen können.

Der mir von einem Händler geschilderte Vorfall aktiver Monitore während des geöffneten Weihnachtsmarktes war leider im Detail nicht mehr aufklärbar. Die Sicherheitsfirma hatte mir glaubhaft versichert, dass deren Mitarbeiter jeweils zum Dienstende, d. h. in den frühen Morgenstunden, die Monitore ausgeschaltet und den Aufzeichnungsbetrieb eingestellt hatten. Die Tatsache, dass der Händler während des geöffneten Weihnachtsmarktes feststellen musste, dass die Monitore jedenfalls auch zu diesem Zeitpunkt eingeschaltet

gewesen waren, ließ sich damit nur so erklären, dass diese nicht gegen eine unbefugte Inbetriebnahme gesichert und daher durch Mitarbeiter entweder der dort gleichfalls tätigen Tontechnikfirma oder aber des Veranstalters unbefugt eingeschaltet worden waren.

Für den darauffolgenden Weihnachtsmarkt hat mir der Veranstalter u. a. zugesichert, dass in allen Verträgen mit Händlern, Schaustellern usw. auf die Videoüberwachung innerhalb der Nachtstunden hingewiesen wird und dass der Sicherheitsfirma wirksame Schutzmaßnahmen gegen die unbefugte Inbetriebnahme der Monitore in deren Abwesenheit, d. h. insbesondere während der Öffnungszeiten des Marktes, vorgeschrieben werden. Eine Videobeobachtung während der Öffnungszeiten des Weihnachtsmarktes sollte damit zukünftig ausgeschlossen sein.

8.1.8 Tierbeobachtung in Grünanlagen

Der Streifendienst eines städtischen Ordnungsamtes hatte auf einem Fensterbrett eines Wohnblocks eine Videokamera entdeckt und mich darüber unterrichtet. Die Kamera zeigte in Richtung einer naheliegenden Straßenkreuzung und überstreifte dabei die zwischen Wohngebäude und Straße liegende Grünanlage.

Der betreffende Mieter gab mir gegenüber an, die Kamera vorwiegend in den Nachtstunden für die Tierbeobachtung zu nutzen. Obwohl in der Stadt gelegen, fänden sich in der Grünanlage immer mal wieder Feldhasen, Igel und manchmal auch ein Fuchs ein. Dies sei spannender als manches Fernsehprogramm…

Ich habe den Betrieb dieser Videokamera als unzulässig bewertet; der betreffende Mieter hat die Kamera daraufhin unter deutlichem Protest - wer nichts zu verbergen habe, dem könne es doch egal sein, wenn er beobachtet werde - wieder abgebaut.

Die Rechtmäßigkeit einer Videoüberwachung öffentlich zugänglicher Bereiche durch Private bestimmt sich nach § 6b BDSG, wobei im Fall der Videoüberwachung in der Umgebung eines Wohngebäudes als Erlaubnistatbestand nur § 6b Abs. 1 Nr. 3 BDSG in Frage kommt: Zulässig ist eine Videoüberwachung nach dieser Vorschrift dann, wenn sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen (hier: Fahrzeuginsassen, Fußgänger, spielende Kinder, …) überwiegen. Diese Voraussetzungen waren im konkreten Fall nicht erfüllt. Es kann dahinstehen, ob man das Interesse, genau an dieser Stelle Tierbeobachtungen durchzuführen, als berechtigt ansehen kann, zumal - das zeigte die Protestäußerung des Betreibers - damit wohl nicht nur Tiere beobachtet worden waren. In jedem Fall standen einer Videobeobachtung - auf eine Aufzeichnung kommt es vorliegend nicht an, denn die genannte Vorschrift gilt bereits bei bloßer Beobachtung - aber schutzwürdige Interessen Betroffener entgegen, die sich im

öffentlichen Verkehrsraum und in allgemein zugänglichen Bereichen wie der Rasenfläche vor dem Fenster des Mieters unbeobachtet von anderen Personen bewegen wollen und sich dabei schon von der bloßen Existenz einer Videokamera infolge des davon ausgehenden Überwachungsdruckes in ihrem Persönlichkeitsrecht beeinträchtigt fühlen.

8.1.9 Reisezeitermittlung zur Verkehrssteuerung

Ich bin zu einem Kamerasystem angefragt worden, welches Reisezeiten auf konkreten Straßen-Streckenabschnitten anhand von detektierten Fahrzeugkennzeichen ermittelt. Das mir vorgelegte, auf einer automatischen Kfz-Kennzeichenerkennung basierende Lösungskonzept zeichne sich durch eine hohe Genauigkeit und Wiedererkennungsrate aus und garantiere damit die benötigte hohe Qualität der Reisezeitdaten. Es ging dabei nicht um einen dauerhaften, sondern lediglich um einen zeitlich begrenzten Einsatz, mit dem der tatsächliche Einfluss einer neuartigen Lichtsignalanlagensteuerung (LSA-Selbststeuerung) auf den Verkehrsfluss bewertet werden sollte.

Nach Prüfung der mir vorgelegten Unterlagen habe ich die mit der Durchführung des Projektes verbundene Erhebung und Verarbeitung personenbezogener Daten als nach § 6b Abs. 1 Nr. 3 BDSG zulässig bewertet. Anhaltspunkte für das Überwiegen schutzwürdiger Interessen Betroffener bestanden wegen der sofortigen, noch in der Kamera erfolgenden Anonymisierung (keine Rückverfolgbarkeit) der erfassten Kennzeichendaten nicht.

Ich habe allerdings darauf hingewiesen, dass nach § 6b Abs. 2 BDSG der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen (Hinweisschilder) erkennbar zu machen sind. Zur Minderung der in diesem Zusammenhang zu erwartenden Anfragen aus der Bevölkerung habe ich zudem empfohlen, das Projekt kurz vor dem Start in der lokalen Presse vorzustellen.

8.1.10 Kraftsportraum

Von einem Vereinsmitglied erhielt ich den Hinweis auf eine im Trainingsraum der Abteilungen Kraftsport und Fitness installierte Videokamera. Anlass für die Videoüberwachung sei ein drei Jahre zurückliegender Fall nächtlichen Vandalismus gewesen.

Der Verein führte dazu aus, dass die Sportfreunde der Abteilung Kraftsport selbstständig trainieren dürften und teilweise einen eigenen Schlüssel hätten bzw. diesen auch untereinander weitergeben würden. Es sei daher schwierig bis unmöglich, einzelnen Mitgliedern oder gar Dritten Diebstahlhandlungen, Sachbeschädigungen oder die Verursachung allgemeiner Unordnung zuzuordnen und nachzuweisen.

Die Rechtmäßigkeit der Videoüberwachung in Vereinsräumlichkeiten bestimmt sich nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG: Zulässig ist eine Videoüberwachung nach dieser Vorschrift, soweit sie zur Wahrung berechtigter Interessen des Vereins erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der dort trainierenden Vereinsmitglieder am Ausschluss der Überwachung überwiegt.

Eine Videoüberwachung ist nur dann erforderlich, wenn sie geeignet ist, den angestrebten Zweck zu erreichen und es keine milderen Mittel gibt, mit denen der Zweck gleichfalls erreicht werden kann. Außerdem muss die Überwachungsmaßnahme auch verhältnismäßig sein. Diese Voraussetzungen waren vorliegend nicht erfüllt - schon aus diesem Grund ist der Betrieb der Videokamera damit unzulässig gewesen. Zwar bestehen keine Einwände hinsichtlich der Eignung der Videoüberwachung für das Erreichen der vom Vereinsvorstand angegebenen Zwecke, jedoch sind eine Reihe milderer, d. h. deutlich weniger in die Persönlichkeitsrechte der Mitglieder eingreifende Mittel realisierbar, mit denen die verfolgten Ziele gleichfalls bzw. sogar noch besser erreicht werden können. Dazu zähle ich beispielsweise die Einführung fester Trainingszeiten mit entsprechenden Aufsichtspersonen (diese können natürlich auch selbst trainieren) und eine restriktivere Schlüsselvergabe einschließlich einer entsprechenden Dokumentation (Schlüsselbuch) für die übrigen Zeiten. Unabhängig davon sollte der Verein in diesem Zusammenhang ohnehin prüfen, ob ihm als Betreiber des Kraftsportraumes nicht sogar ständige Aufsichtspflichten (vgl. OLG Hamm, NJW-RR 1992, 243 f.) obliegen, er also für den Fall von Verletzungen zur Verfügung stehen muss und in der Pflicht ist, die Fitnessgeräte und Räumlichkeiten so in Ordnung und gefahrlos zu halten sowie ständig zu kontrollieren, dass die Nutzer keine Gefährdung und Verletzung ihrer Gesundheit und ihres Lebens erleiden (vgl. OLG Stuttgart, NJW-RR 1988, 1082 f.).

Des Weiteren stehen einer Videoüberwachung aber auch und vor allem schutzwürdige Interessen der Betroffenen entgegen. Da es sich bei einem Trainingsraum um eine Freizeiteinrichtung handelt, sind diese Betroffeneninteressen besonders schutzwürdig. Die trainierenden Sportler geben sich hier wesentlich lockerer und unkonventioneller, als das etwa bei beruflichen Tätigkeiten oder privaten Besorgungen der Fall ist, und vertrauen dabei auf die besondere Privatheit des speziell für sportliche Belange und eine längere Verweildauer konzipierten Umfeldes. Die Vereinsmitglieder haben ein schutzwürdiges Interesse daran, dass ihre sportlichen, die individuelle Leistungsfähigkeit (positiv oder negativ) widerspiegelnden Aktivitäten und der dabei deutlich hervortretende Fitnesszustand ihres Körpers während ihres Aufenthalts im Kraftsportraum nicht permanent beobachtet, aufgezeichnet und nachfolgend für eine - für sie - unbestimmte Zeit vorgehalten wird, ohne dass sie die weitere Verwendung bzw. auch Löschung in irgendeiner Form kontrollieren oder beeinflussen können.

Der Verein ist meiner Forderung nach Einstellung der Videoüberwachung nachgekommen und hat die Kamera deinstalliert. Auf den im gleichen Kontext erfolgten Aushang von Mitgliederdaten gehe ich im Pkt. 8.7.4 näher ein.

8.1.11 Sportschwimmhalle

In einer neu eröffneten Sportschwimmhalle hatte der Betreiber, eine städtische Gesellschaft, Videoüberwachungstechnik installiert. Auf den im Internet veröffentlichten Fotos von der Eröffnungsfeier waren dabei auch zwei Kameras im Bereich des Schwimmbeckens erkennbar.

Auf meine schriftliche Anfrage hin ist mir mitgeteilt worden, dass es sich um keine öffentliche Schwimmhalle handele, vielmehr stehe die Sportschwimmhalle nur Vereinen, Schulträgern oder anderen vergleichbaren Nutzern nach vorheriger Vereinbarung zur Verfügung. Es sei regelmäßig kein Personal der Betreibergesellschaft vor Ort; die Einhaltung der Ordnung und Sicherheit im Objekt obliege dem jeweiligen Nutzer. Die u. a. zur Überwachung des Schwimmbeckens bestimmten Kameras dienten dem Zweck, dass der jeweilige Nutzer die Erfüllung der ihm obliegenden Verkehrssicherungspflicht erforderlichenfalls dokumentieren kann, falls er von den von ihm betreuten Schwimmerinnen und Schwimmer in dieser Hinsicht in Anspruch genommen werden sollte. Im Übrigen ginge es um die Vermeidung und Aufklärung von Hausrechtsverstößen und Vandalismusvorfällen.

Zunächst war zu klären, auf welcher gesetzlichen Grundlage die datenschutzrechtliche Prüfung vorzunehmen war. Ich bin insoweit davon ausgegangen, dass es sich - jedenfalls was die angegebenen Nutzungen betraf - um keinen öffentlich zugänglichen Raum im Sinne des § 6b BDSG handelt. Dies wird allerdings regelmäßig dann anders zu bewerten sein, wenn in der Halle auch Sportwettkämpfe mit Zuschauern durchgeführt werden. Letztendlich kommt es darauf aber auch nicht entscheidend an, denn auch nach der (in nicht öffentlich zugänglichen Räumen) alternativ zu § 6b BDSG anwendbaren Vorschrift des § 28 BDSG muss die Videoüberwachung zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich sein und es darf kein Grund zu der Annahme bestehen, dass das schutzwürdige Interesse der Betroffenen am Ausschluss der Überwachung überwiegt (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG).

Der angegebene Fremdzweck, die Nutzer der Sportschwimmhalle könnten mit Hilfe der Kameras ggf. beweisen, dass sie ihren Verpflichtungen gegenüber dem in eigener Verantwortung betreuten Personenkreis ausreichend nachgekommen sind, konnte eine Videoüberwachung nicht rechtfertigen. Nach dem Wortlaut des § 28 Abs. 1 Satz 1 Nr. 2

BDSG sind hierfür nur berechtigte Interessen der verantwortlichen Stelle selbst heranzuziehen. Unabhängig davon konnte ich mir auch nicht vorstellen, dass eine mit dieser Zielrichtung erfolgende Videoüberwachung von den Nutzern tatsächlich gewünscht sein könnte, da sie ja selbst keine Verfügungsgewalt über die Videoaufzeichnungen gehabt hätten.

Als berechtigter Zweck der Betreibergesellschaft verblieb damit lediglich die Aufklärung von Vandalismusvorfällen. Hierzu war eine Videoüberwachung aber nicht erforderlich, denn dem Betreiber sind die Nutzer der Halle, deren Nutzungszeiten und die dort für die Einhaltung von Sicherheit und Ordnung verantwortlichen Personen regelmäßig bekannt, so dass eventuelle Vorkommnisse, insbesondere Sachbeschädigungen auch auf andere Art und Weise aufgeklärt bzw. konkreten Nutzern zugeordnet werden können, zumal sich zumindest „sporadisch“ auch immer wieder ein Techniker der Betreibergesellschaft in der Schwimmhalle aufhielt und der Betreiber im Rahmen seiner eigenen Verkehrssicherungspflichten ohnehin regelmäßige Kontrollgänge durch die Anlage durchführen muss. Abgesehen davon ist ein diesbezügliches Überwachungsinteresse nur dann als berechtigt anzusehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Es müssen konkrete Tatsachen vorliegen, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen oder besondere Vorkommnisse in der Vergangenheit. Dies konnte vorliegend schon deshalb nicht der Fall sein, weil die Halle gerade eben erst neu eröffnet worden war. In bestimmten Fällen kann zwar auch eine abstrakte Gefährdungslage ausreichend sein, etwa wenn eine Situation vorliegt, die nach der Lebenserfahrung typischerweise gefährlich ist, so in Geschäften, in denen wertvolle Waren verkauft werden (z. B. Juweliere) oder die im Hinblick auf Vermögens- und Eigentumsdelikte potentiell besonders gefährdet sind (z. B. Tankstellen). Bei einer Sportschwimmhalle, die nur einem begrenzten, festgelegten und damit bekannten Nutzerkreis zur Verfügung steht, liegt eine solche abstrakte Gefährdungslage aber sicherlich nicht vor.

Die Videoüberwachung der Sportschwimmhalle war damit schon mangels Erforderlichkeit unzulässig.

Unabhängig davon standen einer Videoüberwachung aber auch überwiegende schutzwürdige Betroffeneninteressen entgegen. Es verstößt gegen die Persönlichkeitsrechte der Nutzer der Schwimmhalle, wenn sie während ihres ausbildungsmäßig (Schüler) oder berufsmäßig (Lehrer) bedingten Aufenthaltes oder während der ihrer Freizeitgestaltung (Vereine) zuzurechnenden sportlichen Betätigung in der Schwimmhalle - lediglich mit Badesachen bekleidet - permanent der Kontrolle durch einen Dritten unterliegen und dabei jede ihrer Bewegungen mittels entsprechender Aufzeichnungen dokumentiert und somit innerhalb der Speicherfristen nachvollziehbar wird, ohne dass sie darauf Einfluss ausüben, und sich insbesondere dieser Überwachung auch nicht entziehen können, weil

sie eben zum Schulbesuch bzw. ihrem Arbeitgeber gegenüber verpflichtet sind bzw. sonst keine alternative Möglichkeit haben, ihren sportlichen Aktivitäten nachzugehen.

In der Konsequenz der somit unzulässigen Videoüberwachung, insbesondere wegen des auch von inaktiven Kameras ausgehenden Überwachungsdrucks, waren die Kameras in der eigentlichen Schwimmhalle und in der Garderobe mangels gesetzeskonformer Nutzungsmöglichkeit wieder zu demontieren. Der Betrieb der auf die Eingangstür gerichteten Kameras könnte ggf. zulässig sein, wenn hierfür noch eine entsprechende Gefährdungslage nachgewiesen wird.

8.1.12 Liftanlagen in Wintersportgebieten

In Österreich schon länger praktiziert wird nun zunehmend auch in Deutschland, nicht zuletzt auch in Sachsen, der Kontrolldruck auf Skipassbetrüger erhöht. Dem Vernehmen nach entstehen den Liftbetreibern in jeder Saison erhebliche (bis 10 % der Einnahmen) Verluste, indem die regelmäßig nicht übertragbaren Skipässe durch mehrere Personen gemeinsam genutzt oder weiterverkauft werden. Natürlich ist ein 6-Tages-Skipass billiger als zwei 3-Tages-Skipässe und wenn man mit Kleinkindern unterwegs ist und immer nur ein Elternteil Skifahren kann, dann ist ein einziger, länger gültiger Skipass eben deutlich preiswerter. Auch wenn man - aus welchen Gründen auch immer - das Skifahren etwas eher beenden muss, freut man sich, wenn man wenigstens einen Teilbetrag der doch recht hohen Kosten durch einen Weiterverkauf wieder einspielen kann. Pech nur, dass die AGB einen Weiterverkauf oder eine Übertragung auf eine andere Person regelmäßig ausschließen. Nur leider liest sich die AGB im Allgemeinen niemand durch, sodass es vielen Skifahrern nicht bewusst ist, dass Skipässe nicht übertragbar sind. Erst wenn der Skipass nicht mehr funktioniert und man sich um Klärung bzw. Ersatz bemüht, wird dann das Problem bekannt und im Fall des unerlaubten Weiterverkaufs trifft es dann auch noch den gutgläubigen Käufer…

Passiert ein Skifahrer das erste Mal an einem Tag das Drehkreuz eines Skiliftes, schießt die Kamera ein Kopffoto. Das Foto wird mit der gleichzeitig ausgelesenen Skipassnummer verknüpft und für die Geltungsdauer des Skipasses gespeichert. Bei jeder weiteren Nutzung eines Skiliftes (mit Zugangskontrolle) wird ein neues Foto erstellt und kann dann zum manuellen Vergleich - die personalintensiven Kontrollen können natürlich nur stichprobenhaft erfolgen - auf dem Kontrollbildschirm dem zuerst erstellten Foto gegenübergestellt werden. Wird auf diese Weise ein offensichtlicher - wegen der markanten Kleidungen und Helme oft schnell erkennbarer - Missbrauch, d. h. ein Nutzerwechsel, festgestellt, kann der betreffende Skifahrer entweder sofort angesprochen oder aber dessen Skipass für die weitere Nutzung gesperrt werden.

Ich habe die Fotokontrollen auf der Grundlage von § 6b Abs. 1 Nr. 3, Abs. 3 BDSG als zulässig bewertet. Der Begriff der Beobachtung erfasst auch die digitale Fotografie, sofern eine gewisse zeitliche Dauer zugrunde liegt (vgl. Pkt. 2.1.1 der Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ des Düsseldorfer Kreises = Pkt. 14.3.1 dieses TB). Die Fotokontrollen sind in den AGB der Liftbetreiber entsprechend benannt, damit Vertragsbestandteil und angesichts der hohen Missbrauchszahlen auch erforderlich. Die Fotos werden nur für die Gültigkeitsdauer des Skipasses gespeichert und anschließend sofort gelöscht (§ 6b Abs. 5 BDSG).

Wesentliche datenschutzrechtliche Anforderungen an die Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind das Direkterhebungsprinzip und die Transparenz. § 4 Abs. 2 BDSG gibt insoweit vor, dass personenbezogene Daten (hier: Fotoaufnahmen) - von Ausnahmen abgesehen - direkt beim Betroffenen und mit seiner Kenntnis erhoben werden müssen. Darüber hinaus treffen die verantwortliche Stelle nach § 4 Abs. 3 Satz 1 BDSG eine Reihe von Unterrichtungspflichten, insbesondere auch hinsichtlich der Zweckbestimmung.

Die ein Skigebiet nutzenden Wintersportler sind also ausreichend deutlich über die Anfertigung von Fotoaufnahmen zum Zweck der Missbrauchskontrolle bezüglich der Skipässe zu unterrichten. Angesichts des unzweifelhaft stark präventiven Charakters einer solchen Unterrichtung sollten entsprechende Informationen auch im Interesse der Liftbetreiber liegen. Ein kurzer Hinweis „Fotokontrolle möglich“ in den Beförderungsbedingungen mag formal zwar möglicherweise ausreichend sein, wird dem präventiven Anliegen tatsächlich aber wohl kaum gerecht. Insoweit besonders geeignet erscheinen mir zusätzliche, diese Thematik aufgreifende Ausführungen zum Kartenmissbrauch in den üblicherweise eingesetzten Flyern des jeweiligen Skigebietes sowie deutlich wahrnehmbare, mithin also großformatige, Hinweise zur Nichtübertragbarkeit der Skipässe und der diesbezüglichen Fotokontrollen an den Skipass-Verkaufsstellen und auch den Liftanlagen.

8.1.13 Straßenbahnen und Busse außerhalb des Fahrgastbetriebs

Im Berichtszeitraum erlangte ich Kenntnis davon, dass ein Verkehrsunternehmen in seinen Straßenbahnen und Bussen auch außerhalb des Fahrgasteinsatzes, also bei Reinigungs- und Wartungsarbeiten sowie bei Überführungs-, Werkstatt-, Probe- und Fahrschulfahrten, permanent Videoaufzeichnungen tätigte und so personenbezogene Daten des Reinigungs-, Betriebs- und Wartungspersonals erhoben wurden, was weder datenschutzrechtlich erforderlich, noch in Anbetracht der Rechtsprechung des Bundesarbeitsgerichts zur Beschäftigtenüberwachung zulässig war.

Einziger und insoweit keinesfalls zulässiger Grund für die Videografie war, dass die eigentlich für den Fahrgasteinsatz konzipierte und auch allein damit begründbare Überwachung automatisch mit der Betriebsfähigkeit der Fahrzeuge einsetzte und manuell, etwa durch einen Werkstattschalter, nicht ausgeschaltet werden konnte, so dass außerhalb des Fahrgasteinsatzes ebenso eine Aufzeichnung stattfand.

Anders als vom Unternehmen zunächst vorgetragen, kann ein im Sinne von § 32 Abs. 1 Satz 1 oder § 28 Abs. 1 Satz 1 Nr. 2 BDSG legitimes Beobachtungserfordernis und damit eine Rechtfertigung des Eingriffs in das Grundrecht auf informationelle Selbstbestimmung der betroffenen Beschäftigten aber nicht einfach aus der von dem Unternehmen verantworteten technischen Beschaffenheit der Anlage hergeleitet werden. Es widerspricht dem Begriff des datenschutzrechtlichen Erfordernisses grundlegend, wenn die Notwendigkeit einer Datenverarbeitung allein dem Umstand geschuldet ist, dass die verantwortliche Stelle eine technische Anlage angeschafft hat, die sich nicht anders betreiben lässt, obwohl der Grundrechtseingriff bei einer anderen (unternehmerischen) Entscheidung - etwa für eine andere Anlage mit entsprechenden Möglichkeiten - problemlos hätte vermieden werden können.

Maßnahmen des Unternehmens, die eine Nutzung der Daten entgegen der Interessen der Beschäftigten ausschließen sollen, führen dabei zu keiner anderen rechtlichen Bewertung, denn nach der Systematik des Bundesdatenschutzgesetzes ist schon die Erhebung und nicht erst die Zweckänderung bzw. eine bestimmte Nutzung verboten (§ 4 Abs. 1 BDSG).

Das Unternehmen war jedoch bereit, bis zu einer Umrüstung bzw. der Nachrüstung einer Werkstattschaltung einstweilen im Werkstatt-, Überführungs- und Fahrschulbetrieb Kameraabdeckungen zu verwenden, so dass für mich kein Anlass zu weiterer Aufsicht, insbesondere zu einer hierauf gerichteten Anordnung bestand.

8.1.14 Digitale Türspione

Herkömmliche Türspione können ohne bauliche Veränderungen durch digitale Türspione ersetzt werden. Von außen sind digitale Türspione nicht ohne weiteres erkennbar, d. h. Betroffene können kaum zwischen einem normalen und einem digitalen Türspion unterscheiden. Digitale Türspione können manuell von innen oder von außen über den Klingelknopf aktiviert werden, es ist aber auch möglich, die Videoüberwachung mit Bewegungssensoren zu koppeln. Datenschutzrechtlich besonders problematisch ist die Möglichkeit der Aufzeichnung.

Wegen des bestehenden externen Bezuges der Videoüberwachung

- Anfertigung von Beweismitteln zur externen Verwendung,
- Erfassung von Bereichen, die über die eigene Wohnung hinausgehen, und
- Erfassung von Personen, die nicht dem familiären Umfeld zuzurechnen sind,

liegt keine persönlich-familiäre Tätigkeit vor (§ 1 Abs. 2 Nr. 3 BDSG).

Ob es sich um eine Überwachung öffentlich zugänglicher Räume handelt, bedarf einer Einzelfallbetrachtung. Ist dies der Fall hat die datenschutzrechtliche Bewertung nach § 6b BDSG zu erfolgen, andernfalls nach § 28 BDSG.

Die Zulässigkeit des Betriebs eines digitalen Türspions ist damit in jedem Fall im Rahmen einer Interessenabwägung zu prüfen. Auf das Hausrecht (§ 6b Abs. 1 Nr. 2 BDSG) kann man sich in diesem Fall allerdings nicht beziehen, denn dies endet vorliegend an der Wohnungstür. Ein Wohnungsbesitzer hat die Mitbenutzung des Hausflurs durch andere Mieter und deren Besucher hinzunehmen.

Ein berechtigtes Interesse (§ 6b Abs. 1 Nr. 3 BDSG) könnte bei Kindern, gehbehinderten und älteren Personen bestehen - alle anderen können grundsätzlich auch durch einen herkömmlichen Türspion schauen. Hinsichtlich der schutzwürdigen Interessen der Betroffenen ist deren Anspruch zu beachten, jedenfalls von einer anlasslosen Überwachung verschont zu bleiben, zumal der Zugang zur Wohnung schon den Kernbereich privater Lebensführung tangiert. Durch die einfache Bedienung ist zudem eine geringe Hemmschwelle vorhanden, digitale Türspione offensiv bis hin zum Dauerbetrieb (anlassfreie Dauerbeobachtung) zu nutzen.

Digitale Türspione können daher im Regelfall nicht nach §§ 6b, 28 BDSG zulässigerweise betrieben werden.

Das AG München hatte Ende 2013 einen ähnlichen Fall zu bewerten und im Urteil vom 4. Dezember 2013 (Az.: 413 C 26749/13) schließlich entschieden, dass die Überwachung des Hausflurs mit einem digitalen Türspion das allgemeine Persönlichkeitsrecht von Mitmietern und deren Besuchern verletzt. Das allgemeine Persönlichkeitsrecht gemäß Art. 2 Abs. 1 GG umfasse auch die Freiheit vor unerwünschter Kontrolle oder Überwachung durch Dritte, insbesondere in der Privat- und Intimsphäre im häuslichen und privaten Bereich. Dies beinhalte für die Mitmieter nicht nur die Freiheit, jederzeit die Wohnung zu verlassen oder zu betreten, ohne dass ein Mitmieter dies stets überwacht und jederzeit feststellen könne. Es beinhalte darüber hinaus auch das Recht, ungestört und nicht überwacht Besuch empfangen zu können.

8.1.15 Videoprojektion in einer Fußgängerzone

Viel Medienwirbel hatten gehäufte Anzeigen von Falschparkern in einer Fußgängerzone - wohl in erster Linie Lieferfahrzeuge und dort tätige Handwerker betreffend - erzeugt. Anwohner sollten dort seit einiger Zeit Falschparker filmen und die Daten dann an das Ordnungsamt weitergeben. Prompt wurden auch videokameraähnliche Geräte an einem Balkon einer Wohnung entdeckt und eine illegale Videoüberwachung vermutet. Ich habe mich dieser Angelegenheit angenommen und festgestellt, dass es sich bei den vermeintlichen Videokameras auf dem Balkon nicht um Aufnahmetechnik, sondern stattdessen um Videoprojektionstechnik gehandelt hat. In den Abendstunden wurden mit dieser Technik - nicht personenbezogene - Werbebotschaften auf den Gehweg projiziert, um das nahegelegene Stadtviertel bekannter zu machen. Die dem Ordnungsamt im Rahmen der Anzeigen zugeleiteten Beweisfotos waren stattdessen von einer anderen Person mit einer Digitalkamera erstellt worden.

8.2 Internet

8.2.1 Löschung von Kundenaccounts

Mitunter - meist aus negativen Erfahrungen heraus - entscheiden sich Kunden dazu, nie wieder bei einem konkreten Online-Händler etwas zu erwerben. Sie sind daher an einer nachhaltigen Beendigung der bis dahin bestehenden Geschäftsbeziehung interessiert und verlangen dann die vollständige Löschung aller zu ihrer Person gespeicherten Daten, vor allem aber auch des eingerichteten Kundenaccounts. Da dies regelmäßig nicht vollumfänglich gelingt bzw. auch nicht gelingen kann, wenden sie sich anschließend an mich.

Nach den einschlägigen steuer- und handelsrechtlichen Vorschriften (§ 257 HGB, § 147 AO) ist es allein geboten, neben den Daten bisheriger Rechtsgeschäfte nur solche Daten zur Person des Kunden (in gesperrter Form) zu speichern, die seine (eindeutige) Identifizierung (mit dem Rechtsgeschäft) ermöglichen. Alle anderen Daten zur Person des Kunden sind nach Ende der Geschäftsbeziehung zu löschen, § 35 Abs. 2 Satz 2 Nr. 3, Abs. 3 Nr. 1 BDSG.

Auf die Beseitigung eines Kundenaccounts bezogene Löschungsforderungen sind also berechtigt. Nach den steuer- und handelsrechtlichen Vorschriften sind verantwortliche Stellen zwar verpflichtet, die Daten von Rechtsgeschäften weiter (in der Buchhaltung) zu speichern, jedoch erfordert dies keine dauerhafte Unterhaltung eines Kundenkontos und schon gar nicht die dauerhafte Bereitstellung einer darauf bezogenen Zugriffsmöglichkeit über das Internet. Wenn also ein Kunde keine dauerhafte Einrichtung eines Kundenkontos wünscht bzw. die Löschung eines eingerichteten Kundenkontos fordert, so ist diesem Wunsch zu entsprechen, d. h. die Zugangsdaten des Kunden sind zu löschen. Dies gilt

auch für dort ggf. noch vorhandene Buchungsdaten, denn diese haben längst auch Eingang in die Buchhaltung gefunden und sind (nur) dort bis zum Ablauf der steuer- und handelsrechtlichen Aufbewahrungsfristen weiter zu speichern.

Nach den oben erwähnten Vorgaben des Handels- und Steuerrechts sind Unternehmen im Übrigen aber verpflichtet, kaufmännische Unterlagen bzw. Daten sechs bzw. zehn Jahre aufzubewahren. In diesen Fällen tritt an die Stelle der sonst nach § 35 Abs. 2 Satz 2 Nr. 3 BDSG gebotenen Löschung eine Sperrung (§ 35 Abs. 3 Nr. 1 BDSG). Mit der Sperrung verbunden ist ein relatives Nutzungsverbot der gespeicherten Daten. Bis auf wenige, in § 35 Abs. 8 BDSG festgelegte Ausnahmen dürfen gesperrte Daten durch die verantwortliche Stelle nicht mehr übermittelt oder genutzt werden.

8.2.2 Werbewiderspruch im Impressum

Der Betreiber einer Website hatte in sein Impressum deutlich sichtbar und rot hervorgehoben folgenden Hinweis aufgenommen:

ACHTUNG: Die Verwendung der Kontaktdaten des Impressums zur gewerblichen Werbung, sei es per Post, Fax, E-Mail, Telefon etc., ist ausdrücklich nicht erwünscht. Es sei denn, Herr XY (Betreiber) hat zuvor seine schriftliche Einwilligung erteilt. Herr XY (Betreiber) und alle auf dieser Webseite genannten Personen widersprechen hiermit jeder kommerziellen Verwendung, Speicherung, Vermietung, Vermittlung und Weitergabe ihrer Daten.

Dennoch waren seine Kontaktdaten nachweislich aus diesem Impressum erhoben und für Werbezwecke verarbeitet und genutzt worden.

Soweit wie im hier betrachteten Fall der Widerspruch nicht direkt gegenüber der verantwortlichen Stelle erklärt worden ist, unterliegt die verantwortliche Stelle bezüglich des Werbewiderspruchs einer zumindest begrenzten Nachforschungspflicht (vgl. Simitis, BDSG, 7. Aufl., Rdnr. 260 zu § 28). In jedem Fall erstreckt sie sich aber auf Äußerungen, die ihr zugegangen sind oder zugänglich sein müssen. Im Fall des Betreibers der Website ist der Widerspruch genau an der Stelle vermerkt gewesen, an der die Kontaktdaten zuvor erhoben worden waren. Die verantwortliche Stelle konnte sich also nicht auf die Behauptung zurückziehen, dass ihr der Widerspruch nicht bekannt gewesen sei.

8.2.3 Versand von Werbemails an eine Sperrliste

Ein Internetunternehmen hatte eine Onlinekampagne (Newsletter) für einen Dritten durchgeführt. Dieser Newsletter hatte ausschließlich ein (fremdes) Angebot des Dritten zum Inhalt und sollte über einen eigenen Newsletterverteiler versandt werden. Durch

einen Bedienerfehler sind dann allerdings (externe) Sperrlisten anderer Unternehmen für den Versand genutzt worden. Diese Sperrlisten waren von den betroffenen Firmen ursprünglich an das Internetunternehmen übermittelt worden, um bei vorherigen, selbst beauftragten Aussendungen die jeweils in der Sperrliste enthaltenen E-Mail-Adressen vom entsprechenden Versand auszuschließen.

Zur rechtlichen Bewertung:

Die Nutzung der E-Mail-Adressen eigener Kunden für Zwecke der Werbung für fremde Angebote richtet sich nach § 28 Abs. 3 Sätze 5 und 6 BDSG:

Unabhängig vom Vorliegen der Voraussetzungen des Satzes 2 dürfen personenbezogene Daten für Zwecke der Werbung für fremde Angebote genutzt werden, wenn für den Betroffenen bei der Ansprache zum Zwecke der Werbung die für die Nutzung der Daten verantwortliche Stelle eindeutig erkennbar ist. Eine Verarbeitung oder Nutzung nach den Sätzen 2 bis 4 (bzw. 5 = allgemein anerkannter Redaktionsfehler) ist nur zulässig, soweit schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

Nach dieser Vorschrift ist eine Nutzung eigener Newsletterverteiler für Zwecke der Fremdwerbung generell ausgeschlossen, denn der in Satz 5 in Bezug genommene Satz 2 beschränkt sich auf die Nutzung von Listendaten, bei denen die E-Mail-Adresse aber nicht enthalten ist.

Unabhängig davon stehen einer solchen Werbeaktion aber auch schutzwürdige Betroffeneninteressen entgegen, da in diesem Zusammenhang zusätzlich die Vorgaben des Gesetzes gegen den unlauteren Wettbewerb zu beachten sind. § 7 Abs. 3 Nr. 2 UWG legt u. a. fest, dass bei fehlender ausdrücklicher Einwilligung des Betroffenen eine unzumutbare Belästigung bei einer Werbung unter Verwendung elektronischer Post nur dann nicht anzunehmen ist, wenn der Unternehmer die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet. Vorliegend handelte es sich aber um Fremdwerbung.

Damit ist die grundsätzliche Praxis, eigene Newsletterverteiler für fremde Werbezwecke zu nutzen, in jedem Fall unzulässig.

Wenn schon die Nutzung eigener Adressverteiler für fremde Werbezwecke generell unzulässig ist, besteht - unabhängig von der Tatsache, dass sich die in den Sperrlisten enthaltenen Werbewidersprüche auf ein anderes Unternehmen bezogen und gegenüber dem versendenden Unternehmen keine Wirkung entfalten konnten - auch kein Grund,

diesbezügliche Sperrlisten überhaupt zu erheben und zu verarbeiten. Das Internetunternehmen hatte also die Sperrlisten unzulässiger Weise verarbeitet, die Ersteller der Sperrlisten hatten diese unzulässiger Weise an das Internetunternehmen übermittelt.

Im konkreten Einzelfall hinzu kam die der Zweckbestimmung vollkommen entgegengesetzte Nutzung der betreffenden Sperrlisten. Dies stellte einen Verstoß gegen § 28 Abs. 5 Satz 1 BDSG dar, wonach der Dritte (hier: das Internetunternehmen), dem die Daten übermittelt worden sind, diese nur für den Zweck verarbeiten oder nutzen darf, zu dessen Erfüllung sie ihm übermittelt worden sind.

8.2.4 Offene E-Mail-Verteiler

Permanent wiederkehrend erreichen mich Eingaben zum Erhalt von Newslettern oder anderweitigen Werbe-E-Mails mit offener Empfängerliste (vgl. dazu 5. TB, Pkt. 4.3.2.4).

Mindestens dann, wenn sich die E-Mail-Adressen vor der Domain-Angabe aus Vornamen und Nachnamen zusammensetzen, handelt es sich unzweifelhaft um personenbezogene Daten im Sinne des Datenschutzrechts. Mit dem Versand über einen offenen Verteiler (Adressen im „AN“- bzw. „TO“- oder „CC“-Feld) werden diese E-Mail-Adressen sowie die sich aus dem Inhalt der E-Mail ergebenden verbindenden Merkmale des Adressatenkreises jeweils allen anderen Empfängern bekanntgegeben und somit im datenschutzrechtlichen Sinne übermittelt.

Eine Rechtsgrundlage hierfür ist regelmäßig nicht ersichtlich; von den verantwortlichen Stellen ist auch nicht vorgetragen worden, dass diese Übermittlungen gewollt und zulässig gewesen seien. Stattdessen hat es sich in allen Fällen um individuelle Fehlleistungen einzelner Mitarbeiter gehandelt, die die E-Mail-Adressen in das falsche Adressfeld - korrekt wäre die Nutzung des BCC-Feldes gewesen - eingetragen hatten.

Unzulässige Übermittlung personenbezogener Daten können als Ordnungswidrigkeiten verfolgt werden. Das Bayerische LDA hat 2013 als erste Aufsichtsbehörde derartige Verstöße mit einem Bußgeld geahndet; inzwischen sind auch Beispiele aus anderen Bundesländern bekannt. Ich selbst habe dies bisher noch nicht praktiziert, schließe das für die Zukunft aber auch nicht aus.

8.2.5 Wer entscheidet über Kinderfotos auf Facebook?

Nicht selten erreichen meine Behörde Eingaben zu datenschutzrechtlichen Problemen, deren eigentliche Ursache innerfamiliäre Konflikte sind. So auch in diesem Fall:

Eine vom Kindsvater getrennt lebende Mutter störte sich daran, dass die neue Lebensgefährtin ihres Ehemannes auf ihrer Facebook-Seite Fotos des gemeinsamen Sohnes - hier in quasi neuer familiärer Eintracht mit dem Vater bzw. ihrem Noch-Ehemann - veröffentlichte, womit sie als Mutter - auch aus Gründen des Persönlichkeitsrechtsschutzes des Kindes - grundsätzlich nicht einverstanden sei. Ihr habe ich mitgeteilt, dass in Anbetracht des Alters des Kindes die Frage der datenschutzrechtlichen Entscheidungsbefugnis über eine Internetveröffentlichung von Bildern, die es zeigen, zwar eine Angelegenheit der gemeinsamen Personensorge mit dem Kindsvater ist. Unterschiedliche Auffassungen der Sorgeberechtigten und sich daraus ergebende Konflikte sind jedoch zivilrechtlich zu klären und keine Angelegenheit der Datenschutzaufsicht. Ich habe daher ein Tätigwerden abgelehnt.

8.2.6 Personenbezogene Fahndung und Warnung

Die Inhaberin eines Gastronomiebetriebs veröffentlichte auf der Facebook-Seite ihres Restaurants eine Fotografie der Vorderseite eines fremden Personalausweises mit allen dortigen Daten und dem Lichtbild des Inhabers, verbunden mit der Warnung, er sei ein polizeibekannter Straftäter, der im Restaurant gestohlen habe, und sich (weiterhin) im Ortsteil ihres Betriebs aufhalte. Das Bild des Ausweises hatte sie - offenbar mit Einverständnis des Betroffenen - machen können, als sie ihn beim Diebstahl stellte. Dieser Facebook-Eintrag fiel Dritten auf, die umgehend meine Behörde informierten.

Rechtlich gilt: Personenfahndungen mit Lichtbildern zu Strafverfolgungszwecken sind allein hoheitliche Aufgabe der Strafverfolgungsbehörden nach Maßgabe der §§ 131a und 131b StPO. Auch die gefahrenabwehrrechtliche Warnung vor vermeintlich kriminellen Personen obliegt allein den hierzu berufenen Behörden nach Maßgabe des allgemeinen und besonderen Polizeirechts.

Privaten ist eine Veröffentlichung von Lichtbildern zu solchen Zwecken gemäß den §§ 22, 24 KunstUrhG verboten, der Verstoß nach § 33 KunstUrhG strafbar. Zudem besteht - auch soweit nur die Personalien ohne ein Lichtbild veröffentlicht werden - mangels berechtigten Interesses ebenso keine datenschutzrechtliche Übermittlungsbefugnis im Sinne von § 28 Abs. 2 Nr. 2b BDSG. Die Veröffentlichung kann folglich als unbefugte Übermittlung nicht-öffentlich zugänglicher Daten bußrechtlich verfolgt werden. Bei Vorliegen einer Rufschädigungsabsicht kommt auch eine Straftat nach den §§ 43 Abs. 2 Nr. 1, 44 Abs. 1 BDSG in Betracht.

Ich habe daher die Restaurantbesitzerin zur Entfernung des Eintrags verpflichtet und den Betroffenen über den Verstoß unterrichtet und ihn auf seine Anzeigebefugnis hingewiesen.

8.2.7 Kundenwiedererkennung durch Cookies

Mich erreichte die Beschwerde eines Nutzers eines Reisevermittlungsportals, der sich einige Reiseangebote angesehen und anschließend vom Portalbetreiber eine E-Mail mit einer Zusammenfassung der gerade angesehen Seiten, gedacht als „Ermutigung“ zur Buchung, erhalten hatte. Die E-Mail erreichte ihn allerdings, ohne dass er dem Portalbetreiber zu Buchungszwecken seine E-Mail-Adresse durchgegeben hatte. Er vermutete, dass das Unternehmen aus seiner IP-Adresse seine Identität und seine E-Mail-Adresse - möglicherweise unter Rückgriff auf frühere Buchungen - erschlossen und auf diese Weise den Datenschutz verletzt habe.

Der Reisevermittler hat mir dazu mitgeteilt, dass die Adress- und E-Mail-Daten des Beschwerdeführers aus einer zu einem früheren Zeitpunkt über das gleiche Buchungsportal durchgeführten Reisebuchung stammten. Im Zusammenhang mit dieser Reisebuchung sei auf seinem Computer ein Cookie gespeichert worden, der es dem Portalbetreiber dann bei den erneuten Recherchen ermöglicht habe, eine Verbindung zu seiner früheren Buchung und damit auch zu der seinerzeit angegebenen E-Mail-Adresse herzustellen.

Da auch in der Datenschutzerklärung ausführlich auf diese Nutzung von Cookies hingewiesen worden war, habe ich einen Datenschutzverstoß verneint. Die aus einer früheren Buchung stammende E-Mail-Adresse war in diesem Fall zulässigerweise zur Werbung für eigene Produkte genutzt worden (§ 28 Abs. 3 Satz 2 Nr. 1, Satz 3 und Satz 6 BDSG; § 7 Abs. 3 UWG).

Ich habe den Beschwerdeführer darauf aufmerksam gemacht, dass er durch manuelles Löschen der Cookies auf seinem Computer verhindern kann, dass er bei weiteren Recherchen auf dem gleichen Portal erneut vergleichbare E-Mails erhält. Er kann seinen Browser aber auch generell so einstellen, dass Cookies nach jeder Internetsitzung automatisch gelöscht werden. Davon unabhängig kann er die Zusendung weiterer Werbemails auch dadurch unterbinden, dass er den Abmeldelink am Ende der Werbe-E-Mail anklickt oder - wie auch durch andere Anbieter häufig angeboten - eine E-Mail mit dem Betreff „Abmeldung: *E-Mail-Adresse des Nutzers*“ an die gleichfalls am Ende der Werbe-E-Mail angegebene E-Mail-Adresse des Portalbetreibers sendet.

8.2.8 Keine Ausweiskopien mehr im E-Commerce

Das VG Hannover hat in seinem Urteil vom 28. November 2013 (10 A 5342/11, in: juris) klargestellt, dass das Personalausweisgesetz jedenfalls dann, wenn es um die automatisierte Erhebung und Verarbeitung personenbezogener Daten aus dem Personalausweis oder mithilfe des Personalausweises geht, in seinem dritten Abschnitt (§§ 14-20) eine abschließende, § 28 BDSG verdrängende Regelung enthält. Dies betrifft nach Aussage

des Gerichts insbesondere auch alle Verfahren, bei denen Personalausweise gescannt und anschließend in elektronischer Form auf einem Rechner gespeichert werden. Nach den datenschutzrechtlichen Bestimmungen des Personalausweisgesetzes ist das Scannen und Speichern von Personalausweisen unzulässig.

Damit besteht jetzt (vgl. dazu 4. TB, Pkt. 4.2.2.11; 5. TB, Pkt. 4.3.15.2) praktisch keine Möglichkeit mehr, von Kunden im Zuge der Identitätsprüfung im Onlinehandel eine elektronische Personalausweiskopie (per E-Mail oder per Upload) zu fordern.

In dem durch das VG Hannover beurteilten Fall hatte die verantwortliche Stelle den Personalausweis selber gescannt, während Onlinehändler dies dem Kunden auftragen und ihm darüber hinaus noch aufgeben, die so erzeugte Datei an sie zur weiteren Bearbeitung und Nutzung zu übertragen. Im Übrigen besteht kein Unterschied, d. h. in beiden Fällen findet anschließend eine automatisierte Verarbeitung (Speicherung) identischer Daten statt. Festzuhalten ist, dass der Kunde seinen Personalausweis nur deshalb scannt, weil die Onlinehändler das so fordern und anders keine Buchung zu realisieren ist. Damit ist auch der Scanvorgang - obwohl rein technisch durch den Kunden durchgeführt - allein dem Verantwortungsbereich der Händler zuzuordnen, denn nur sie veranlassen den Kunden zu dieser Handlung. Das praktizierte Verfahren wird in seiner Gesamtheit von den Händlern so vorgegeben und ist daher insgesamt auch durch diese zu verantworten. Die Vorschriften des Personalausweisgesetzes können nicht dadurch umgangen werden, dass der unmittelbare, rein physische Umgang mit dem Personalausweis dem Kunden überlassen wird, man sich also bei diesem Verarbeitungsschritt des Kunden lediglich bedient. Es wäre zu einfach und würde dem Zweck der Norm vollkommen zuwiderlaufen, wenn sich die verantwortliche Stelle auf diese Weise ganz einfach aus ihrer Verantwortung stehlen könnte. Dann bräuchte eine verantwortliche Stelle sich auch im direkten Kontakt mit dem Kunden nur hinstellen und den Kunden selbst den Scanner bedienen lassen.

Als Alternativen zur Durchführung der Identitätsprüfung kommen die Einsendung teilgeschwärzter Personalausweiskopien auf dem Postweg und per Fax oder andere Verfahren zur Identitätsprüfung, wie beispielsweise das Postident-Verfahren oder der elektronische Identitätsnachweis in Betracht.

1. Senden Kunden eine teilgeschwärzte Personalausweiskopie auf dem Postweg oder per Fax - vorausgesetzt Faxsendungen laufen bei den Händlern auf herkömmlichen Faxgeräten ein - ein, liegt die Kopie dort nur in Papierform vor und kann dann in vergleichbarer Weise geprüft werden, wie das in der Vergangenheit bereits mit den per E-Mail eingesandten Ausweiskopien erfolgt war. Mangels automatisierter Verarbeitung der in der Ausweiskopie enthaltenen personenbezogenen Daten ist § 20 Abs. 2 PAuswG in

diesem Fall nicht einschlägig und § 20 Abs. 1 PAuswG steht einer solchen Verfahrensweise nicht grundsätzlich entgegen (vgl. 5. TB, Pkt. 4.3.9.2).

Die Argumentation eines Onlinehändlers mir gegenüber, dass bei weitem nicht jeder in Frage kommende Kunde über einen Fax-Anschluss verfüge und der herkömmliche Postweg im Großteil der Fälle zu langwierig wäre, weise ich zurück. Tatsächlich beträgt die Postlaufzeit heutzutage im Regelfall lediglich einen Tag und ebenso wie nicht jeder Kunde über einen Faxanschluss verfügt, verfügt auch nicht jeder Kunde über eine Scanmöglichkeit. Auf Letzteres stützt sich aber die in der Vergangenheit praktizierte Verfahrensweise.

2. Eine wenn auch aufwändigere, so doch deutlich sichere Identifikationsmöglichkeit als die optische Prüfung einer Personalausweiskopie bietet das Postident-Verfahren. Dabei ist insbesondere zu beachten, dass gerade die Erstellung einer Ausweiskopie durch den Kunden abhängig von dessen Fähigkeiten und technischen Ressourcen mit starken Qualitätsmängeln behaftet sein kann und zudem eine Reihe von Fälschungsmöglichkeiten bietet, sodass die Identitätsprüfung auf der Basis einer bloßen Ausweiskopie ohnehin eine nur sehr eingeschränkte Sicherheit gewährleistet.

3. Schließlich ist darauf hinzuweisen, dass der neue Personalausweis mit der Funktionalität des Elektronischen Identitätsnachweises (vgl. § 18 PAuswG) eine Möglichkeit aufweist, die genau den von den Onlinehändlern verfolgten Zweck erfüllt. Ein Personalausweisinhaber kann seinen Personalausweis auch dazu verwenden, seine Identität gegenüber nicht-öffentlichen Stellen elektronisch und damit auch über das Internet, d. h. ohne Medienbruch und ohne beachtenswerte Verzögerung, nachzuweisen. Dem eventuellen Gegenargument der noch geringen Verbreitung dieses Verfahrens ist entgegenzuhalten, dass die weitere Verbreitung und die Bereitschaft unter den Personalausweisinhabern, dieses Verfahren ihrerseits auch anzuwenden, natürlich nur dadurch gefördert wird, dass auch nicht-öffentliche Stellen entsprechende Angebote vorhalten.

4. Die vorliegende Aufzählung ist nicht abschließend. Es obliegt den Onlinehändlern, ggf. auch andere Verfahrensweisen - so sie den datenschutzrechtlichen Vorschriften genügen - zur Anwendung zu bringen.

Bei ausländischen Personalausweisen bzw. sonstigen Identifikationspapieren sind die Vorschriften des Personalausweisgesetzes nicht anwendbar. Nach Nr. 4 der Anlage zu § 9 BDSG ist hier jedoch zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, d. h. von den Händlern ist diesbezüglich eine sichere Übertragungsmöglichkeit zu eröffnen. Dies kann beispielsweise mittels einer allgemein verfügbaren E-Mail-

Verschlüsselung (z. B. PGP) oder mit einem Upload über eine SSL-gesicherte Verbindung erreicht werden.

8.3 Arbeitnehmerdatenschutz

8.3.1 Werbeschreiben an einen gekündigten Mitarbeiter

Vom Empfänger zweier Werbeschreiben eines Möbelhauses bin ich wegen der Nichtbeachtung seines Werbewiderspruchs angesprochen worden. Dabei hat es in der Tat ein wenig bizarr gewirkt, dass es sich um einen ehemaligen Mitarbeiter des Möbelhauses handelte, der gekündigt und mit einem Hausverbot belegt worden war.

Dass es sich bei der Werbepost nicht um eine Schikane seines ehemaligen Arbeitgebers handelte, konnte ich dem Beschwerdeführer schon nach Prüfung der Werbeschreiben mitteilen. Am unteren Rand der betreffenden Werbeschreiben fand sich nämlich der Hinweis, dass für die Verwendung seiner Adresse die Deutsche Post Direkt GmbH verantwortlich war. Ich habe dem Beschwerdeführer daher zunächst empfohlen, gemäß § 28 Abs. 4 Satz 1 BDSG in jedem Fall auch gegenüber der Deutschen Post Direkt GmbH der weiteren Verwendung seiner Adressdaten für Zwecke der Werbung und der Markt- und Meinungsforschung zu widersprechen. Zum einen kann er damit definitiv ausschließen, dass das Möbelhaus nochmals seine dort gespeicherten Adressdaten für eigene Werbezwecke nutzen kann, zum anderen unterbindet er auf diese Weise auch die werbliche Nutzung dieser Daten durch beliebige andere Unternehmen.

Das Möbelhaus hatte seinen ehemaligen Arbeitnehmer also nicht deshalb angeschrieben, weil er wegen seines inzwischen beendeten Arbeitsverhältnisses noch in dessen Datenbeständen gespeichert war. Vielmehr ist seine Anschrift durch die Deutsche Post Direkt GmbH über einen so genannten Lettershop bereitgestellt worden, wobei das Möbelhaus lediglich das Postleitzahlengebiet der Adressaten vorgegeben hatte und die genutzten Anschriften selbst zu keinem Zeitpunkt zu Gesicht bekommen hat. Im konkreten Fall ist dem Möbelhaus somit erst durch den Werbewiderspruch bekanntgeworden, dass auch ein ehemaliger Arbeitnehmer zu den Adressaten gehört hat.

Die vermeintliche Nichtbeachtung des Werbewiderspruches erklärte sich damit, dass die Anschrift des Beschwerdeführers zwar sofort nach Erhalt des Widerspruchs in die unternehmensinterne Sperrliste des Möbelhauses aufgenommen worden ist, die Vorbereitungen für das zweite Werbeschreiben zu diesem Zeitpunkt aber bereits abgeschlossen waren, sodass er das betreffende zweite Werbeschreiben trotz seines - kurz vorher eingegangenen - Widerspruchs noch zugesandt bekommen hat.

8.3.2 Weitergabe von Beschäftigtendaten an potentiellen neuen Arbeitgeber

Ein Unternehmen schloss aus Kostengründen sein bisheriges Callcenter und hatte deswegen den dortigen Beschäftigten gekündigt; die Callcenter-Leistungen sollten künftig von einem externen Dienstleister erbracht werden. Um den Betroffenen jedoch eine Weiterbeschäftigung zu ermöglichen und dem beauftragten Dienstleister bereits mit den Aufgaben vertrautes Personal zu verschaffen, gab das Unternehmen die Namen und privaten Telefonnummern der betroffenen Mitarbeiter an den neuen Callcenter-Betreiber weiter. Dieser kontaktierte diese in der Folgezeit telefonisch und unterbreitete ihnen das Angebot einer Anschlussbeschäftigung, allerdings zu weit schlechteren Bedingungen als bisher.

Die über die als unredlich empfundene Kündigung und die schlechteren Konditionen einer Weiterbeschäftigung erbosten Beschäftigten fragten meine Behörde, ob ihr bisheriger Arbeitgeber befugt gewesen sei, ihre Namen und privaten Telefonnummern weiterzugeben und ob der neue Callcenter-Betreiber diese Daten hätte erheben und verarbeiten dürfen.

Ihnen habe ich mitgeteilt, dass ich die Übermittlung ihrer Daten ebenso für rechtswidrig halte, wie die weitere Nutzung und Verarbeitung der Daten durch den potentiellen neuen Arbeitgeber. Das Verarbeitungshandeln beider Unternehmen war weder für die Durchführung und Beendigung des bisherigen Arbeitsverhältnisses objektiv erforderlich, noch bestanden anerkennenswerte Interessen am Informationsaustausch, die dem Interesse der Beschäftigten gegenüber vorrangig wären, ausschließlich selbst darüber zu entscheiden, ob sie wegen einer baldigen Arbeitslosigkeit und einer möglichen Anschlussbeschäftigung bei anderen Arbeitgebern vorstellig werden möchten (§ 32 Abs. 1 Satz 1 BDSG). Ihr bisheriger Arbeitgeber hätte eine Übermittlung von Namen und Erreichbarkeiten also allein mit der Einwilligung der Betroffenen tätigen dürfen, sprich auf die besondere Nachfrage, ob sie sich vorstellen können, künftig für das Nachfolgeunternehmen zu arbeiten und ob dieses deswegen die Daten erhalten und Kontakt aufnehmen darf.

Zudem habe ich darauf hingewiesen, dass schon ihrem bisherigen Arbeitgeber die Erhebung und Verarbeitung privater Telefonnummern allein bei einem objektiven Erfordernis einer besonderen außerdienstlichen Erreichbarkeit (z. B. Rufbereitschaft / Beschäftigungsverhältnis mit flexiblem Personaleinsatz) gestattet ist, da Arbeitnehmer ansonsten ein schutzwürdiges Interesse daran haben, dass ihre privaten Kommunikationsmittel als der Privatsphäre zugehörig respektiert werden und eine stetige Erreichbarkeit durch Vorgesetzte nicht ihr Freizeitempfinden und -verhalten beeinträchtigt. Eine aus meiner Sicht gebotene bußrechtliche Ahndung des Vorgangs steht noch aus.

8.3.3 Einsicht in Arbeitszeitkonten von Kollegen

Im Wege der Beratung fragte mich ein Unternehmen, ob es zulässig sei, wenn Mitarbeiter auch die Arbeitszeitkonten ihrer Kollegen einsehen können. Eine gemeinsame Übersicht habe den Vorteil, dass jeder Mitarbeiter einer Abteilung die geplanten Urlaube und Freistellungen seiner Kollegen einsehen und so gemeinsame Veranstaltungen wie beispielsweise Weiterbildungen besser planen oder bei gewünschten Dienstplanänderungen erkennen könne, wer dafür potentiell überhaupt in Frage kommt.

Ihm habe ich geantwortet, dass die vom Arbeitgeber verantwortete Möglichkeit, die Arbeitszeiten unter Kollegen wechselseitig einzusehen, datenschutzrechtlich noch keine Übermittlung, sondern lediglich eine betriebliche Nutzung von Beschäftigtendaten ist. Trotzdem ist sie nach § 32 Abs. 1 Satz 1 bzw. § 28 Abs. 1 Satz 1 Nr. 2 BDSG nur zulässig, soweit sie für einen geregelten Dienstbetrieb zwingend erforderlich ist und keine schutzwürdigen Interessen der Betroffenen entgegenstehen, was ich jedoch angesichts der Risiken einer weder wünschenswerten, noch arbeitsrechtlich erlaubten Sozialkontrolle der Mitarbeiter untereinander für im Regelfall nicht gegeben halte.

Eine andere Sichtweise wäre allenfalls dann vertretbar, wenn folgende Voraussetzungen erfüllt sind:

1. Eine wechselseitige Einsicht ist nur innerhalb einer begrenzten Organisationseinheit möglich, also im Kreis von Personen, die ihre Arbeits- bzw. Abwesenheitszeiten aufeinander abstimmen bzw. hiervon zwingend Kenntnis nehmen müssen.
2. Eine Rückschau auf vergangene Zeiträume ist begrenzt, maximal auf den jeweiligen Vormonat.
3. Krankheitsbedingte oder sonst allein in der Person des Beschäftigten liegende Abwesenheiten sind als solche nicht ausgewiesen oder erkennbar.
4. Kommen- und Gehen-Zeiten sowie Angaben zum Arbeitszeitsaldo (Plus- und Minusstunden) können von Kollegen nicht eingesehen werden.

Der datenschutzrechtlich verantwortlichen Stelle habe ich letztlich statt eines mitarbeiterübergreifenden Zugriffs auf Zeiterfassungskonten empfohlen, lieber einen gesonderten Abwesenheits- und Dienstkalender zu führen, der insoweit datensparsamer ist und notwendige Abstimmungen gleichermaßen erlaubt.

8.3.4 GPS in Firmenfahrzeugen

Im Berichtszeitraum hatte ich mich erneut (vgl. 5. TB, Pkt. 4.3.3.8) in mehreren Fällen mit der Ausrüstung von Firmenfahrzeugen mit GPS-Empfängern zu befassen.

Durch Auswertung der GPS-Daten kann festgestellt werden, zu welchem Zeitpunkt sich die Empfangsgeräte, die in den von den Beschäftigten genutzten Fahrzeug installiert sind, an welchem Ort befunden haben. Das System ermöglicht damit, den genauen Aufenthalt von Beschäftigten, soweit sie sich in oder in unmittelbarer Nähe ihrer Einsatzfahrzeuge befinden, in zeitlicher und örtlicher Hinsicht permanent abzubilden und zu verfolgen. Auch wenn sich diese Angaben unmittelbar nur auf das Empfangsgerät beziehen, entsteht durch die beim Arbeitgeber mögliche Gerätezuordnung zu den ein entsprechend ausgerüstetes Fahrzeug führenden Beschäftigten regelmäßig ein Personenbezug. Die Standortdaten der GPS-Empfangsgeräte stellen daher personenbezogene Daten im Sinne von § 3 Abs. 1 BDSG dar.

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

Im Arbeitsverhältnis lässt sich die grundsätzlich in § 32 Abs. 1 BDSG geregelte Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten nur in engen Grenzen auf Einwilligungen der Beschäftigten stützen, denn aufgrund des Abhängigkeitsverhältnisses zum Arbeitgeber liegt die für eine Einwilligung vorauszusetzende Freiwilligkeit der Entscheidung (vgl. § 4a Abs. 1 BDSG) in aller Regel nicht vor. Dies gilt natürlich und gerade auch für die hier zu betrachtende, ausschließlich dem Arbeitgeber nutzende und für die Arbeitnehmer mit einem ständigen Überwachungsdruck, also der Gewissheit, dass der Arbeitgeber ständig genau über den Fahrzeugstandort und jede Fahrzeugbewegung informiert ist, verbundene Verarbeitung von Standortdaten.

In der Regel soll das Ortungssystem - neben der datenschutzrechtlich unbedenklichen Fahrzeugverfolgung im Diebstahlsfall - ausschließlich für Zwecke der Fahrzeug- bzw. Mitarbeiterdisposition eingesetzt werden. Ich betrachte dies im Falle eines bundesweiten, jeweils über mehrere Tage andauernden Einsatzes der Beschäftigten durchaus als legitimen, durch § 32 BDSG gedeckten Zweck. Nach § 32 Abs. 1 Satz 1 BDSG dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist.

Allerdings zeigt diese Vorschrift - ebenso wie § 3a BDSG: Datenvermeidung und Datensparsamkeit - zugleich die Grenzen der Datenverarbeitung auf, denn zulässig ist eine Datenverarbeitung nur, soweit diese für den verfolgten Zweck auch erforderlich ist. In den meisten Fällen sollte es daher vollkommen ausreichend sein, wenn der Arbeitgeber die Standortdaten seiner Beschäftigten ausschließlich in Echtzeit verarbeitet und nutzt. Sowohl für die Zwecke der Fahrzeug- bzw. Beschäftigtendisposition als auch im Fall eines

Fahrzeugdiebstahls genügt die Kenntnis des aktuellen Fahrzeugstandortes und der aus dessen Veränderung erkennbaren Bewegungsrichtung. Eine Zulässigkeit für die Speicherung der Standortdaten besteht daher im Regelfall nicht.

Die Speicherung der Standortdaten birgt bzw. vergrößert darüber hinaus auch immer die Gefahr der nachträglichen zweckfremden Nutzung der Daten zur Verhaltenskontrolle. Unzweifelhaft geben die mittels des GPS-Systems erhobenen Stand- und Fahrzeiten der Einsatzfahrzeuge Auskunft über das Verhalten der Arbeitnehmer, beispielsweise über die die reinen Arbeitszeiten am Einsatzort überschreitenden Aufenthaltszeiten, die Anzahl und Orte der Pausen während der Fahrt, die Fahrtroute, die Durchschnittsgeschwindigkeit etc. Dies ist auch der Grund, weshalb Arbeitgeber regelmäßig verpflichtet sind, vor Einsatz des Ortungssystems eine Vorabkontrolle durchzuführen. Nach § 4d Abs. 5 BDSG ist eine Vorabkontrolle immer dann durchzuführen, wenn automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen. Dass diese Risiken vorliegend in der ständigen Überwachung der Arbeitnehmer und einer drohenden Verhaltenskontrolle liegen, kann nicht ernsthaft bestritten werden. Dabei unterstelle ich weder, dass die betreffenden Arbeitgeber dies so praktizieren noch überhaupt beabsichtigen - in der Vorschrift geht es um das bloße Risiko.

Eine Vorabkontrolle stellt eine materielle Rechtmäßigkeitsprüfung dar, die unter besonderer Beachtung der getroffenen technischen und organisatorischen Datensicherungsmaßnahmen (§ 9 BDSG), der Beachtung der Grundsätze von Datenvermeidung und Datensparsamkeit (§ 3a BDSG), der Wahrung der Betroffenenrechte (§ 6 BDSG) und der Transparenzregeln (§§ 4 Abs. 3, 6c Abs. 1 BDSG) zu erfolgen hat. Ziel ist es, ausgehend vom Zweck der Datenverarbeitung und den technischen Möglichkeiten des zu prüfenden Systems dessen tatsächlichen Gebrauch so zu regeln, dass er den datenschutzrechtlichen Anforderungen entspricht. Unzulässige Speicher- und Auswertungsfunktionalitäten, insbesondere solche, die nur der individuellen Überwachung von Beschäftigten dienen können, sind regelmäßig technisch zu unterbinden. Von nicht zu unterschätzender Bedeutung ist schließlich auch eine größtmögliche Transparenz für die Betroffenen. Nur wenn die Mitarbeiter in ausreichender Weise darüber unterrichtet werden, welche konkreten Daten unter welchen Umständen zu welchen Zwecken durch wen wie lange erhoben, verarbeitet und genutzt werden, ist den Transparenzanforderungen des Bundesdatenschutzgesetzes Genüge getan und kann mit entsprechender Akzeptanz in der Mitarbeiterschaft gerechnet werden. Eine bloße Information, dass ab einem bestimmten Zeitpunkt in allen Einsatzfahrzeugen des Unternehmens ein Ortungssystem zum Einsatz kommt, ist keinesfalls ausreichend.

Für den Einsatz von GPS-Systemen lassen sich im Ergebnis folgende Grundsätze aufstellen:

Der offene Einsatz von Ortungssystemen zur Koordinierung des Einsatzes von Fahrzeugen und Mitarbeitern ist

1. unter Beachtung betriebsverfassungsrechtlicher Vorgaben,
2. und der Durchführung einer datenschutzrechtlichen Vorabkontrolle

auf Grundlage von § 32 Abs. 1 Satz 1 BDSG insoweit datenschutzrechtlich zulässig, wie es aus betrieblichen Gründen

1. erforderlich ist, den Standort des georteten oder den gleichzeitigen Einsatz anderer Fahrzeuge oder verschiedener Mitarbeiter kurzfristig zu beeinflussen,
2. sich die Datenerhebung auf den geografischen Standort des Fahrzeugs beschränkt und
3. die Daten sofort gelöscht werden, sobald das geortete Fahrzeug seine Position ändert.

Eine Erhebung und Verarbeitung für andere Zwecke bzw. eine Zweckänderung der Daten ist unzulässig.

8.3.5 Daten und Fotos von Mitarbeitern auf der Firmenhomepage und im Intranet

Immer wieder erreichen mich Anfragen dazu, ob Angaben zu Mitarbeitern und Fotos zu ihrer Person im Internetauftritt oder Intranet des Arbeitgebers zulässig sind. Insbesondere wurde mehrfach die Frage aufgeworfen, ob sie zu löschen sind, sobald der Betroffene das Unternehmen verlassen hat. Hierbei gilt:

1. Identitäten, berufliche Kontaktdaten, Aufgabenbereiche bzw. Zuständigkeiten sowie im besonderen Einzelfall Qualifikationen und Angaben zur Ausbildung oder dem Werdegang eines Mitarbeiters dürfen ohne dessen Einwilligung nur insoweit inner- und außerbetrieblich veröffentlicht werden, wie dies für einen geregelten, branchenüblichen Geschäftsbetrieb zwingend erforderlich und verhältnismäßig ist oder jedenfalls ein berechtigtes Interesse des Arbeitgebers hieran besteht, und dem gegenüber keine schutzwürdigen Interessen der Betroffenen vorrangig sind (§§ 32 Abs. 1 Satz 1 bzw. 28 Abs. 1 Satz 1 Nr. 2 BDSG). Diese Rechtfertigung des Eingriffs in das Persönlichkeitsrecht entfällt aber mit dem Ausscheiden des Beschäftigten aus dem Unternehmen, da er für dieses nicht länger Tätigkeiten erbringt, als dessen Ansprechpartner zur Verfügung steht oder sonst für seinen Arbeitgeber weiter einsteht. Demgemäß sind - auch ohne besonderes Verlangen des Betroffenen - im Regelfall alle Angaben zu seiner Person insoweit unverzüglich zu löschen (§ 35 Abs. 2 Satz 2 Nr. 3 BDSG).
2. Für Fotos oder Videosequenzen, die im Schwerpunkt Beschäftigte zeigen, gilt nach Auffassung des Bundesarbeitsgerichts auch im Arbeitsrechtsverhältnis das Kunstur-

heberrechtsgesetz, das für Veröffentlichungen von Bildnissen grundsätzlich eine Einwilligung des Betroffenen verlangt (§ 22), die angesichts der Bedeutung des Rechts der Arbeitnehmer, auch im Arbeitsverhältnis ihr Grundrecht auf informationelle Selbstbestimmung frei auszuüben, immer der Schriftform bedarf. Nur so könne verdeutlicht werden, dass die Einwilligung der Arbeitnehmer zur Veröffentlichung ihrer Bildnisse unabhängig von den jeweiligen Verpflichtungen aus dem eingegangenen Arbeitsverhältnis erfolgt und dass die Erteilung oder Verweigerung der Einwilligung für das Arbeitsverhältnis keine Folgen haben dürfen (BAG, Urteil vom 11. Dezember 2014, 8 AZR 1010/13, in: juris). Dieses Einverständnis, dessen Freiwilligkeit in Anbetracht der Besonderheiten der Arbeitsrechtsbeziehung nicht fraglich sein darf, ist widerruflich und führt bei Ausübung dieses Rechts dazu, dass die Aufnahmen entsprechend § 35 Abs. 2 Satz 2 Nr. 3 BDSG unverzüglich zu löschen sind, nicht jedoch automatisch beim Ausscheiden des Mitarbeiters, da das besondere Einverständnis - wenn es nicht unter Vorbehalt gestellt oder befristet wurde - zunächst einmal fortwirkt (BAG a. a. O.). Dies gilt - in ergänzender Anwendung der Bestimmungen des allgemeinen Datenschutzrechts - allerdings nur für solche Aufnahmen, an deren Veröffentlichung der Arbeitgeber auch über die Dauer des Arbeitsverhältnisses hinaus jedenfalls ein berechtigtes Interesse geltend machen kann und dem insoweit gegenüber keine gegenläufigen schutzwürdigen Interessen des Beschäftigten überwiegen (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG).

3. Ist ein Mitarbeiter auf Bildaufnahmen zwar erkennbar, steht jedoch nicht im Focus der Aufnahme, sondern ist er nur deren Beiwerk, ist eine Veröffentlichung zwar nach § 23 Abs. 1 Nr. 2 KunstUrhG persönlichkeitsrechtlich grundsätzlich einwilligungsfrei. Datenschutzrechtlich ist jedoch wegen der Verarbeitung von Beschäftigtendaten bei einem berechtigten Interesse an der Veröffentlichung gleichwohl eine Abwägung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG vorzunehmen, die gerade im Fall des Ausscheidens eines Mitarbeiters eine Löschung gemäß § 35 Abs. 2 Satz 2 Nr. 3 BDSG gebieten kann. Anderes gilt möglicherweise dann, wenn der Beschäftigte bei einem besonderen betrieblichen Ereignis oder aber zusammen mit weiteren Beschäftigten aufgenommen wurde. Fotos auch ausgeschiedener Mitarbeiter im Intranet, die an solchen innerbetrieblichen Ereignissen teilgenommen haben, die das Betriebsklima fördern, wie etwa Betriebsausflüge, Weihnachtsfeiern oder Jubiläen, sind im Regelfall zulässig, solange der Einzelne auch hier nicht der „Fotoschwerpunkt“ sondern lediglich „Beiwerk“ der Szenerie im Sinne von § 23 Abs. 1 Nr. 2 KunstUrhG ist und gemessen an § 28 Abs. 1 Satz 1 Nr. 2 BDSG (auch sonst) keine Anhaltspunkte für entgegenstehende schutzwürdige Interessen bestehen, wie etwa eine mögliche Ehrenrührigkeit der Aufnahme (z. B. Intimitäten, Alkoholexzesse, skurrile Posen).

8.3.6 Überprüfung der Einhaltung des Mindestlohngesetzes bei Auftragnehmern

Mit Einführung des gesetzlichen Mindestlohnes zum Ende des Berichtszeitraums erreichten mich gleich mehrere Anfragen von Unternehmen, inwieweit sie Beschäftigtendaten ihrer Subunternehmer und deren Subunternehmer erheben und verarbeiten dürfen, um die Einhaltung der gesetzlichen Bestimmungen, für die auch sie haften, zu kontrollieren, gerade weil die Bestimmungen des Mindestlohngesetzes offen lassen, welche Prüfungen dem Auftraggeber obliegen.

Ihnen habe ich mitgeteilt, dass es mangels entsprechender gesetzlicher Vorgaben und in Anbetracht der gesetzgeberischen Entscheidung, dass Auftraggeber für Mindestlohnverstöße ihrer Subunternehmer immer, also verschuldensunabhängig, haften, jedenfalls kein zwingendes Erfordernis zur Erhebung und Verarbeitung fremder Beschäftigtendaten im Sinne von § 28 Abs. 1 Satz 1 Nr. 1 BDSG gibt, da Auftraggeber mit einer Erhebung und Verarbeitung fremder Beschäftigtendaten des Auftragnehmers ihr Haftungsrisiko lediglich minimieren, aber nicht völlig ausschließen können (§ 13 MiLoG i. V. m. § 14 AEntG). Eine vollständige oder auch nur stichprobenartige Verarbeitung der Daten von Beschäftigten des Subunternehmers durch den Auftraggeber ist also gerade kein taugliches und damit unvermeidbares, also zwingend erforderliches Mittel im Sinne von § 28 Abs. 1 Satz 1 Nr. 1 BDSG, einer Haftung zu entgehen, sondern lediglich eine von vielen möglichen Maßnahmen zur Risikominimierung.

In Anbetracht des schutzwürdigen Interesses der Beschäftigten, von Verarbeitungen zu ihrer Person - insbesondere durch Dritte - grundsätzlich verschont zu bleiben, kann das insoweit verbleibende berechtigte Interesse im Sinne von § 28 Abs. 1 Satz 1 Nr. 2 BDSG an einer personenbezogenen Datenverarbeitung somit allenfalls dann bestehen, wenn der Auftraggeber alle anderen - verarbeitungsfreien - Möglichkeiten vollständig ausgeschöpft hat und das Restrisiko den Betroffeneninteressen gegenüber gleichwohl überwiegt, was allerdings schwer begründbar erscheint. Der Verarbeitende müsste jedenfalls darlegen können, weshalb beispielsweise vertragliche Zusicherungen, Konventionalstrafen, Bürgschaftserklärungen Dritter sowie eine Prüfung anonymisierter (Gehalts-)Unterlagen für sich oder zusammen genommen das verbleibende Risiko nicht tragbar erscheinen lässt und den Grundrechtseingriff zu Lasten Beschäftigter somit rechtfertigt.

An dieser Betrachtung ändert auch der Bußgeldtatbestand des § 21 Abs. 2 MiLoG nichts. Denn ein bußgeldbewehrter fahrlässiger Pflichtverstoß wäre in Anbetracht des gegenläufigen Risikos des Normadressaten, gegen § 43 Abs. 2 Nr. 1 BDSG zu verstoßen, nur dann normenklar anzunehmen, wenn der Gesetzgeber ihm eine Datenverarbeitung auferlegt hätte.

Auch die übrigen Aufsichtsbehörden teilen meine Auffassung, siehe dazu die Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. bis 19. März 2015 in Wiesbaden „Mindestlohngesetz und Datenschutz“ (siehe Anlage 3).

8.3.7 Videoüberwachung eines Werkstattmitarbeiters

Der einzige Werkstattmitarbeiter eines kleinen Metallbaubetriebes hatte sich wegen einer Videoüberwachung der Werkstatt an mich gewandt. Meine örtliche Überprüfung hat dann überraschender Weise ergeben, dass der Firmeninhaber in seiner Werkstatt eine Babyfon-Kamera vom Typ Motorola MBP 36 betrieben hatte, die den überwiegenden Teil der Werkstatt erfasste und deren Bilder an einem kleinen 3,5“-Monitor, der so genannten Eltern-Einheit, zur Anzeige gebracht werden konnten. In gleicher Weise wie die Videobilder werden dabei auch Audiodaten übertragen. Die Kamera war in der linken hinteren Ecke der Werkstatt in erhöhter Position auf einer Reihe von Aktenordnern positioniert und erfasste auf diese Weise die gesamte Werkstatt. Der Monitor war im Büro aufgestellt. Als Grund für den Kameraeinsatz nannte mir der Firmeninhaber die Vermutung, dass sein einziger gewerblicher Mitarbeiter die im Büro geführten Gespräche belausche. Als konkretes Beispiel nannte er ein Kundengespräch wegen des Erwerbs von Metallprofilen. Noch bevor das Gespräch beendet gewesen sei, hätte sein Mitarbeiter schon mit den fertig zugeschnittenen Profilen in der Bürotür gestanden.

Zum Zeitpunkt meiner Kontrolle war die Eltern-Einheit zwar außer Betrieb - die Akkus waren entladen und das Ladekabel nicht auffindbar. Der Firmeninhaber bestätigte mir jedoch, das Gerät jedenfalls in der Zeit unmittelbar nach der Installation tatsächlich genutzt zu haben. Er habe sich schon gewundert, dass sein Mitarbeiter die Kamera so schnell entdeckt habe. Auf Nachfrage teilte er darüber hinaus noch mit, dass sein Mitarbeiter bislang seine Pausen immer in der Werkstatt verbracht habe, in letzter Zeit aber dazu sein Auto aufsuche…

Dass diese Videoüberwachung unzulässig war lag klar auf der Hand:

§ 32 Abs. 1 Satz 1 BDSG erlaubt die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses, wenn dies für dessen Durchführung erforderlich ist. Ein solches Erfordernis bestand vorliegend nicht und war auch nicht vorgetragen worden.

Darüber hinaus dürfen personenbezogene Daten eines Beschäftigten nach § 32 Abs. 1 Satz 2 BDSG zur Aufdeckung von Straftaten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige

Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind. Der Firmeninhaber und seine im Büro mitarbeitende Ehefrau haben mir dazu vorgetragen, dass sie sich von ihrem Werkstattmitarbeiter bei Kunden- bzw. Bürogesprächen belauscht gefühlt haben. Ich konnte dies indes in keiner Weise nachvollziehen. In den mir geschilderten Fällen ist es stattdessen offensichtlich so gewesen, dass der Mitarbeiter - möglicherweise unvermeidbar - Teile der in der Werkstatt selbst oder im Büro bei geöffneter Tür geführten Gespräche zur Kenntnis genommen hat. Eine Straftat war daher insoweit nicht anzunehmen - schon deshalb war diese Überwachungsmaßnahme auch vor dem Hintergrund des § 32 Abs. 1 Satz 2 BDSG unzulässig.

Unabhängig davon war die - zunächst sogar verdeckt, d. h. ohne Kenntnis des Mitarbeiters durchgeführte - Überwachungsmaßnahme angesichts der erhobenen Vorwürfe aber auch unverhältnismäßig. Eine dauerhafte Überwachung am Arbeitsplatz wiederholt sich potenziell an jedem Arbeitstag und erstreckt sich über die gesamte Arbeitszeit. Er als Arbeitnehmer kann den Aufenthalt in dem überwachten Bereich weder vermeiden noch sich der Überwachung durch ein Verlassen seines Arbeitsplatzes entziehen; die Eingriffsintensität wegen des damit verbundenen Überwachungsdrucks ist somit besonders groß (BAG, Beschluss vom 29. Juni 2004, 1 ABR 21/03, in: 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, in: juris). Der Firmeninhaber hat es insoweit selbst in der Hand gehabt, durch entsprechende Vorsichtsmaßnahmen - z. B. geschlossene Bürotüren oder augenscheinliche Kontrolle der aktuellen Tätigkeit seines Mitarbeiters - auf weniger in das Persönlichkeitsrecht eingreifende Weise auszuschließen, dass sein Mitarbeiter ggf. vertrauliche Informationen weder zufällig noch gewollt zur Kenntnis nehmen kann.

Was die - einem Babyfon immanente - Tonübertragung betrifft, sollte sogar der Straftatbestand des § 201 Abs. 2 Satz 1 Nr. 1 StGB erfüllt gewesen sein. Dies zu prüfen obliegt allerdings den Strafverfolgungsbehörden und würde einen entsprechenden Strafantrag des Betroffenen erfordern (§ 205 Abs. 1 StGB). Ob der Betroffene nach meinem Hinweis davon Gebrauch gemacht hat, ist mir nicht bekannt.

Noch während meiner örtlichen Kontrolle ist das Babyfon wieder aus der Werkstatt entfernt worden.

8.4 Gesundheitswesen

8.4.1 Einschaltung eines Rechtsanwaltes durch einen Arzt

Wenn sich ein Arzt in einem Streitfall mit einem Patienten eines Rechtsanwaltes bedient, darf er dann Patientendaten an diesen Rechtsanwalt weitergeben?

Auch ein Arzt muss grundsätzlich die Möglichkeit haben, sich zur Wahrung seiner rechtlichen Interessen anwaltlicher Hilfe zu bedienen. Es kann dabei auch nicht darauf ankommen, welche inhaltliche Qualität der jeweilige Streitgegenstand hat - eine diesbezügliche Abgrenzung wäre ohnehin nur sehr schwer möglich - und auch nicht darauf, ob es sich um eine gerichtliche Auseinandersetzung handelt oder eine solche möglicherweise in Aussicht steht. Mithin dürfen Unterlagen, die der bevollmächtigte Rechtsanwalt für eine angemessene Vertretung der rechtlichen Interessen des Arztes benötigt, auf der Grundlage des § 28 Abs. 6 Nr. 3 BDSG an den Rechtsanwalt übergeben werden. Maßstab einer zulässigen Übermittlung ist dabei die Erforderlichkeit, d. h. es dürfen nur die Aktenteile übergeben werden, die im jeweiligen Einzelfall auch tatsächlich zur Verteidigung der Rechte des Arztes erforderlich sind.

Der BGH (Urteil vom 23. Juni 1993, VIII ZR 226/92, in: juris) hat grundsätzlich bestätigt, das ein Arzt sich zur berechtigten Wahrnehmung eigener Interessen auch der Hilfe eines Rechtsanwaltes bedienen darf und dass in diesem Zusammenhang auch die Offenbarung von Behandlungsdaten gerechtfertigt sein kann, um etwaigen Einwendungen des Patienten zu begegnen. Jedoch ist der Arzt dabei zu einer sorgfältigen, am Grundsatz der Verhältnismäßigkeit ausgerichteten Abwägung zwischen seinen eigenen berechtigten Interessen und dem Geheimhaltungsbedürfnis des Patienten gehalten. Die Preisgabe von Behandlungsdaten ist auf das angemessene, zur Durchsetzung der jeweiligen Rechtsposition erforderliche Maß zu beschränken. Dazu gehört auch, dass der Kreis derjenigen, denen die Behandlungsdaten zugänglich gemacht werden, möglichst klein zu halten ist.

8.4.2 Herausgabe der Patientenverfügung nach dem Tod

Der Ehemann einer krankheitsbedingt Verstorbenen wandte sich an meine Behörde, weil das zuletzt behandelnde Krankenhaus nach dem Tod der Betroffenen deren Patientenverfügung nicht herausgeben wollte. Er fragte sich, weshalb eine Erklärung, mit der eine volljährige Person für den Fall ihrer Entscheidungsunfähigkeit schriftlich im Voraus festlegt, ob und wie sie in bestimmten Situationen ärztlich behandelt werden möchte (vgl. § 1901a BGB), noch über den Zeitpunkt des Todes, mit dem logischerweise auch die Behandlung endet, hinaus trotzdem weiter aufbewahrt werden muss.

Ihm habe ich mitgeteilt, dass ein solche Unterlage jedenfalls dann zur Patientenakte zu nehmen ist, wenn sie im Behandlungsprozess Bedeutung erlangt hat und dies deshalb der Dokumentation bedarf. In diesem Fall besteht die Verpflichtung und damit auch die Befugnis zu einer Aufbewahrung für die Dauer von zehn Jahren nach Abschluss der Behandlung (vgl. § 630f BGB). Nur wenn eine solche Erklärung des Patienten nach jeder in Betracht kommenden Sichtweise ohne Relevanz im Behandlungsprozess geblieben wäre, bestünde also überhaupt eine etwaige Verpflichtung der Klinik, das Dokument zu vernichten. Diese Vernichtung kann ein Hinterbliebener aber nur allgemein zivilrechtlich erstreiten, da datenschutzrechtliche Ansprüche des Erklärenden nicht auf seine Erben übergehen, sondern als höchstpersönliche Ansprüche mit dem Tode erlöschen, zumal § 630g BGB nichts anderes hierzu bestimmt. Zwar besteht auch häufig ein datenschutzrechtlicher Doppelbezug zu Personen, die in der Patientenverfügung als Betreuer benannt werden. Diesen Zusammenhang halte ich aber wegen der Einseitigkeit der Willenserklärung für rechtlich irrelevant, so dass es beim Zivilrechtsweg verbleibt.

8.4.3 Weitergabe von Informationen aus einer gemeinsamen psychologischen Beratung von Mutter und Kind an den Kindsvater

Eine Mutter nahm gemeinsam mit ihrem dreijährigen Sohn an einer frühkindlichen Beziehungsberatung einer psychologischen Beratungsstelle teil. Wegen fehlenden Vertrauens beendete die Mutter die Beratung jedoch vorzeitig, wollte aber dann der Beratungsstelle untersagen, gegenüber dem (ebenso personensorgeberechtigten) Kindsvater, mit dem sie einen Sorgerechtsstreit austrug, beratend tätig zu werden, als dieser sich wegen eines eigenen Beratungsbedarfs ebenso dort betreuen lassen wollte. Sie fürchtete um die Vertraulichkeit ihrer bisherigen Gespräche, auch soweit es das gemeinsame Kind betraf. Auf ihre Nachfrage bei meiner Behörde habe ich ihr Folgendes mitteilen wollen, wozu es aber nicht mehr kam, weil sie ihre Petition vor meinem Postausgang aus mir unbekannten Gründen zurückzog:

Berufspsychologen sowie (sonstige) in der Familien- und Erziehungsberatung anerkannter Stellen Tätige sind in strafbewehrter Weise verpflichtet, das Beratungsgeheimnis zu wahren (§ 203 Abs. 1 Nr. 2 und 4 StGB). Ohne das Einverständnis der Petentin hätte also ihre ehemalige Beraterin ihrem Mann bezogen auf ihre Person kein schutzwürdiges Wissen preisgeben dürfen, welches aus ihrer Beratung stammt. Soweit es sich allerdings um solche Umstände handelt, welche die (besonderen) persönlichen Verhältnisse ihres dreijährigen Sohnes betreffen, zu dessen (gemeinsamer) Personensorge auch ihr Mann befugt ist, kann eine etwaige Informationsweitergabe jedenfalls bei Gründen des Kindeswohles schwerlich als unbefugt angesehen werden, denn seine psychologische Betreuung ist von der Erziehungsverantwortung des anderen Personensorgeberechtigten (§ 1687

Abs. 1 Satz 1 BGB) und (damit) von seinem Auskunftsrecht (§ 1686 BGB) umfasst. Maßgeblich sind jedoch die Umstände des Einzelfalls.

8.5 Handel, Gewerbe, Dienstleistungen

8.5.1 Post von Anwälten anderer Fondsanleger

Immer wieder erhalten Fondsanleger unverlangt Post von Anwälten anderer Anleger. Mehrfach habe ich daher die Frage gestellt bekommen, inwieweit fremde Anwälte die Kontaktdaten anderer Anleger, die sie bisher nicht vertreten, von der Fondgesellschaft hätten bekommen und verarbeiten dürfen.

Der Bundesgerichtshof hat sowohl für einen Anleger, der an einer Publikumsgesellschaft in Form einer Gesellschaft bürgerlichen Rechts (Beschluss vom 21. September 2009, II ZR 264/08, in: juris) beteiligt ist, als auch für einen Treuhandkommanditisten (Urteil vom 11. Januar 2011, II ZR 187/09, in: juris) entschieden, dass dieser aus Gründen der Transparenz und eingedenk des wechselseitigen Rechtsverhältnisses gemäß § 716 BGB auch ohne besonderen Anlass Auskunft über die Namen und Anschriften seiner Mitgesellschafter verlangen kann. Eine Klausel im Gesellschaftsvertrag, die einen solchen Anspruch ausschließt, sei unwirksam. Ein schützenswertes Interesse der Mitgesellschafter untereinander auf Anonymität bestehe weder allgemein, noch unter datenschutzrechtlichen Gesichtspunkten. Eine abstrakte Missbrauchsgefahr ändere daran nichts, da jedenfalls rechtlich die Verpflichtung bestehe, die Daten ausschließlich für originäre und damit legitime Zwecke im Kontext des Gesellschaftsverhältnisses bis zur Grenze des Verbots unzulässiger Rechtsausübung (§ 242 BGB) und des Schikaneverbots (§ 226 BGB) zu nutzen und zu verarbeiten. Es bestehe ein allgemeiner zivilrechtlicher Grundsatz, seinen Vertragspartner kennen, - auch über einen Bevollmächtigten - kontaktieren und insoweit Daten verarbeiten zu dürfen. Dieser Auffassung folge auch ich.

Keine datenschutzrechtliche Bedenken habe ich daher, wenn fremde Bevollmächtigte andere Anleger wegen eines rechtlichen Interesses ihrer Mandanten anschreiben (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Dies gilt allerdings nicht, wenn der Inhalt des Schreibens werblicher Natur ist, der Anwalt also unter Bezugnahme auf seine Vertretung anderer Anleger weitere Mandanten zu gewinnen sucht, denn dann handelt er nicht mehr im berechtigten Interesse seiner Mandanten, sondern im eigenen Geschäftsinteresse. Ein solch werbliches Schreiben ist ihm aber ohne Einwilligung der Betroffenen verboten, weil die Voraussetzungen von § 28 Abs. 3 Satz 2 Nr. 1 BDSG nicht vorliegen. Nach dieser Bestimmung kann zwar die Verwendung vorhandener postalischer Anschriften als sogenannte Listendaten für eigene Werbezwecke zulässig sein, wenn sie der Verwender im Rahmen eines Schuldverhältnisses zulässigerweise nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG erhoben hat. Hier hat der Anwalt die Daten jedoch nicht wegen eines eigenen

Schuldverhältnisses zu den datenschutzrechtlich Betroffenen, sondern wegen eines Auskunftsanspruchs seiner Mandanten erhalten. Die Privilegierung greift daher nicht.

Wegen eines unzulässigen werblichen Schreibens an Fondsanleger habe ich einem Anwalt bereits ein Bußgeld auferlegt.

8.5.2 Mitteilung eines anderweitig gefundenen Jobs an erfolglosen Arbeitsvermittler

Eine Arbeitsuchende hatte - gefördert von der Arbeitsagentur - zunächst über einen privaten Vermittler versucht, einen neuen Job zu finden. Dessen Bemühungen blieben jedoch ohne Erfolg. Schließlich fand die Betroffene auf anderem Wege einen Arbeitsplatz. Sie wunderte sich jedoch darüber, dass ihr ehemaliger Arbeitsvermittler von ihr wissen wollte, wann sie bei wem eine neue Tätigkeit gefunden hatte. Als der Vermittler rechtliche Schritte für den Fall der Auskunftsverweigerung ankündigte, fragte sie mich, ob der Arbeitsvermittler diese Informationen tatsächlich erheben dürfe. Dies verhält sich wie folgt:

Die Befugnis (im Sinne von § 28 Abs. 1 Satz 1 Nr. 1 BDSG) eines ehemaligen Arbeitsplatzvermittlers, die genannten Angaben zu erfragen, folgt aus § 298 Abs. 1 Satz 1 SGB III i. V. m. §§ 652 ff., 242 BGB i. V. m. dem Vermittlungsvertrag. Bei dem zwischen einem privaten Arbeitsvermittler und dem Arbeitsuchenden abgeschlossene Vermittlungsvertrag handelt es sich um ein Rechtsgeschäft in der besonderen Ausprägung eines Maklervertrags (vgl. Sächsisches LSG, Urteil vom 2. Dezember 2004, L 3 AL 319/03, in: juris). In Ermangelung vorrangiger Regelungen im Sozialgesetzbuch Drittes Buch gelten daher die vom Bundesgerichtshof allgemein zum Maklerrecht entwickelten Grundsätze, wonach ein Makler innerhalb bestehender vertraglicher Beziehungen von seinem Auftraggeber Auskunft über die für die Entstehung und Berechnung seines Provisionsanspruchs maßgeblichen Umstände verlangen kann (vgl. BGH, Beschluss vom 27. Juli 2000, III ZR 279/99, in: juris). Die Angabe, wann welche Tätigkeit bei wem aufgenommen wurde, ist für den Makler insoweit im genannten Sinne maßgeblich und damit erforderlich, um hinsichtlich eines etwaigen Provisionsanspruchs prüfen zu können, ob es sich um eine Stelle handelt, die aus seinem Portefeuille stammt und die ihm deshalb zu vergüten wäre. Demgemäß ist das Handeln des Arbeitsplatzvermittlers datenschutzrechtlich nicht zu beanstanden.

8.5.3 Private Arbeitsvermittlerin wirft Bewerbungsunterlagen sorglos in die Mülltonne

Auch für private Arbeitsvermittler gilt, hier nach § 298 SGB III als besonderer bereichsspezifischer Vorschrift, dass sie Daten über zu besetzende Ausbildungs- und Arbeitsplätze und über Ausbildungssuchende sowie Arbeitnehmerinnen und Arbeitnehmer nur

erheben, verarbeiten und nutzen dürfen, soweit dies für die Verrichtung ihrer Vermittlungstätigkeit erforderlich ist. Von Betroffenen zur Verfügung gestellte Unterlagen sind unmittelbar nach Abschluss der Vermittlungstätigkeit zurückzugeben. Die übrigen Geschäftsunterlagen des Vermittlers sind nach Abschluss der Vermittlungstätigkeit drei Jahre aufzubewahren. Und selbstverständlich haben auch private Arbeitsvermittler nach § 9 Satz 1 BDSG i. V. m. der zugehörigen Anlage zu diesem Gesetz als datenschutzrechtlich verantwortliche Stelle i. S. v. § 3 Abs. 7 BDSG jene technischen und organisatorischen Maßnahmen zu tätigen, die erforderlich sind, um zu gewährleisten, dass personenbezogene Daten nicht unbefugt von Dritten gelesen werden können, mithin also u. a. die

1. zugriffsgeschützte Verwahrung personenbezogener Daten sowie die
2. datenschutzgerechte Vernichtung etwaig zu löschender Daten in der Weise, dass diese nicht oder nur noch mit unverhältnismäßigem Aufwand wieder rekonstruiert werden können, etwa durch ein Schreddern von Schriftstücken mittels eines Aktenvernichters.

Im Berichtszeitraum erreichte mich allerdings der Hinweis, dass eine private Arbeitsvermittlerin bei Auszug aus einem Gemeinschaftsbüro nicht mehr aufzubewahrende Bewerbungsunterlagen unter Missachtung der genannten Vorschriften einfach in einer offen zugänglichen blauen Papiermülltonne im Mehrparteienhaus ihres Büros unvernichtet, also lesbar, entsorgt hatte, was dort Dritten aufgefallen war. Ihr gegenüber musste ich auf Grundlage von § 38 Abs. 5 Satz 1 BDSG eine datenschutzgerechte Entsorgung der Akten anordnen (vgl. Pkt. 10.2). Dieser Anordnung hat sich die private Arbeitsvermittlerin dann auch gefügt, so dass ich meine Aufsicht beenden konnte.

Wer als privater Arbeitsvermittler durch eine nicht datenschutzgerechte Entsorgung personenbezogener Daten, hier Schriftgut i. S. v. § 298 Abs. 1 SGB III, allerdings billigend in Kauf nimmt, dass Dritte hiervon unbefugt Kenntnis nehmen und es hierauf zu einer solchen Übermittlung kommt, handelt in vorsätzlicher Weise ordnungswidrig (§ 404 Abs. 2 Nr. 12 SGB III). Die Ordnungswidrigkeit kann mit einem Bußgeld bis zu 30.000 Euro geahndet werden (§ 404 Abs. 3 SGB III), in fahrlässiger Begehung mit einem Bußgeld bis zu 15.000 Euro (§ 17 Abs. 2 OWiG). Ich habe daher gemäß § 38 Abs. 1 Satz 6 BDSG den Vorgang bei der Bundesagentur für Arbeit angezeigt, die gemäß § 405 Abs. 1 Nr. 2 SGB III insoweit für die Verfolgung und Ahndung zuständig ist.

8.5.4 PIN-Ausdruck am EC-Kartenlesegerät

Ein Einzelhandelskunde unterrichtete mich über eine Unregelmäßigkeit bei einem elektronischen Bezahlvorgang. Er habe seinen Einkauf bargeldlos per EC-Cash bezahlen

wollen, jedoch sei dann auf einmal die von ihm eingegebene PIN auf dem Display des Kartenlesegerätes zu sehen gewesen.

So wie mir der Sachverhalt geschildert worden war, konnte es sich nur um eine individuelle Fehlbedienung des Kartenlesegerätes durch den Verkäufer gehandelt haben. Vergleichbare Fälle sind mir anderweitig bislang nicht bekanntgeworden.

Üblicherweise läuft ein Zahlungsvorgang so ab, dass der Verkäufer zunächst den Zahlbetrag in den Kartenleser eintippt und diese Eingabe durch Betätigung einer weiteren Taste (z. B. „OK“ oder „Best“ für Bestätigung) abschließt. Danach erfolgt die Aufforderung zum Einstecken der Zahlungskarte und die Aufforderung zur Eingabe der PIN, die ihrerseits wiederum mit der Bestätigungstaste abzuschließen ist.

In dem betreffenden Fall hatte der Verkäufer die Eingabe des Zahlbetrages offensichtlich nicht mit der Bestätigungstaste abgeschlossen, als er dem Kunden den Kartenleser zur Eingabe der PIN reichte. Die danach durch den Kunden erfolgte Eingabe der PIN hatte der Kartenleser daher als Fortsetzung der Eingabe des Kaufbetrages interpretiert. Dies wurde daran deutlich, dass sich die PIN auf dem Kundenbeleg nahtlos an die Kaufsumme anfügte und auch die Kommastelle weiter nach hinten gerückt war, sich also logischerweise genau in der Mitte der vierstelligen PIN befand. Der Kartenleser interpretiert die letzten beiden Ziffern einer Zahlbetragseingabe immer als die Cent-Beträge. Aus dem ursprünglichen Zahlbetrag von 735,00 € war so ein Zahlbetrag von 7.350.0xx,xx € geworden. Erst im nächsten Schritt hätte der Kartenleser dann also zur PIN-Eingabe aufgefordert. Der Verkäufer hat den Zahlungsvorgang an dieser Stelle abgebrochen; der zweite Versuch verlief dann erfolgreich. Nichtsdestoweniger hat der Kunde anschließend unverzüglich seine Zahlungskarte sperren lassen.

Eigentlich hätte auch dem Kunden vor der PIN-Eingabe auffallen müssen, dass im Display des Lesegerätes noch der Zahlbetrag und keine Aufforderung zur PIN-Eingabe gestanden haben muss. Nichtsdestoweniger ist es aber auch durchaus nachvollziehbar, dass er sich weniger auf das Display, sondern mehr auf die korrekte Eingabe der PIN konzentriert hatte, zumal die PIN ja ohnehin nicht im Klartext im Display angezeigt wird. Daher wird im konkreten Fall nicht nur dem - insoweit natürlich maßgeblich verantwortlichen - Verkäufer, sondern auch dem Kunden entgangen sein, dass der Kartenleser noch gar nicht für die PIN-Eingabe bereit war, sondern sich noch im Eingabemodus für den Zahlbetrag befunden hatte.

Eine Schwachstelle im genutzten Zahlungssystem konnte ich vorliegend also nicht entdecken. Der geschilderte Vorfall hatte seine Ursache offensichtlich in erster Linie in einer individuellen Unkonzentriertheit des Verkäufers.

8.5.5 Aushang eines Hausverbots

Durch Polizeibeamte bin ich - ausgehend von einer diesbezüglichen Mitteilung der Mutter des Betroffenen - darüber informiert worden, dass einem jungen Mann nach einem nächtlichen Zwischenfall (Mitarbeiterbeleidigung in erheblichem Maß) an einer Tankstelle Hausverbot ausgesprochen worden war und der Tankstellenpächter dieses Hausverbot öffentlich an seiner Tankstelle ausgehängt hatte. Die Polizei hatte den diesbezüglichen Aushang sichergestellt und mir übergeben.

Der öffentliche Aushang des ausgesprochenen Hausverbots stellt einen Verstoß gegen § 28 Abs. 1 Satz 1 Nr. 2 BDSG dar und war folglich unzulässig.

Mit dem öffentlichen Aushang des Hausverbots sind Daten zur Person des Betroffenen der Öffentlichkeit bekanntgegeben und somit im datenschutzrechtlichen Sinne an einen unbestimmten Personenkreis übermittelt worden. Nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG wäre dies nur zulässig gewesen, wenn es zur Wahrung berechtigter Interessen des Tankstellenpächters erforderlich gewesen wäre und kein Grund zu der Annahme bestanden hätte, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Veröffentlichung überwogen hätte. Diese Voraussetzungen waren nicht erfüllt.

Zur Durchsetzung des Hausrechts hätte es genügt, wenn lediglich der Betroffene persönlich über das Hausverbot informiert und im Übrigen darüber hinaus noch die Mitarbeiter der Tankstelle davon in Kenntnis gesetzt worden wären. Der öffentliche Aushang des Hausverbots war dazu nicht erforderlich. Wegen der mit dem Aushang des Hausverbots verbundenen Prangerwirkung und des großen Empfängerkreises ohne jegliches berechtigte Informationsinteresse war darüber hinaus auch von überwiegenden schutzwürdigen Interessen des Betroffenen auszugehen.

Der Tankstellenpächter hat dieser Bewertung schließlich zugestimmt und eine Wiederholung seinerseits ausgeschlossen.

Die vorstehende Bewertung bezieht sich ausschließlich auf den Aushang des Hausverbots. Ob das Hausverbot berechtigterweise ausgesprochen worden ist, habe ich ebenso wenig zu beurteilen wie den auslösenden nächtlichen Vorfall.

8.5.6 Personalausweis und Gesundheitskarte sind keine Pfandobjekte

Vor bereits mehr als vier Jahren, am 1. November 2010, ist das Gesetz über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften (BGBl. I 2009, S. 1346 ff.) in Kraft getreten, welches in Artikel 1 das novellierte Personalausweisgesetz enthält.

Bereits in meinem 5. TB habe ich unter Pkt. 4.3.15.1 darauf hingewiesen, dass nach dem neuen § 1 Abs. 1 Satz 3 PAuswG vom Ausweisinhaber nicht mehr verlangt werden darf, den Personalausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben.

Offensichtlich ist diese Vorschrift immer noch weitgehend unbekannt. Ich habe immer wieder verantwortliche Stellen darauf hinzuweisen, dass es jetzt unzulässig ist, den Personalausweis als Pfandobjekt zu verlangen. Beispiele dieser rechtswidrigen Praxis ließen sich viele aufzählen, stellvertretend seien die Ausleihe von Rollatoren, Audioguides, Schlittschuhen oder Bollerwagen genannt.

Auch die Hinterlegung der Gesundheitskarte sehe ich als unzulässig an. Aus den insoweit einschlägigen Vorschriften des § 28 Abs. 1 Satz 1 Nrn. 1 und 2 BDSG ergibt sich keine Zulässigkeit für eine auch nur temporäre Erhebung und Verarbeitung der auf der Karte enthaltenen (sensiblen) Versicherungsdaten. Die mit der Hinterlegung der Gesundheitskarte verbundene Verarbeitung personenbezogener Daten ist für den Zweck der Ausleihe nicht erforderlich, zudem stehen einer solchen Aufgabe des Gewahrsams schutzwürdige Betroffeneninteressen entgegen.

8.6 Sparkassen / Banken

8.6.1 Geldwechsel am Bankschalter

Der Kunde einer Sparkasse, die wegen § 2 Abs. 3 SächsDSG als öffentlich-rechtliches Kreditinstitut - wie jede andere Bank auch - die Vorschriften des Bundesdatenschutzgesetzes mit Ausnahme jener des zweiten Abschnitts anzuwenden hat, störte sich daran, dass am Schalter immer wieder die Information zu seiner Person erfasst wurde, wenn er 50-Euro-Scheine, die er zuvor aus dem Geldautomat gezogen hatte, unentgeltlich gegen kleinere Scheine wechselte. Auf seine schriftliche Nachfrage wurde ihm erklärt, dass der Vorgang „lediglich“ für die - nicht weiter konkretisierte - „transparente Gestaltung der internen Geschäftsprozesse erhoben“ werde und dem keine schutzwürdigen Interessen des Betroffenen im Sinne von § 28 Abs. 1 Satz 1 Nr. 2 BDSG entgegenstünden. Diese - kaum als Auskunft im Sinne von § 34 Abs. 1 Satz 1 BDSG zu wertende - Begründung war für mich nicht nachvollziehbar, ebenso wenig wie die Interessenabwägung oder weitere Begründungsversuche des Kreditinstituts. Ich habe der Sparkasse daher mitgeteilt, dass es aus meiner Sicht keiner vorgangsbezogenen Datenerhebung zur Person eigener Kunden bedarf, wenn diese - als solche bei dem Kreditinstitut identifiziert - von dem kostenlosen Service des Kreditinstituts Gebrauch machen, am Schalter größere Banknoten in kleinere zu wechseln, da

1. kein Fall von § 3 Abs. 2 Satz 1 Nr. 2 GwG vorliegt, dies also von Rechts wegen nicht geboten ist,

2. wegen der Entgeltfreiheit kein Verarbeitungserfordernis im Sinne von § 28 Abs. 1 Satz 1 Nr. 1 BDSG besteht und

3. schutzwürdige Interesse der Betroffenen am Ausschluss der Verarbeitung (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG) in Bezug auf etwaige Controlling- und Prozesssteuerungsinteressen der Sparkasse, so sie denn hier überhaupt berechtigt wären, jedenfalls solange überwiegen, wie der Kunde nicht

   a. Barbeträge über 1.000,00 € zu tauschen sucht oder

   b. im Einzelfall besondere Anhaltspunkte für eine Geldwäsche, einen etwaig (sonst) rechtswidrigen Kontext der Transaktion oder den (gewerblichen) Missbrauch des Serviceangebots bestehen, was allerdings dann (jeweils) - im Sinne der Revisionsfähigkeit des Verarbeitungshandelns - nachprüfbar zu dokumentieren wäre.

Dieser Sichtweise ist die Sparkasse - nach Rücksprache mit dem Sparkassenverband - dann auch gefolgt und hat ihre Praxis geändert.

8.6.2 Auskunft über Bankschließfächer an Sozialbehörde

Ein Leistungsbezieher, dem angelastet wurde, Vermögen, welches für die Gewähr seiner Sozialleistung bedeutsam war, verheimlicht zu haben, fragte mich, ob seine Hausbank der Sozialbehörde Mitteilungen über sein dortiges Bankschließfach tätigen durfte.

Ich habe ihm mitgeteilt, dass es entgegen seiner Auffassung kein absolutes „Bankgeheimnis“ gibt und dass nach § 60 Abs. 2 SGB II alle Stellen, also auch Kreditinstitute, die Guthaben eines Leistungsbeziehers führen oder dessen Vermögensgegenstände verwahren, der Agentur für Arbeit auf Verlangen hierüber sowie über das damit im Zusammenhang stehende Einkommen oder Vermögen Auskunft zu erteilen haben, soweit dies zur Durchführung der Aufgaben des Leistungsträgers, in seinem Fall zur Prüfung der Bedürftigkeit, erforderlich ist. Um Leistungsmissbrauch wirksam auszuschließen, hat der Gesetzgeber diese, aus meiner Sicht verfassungsrechtlich zulässige Mitwirkungs- bzw. Offenbarungspflicht geschaffen, welche die Informationsweitergabe als gesetzliche Übermittlungsbefugnis im Sinne von § 4 Abs. 1 BDSG rechtlich trägt.

8.6.3 Prüfpflichten eines Kreditinstituts beim Lastschrifteinzug

Es kommt hin und wieder vor, dass Lastschriften fehlerhaft, insbesondere auf ein falsches Konto bezogen, ausgeführt werden. Die Kontoinhaber können dagegen aber mit einem Widerspruch gegen die Lastschrift vorgehen und sich so die auf fälschliche oder auch unzulässige Weise abgebuchten Beträge wieder gutschreiben lassen.

Eine Bankkundin hatte für solch einen Vorfall überhaupt kein Verständnis. Für sie war es vollkommen unverständlich, wie jemand ohne ihre Ermächtigung auf ihr Konto hatte zugreifen können und dass die Bank überhaupt nicht mehr prüft, ob Kontoinhaber, Bankleitzahl und Kontonummer zusammenpassen.

Das in dem kurz geschilderten Fall zur Anwendung gekommene elektronische Lastschrifteinzugsverfahren ist ein bargeldloses Inkasso-Verfahren. Dabei erteilt der Zahlungsempfänger (Gläubiger) mit einem Lastschrift-Formular bzw. auf elektronischem Weg der Bank des Schuldners den Auftrag, einen bestimmten Betrag vom Konto des Schuldners abzubuchen und auf das Konto des Zahlungsempfängers zu überweisen. Voraussetzung dafür ist, dass der Schuldner dem Gläubiger eine Einzugsermächtigung gegeben hat. Diese Einzugsermächtigung liegt jedoch nur dem Zahlungsempfänger, nicht jedoch der ausführenden Bank vor. Die ausführende Bank kann deshalb auch die formelle und materielle Berechtigung einer Lastschrift nicht prüfen. Der Zahlungsempfänger versichert der Bank mit dem Einreichen des Lastschriftauftrages allerdings, dass ihm die dafür erforderliche Ermächtigung des Schuldners vorliegt. Die Interessen des Schuldners werden dadurch gewahrt, dass dieser das Recht hat, einer im Rahmen des Lastschrifteinzugsverfahrens erfolgten Abbuchung bis acht Wochen nach der Belastungsbuchung zu widersprechen. Bei einer nicht vorhandenen Einzugsermächtigung und damit einer unautorisierten Lastschrift beträgt die Widerspruchsfrist sogar 13 Monate.

Auch bei einer SEPA-Lastschrift liegt der Bank des Schuldners die Einzugsermächtigung nicht zur Prüfung vor. Die Widerspruchsfrist für autorisierte Lastschriften ist auch hier auf acht Wochen ab Belastungsdatum und für nicht autorisierte Belastungen auf 13 Monate festgelegt.

In den seit November 2009 in Deutschland geltenden neuen Banken-AGB ist im Übrigen festgelegt, dass bei Überweisungen nur noch Kontonummer und Bankleitzahl maßgeblich sind. Die gesetzliche Prüfungspflicht der Banken bei erkennbar falschen Angaben (Abweichung von Empfängername und Kontonummer) ist entfallen. Diese Änderung in den Banken-AGB geht auf die EU-Zahlungsdiensterichtlinie zurück, die eine Beschleunigung des Zahlungsverkehrs insbesondere ins Ausland zum Ziel hat. Weil aufgrund der kurzen Ausführungsfristen für Zahlungsvorgänge eine vollautomatische Verarbeitung der Transaktionsvorgänge erforderlich ist, sind Kreditinstitute nicht mehr verpflichtet, den Namen des Kontoinhabers und die Kontonummer auf ihre Plausibilität hin abzugleichen.

8.6.4 Abforderung neuer Ausweiskopien nach Ablauf des Gültigkeitsdatums

Ein Bankkunde wurde um eine aktuelle Kopie seines Personalausweises gebeten. Unter Verweis darauf, dass der Bank bereits eine Kopie seines - inzwischen allerdings

abgelaufenen - Ausweises vorliege, fragte mich der Bankkunde, ob dieses Verlangen mit den datenschutzrechtlichen Vorgaben in Einklang stünde.

Ich konnte den Schilderungen des Betroffenen keine Anhaltspunkte für eine Datenschutzverletzung entnehmen. Das erneute Identifizierungsverlangen seiner Bank stand im Einklang mit den Vorschriften des Geldwäschegesetzes.

Das Geldwäschegesetz verpflichtet Kreditinstitute zunächst bereits bei der Begründung einer Geschäftsbeziehung zur Identifizierung ihrer Vertragspartner (§ 3 Abs. 1 Nr. 1, Abs. 2 Nr. 1 GwG). Zur Überprüfung der Identität des Vertragspartners hat sich das Kreditinstitut dabei anhand eines gültigen amtlichen Lichtbildausweises zu vergewissern, dass die von diesem angegebenen Identifizierungsdaten zutreffend sind (§ 4 Abs. 4 Satz 1 Nr. 1 GwG). Hierüber sind entsprechende Aufzeichnungen anzufertigen, wozu auch die Art, die Nummer und die ausstellende Behörde des vorgelegten Ausweisdokuments gehören (§ 8 Abs. 1 Satz 2 GwG). Nach § 8 Abs. 1 Satz 3 GwG können diese Aufzeichnungen auch durch Anfertigung und Aufbewahrung einer Ausweiskopie erfolgen (vgl. 5. TB, Pkt. 4.3.15.5).

Im Fall, dass ein zu einem früheren Zeitpunkt zur Identifizierung eingesetzter Personalausweis inzwischen seine Gültigkeit verloren hat, sind Kreditinstitute auch berechtigt, von ihren Kunden eine aktuelle Ausweiskopie zu verlangen. Dies ergibt sich aus § 4 Abs. 6 GwG, wonach Kunden ihrem Kreditinstitut die zur Erfüllung ihrer Identifizierungspflichten notwendigen Informationen und Unterlagen zur Verfügung zu stellen und sich im Laufe der Geschäftsbeziehung ergebende Änderungen unverzüglich anzuzeigen haben.

8.7 Vereine / Verbände

8.7.1 Datenerhebung beim Verkauf von Gästetickets im Fußball

Das Thema Eintrittskartenverkauf bei Fußballspielen beschäftigt mich in verschiedenen Varianten immer wieder (vgl. dazu 5. TB, Pkt. 4.3.7.1 und 6. TB, Pkt. 8.7.1). Als Begründung für die in diesem Zusammenhang erfolgende Erhebung, Verarbeitung und Nutzung der Zuschauerdaten werden regelmäßig Sicherheitsbelange angeführt - man möchte auf diese Weise ausschließen, dass gewaltbereite Fans in den Besitz von Eintrittskarten bzw. ins Stadion gelangen. Ein tragfähiges Gesamtkonzept unter Berücksichtigung datenschutzrechtlicher Vorschriften war in den mir bekannt gewordenen Fällen allerdings bislang nicht erkennbar, so dass ich die Erhebung, Verarbeitung und Nutzung der Käufer- bzw. Zuschauerdaten jeweils beanstanden musste.

In dem mir dieses Mal vorgetragenen Fall soll ein Verein Gästekarten nur gegen Vorlage des Personalausweises und unter Erhebung personenbezogener Daten der Käufer verkauft haben. Dabei sei für den Käufer letztendlich unklar geblieben, welche Daten aus dem Ausweis tatsächlich erhoben und zu welchem Zweck durch wen verarbeitet worden sind bzw. werden sollten. Im Gegensatz dazu hätten Eintrittskarten für die Zuschauerblöcke der Heimmannschaft ohne eine solche Datenerfassung erworben werden können.

Ausgangspunkt für die vorgenommene Datenerhebung - so wurde mir vom Verein daraufhin mitgeteilt - seien Aufrufe von Fans anderer Vereine im Internet gewesen, zu dem betreffenden Heimspiel zu erscheinen und die Gastmannschaft zu unterstützen. Um erkennen zu können, ob polizeibekannte gewaltbereite Fans Karten erwerben und aus welchen Städten Fangruppen zu erwarten sind, sei in Absprache mit der Polizei beschlossen worden, Daten von Käufern von Gästekarten zu erheben. Von den Käufern der Eintrittskarten für den Gästeblock seien Name und Anschrift erhoben und auch an die Polizei weitergegeben worden.

Die Erhebung und Verarbeitung der Adressdaten der Käufer von Eintrittskarten für den Gästeblock ist unzulässig gewesen:

Nach § 4 BDSG sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Eine (schriftliche) Einwilligung der Käufer von Gästekarten hatte der gastgebende Verein nicht eingeholt. Eine andere Rechtsvorschrift ist nicht ersichtlich, so dass für die Zulässigkeitsbeurteilung nur das Bundesdatenschutzgesetz selbst zugrunde zu legen war. Von den Erlaubnistatbeständen des Bundesdatenschutzgesetzes kamen dabei nur § 28 Abs. 1 Satz 1 Nr. 1 oder 2 BDSG in Betracht.

§ 28 Abs. 1 Satz 1 Nr. 1 BDSG regelt, dass das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig ist, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen Schuldverhältnisses mit dem Betroffenen (hier: Kaufvertrag) erforderlich ist.

Da die Käufer die Tickets an der Vorverkaufskasse sofort persönlich ausgehändigt bekommen haben, wurden deren Adressdaten im Rahmen des Ticketverkaufs nicht benötigt, d. h. aus § 28 Abs. 1 Satz 1 Nr. 1 BDSG ergab sich insoweit keine Berechtigung zur Erfassung von Käuferdaten.

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

Als berechtigtes Interesse hatte der gastgebende Verein angegeben, dass man damit habe erkennen wollen, ob polizeibekannte und möglicherweise gewaltbereite Fans Karten erwerben, und auch, dass man einen Überblick darüber habe erhalten wollen, aus welchen Städten (gewaltbereite) Fangruppen zu erwarten sind, die sich möglicherweise dem im Internet verbreiteten Aufruf zur Unterstützung der Gastmannschaft anschließen könnten.

Für diese Zwecke war die Erhebung der Käuferdaten jedoch gleichfalls nicht erforderlich. Zunächst fehlt es schon an der Eignung der Käuferdaten, um die genannten Zwecke zu erreichen, denn wie dargestellt war von Interesse, woher die Zuschauer kommen und nicht die Käufer der Karten. Angaben zum Käufer von Gästekarten erlauben keine verlässlichen Aussagen zu den Personen, die die Eintrittskarten dann tatsächlich nutzen. Die Erhebung von Name und kompletter Anschrift war im Übrigen - unter Zurückstellung der gerade erfolgten Überlegungen - auch unter dem Aspekt der Verhältnismäßigkeit nicht erforderlich, denn für die Bestimmung der Herkunftsorte wäre es in jedem Fall ausreichend gewesen, lediglich den Wohnort des Käufers zu erfassen.

Im Weiteren hat die Erfassung der Käuferdaten aber auch deren schutzwürdige Interessen verletzt. Käufer von Gästetickets müssen es nicht hinnehmen, als potentiell gefährlich eingestuft zu werden und deshalb anders als alle anderen Zuschauer nur gegen Preisgabe ihrer Anschriftendaten Tickets kaufen zu können.

Aus der Unzulässigkeit der Speicherung folgt unmittelbar auch die Pflicht zur Löschung der gespeicherten Käuferdaten (vgl. § 35 Abs. 2 Satz 2 Nr. 1 BDSG).

Es reicht davon abgesehen auch nicht aus, die Kartenkäufer lediglich auf Nachfrage über den Zweck der Datenerhebung, -verarbeitung und -nutzung und über vorgesehene Empfänger (hier: Polizei) zu informieren. Der gastgebende Verein hätte an dieser Stelle von sich aus über diese Punkte informieren und dabei auch klarstellen (lassen) müssen, dass der Verein selbst insoweit verantwortliche Stelle ist und nicht etwa die Stadionbetreibergesellschaft (bzw. deren Vorverkaufsstelle).

8.7.2 Unterrichtung anderer Fußballvereine über bestehende Hausverbote

Noch einmal geht es um Fußball und um die Frage der Gewährleistung der Sicherheit bzw. der Verhinderung von Fan-Ausschreitungen.

Ein Fußballverein, der ständig Probleme mit den eigenen Ultras hatte (es bestanden gegen deren Mitglieder schon in zehn Fällen Hausverbote), wollte verhindern, dass diese Fans bei einem Fußballspiel ohne Beteiligung der eigenen Mannschaft „kleinere Auseinandersetzungen und Beleidigungen“ provozieren, da dies auf den eigenen Verein dann wieder zurückfallen könnte. Den Grund für diese Vermutung bildete eine Fanfreundschaft zwischen den eigenen Ultras und den Fans einer der beiden gegeneinander spielenden Mannschaften. Beabsichtigt war daher, die ausgesprochenen Hausverbote an die Gastgebermannschaft zu übermitteln und auf diese Weise zu verhindern, dass die betreffenden Personen überhaupt erst in die Spielstätte gelangen. Nach dem Spiel sollten die Daten sofort wieder gelöscht werden.

Ich habe dem Verein dazu Folgendes mitgeteilt:
Das Hausrecht beinhaltet die Befugnis, darüber zu entscheiden, wer bestimmte Gebäude oder befriedetes Besitztum betreten und darin verweilen darf. Inhaber des Hausrechts sind daher grundsätzlich befugt, die zum Schutz des Objekts bzw. zur Abwehr des unbefugten Betretens erforderlichen Maßnahmen zu treffen und insoweit auch Hausverbote auszusprechen. Die diesbezüglichen Anforderungen sind insoweit also vergleichsweise niedrig anzusetzen.

Das Hausverbot und damit auch die Befugnis, Hausverbote auszusprechen, enden jedoch grundsätzlich an der Grundstücksgrenze. Eine Befugnis, Informationen über die betroffenen Personen an andere Stellen zu übermitteln, ergibt sich daraus nicht, insbesondere stellen ausgesprochene Hausverbote keine Rechtsgrundlage für eine Übermittlung dar. In Frage käme insoweit allenfalls die Vorschrift des § 28 Abs. 1 Satz 1 Nr. 2 BDSG, die eine Abwägung der berechtigten Interessen des Hausrechtsinhabers mit den schutzwürdigen Interessen der Betroffenen beinhaltet. Dabei muss die Übermittlung aber auch erforderlich sein, um den dargestellten Zweck zu erreichen. Insoweit war es schon zweifelhaft, ob der Gastgeberverein ohne nähere eigene Kenntnis der Personen überhaupt in der Lage gewesen wäre, diese bei den Einlasskontrollen zu identifizieren, denn dies würde wohl mindestens entsprechende Ausweiskontrollen voraussetzen. Unabhängig davon bestand jedoch auch Grund zur Annahme überwiegender schutzwürdiger Betroffeneninteressen, denn es kann nicht ohne weiteres davon ausgegangen werden, dass sich die Betroffenen im gegnerischen Stadion nicht im Wesentlichen friedfertig verhalten, sondern stattdessen

möglicherweise Straftaten begehen. Die bloße Möglichkeit „kleinerer Auseinandersetzungen“, die im Fußball immer wieder vorkommen, reicht insoweit als Rechtfertigung einer Übermittlung nicht aus.

Eine Weitergabe der Daten über die ausgesprochenen Hausverbote an den Gastgeberverein wäre daher unzulässig gewesen.

8.7.3 Öffentlicher Aushang säumiger Beitragsschuldner eines Turnvereins

Der Vorstand eines Turnvereins hatte beschlossen, am sogenannten „Schwarzen Brett“ im Eingangsbereich der von ihm genutzten Turnhalle eine regelmäßig aktualisierte Liste von Vereinsmitgliedern auszuhängen, die fällige Vereinsbeiträge nicht gezahlt hatten. Ziel war es, so Einfluss auf die Zahlungsmoral zu nehmen.

Auf den Hinweis eines Vereinsmitgliedes habe ich den Sachverhalt vor Ort von der Polizei in Amtshilfe im Wege der Nachschau prüfen und dokumentieren lassen. Rechtlich habe ich den Vorgang dann wie folgt bewertet:

Aushänge eines Vereins in einer Vereinssportanlage stellen datenschutzrechtlich (zunächst) eine Übermittlung an die Gemeinschaft der Vereinsmitglieder dar. Ist der Bereich des Aushangs auch für andere Personen (z. B. Gäste, Mitbenutzer oder Reinigungspersonal) zugänglich, steht auch die Übermittlung an weitere - vereinsfremde - Personen in Rede, ungeachtet dessen, ob die Mitteilung allein oder in erster Linie für Vereinsmitglieder bestimmt ist.

Wenn keine Einwilligung der betroffenen Vereinsmitglieder vorliegt, dass bestimmte Angaben zu ihrer 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 Vereines an der Mitteilung besteht, dem kein schutzwürdiges Interesse des Betroffenen entgegensteht. Typische zulässige Aushänge eines Sportvereins sind hiernach beispielsweise Aushänge zu Wettkampfergebnissen, Mannschaftsaufstellungen 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. Das Persön-

lichkeitsrecht der Betroffenen überwiegt in diesem Fall grundsätzlich jedes Mitteilungsinteresse des Vereins, denn mit dem öffentlichen Anprangern vermeintlicher oder tatsächlicher Außenstände als Mittel der Beitreibung oder als Präventionsmaßnahme zur Verbesserung der allgemeinen Zahlungsmoral soll ein sozialer Druck jenseits der Grenzen gesetzlich erlaubter Instrumente zum Einzug finanzieller Forderungen aufgebaut bzw. genutzt werden.

Da der Vereinsvorstand den Aushang nach meinem Tätigwerden sofort entfernte, bestand für mich keine Notwendigkeit mehr, dies noch förmlich anordnen zu müssen. Der Verein hat für das Handeln seines Vorstandes eine - des gemeinnützigen Vereinszwecks wegen - geringe Geldbuße bezahlen müssen (vgl. Pkt. 11.2).

8.7.4 Aushang von Mitgliederlisten zwecks Zutrittskontrolle

In einem für Vereinsmitglieder und Gäste zugänglichen Schaukasten eines Sportvereins befand sich ein Aushang mit personenbezogenen Daten der Abteilung Kraftsport. Von einem Vereinsmitglied, das dies nicht länger hinnehmen wollte, wurde mir berichtet, dass dazu alle Mitglieder der Abteilung per Vorstandsbeschluss genötigt worden seien, ein Passfoto abzugeben, welches zusammen mit Name, Vorname, Eintritts- und Geburtsdatum sowie Funktion in Listenform im Schaukasten ausgehängt worden sei.

Den Angaben des Vereins zufolge diente der jährlich aktualisierte Aushang Kontrollzwecken des Vorstandes und der Mitglieder untereinander. Da sich nicht alle Sportfreunde persönlich kennen würden und die Nutzung des Kraftsportraums auch individuell, d. h. ohne Aufsicht außerhalb einer Übungsgruppe, gewährleistet werden sollte - hierfür waren mehrere Schlüssel im Umlauf, die die Mitglieder auch untereinander weitergeben konnten -, wäre dies als Möglichkeit gesehen worden, sich unbefugt in den Vereinsräumlichkeiten aufhaltende Personen zu erkennen und ggf. aus den Räumlichkeiten zu verweisen (vgl. dazu auch die Problematik der Videoüberwachung des Kraftsportraums: Pkt. 8.1.10).

Die Veröffentlichung der Mitgliederdaten der Vereinsabteilung Kraftsport ist unzulässig gewesen. Der Vorstand hat diesen Aushang nach meiner diesbezüglichen Mitteilung sofort entfernt.

Ein Verein darf nach § 4 Abs. 1 BDSG personenbezogene Daten seiner Mitglieder nur erheben, verarbeiten oder nutzen, wenn eine Vorschrift dieses Gesetzes oder eine sonstige Rechtsvorschrift dies erlaubt oder soweit der Betroffene eingewilligt hat. Als Rechtsvorschrift kommt hier in erster Linie § 28 Abs. 1 Satz 1 Nr. 1 BDSG (Zweckbestimmung eines Vertragsverhältnisses) in Betracht. Die Mitgliedschaft in einem Verein ist als Vertragsverhältnis zwischen den Mitgliedern und dem Verein anzusehen, dessen Inhalt im

Wesentlichen durch die Vereinssatzung vorgegeben wird. Mitgliederdaten dürfen dabei grundsätzlich nur zur Verfolgung des Vereinszwecks bzw. zur Betreuung und Verwaltung von Mitgliedern erhoben, verarbeitet und genutzt werden.

Die Bekanntgabe der oben aufgeführten Mitgliederdaten in einem Schaukasten stellt eine Übermittlung (an Gäste bzw. andere Vereinsmitglieder) im Sinne von § 3 Abs. 4 Nr. 3 BDSG dar, die weder zur Verfolgung des Vereinszwecks noch zur Betreuung und Verwaltung der Vereinsmitglieder erforderlich und damit nicht durch § 28 Abs. 1 Satz 1 Nr. 1 BDSG gedeckt, mithin also unzulässig gewesen ist.

8.7.5 Nachweis der Bedürftigkeit bei der Ausgabe kostenloser Lebensmittel

Eine als Verein organisierte private karitative Einrichtung gab kostenlos Lebensmittel, die sie zuvor vom Einzelhandel als Spende erhalten hatte, an örtliche Bedürftige aus. Um jedoch in den Genuss der freiwilligen sozialen Leistung zu kommen, mussten Hilfesuchende aktuelle behördliche Sozialleistungsbescheide vorlegen, die von der Einrichtung kopiert und zu den dortigen Unterlagen genommen wurden. An letzterem störte sich jedoch eine Hilfesuchende, die meine Behörde um Prüfung bat.

Ihr und dem Verein habe ich mitgeteilt, dass die Daten Hilfesuchender wegen der Gewähr einer Leistung - hier der Ausgabe von Lebensmitteln an einkommensschwache Personen - jedoch nur insoweit erhoben, verarbeitet und genutzt werden dürfen, wie dies für die Feststellung der Bedürftigkeit und der (sonstigen) Einhaltung der Hilfskriterien des Helfenden erforderlich ist (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Aktuelle Bescheide öffentlicher Leistungsträger sind zwar ein tauglicher Nachweis eines finanziellen Unterstützungsbedarfs. Allerdings reicht zur Prüfung in der Regel eine Einsichtnahme in derartige Dokumente aus. Zu Dokumentationszwecken nicht erforderlich ist hingegen die Fertigung und der Einbehalt von Ablichtungen, da die Hilfseinrichtung zur Person des Bedürftigen in ihren Unterlagen hinreichend vermerken kann, wann welches Dokument welchen Datums welcher Behörde mit welcher zeitlichen Gültigkeit und welcher Aussage zur Glaubhaftmachung der Bedürftigkeit vorgelegt wurde, zumal bei einer Ablichtung der Bescheide regelmäßig eine Vielzahl weiterer Daten erhoben wird, die jedenfalls der Lebensmittelausgabe wegen nicht benötigt werden.

Auf mein Tätigwerden hin hat die verantwortliche Stelle ihre bisherige Praxis geändert. Künftig wird nur noch in einem Formular festgehalten, wodurch der Nachweis erbracht wurde. Bereits erhobene Ablichtungen wurden vernichtet.

8.8 Handels- und Wirtschaftsauskunfteien / Inkassobüros

8.8.1 Überprüfung des berechtigten Abrufinteresses bei Auskunftsempfängern

§ 29 Abs. 2 Satz 5 BDSG regelt, dass Wirtschaftsauskunfteien das Vorliegen eines berechtigten Interesses bei den Auskunftsempfängern im Stichprobenverfahren einzelfallbezogen festzustellen und zu überprüfen haben.

Im Rahmen einer Überprüfung einer Wirtschaftsauskunftei bin ich darauf hingewiesen worden, dass es Unternehmen gibt, die in diesem Zusammenhang der Wirtschaftsauskunftei die Vorlage von Unterlagen (in Kopie), aus denen sich das berechtigte Abrufinteresse ergibt, verweigern.

Zur Rechtslage ist Folgendes auszuführen:
Eine Überprüfung des berechtigten Abfrageinteresses erfordert in der Regel die Vorlage von Dokumenten; lediglich ausnahmsweise und nur unter besonderen Umständen kann eine schlichte Erklärung des Datenempfängers ausreichen. Nur so kann die übermittelnde Stelle ihren gesetzlichen Pflichten tatsächlich vollumfänglich nachkommen und in substantiierter Weise das Vorliegen eines berechtigten Abfrageinteresses feststellen und überprüfen. Eine bloße Bestätigung des Auskunftsempfängers darüber, dass ein berechtigtes Interesse vorgelegen hat, wiederholt nur die bereits bei Anforderung der Auskunft erfolgte glaubhafte Darlegung des berechtigten Interesses und ist daher insoweit ebenso wenig ausreichend wie eine gleichlautende Bestätigung des Datenschutzbeauftragten des Auskunftsempfängers. Nach dem Gesetzeswortlaut hat nicht der Datenempfänger das Vorliegen eines berechtigten Interesses einzelfallbezogen festzustellen, sondern die übermittelnde Stelle. Soweit Datenempfänger entsprechende Auskünfte oder Unterlagen aus Datenschutzgründen mit Verweis auf bestehende Verschwiegenheitspflichten verweigern, ist dem entgegenzuhalten, dass es sich dabei um eine gesetzliche Vorgabe handelt. Würde man einer solchen Argumentation folgen, hätte der Auskunftsempfänger zudem schon mit der Anfrage bei der Wirtschaftsauskunftei gegen diese Verschwiegenheitspflichten verstoßen, denn schon dadurch werden Informationen über das Bestehen einer Geschäftsverbindung mit dem Betroffenen bzw. das Interesse an einer solchen übermittelt.

Diese Auffassung ist mit den Datenschutzaufsichtsbehörden der anderen Bundesländer abgestimmt. Soweit sich in den mir mitgeteilten Fällen sächsische Unternehmen geweigert hatten, der betreffenden Wirtschaftsauskunftei entsprechende Unterlagen vorzulegen, habe ich mich direkt an diese gewandt; in den verbleibenden Fällen habe ich die jeweils zuständige Aufsichtsbehörde informiert.

8.8.2 Datenweitergabe an Inkassodienstleister bei bestrittener Forderung

Darf ein Unternehmer die Daten eines Schuldners zum Zweck der Beitreibung an einen Inkassodienstleister übermitteln, wenn dieser die Forderung bestritten hat, ein Zahlungsanspruch also möglicherweise gar nicht besteht?

Die Inanspruchnahme eines registrierten Inkassounternehmens zur Einziehung einer Forderung ist eine nach dem Rechtsdienstleistungsgesetz gestattete außergerichtliche Rechtsdienstleistung (§§ 2 Abs. 2, 10 Abs. 1 Satz 1 Nr. 1 RDG). Datenschutzrechtlich erlaubt dabei § 28 Abs. 1 Satz 1 Nr. 2 BDSG die Übermittlung der Daten eines auch nur vermeintlichen Schuldners an einen Inkassodienstleister, denn schon das (jedenfalls nicht völlig willkürliche) Behaupten bzw. Geltendmachen einer Forderung mittels eines Rechtsdienstleisters ist ein berechtigtes (rechtliches) Interesse an einer zunächst außergerichtlichen Klärung des Schuldverhältnisses, das dem Interesse auch des nur vermeintlichen Schuldners an einem Ausschluss der Übermittlung vorgeht, da dieser sich der Forderung rechtlich erwehren und eine abschließende Klärung des zivilrechtlichen Anspruchs ohnehin nur gerichtlich herbeigeführt werden kann. Mithin handelt es sich bei dem mir vorgetragenen Sachverhalt um eine außerhalb des Datenschutzrechtes liegende zivilrechtliche Vorfrage, die von der Datenschutzaufsichtsbehörde nicht mit Wirkung für die Parteien beantwortet werden kann.

8.9 Wohnungswirtschaft

8.9.1 Werbung an WEG-Mitglieder nach Verkauf einer Wohnung

Ein Immobilienmakler war mit dem Verkauf einer Wohnung beauftragt worden und hatte in diesem Zusammenhang Kenntnis der Anschriften aller WEG-Mitglieder erlangt. Nach erfolgreichem Verkauf der Wohnung hatte er sich dann an alle Wohnungseigentümer gewandt und auch ihnen für den Fall einer Verkaufsabsicht seine Dienst angeboten. Mir ist der Fall bekanntgeworden, weil sich einer der Miteigentümer gewundert hatte, dass der Makler seine Adresse kannte. Im Rahmen eines zunächst (bis zu meiner Einbeziehung) erfolglosen Auskunftsersuchens nach § 34 BDSG wollte er von dem Makler wissen, woher er seine Adresse hatte.

Ich habe diese Verarbeitung und Nutzung der personenbezogenen Daten der verbleibenden WEG-Mitglieder als rechtswidrig bewertet:

Nach § 28 Abs. 3 Satz 1 BDSG ist die Verarbeitung und Nutzung personenbezogener Daten für Werbezwecke zulässig, soweit der Betroffene eingewilligt hat. Eine solche Einwilligung hatte dem Makler ersichtlich nicht vorgelegen, denn dann wäre es gar nicht erst zu der Auskunftsforderung des Betroffenen gekommen.

Nach § 28 Abs. 3 Satz 2 Nr. 1 BDSG ist die Verarbeitung und Nutzung personenbezogener Daten für Werbezwecke darüber hinaus auch zulässig, wenn diese Daten im Rahmen eines Vertragsverhältnisses direkt bei den Betroffenen oder aus allgemein zugänglichen Adress-, Rufnummern-, Branchen- oder vergleichbaren Verhältnissen erhoben worden sind. Diese Voraussetzungen lagen hier aber gleichfalls nicht vor. Stattdessen waren diese Daten von einem Miteigentümer erhoben worden.

8.9.2 Elektronische Müllschleuse

Ein Ehepaar wurde von seinem Vermieter abgemahnt, weil es auffällig wenig Restmüll über die Restmüllschleuse seiner Wohnanlage entsorgt haben soll, was für den Vermieter zwingend bedeutete, dass seine Mieter - um Kosten zu sparen - ihren Müll wohl anderweitig und sicherlich rechtswidrig entsorgten; er forderte sie daher unter Erinnerung ihrer miet- und abfallrechtlichen Pflichten zu einer Verhaltensänderung auf. Auf die Nachfrage des Paares, das den Vorwurf vehement zurückwies, woher er denn wisse, wieviel Restmüll jeder Haushalt der Mehrparteienanlage über die hauseigene Müllschleuse entsorge, teilte er ihnen mit, dass der elektronische Chip, den jede Wohnung zur Öffnung der Müllschleuse besitze, die zeitliche Erfassung jeder Müllschüttung erlaube und in ihrem Fall die Auswertung der Häufigkeit und zeitlichen Abstände der Entsorgung deutlich von dem anderer, vergleichbarer Haushalte abweiche. Über die Behauptung und Datenverarbeitung ihres Vermieters entsetzt, bat mich das betroffene Paar um eine datenschutzrechtliche Prüfung des Vorgangs.

Ihnen und dem Vermieter habe ich nach Prüfung des Sachverhalts mitgeteilt, dass eine Datenverarbeitung allenfalls in dem Umfang zulässig ist, wie die Daten zur Berechnung der Kostenumlage des Müllsystems auf die jeweiligen Mietparteien benötigt werden (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Werden die Daten aber (zweckgeändert) auch für die Ermittlung etwaigen Fehlverhaltens, hier einer vermuteten Fehlentsorgung von Restmüll, genutzt, halte ich dies jedoch schon allein deshalb für unzulässig, weil die Zahl der Schüttungen nicht den Nachweis rechtswidriger Entsorgung bringen kann. Es mag zwar sein, dass derjenige, der lediglich wenige Schüttungen tätigt, seinen Müll zum Schaden der Hausgemeinschaft oder Allgemeinheit fehlerhaft entsorgt. Den Beweis dafür kann der Vermieter aber über das Ergebnis dieser Datenverarbeitung keinesfalls rechtssicher führen, denn möglicherweise hat gerade jener Mieter, dessen Entsorgungsverhalten auf den ersten Blick atypisch erscheint, solche Maßnahmen zur Müllvermeidung erfolgreich getätigt, zu denen das System erziehen will. Im Datenschutzrecht gilt: Ist eine Datenverarbeitung untauglich, den ihr zugrundeliegenden Zweck zu erreichen, ist sie weder erforderlich, noch verfolgt sie ein berechtigtes Interesse (§ 28 Abs. 1 Satz 1 Nr. 2 BDSG), so dass sie - ohne Einwilligung der Betroffenen - stets unzulässig ist.

Unter Hinweis auf die Rechtslage war der Vermieter schließlich auch bereit, künftig von einer Nutzung der Abrechnungsdaten (Schüttungen) zur Aufklärung (vermeintlich) rechtswidriger Entsorgung abzusehen.

8.9.3 Weitergabe von Mieterdaten an potentielle Immobilienkäufer

Die mir mitgeteilte Weitergabe von Mieterdaten (Name, Vorname, Zimmer-Nummer, Zimmerfläche, Miethöhe, Kaution, Zahlungsrückstand) eines als Studentenwohnheim genutzten Gebäudes durch einen Immobilienmakler an potentielle Käufer der Immobilie war infolge Verstoßes gegen die §§ 4, 28 BDSG unzulässig.

Die vorstehend genannten personenbezogenen Daten waren dem Makler vom Studentenwerk (Verkäufer) übergeben und von ihm anschließend gespeichert und an potentielle Kaufinteressenten übermittelt worden. Nach § 4 Abs. 1 BDSG ist eine Verarbeitung personenbezogener Daten aber nur zulässig, soweit das Bundesdatenschutzgesetz selbst oder eine andere Rechtsvorschrift dies erlaubt oder die Betroffenen eingewilligt haben. Diese Voraussetzungen lagen hier nicht vor.

Soweit der Makler mir gegenüber die Auffassung vertreten hatte, dass er darauf vertrauen durfte, dass die Übermittlung der Mieterdaten durch das Studentenwerk im Vorfeld mit den Betroffenen abgestimmt worden war, stellte dies zunächst einmal keine Erlaubnis für eine weitergehende Übermittlung durch ihn selbst dar. Dessen ungeachtet war es zweifellos lebensfremd anzunehmen, dass ein Verkäufer im Zuge des Verkaufes einer Immobilie von seinen mehr als 200 Mietern eine (schriftliche - vgl. § 4a BDSG) Einwilligung zur Übermittlung ihrer Daten einholt bzw. sich überhaupt mit ihnen diesbezüglich abstimmt. Der Makler hätte sich dieser Einwilligungen also entsprechend vergewissern müssen.

Auch mit § 28 BDSG ließ sich die Verarbeitung der Mieterdaten nicht rechtfertigen. Als Erlaubnistatbestand in Betracht kam insoweit allenfalls § 28 Abs. 1 Satz 1 Nr. 2 BDSG: Danach ist eine Datenverarbeitung zulässig, soweit sie zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Mieter am Ausschluss der Verarbeitung überwiegt. Vorliegend mangelte es aber schon an der Erforderlichkeit der Übermittlung. Der Makler hätte die Kaufinteressenten auch ohne Angabe personenbezogener Daten der Mieter über die wesentlichen Eigenschaften der Immobilie und die Renditeerwartungen informieren können. Die Mietverträge als solche hätten auch als Mustermietverträge bzw. in anonymisierter Form bereitgestellt werden können und auch die nach Ausführungen des Maklers notwendigen Informationen über die Zusammensetzung der Mieterschaft (sowie über die aktuell erzielten Mieteinkünfte) hätten in Übersichtsform (Beschränkung auf Zahlenangaben) dargestellt werden können. Einer Übermittlung personenbezogener Mieterdaten

hat es hierzu nicht bedurft; sie ließ sich auch nicht wie behauptet aus den allgemein gehaltenen Formulierungen des vorgelegten Maklervertrages ableiten bzw. damit rechtfertigen. Einer Datenübermittlung an Kaufinteressenten standen darüber hinaus auch schutzwürdige Interessen der Mieter entgegen. Deren informationelles Selbstbestimmungsrecht ist verletzt, wenn Angaben über ihr Mietverhältnis ohne ihr Wissen an ihnen der Anzahl und der Person nach unbekannte potentielle Käufer verteilt werden. Sie werden dadurch unnötig Risiken durch die weitere, von ihnen nicht kontrollierbare Verarbeitung und Nutzung ihrer Daten bei den Kaufinteressenten ausgesetzt und haben zudem mangels Kenntnis der Datenempfänger einerseits wie der Datenübermittlung überhaupt andererseits diesbezüglich auch keinerlei Handlungsmöglichkeit.

8.9.4 Feststellung von Abstimmungsergebnissen bei WEG-Versammlungen

Das Mitglied einer WEG mit insgesamt 96 Eigentümern war mit den Modalitäten der Ermittlung der Abstimmungsergebnisse bei den WEG-Versammlungen nicht einverstanden. Das diesbezügliche Verfahren schilderte er mir wie folgt: Jedem Eigentümer würden zu Beginn der Versammlung Abstimmungszettel überreicht, die mit Vor- und Zunamen und der Wohnungsnummer gekennzeichnet seien. Der Eigentümer könne dann seine Kreuze bei ja, nein oder bei Enthaltung machen. Die Ergebnisse würden in einen Computer eingegeben und anschließend sofort bekannt gegeben. Damit ergebe sich eine Gesamtübersicht, welcher Eigentümer zu welchem Tagesordnungspunkt welche Position eingenommen habe. Dies sei nicht etwa geheim, sondern würde von der Hausverwaltung in einer Liste dokumentiert. Mit seinem Datenschutzverständnis wäre das jedenfalls nicht zu vereinbaren.

Angesichts dessen, dass es sich im konkreten Fall um eine vergleichsweise große Eigentümergemeinschaft gehandelt hat und die Miteigentumsanteile nicht gleichmäßig auf die Eigentümer verteilt waren, wäre es bei Abstimmungen mittels Handzeichens sehr schwierig bis unmöglich gewesen, das Abstimmungsergebnis korrekt und für die Eigentümer nachvollziehbar festzustellen. Ich habe daher keine Einwände, wenn hier entsprechende Hilfsmittel - in diesem Fall eigentümerbezogene Stimmzettel zur Einarbeitung in eine Abstimmliste mit automatisierter Feststellung des Abstimmergebnisses - zum Einsatz kommen, zumal dieser Modus der Ausübung des Stimmrechts vorher bekanntgegeben und über einen Beschluss der Versammlung abgesichert war.

Die weitere Aufbewahrung der Abstimmliste zu Dokumentations- und Transparenzzwecken habe ich jedoch nur eingeschränkt für zulässig erachtet und zwar nur solange, wie gegen formell-rechtliche Fehler bei der Beschlussfassung noch vorgegangen werden kann. Als insoweit maßgebliche Frist ist die für Beschlussanfechtungen in § 46 WEG festgelegte Monatsfrist anzusehen. Danach muss eine Beschlussanfechtung binnen eines

Monats seit Beschlussfassung gerichtlich geltend gemacht werden. Die Monatsfrist beginnt dabei mit dem Tag der Beschlussfassung, also derjenigen Eigentümerversammlung, auf welcher der Beschluss gefasst worden ist.

Vom Verwalter ist vorgetragen worden, dass eine diesbezügliche Klage anschließend innerhalb von zwei weiteren Monaten begründet werden müsse. Erfolgt keine Begründung durch den Kläger, würde die Klage durch das Amtsgericht nicht weiter bearbeitet. Der Verwalter erhalte erst eine Nachricht, wenn die Klage auch begründet worden ist. Im Ergebnis habe ich eine Speicherung der Abstimmungsliste über einen Zeitraum von maximal sechs Monaten, im Fall einer Klage natürlich bis zum Abschluss des Klageverfahrens, als zulässig bewertet. Darüber hinaus besteht keine Notwendigkeit mehr, das Abstimmverhalten bzgl. eines nicht mehr angreifbaren Beschlusses noch weiter personenbezogen zu dokumentieren.

Der Beschwerdeführer war mit diesem Ergebnis überhaupt nicht einverstanden und hielt mir anschließend noch vor, dass schließlich auch bei Bundestagswahlen neutrale Stimmzettel verwendet würden und keine namentliche Erfassung der Wähler erfolge. Dabei hatte er allerdings übersehen, dass offene Beschlussfassungen in Wohnungseigentümergemeinschaften oder anderen Gremien entgegen seiner Ansicht keinesfalls mit (geheimen) Wahlen gleichzusetzen sind.

8.9.5 Abforderung von Personalausweiskopien durch Makler und Vermieter

Mir ist ein Hinweis gegeben worden, dass ein Immobilienunternehmen im Zuge der Vermietung von Wohnungen auch Personalausweiskopien von den Mietinteressenten einfordert. Auf ihre Rückfragen hätten Mietinteressenten dabei die Antwort erhalten, dass „bei Mietschulden der Anwalt nach einer Ausweiskopie frage“ oder dass man „die Kopie für eine Schufa-Abfrage benötige“.

Nachdem ich dies der verantwortlichen Stelle vorgehalten hatte, hat sich diese darauf berufen, dass Personalausweiskopien von den jeweiligen Auftraggebern bzw. Eigentümern der von ihr verwalteten Objekte gefordert würden und dies in der Wohnungswirtschaft absolut üblich, mithin gängige Praxis sei. Zudem sei in den Mieterselbstauskünften und in den Mietverträgen eine entsprechende Einwilligungserklärung enthalten.

Es kann dahinstehen und bedarf daher keiner weiteren Erörterung, ob die Abforderung von Ausweiskopien tatsächlich wie von der verantwortlichen Stelle behauptet allgemein gängige Praxis in der Wohnungswirtschaft ist, denn dies ändert nichts an der Rechtswidrigkeit einer solchen Verfahrensweise.

Das Personalausweisgesetz bestimmt in seinem § 20 Abs. 1, dass der Inhaber den Ausweis bei nicht-öffentlichen Stellen als Identitätsnachweis und Legitimationspapier verwenden kann. Da bei einer Ausweiskopie aber eine Vielzahl von für die Identifizierung nicht erforderliche Daten erhoben, verarbeitet und genutzt werden, verstößt die Anfertigung von Personalausweiskopien jedenfalls im direkten Kundenkontakt, d. h. immer dann, wenn eine Identifizierung des Kunden durch eine direkte Einsichtnahme in den Ausweis des Kunden und den Abgleich der Ausweisdaten mit den zuvor erhobenen Kundendaten möglich ist, gegen § 28 Abs. 1 Satz 1 Nrn. 1 und 2 BDSG und ist damit unzulässig. Den Interessen eines Vermieters ist Genüge getan, wenn die Angaben des Mietinteressenten bzw. des zukünftigen Mieters durch Einsichtnahme in den Personalausweis überprüft werden und der Umstand der Überprüfung dokumentiert wird.

Dies ist einhellige Auffassung der Aufsichtsbehörden aller Bundesländer. Ich verweise dazu auch auf die gemeinsame Orientierungshilfe der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 27. Januar 2014 zur Einholung von Selbstauskünften bei Mietinteressenten (vgl. Pkt. 14.2.1).

Auch eine Einwilligung kann die Anfertigung von Personalausweiskopien nicht legitimieren, denn nach § 4a Abs. 1 Satz 1 BDSG erfordert eine wirksame Einwilligung die freie Entscheidung des Betroffenen. Eine solche Wahlfreiheit wäre aber nur dann gegeben, wenn der Abschluss eines Mietvertrags auch ohne eine Personalausweiskopie möglich wäre. Dies war aber weder nach den Ausführungen des Maklers - dies sei eine Vorgabe seiner Auftraggeber - noch nach der Formulierung der diesbezüglichen Klausel in den Selbstauskunftsbögen bzw. Mietverträgen anzunehmen und entspräche im Übrigen wohl auch nicht der Lebenswirklichkeit. Für die Mietinteressenten bestünde damit eine Drucksituation, in welcher keine freiwillige Erklärung zustande kommen kann. Im Ergebnis ist also die Abforderung bzw. Anfertigung von Personalausweiskopien von Mietbewerbern unter datenschutzrechtlichen Gesichtspunkten in jedem Fall unzulässig.

8.10 Schulen / Kindertagesstätten

8.10.1 Biometrische Essensausgabe in einer Schule

Ein rechtlich selbständiger Kantinenbetreiber einer Privatschule wollte die Schulspeisung künftig nur noch auf Grundlage einer biometrischen Authentifikation mittels Fingerprint, also elektronischem Fingerabdruck, durchführen. Hiervon versprach er sich eine zügigere Ausgabe und Abrechnung der Speisen. Dies erregte allerdings - zu Recht - den Unmut datenschutzrechtlich besorgter Eltern.

Ihnen, der Schule und dem Kantinenbetreiber habe ich mitgeteilt, dass es für die Einführung eines solchen Ausgabe- und Abrechnungssystems kein datenschutzrechtlich

anerkennenswertes Erfordernis oder Bedürfnis im Sinne von § 28 Abs. 1 Satz 1 Nr. 1 oder 2 BDSG gibt, so dass es allenfalls auf freiwilliger Grundlage, also bei Einwilligung der Betroffenen, hätte eingeführt werden können. Der Kantinenbetreiber hätte das System somit nur solchen Schülern anbieten können, deren Personensorgeberechtigten ausdrücklich schriftlich zugestimmt haben, wobei die Einwilligung jederzeit widerruflich und nicht nur pro forma freiwillig hätte sein müssen (§§ 4 Abs. 1, 4a Abs. 1 BDSG). Ab einem Alter von 14 Jahren hätte ich neben einer Erklärung der Personensorgeberechtigten zudem auch eine Einwilligung der betroffenen Schüler verlangt, da ihre Grundrechtsmündigkeit ab diesem Alter vermutet werden darf.

Freiwillig und damit im Sinne des Datenschutzrechts tragfähig wären die Erklärungen überhaupt nur, wenn denjenigen, die nicht an dem System teilnehmen möchten, keine besonderen Nachteile, wie etwa andere Preise, drohen. Der Kantinenbetreiber hätte ihnen also in jedem Fall ein alternatives, gleichwertiges und den Grundsätzen der Datensparsamkeit genügendes Verfahren der Essensausgabe anbieten müssen, um sich auf eine tatsächliche Freiwilligkeit der Teilnehmer berufen zu können.

Dessen ungeachtet halte ich es - dies habe ich dem Kantinenbetreiber als allgemeinen Hinweis auch so mitgeteilt - pädagogisch für verfehlt, Minderjährige an die - quasi selbstverständliche - Preisgabe und Verarbeitung individueller Merkmale ihrer Papillarleisten für (banale) Zwecke der daktyloskopischen Authentifikation gewöhnen zu wollen.

Der Betreiber der Schulkantine hat wegen der rechtlichen Hürden und meiner datenschutzpolitischen Kritik sowie des Protestes aus der Elternschaft auf die Einführung einer biometrischen Authentifikation bei der Essensausgabe dann doch verzichtet.

8.10.2 Einsatz cloudbasierter Dienste im Schulunterricht (Google Apps for Education)

Eine private Schule fragte mich, ob ich Bedenken gegen den schulischen Einsatz des - im Wesentlichen cloudbasierten - Dienstes Google Apps for Education hätte. Dieses habe ich bejaht und aufsichtliche Maßnahmen sowie bußrechtliche Sanktionen für den Fall des Einsatzes in Schulen nicht ausgeschlossen:

Mit einer Inanspruchnahme der angebotenen Services geht eine Schule ein Auftragsdatenverarbeitungsverhältnis ein, das nach hiesigem Recht nur trägt, wenn sie als weiterhin uneingeschränkt verantwortliche Stelle über einen Auftragsdatenverarbeitungsvertrag die notwendige Transparenz der Verarbeitung und die Einhaltung hiesiger Datenschutzbestimmungen hinreichend sicherstellen kann.

Daran habe ich aber erhebliche Zweifel, denn Google legt weder den einsetzenden Stellen noch den europäischen Aufsichtsbehörden bis dato weite Teile seiner Verarbeitung offen. Mithin ist fraglich, wie hiesige Stellen, die den Dienst nutzen, die ihnen obliegende Kontrolle des Verarbeitungshandelns von Google auch nur im Ansatz wahrnehmen und ggf. auch durchsetzen wollen. Völlig ungeklärt ist zudem der Zugriff Dritter auf die Daten, etwa durch Stellen anderer Staaten, die nicht gewillt sind, die Grundrechtssphäre hiesiger Betroffener zu respektieren, dies gilt insbesondere für Versuche der Gerichtsbarkeit der Vereinigten Staaten von Amerika außerhalb bestehender Rechtshilfeabkommen Daten auf europäischen Servern ihrer Entscheidungsgewalt zu unterwerfen. Ich habe daher dringend empfohlen, auf alternative Angebote auszuweichen. Ferner habe ich der Schule ergänzend mitgeteilt, dass eine datenschutzrechtliche Einwilligung in eine Verarbeitung zur Person Minderjähriger eine Einverständniserklärung aller Personensorgeberechtigten verlangt. Zudem bedarf es auch des Einverständnisses des Minderjährigen selbst, sobald dieser aufgrund seiner persönlichen Reife die Tragweite der Erklärung bereits zu erfassen vermag, was erfahrungsgemäß jedenfalls ab einem Alter von 14 Jahren anzunehmen wäre.

8.10.3 Foto- und Filmaufnahmen in Kindertagesstätten

Eine Mutter hatte in der Kindertagesstätte, die ihre Kinder besuchten, eine Einwilligung bezüglich der Anfertigung von Foto- und Filmaufnahmen erklärt. Später hatte sie diese Einwilligung widerrufen und die Löschung der vorhandenen Aufnahmen gefordert. Nunmehr machte sie mir gegenüber geltend, dass ihrem Löschungsverlangen nicht nachgekommen worden sei und bat mich in diesem Zusammenhang um Unterstützung.

Ich konnte dem Löschungsverlangen der Petentin nur teilweise Geltung verschaffen, denn für die Rechtmäßigkeit der Anfertigung und weiteren Verwendung von Foto- und Filmaufnahmen gilt Folgendes:

Die Erklärung der Einwilligung in Foto- und Filmaufnahmen stellt eine Einwilligung in ein Datenverarbeitungshandeln dar. Sie muss daher den Anforderungen des § 4a BDSG genügen, d. h. sie muss grundsätzlich informiert und schriftlich erfolgen. Die wirksame Einwilligung rechtfertigt den mit der Anfertigung und Verwendung von Foto- und Filmaufnahmen verbundenen Eingriff in das allgemeine Persönlichkeitsrecht und nimmt diesem die Rechtswidrigkeit.

Die Einwilligung kann widerrufen werden. Allerdings entfaltet der Widerruf seine Wirkung erst für die Zukunft. Die in der Vergangenheit auf Grundlage der Einwilligungserklärung erfolgte Anfertigung von Foto- und Filmaufnahmen wird durch deren späteren

Widerruf nicht rechtswidrig. Entsprechendes gilt - je nach Umfang der erteilten Einwilligung - auch für die bis dahin erfolgte Speicherung, Übermittlung oder Nutzung. Für die Zukunft entfällt jedoch die rechtfertigende Wirkung der Einwilligung mit der Folge, dass die Fotos zu löschen sind. Für Aufnahmen, auf denen nur die von der widerrufenen Einwilligung betroffene Person zu sehen ist, gestaltet sich dies unproblematisch. Weitaus problematischer gestaltet sich die Rechtslage, wenn auf der in Rede stehenden Aufnahme mehrere Personen abgebildet sind (sogenannte Mehrpersonenaufnahme). Hier ist nach der Rechtsprechung nur in Ausnahmefällen ein wirksamer Widerruf möglich. Voraussetzung für die Wirksamkeit des Widerrufs ist in diesen Fällen das Vorliegen eines wichtigen Grundes. Darüber hinaus ist eine Interessenabwägung zwischen den Interessen der widerrufenden Person, den (weiteren) abgebildeten Personen bzw. denjenigen des Aufnehmenden durchzuführen.

8.10.4 Videobeobachtung und -dokumentation der kindlichen Entwicklung

Die Erzieher in den sächsischen Kindertageseinrichtungen sind aufgefordert, die individuelle Entwicklung der Kinder zu beobachten. Diese Beobachtungen werden schriftlich festgehalten und dienen dazu, Entwicklungsfortschritte der Kinder über einen längeren Zeitraum hinweg zu dokumentieren. Sie bilden dabei auch die Grundlage für Entwicklungsgespräche mit den Eltern, diese sollten regelmäßig über den Prozess und den Inhalt der Dokumentation informiert werden.

Für den Einsatz gezielter Beobachtungsinstrumente ist dabei Folgendes zu beachten: Für das Erheben und Speichern von Videoaufzeichnungen ist das Einverständnis der Eltern einzuholen. Denn eine gesetzliche Grundlage für Videoaufzeichnungen gibt es aus meiner Sicht nicht. Die Eltern sind daher zunächst über die Art der Videoaufzeichnungen, insbesondere auch über deren Umfang (Dauer) und ggf. Speicherung sowie Löschungsfristen aufzuklären.

8.10.5 Betreuung in Kindertagesstätten während Schließzeiten nur nach Vorlage abgelehnter Urlaubsanträge?

Ein Petent wandte sich mit der Frage an mich, ob sächsische Kindertagesstätten einen Anspruch darauf hätten, dass ihnen in Schließzeiten ein Nachweis erbracht wird, dass die Personensorgeberechtigten die Betreuung nicht selbst wahrnehmen können. Im konkreten Fall forderte die Kindertagesstätte von den Personensorgeberechtigten eine Bestätigung, dass deren Arbeitgeber während der Schließzeit die Urlaubsgewährung verweigert hatte.

Ich habe dies für alle Kindertagesstätten - gleich ob in öffentlicher oder in freier Trägerschaft - verneint. Für die hier betrachteten Kindertagesstätten in freier Trägerschaft gilt Folgendes:

Bei der Anforderung einer Bescheinigung über die Nichtgewährung von Urlaub handelt es sich um eine Datenerhebung. Eine solche ist bei Kindertagesstätten in freier Trägerschaft nur nach Maßgabe des § 28 Abs. 1 BDSG statthaft. Gemäß § 28 Abs. 1 Satz 1 Nr. 1 BDSG ist das Erheben personenbezogener Daten für die Erfüllung eigener Geschäftszwecke zulässig, wenn es für die Durchführung eines rechtsgeschäftlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

Zwischen den Personensorgeberechtigten und der Kindertagesstätte besteht regelmäßig ein Vertrag über die Betreuung des Kindes. Dieser Betreuungsvertrag ist Ausfluss des aus § 24 SGB VIII resultierenden Anspruchs auf Förderung des Kindes in einer Tageseinrichtung. Dieser Anspruch auf Betreuung besteht unabhängig davon, ob die Personensorgeberechtigten die Betreuung selbst wahrnehmen können oder nicht. Ausgehend hiervon sind keine Gründe ersichtlich, die die Anforderung einer Arbeitgeberbescheinigung über die Nichtgewährung von Urlaub erforderlich machen würden.

8.11 Betrieblicher Datenschutzbeauftragter

8.11.1 Benennung eines Stellvertreters

Das Bundesdatenschutzgesetz enthält - anders als das Sächsische Datenschutzgesetz - keine Regelung hinsichtlich der Bestellung eines Vertreters des betrieblichen Datenschutzbeauftragten. Eine Bestellpflicht besteht mithin nicht. Einen Stellvertreter im eigentlichen bzw. engeren Sinne kann es angesichts der fehlenden Regelung im Bundesdatenschutzgesetz auch nicht geben, d. h. der bestellte Datenschutzbeauftragte ist und bleibt in dieser Funktion allein verantwortlich.

Gleichwohl - und das habe ich auf eine Anfrage hin mitgeteilt - empfehle ich die Benennung eines Vertreters, damit auch bei Abwesenheit des bestellten Datenschutzbeauftragten unaufschiebbare Maßnahmen bei der Geschäftsleitung veranlasst werden können. Bei einer absehbar längeren Abwesenheit (z. B. wegen Krankheit oder Freistellung) des Datenschutzbeauftragten sehe ich eine diesbezügliche Festlegung sogar als geboten an. Dies ergibt sich einerseits aus der Regelung des § 4f Abs. 5 Satz 1 BDSG, wonach die verantwortliche Stelle den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen und ihm, soweit erforderlich (was in diesem Fall zu bejahen wäre), auch Hilfspersonal zur Verfügung zu stellen hat, andererseits aus der Kontrollfunktion des betrieblichen Datenschutzbeauftragten (§ 4g Abs. 1 Satz 4 BDSG), die andernfalls ohne Weiteres unterlaufen werden könnte, indem längere Abwesenheitszeiten des Datenschutzschutzbeauftragten von der verantwortlichen Stelle dazu genutzt werden könnten, datenschutzwidrige Verarbeitungen durchzuführen bzw. in die Wege zu leiten.

Im Hinblick darauf, dass ein solcher Vertreter den bestellten Datenschutzbeauftragten bei kurzfristigen Verhinderungen oder längeren Abwesenheiten ersetzen soll bzw. muss, sind auch bei seiner Auswahl die für eine Bestellung geltenden Bedingungen, vor allem der Ausschluss von Interessenkollisionen, zu beachten (vgl. Simitis, BDSG, 7. Aufl., Rdnr. 145 zu § 4f). Aus den gleichen Erwägungen heraus muss auch dem benannten Vertreter und - je nach Aufgabengebiet - auch sonstigen Hilfspersonen im Sinne von § 4f Abs. 5 Satz 1 BDSG die Möglichkeit eines angemessenen Fachkundeerwerbs eingeräumt werden.

8.11.2 Kündigungsfristen bei externen Datenschutzbeauftragten

Bei der Beantwortung einer Anfrage zu Kündigungsfristen bei externen Datenschutzbeauftragten habe ich zunächst auf den Beschluss des Düsseldorfer Kreises zu den Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f Abs. 2 und 3 BDSG vom 24./25. November 2010 (vgl. 5. TB, Pkt. 13.6.3) verwiesen.

Danach muss bei der Bestellung von externen Datenschutzbeauftragten der Dienstvertrag im Hinblick auf das Benachteiligungsverbot des § 4f Abs. 3 Satz 3 BDSG so ausgestaltet sein, dass eine unabhängige Erfüllung der gesetzlichen Aufgaben durch entsprechende Kündigungsfristen, Zahlungsmodalitäten, Haftungsfreistellungen und Dokumentationspflichten gewährleistet wird. § 4f Abs. 3 BDSG schränkt insoweit die grundsätzliche Vertragsfreiheit ein. Empfohlen wird grundsätzlich eine Mindestvertragslaufzeit von vier Jahren.

Zu den Kündigungsfristen trifft der Beschluss keine konkrete Aussage. Da jedoch der Abberufungsschutz des § 4f Abs. 3 Satz 4 BDSG grundsätzlich auch für den externen Datenschutzbeauftragten gilt, messe ich den Kündigungsfristen nur eine untergeordnete, in erster Linie für die Kündigung durch den Datenschutzbeauftragten selbst relevante Bedeutung zu und bewerte auch eine Kündigungsfrist von sechs Monaten insoweit als akzeptabel. Nichtsdestoweniger betrachte ich eine für beide Vertragsparteien vereinbarte, voraussetzungsfreie Kündigungsmöglichkeit (einfache Kündigung ohne besondere Gründe) eines auf unbefristete Zeit geschlossenen Vertrages als eine sehr kritische, möglicherweise sogar nichtige Regelung (vgl. dazu Bergmann/Möhrle/Herb, Datenschutzrecht, Stand 2/2015, Rdnr. 141 zu § 4f BDSG).

8.12 Rechte Betroffener

8.12.1 Kein Anspruch auf Mitteilung über eine erfolgte Datenlöschung

Gleich mehrfach erreichten mich Eingaben von Personen, die bei den jeweils verantwortlichen Stellen eine Löschung ihrer Daten verlangt hatten, jedoch binnen der gesetzten Fristen oder nach Ablauf üblicher Bearbeitungszeiten keine Mitteilung über die tatsächliche Vornahme der - in allen Fällen unzweifelhaft gebotenen - Löschung erhielten und mich deshalb um Aufsicht baten.

Nach der Systematik des Bundesdatenschutzgesetzes besteht jedoch allein die Pflicht - und zwar nicht nur auf Verlangen - personenbezogene Daten unverzüglich zu löschen, sobald die Voraussetzungen einer Löschung erfüllt sind (§ 35 Abs. 2 Satz 2 BDSG). Eine Rechtspflicht, explizit den Vollzug der gesetzlichen Löschverpflichtung - auch bei Nachfrage - mitzuteilen, hat der Gesetzgeber nicht vorgesehen. Sie lässt sich auch nicht als Annex zur Löschverpflichtung oder abstrakt aus der allgemeinen gesetzlichen Auskunftsverpflichtung nach § 34 Abs. 1 BDSG mittelbar herleiten.

Betroffenen bleibt also im Fall des Ausbleibens einer Mitteilung allein, auf Grundlage von § 34 Abs. 1 BDSG formal die Auskunft zu (noch) gespeicherten Daten zu beantragen, um auf diese Weise herauszufinden, ob die zu löschenden Daten immer noch gespeichert sind, also eine Löschung nicht erfolgt ist. Dies ist sicher umständlich und sollte gesetzgeberisch anders gelöst werden. Lediglich wenn dieser Auskunftsanspruch nicht befriedigt wird oder nach der Auskunft feststeht, dass eine verpflichtende Löschung nicht vollzogen wurde, besteht derzeit Raum für meine Aufsicht und die Möglichkeit einer bußgeldrechtlichen Sanktion.

8.13 Parteien

8.13.1 Online-Aufnahmeanträge

Im Rahmen meiner Aufsichtstätigkeit bin ich auf die Online-Mitgliederaufnahmeanträge einer sächsischen Landespartei gestoßen, die über eine ungesicherte Internetverbindung angeboten worden waren. Zudem enthielten die dazugehörigen Hinweise zum Datenschutz u. a. die Aussage, dass die Partei die in diesem Aufnahmeantrag enthaltenen personenbezogenen Daten ausschließlich für parteiinterne Zwecke verarbeitet und dies der vorherigen schriftlichen Einwilligung bedürfe, die gleichzeitig mit dem Mitgliedschaftsantrag erteilt werde.

Die über den Online-Aufnahmeantrag erfolgende Erhebung personenbezogener Daten der Beitrittsinteressenten über eine unverschlüsselte Internetverbindung widersprach sowohl den Vorschriften des § 13 Abs. 4 TMG, wonach verantwortliche Stellen

sicherzustellen haben, dass die Nutzer Telemedien gegen die Kenntnisnahme Dritter geschützt in Anspruch nehmen können, als 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. Ich habe die Partei daher aufgefordert, für die Online-Aufnahmeanträge entweder eine SSL-verschlüsselte Verbindung - was letztendlich so umgesetzt worden ist - bereitzustellen oder aber auf diese Möglichkeit gleich ganz zu verzichten.

Die eingangs erwähnten Hinweise zum Datenschutz gaben die Rechtslage nicht korrekt wieder. Abgesehen davon, dass der Inhalt des Online-Aufnahmeantrags nicht den Anforderungen des § 4a BDSG (Einwilligung) genügte, bedarf die Erhebung, Verarbeitung und Nutzung von Mitgliederdaten zu mitgliedsschaftlichen und parteiinternen Zwecken überhaupt keiner schriftlichen Einwilligung im eigentlichen Sinn, sondern ist stattdessen mit § 28 Abs. 1 Satz 1 Nr. 1 und Abs. 9 BDSG zu rechtfertigen. Auch die Datenschutzhinweise wurden entsprechend überarbeitet.

8.13.2 Nutzung personenbezogener Daten für Wahlwerbung

Weil ein Bürger unverlangt Wahlwerbung einer Partei erhalten und die Partei nicht auf sein Auskunftsersuchen nach § 34 BDSG reagiert hatte, erlangte ich Kenntnis von diesem Wahlwerbeschreiben und dabei insbesondere auch von der Tatsache, dass dieses Schreiben nicht den nach § 28 Abs. 4 Satz 2 BDSG vorgeschriebenen Hinweis auf das Widerspruchsrecht enthalten hatte.

Die Herkunft der Daten konnte leider nicht mehr eindeutig nachvollzogen werden, denn die verantwortliche Stelle behauptete, die genutzte Anschrift über einen Informationscoupon erhalten und diesen bereits vernichtet zu haben, während der Betroffene jeglichen früheren Kontakt bzw. jegliche Informationsanforderung bestritt.

Die betreffende Partei sah auch nicht ein, dass sie dieses Werbeschreiben mit einem Hinweis auf das Widerspruchsrecht hätte versehen müssen. Sie argumentierte damit, dass der Empfänger - als solcher vermeintlich identisch mit dem Absender des Informationscoupons - die Zusendung von Informationsmaterial ausdrücklich gewünscht habe. Damit läge nicht die im Bereich der Werbung typische Situation vor, dass die Daten des Betroffenen ohne seinen Willen verwendet werden. Wer als Betroffener seine Daten selbst in Umlauf bringe, könne nicht schutzwürdiger Weise genauso behandelt werden wie der nichtsahnende Werbekunde.

Ich habe Folgendes entgegnet:

§ 28 Abs. 4 Satz 2 BDSG regelt die Unterrichtungspflicht eindeutig und ohne jegliche Einschränkung bzw. Voraussetzung. Das Widerspruchsrecht und damit auch die Unterrichtungspflicht besteht auch unabhängig davon, wofür geworben wird. Selbst Werbemaßnahmen politischer Parteien fallen in den Anwendungsbereich dieser Vorschrift. Dass es sich bei dem zugesandten Informationsblatt unzweifelhaft um Wahlwerbung gehandelt hatte, zeigte der Aufruf am Ende des Schreibens, der betreffenden Partei bei den anstehenden Wahlen seine Stimmen zu geben.

Soweit man vertritt, dass mit dem Ausfüllen und Einsenden eines Coupons in Hinblick auf die Zusendung von Informationsmaterial bereits ein rechtsgeschäftliches oder rechtsgeschäftsähnliches Schuldverhältnis begründet wird, gilt die Unterrichtungspflicht zudem schon in Bezug auf die Bereitstellung des Coupons. Nach § 28 Abs. 4 Satz 2 BDSG ist der Betroffene nämlich auch bei Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses über das Widerspruchsrecht zu unterrichten. Mithin wäre der Verstoß ungeachtet einer etwaigen Verwendung für Werbezwecke in gleicher Weise gegeben gewesen, denn dann hätte die Unterrichtung bereits auf dem Coupon erfolgen müssen.

In einem anderen Fall von Wahlwerbung gestaltete sich die Aufklärung der Datenherkunft einfacher. Der Absender hatte sich in diesem Fall ausschließlich an Erstwähler gewandt und die dafür genutzten Adressen auf der Grundlage von § 33 SächsMG zulässigerweise von den sächsischen Gemeinden bezogen.

§ 33 Abs. 1 SächsMG regelt diesbezüglich, dass die Meldebehörde Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit Wahlen zu parlamentarischen und kommunalen Vertretungskörperschaften in den sechs der Wahl vorangehenden Monaten eine Gruppenauskunft aus dem Melderegister über die in § 32 Abs. 1 Satz 1 SächsMG bezeichneten Daten von Gruppen von Wahlberechtigten erteilen darf, für deren Zusammensetzung das Lebensalter der Betroffenen bestimmend ist. Der Empfänger hat die Daten spätestens einen Monat nach der Wahl zu löschen.

Einen Datenschutzverstoß konnte ich insoweit also nicht feststellen. Ich habe die Betroffenen, die sich an mich gewandt haben, darauf hingewiesen, dass sie nach § 33 Abs. 4 Satz 1 SächsMG bei ihrer Meldebehörde einer Übermittlung ihrer Daten für Zwecke der Wahlwerbung widersprechen und damit zukünftig für sich den Erhalt vergleichbarer Wahlwerbeschreiben ausschließen können.

Nichtsdestoweniger musste ich aber auch hier feststellen, dass die Wahlwerbeschreiben keine Unterrichtung nach § 28 Abs. 4 Satz 2 BDSG enthielten. Die verantwortliche Stelle hat diese Regelung vorliegend für nicht anwendbar gehalten, weil eine Unterrichtung über

das Widerspruchsrecht ins Leere laufen würde, denn zu dem Zeitpunkt, zu dem die möglichen Widerspruchsführer ihren Widerspruch hätten einlegen können, seien die sie betreffenden Datensätze bereits wieder wie von § 33 Abs. 1 Satz 4 SächsMG gefordert gelöscht gewesen. Es wäre im konkreten Fall nicht einmal mehr möglich, zu überprüfen, ob die Daten des Widerspruchsführers tatsächlich für die Versendung des betreffenden Wahlwerbeschreibens verwendet worden waren.

Diese Auffassung teile ich nicht.

Auch die Vorschriften des § 33 Abs. 1 Satz 4 SächsMG (Löschungspflicht spätestens einen Monat nach der Wahl) und des über § 33 Abs. 1 Satz 3 anwendbaren § 32a Abs. 4 SächsMG (strenge Zweckbindung) entbinden nicht von der Unterrichtungspflicht.

Für die Unterrichtungspflicht nach § 28 Abs. 4 Satz 2 BDSG ist es unbeachtlich, ob die verantwortliche Stelle zum Zeitpunkt der Versendung eines Werbeschreibens die Verwendung des genutzten Adressdatenbestandes für ein weiteres Werbeschreiben bereits plant, eine solche Verwendung für sich zu diesem Zeitpunkt ausschließt oder durch eine (hier spätestens einen Monat nach der Wahl sogar vorgeschriebene) Löschung der Daten sogar unmöglich macht. Denn es ist jederzeit möglich, dass die Adressdaten der Empfänger zu einem späteren Zeitpunkt erneut in die Verfügungsgewalt der verantwortlichen Stelle gelangen, sei es durch eine erneute Gruppenauskunft, sei es über einen Adresshändler, über die Begründung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses oder auf andere legitime Art und Weise.

Ein nach § 28 Abs. 4 Satz 1 BDSG eingelegter Werbewiderspruch ist durch die verantwortliche Stelle für die Zukunft zu beachten, unabhängig davon, ob die verantwortliche Stelle darüber hinaus noch Daten zum Betroffenen gespeichert hat. Die verantwortliche Stelle hat die Daten des Betroffenen dazu in eine Sperrliste oder Sperrdatei aufzunehmen, die Adressliste bei jeder zukünftigen Werbeaktion gegen diese Sperrliste abzugleichen und auf diese Art und Weise die erneute Ansprache der betreffenden Person für Werbezwecke auszuschließen. Genau das ist Sinn und Zweck eines Widerspruchs nach § 28 Abs. 4 Satz 1 BDSG und nur so, d. h. mittels einer Sperrliste oder Sperrdatei, kann das Widerspruchsrecht dann auch tatsächlich gewährleistet werden.

Es ist dabei unter keinen Gesichtspunkten erforderlich, eingehende Widersprüche mit den Empfängern einer vorangegangenen Werbesendung abzugleichen, denn das Widerspruchsrecht besteht unabhängig von einer bereits erfolgten Verwendung der Adressdaten für Werbezwecke. Dies ergibt sich schon daraus, dass die Unterrichtungspflicht auch im Rahmen der Begründung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses besteht (vgl. § 28 Abs. 4 Satz 2 BDSG), im Übrigen das Einlegen

eines Widerspruchs nach § 28 Abs. 4 Satz 1 BDSG aber auch keinerlei vorherige werbliche Verwendung der Daten voraussetzt. Ein Widerspruch kann auch rein vorsorglich eingelegt werden.

Es kann damit keine Rede davon sein, dass ein eingelegter Widerspruch im Fall der bereits erfolgten Löschung der Daten des Betroffenen ins Leere laufen würde, denn es geht dabei ja nicht um die Forderung der (bereits erfolgten) Löschung der Daten, sondern um die Vermeidung einer zukünftigen Ansprache für Werbezwecke. Die verantwortliche Stelle hat den Widerspruch bei sich zu vermerken und beim zukünftigen Versand von Werbeschreiben zu beachten. Eine Datenlöschung ist nicht geeignet, eine erneute Ansprache zu Werbezwecken zu einem späteren Zeitpunkt wirksam zu verhindern.

8.14 Informationspflichten bei Datenpannen

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

Im Berichtszeitraum sind bei mir 24 solcher Meldungen eingegangen. In fünf 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 keine Datenarten nach § 42a Satz 1 BDSG betroffen waren.

In 19 Fällen hat eine Meldepflicht bestanden:

- Kreditkartendatenabgriffe bei Unternehmen der Reise- und Gastronomiebranche (fünf Meldungen) (Kreditkartendaten)
- Verlust von Archivkisten in einem Kreditinstitut (Gesundheitsdaten)
- Verlust einer Patientenakte beim Postversand von einem externen Archiv an ein Krankenhaus (Gesundheitsdaten)
- Fehlkuvertierung von Schreiben eines Kreditinstituts (Kontodaten)
- Abruf fremder Kontoauszüge durch fehlerhaft codierte EC-Karte (Kontodaten)
- ungesicherte Ablage von Vertragsdaten eines Cateringunternehmens auf einem Webserver (Kontodaten)
- Hackerangriff auf eine Partnerbörse (Daten zu religiösen Überzeugungen)

- Diebstahl einer Laptoptasche mit Akten zu Hilfeplänen Jugendlicher (Gesundheitsdaten)
- Abruf von Daten zu Krankschreibungen, Unfallanzeigen und arbeitsmedizinischen Beurteilungen aus einem unzureichend gesichertem Netzlaufwerk (Gesundheitsdaten)
- Weiterleitung von Patientendaten an privaten E-Mail-Account eines Mitarbeiters einer Pflegeeinrichtung (Gesundheitsdaten)
- Veröffentlichung von Mitgliederdaten einer Partei via Twitter (Daten zu politischen Meinungen
- Fehlversand von Dokumenten infolge Adressatenverwechslung durch eine Versicherung (Gesundheits- und Kontodaten)
- Diebstahl einer Patientenakte aus dem Dienstwagen eines Pflegedienstes (Gesundheitsdaten)
- unbefugte Übermittlung von Daten über Schwangerschaftsabbruch durch Mitarbeiter der Speiseversorgung in einem Krankenhaus (Gesundheitsdaten)
- Abruf von Schüler- und Lehrerdaten von unzureichend gesichertem Internetnetzwerk (Kontodaten)

Die Auflistung zeigt einen deutlichen Schwerpunkt bei personenbezogenen Daten zu Bank- und Kreditkartenkonten (elf Meldungen); sieben Meldungen betrafen Gesundheitsdaten.

Hinsichtlich der verantwortlichen Stellen kristallisieren sich keine besonderen Schwerpunkte heraus; eine leichte Häufung zeigt sich naturgemäß bei Unternehmen aus der Gesundheits- und Pflegebranche sowie bei Kreditinstituten, was aber daran liegen dürfte, dass gerade diesen Unternehmen der Umgang mit Gesundheitsdaten bzw. mit Daten zu Bank- und Kreditkartenkonten in besonderem Maße immanent ist.

Immer wieder gern wird Computertechnik gestohlen, wobei es den Dieben hier wohl in erster Linie auf die Technik, weniger auf die darauf gespeicherten Daten ankommt. Umso größere Bedeutung kommt also - gerade bei besonders sensiblen Daten gemäß § 3 Abs. 9 BDSG - den getroffenen Sicherheitsmaßnahmen, insbesondere einer dem Stand der Technik entsprechende Verschlüsselung, zu, damit auch nach einem zumeist technikfokussierten Diebstahl zumindest die gespeicherten Daten wirksam geschützt sind. Die der Aufsichtsbehörde insgesamt gemeldeten Fälle zeigen, dass insbesondere Laptops möglichst nicht (sichtbar) in Fahrzeugen gelassen werden sollten, da dies schnell entsprechende Begehrlichkeiten Dritter weckt - eigentlich eine Binsenweisheit. Das Beispiel der gestohlenen Laptoptasche, in der sich dann - wohl zur Enttäuschung des Diebes - nur Akten befanden, unterstreicht dies ohne Frage.

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

9 Öffentlichkeitsarbeit

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

Mit dem nunmehr bereits siebenten Tätigkeitsbericht zum Datenschutz im nicht-öffentlichen Bereich erfülle ich meine Verpflichtung, die Öffentlichkeit alle zwei Jahre über die Tätigkeit der Aufsichtsbehörde zu informieren. Auch dieser Bericht kann - ebenso wie alle vorangegangenen Berichte per Download von meinem Internetauftritt *http://www.datenschutz.sachsen.de* - bezogen werden. Darüber hinaus halte ich im Internet weitere Informationen zu aktuellen Datenschutzthemen wie 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 nicht entsprechen. Ich bedauere dies ausdrücklich, muss aber zur Kenntnis nehmen, dass die mir aktuell zugestandenen personellen Ressourcen die Wahrnehmung derartiger Aufgaben einfach nicht zulassen.

Aus dem gleichen Grund konnte ich auch eine Teilnahme an den vierteljährlich stattfindenden Tagungen des GDD-Erfa-Kreises Sachsen leider nur noch in sehr wenigen Fällen realisieren.

10 Durchsetzung der Rechte und Befugnisse der Aufsichtsbehörde

10.1 Förmliche Heranziehung zur Auskunft

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

Förmliche Auskunftsheranziehungsbescheide sind unverändert ein adäquates und wirksames Mittel, um von verantwortlichen Stellen, die mindestens zwei aufsichtsbehördliche Schreiben ignoriert haben oder die Auskunftserteilung aktiv verweigern, die zur Aufgabenerfüllung erforderlichen Auskünfte zu erhalten.

Im Berichtszeitraum mussten 20 förmliche Verfahren zur Auskunftsheranziehung eingeleitet werden:

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

In fast allen Fällen wurden schließlich - mal früher, mal später - die geforderten Auskünfte erteilt; Rechtsmittel gegen meine Heranziehungsbescheide werden überhaupt nur ganz selten eingelegt, wobei es sich dann regelmäßig um verantwortliche Stellen handelt, die zuvor aktiv die Auskunftserteilung verweigert haben. Im Berichtszeitraum hatte ich lediglich einen solchen Fall zu verzeichnen; die gerichtliche Entscheidung hierzu stand zum Redaktionsschluss noch aus.

Unternehmen, die die aufsichtsbehördlichen Auskunftsersuchen ignorieren, reagieren zumeist auch nicht auf den Heranziehungsbescheid und regen sich erst nach Erhalt des darauf folgenden Zwangsgeldbescheides. Zu diesem Zeitpunkt ist eine Klage gegen den

Heranziehungsbescheid aber regelmäßig nicht mehr möglich, denn ein Zwangsgeldbescheid wird erst dann erlassen, wenn der vorangegangene Heranziehungsbescheid bereits bestandskräftig ist.

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 hat 35.200 € betragen.

Der Erlass eines Bescheides zur Festsetzung eines Zwangsgeldes hat regelmäßig 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.

10.2 Anordnungen

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

Im Berichtszeitraum habe ich alles in allem acht Anordnungen erlassen müssen. Alle Anordnungen sind bestandskräftig geworden; in vier Fällen musste ich anschließend aber noch ein Zwangsgeld festsetzen, weil die verantwortliche Stelle meiner Anordnung nicht (sogleich) Folge geleistet hatte. Insgesamt sind dabei Zwangsgelder in Höhe von 8000 € festgesetzt worden.

Besonders erwähnenswert ist ein Fall, in der das festgesetzte Zwangsgeld seiner Aufgabe leider nicht gerecht werden konnte, weil die betreffende Person praktisch mittellos war und die beantragte Vollstreckung des Zwangsgeldes daher im Ergebnis fruchtlos geblieben ist. Inhaltlich ging es um die Entfernung aller Personenbezüge aus einer in Ruf schädigender Weise vorgenommenen Internetveröffentlichung zu einem Mitarbeiter der öffentlichen Verwaltung. Die Veröffentlichung vorgenommen hatte ein Angehöriger der

sogenannten Reichsbürgerbewegung, einer Bewegung, deren Mitglieder aus ideologischen Gründen hoheitliche Befugnisse hiesiger Behörden und ihrer Amtswalter ablehnen. Angesichts der - auch daraus resultierenden - Uneinsichtigkeit der betreffenden Person blieb mir in diesem Fall nichts weiter übrig, als das Zwangsverfahren mit einem Antrag auf Erlass eines Haftbefehls gemäß § 23 SächsVwVG fortzuführen. Das zuständige Amtsgericht ist meinem Antrag gefolgt und hat gegen den Reichsbürger eine Zwangshaft für die Dauer von fünf Tagen angeordnet. Der Haftbefehl steht zur Vollstreckung an; der zuständige Gerichtsvollzieher hat des Reichsbürgers bislang allerdings noch nicht habhaft werden können.

Gegen dieselbe Person habe ich in einem anderen Fall noch eine weitere Anordnung erlassen, dort aber vor dem Hintergrund des vorstehend geschilderten Verfahrens bislang noch von Vollstreckungsmaßnahmen abgesehen. Ähnlich geartet ist ein anderer Fall, in dem es gleichfalls um die Entfernung rufschädigender Inhalte aus dem Internet geht. Hier hat sich die verantwortliche Person den eingeleiteten Vollstreckungsmaßnahmen mangels einer zustellungsfähigen Postanschrift bislang entziehen können. Von der zuletzt zuständigen Meldebehörde ist diese Person von Amts wegen nach unbekannt abgemeldet worden.

In zwei weiteren Fällen hat meine Anordnung dazu geführt, dass die rechtswidrig im Internet veröffentlichten Inhalte wieder entfernt worden sind. In einem dieser Fälle habe ich anschließend von meiner Strafantragsbefugnis Gebrauch gemacht (s. Pkt. 12).

Die verbleibenden drei Anordnungen betrafen

- die ordnungsgemäße Verwahrung der aus der Tätigkeit eines Arbeitsvermittlers stammenden Bewerbungsunterlagen, die unter Missachtung von § 9 BDSG und unter Verstoß gegen § 298 Abs. 1 SGB III in einer offen zugänglichen blauen Papiermülltonne entsorgt und durch einen Dritten vorübergehend sichergestellt worden waren,
- die Bestellung eines betrieblichen Datenschutzbeauftragten und
- die Auftragserteilung an einen Auftragsdatenverarbeiter unter Berücksichtigung der Vorgaben des § 11 Abs. 2 Satz 2 BDSG.

Im Fall der letztgenannten Anordnung habe ich nach einem halben Jahr eine nochmalige Kontrolle durchgeführt und feststellen müssen, dass die in der Zwischenzeit erteilten Auftragsdatenverarbeitungsaufträge immer noch nicht den gesetzlichen Anforderungen entsprachen. Ich habe daher zur Durchsetzung meiner Forderung ein - von der verantwortlichen Stelle auch bezahltes - Zwangsgeld in Höhe von 5000 € festgesetzt. Inzwischen hat mir das Unternehmen zugesichert, weitere Aufträge nur unter Beachtung der gesetzlichen Anforderungen zu erteilen. Die Einhaltung dieser Zusage werde ich zu gegebener

Zeit erneut überprüfen. Unabhängig davon habe ich in dieser Angelegenheit auch ein Ordnungswidrigkeitenverfahren (§ 43 Abs. 1 Nr. 11 BDSG) eingeleitet.

10.3 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 (§ 40 SächsDSG, vgl. Anlage 1) - auf diese Ergänzung habe ich im Berichtszeitraum hingewirkt.

Nach der neuen Regelung darf ich von nicht-öffentlichen Stellen, die ich kontrolliert habe, einen Kostenausgleich verlangen, wenn ich bei meiner Prüfung Datenschutzverstöße festgestellt habe. Auch datenschutzrechtliche Beratungen nicht-öffentlicher Stellen sind künftig nach pauschalierten Sätzen kostenpflichtig. Lediglich Kontrollen und Beratungen einfacher Art sowie die Beratung von Stellen ohne Gewinnerzielungsabsicht, wie etwa gemeinnützigen Vereinen, bleiben kostenfrei. Selbstverständlich werden auch keine Kosten von denen erhoben, die sich an mich wenden, weil sie der Ansicht sind, in ihren Datenschutzrechten verletzt zu sein oder Hinweise auf Datenschutzverletzungen haben. Anordnungen, Untersagungen, Abberufungen von Datenschutzbeauftragten sowie bestimmte Prüfungen, Verfahren oder Genehmigungen sind - nunmehr nach besonderem Kostenrecht - weiterhin kostenpflichtig. Die neuen Bestimmungen erlauben mir zudem erstmals ausdrücklich, in völliger Unabhängigkeit meines Amtes auch auf die Erhebung von Kosten zu verzichten, wenn dies im Einzelfall der Billigkeit entspricht, etwa in einer wirtschaftlichen Notlage des Kostenschuldners.

Mit der neuen und transparenten Regelung reagiert der Gesetzgeber auf den erheblich gestiegenen Geschäftsanfall. Er bedient sich dabei solcher Regelungen, wie sie auch in anderen Ländern, z. B. in Hamburg, Niedersachsen, Berlin, Thüringen, Bayern oder Baden-Württemberg, oder anderen aufsichtlichen Bereichen, wie etwa bei der Lebensmittelaufsicht, bereits gängige Praxis sind. Grundgedanke der Regelungen ist, dass dort, wo es gemessen am Verwaltungsaufwand der Billigkeit entspricht, datenschutzrechtlich verantwortliche Stellen an den stets wachsenden Kosten ihrer Aufsicht angemessen beteiligt werden. Damit wird auch die Möglichkeit geschaffen, über die teilweise Refinanzierung der Aufsicht Spielräume für dringend benötigtes neues Aufsichtspersonal zu schaffen. Dies begrüße ich ausdrücklich, gerade weil in letzter Zeit mit dem Geschäftsanfall der Verwaltungsaufwand erheblich gestiegen und es nicht einzusehen ist, weshalb meine Behörde Wettbewerbsunternehmen, Anwälte und entgeltlich tätige externe Datenschutzbeauftragte jedenfalls dann weiter kostenlos beraten soll, wenn es sich nicht um einfache Auskünfte handelt und eine wirtschaftlich leistungsfähige Stelle dadurch die Kosten einer

anderweitig ebenso möglichen Rechtsberatung oder eigenen Prüfung spart. In einigen Fällen bestand in der Vergangenheit sogar Anlass zu der Vermutung, dass entgeltlich tätige externe Datenschutzbeauftragte oder Rechtsbeistände eine kostenlose Rechtsberatung durch meine Behörde in Anspruch nahmen und dann als eigene Dienstleistung gegenüber ihren Auftraggebern abgerechnet haben. Auch deshalb war eine angemessene Neuregelung erforderlich.

11 Ordnungswidrigkeitenverfahren

11.1 Erweiterung der Verfolgungszuständigkeit

Ich hatte mich schon länger dafür eingesetzt, dass mir die Sächsische Staatsregierung neben der bereits bestehenden Zuständigkeit für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach dem Bundesdatenschutzgesetz auch die Verfolgungszuständigkeit für die datenschutzrechtlich begründeten Ordnungswidrigkeitentatbestände des Telemediengesetzes überträgt. Bisher bestand für diese Tatbestände eine Auffangzuständigkeit der - ansonsten mit dem für nicht-öffentliche Stellen geltenden Datenschutzrecht nicht weiter befassten - Landkreise und kreisfreien Städte. Ein weiteres Anliegen war es mir, auch die Verfolgungszuständigkeit für den Auffangtatbestand der Verletzung der Aufsichtspflicht in Betrieben und Unternehmen (§ 130 OWiG) zugewiesen zu bekommen. § 130 OWiG ist eine selbstständige Bußgeldvorschrift zur Ahndung der Verletzung der dem Inhaber oder einer ihm gleichgestellten Leitungsperson obliegenden allgemeinen Aufsichtspflicht im Unternehmen, die als Auffangtatbestand nur dann zur Anwendung kommt, wenn ein konkreter Bezug des Inhabers zu einer betriebsbezogenen Ordnungswidrigkeit nicht nachweisbar ist. Es geht hier also um ein Pflichtverletzungen bzw. Ordnungswidrigkeiten der Mitarbeiter begünstigendes Organisationsverschulden des Leitungspersonals.

Die Sächsische Staatsregierung hat nunmehr die Ordnungswidrigkeiten-Zuständigkeitsverordnung in diesem Sinne geändert und mir auch diese beiden Zuständigkeiten übertragen. § 15 - Zuständigkeit des Sächsischen Datenschutzbeauftragten - der am 13. Juli 2014 in Kraft getretenen Verordnung vom 16. Juni 2014 (SächsGVBl. 2014, S. 342 ff.) regelt jetzt Folgendes:

Der Sächsische Datenschutzbeauftragte ist zuständig für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach

1. § 43 des Bundesdatenschutzgesetzes (BDSG) in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814) geändert worden ist, in der jeweils geltenden Fassung,

2. § 16 Abs. 2 Nr. 2 bis 5 TMG,

...

5. § 130 OWiG, wenn eine mit Strafe oder Geldbuße bedrohte Verletzung von Pflichten begangen wird, deren Einhaltung der Sächsische Datenschutzbeauftragte als Aufsichtsbehörde nach § 38 BDSG zu überwachen hat.

Damit wird die mir obliegende Datenschutzaufsicht im nicht-öffentlichen Bereich jetzt - sachgerecht - durch eine umfassende Verfolgungszuständigkeit für datenschutzrechtliche Ordnungswidrigkeiten ergänzt.

11.2 Durchgeführte Ordnungswidrigkeiten

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 88 neue Bußgeldverfahren zu verzeichnen gewesen; 29 weitere Verfahren stammten noch aus den Vorjahren (vgl. 6. TB, Pkt. 11.1).

Von den somit bei mir im Berichtszeitraum insgesamt 117 anhängigen Verfahren sind 49 mit einem Bußgeld abgeschlossen und 41 eingestellt worden. In fünf Fällen war ich nicht zuständig und 22 Verfahren waren zum Ende des Berichtszeitraums noch nicht abgeschlossen.

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

Die vorstehende Übersicht zeigt, dass die Anzahl der neuen Bußgeldverfahren (nur) um etwa 10 % gestiegen ist, während sich die Höhe der festgesetzten Bußgelder fast versiebenfacht hat. Es sind also deutlich höhere Bußgelder als noch in den Vorjahren festgesetzt worden. Die wegen der Höhe der festgesetzten Bußgelder herausragenden, insoweit mit 249.482 € ca. 70 % der Gesamtsumme umfassenden elf Fälle betrafen in erster Linie formale Verstöße

- gegen die Auskunftspflicht gegenüber der Aufsichtsbehörde
  (2-mal 50.000 €, 1-mal 10.000 €),

- gegen die Pflicht zur Bestellung eines Datenschutzbeauftragten (2-mal 25.000 €, 1-mal 15.000 €, 1-mal 10.000 €),
- gegen die Pflicht zur Unterrichtung der Empfänger von Werbeschreiben über ihr Widerspruchsrecht (13.482 €) und
- gegen die Pflicht zur Erteilung schriftlicher Auftragsdatenverarbeitungsaufträge (10.000 €),

in zwei Fällen aber auch materielle Rechtsverletzungen, so

- die Übermittlung von Reisebuchungsdaten an andere Kunden (25.000 €) und
- die Erhebung und Verarbeitung von Gesundheitsdaten Beschäftigter im Rahmen von Krankenrückkehrgesprächen (16.000 €).

Aus dem Bereich des § 43 Abs. 1 BDSG (formale Rechtsverstöße) sind in der Summe (40 Fälle) folgende Sachverhalte mit Bußgeldern belegt worden:

- Verstoß gegen die Meldepflichten nach § 4d BDSG (zwei Fälle)
- unterlassene Bestellung eines Datenschutzbeauftragten (§ 4f Abs. 1 BDSG) (16 Fälle)
- Verstöße gegen die Auskunftspflichten gegenüber der Aufsichtsbehörde (§ 38 Abs. 3 BDSG) (acht Fälle)
- in Werbeschreiben unterlassene Unterrichtungen über das Widerspruchsrecht (§ 28 Abs. 4 Satz 2 BDSG) (sechs Fälle)
- unterlassene oder nicht rechtzeitige Erteilung von Auskünften an den Betroffenen (§ 34 Abs. 1 BDSG) (fünf Fälle)
- Verstoß gegen die inhaltlichen Vorgaben bei Auftragsdatenverarbeitungsverträgen (§ 11 Abs. 2 Satz 2 BDSG) (drei Fälle)

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

- Erhebung und Verarbeitung personenbezogener Daten mittels eines heimlich an einem Privatfahrzeug angebrachten GPS-Trackers
- Videoüberwachung der Arbeitsräume einer Bäckerei
- Erhebung und Verarbeitung von Gesundheitsdaten Beschäftigter im Rahmen von Krankenrückkehrgesprächen
- Übermittlung von Reisebuchungsdaten an andere Kunden
- Weiterleitung einer privaten E-Mail an den Arbeitgeber des Betroffenen
- Aushang einer Liste mit Beitragsschuldnern im Verein
- Aushang detaillierter Mitgliederlisten im Verein

- Übermittlung von Mitgliederdaten durch eine Interessenvertretung an Abgeordnete (zwei Fälle)

Im Bereich der formellen Verstöße ist eine deutliche Zunahme der geahndeten Verstöße gegen die Pflicht zur Bestellung eines Datenschutzbeauftragten festzustellen. Dabei handelt es sich ausnahmslos um Nebenerkenntnisse aus der Aufsichtstätigkeit, denn die Prüfung der Bestellung eines Datenschutzbeauftragten ist regelmäßiger Bestandteil jeder Datenschutzkontrolle. Die jeweils mindestens vierstelligen, teilweise auch im fünfstelligen Bereich liegenden Bußgelder sollten verdeutlichen, dass es sich - abgesehen von dem dann im Unternehmen fehlenden Datenschutzsachverstand und der aus diesem Grund drohenden Datenschutzverletzungen - auch aus finanziellen Erwägungen heraus nicht lohnt, auf die Bestellung eines Datenschutzbeauftragten zu verzichten.

Wenn die Bußgelder mehr als 200 € 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 20 Fällen zu solch einem Gewerbezentralregistereintrag geführt.

12 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 zwei Fällen einen Strafantrag gestellt. Ein Strafantrag betraf dabei die - gegen Entgelt erfolgte - Übermittlung nicht allgemein zugänglicher Adress- und Kontaktdaten für Werbezwecke; in dem anderen Fall ging es um eine - mit dem Ziel der Rufschädigung erfolgte - Veröffentlichung personenbezogener Daten im Internet.

13 Zusammenarbeit mit anderen Aufsichtsbehörden

Die Datenschutzaufsichtsbehörden der Bundesländer treffen sich zweimal jährlich zum sogenannten *Düsseldorfer Kreis*, um ihre Rechtsauffassungen in grundsätzlichen oder sonst besonders wichtigen datenschutzrechtlichen Fragen sowie in länderübergreifenden Sachverhalten untereinander abzustimmen; zwischen den Tagungen geschieht dies bei Notwendigkeit auch im schriftlichen Verfahren. An diesen Tagungen nehme ich regelmäßig teil; die im Berichtszeitraum gefassten Beschlüsse sind unter Pkt. 14 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 und allgemein interessierende datenschutzrechtliche Fragestellungen untereinander sowie entweder regelmäßig oder auf besondere Einladung hin auch mit Vertretern der Wirtschaft, insbesondere mit Wirtschaftsverbänden, diskutiert werden. In den Arbeitsgruppen werden zudem auch viele Beschlüsse für den Düsseldorfer Kreis vorbereitet. Im Berichtszeitraum war meine Behörde wiederum in den Arbeitsgruppen

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

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 zuzuordnen sind, andererseits dienen diese Treffen dem Austausch praktischer Kontrollerfahrungen, insbesondere auch der gegenseitigen Unterrichtung über durchgeführte Regelkontrollen (vgl. Pkt. 3 dieses Berichts). 2013 fand der Workshop beim Landesbeauftragten für den Datenschutz Niedersachsen und 2014 bei der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg statt.

14 Beschlüsse des Düsseldorfer Kreises

14.1 Beschluss vom 11./12. September 2013

14.1.1 Datenübermittlung in Drittstaaten erfordert Prüfung in zwei Stufen

Bei Datenübermittlungen in einen Drittstaat, also einen Staat außerhalb des Europäischen Wirtschaftsraums, sind Datenschutzfragen auf zwei Stufen zu prüfen:

Auf der ersten Stufe ist es erforderlich, dass die Datenübermittlung durch eine Einwilligung der betroffenen Person oder eine Rechtsvorschrift gerechtfertigt ist. Hierbei gelten die allgemeinen Datenschutzvorschriften (z. B. §§ 28 und 32 Bundesdatenschutzgesetz (BDSG)) mit der Besonderheit, dass trotz Vorliegens einer Auftragsdatenverarbeitung die Datenübermittlung nach § 4 Abs. 1 BDSG zulässig sein muss (vgl. § 3 Abs. 8 BDSG). Bei Auftragsdatenverarbeitung ist der Prüfungsmaßstab in der Regel § 28 Abs. 1 Satz 1 Nr. 2 BDSG, bei sensitiven Daten ist § 28 Abs. 6 ff. BDSG zu beachten.

Auf der zweiten Stufe ist zu prüfen, ob im Ausland ein angemessenes Datenschutzniveau besteht oder die Ausnahmen nach § 4c BDSG vorliegen.

Die Datenübermittlung ist nur zulässig, wenn auf beiden Stufen ein positives Prüfungsergebnis vorliegt.

14.2 Beschluss vom 27. Januar 2014

14.2.1 Orientierungshilfe zur „Einholung von Selbstauskünften bei Mietinteressenten“

Vor der Vermietung von Wohnraum erheben Vermieter bei den Mietinteressenten zum Teil sehr umfangreiche persönliche Angaben, auf deren Basis sie ihre Entscheidung über den Vertragsabschluss treffen. An der Beantwortung solcher Selbstauskünfte muss der Vermieter jedoch ein berechtigtes Interesse haben und es dürfen nur solche Daten erhoben werden, die zur Durchführung des Mietvertrags erforderlich sind. Die legitimerweise zu stellenden Fragen basieren folglich auf einer Abwägung der Interessen des Vermieters gegenüber dem Recht des Mietinteressenten auf informationelle Selbstbestimmung.

Die Orientierungshilfe „Einholung von Selbstauskünften bei Mietinteressenten“ zeigt die wichtigsten Grundsätze auf. Für häufige Fallgestaltungen wird - ohne Anspruch auf Vollständigkeit - dargestellt, was zulässig ist.

Orientierungshilfe „Einholung von Selbstauskünften bei Mietinteressenten“

Einleitung

Vor der Vermietung von Wohnraum erheben Vermieter bei den Mietinteressenten persönliche Angaben, auf deren Basis eine Entscheidung über den Vertragsabschluss getroffen werden soll. An der Beantwortung der Fragen muss der Vermieter ein berechtigtes Interesse haben oder es dürfen nur solche Daten erhoben werden, die zur Durchführung des Mietvertrags erforderlich sind. Auf Basis einer Interessenabwägung muss das Recht des Mietinteressenten auf informationelle Selbstbestimmung Beachtung finden.

Die Verwendung von Einwilligungserklärungen gegenüber Mietinteressenten in Formularen zur Selbstauskunft ist nicht als das richtige Mittel zur Datenerhebung anzusehen. Eine wirksame Einwilligung erfordert nach § 4a Abs. 1 Satz 1 BDSG eine freie Entscheidung des Betroffenen. Dem Mietinteressenten wird dabei suggeriert, er habe bezüglich der gewünschten Angaben von Vermieterseite ein Wahlrecht. Wird der Abschluss des Mietvertrags von der Erhebung bestimmter Angaben beim Mietinteressenten abhängig gemacht, fehlt diese Wahlfreiheit und es entsteht eine Drucksituation, in welcher keine freiwillige Erklärung zustande kommt.

Bezüglich der Datenerhebung kann zwischen bis zu drei Zeitpunkten differenziert werden: (a) dem Besichtigungstermin, (b) der vorvertraglichen Phase, in welcher der Mietinteressent dem künftigen Vermieter mitteilt, eine konkrete Wohnung anmieten zu wollen und (c) der Entscheidung des künftigen Vermieters für einen bestimmten Mietinteressenten.

Die Zulässigkeit der Erhebung einer Selbstauskunft richtet sich im Besichtigungstermin regelmäßig nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG. Spätestens nach der Erklärung des Mietinteressenten, eine konkrete Wohnung anmieten zu wollen, entsteht dann ein vorvertragliches Schuldverhältnis zum künftigen Vermieter, so dass § 28 Abs. 1 Satz 1 Nr. 1 BDSG maßgebend ist. Steht dem Vermieter für die Datenerhebung eine gesetzliche Grundlage nach § 28 Abs. 1 Satz 1 Nr. 1 oder Nr. 2 BDSG zur Verfügung, so kommt es auf die Anforderungen nach § 4a Abs. 1 Satz 1 BDSG nicht an bzw. ein Rückgriff auf das Konstrukt der Einwilligung wäre auch falsch, denn für den Mietinteressenten würde wiederum der Eindruck entstehen, dass die Offenbarung der Informationen seinem Wahlrecht unterliegt. Bei der Anwendung von § 28 Abs. 1 Satz 1 Nr. 1 und Nr. 2 BDSG kommt es dann im Rahmen der Erforderlichkeitsprüfung darauf an, ob von Seiten des Interessenten aus Offenbarungspflichten bestehen bzw. ob von Vermieterseite aus zulässige Fragen gestellt werden. Unzulässige Fragen müssen demnach nicht beantwortet werden (Blank, in: Schmidt-Futterer, Kommentar zum Mietrecht, 11. Auflage 2013, § 543, Rn. 204).

Maßgebend für die Beurteilung des Fragerechts des Vermieters ist, inwieweit die begehrten Angaben mit dem Mietverhältnis über Wohnraum in einem objektiven Zusammenhang stehen und ob schutzwürdige Interessen des Mietinteressenten am Ausschluss der Datenerhebung bestehen.

Die folgende Darstellung ist nicht im Sinne einer abschließenden Aufzählung zu verstehen:

a) Besichtigungstermin

Strebt der Mietinteressent nur eine Besichtigung der Räumlichkeiten an, so wäre es etwa nicht erforderlich, Angaben zu den wirtschaftlichen Verhältnissen zu erfragen. Erfragt werden dürfen:

aa) Angaben zur Identifikation

Hierzu zählen Name, Vorname und Anschrift. Der Vermieter wäre auch befugt, im Falle der Besichtigung allein durch den Mietinteressenten die Angaben durch Vorzeigen eines Personalausweises zu überprüfen und den Umstand der Überprüfung zu dokumentieren. Die Anfertigung einer Ausweiskopie ist nicht erforderlich und damit unzulässig.

bb) Angaben aus Wohnberechtigungsschein

Der künftige Vermieter darf nach § 27 Abs. 1 Wohnraumförderungsgesetz (WoFG) eine Wohnung, die im Rahmen eines Programms zur sozialen Wohnraumförderung errichtet wurde, nur einem Wohnungssuchenden zum Gebrauch überlassen, wenn dieser ihm vorher seine Wohnberechtigung durch Übergabe eines Wohnberechtigungsscheins nachweist. Möchte der Mietinteressent eine solche Wohnung besichtigen, sind Angaben zum Vorliegen eines Wohnberechtigungsscheins sowie zur genehmigten Wohnfläche und Anzahl der Wohnräume erforderlich, da nur in diesem Fall ein Besichtigungstermin sinnvoll ist. Eine Kopie des Wohnberechtigungsscheins darf erst nach der Erklärung des Mietinteressenten, eine Wohnung anmieten zu wollen, erfolgen, da die in dem Formular aufgeführten Angaben zu den Namen und Vornamen der im Haushalt des Mietinteressenten befindlichen Personen im Besichtigungstermin nicht erforderlich sind.

cc) Angaben zu Haustieren

Fragen des Vermieters nach dem beabsichtigten Einbringen von Haustieren sind zulässig, soweit die Tierhaltung nicht zum vertragsgemäßen Gebrauch der Mietsache zählt und folglich zustimmungsbedürftig ist. Entsprechende Fragen sind zulässig, soweit dies nicht Kleintiere betrifft (z. B. Zierfische, Mäuse, Hamster).

b) Erklärung des Mietinteressenten, eine Wohnung anmieten zu wollen

aa) Familienstand und Angaben zu den im Haushalt lebenden Personen

Angaben zum Familienstand des Mietinteressenten werden oft im Hinblick auf die gesamtschuldnerische Haftung von Ehegatten gefordert. Allein aus dieser Zwecksetzung heraus ist kein berechtigtes Vermieterinteresse gegeben, da Ehegatten nicht zwangsläufig gemeinsam Mietvertragsparteien sein müssen. Soweit nur ein Ehegatte den Wohn-Mietvertrag unterzeichnen möchte und im Hinblick auf die äußere Gestaltung des Mietvertrags und die mündlichen Absprachen nicht davon ausgegangen werden kann, dass auch der andere Ehegatte Mietvertragspartei wird, greift keine gesamtschuldnerische Haftung ein. Schließlich ginge auch das Argument ins Leere, von Vermieterseite aus einer möglichen Gebrauchsüberlassung an Dritte zuvor zu kommen, denn nach § 553 Abs. 1 BGB hätte der Mieter im Regelfall ein berechtigtes Interesse daran, dem Ehegatten den Wohnraum zur Nutzung zu überlassen.

Die Anzahl der einziehenden Personen und Informationen darüber, ob es sich um Kinder und/oder Erwachsene handelt, dürfen erfragt werden, da dies für die Beurteilung der Wohnungsnutzung erforderlich ist. Weitere Angaben dürfen zu diesen Personen nicht eingeholt werden, es sei denn, diese möchten Mietvertragspartner sein.

bb) Eröffnetes Insolvenzverfahren, Angabe einer Vermögensauskunft, Räumungstitel wegen Mietzinsrückständen

Die Frage nach einem eröffneten Verbraucherinsolvenzverfahren ist zulässig, da den Mietinteressenten eine Offenbarungspflicht trifft. Das Insolvenzverfahren führt dazu, dass das gesamte pfändbare Vermögen zur Insolvenzmasse gehört und dem Mietinteressenten nur die nicht pfändbaren Vermögensteile zur Verfügung stehen (LG Bonn, Beschluss v. 16.11.2005, Az.: 6 T 312/05 und 6 S 226/05).

Bei der Angabe einer Vermögensauskunft (§ 802c Abs. 3 ZPO) sind Mietzinsansprüche des Vermieters nicht in gleicher Weise gefährdet (LG Bonn, Beschluss v. 16.11.2005, Az.: 6 T 312/05 und 6 S 226/05). Ob in begründeten Fällen ein Fragerecht nach abgegebenen Vermögensauskünften besteht, hängt u. a. davon ab, nach welchem Zeitraum gefragt wird. Ferner ist zu berücksichtigen, dass gemäß § 882f Satz 1 Nr. 4 ZPO eine Einsicht in das Schuldnerverzeichnis unter bestimmten Voraussetzungen möglich ist und zum Inhalt eines solchen Verzeichnisses auch Eintragungsanordnungen nach § 882c ZPO zählen. Nach § 882f Satz 1 Nr. 4 ZPO ist die Einsicht in das Schuldnerverzeichnis jedem gestattet, der darlegt, Angaben nach § 882b ZPO zu benötigen, um wirtschaftliche Nachteile abzuwenden, die daraus entstehen können, dass Schuldner ihren Zahlungsverpflichtungen nicht nachkommen. Im Hinblick auf den erheblichen Eingriff in das Recht auf

informationelle Selbstbestimmung des Mietinteressenten ist bei der Anwendung von § 882f Satz 1 Nr. 4 ZPO vor allem der Verhältnismäßigkeitsgrundsatz zu beachten. Ferner muss den wirtschaftlichen Nachteilen bedeutsames Gewicht zukommen (Utermark, in: Vorwerk/Wolf, Beck`scher Online-Kommentar ZPO, 2013, § 882f, Rn 7). An die Zulässigkeit einer Datenerhebung beim Vollstreckungsgericht nach § 882f Satz 1 Nr. 4 ZPO sind ähnlich hohe Anforderungen zu stellen, wie im Rahmen einer Datenerhebung nach § 28 Abs. 1 Satz 1 BDSG beim Mietinteressenten.

Fragen nach Räumungstiteln wegen Mietzinsrückständen sind dann zulässig, wenn diese aufgrund der zeitlichen Nähe noch Auskunft darüber geben können, ob künftige Mietzinsansprüche gefährdet wären. Dies kann der Fall sein, wenn bezüglich eines bestehenden Wohnraummietverhältnis mit einem anderen Vermieter die Zwangsräumung wegen Mietzinsrückständen droht (AG Wolfsburg, Urteil v. 09.08.2000, Az.: 22 C 498/99). Fragen danach, ob in den letzten fünf Jahren Räumungsklagen wegen Mietzinsrückständen eingeleitet oder durchgeführt wurden, in welchen das Verfahren mit einem Räumungstitel abgeschlossen wurde, werden als zulässig angesehen (LG Wuppertal, Urteil v. 17.11.1998, Az.: 16 S 149/98).

cc) Religion, Rasse, ethnische Herkunft bzw. Staatsangehörigkeit

Nach § 19 Abs. 1 und 3 AGG ist bezüglich der Rasse, der ethnischen Herkunft und der Religion bei der Vermietung von Wohnraum eine unterschiedliche Behandlung im Hinblick auf die Schaffung und Erhaltung sozial stabiler Bewohnerstrukturen und ausgewogener Siedlungsstrukturen sowie ausgeglichener wirtschaftlicher, sozialer und kultureller Verhältnisse zulässig. Es fehlt regelmäßig an der Erforderlichkeit der Datenerhebung, da die Anforderungen nach den §§ 19, 20 AGG kaum erfüllt sein werden. Hierfür müsste zur Schaffung und Erhaltung sozial stabiler Bewohnerstrukturen und ausgewogener Siedlungsstrukturen sowie ausgeglichener wirtschaftlicher, sozialer und kultureller Verhältnisse zunächst ein tragfähiges Vermietungskonzept vorliegen. Das Konzept muss auch zur Prüfung sachlicher Gründe (vgl. etwa § 20 Abs. 1 Nr. 4 AGG) Auskunft geben, die eine Ungleichbehandlung rechtfertigen und folglich zur Entschärfung von Konflikten beitragen können. Eine pauschale Abfrage der Angaben ist daher unzulässig.

dd) Vorstrafen und strafrechtliche Ermittlungsverfahren

Die Erhebung von Angaben zu Vorstrafen ist grundsätzlich nicht erforderlich und damit unzulässig. Berücksichtigt werden muss zum einen, dass bestimmte Strafen nicht in ein polizeiliches Führungszeugnis aufzunehmen sind, § 32 Abs. 2 BZRG, und sich schon deshalb keine darüber hinaus gehenden Mitteilungspflichten gegenüber einem Vermieter

ergeben können. Weiterhin hat die Rechtsprechung eine Offenbarung von Vorstrafen bisher nur im Zusammenhang mit der Begründung von Arbeitsverhältnissen als zulässig angesehen, wenn ein klarer Bezug zu einer entsprechenden Tätigkeit besteht, wie etwa das Fragen nach Vermögensdelikten bei einer Beschäftigung im Kassenbereich eines Kreditinstituts. Dabei steht die Frage nach der Geeignetheit eines Bewerbers im Mittelpunkt. Bei der Anbahnung von Mietverhältnissen besteht grundsätzlich keine vergleichbare Gefährdungslage, da hier die Frage nach der Bonität des Mietinteressenten von zentraler Bedeutung ist. Gegen die Erhebung von Informationen zu laufenden strafrechtlichen Ermittlungsverfahren spricht schon die verfassungsrechtlich und auch in Art. 6 Abs. 2 EMRK verankerte Unschuldsvermutung.

ee) Heiratsabsichten, Schwangerschaften, Kinderwünsche

Angaben zu Heiratsabsichten, bestehenden Schwangerschaften und Kinderwünschen zählen zum Kernbereich privater Lebensgestaltung. Fragen hierzu sind unzulässig. Eine Aufnahme von Kindern und Ehegatten in der Wohnung wäre für den Mietinteressenten schon nicht erlaubnispflichtig im Sinne von § 553 Abs. 1 Satz 1 BGB, denn diese Personen sind in Anwendung von Art. 6 Abs. 1 GG bereits keine Dritten (§ 553 Abs. 1 BGB), sondern nahe Familienangehörige. Der Mieter muss die Aufnahme von Familienangehörigen nur anzeigen. Einer Aufnahmeerlaubnis durch den Vermieter bedarf es nicht.

ff) Mitgliedschaften in Parteien und Mietvereinen

Es besteht keine Verpflichtung, über die Zugehörigkeit zu Parteien oder Mietervereinen Auskunft zu geben. Mit den Angaben wird zudem noch keine Aussage zur Bonität des Mietinteressenten bzw. zu dessen Zahlungsfähigkeit und Zahlungswilligkeit getroffen.

gg) Angaben zum Arbeitgeber, zum Beschäftigungsverhältnis und zum Beruf

Für die Entscheidung über den Abschluss eines Mietvertrags darf nach dem Beruf und dem Arbeitgeber als Kriterium zur Beurteilung der Bonität des Mietinteressenten gefragt werden. Die Dauer einer Beschäftigung bietet in einer mobilen Gesellschaft hingegen keine Gewissheit über die Fortdauer und Beständigkeit des Beschäftigungsverhältnisses und ist daher ungeeignet, das Sicherungsbedürfnis des Vermieters zu erfüllen. Fragen nach der Dauer der Beschäftigung sind damit unzulässig.

hh) Einkommensverhältnisse

Die Erfragung der Höhe des Nettoeinkommens und desjenigen Betrags, der nach Abzug der laufenden monatlichen Belastungen für die Tilgung des Mietzinses zur Verfügung steht, ist regelmäßig erforderlich. Bezüglich der Höhe des Nettoeinkommens wäre jedoch

auch die Angabe einer bestimmten Betragsgrenze durch den Mietinteressenten ausreichend, verbunden mit dem Hinweis, dass diese Grenze überschritten wird. Im Hinblick auf die monatlichen Belastungen ist die Erfragung der Forderungsgründe (Unterhaltsverpflichtungen, Darlehensverbindlichkeiten etc.) unzulässig, da dies für die Beurteilung der Bonität nicht erforderlich ist.

Fragen nach den Einkommensverhältnissen sind unzulässig, wenn die Mietzahlungen vollständig von dritter Stelle für den Mieter übernommen und direkt an den Vermieter geleistet werden sollen, was bei Empfängern von Arbeitslosengeld II der Fall sein kann. Empfänger von Arbeitslosengeld II müssen für die Durchführung einer solchen Direktzahlung gegenüber dem Jobcenter eine entsprechende Erklärung abgeben, § 22 Abs. 7 Satz 1 SGB II. Direktzahlungen an den Vermieter werden nach § 22 Abs. 7 Satz 2 SGB II von Amts wegen vorgenommen, wenn eine zweckentsprechende Verwendung der gewährten Mittel durch den Empfänger von Arbeitslosengeld II nicht sichergestellt ist.

ii) Angaben zu bisherigen Vermietern

Fragen nach den Kontaktinformationen aktueller oder früherer Vermieter des Mietinteressenten (z. B. Name, Anschrift, Telefonnummer, E-Mail-Adresse) sind unzulässig. Solche Angaben wären für die Entscheidung über die Begründung eines Mietverhältnisses nicht erforderlich und würden eine dem Grundsatz der Direkterhebung (§ 4 Abs. 2 Satz 1 BDSG) widersprechende Datenerhebung bei Dritten über den Mietinteressenten ermöglichen.

c) Entscheidung des künftigen Vermieters für einen bestimmten Mietinteressenten

Der künftige Vermieter möchte nun mit dem einzigen Mietinteressenten für eine konkrete Wohnung einen Mietvertrag schließen. Haben sich zwei oder mehrere Mietinteressenten für eine konkrete Wohnung entschieden, so trifft der künftige Vermieter die Entscheidung für einen bestimmten Mietinteressenten (Erstplatzierter). Nach dieser Entscheidung kann die Einholung weiterer Informationen beim Erstplatzierten erforderlich sein.

aa) Nachweise zu den Einkommensverhältnissen

Der künftige Vermieter kann bereits bei der Erfragung der Höhe des Nettoeinkommens und der Höhe der monatlichen Belastungen darauf hinweisen, dass für den Fall einer positiven Entscheidung für den Mietinteressenten quasi unmittelbar vor Unterzeichnung des Vertrags noch Nachweise zu den Einkommensverhältnissen vorgelegt werden müssen, z. B. eine Lohn- oder Gehaltsabrechnung, ein Kontoauszug oder ein Einkommensteuerbescheid in Kopie - jeweils unter Schwärzung der nicht erforderlichen Angaben. Als Nachweis ist auch eine Bescheinigung des Arbeitgebers ausreichend, dass die Angaben des

Mietinteressenten bezüglich der Angabe einer bestimmten Nettobetragsgrenze, die überschritten wird, zutreffend sind.

bb) Vorlage der Selbstauskunft nach Anfrage bei einer Auskunftei

Der künftige Vermieter benötigt Informationen zu den wirtschaftlichen Verhältnissen des Mietinteressenten, um dessen Zahlungsfähigkeit bezüglich des Mietzinses beurteilen zu können. Selbstauskünfte, die Mietinteressenten bei Auskunfteien (z. B. SCHUFA) selbst einholen können, enthalten wesentlich mehr Angaben über deren wirtschaftliche Verhältnisse, als für eine solche Beurteilung erforderlich sind. Schon aus diesem Grund wäre die Forderung des künftigen Vermieters an den Mietinteressenten, eine solche Selbstauskunft vorzulegen, unzulässig.

Da die Verwendung von Einwilligungserklärungen gegenüber dem Mietinteressenten in Formularen zur Selbstauskunft nicht als das richtige Mittel zur Datenerhebung anzusehen ist, wäre auch das Verlangen des künftigen Vermieters, eine Einwilligungserklärung für die Einholung einer Bonitätsauskunft abzugeben, nicht rechtmäßig. Zur Einholung von Bonitätsauskünften über den Mietinteressenten wäre der Vermieter nur dann befugt, wenn die Voraussetzungen einer gesetzlichen Vorschrift (§ 28 Abs. 1 Satz 1 Nr. 1 oder Nr. 2 BDSG) erfüllt sind.[1]

14.3 Beschluss vom 19. Februar 2014

14.3.1 Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“

Inhaltsübersicht

[1] Vgl. zur Einholung von Bonitätsauskünften über Mietinteressenten gegenüber Auskunfteien den Beschluss der Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich vom 22. Oktober 2009 „Bonitätsauskünfte über Mietinteressenten nur eingeschränkt zulässig“.

1. Chancen und Risiken einer Videoüberwachung

Videoüberwachung (zum Begriff s. 2.1.1.) ist vermeintlich in der Lage, bei gewissen Sicherheitsproblemen eine einfache Lösung zu bieten. So können etwa unübersichtliche Gebäudekomplexe zu verschiedensten Tages- und Nachtzeiten leicht überwacht werden. Die Aufsicht über das System kann zentral und mit wenig Personalaufwand erfolgen. Die Technik ist erschwinglich und regelmäßig ohne besondere Kenntnisse zu installieren.

Die datenschutzrechtliche Relevanz der Videoüberwachung wird von den Betreibern einer Videoüberwachungsanlage jedoch häufig falsch eingeschätzt. Jeder Mensch hat grundsätzlich das Recht, sich in der Öffentlichkeit frei zu bewegen, ohne dass sein Verhalten permanent mit Hilfe von Kameras beobachtet oder aufgezeichnet wird. Die Tatsache beobachtet zu werden, kann bei vielen Personen eine Änderung ihres Auftretens bewirken, weil die Gefahr besteht, dass das eigene Verhalten überprüft und nicht autorisiert z. B. im Internet veröffentlicht wird. Bei einer ununterbrochenen Überwachung kann das Wissen, dass jede Bewegung und jede Geste von einer Kamera überwacht wird, mit weitreichenden psychologischen Auswirkungen verbunden sein. Der Einzelne fühlt sich ständig beobachtet und ist dadurch einem permanenten Überwachungsdruck ausgesetzt.

Mit dem Einsatz von Videoüberwachungsanlagen sind weitere Risiken verbunden. Es besteht die Gefahr, dass Aufzeichnungen missbraucht oder für fremde Zwecke genutzt werden. Elektronische Bilder können ohne weiteres gespeichert, kopiert und unbegrenzt an eine Vielzahl von Empfängern in kürzester Zeit und ohne finanziellen Aufwand weitergeleitet werden. Umfassende räumliche und zeitliche Überwachungen ermöglichen die

Erstellung von Bewegungs- und Verhaltensprofilen. Hinzu kommt, dass „intelligente“ Videoüberwachungssysteme keine reine Zukunftsmusik mehr sind. Technisch ist es beispielsweise möglich, gezielt einzelne Personen automatisiert über eine große räumliche Distanz zu verfolgen und mittels Bilderabgleich in Datenbanken eindeutig zu identifizieren. Machbar ist es auch, „auffällige“ oder vermeintlich nicht normale Bewegungen und Verhaltensmuster herauszufiltern, anzuzeigen und gegebenenfalls Alarm auszulösen.

Diese Orientierungshilfe soll darüber informieren, unter welchen Voraussetzungen eine Videoüberwachung zulässig ist und welche gesetzlichen Vorgaben dabei einzuhalten sind. Sofern mit einer Kamera personenbezogene Daten erhoben werden, also z. B. Personen oder Kfz-Kennzeichen erkennbar sind, bedarf es nach dem sog. Verbot mit Erlaubnisvorbehalt einer rechtlichen Grundlage für die Datenverarbeitung. Zu unterscheiden ist dabei zwischen der Videoüberwachung durch nicht-öffentliche Stellen in öffentlich zugänglichen Räumen (§ 6b des Bundesdatenschutzgesetzes [BDSG]), der Videoüberwachung von Beschäftigten (§ 32 Abs. 1 BDSG) und einer sonstigen Videoüberwachung in nicht öffentlich zugänglichen Räumen (§ 28 BDSG). Am Ende finden Sie einen Fragenkatalog, der Verantwortlichen und Datenschutzbeauftragten als Checkliste dienen kann.

2. Zulässigkeit einer Videoüberwachung durch nicht-öffentliche Stellen in öffentlich zugänglichen Räumen

Maßgebliche Vorschrift für die Zulässigkeitsprüfung einer Videoüberwachungsanlage ist § 6b BDSG, welche die Videoüberwachung von öffentlich zugänglichen Räumen durch nicht-öffentliche Stellen regelt. Nicht-öffentliche Stellen sind private Betreiber von Videotechnik, z. B. Unternehmen oder Privatpersonen.

2.1. Anwendungsbereich und Voraussetzungen des § 6b Absatz 1 BDSG

Im Folgenden wird beschrieben, wann diese Vorschrift Anwendung findet und welche Anforderungen sie an eine Videoüberwachungsanlage stellt.

2.1.1. Wann liegt eine Videoüberwachung vor?

§ 6b Abs. 1 BDSG definiert die Videoüberwachung als Beobachtung mit „optisch-elektronischen Einrichtungen“. Von diesem Begriff werden nicht nur handelsübliche Videokameras, sondern jegliche Geräte, die sich zur Beobachtung eignen, erfasst. Dabei ist irrelevant, ob sie über eine Zoomfunktion oder eine Schwenkvorrichtung verfügen, ob die Kamera stabil montiert oder frei beweglich ist. Auch der Einsatz von Webcams, Wildkameras, digitalen Fotoapparaten oder Mobiltelefonen mit integrierter Kamera ist grundsätzlich als Videoüberwachung anzusehen (s. hierzu auch Nr. 3.1.). Voraussetzung ist dabei jeweils die Erhebung personenbezogener Daten, das heißt, dass Personen auf den

Aufnahmen erkennbar sein müssen oder sonst Rückschlüsse auf die Identität einer Person möglich sind.

Der Begriff der Videoüberwachung umfasst sowohl die Videobeobachtung, bei der eine Live-Übertragung der Bilder auf einen Monitor erfolgt, als auch die Videoaufzeichnung, bei der die Aufnahmen gespeichert werden. Eine Videoüberwachung liegt bereits vor, sobald die Möglichkeit der Beobachtung gegeben ist, das bedeutet, dass unabhängig von einer möglichen Speicherung oder Aufzeichnung der Bilder schon bei bloßer Live-Beobachtung mittels optisch-elektronischer Einrichtung die Vorgaben des § 6b BDSG einzuhalten sind. Der Begriff der Beobachtung erfasst auch die digitale Fotografie, sofern eine gewisse zeitliche Dauer zugrunde liegt. Damit unterfällt beispielsweise das Anfertigen von Fotos in kurzen Zeitintervallen ebenfalls der Vorschrift. Die gezielte Beobachtung einzelner Personen wird nicht vorausgesetzt. Die Überwachungsmaßnahme setzt selbst dann bereits mit der Inbetriebnahme der Kameras ein, wenn die Geräte erst im Bedarfs- oder Alarmfall aufzeichnen.

Bei bloßen Kameraattrappen oder unzutreffenden Hinweisen auf eine Videoüberwachung gehen die Datenschutzaufsichtsbehörden der meisten Bundesländer davon aus, dass das Bundesdatenschutzgesetz nicht zur Anwendung kommt, da es sich bei Attrappen um keine optisch-elektronische Einrichtungen handelt und deshalb keine personenbezogenen Daten erhoben werden. Allerdings erweckt auch das Anbringen von Kameraattrappen und unzutreffenden Hinweisen bei Personen, die diese zur Kenntnis nehmen, regelmäßig den Eindruck, dass sie tatsächlich videoüberwacht werden. Da die fehlende Funktionsfähigkeit der Kamera von außen nicht erkennbar ist, kann ein Überwachungsdruck hervorgerufen werden[1], der eine Beeinträchtigung des Persönlichkeitsrechts darstellen und damit zivilrechtliche Abwehransprüche auslösen kann. Diese müssen notfalls im Klageweg durchgesetzt werden. Ob darüber hinaus ein aufsichtsbehördliches Einschreiten gegen eine Attrappe in Betracht kommt, differiert danach, ob die örtlich zuständige Aufsichtsbehörde hierfür auch eine sachliche Zuständigkeit anerkennt. Dies erfahren Betroffene ggf. auf Nachfrage.

2.1.2. Was ist ein öffentlich zugänglicher Raum?

Die Anwendung des § 6b BDSG setzt voraus, dass ein öffentlich zugänglicher Raum beobachtet wird. Hierbei handelt es sich um Bereiche innerhalb oder außerhalb von Gebäuden, die nach dem erkennbaren Willen des Berechtigten (z. B. des Grundstückseigentümers) von Jedermann genutzt oder betreten werden dürfen. Ein öffentlicher Raum liegt auch dann vor, wenn für den Zugang besondere allgemeine Voraussetzungen, wie etwa ein bestimmtes Mindestalter, erfüllt sein müssen, ein Eintrittspreis zu errichten ist oder

[1] LG Bonn, Urteil vom 16. November 2004 - 8 S 139/04; AG Lichtenberg, Beschluss vom 24.01.2008 - 10 C 156/07.

die Öffnung nur zu bestimmten Zeiten erfolgt. Darauf, ob der überwachte Bereich Privateigentum ist oder nicht, kommt es nicht an.

Zu den öffentlich zugänglichen Räumen gehören neben öffentlichen Verkehrsflächen beispielsweise Ausstellungsräume eines Museums, Verkaufsräume, Schalterhallen, Tankstellen, Biergärten, öffentliche Parkhäuser, Gasträume von Gaststätten oder Hotelfoyers.

Nicht öffentlich zugänglich sind demgegenüber Räume, die nur von einem bestimmten und abschließend definierten Personenkreis betreten werden können oder dürfen. Hierzu gehören etwa Büros oder Produktionsbereiche ohne Publikumsverkehr. Entscheidend ist hierbei, dass die Nicht-Öffentlichkeit durch Verbotsschilder oder den Kontext der Umgebung erkennbar ist. Die eigene private Wohnung zählt z. B. zu den nicht öffentlich zugänglichen Räumen. Zu beachten ist allerdings, dass die Einordnung als nicht öffentlich zugänglicher Raum vom Einzelfall abhängig ist. Das Treppenhaus eines Wohnhauses ist beispielsweise grundsätzlich ein nicht öffentlich zugänglicher Raum. Befindet sich im Haus allerdings eine Arztpraxis oder eine Anwaltskanzlei mit offenem Publikumsverkehr, dann ist dies bereits ausreichend, um das Treppenhaus während der Geschäftszeiten als öffentlich zugänglich einzuordnen. Eine Videoüberwachung nicht-öffentlich zugänglicher Räume kann unter Umständen nach § 28 BDSG zu beurteilen sein (s. unten Nr. 5.).

Eine Überwachung öffentlich zugänglicher Räume liegt auch dann vor, wenn außer einem privaten Grundstück auch der öffentliche Verkehrsraum in der Umgebung und die sich dort befindlichen Personen erfasst werden. Bei einem Nachbargrundstück handelt es sich nicht um einen öffentlichen Raum; dessen Beobachtung ist daher nicht von § 6b BDSG erfasst. Allerdings greift eine Überwachung von Nachbargrundstücken in die Persönlichkeitsrechte des Nachbarn ein. Dieser kann sich daher auf zivilrechtlichem Weg mittels Abwehr- und Unterlassungsansprüchen gegen die Videoüberwachung zur Wehr setzen (zur Videoüberwachung im Nachbarschaftsverhältnis vgl. unten Nr. 5).

2.1.3. Zulässigkeit einer Videoüberwachung öffentlich zugänglicher Räume

Nach § 6b Absatz 1 BDSG ist das Beobachten öffentlich zugänglicher Räume per Videoüberwachung nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke (2.1.3.1.) erforderlich ist (2.1.3.2.) und keine Anhaltspunkte für das Vorliegen überwiegender schutzwürdiger Interessen der betroffenen Personen bestehen (2.1.3.3.).

2.1.3.1. Zweck der Videoüberwachung

Bevor eine Videoüberwachung installiert wird, ist zu konkretisieren, welches Ziel damit erreicht werden soll. Ein berechtigtes Interesse für den Betrieb einer Videoüberwachungsanlage kann ideeller, wirtschaftlicher oder rechtlicher Natur sein. Soll die Videoüberwachung dazu eingesetzt werden, vor Einbrüchen, Diebstählen oder Vandalismus zu schützen, ist darin grundsätzlich ein berechtigtes Interesse zu sehen, wenn eine tatsächliche Gefahrenlage nachgewiesen werden kann. Zu fordern sind konkrete Tatsachen, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen oder besondere Vorkommnisse in der Vergangenheit. Ratsam ist es daher, entsprechende Ereignisse sorgfältig zu dokumentieren (Datum, Art des Vorfalls, Schadenshöhe) oder etwaige Strafanzeigen aufzubewahren. Auch die Beweissicherung durch die Aufzeichnung kann ein solches berechtigtes Interesse darstellen.

In bestimmten Fällen kann auch eine abstrakte Gefährdungslage ausreichend sein, wenn eine Situation vorliegt, die nach der Lebenserfahrung typischerweise gefährlich ist, z. B. in Geschäften, die wertvolle Ware verkaufen (z. B. Juweliere) oder die im Hinblick auf Vermögens- und Eigentumsdelikte potentiell besonders gefährdet sind (z. B. Tankstellen).

Darüber hinaus ist im Vorhinein konkret festzulegen und schriftlich zu dokumentieren, welchem Zweck die Videoüberwachung im Einzelfall dienen soll. Dabei ist der Überwachungszweck jeder einzelnen Kamera gesondert und konkret anzugeben.

2.1.3.2. Geeignetheit und Erforderlichkeit der Videoüberwachung

Vor dem Einsatz eines Videoüberwachungssystems ist zu überprüfen, ob es tatsächlich für den festgelegten Zweck geeignet und erforderlich ist. Die Erforderlichkeit einer Videoüberwachung kann nur dann bejaht werden, wenn der beabsichtigte Zweck nicht genauso gut mit einem anderen (wirtschaftlich und organisatorisch) zumutbaren, in die Rechte des Betroffenen weniger eingreifenden, Mittel erreicht werden kann.

Vor der Installation einer Videoüberwachungsanlage muss man sich deshalb mit zumutbaren alternativen Methoden auseinandersetzen, die in das Persönlichkeitsrecht des Einzelnen weniger eingreifen. Eine Umzäunung, regelmäßige Kontrollgänge von Bewachungspersonal, der Einsatz eines Pförtners, der Einbau von Sicherheitsschlössern oder von einbruchssicheren Fenstern und Türen können beispielsweise ebenfalls einen wirksamen Schutz gegen Einbruch und Diebstahl bieten. Das Auftragen von spezieller Oberflächenbeschichtung kann Schutz vor Beschädigungen durch Graffiti bieten.

Des Weiteren muss vor Inbetriebnahme einer Kameraanlage eine Überprüfung dahingehend erfolgen, an welchen Orten und zu welchen Zeiten eine Überwachung unbedingt notwendig erscheint. Häufig kann eine Überwachung in den Nachtstunden oder außerhalb der Geschäftszeiten ausreichend sein.

Im Rahmen der Erforderlichkeit ist ferner zu untersuchen, ob eine reine Beobachtung im Wege des Live-Monitorings ausreichend ist, oder ob es zum Erreichen des Überwachungszwecks einer (regelmäßig eingriffsintensiveren) Aufzeichnung bedarf. In diesem Zusammenhang ist zu betonen, dass eine reine Aufzeichnung (blackbox) für präventive Zwecke nicht geeignet ist, da keine direkte Interventionsmöglichkeit besteht. Diese ist nur bei einem Monitoring gegeben, da dann z. B. Sicherheitspersonal unmittelbar eingreifen kann. Das bedeutet, dass eine Videoaufzeichnung zur Verhinderung von Unfällen oder Straftaten nicht geeignet ist.

Unter dem Aspekt der Datenvermeidung und Datensparsamkeit ist weiterhin zu prüfen, ob durch den Einsatz spezieller Technik bestimmte Bereiche des Aufnahmefeldes ausgeblendet oder die Gesichter der sich in diesen Bereichen aufhaltenden Personen „verschleiert“ werden können.

2.1.3.3. Beachtung der schutzwürdigen Interessen des Betroffenen

Auch wenn eine Videoüberwachung zur Wahrung des Hausrechts oder zur Wahrnehmung eines berechtigten Interesses erforderlich ist, darf sie nur in Betrieb genommen werden, wenn schutzwürdige Interessen der Betroffenen nicht überwiegen. An dieser Stelle ist eine Abwägung zwischen den berechtigten Interessen des Überwachenden und dem von der Überwachung Betroffenen vorzunehmen. Maßstab der Bewertung ist das informationelle Selbstbestimmungsrecht als besondere Ausprägung des Persönlichkeitsrechts auf der einen und der Schutz des Eigentums oder der körperlichen Unversehrtheit auf der anderen Seite. Bei der Abwägung sind die Gesamtumstände jedes Einzelfalls maßgeblich. Entscheidend ist häufig die Eingriffsintensität der jeweiligen Maßnahme. Diese wird durch Art der erfassten Informationen (Informationsgehalt), Umfang der erfassten Informationen (Informationsdichte, zeitliches und räumliches Ausmaß), den betroffenen Personenkreis, die Interessenlage der betroffenen Personengruppen, das Vorhandensein von Ausweichmöglichkeiten sowie Art und Umfang der Verwertung der erhobenen Daten bestimmt. In den Fällen, in denen die Videoaufnahmen nicht nur auf einen Monitor übertragen, sondern auch aufgezeichnet werden sollen, ist eine diesbezügliche Abwägung mit den schutzwürdigen Interessen der Betroffenen erneut vorzunehmen.

Grundsätzlich unzulässig sind Beobachtungen, die die Intimsphäre der Menschen verletzen, etwa die Überwachung von Toiletten, Saunas, Duschen oder Umkleidekabinen.

Die schutzwürdigen Interessen überwiegen außerdem häufig dort, wo die Entfaltung der Persönlichkeit im Vordergrund steht, beispielsweise in Restaurants, Erlebnis- und Erholungsparks, wo Leute kommunizieren, essen und trinken oder sich erholen.

Auch eine permanente Überwachung, der eine betroffene Person nicht ausweichen kann, stellt einen gravierenderen Eingriff dar als eine Beobachtung, die lediglich zeitweise erfolgt und nur Teilbereiche des Raumes erfasst. Dies ist zum Beispiel bei der dauerhaften Überwachung von öffentlichen Zufahrten und Eingängen zu Mehrfamilienhäusern relevant, da die Bewohner auf die Nutzung des überwachten Bereichs angewiesen sind.

Grundsätzlich gilt, je mehr persönliche Informationen aufgrund der Überwachung erhoben werden, desto intensiver ist der Eingriff in die Grundrechte und in die schutzwürdigen Interessen der Betroffenen.

Ermöglicht die Qualität der Aufnahme keine Personenbeziehbarkeit, sind schutzwürdige Interessen Betroffener schon deshalb nicht verletzt, weil es an einer Datenerhebung im Sinne des § 3 Absatz 3 BDSG fehlt.

2.2. Einzelne Maßnahmen vor Einrichtung einer Videoüberwachung

Vor dem Einsatz einer Videoüberwachungsanlage gilt es im Vorhinein einige Maßnahmen und Voraussetzungen nach dem Bundesdatenschutzgesetz durchzuführen und einzuhalten.

2.2.1. Verfahrensverzeichnis, Vorabkontrolle, Sicherungspflichten

Vor Beginn der Videoüberwachung ist seitens der verantwortlichen Stelle der konkrete Zweck der Überwachungsmaßnahme (vgl. Nr. 2.1.3.1.) schriftlich festzulegen. Zudem sind technische und organisatorische Maßnahmen zu treffen (§ 9 BDSG), um die Sicherheit der Daten zu gewährleisten.

Vor der Inbetriebnahme einer Videoüberwachung ist eine Vorabkontrolle nach § 4d Absatz 5 BDSG erforderlich, wenn bei dem Einsatz der Videotechnik von besonderen Risiken für die Rechte und Freiheiten der Betroffenen auszugehen ist. Nach der Gesetzesbegründung bestehen besondere Risiken, wenn Überwachungskameras „in größerer Zahl und zentral kontrolliert eingesetzt werden“ (BT-Drs. 14/5793, S. 62). Der betriebliche Datenschutzbeauftragte hat gemäß § 4d Absatz 6 BDSG die Vorabkontrolle durchzuführen und das Ergebnis sowie die Begründung schriftlich zu dokumentieren.

Unabhängig von der Durchführung einer Vorabkontrolle ergibt sich das Erfordernis der vorherigen Zweckbestimmung aus § 6b Absatz 1 Nr. 3 BDSG, wenn die Videoüberwachung zur Wahrnehmung berechtigter Interessen erfolgt. Darüber hinaus ist für Verfahren, die automatisiert Daten verarbeiten, eine Verfahrensübersicht zu erstellen (vgl. § 4g Absatz 2 und 2a BDSG). Eine Videoüberwachung ist jedenfalls dann, wenn sie mittels digitaler Technik erfolgt, als automatisierte Verarbeitung zu qualifizieren. Welche Angaben in diese Übersicht aufgenommen werden müssen, zählt § 4e Satz 1 BDSG verbindlich und abschließend auf. Der dort geforderten allgemeinen Beschreibung der technisch-organisatorischen Maßnahmen zum Schutz der Daten kommt bei der Videoüberwachung besondere Bedeutung zu. Die Videobilddaten unterliegen wegen der sich aus einer unsachgemäßen Handhabung möglicherweise für den Betroffenen ergebenen Beeinträchtigungen entsprechend hohen Schutzkontrollen sowohl hinsichtlich des Zutritts, Zugangs und Zugriffs, aber auch der Weitergabe an Strafverfolgungsbehörden im Deliktfall. In der Verfahrensübersicht sind darüber hinaus die zugriffsberechtigten Personen zu benennen.

Die Verfahrensübersicht ist von der verantwortlichen Stelle zu erstellen und dem betrieblichen Datenschutzbeauftragten zur Verfügung zu stellen. Dieser muss die Inhalte der Verfahrensübersicht bis auf die Angaben zu dem Bereich des Datensicherheitsmanagements auf Antrag jedermann zugänglich machen. Dieses öffentlich zugängliche Papier nennt man Verfahrens- oder auch „Jedermannverzeichnis“. Sofern keine Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten besteht, fällt dem Leiter der nicht-öffentlichen Stelle die Pflicht zu, die Erfüllung dieser Aufgaben des betrieblichen Datenschutzbeauftragten in anderer Weise sicherzustellen.

2.2.2. Hinweispflicht

Nach § 6b Absatz 2 BDSG sind der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen. Der Hinweis kann mit Hilfe entsprechender Schilder oder graphischer Symbole (z. B. Piktogramm nach DIN 33450) erfolgen. Er ist so (etwa in Augenhöhe) anzubringen, dass der Betroffene vor dem Betreten des überwachten Bereichs den Umstand der Beobachtung erkennen kann. 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. Außerdem muss die für die Datenverarbeitung verantwortliche Stelle erkennbar sein, das heißt, wer genau die Videodaten erhebt, verarbeitet oder nutzt. Entscheidend ist dabei, dass für den Betroffenen problemlos feststellbar ist, an wen er sich bezüglich der Wahrung seiner Rechte ggf. wenden kann. Daher ist die verantwortliche Stelle grundsätzlich mit ihren Kontaktdaten explizit auf dem Hinweisschild zu nennen.

2.3. Durchführung einer zulässigen Videoüberwachung

2.3.1. Speicherdauer

Gemäß § 6b Absatz 5 BDSG sind die Daten der Videoüberwachung unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Das ist der Fall, wenn eine Gefahr nicht weiter abgewendet werden muss oder eine Beweissicherung nicht notwendig ist. Ist es beispielsweise an einer Tankstelle zu keinem Überfall oder Diebstahl gekommen, werden Videoaufzeichnungen für Beweiszwecke nicht mehr benötigt und sind daher zu löschen. Ob eine Sicherung des Materials notwendig ist, dürfte grundsätzlich innerhalb von ein bis zwei Tagen geklärt werden können.[2] Das bedeutet, dass Videoaufzeichnungen grundsätzlich nach 48 Stunden zu löschen sind. In begründeten Einzelfällen kann eine längere Speicherfrist angenommen werden, etwa wenn an Wochenenden und Feiertagen kein Geschäftsbetrieb erfolgt. Da sich die gesetzliche Speicherdauer am Aufzeichnungszweck orientiert, kann der Zeitpunkt der Löschpflicht je nach Einzelfall variieren.

Dem Löschungsgebot wird am wirksamsten durch eine automatisierte periodische Löschung, z. B. durch Selbstüberschreiben zurück liegender Aufnahmen, entsprochen.

2.3.2. Unterrichtungspflicht

Werden die Kameraaufnahmen einer bestimmten Person zugeordnet, ist diese Person darüber zu unterrichten (§ 6b Absatz 4 BDSG). Zweck dieser Regelung ist es, Transparenz zu schaffen und der identifizierten Person die Überprüfung der Rechtmäßigkeit der Datenverarbeitung und die Verfolgung ihrer Rechte zu ermöglichen. Inhaltlich geht die Unterrichtungspflicht über die Hinweispflicht hinaus. Eine Unterrichtung hat über die Art der Daten, die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und die Identität der verarbeitenden Stelle zu erfolgen. Die Notwendigkeit einer Benachrichtigung besteht erst bei einer tatsächlichen Zuordnung, allein die Möglichkeit dazu macht eine Benachrichtigung noch nicht erforderlich. Die Benachrichtigung hat bei der erstmaligen Zuordnung zu erfolgen.

2.3.3. Tonaufzeichnungen

Für solche Überwachungsmaßnahmen ist im Strafgesetzbuch (StGB) mit § 201 (Verletzung der Vertraulichkeit des Wortes) eine Regelung enthalten, die es unter Strafandrohung verbietet, das nichtöffentlich gesprochene Wort aufzuzeichnen oder abzuhören.

[2] Vgl. die Gesetzesbegründung, BT-Drs. 14/5793, S. 63.

Sofern eine Videoüberwachungskamera daher über eine Audiofunktion verfügt, ist diese irreversibel zu deaktivieren.

2.3.4. Überprüfung der Rechtmäßigkeitsvoraussetzungen

Der Betreiber einer Videoüberwachungsanlage ist verpflichtet, die rechtlichen Voraussetzungen für den Betrieb in regelmäßigen Abständen zu überprüfen. Insbesondere die Frage der Geeignetheit und Erforderlichkeit der Maßnahme ist zu evaluieren. Lassen sich zum Beispiel nach Ablauf eines Jahres, in dem die Kamera in Betrieb war, 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 Videoüberwachung nicht weiter betrieben werden. Dies kann auch Teilbereiche einer Überwachung betreffen. Das Ergebnis der Überprüfung sollte schriftlich dokumentiert werden.

3. Besondere Fallkonstellationen

3.1. Webcams

Webcams ermöglichen es, Live-Aufnahmen ins Internet einzustellen und damit einer unbestimmten Zahl von Personen weltweit zugänglich zu machen. Problematisch ist dabei, dass Persönlichkeitsrechtsverletzungen bei einer Live-Übertragung nicht mehr rückgängig gemacht werden können. Für zufällig von der Kamera erfasste Personen besteht daher ein großes Risiko, das durch die steigende Qualität und die einfache Möglichkeit der technischen Vervielfältigung und Bearbeitung der Aufnahmen noch erhöht wird. Der Einsatz einer Webcam ist nur dann datenschutzrechtlich unbedenklich, sofern auf den aufgenommenen Bildern - etwa aufgrund der Kamerapositionierung, fehlender Zoom-Möglichkeiten oder niedriger Auflösung - Personen oder Kfz-Kennzeichen nicht erkannt werden können.

3.2. Videoüberwachung in der Gastronomie

Die Videoüberwachung des Gastraumes einer Gaststätte[3] ist nach § 6b BDSG im Regelfall datenschutzrechtlich unzulässig. Jedenfalls die mit Tischen und Sitzgelegenheiten ausgestatteten Gastronomiebereiche sind Kundenbereiche, die zum längeren Verweilen, Entspannen und Kommunizieren einladen und damit nicht mit Videokameras überwacht werden dürfen.[4] Das dem Freizeitbereich zuzurechnende Verhalten als Gast einer Gaststätte geht mit einem besonders hohen Schutzbedarf des Persönlichkeitsrechts des

[3] Gemeint ist die Gaststätte im Sinne des Gaststättengesetzes (GastG), d. h. ein Betrieb, in welchem Getränke und/oder Speisen zum Verzehr an Ort und Stelle verabreicht werden und der jedermann oder bestimmten Personenkreisen zugänglich ist (vgl. § 1 GastG). Unter den Gaststättenbegriff fallen somit auch Cafés, Imbisslokale, Schnellrestaurants etc.

[4] Vgl. AG Hamburg, Urteil vom 22.04.2008 - 4 C 134/08.

Betroffenen einher. Eine Videoüberwachung stört die unbeeinträchtigte Kommunikation und den unbeobachteten Aufenthalt der Gaststättenbesucher und greift damit besonders intensiv in das Persönlichkeitsrecht des Gastes ein. Das schutzwürdige Interesse des Besuchers überwiegt im Normalfall das berechtigte Interesse des Gastronomieinhabers an einer Überwachung, weshalb sich dessen Interesse nur in seltenen Ausnahmefällen durchsetzen kann.

Gleiches gilt für Café- und Gastrobereiche in Bäckereien, Tankstellen, Hotels etc.

4. Videoüberwachung von Beschäftigten

Besonders hohe Anforderungen an die Erforderlichkeit der Überwachung nach § 6b BDSG gelten, wenn in öffentlich zugänglichen Räumen mit Publikumsverkehr gleichzeitig Arbeitsplätze überwacht werden, zum Beispiel in Verkaufsräumen im Einzelhandel. In solchen Fällen ist nicht nur die Persönlichkeitssphäre der Kunden betroffen, sondern es kommt auch zu einer Überwachung der dort tätigen Beschäftigten. Für solche Bereiche, in denen die Wahrscheinlichkeit von Straftaten zu einem geschäftstypischen Risiko gehört und die Erfassung der Beschäftigten lediglich eine Nebenfolge der zulässigen Überwachung des Publikumsverkehrs darstellt, überwiegt in Einzelfällen das berechtigte Interesse des Arbeitgebers Straftaten vorzubeugen. Dennoch ist bei der Installation der Videoüberwachung das Einrichten von sog. Privatzonen, d. h. das dauerhafte Ausblenden von Bereichen, in denen sich Beschäftigte länger aufhalten, erforderlich. Je weniger Rückzugsmöglichkeiten den Beschäftigten in nicht überwachten Bereichen zur Verfügung stehen, desto eher überwiegen deren schutzwürdige Interessen.

Das Erheben, Verarbeiten oder Nutzen von personenbezogenen Daten der Beschäftigten durch eine Videoanlage kann in der Regel nicht auf § 32 Absatz 1 Satz 1 BDSG gestützt werden. Denkbar sind offene Überwachungsmaßnahmen danach jedoch insbesondere zur Erfüllung der Schutzpflicht des Arbeitgebers gegenüber den Beschäftigten, wenn eine Videoüberwachung in besonders gefahrträchtigen Arbeitsbereichen erforderlich ist. Jedoch ist in diesem Zusammenhang der Erfassungsbereich auf den sicherheitsrelevanten Bereich zu beschränken und der Beschäftigte soweit wie möglich auszublenden. Eine Überwachung allein zu dem Zweck, einen ordnungsgemäßen Dienstablauf zu gewährleisten, ist nicht gerechtfertigt.

Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nach § 32 Absatz 1 Satz 2 BDSG nur dann erhoben, verarbeitet oder genutzt werden, wenn vorab zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse

des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Eine Videoüberwachung, die in nicht öffentlich zugänglichen Räumen stattfindet und nicht in Zusammenhang mit dem Beschäftigungsverhältnis steht, ist an den Voraussetzungen des § 28 Absatz 1 Satz 1 Nr. 2 BDSG zu messen. Der Einsatz von Videotechnik muss zur Wahrung berechtigter Interessen des Arbeitgebers erforderlich sein und schutzwürdige Interessen des Beschäftigten dürfen nicht überwiegen. So können ausnahmsweise auch Eigentumsinteressen des Arbeitgebers eine Videoüberwachung rechtfertigen, wenn der Beschäftigte nicht im Fokus der Überwachung steht und nicht permanent erfasst wird, z. B. der nächtliche Wachmann, der die zum Zweck der Verhinderung und Aufklärung von Diebstählen videoüberwachten Lagerräume kontrolliert, in denen wertvolle Ware aufbewahrt wird. Aber auch hier ist zuvor zu prüfen, ob weniger einschneidende Mittel in Betracht kommen.

Für die Bewertung der Zulässigkeit einer solchen Maßnahme ist ergänzend die Rechtsprechung des Bundesarbeitsgerichts[5] zugrunde zu legen. In wenigen Ausnahmefällen kann danach die Überwachung von Beschäftigten mittels Kameras durch den Arbeitgeber dann zulässig sein, wenn sie offen erfolgt, die Beschäftigten also wissen, dass ihr Arbeitsplatz videoüberwacht wird. Entscheidend ist, ob der Arbeitgeber ein berechtigtes Interesse an den Kameraaufnahmen hat, etwa um Diebstählen oder Vandalismus durch sein Personal vorzubeugen. Hat er ein solches, berechtigt ihn dieses jedoch nicht ohne Weiteres zur Überwachung. Vielmehr muss sein Interesse mit den schutzwürdigen Interessen des Beschäftigten, nicht in seinem Persönlichkeitsrecht verletzt zu werden, abgewogen werden. Das Persönlichkeitsrecht schützt den Beschäftigten vor einer lückenlosen Überwachung am Arbeitsplatz durch Videoaufnahmen, die ihn einem ständigen Überwachungsdruck aussetzen, dem er sich nicht entziehen kann. Deswegen überwiegt das Beschäftigteninteresse, von einer derartigen Dauerüberwachung verschont zu bleiben, wenn der Arbeitgeber mit der Überwachung nur befürchteten Verfehlungen seiner Beschäftigten präventiv begegnen will, ohne dass hierfür konkrete Anhaltspunkte bestehen.

In der Abwägung wird auch gewichtet, ob den Beschäftigten überhaupt ein kontrollfreier und damit unbeobachteter Arbeitsbereich verbleibt. Zur Kontrolle von Arbeitsleistungen, Sorgfalt und Effizienz sind Kameras keinesfalls erlaubt. Sensible Bereiche wie Umkleidekabinen, sanitäre Räumlichkeiten oder Pausen- und Aufenthaltsräume sind ebenfalls von der Überwachung auszunehmen.

[5] Vgl. insb. BAG, Urteil vom 27.03.2003 - 2 AZR 51/02; Beschluss vom 29.06.2004 - 1 ABR 21/03; Beschluss vom 14.12.2004 - 1 ABR 34/03; Beschluss vom 26.08.2008 - 1 ABR 16/07; Urteil vom 21.06.2012 - 2 AZR 153/11.

Eine heimliche Videoüberwachung ist nur in absoluten Ausnahmefällen zulässig, wenn weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind, die Videoüberwachung praktisch die einzig verbleibende Möglichkeit zur Aufklärung oder zur Verhinderung des Missstandes darstellt und insbesondere im Hinblick auf den angerichteten oder zu verhindernden Schaden nicht unverhältnismäßig ist.

Kann die Datenerhebung und -verarbeitung im Beschäftigungsverhältnis nicht auf eine Rechtsgrundlage gestützt werden, ist die Videoüberwachung wegen § 4 Absatz 1 BDSG (Verbot mit Erlaubnisvorbehalt) unzulässig. Eine etwaige arbeitgeberseitig eingeholte Einwilligung des Beschäftigten ist irrelevant, da es im Beschäftigungsverhältnis in der Regel an der Freiwilligkeitsvoraussetzung des § 4a Absatz 1 Satz 1 BDSG mangelt.

Soweit die Videoüberwachung den gesetzlichen Vorgaben entspricht, kann sie durch eine datenschutzrechtskonforme Betriebsvereinbarung näher geregelt werden. Die Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten sollten näher beschrieben werden. Dazu gehören insbesondere

- Gegenstand der Datenerhebung, -verarbeitung oder -nutzung
- Zweckbindung
- Datenvermeidung- und Datensparsamkeit
- Art und Umfang der erhobenen, verarbeiteten oder genutzten Daten
- Empfänger der Daten
- Rechte der Betroffenen
- Löschfristen
- Technische und organisatorische Maßnahmen wie beispielsweise das Berechtigungskonzept

Soweit ein Betriebsrat nicht existiert, sollte der Arbeitgeber entsprechende Dienstanweisungen erstellen. Zulässige Verfahren zur Videoüberwachung ermöglichen in der Regel eine Bewertung der Persönlichkeit der betroffenen Beschäftigten einschließlich ihrer Fähigkeiten, ihrer Leistungen und ihres Verhaltens. Daher ist nach § 4d Absatz 5 Satz 2 Nr. 2 BDSG regelmäßig eine Vorabkontrolle durchzuführen (vgl. oben Nr. 2.2.1.).

5. Sonstige Videoüberwachung durch nicht-öffentliche Stellen, insbes. Videoüberwachung durch Nachbarn oder Vermieter

Bei der Beurteilung der Zulässigkeit von Videokameras, die an oder in Wohnhäusern angebracht sind, ist nach dem Erfassungsbereich der Kameras zu unterscheiden. Die Videoüberwachung des eigenen, allein genutzten Grundstücks ist zulässig. Allerdings ist zu betonen, dass die Beobachtungsbefugnis des Hausrechtsinhabers grundsätzlich an den

Grundstücksgrenzen endet. Wer außer seinem Grundstück auch öffentlichen Raum wie Straßen, Gehwege oder Parkplätze überwacht, kann sich nicht auf sein Hausrecht stützen, da sich dieses Recht nur auf den privaten Grund und Boden erstreckt. Berechtigte Interessen, beispielsweise der Schutz des Eigentums, stehen in diesen Fällen hinter den schutzwürdigen Interessen der Personen, die in den Erfassungsbereich der Kamera geraten, wie Nachbarn, Passanten und sonstige Verkehrsteilnehmer, in der Regel zurück. Die zur Überwachung und zum Schutz des eigenen Grundstücks zulässig eingesetzte Videoüberwachungstechnik darf daher nicht zur Folge haben, dass - quasi nebenbei - auch anliegende öffentliche Wege und die sich dort aufhaltenden Personen mitüberwacht werden.

Sofern sich die Videoüberwachung auf das Grundstück des Nachbarn erstreckt, ohne dass eine öffentlich zugängliche Fläche betroffen ist, ist die Anwendbarkeit des Bundesdatenschutzgesetzes zumeist deshalb zu verneinen, da es sich um eine persönliche bzw. familiäre Tätigkeit im Sinne des § 1 Absatz 2 Nr. 3 BDSG handelt, welche vom Regelungsbereich des Bundesdatenschutzgesetzes ausgenommen ist. Dies hat zur Folge, dass die Anlage nicht der Kontrolle der Datenschutzaufsichtsbehörden unterliegt. Videoüberwachten Nachbarn stehen jedoch unabhängig davon unter Umständen zivilrechtliche Unterlassungs- und Abwehransprüche zu. Diese müssten auf dem Zivilrechtsweg gegebenenfalls unter Einschaltung eines Rechtsanwalts geltend gemacht werden. Darüber hinaus kann das Beobachten fremder Grundstücke mit einer Videoanlage strafrechtliche Konsequenzen haben, wenn damit der höchst persönliche Lebensbereich der beobachteten Person verletzt wird (vgl. § 201a des Strafgesetzbuchs).

Bei einer Videoüberwachung im Innenbereich eines Mehrfamilienhauses handelt es sich in der Regel um nicht-öffentlich zugängliche Räume, weshalb sich die Zulässigkeit nicht nach § 6b BDSG richtet (vgl. oben Nr. 2.1.2.). In diesen Fällen greift § 28 BDSG, wonach ähnliche Voraussetzungen für eine Videoüberwachung gelten wie in den Fällen des § 6b BDSG. Außerdem besteht in diesen Fällen ebenfalls die Möglichkeit, mit zivilrechtlichen Unterlassungs- und Abwehransprüchen gegen einen etwaigen Eingriff in das Persönlichkeitsrecht vorzugehen. So stellt eine dauerhafte Überwachung im Innenbereich eines Mehrfamilienhauses, zum Beispiel in Treppenaufgängen, im Fahrstuhlvorraum und im Fahrstuhl selbst, einen schweren Eingriff in das allgemeine Persönlichkeitsrecht der Betroffenen dar. In der hierzu ergangenen zivilrechtlichen Rechtsprechung[6] besteht Einigkeit darüber, dass eine Rundumüberwachung des sozialen Lebens nicht dadurch gerechtfertigt werden kann, dass der Vermieter mit der Überwachung Schmierereien,

[6] Vgl. beispielsweise LG Berlin, Urteil vom 23.05.2005 - 62 S 37/05; KG Berlin, Beschluss vom 04.08.2008 - 8 U 83/08; AG München, Urteil vom 16.10.2009 - 423 C 34037/08.

Verschmutzungen oder einmaligen Vandalismus verhindern möchte. In der Regel überwiegen daher die schutzwürdigen Interessen der Mieter und Besucher als Betroffene.

6. Checkliste für den Betreiber einer Videoüberwachung öffentlich zugänglicher Räume

Planen Sie die Installation von Videokameras oder betreiben Sie bereits eine Videoüberwachungsanlage? Folgende Fragen sollten Sie für eine zulässige Überwachungsmaßnahme beantworten können:

1. Welche Bereiche sollen überwacht werden?
   - öffentlich zugänglicher Raum (z. B. Kundenbereiche);
   - Mitarbeiterräume;
   - öffentliche Flächen (z. B. Gehwege)

2. Dient die Videoüberwachung der
   - Wahrung des Hausrechts
   oder
   - Wahrung eines anderen berechtigten Interesses (Zweck)?
   Wenn ja, welchem?
   Besteht eine Gefährdungslage und auf welche Tatsachen, z. B. Vorkommnisse in der Vergangenheit, gründet sich diese?

3. Wurde der Zweck der Videoüberwachung schriftlich festgelegt?

4. Warum ist die Videoüberwachung geeignet, den festgelegten Zweck zu erreichen?

5. Warum ist die Videoüberwachung erforderlich und warum gibt es keine milderen Mittel, die für das Persönlichkeitsrecht der Betroffenen weniger einschneidend sind?

6. Welche schutzwürdigen Interessen der Betroffenen haben Sie mit welchem Ergebnis in die Interessenabwägung einbezogen?

7. Ist eine Beobachtung der Bilder auf einem Monitor ohne Aufzeichnung der Bilddaten ausreichend? Wenn nein, warum nicht?

8. Sofern aufgezeichnet wird, wann werden die Aufnahmen gelöscht? Wenn das Löschen nicht innerhalb von 48 Stunden erfolgt, begründen Sie bitte das spätere Löschen.

9. Zu welchen Zeiten erfolgt die Videoüberwachung und wer hält sich üblicherweise zu dieser Zeit im überwachten Bereich auf?

10. Wenn eine Videoüberwachung rund um die Uhr erfolgt, warum halten Sie sie für erforderlich bzw. warum kann sie nicht zeitlich eingeschränkt werden, z. B. auf außerhalb der Geschäftszeiten oder die Nachtstunden?

11. Werden bestimmte Bereiche der Überwachung ausgeblendet oder verpixelt? Wenn nein, warum nicht?

12. Über welche Möglichkeiten verfügt die Videokamera und welche hiervon sind für die Überwachung nicht erforderlich und ggf. zu deaktivieren?
    - hinsichtlich der Ausrichtung, z. B. schwenkbar oder variabel, Dome-Kamera
    - bezüglich der Funktionalität, z. B. Zoomobjektive, Funkkameras, Audiofunktion

13. Wurde geprüft, ob eine Vorabkontrolle erforderlich ist und wurde sie ggf. durch die bzw. den betrieblichen Datenschutzbeauftragten durchgeführt? Wenn nein, warum ist eine Vorabkontrolle nicht erforderlich?

14. Wird auf die Videoüberwachung so hingewiesen, dass der Betroffene vor Betreten des überwachten Bereichs den Umstand der Beobachtung erkennen kann?

15. Wird in dem Hinweis die verantwortliche Stelle genannt?

16. Unter welchen Voraussetzungen wird Einsicht in die Aufnahmen genommen?
    Durch wen?
    Ist die Protokollierung der Einsichtnahme sichergestellt?
    Wurden die zugriffsberechtigten Personen auf das Datengeheimnis verpflichtet?

17. Wurden die technisch-organisatorischen Maßnahmen zum Schutz der Daten nach § 9 BDSG (und der Anlage hierzu) getroffen?

18. Gibt es im Unternehmen einen Betriebsrat und wurde mit diesem eine Betriebsvereinbarung zur Videoüberwachung getroffen?

Rein vorsorglich weisen wir darauf hin, dass eine Beschäftigung mit diesen Fragen nicht automatisch zur Zulässigkeit der Videoüberwachungsmaßnahme führt.

Haben Sie zu dem Betrieb der Videoüberwachungsanlage konkrete Fragen, können Sie sich gerne an die für Sie zuständige Datenschutzaufsichtsbehörde wenden. Maßgeblich ist grundsätzlich der Sitz des Betreibers. Eine Übersicht über die Kontaktdaten erhalten Sie beispielsweise unter http://www.baden-wuerttemberg.datenschutz.de/die-aufsichtsbehorden-der-lander/.

14.4 Beschlüsse vom 25./26. Februar 2014

14.4.1 Modelle zur Vergabe von Prüfzertifikaten, die im Wege der Selbstregulierung entwickelt und durchgeführt werden

I. Ausgangslage

Freiwillige Audits leisten einen bedeutenden Beitrag für den Datenschutz, weil sie als aus eigenem Antrieb veranlasste Maßnahme die Chance in sich bergen, zu mehr Datenschutz in der Fläche zu gelangen.

Datenschutz sollte ein Wettbewerbsvorteil sein. Unternehmen, die sich um einen hohen Datenschutzstandard bemühen, möchten dies auch anerkannt sehen. Ein Datenschutzzertifikat ist ein wichtiges Signal an diese Unternehmen.

Zugleich trägt ein Zertifikat dazu bei, das Vertrauen von Bürgerinnen und Bürgern, Verbraucherinnen und Verbraucher in den achtsamen Umgang mit ihren Daten zu fördern.

Eigenverantwortung ist eine wichtige Säule für einen funktionierenden Datenschutz.

Der Ruf nach einem Audit hat im Zuge der Diskussion um den Europäischen Rechtsrahmen weiteren Auftrieb erhalten. Initiativen auf Landesebene und nunmehr auch auf Bundesebene haben dieses Anliegen aufgegriffen.

II. Erprobung von Modellen, Anforderungen

Die Gesetzgeber haben bisher lediglich einzelne Teilregelungen zu Zertifizierungen getroffen.

Der Düsseldorfer Kreis unterstützt weitergehende Bemühungen, Erfahrungen mit Zertifizierungen zu sammeln, die in **eigener** Verantwortung im Wege der Selbstregulierung auf der Grundlage von Standards erfolgen, die die Aufsichtsbehörden befürworten.

Verlässliche Aussagen für Bürgerinnen und Bürger, für Verbraucherinnen und Verbraucher erfordern, dass Zertifizierungsdienste anbietende Stellen (Zertifizierungsdienste) geeignete inhaltliche und organisatorische Vorkehrungen für derartige Verfahren mit dem Ziel treffen, eine sachgerechte und unabhängige Bewertung zu gewährleisten.

Dazu gehören im Kern folgende, von Zertifizierungsdiensten zu bearbeitende Strukturelemente:

- Prüffähige Standards, die von den Aufsichtsbehörden befürwortet werden, zu entwickeln, zu veröffentlichen und zur Nutzung für Dritte freizugeben,

- beim Zertifizierungsprozess zwischen verschiedenen Ebenen zu unterscheiden (Prüfung, Zertifizierung, Akkreditierung),

- für verschiedene auf Ebenen und/oder in Verfahrensabschnitten anfallende Aufgaben voneinander abzugrenzende Rollen der jeweils Mitwirkenden vorzusehen,

- Regelungen zur Vermeidung von Interessenkollisionen der an einem Zertifizierungsprozess Beteiligten zu treffen,

- Anforderungen an die Eignung als Prüferin und Prüfer festzulegen und diesen Personenkreis für Zertifizierungen zu qualifizieren,

- den geprüften Sachbereich so zu umschreiben, dass Bürgerinnen und Bürger, Kundinnen und Kunden die Reichweite der Prüfaussage ohne weiteres dem Zertifikat entnehmen können,

- Bedingungen für Erteilung, Geltungsdauer und Entzug von Zertifikaten zu bestimmen,

- Zertifikate zusammen mit den wesentlichen Ergebnissen der Prüfberichte zu veröffentlichen.

III. Abstimmung im Düsseldorfer Kreis

Der Düsseldorfer Kreis verfolgt die Entwicklung von sowohl auf Landesebene mit dieser Zielrichtung begleiteten Initiativen als auch auf Bundesebene begonnenen weiteren Initiativen. Er beteiligt sich an einer ergebnisoffenen Diskussion, um zu optimalen Verfahrensgestaltungen zu gelangen.

Die im Düsseldorfer Kreis zusammenwirkenden Aufsichtsbehörden sehen daher als gemeinsame Aufgabe, sich auf inhaltliche und verfahrensmäßige Anforderungen für Zertifizierungsverfahren zu verständigen und zu Beratungsersuchen im Interesse einer bundesweit einheitlichen Aufsichtspraxis auf im Düsseldorfer Kreis abgestimmter Grundlage Stellung zu nehmen.

14.4.2 Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams)

Mittlerweile nimmt der Einsatz sog. Dashcams auch in Deutschland immer mehr zu, um, so die standardmäßige Begründung, im Falle eines Unfalls den Hergang nachvollziehen und das Video gegebenenfalls als Nachweis bei der Regulierung von Schadensfällen und der Klärung von Haftungsfragen heranziehen zu können.

Die Aufsichtsbehörden des Bundes und der Länder für den Datenschutz im nichtöffentlichen Bereich machen darauf aufmerksam, dass der Einsatz solcher Kameras - jedenfalls sofern dieser nicht ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt - datenschutzrechtlich unzulässig ist.

Soweit mit den Dashcams in öffentlich zugänglichen Bereichen gefilmt wird und als Hauptzweck der Aufnahmen die Weitergabe von Filmaufnahmen zur Dokumentation eines Unfallhergangs angegeben wird, ist der Einsatz - auch wenn die Kameras von Privatpersonen eingesetzt werden - an den Regelungen des Bundesdatenschutzgesetzes zu messen. Gemäß § 6b Abs. 1 Nr. 3 und Abs. 3 des Bundesdatenschutzgesetzes (BDSG) ist eine Beobachtung und Aufzeichnung mittels Videokameras nur zulässig, soweit dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Diese Voraussetzungen sind in aller Regel nicht erfüllt, da die schutzwürdigen Interessen der Verkehrsteilnehmer überwiegen. 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. Dashcams zeichnen den Verkehr sowie Personen, die sich in der Nähe einer Straße aufhalten, ohne Anlass und permanent auf, so dass eine Vielzahl von Verkehrsteilnehmern betroffen ist, die sämtlich unter einen Generalverdacht gestellt werden, ohne dass sie von der Überwachung Kenntnis erlangen oder sich dieser entziehen können. 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.

14.5 Beschluss vom Mai 2014

14.5.1 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.

14.6 Beschluss vom 16. Juni 2014

14.6.1 Orientierungshilfe zu den „Datenschutzanforderungen an App-Entwickler und App-Anbieter

Die Orientierungshilfe richtet sich an Entwickler und Anbieter mobiler Applikationen (Apps). Sie zeigt datenschutzrechtliche und technische Anforderungen auf und macht diese anhand plakativer Beispiele verständlich.

Inhaltsverzeichnis

1. Zielgruppe und Ziel

Zielgruppe dieser Orientierungshilfe sind Entwickler und Anbieter[1] mobiler Applikationen (Apps) im nicht-öffentlichen Bereich[2], die als Telemediendienst zu qualifizieren sind und auf die ganz oder auf Teil-Dienste der App die datenschutzrechtlichen Regelungen der §§ 11 ff. des Telemediengesetzes (TMG) vollumfänglich Anwendung finden.[3] Nicht im Fokus dieser Orientierungshilfe stehen somit App-Angebote, deren Dienst ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze besteht bzw. Rundfunk (i. S. d. § 2 des Rundfunkstaatsvertrages-RStV) darstellen oder die offline[4] betrieben werden. Auch werden Apps, welche Teil des jeweiligen Betriebssystems sind und Besonderheiten von Apps[5], die für spezielle Endgeräte wie z. B. Smart-TVs oder Smart-Watches entwickelt und angeboten werden, nicht im Rahmen dieses Dokumentes berücksichtigt.[6] Die Orientierungshilfe bezieht sich ausschließlich auf (Online-) Apps für Smartphones und Tablets.

App-Entwickler sollten bereits in der Entstehungs- und Entwicklungsphase einer App die datenschutzrechtlichen Vorgaben kennen und durch datenschutzgerechte Gestaltung („privacy by design“) sowie datenschutzfreundliche Voreinstellungen („privacy by default“) dafür Sorge tragen, dass die App später ohne datenschutzrechtliche Mängel angeboten werden kann. Soweit der Entwickler in der Anwendungsphase[7] (z. B. im Rahmen von Fehlermeldungen) personenbezogene Daten erhält und verwendet[8], ist er selbst Adressat datenschutzrechtlicher Anforderungen und muss diese kennen und umsetzen.

Wird eine App nicht datenschutzkonform angeboten, weil unzulässig personenbezogene Daten erhoben und verwendet werden, können insbesondere den **App-Anbieter** als verantwortliche Stelle aufsichtsrechtliche Maßnahmen oder Bußgelder treffen.

---

[1] Die Trennung wird vorgenommen, da für die Entwicklung einer App häufig externe Dienstleister beauftragt werden. Soweit die App vom App-Anbieter selbst entwickelt wird, fallen beide Eigenschaften zusammen, so dass von diesem die vorgestellten Regelungen sowohl in der Entwicklung als auch während des Produktivbetriebes zu beachten sind.

[2] Die Orientierungshilfe findet nur für nicht-öffentliche Stellen direkte Anwendung. In Kapitel 9.4 wird ein knapper Hinweis für öffentliche Stellen gegeben.

[3] Die §§ 11 ff. TMG finden vollumfänglich Anwendung, soweit es sich um einen Telemediendienst handelt, der nicht überwiegend in der Übertragung von Signalen über Telekommunikationsnetze besteht (vgl. § 11 Abs. 3 TMG).

[4] Entscheidend dabei ist nicht der Verwendungszweck der App, sondern ob tatsächlich Daten übermittelt werden. Dies ist für den Nutzer allerdings nur schwer zu erkennen.

[5] Die in dieser Orientierungshilfe dargestellten Grundsätze gelten jedoch auch für solche Apps, soweit diese als Telemedien gelten.

[6] Somit gilt die Orientierungshilfe grundsätzlich direkt für alle Apps, die
- keinen Messenger-Dienst oder VoIP-Dienst anbieten,
- keinen Rundfunk anbieten (Radio, TV) und
- eine Online-Verbindung bei der Nutzung benötigen (vgl. Fn.4).

[7] Unter Anwendungsphase ist der Produktivbetrieb der App zu verstehen.

[8] Der Begriff „Verwenden“ personenbezogener Daten wird in den §§ 11 ff. TMG verwendet. 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.

Um dieser Verantwortung gerecht zu werden, muss bei der Entwicklung und bei dem Angebot einer App beachtet werden, dass die Erhebung und Verwendung personenbezogener Daten datenschutzrechtlichen Regelungen unterliegt. Um aufzuzeigen, in welchem datenschutzrechtlichen Rahmen sich App-Anbieter und ggf. auch App-Entwickler bewegen, geht die Orientierungshilfe nach einer kurzen Darstellung der Grundlagen auf den anzuwendenden Rechtsrahmen (Kapitel 2), die Verantwortlichkeiten (Kapitel 3), auf die Erlaubnistatbestände und die allgemein zu beachtenden Datenschutzgrundsätze (Kapitel 4) sowie die Nutzerrechte (Kapitel 5) ein. Im Anschluss daran werden grundlegende Anforderungen an den technischen Datenschutz (Kapitel 6) und die Problematik eines erhöhten Schutzbedarfs bei dem Umgang mit besonderen Arten personenbezogener Daten (Kapitel 7) besprochen. Zuletzt werden die mit dieser Orientierungshilfe angesprochenen Akteure auf die Konsequenzen eines unzulässigen Datenumgangs und auf Besonderheiten hingewiesen (Kapitel 8 und 9).

2. Anwendbarkeit deutschen Datenschutzrechts

2.1. Räumlicher Anwendungsbereich

App-Anbieter und weitere datenverarbeitende Stellen müssen sich gem. § 1 Bundesdatenschutzgesetz (BDSG) an die deutschen Datenschutzgesetze halten, soweit diese ihren Sitz bzw. eine datenverarbeitende Niederlassung in der Bundesrepublik Deutschland (BRD) haben. Befindet sich weder der Sitz des App-Anbieters noch eine datenverarbeitende Niederlassung desselben innerhalb der BRD, ist danach zu unterscheiden, ob sich der Sitz bzw. eine datenverarbeitende Niederlassung innerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR, umfasst zusätzlich zu den Mitgliedsstaaten noch Island, Norwegen, Liechtenstein) befindet. Trifft dies zu, ist das jeweils nationale Datenschutzrecht des Mitgliedstaats oder Vertragsstaats anzuwenden. Liegen der Sitz und etwaige Niederlassungen ausschließlich außerhalb der EU bzw. des EWR, ist der Anwendungsbereich des deutschen Datenschutzrechts eröffnet, wenn personenbezogene Daten im Inland (BRD) mittels der App erhoben und verwendet werden.[9]

Beispiele:

- Ein App-Anbieter mit Sitz/Niederlassung in München erhebt mittels seiner App personenbezogene Daten: Deutsches Datenschutzrecht findet Anwendung.
- Ein amerikanisches Unternehmen mit einer für die Datenverarbeitung relevanten Niederlassung in Irland (und nicht in Deutschland) erhebt mittels seiner App personenbezogene Daten bei Bewohnern Deutschlands: Irisches Datenschutzrecht findet Anwendung.

[9] Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten der Artikel 29 Gruppe, WP 202, Ziffer 3.1, vgl. auch Stellungnahme 8/2010 zum anwendbaren Recht der Artikel 29 Gruppe, WP 179, Kapitel III.4 und IV.2.

- Ein Unternehmen mit Sitz in China ohne weitere Niederlassung in Europa erhebt mittels einer App personenbezogene Daten bei Bewohnern Deutschlands: Deutsches Datenschutzrecht findet Anwendung.

2.2. Sachlicher Anwendungsbereich

Der sachliche Anwendungsbereich des Datenschutzrechts ist eröffnet, soweit es um den Umgang mit personenbezogenen Daten geht. Ein personenbezogenes Datum i. S. d. § 3 Abs. 1 BDSG ist gegeben, soweit eine Information, direkt oder auch nur mit Hilfe von Zusatzwissen (Bestimmbarkeit), auf eine Person zurückgeführt werden kann. Die Bestimmbarkeit einer Person im Zusammenhang mit mobilen Geräten und Apps ist insbesondere bei folgenden Informationen zu bejahen[10]:

- **IP-Adresse** des Nutzers, welche in der Regel als personenbezogenes Datum gilt. Dieser bedarf es auch bei Apps notwendigerweise für die Internetkommunikation.

- Eindeutige **Geräte- und Kartenkennungen**, die dauerhaft mit dem Gerät bzw. der Karte verbunden sind, können regelmäßig durch verschiedene Stellen einer Person zugeordnet werden. So werden die Kennungen mitunter von den Netzbetreibern gemeinsam mit dem Namen etc. einer Person gespeichert oder die Kennungen in Verbindung mit einer Registrierung der registrierten Person zugeordnet.
  Die bekanntesten Kennungen sind die:
  - IMEI: International Mobile Equipment Identity (=Gerätenummer)
  - UDID: Unique Device ID (=Gerätenummer eines iOS-Gerätes)
  - IMSI: International Mobile Subscriber Identity (=Kartennummer)
  - MAC-Adresse: Media AccessControl-Adresse (=Hardware-Adresse eines Netzwerkadapters)
  - MSISDN: Mobile Subscriber ISDN-Number (=Mobilfunknummer)

- **Name des Telefons**, soweit ein Nutzer sein Telefon unter Verwendung des eigenen Namens benennt.

- **Standortdaten** können zumeist ebenfalls einer bestimmbaren Person zugeordnet werden, da oftmals zu dem Standortdatum ein weiteres Datum, wie z. B. die IP-Adresse oder eine anderweitige eindeutige Kennung mitgesandt wird. Darüber hinaus kann eine Person bei Kumulierung mehrerer Standortdaten aufgrund eines Bewegungsprofils identifizierbar sein, wenn hierdurch ein bestimmtes, individuelles Bewegungsverhalten erfasst wird (z. B. Weg zur Arbeit).

[10] Vgl. hierzu auch: Stellungnahme 02/2013 zu Apps auf intelligenten Endgeräten der Artikel 29 Gruppe, WP 202, Ziffer 3.1.

- **Audiodaten** mit Stimmaufnahmen stellen ebenfalls personenbezogene Daten dar, da durch einen Stimmabgleich die Person, der die Audiodaten zuzuordnen sind, eindeutig identifiziert werden kann. Dies gilt entsprechend für **Foto- und Filmaufnahmen** einer Person.

- **Daten für biometrische Erkennungsverfahren** wie der Fingerabdruck, die Iris und die Gesichtsgeometrie sollen gerade dazu dienen, eine einzelne Person eindeutig zu identifizieren und stellen somit personenbezogene Daten dar.

- **Informationen über die App-Nutzung**: Welche App wurde z. B. wann durch den Nutzer genutzt.

Neben diesen, besonders hervorgehobenen personenbezogenen Daten, können zahlreiche weitere Informationen, die auf dem mobilen Gerät gespeichert sind, von diesem generiert oder durch den Nutzer eingegeben werden, unter die o. g. Definition der personenbezogenen Daten fallen. Hierzu gehören bspw. Kontaktdaten im Adressbuch, Kalendereinträge, Registrierungsdaten, Anruflisten, Nachrichten (z. B. SMS, E-Mails), Namen, Adressen und Kontoverbindungsdaten.

3. Verantwortlichkeiten

Adressat datenschutzrechtlicher Vorgaben für den Datenumgang ist vorliegend[11] grundsätzlich der App-Anbieter, als diejenige Stelle, die die personenbezogenen Daten für sich selbst erhebt (vgl. § 3 Abs. 7 HS. 1 BDSG). Dies gilt auch, soweit der App-Anbieter seine App nicht selbst entwickelt hat, sondern diese „nur“ anbietet. Auch in diesem Fall obliegt es dem App-Anbieter als verantwortliche Stelle, sich über den Datenumgang, welcher mittels der App stattfindet, zu informieren und die Einhaltung der einschlägigen datenschutzrechtlichen Anforderungen zu überprüfen. Bei einer Überprüfung des App-Angebotes durch die Aufsichtsbehörde kann nicht auf den App-Entwickler verwiesen werden. Auch für den Nutzer der App ist der App-Anbieter die Anlaufstelle für seine Nutzerrechte (z. B. Auskunft, Löschung etc.).

Auch wenn die personenbezogenen Daten von einer Stelle im Auftrag des App-Anbieters erhoben und verwendet werden, ist der App-Anbieter weiterhin als verantwortliche Stelle Adressat der datenschutzrechtlichen Anforderungen (vgl. § 3 Abs. 7 HS. 2 BDSG). Durch die Vergabe der Datenverarbeitung an einen Dienstleister wird er zum Auftraggeber, der Dienstleister wird Auftragnehmer. Bei der Auftragsdatenverarbeitung ergeben sich für den App-Anbieter vielfältige Sorgfalts- und Kontrollverpflichtungen, welche in § 11

[11] Die vorliegende Orientierungshilfe richtet sich ausschließlich an App-Anbieter und App-Entwickler, nicht jedoch an weitere mögliche Akteure wie z. B. Werbenetzwerkbetreiber und Nutzer.

BDSG dargestellt und geregelt sind. Die Erfüllung der Vorgaben zur Auftragsdatenverarbeitung erfordert zum einen eine geeignete und rechtssichere Ausgestaltung der Verträge mit dem Auftragnehmer. Weiterhin ergeben sich für den Auftraggeber fortwährende Kontrollpflichten. So soll er z. B. durch das Führen von Protokollen über Vor-Ort-Kontrollen beim Auftragnehmer jederzeit die Ausübung der ihm obliegenden Sorgfalts- und Kontrollverpflichtungen nachweisen können. Unter Umständen können geeignete Zertifizierungen bzw. Gütesiegel eine Vor-Ort-Kontrolle ersetzen.[12]
Der Auftragnehmer ist hingegen verpflichtet, streng weisungsgebunden zu agieren und die personenbezogenen Daten einzig für die Zwecke der verantwortlichen Stelle zu erheben und zu verwenden.[13] Obwohl er verpflichtet ist, die Weisungen des Auftraggebers zu befolgen, obliegt es ihm, den Auftraggeber unverzüglich darauf hinzuweisen, soweit eine Weisung gegen Datenschutzbestimmungen verstößt.

Beispiele:

- Wird die App auftragsgemäß über den Server eines Dienstleisters betrieben und werden die personenbezogenen Daten dort gespeichert, so ist der App-Anbieter als Auftraggeber die datenschutzrechtlich verantwortliche Stelle.
- Wird ein Verfahren zur Reichweitenmessung eingesetzt und die Auswertung durch einen Dienstleister durchgeführt, ist der App-Anbieter als Auftraggeber die datenschutzrechtlich verantwortliche Stelle.

Auch wenn Dienstleister für den technischen Betrieb einer App eingesetzt werden, konkret Cloud-Anbieter, welche unentgeltlich oder gegen Bezahlung Datenverarbeitungsressourcen wie Speicherplatz oder Rechenleistung bereitstellen, trifft ebenfalls der datenschutzrechtliche Sachverhalt der Auftragsdatenverarbeitung zu.

Bei Cloud-Diensten sitzt der Auftragnehmer häufig nicht im Inland und nicht innerhalb eines Mitgliedstaats der EU oder eines Vertragsstaats des EWR und/oder findet die Datenverarbeitung ganz oder teilweise im außereuropäischen Raum statt, beispielsweise in den USA oder in Asien. Somit liegt regelmäßig eine Datenübermittlung[14] in Drittstaaten vor. Zu den Pflichten bei der Auftragsdatenverarbeitung kommen dann weitere Anforderungen hinzu. So muss z. B. im Rahmen der Vertragsgestaltung die Zulässigkeit der

[12] Vgl. Orientierungshilfe „Cloud-Computing der Arbeitsgruppen Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26.09.2011, Kapitel 3.2. Abrufbar unter https://www.datenschutz.rlp.de/downloads/oh/ak_oh_cloudcomputing.pdf.

[13] Weitere Informationen zur Auftragsdatenverarbeitung: http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/BayLDA_Auftragsdatenverarbeitung.pdf.

[14] Im Gegensatz zum innereuropäischen Datenumgang liegt ein Übermittlung an einen Dritten vor, vgl. § 3 Abs. 8 S. 1 BDSG. Neben der datenschutzrechtlichen Erlaubnis zur Übermittlung bedarf es in einer zweiten Stufe eines angemessenen Datenschutzniveaus.

Datenverarbeitung und die Zweckbindung der verarbeiteten Daten explizit thematisiert und definiert werden.[15]

Beispiel:
Die Daten, welche über die Endgeräte der App-Nutzer erhoben werden, werden je nachdem an welchem Ort Speicherplatz vorhanden ist, in Frankreich, in den USA oder auf Indonesien gespeichert.

Neben dem App-Anbieter kann es weitere Verantwortlichkeiten geben:

- Sobald ein App-Entwickler rechtswidrig agiert, indem er z.B. entgegen den Weisungen des Auftraggebers personenbezogene Daten erhebt und verwendet bzw. über den Umfang einer Weisung oder eines (Entwickler-) Auftrages hinaus datenverarbeitend tätig wird oder personenbezogene Daten ohne Erlaubnis und somit unzulässigerweise eigenständig erhebt und verwendet, kann der App-Entwickler selbst zu einer verantwortlichen Stelle werden.
  Der App-Entwickler als Auftragnehmer ist streng weisungsgebunden und muss den Auftraggeber auf Weisungen, die gegen datenschutzrechtliche Bestimmungen verstoßen hinweisen, während der Auftraggeber den Auftragnehmer kontrollieren muss, um einen weisungswidrigen Datenumgang zu verhindern (vgl. auch oben).
  Der App-Entwickler als verantwortliche Stelle ist an den Grundsatz des Verbots mit Erlaubnisvorbehalt gebunden und bedarf für jegliche Datenerhebung und -verwendung einer Erlaubnis.

  Beispiel:
  Eine App sendet bei einem Fehler automatisiert eine entsprechende Meldung an den App-Entwickler, ohne dass der App-Anbieter eine Fehlerkontrolle angeordnet bzw. von einer solchen Kenntnis hat. Da die Datenerhebung und -verwendung außerhalb eines Auftrages stattfindet und keine Rechtsgrundlage für die Erhebung und Verwendung der personenbezogenen Daten (zumindest die IP-Adresse wird übertragen) ersichtlich ist, handelt der App-Entwickler widerrechtlich.

- Der Betreiber eines App-Stores kann die für die Datenverarbeitung verantwortliche Stelle sein, soweit er (zusätzlich zum Anbieter der App) zu eigenen Zwecken personenbezogene Daten des Endnutzers erhebt oder verwendet und den Umfang der Datenerhebung und -verwendung festlegt.

[15] Weitere Informationen zum Thema Nutzung von Cloud-Diensten und der hierbei entstehenden Verantwortung und Kontrolle durch den Auftraggeber liefert die „Orientierungshilfe Cloud Computing“ der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, erhältlich unter http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf (Version 01, 29.09.2011).

Beispiele:

- Ein Nutzer muss sich bei einem App-Store anmelden, um hierüber eine bestimmte App herunterladen zu können. Die bei dem App-Store angegebenen Daten werden von diesem zu (eigenen) Abrechnungszwecken erhoben und verwendet.
- Verwaltung von Abonnenten einer Zeitungs-App durch den App-Store, ohne dass der App-Betreiber die Abonnentendaten mitgeteilt bekommt bzw. Zugriff darauf nehmen kann. Der App-Store ist für die Verwaltung der Abonnenten verantwortliche Stelle.

4. Erlaubnistatbestände und Datenschutzgrundsätze

4.1. Erlaubnistatbestände

Im Datenschutzrecht gilt der Grundsatz des Verbotes mit Erlaubnisvorbehalt. Dies bedeutet, dass die Erhebung und Verwendung personenbezogener Daten grundsätzlich verboten ist, es sei denn, es existiert eine Erlaubnis dazu. Eine solche Erlaubnis kann sich einerseits aus einer Rechtsvorschrift oder aus einer Einwilligung[16] des Nutzers bzw. der betroffenen Person ergeben.

Während das BDSG als allgemeines Datenschutzgesetz gilt, sind u.a. die datenschutzrechtlichen Regelungen des TMG (§§ 11 ff. TMG) bereichsspezifische Rechtsvorschriften, welche den allgemeinen Datenschutzgesetzen vorgehen. So finden die Vorschriften des TMG immer dann Anwendung, wenn es um den Datenumgang auf der Diensteebene geht, d. h. bei einem Umgang mit Daten, die zur Bereitstellung des Dienstes erhoben und verwendet werden. Im Fokus sind einerseits die Bestandsdaten (vgl. § 14 TMG) und andererseits die Nutzungsdaten (vgl. § 15 TMG). Hiervon zu unterscheiden sind die Inhaltsdaten, also u. a. die Daten, die durch die App beim Anwender abgefragt werden - für diese Daten gelten in der Regel die allgemeinen Datenschutzgesetze (im nichtöffentlichen Bereich das BDSG).
Soweit personenbezogene Daten zur Bereitstellung des Telemedienangebots erhoben und verwendet werden sollen, bedarf es entweder einer Erlaubnis dazu in einer Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht oder einer Einwilligung des Nutzers, um die personenbezogenen Daten zulässigerweise erheben und verwenden zu können (vgl. § 12 Abs. 1 TMG).

Auf die im vorliegenden Kontext relevanten Erlaubnisse und Anforderungen an eine wirksame Einwilligung wird im Folgenden eingegangen:

[16] Soweit eine solche in Betracht kommt, vgl. Kapitel 4.1.3.

4.1.1. Erlaubnisse aus dem TMG

Die datenschutzrechtlichen Regelungen des TMG 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 S. 2 TMG) behandelt.[17]

4.1.1.1. Bestandsdaten

Gem. **§ 14 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. Welche personenbezogenen Daten konkret für diese Zwecke erforderlich sind, wird durch den jeweiligen Nutzungsvertrag bestimmt, der zwischen dem Diensteanbieter und dem Nutzer abgeschlossen wird. Zu den Bestandsdaten können insbesondere Name, Anschrift, Rufnummer, Registrierungsdaten und Zahlungsdaten zählen.

Nicht unter die Bestandsdaten sind die personenbezogenen Daten zu fassen, welche zwar über eine App erhoben werden, jedoch nicht zur Nutzung des Telemediums „App“ erforderlich sind, sondern für weitere, außerhalb des Telemediendienstes liegende Zwecke erhoben und verwendet werden (vgl. dazu unter Kapitel 4.1.2).

Beispiele:

- App eines sozialen Netzwerks oder Online-Portals:
  Die Zulässigkeit der Erhebung und Verwendung der bei der Registrierung angegebenen Daten ist nach dem TMG zu bewerten (= Bestandsdaten).
- Bestellung eines Buches bei einem Online-Versandhaus über die Versandhaus-App:
  Die für die Abwicklung des Kaufvertrags und die Lieferung des bestellten Buches erforderlichen personenbezogenen Daten sind als sogenannte Inhaltsdaten unter die Vorgaben des BDSG zu fassen. Der Telemediendienst an sich kann grundsätzlich auch ohne Vornahme einer Bestellung und Angabe der Adress- und Zahlungsdaten genutzt werden.

[17] Im Gegensatz dazu muss auf der Inhaltsebene zwischen dem öffentlichen und dem nicht-öffentlichen Bereich unterschieden werden (vgl. Kapitel 4.1.2).

4.1.1.2. Nutzungsdaten

4.1.1.2.1. Inanspruchnahme des Dienstes

Als Nutzungsdaten werden gem. § 15 Abs. 1 TMG hingegen diejenigen personenbezogenen Daten bezeichnet, die erforderlich sind, um die Inanspruchnahme des Dienstes zu ermöglichen. Das Gesetz zählt dabei

- Merkmale zur Identifikation des Nutzers,
- Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und
- Angaben über die vom Nutzer in Anspruch genommenen Telemedien auf.

Bei dieser Aufzählung handelt es sich nicht um eine abschließende Aufzählung. Zu den Nutzungsdaten zählen somit alle personenbezogenen Daten, welche notwendigerweise zur Nutzung der App durch den Diensteanbieter erhoben und verwendet werden müssen, wie z. B. die IP-Adresse oder - soweit im Einzelfall erforderlich - eindeutige Kennnummern oder der Standort. Für die Erbringung des Dienstes ist die Erhebung und Verwendung dieser Nutzungsdaten zulässig.

Beispiel:
Bedarf es für das Funktionieren der App des aktuellen Standortes, z. B. um die Wegstrecke zu einer angegebenen Adresse berechnen zu können, so darf das Standortdatum für diesen konkreten Zweck erhoben und verwendet werden.

4.1.1.2.2. Nutzungsprofil unter Pseudonym

§ 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 unter Pseudonym, soweit der Nutzer nicht widerspricht.[18]

Die Regelungen des § 15 Abs. 3 TMG berechtigen nur den Diensteanbieter selbst oder seine Auftragnehmer[19] zur Erstellung pseudonymisierter 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 S. 3 TMG).

[18] Soweit Art. 5 Abs. 3 der ePrivacy-Richtlinie (2002/58/EG in der Fassung 2009/136/EG) künftig Anwendung findet, ist bei der Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind (u. a. beim Einsatz von Cookies), grundsätzlich eine Einwilligung des Nutzers einzuholen.

[19] Die Einschaltung von Dienstleistern innerhalb der EU/ des EWR ist im Rahmen der Bestimmungen zur Auftragsdatenverarbeitung nach § 11 BDSG unter den dort genannten Voraussetzungen möglich.

Der Nutzer muss vom Diensteanbieter auf die Erstellung eines solchen Nutzungsprofils und die Möglichkeit dieser zu widersprechen hingewiesen werden. Dies muss zumindest im Rahmen der Datenschutzerklärung (vgl. Kapitel 5.2) geschehen.
Eindeutige Geräte- und Kartenkennungen wie die IMEI-Nummer (vgl. Kapitel 2.2) oder auch die IP-Adresse stellen kein Pseudonym dar. Diese Daten dürfen auch nicht in das Nutzungsprofil einfließen, da die Zusammenführung pseudonymer Nutzungsprofile mit Daten über den Träger des Pseudonyms unzulässig ist (Verstoß gegen § 15 Abs. 3 S. 3 TMG, § 13 Abs. 4 Nr. 6 TMG).

Die Widerspruchsmöglichkeit muss effektiv und angemessen sein. Es sollte daher eine direkte Opt-Out Möglichkeit (Link, Möglichkeit des Auskreuzens) für den Nutzer vorgehalten werden, welche mit möglichst einem Klick aktiviert werden kann. Der bloße Hinweis auf bestimmte Einstellungsmöglichkeiten am Gerät etc. genügt nicht. Stattdessen ist zumindest eine konkrete Anleitung, welche die Vornahme der entsprechenden Einstellungen geräteangepasst Schritt für Schritt darstellt, erforderlich. Auch 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).[20]

Widerspricht der Betroffene der Profilbildung unter Pseudonym, so sind etwa vorhandene Profildaten zu löschen oder wirksam zu anonymisieren.

Im Zusammenhang mit Apps wird die soeben dargestellte Erlaubnis insbesondere in den folgenden Konstellationen benötigt:

- **Reichweitenmessung**

Eine Nutzungsprofilerstellung unter Pseudonym gem. § 15 Abs. 3 TMG findet insbesondere zur Reichweitenmessung statt. Mittels einer Reichweitenmessung kann ein App-Anbieter feststellen, in welchem Umfang und auf welche Weise sein App-Angebot genutzt wird.

Auf die Voraussetzungen für die „Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten“ wurde vom Düsseldorfer Kreis

[20] Eine solche Möglichkeit zum Opt-out kann technisch jedoch erst innerhalb der App, d. h. nach deren Installation realisiert werden. Dies ist insbesondere dann zu beachten, wenn die Widerspruchsmöglichkeit in der Datenschutzerklärung enthalten ist, welche bereits innerhalb des App-Stores bzw. vor dem Start der App zum Abruf bereitgestellt werden muss (vgl. Kapitel 5.2).

mit Beschluss vom 26./27. November 2009 hingewiesen.[21] Diese Voraussetzungen sind auch bei einem Einsatz solcher Verfahren in Apps entsprechend 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,
- Unterrichtung über Erstellung pseudonymer Nutzungsprofile und über die Widerspruchsmöglichkeit und
- soweit ein Dienstleister eingesetzt wird, Abschluss eines Auftragsdatenverarbeitungsvertrages gem. § 11 BDSG.

Soweit etablierte Verfahren zur Reichweitenmessung eingesetzt werden, ist beim Einbau von Standardwiderspruchslösungen über die oben dargestellten Anforderungen an die Angemessenheit einer Widerspruchsmöglichkeit darauf zu achten, dass ein ausgeübter Widerspruch effektiv ist. Dies bedeutet z. B., dass ein im nativen Teil einer App gesetzter Widerspruch auch im Webview einer App, sofern vorhanden, wirksam ist.

- **Werbefinanzierte Apps**

Viele Apps können gebührenfrei genutzt werden. Allerdings werden diese Angebote vielfach durch eine Verarbeitung von Nutzungsdaten zu Werbezwecken finanziert. Dazu können beispielsweise auch die jeweiligen Aufenthaltsorte (Standortdaten) der Betroffenen verwendet werden, um ihnen möglichst passgenaue Werbung zu präsentieren. Werden Standortdaten für die Bewerbung erhoben und verwendet, so ist dies nur mit einer gesetzlichen Erlaubnis oder der Einwilligung des Nutzers möglich, soweit es sich bei den Standortdaten um personenbezogene Daten handelt (vgl. Kapitel 2.2).

Soweit die Erhebung und Verwendung der Nutzungsdaten von § 15 Abs. 3 TMG gedeckt ist, ist den Betroffenen ein wirksames Widerspruchsrecht einzuräumen. Signalisiert der Nutzer durch besondere Einstellungen auf seinem Endgerät, dass er eine Verarbeitung seiner Nutzungsdaten für Werbezwecke nicht wünscht, so ist auch[22] diese Erklärung als Widerspruch zu werten und durch den Diensteanbieter zu beachten.

[21] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 26./27. November 2009 in Stralsund „Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten“, abrufbar unter http://www.lda.bayern.de/onlinepruefung/Beschluss_Reichweitenmessung.pdf.

[22] Einstellungen auf dem Endgerät können unter Umständen eine wirksame Widerspruchsmöglichkeit darstellen, wenn durch den App-Anbieter die Wirksamkeit des Widerspruchs tatsächlich sichergestellt werden kann. Ist dies nicht möglich, so entbindet die Möglichkeit, bestimmte Einstellungen an den Endgeräten vornehmen zu können, den App-Anbieter nicht von der Verpflichtung eine (zusätzliche) wirksame Widerspruchsmöglichkeit anzubieten.

Über die oben beschriebene Erstellung von Nutzungsprofilen unter Pseudonym hinaus ist die Verarbeitung von Nutzungsdaten für Werbezwecke nur gestattet, wenn eine gesetzliche Erlaubnis (§ 15 Abs. 1 TMG) vorliegt oder der Nutzer wirksam in diese Verwendung der Nutzungsdaten für diesen Zweck eingewilligt hat.

4.1.1.3. Verwendung zu Abrechnungszwecken

Soweit die Nutzungsdaten durch den App-Anbieter bzw. App-Store-Betreiber für die Abrechnung kostenpflichtiger App-Angebote verwendet werden, handelt es sich um Abrechnungsdaten, deren Verwendung in den §§ 15 Abs. 2, 4 ff. TMG geregelt wird. Der Diensteanbieter darf Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus verwenden, wenn es für Zwecke der Abrechnung mit dem Nutzer erforderlich ist.

4.1.2. Erlaubnisse 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 BDSG Anwendung. Ein Datenumgang auf der Inhaltsebene ist dann anzunehmen, wenn online Daten zwischen dem Nutzer und dem App-Anbieter ausgetauscht werden, um ein Vertrags- oder Leistungsverhältnis zu begründen, das selbst keinen Telemediendienst darstellt („Offline-Vertrag“) oder aber solche, die ein Nutzer selbst in die App eingibt (ausgenommen sind Bestandsdaten, s. unter Kapitel 4.1.1.1). Zwar werden die Daten unter Anwendung des Telemediendienstes „App“ 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.

<u>Beispiele:</u>

- App eines Pizzadienstes, mittels welcher man Speisen und Getränke bestellt:
  Die Zulässigkeit der Erhebung und Verwendung der bei der Bestellung angegebenen Daten durch den Pizzadienst als verantwortliche Stelle ist nach dem BDSG zu bewerten, da die Umsetzung der Bestellung offline ausgeführt wird. Daten über z. B. den Zeitpunkt des Aufrufs der App oder das Klickverhalten in der App sind hingegen Nutzungsdaten im Sinne des TMG.
- Daten, die in ein Kontaktformular eingegeben werden, bspw. um eine Beschwerde anzubringen, soweit sie sich auf ein durch die App ermöglichtes Leistungsverhältnis außerhalb der App beziehen.

- Bei einer Kalender-App zählen die Daten über Termine oder bei einer Adress-App die Namen und Telefonnummern der Freunde zu den Inhaltsdaten.
- Bei der App eines sozialen Netzwerkes zählen die Profildaten eines persönlichen Profils und die Inhalte der Kommunikation zu den Inhaltsdaten.[23]

4.1.3. Einwilligung

Existiert kein gesetzlicher Erlaubnistatbestand, sind die Erhebung und Verwendung personenbezogener Daten dennoch im Regelfall mit einer wirksamen Einwilligung der betroffenen Person bzw. des Nutzers möglich.
Soweit eine Einwilligung in Betracht kommt, sind die Voraussetzungen für eine wirksame Einwilligung - je nachdem ob das 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 TMG für Telemedien die Einholung einer elektronischen Einwilligung.

Eine Einwilligung kann gegenüber dem Telemedienanbieter[24] elektronisch erklärt werden, wenn die Vorgaben des § 13 Abs. 2 und Abs. 3 TMG eingehalten werden. Hiernach wird verlangt, dass
- der Nutzer seine Einwilligung bewusst und eindeutig erklärt hat (z. B. durch Ankreuzen einer vorformulierten Einwilligung)[25],
- 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.[26] Hierauf ist der Nutzer bereits vor Erteilung der Einwilligung hinzuweisen.

Die Einwilligung muss freiwillig durch den Nutzer abgegeben worden sein.

---

[23] Vgl. Orientierungshilfe „Soziale Netzwerke“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14.03.2013, Kapitel 4.2.1.

[24] § 4a Abs. 1 S. 3 BDSG sieht eine Ausnahme vom Schriftformerfordernis vor, wenn wegen besonderer Umstände eine andere Form angemessen ist. Solche besonderen Umstände liegen nicht generell dann vor, wenn eine Einwilligung (außerhalb des TMG) bei der Nutzung einer App eingeholt werden soll. Im Regelfall ist deshalb gem. § 126 Abs. 3 i. V. m. § 126a BGB eine qualifizierte elektronische Signatur nach dem Signaturgesetz zu verlangen. Eine entsprechende Anwendung des § 13 Abs. 2, 3 TMG auf Einwilligungen außerhalb des TMG ist umstritten, so dass es entweder der Schriftform, der elektronischen Form gem. § 126a BGB oder besonderer Umstände, welche zur Angemessenheit einer anderen Form als der Schriftform führt, bedarf.

[25] Eine bewusste und eindeutige Einwilligung kann nicht über eine Opt-out-Lösung erlangt werden, bei der der Nutzer erst die entsprechende Voreinstellung abwählen muss, indem er z. B. ein bereits aktiviertes Kreuzchen deaktivieren muss.

[26] Es handelt sich nicht um eine wirksame Einwilligung, wenn der Nutzer entweder den Dienst „so nehmen muss, wie er ist“ oder den Dienst nicht in Anspruch nehmen kann und ein Widerruf der „Einwilligung“ nur durch Beendigung des Nutzungsvertrages möglich ist.

4.2. Datenschutzgrundsätze

4.2.1. Grundsatz der Direkterhebung

Gem. § 4 Abs. 2 S. 1 BDSG sind personenbezogene Daten grundsätzlich beim Betroffenen zu erheben. Ausnahmen bestehen nach § 4 Abs. 2 S. 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 Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte für die Beeinträchtigung eines überwiegend schutzwürdigen Interesses der betroffenen Person besteht. Die betroffene Person soll wissen, wer welche Daten zu welchen Zwecken über sie erhebt, verarbeitet und nutzt. Die personenbezogenen Daten müssen somit nicht nur bei ihr direkt, sondern auch unter Mitwirkung erlangt werden. Diese Mitwirkung kann sowohl aktiv als auch passiv durch die betroffene Person geschehen. In beiden Fällen muss die betroffene Person allerdings über die Datenerhebung Bescheid wissen. Findet eine Datenerhebung heimlich statt, so wird der Grundsatz der Direkterhebung verletzt, soweit nicht eine der genannten Ausnahmen greift.

Im Rahmen eines App-Angebotes ist es daher notwendig, den Nutzer konkret über die Erhebung und Verwendung seiner personenbezogenen Daten zu informieren.

Werden Daten von Dritten z. B. bei Adressbuch-Apps oder Apps mit Verbindung zu sozialen Netzwerken (Freundesliste) über eine App erhoben und verwendet, stellt sich die Frage, inwieweit dies zulässig ist. So hat das KG Berlin (Urteil vom 24.01.2014 - 5 U 42/12) im Zusammenhang mit der Erstellung einer Freundesliste und der Möglichkeit des Versands von Einladungs-E-Mails entschieden, dass es „an einer E-Mail-Werbung des Unternehmens fehlen [kann], wenn das Unternehmen zwar Nutzer auffordert, anderen Verbrauchern Einladungs-E-Mails zu übersenden, das Unternehmen dabei aber nur technische Hilfe leistet, damit die Nutzer bequem eine solche eigene persönliche Einladungs-E-Mail an Verwandte, Freunde und Bekannte versenden können.“[27]

Eine solche Einladungs-E-Mail ist allein dem privaten Nutzer zuzurechnen, wenn dieser sich in Kenntnis aller wesentlichen Umstände - und damit eigenverantwortlich - zur Versendung dieser E-Mails entschließt. Der auch für das Unternehmen werbende Effekt wird dabei durch den privaten Zweck der Einladungs-E-Mails verdrängt. Denn dem Nutzer geht es dabei allein darum, mit den von ihm Eingeladenen ebenfalls über das soziale Netzwerk und die von diesem gebotenen Vorteile kommunizieren zu können. Es muss keinem Verbraucher verwehrt werden, Freunden und Bekannten in einer E-Mail einen konkreten Hinweis auf ein von ihm für gut befundenes Produkt zu geben.

[27] Vgl. Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke der Artikel-29-Datenschutzgruppe, WP 163, Ziff. 3.8 Abs. 2, Seite 12.

4.2.2. Grundsatz der Datenvermeidung und der Datensparsamkeit

Nach dem in § 3a BDSG normierten Grundsatz der Datenvermeidung und der Datensparsamkeit sollten so wenig personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden. Diesem Ziel kann auch eine Pseudonymisierung i. S. d. § 3 Abs. 6a BDSG oder Anonymisierung i. S. d. § 3 Abs. 6 BDSG von Daten dienen. Aus diesem Grund ist bereits bei der Entwicklung einer App darauf zu achten, dass durch diese später nur diejenigen personenbezogenen Daten erhoben und verwendet werden, die erforderlich sind.

4.2.3. Grundsatz der anonymen und pseudonymen Nutzung

Soweit es dem Diensteanbieter technisch möglich und zumutbar ist, hat der Diensteanbieter 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 Pseudonym zu agieren, wenngleich eine Offenlegung der Identität gegenüber dem Diensteanbieter zur Erschwerung von Missbrauch hingenommen werden kann.[28]

4.2.4. Grundsatz der Zweckbindung

Jeder Umgang mit personenbezogenen Daten muss einen bestimmten, legitimen Zweck verfolgen. Eine Datensammlung ohne Verfolgung eines konkret festgelegten Zwecks ist genauso wenig zulässig wie die Änderung eines Zweckes und der Verwendung der bis dahin gesammelten Daten für diesen neuen Zweck, ohne dass auch für diesen Datenumgang eine Erlaubnis existiert. Soweit der verfolgte Zweck wegfällt, sind die personenbezogenen Daten grundsätzlich zu löschen. Bei Vorhandensein von Aufbewahrungsfristen (etwa nach Vorgaben der Abgabenordnung oder des Handelsgesetzbuches) o. ä. sind die Daten zu sperren und damit von den aktuellen Produktivdaten zu trennen.

Der Grundsatz der Zweckbindung spielt im Zusammenhang mit der Einholung von Berechtigungen und der damit zusammenhängenden Möglichkeit, Zugriff auf zahlreiche Daten nehmen zu können, eine besondere Rolle, sofern die Plattformen ein Berechtigungskonzept unterstützen. Dabei gelten die folgenden Anforderungen:

- Es dürfen nur die für die App erforderlichen Berechtigungen vom Nutzer angefordert werden. Dabei sind die Möglichkeiten, die die Plattform für die Rechtevergabe bietet,

[28] Vgl. Kapitel 4.5 der Orientierungshilfe „Soziale Netzwerke“ der Konferenz der Datenschutzbeauftragten und der Länder vom 14.03.2013.

auszuschöpfen. Einige Betriebssysteme bieten Berechtigungen nur in festen Kombinationen an, welche neben dem erforderlichen Recht auch nicht benötigte enthalten.[29] Soweit das durch die Begrenzung auf neuere Betriebssystemversionen vermieden werden kann, ist dies bei Entwicklung der App zu berücksichtigen. Lässt sich eine unnötige Berechtigungsgewährung nicht vermeiden, sollte der Anbieter in der Datenschutzerklärung (siehe Kapitel 5.2.4) über diesen Umstand aufklären und sich gegenüber dem Nutzer dazu verpflichten, von dem nicht erforderlichen Recht keinen Gebrauch zu machen.

- Auch wenn ein Nutzer bei der Installation einer App pauschale Berechtigungen erteilt, darf die verantwortliche Stelle dennoch lediglich auf diejenigen Daten zugreifen, die für den verfolgten legitimen Zweck benötigt werden. So ist z.B. ein Zugriff auf das gesamte Adressbuch des Geräts mit all den darin hinterlegten persönlichen Informationen des Nutzers und seiner Kontakte und deren Verwendung nicht zulässig, wenn lediglich z. B. eine Adresse für die Navigation mit einer App benötigt wird.

4.2.5. Grundsatz der Erforderlichkeit

Sofern Möglichkeiten bestehen, personenbezogene Daten durch Verarbeitungsschritte so zu verändern, dass der Informationsgehalt auf das erforderliche Mindestmaß begrenzt wird, ist dies entsprechend umzusetzen, sofern keine anderen Kriterien dies verhindern.

Beispielsweise sollten Standortdaten nur so genau übertragen werden wie es tatsächlich erforderlich ist. Dies spielt insbesondere bei Umkreissuchen eine wichtige Rolle. Hierbei ist es häufig nicht notwendig, dass der Standort des Nutzers metergenau erhoben und verwendet wird.

Zudem muss sich auch die Speicherdauer eines jeden personenbezogenen Datums am Grundsatz der Erforderlichkeit messen lassen.

5. Unterrichtung des Nutzers und Nutzerrechte

Der App-Anbieter muss zunächst ein Impressum (vgl. § 5 TMG) vorhalten und der Nutzer ist durch den App-Anbieter bereits zu Beginn des Nutzungsvorgangs ohne ein vorhergehendes eigenes Tätigwerden über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten zu informieren (vgl. § 13 Abs. 1 TMG). Daneben stehen dem Nutzer weitere Rechte zu, deren Erfüllung er teilweise aktiv verlangen muss.

[29] Z. B. lässt sich bei Android bis zur Version 4.03 der Zugriff auf das Kontaktverzeichnis nicht erteilen, ohne gleichzeitig Zugriffsrechte auf den Anrufverlauf zu bekommen. Diese Berechtigungskoppelung kann nur umgangen werden, indem die Unterstützung älterer Android-Versionen gezielt ausgeschlossen wird (siehe http://developer.android.com/reference/android/Manifest.permission.html#READ_CALL_LOG).

5.1. Impressum

Nach § 5 TMG haben Telemedienanbieter und somit diejenigen App-Anbieter, welche unter das TMG fallen, für geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien bestimmte Angaben leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu veröffentlichen. Ein geschäftsmäßig angebotenes Telemedium kann nur bei rein privaten Angeboten verneint werden. Ein privates Angebot wird jedoch kaum vorliegen, soweit eine App über einen App-Store angeboten wird. Die Geschäftsmäßigkeit erfordert nicht zwingend eine Gewinnerzielungsabsicht, allerdings wird eine gewisse Nachhaltigkeit und somit ein auf einen längeren Zeitraum ausgerichtetes Angebot verlangt. Apps im Anwendungsbereich dieser Orientierungshilfe (s. Kapitel 1) sind danach grundsätzlich als geschäftsmäßiger Telemediendienst einzuordnen.

Handelt sich bei dem App-Angebot um kommerzielle Kommunikation (Begriffsbestimmungen in § 2 Abs. 5 TMG), die Telemedien oder Bestandteile von Telemedien sind, sind gem. § 6 TMG weitere Voraussetzungen zu beachten.

5.2. Datenschutzerklärung

5.2.1. Pflichten des App-Anbieters

Der App-Anbieter hat gemäß § 13 Abs. 1 S. 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 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 S. 2 TMG). Letztere Unterrichtungspflicht zielt insbesondere auf den Einsatz von Cookies ab, betrifft jedoch nicht nur diese. Auch sollte die Datenschutzerklärung das Datum ihrer Erstellung enthalten.

5.2.2. Hinweise zum Nutzungsbeginn

Eine frühzeitige Verankerung dieser Datenschutzhinweise ist im Gegensatz zu einer Webseite nicht erst nach dem Aufruf des Dienstangebotes möglich, sondern bereits in dem Moment, in welchem die App in einem App-Store eingestellt wurde und vom Nutzer installiert werden kann oder auch vor dem eigentlichen Start der App auf dem Gerät des Nutzers. Die Datenschutzerklärung muss somit entweder im App-Store oder nach dem Herunterladen und vor dem Start der App für den Nutzer zum Abruf bereitgehalten werden. Die größten App-Stores empfehlen App-Anbietern bereits beim Einstellen der

App in den jeweiligen App-Store von dieser Möglichkeit Gebrauch zu machen, um den Nutzer umfassend über die Datenverarbeitung zu informieren.[30]

5.2.3. Jederzeit abrufbereite Unterrichtung

Unabhängig davon, auf welche Weise ein App-Anbieter zu Beginn des Nutzungsvorgangs informiert, muss der Nutzer zusätzlich jederzeit die Datenschutzerklärung abrufen können, so dass eine weitere Verankerung in der App zwingend erforderlich ist. Die Unterrichtung muss dabei jeweils leicht auffindbar platziert werden, so dass dem Nutzer die Kenntnisnahme der Informationen ohne Hindernisse möglich ist. Innerhalb der App kann so z. B. ein Informationsbutton „i“ oder sonstige leicht erreichbare und auffindbare Lösungen, wie „Rechtliches“, „Datenschutzhinweis“ oder „Datenschutzerklärung“ eingebaut werden. Inwieweit sich die Informationen innerhalb der App befinden oder lediglich verlinkt sind, ist grundsätzlich irrelevant. Soweit im Offline-Betrieb einer App personenbezogene Daten auf dem Gerät o. ä. abgelegt werden, um diese bei einem späteren Online-Betrieb zu übertragen, genügt eine Verlinkung auf eine Datenschutzerklärung unter Umständen nicht.

5.2.4. App-spezifische Datenschutzerklärung

Eine einfache Verknüpfung mit den Datenschutzhinweisen eines ähnlichen oder alternativen Webangebotes des gleichen Anbieters genügt nicht den Ansprüchen an eine Unterrichtung nach den Vorschriften des TMG zu dem konkreten Dienst, da es - auch soweit gefühlt der gleiche Dienst angeboten wird - erhebliche Unterschiede geben kann:

Im Gegensatz zu dem Aufruf einer Webseite werden bei der Installation von Apps Berechtigungen bei dem Nutzer eingeholt, mittels derer der App-Anbieter über die Schnittstellen auf die Funktionen des Gerätes und somit auch auf Daten, welche auf dem Gerät gespeichert sind, eingegeben oder generiert werden, zugreifen kann. Während eine App somit auf Funktionen des Geräts potentiell zugreifen kann, wie z. B. Kamera, Mikrofon, Kontaktbuch, Standort, Telefon, SMS etc., ist es durch das bloße Aufrufen einer Webseite für den Webseitenanbieter im Allgemeinen nicht ohne Nutzerbetätigung möglich, über den Internetbrowser auf das Gerät des Nutzers in dieser weitgehenden Form zuzugreifen. Etliche Berechtigungen werden gerade dazu benötigt, personenbezogene Daten zu erheben oder zu verwenden, so dass eine konkrete Unterrichtung des Nutzers zu Art, Umfang

[30] Google legt in Ziffer 4.3 des Android Developer Distribution Agreement (zuletzt abgerufen am 05.02.2014) gegenüber den App-Anbietern fest „Sie sind zudem verpflichtet, den betreffenden Nutzern rechtlich einwandfreie Datenschutzhinweise sowie einen entsprechenden Schutz zu bieten (http://play.google.com/intl/ALL_de/about/developer-distribution-agreement.html)“. Apple fordert in Ziffer 3.1 (b) des iOS Developer Program License Agreement (Version 1-22-10) „All information provided by You and Apple or Your end users in connection with this agreement or Your Application, including without limitation Licensed Application Information, will be current, true, accurate and complete (…)“ (https://www.eff.org/files/20100127_iphone_dev_agr.pdf).

und Zweck des Datenumgangs zwingend erforderlich ist. Soweit Berechtigungen sichtbar eingeholt werden, sind hierbei die jeweilige Berechtigung und die konkret stattfindenden Zugriffe (vgl. Kapitel 4.2.4) zu benennen.[31] Um nicht den Eindruck einer unvollständigen Information entstehen zu lassen, sollte darüber hinaus auch über Berechtigungen unterrichtet werden, welche einen Zugriff zwar ermöglichen, aber nicht für den Zweck der Datenerhebung vom App-Anbieter eingeholt und genutzt werden. Dem Nutzer muss sich beim Lesen der Datenschutzinformation erschließen, zu welchen Zwecken bestimmte Berechtigungen eingeholt werden.[32] Als nicht ausreichend ist eine negative Beschreibung anzusehen, bei der der App-Anbieter ausschließlich darstellt, was er nicht macht. Dem Nutzer ist der Umfang einer Berechtigung im Regelfall nicht bekannt; er kann somit nicht abschätzen, ob es sich um eine abschließende Darstellung handelt oder ob lediglich einige Datenumgänge herausgegriffen werden.

Eine weitere Abweichung zwischen App und Webseite besteht auch bei den Einstellungsmöglichkeiten für den Nutzer. 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 App-Nutzer über Betriebssystemmittel in der Regel nicht möglich, solch gezielte Maßnahmen selbst zu ergreifen. Werden diese allerdings in der Datenschutzerklärung unter Bezugnahme auf die Webseite dargestellt, so dienen diese Informationen nicht dem App-Nutzer. Er muss folglich davon ausgehen, dass die Datenschutzerklärung allgemein auf die Nutzung der App keine Anwendung findet.

5.2.5. Lesbarkeit

Wegen der beschränkten Display-Größe mobiler Endgeräte sind die Datenschutzhinweise vom App-Anbieter derart zu gestalten, dass der Nutzer jederzeit ohne großen Aufwand die gewünschten Informationen erhalten kann. Als besonders benutzerfreundlich hat sich dabei die Einteilung in Kapitel, welche einzeln geöffnet werden können, herausgestellt. Darüber hinaus kann es auch genügen, die wesentlichen Inhalte der Datenschutzerklärung wiederzugeben und für darüber hinausgehende Informationen gut sichtbar auf weitere Erläuterungen sowie die vollständige Datenschutzerklärung zu verlinken. Was die wesentlichen Inhalte der Datenschutzerklärung sind, bestimmt sich anhand des Funktionsumfangs der App. Zu den wesentlichen Inhalten können insbesondere Kontaktinformationen des Anbieters (Firmensitz), Beschreibung der Datenarten, die von der App erhoben

[31] Die standardmäßigen Berechtigungsbeschreibungen genügen aufgrund ihrer Abstraktheit nicht für eine hinreichende Information des Nutzers.

[32] Sobald eine Berechtigung für das Nutzen einer App nicht benötigt wird, sollte vermieden werden, diese vom Nutzer einzufordern, da sonst das Risiko besteht, dass bei künftigen Updates der App die bislang ungenutzte Berechtigung ohne Wissen des Nutzers verwendet wird und ggf. personenbezogene Daten des Nutzers erhoben, verarbeitet oder genutzt werden. Stattdessen muss beim Hinzufügen einer neuen Berechtigung beim Update einer App die Einwilligung des Nutzers eingeholt werden, sofern personenbezogene Daten des Nutzers durch die neue App-Berechtigung berührt werden.

werden (z. B. Standortdaten, Netzkommunikation, Kalender, Adressbuch, etc.), Erläuterung der Zwecke, für die diese Daten erhoben werden, Speicherdauer, Bezeichnung der Dritten, an die Nutzerdaten übermittelt werden, und der Zweck der Übermittlung an Dritte zählen.

5.2.6. Kontaktmöglichkeiten

Um dem Nutzer die unkomplizierte Wahrnehmung seiner Nutzerrechte (vgl. Kapitel 5.3) zu ermöglichen, ist eine einfache Kontaktmöglichkeit (z. B. postalische Adresse, E-Mail Adresse) zu einer bei dem Anbieter für datenschutzrechtliche Fragen zuständigen Stelle in der Datenschutzerklärung zu hinterlegen. Hier kann der App-Anbieter dem Nutzer die Gelegenheit geben, an zentraler Stelle seine Nutzerrechte geltend zu machen.

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 einer App für den Nutzer. App-Anbieter sollten deshalb wie auch bei anderen Verarbeitungen von Nutzerdaten (Bestands-, Nutzungs- und Inhaltsdaten) auf entsprechende Anfragen von Nutzern vorbereitet sein, um bei Bedarf zeitnah reagieren zu können.

6. Technischer Datenschutz

Eine zentrale Rolle bei der datenschutzgerechten Gestaltung spielt die Sicherheit einer App. Bereits im Entwicklungsprozess sollte zur Vermeidung erhöhter Entwicklungs- und Nachbesserungskosten darauf hingewirkt werden, kritische Schwachstellen von vornherein zu vermeiden und das Sicherheitsniveau der App auf ein Niveau zu setzen, das den datenschutzrechtlichen Anforderungen entspricht. Bei Verarbeitung personenbezogener Daten ergeben sich die notwendigen technischen Anforderungen an eine App aus den „Technischen und organisatorischen Maßnahmen“ nach § 9 BDSG (und der dazugehörigen Anlage) und aus § 13 Abs. 4 TMG. Nachfolgend werden zentrale Themenbereiche daraus vorgestellt:

6.1. Anmeldedaten

Im Rahmen einer **Authentifizierung** innerhalb der App ist zu berücksichtigen, dass im Falle einer Passwortauswahl ausreichend komplexe Passwörter entweder erzwungen oder durch explizite Darstellung der Passwortstärke empfohlen werden. Es muss dabei geprüft

werden, ob ein Verfahren mit Benutzername und Passwort als Anmeldekennung ausreicht oder ob das App-Angebot ein höheres Schutzniveau erfordert, das z. B. über eine Zwei-Faktor-Authentifizierung (z. B. über QR-Code, Zertifikate,…) erreicht werden kann. Bei der Passworteingabe sollte dabei die Möglichkeit bestehen, das durch den Nutzer eingetippte Passwort zu maskieren, um die Gefahr sog. Shoulder-Surfing-Angriffe zu minimieren.

Die Speicherung eines Passworts in Klartext lokal auf dem Gerät sollte vermieden werden, da dieses im Falle eines unberechtigten Zugriffs (z. B. durch Verlust, Schadsoftware,…) entwendet werden kann. Stattdessen sollte bei der ersten Anmeldung einer App am App-Server ein Zugangstoken, der für eine App und das eingesetzte Gerät eindeutig ist, zur Authentifizierung erzeugt werden. Zusätzlich sollte es die Möglichkeit geben, diesen Zugangstoken (z. B. bei Verlust des Geräts) über die Webseite des Diensteanbieters sperren zu können. Sofern Passwörter dennoch auf dem Gerät gespeichert werden, ist auf den Einsatz von starken kryptographischen Verfahren nach dem Stand der Technik[33] zu achten.

Bei erhöhtem Schutzbedarf ist eine Speicherung der Zugangsdaten im Allgemeinen nicht zulässig, da mit dieser Funktion, die meist als Komfortmerkmal zur App-Bedienung eingesetzt wird, das notwendige Schutzniveau bei Verlust des Gerätes nicht erreicht werden kann. Zusätzlich ist in diesem Fall darauf zu achten, dass eine Auto-Logout Funktion umgesetzt wird, die nach einer gewissen Zeit der Inaktivität (z. B. 5 Minuten) den Benutzer von der App (und ggf. dem App-Dienst) abmeldet.

Gerätekennungen wie IMEI-Nummern oder MAC-Adressen (oder auch davon abgeleitete Hashwerte) sollten nicht zur Authentifizierung verwendet werden, da diese mit wenig Aufwand gefälscht oder entwendet werden können.

Bei der Realisierung einer Passwort-Vergessen-Funktion ist darauf zu achten, dass das neue Passwort nicht im Klartext an den App-Nutzer übertragen wird. Stattdessen ist, wie bei Webapplikationen üblich, ein zeitlich befristeter Zugangslink (mit z. B. 10 Minuten Gültigkeitsdauer) an den Nutzer zu senden. Bei erhöhtem Schutzbedarf muss ein Passwort verschlüsselt oder über alternative Kommunikationswege (z. B. Telefonhotline mit Geheimwort) übermittelt werden.

Die Rechtevergabe einer App im Rahmen einer **Autorisierung** sollte serverseitig erfolgen, da das Risiko einer Umgehung von App-seitig umgesetzten Sicherheitsmechanismen sehr hoch ist.

[33] BSI - Technische Richtlinie. Kryptographische Verfahren und Schlüssellängen. Version 2014-01. Abrufbar unter: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html.

6.2. Eindeutige Kennungen

App-Entwickler müssen zudem verstärkt darauf achten, keine eindeutigen Daten als Identifizierungswerte im Hintergrund zu übertragen. Werden eindeutige Kennungen, wie z. B. die IMEI-Nummer oder die UDID (vgl. Kapitel 2.2), übertragen, gelten entsprechende Hinweis- und Zweckbindungspflichten (vgl. Kapitel 5.2) zur Datenschutzerklärung.

Sofern für das Nutzen der App eine eindeutige Kennung erforderlich sein sollte, wird empfohlen, eine zufallsgenerierte eindeutige Nummer (ein Token) zu erzeugen, die im Rahmen der App-Nutzung zwar eindeutig ist, außerhalb der App oder bei Neuinstallation jedoch keinen Bezug mehr zum Gerät bzw. Nutzer ermöglicht. Durch solche zufallsgenerierte Token wird die Möglichkeit der App-übergreifenden Nachverfolgung von Nutzern eingeschränkt. Nach Möglichkeit sollte dieser Token regelmäßig ausgewechselt werden.

6.3. Sichere Datenübertragung

Regelmäßig kommuniziert die App auf dem Gerät des Nutzers mit den Server-Backends des Anbieters oder sonstiger Dritter. Um sicherzustellen, dass personenbezogene Daten mit **normalem Schutzbedarf** während des Transports nicht unbefugt gelesen oder verändert werden, sollte sowohl beim Versand als auch beim Empfang entsprechender Daten die Kommunikationsverbindung mit dem Backend durch eine Transportverschlüsselung abgesichert sein. Die App und auch das Backend müssen daher so konfiguriert sein, dass eine sichere Verbindung auf Grundlage einer dem Stand der Technik entsprechenden Protokollvariante nach den Vorgaben des BSI oder höher ausgehandelt wird (zurzeit bspw. TLS 1.1 oder höher). Sollten diese Protokolle etwa aus Kompatibilitätsgründen nicht nutzbar sein, dürfen unsichere Varianten, wie bspw. SSL 3.0 bzw. TLS 1.0, allenfalls für einen kurzen Übergangszeitraum genutzt werden. Das Server-Backend sollte bei der Aushandlung der Verschlüsselung nur starke Chiffren (>= 128 Bit, bspw. 3DES, AES) verwenden und ausreichend große Schlüssellängen (>= 2048 Bit) einsetzen. Dabei sollten nur vertrauenswürdige Zertifikate, also solche, die von einer bekannten Zertifizierungsstelle ausgestellt wurden, zum Einsatz kommen.

Personenbezogene Daten dürfen auch bei der Nutzung von Transportverschlüsselung nicht in der URL bzw. im GET-Parameter der https-Anfrage übermittelt werden, da es durch Protokollierung der Aufrufe auf Seiten der App oder des Backend-Servers (etwa durch den Serverbetreiber) trotz Verschlüsselung zur Offenbarung personenbezogener Daten kommen kann.

Durch den Einsatz kurzlebiger Sitzungsschlüssel (Perfect Forward Secrecy) ist sicherzustellen, dass ein Angreifer aufgezeichnete Verbindungen selbst bei Brechen der Verschlüsselung einer Verbindung nicht nachträglich entschlüsseln kann. Zudem sollte

darauf geachtet werden, dass die zum Einsatz kommenden Softwarebibliotheken zumindest mit FIPS-140-2 Zertifizierung Stufe 1 kompatibel sind.

Werden durch oder an die App Daten mit **erhöhtem Schutzbedarf**, wie z. B. Gesundheits- oder Kreditkartendaten übertragen, so muss mittels Zertifikats- oder Public-Key-Pinning zusätzlich sichergestellt werden, dass Angreifer nicht durch Unterschieben vermeintlich valider Zertifikate die Verbindung kompromittieren können. Die zum Einsatz kommenden kryptographischen Algorithmen und Schlüssellängen müssen sich an der Dauer der Schutzwürdigkeit der personenbezogenen Daten orientieren (z. B. kann eine notwendige Schlüssellänge von bis zu 15360-Bit bei RSA-Verfahren[34] bei Gesundheitsdaten höhere Anforderungen nach sich ziehen, als aktuell eingesetzte Standardverfahren anbieten).

6.4. Lokale Datenspeicherung

Im Rahmen der App-Nutzung werden meist Daten auf dem Gerät lokal gespeichert. Dies können Benutzernamen, Zugangstoken, Cookies, Standortdaten, Adressen und app-spezifische-Daten in lokalen Datenbanken und Einstellungsdateien sein. Hierbei sollten nur diejenigen personenbezogenen Daten gespeichert werden, die unbedingt für den Betrieb der App notwendig sind. Auch die Speicherdauer muss sich an dieser Notwendigkeit orientieren. Diese Daten müssen ausreichend vor unbefugtem Zugriff geschützt werden. Dabei muss davon ausgegangen werden, dass ein Zugriff auf das Dateisystem des Geräts von Seiten eines Angreifers erfolgen kann, auch wenn dieser den Gerätenutzern aufgrund der Plattformbeschränkungen im Allgemeinen nicht möglich ist. Dies gilt insbesondere auch dann, wenn personenbezogene Daten auf der SD-Karte oder einem anderem leicht austauschbaren Datenträger des Geräts gespeichert werden.

Findet eine lokale Datenspeicherung durch eine App statt, ist dafür Sorge zu tragen, dass nach einem Deinstallieren der App auch die lokal gespeicherten personenbezogenen Daten des Nutzers gelöscht werden. Sollte es sich dabei um Daten handeln, die ggf. anderen Apps auf dem Gerät zur Nutzung zur Verfügung gestellt werden, so sollte der Nutzer gezielt bei der Deinstallation gefragt werden, ob er diese persönlichen Daten löschen oder auf dem Gerät belassen möchte.

Bei Speicherung von Daten mit **erhöhtem Schutzbedarf** müssen diese zusätzlich zu den Schutzmechanismen der Geräteplattform (z. B. Sandboxing) mit starken kryptographischen Verfahren nach aktuellem Stand der Technik[35] (z. B. Stand 2014: AES-256)

[34] ENISA, Algorithms, Key Sizes and Parameters Report, 2013 recommendations. Abrufbar unter https://www.enisa.europa.eu/ activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report.

[35] BSI - Technische Richtlinie. Kryptographische Verfahren und Schlüssellängen. Version 2014-01. Abrufbar unter: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html.

abgesichert werden. Statt einer dauerhaften verschlüsselten Speicherung ist es empfehlenswert, die besonderen personenbezogenen Daten auch nur für die Dauer der Anwendung vom Server zur Darstellung an die App zu übertragen - auf eine entsprechend der Speichertechnologien der mobilen Endgeräte geeignete Implementierung wie z. B. wirksame Löschung der verwendeten Speicherbereiche ist dabei zusätzlich zu achten.

6.5. Logging

Die Protokollierung von Fehlermeldungen und Systemereignissen spielt gerade im Entwicklungszustand einer App eine wichtige Rolle. Sobald die App jedoch produktiv und somit im App Store für den Nutzer abrufbar ist, sollte das sogenannte Logging möglichst nicht oder nur eingeschränkt eingesetzt werden. Abhängig von der eingesetzten Logging-Variante besteht zum Beispiel bei Android die Gefahr, dass personenbezogene Daten in das Systemlog geschrieben und durch andere Apps mit der entsprechenden Berechtigung ausgelesen werden können.

Sofern Daten nicht nur an den App-Anbieter, sondern auch an den Entwickler der App geschickt werden, z. B. Fehler-Reports zur App, so ist darauf zu achten, dass keine personenbezogenen Daten übertragen werden. Eine Erhebung und Verwendung personenbezogener Daten des Nutzers einer App ist auf Entwicklerseite in der Regel nicht erforderlich und müsste deshalb im Einzelfall begründet werden und von einem Erlaubnistatbestand gedeckt sein.

6.6. Einbindung von Webseiten

Werden im Rahmen der App-Nutzung Inhalte von Webseiten eingebunden, besteht die Gefahr, dass dadurch auch das ggf. unberechtigte Laden von Drittanbieter-Inhalten datenschutzrechtliche Verstöße wie z. B. eine Reichweitenmessung ohne wirksame Widerspruchsmöglichkeiten nach sich zieht. Es ist technisch möglich, durch einen In-App-Browser ganze Webinhalte in der App zu integrieren, ohne dass es dem Nutzer ersichtlich ist, dass eine Internetseite innerhalb der App aufgerufen wird. Entsprechend ist es hierbei erforderlich, dass bei der Einbindung von Webseiteninhalten in der App darauf geachtet wird, welcher Webseitencode geladen wird. Durch Einstellungen seitens des Entwicklers wie Deaktivierung von JavaScript und Plug-ins kann beispielsweise bereits die Ausführung eines Teils des geladenen Webseitencodes technisch unterbunden werden. Des Weiteren müssen die Drittanbieterinhalte bei der Ausgestaltung der rechtlichen Anforderungen (z. B. der Datenschutzerklärung) beachtet werden.

6.7. Standortdaten

Sofern durch die App auf Standortdaten des Geräts zugegriffen wird, muss darauf geachtet werden, dass dies nur im zulässigen Umfang geschieht. Hierbei gilt es zu berücksichtigen, dass nur in der unbedingt nötigen Auflösung auf die Geodaten zugegriffen werden sollte, d. h. dass eine gezielte Verwaschung des Standorts erfolgt (z. B. statt „München Bahnhofsplatz 1“>„München Stadtmitte“). Dies kann z. B. durch Nullung von Dezimalstellen in den GPS-Koordinaten innerhalb der App vor Versand an den Backend-Server erreicht werden.

Des Weiteren sollten Standortdaten, soweit für die Anwendung möglich, nur lokal auf dem Gerät verarbeitet werden. In Kombination mit einer Standortlogik, die auf verwaschenen Koordinaten beruht, können standortgenaue Dienste ohne Übermittlung des genauen Standorts an den App-Anbieter realisiert werden. Wird z. B. der Standort „München Stadtmitte“ für die Suche nach Geldautomaten an den App-Anbieter übermittelt, so kann Karten- und Automatenstandortmaterial zu diesen verwaschenen Koordinaten an die App geliefert werden. Durch eine lokale Auswertung der genauen Standortdaten in Bezug auf das gelieferte Kartenmaterial können innerhalb der App individuelle Routen für den App-Nutzer ermittelt werden.

Eine Speicherung von Standortdaten auf dem Gerät darf nur dann stattfinden, wenn dies für die Funktionalität der App notwendig ist, da mit diese Daten bei unberechtigtem Zugriff Bewegungsprofile erstellt werden können.

Sofern Standortdaten von der App an das Backend des App-Anbieters gesendet werden, dürfen diese nur in dem Abtastintervall erhoben werden, das entsprechend dem Nutzungszweck der App notwendig ist. So wäre es für die Ermittlung von einer Liste von Geldautomaten nach Drücken auf einen „Suche“-Button nicht erforderlich, alle 10 Sekunden, auch ohne Nutzeraktion, den aktuellen Standort an den App-Anbieter zu übermitteln.

Die Zulässigkeit einer Weitergabe und Nutzung von Standortdaten (auch nach der „Verwaschung“) an den App-Betreiber oder Dritte ist nur zu bejahen, wenn dies entweder erforderlich für die Erbringung des Dienstes ist oder eine Einwilligung des Nutzers vorliegt. Grundsätzlich sollte die Erhebung und Verwendung von Standortdaten jedoch vorher von dem Nutzer freigegeben werden müssen - auch soweit eine ausdrückliche Einwilligung des Nutzers nicht notwendig ist. Zudem wird empfohlen, dem Nutzer zu ermöglichen, die Lokalisierung abzuschalten, auch wenn dann u. U. ein Teildienst (z. B. die Restaurantsuche im Umkreis) nicht genutzt werden kann und ihm eine aktive Lokalisierungsfunktion anzuzeigen.

6.8. Server-Backend

Neben Schutzmechanismen auf Seite der App müssen die beteiligten Server- bzw. Cloud-Dienste ausreichend abgesichert sein. Bei Ermittlung von möglichen Bedrohungen und Risiken muss davon ausgegangen werden, dass ein Angreifer sämtliche in der App hinterlegten Daten wie URL, Passwörter, Tokens und Datenstrukturen in Erfahrung bringen kann (z. B. durch Reverse Engineering der App). Die Schutzmechanismen des Backends müssen vergleichbar wie bei Webapplikationen gegen Möglichkeiten des unbefugten Datenzugriffs wie z. B. durch Injection-Angriffe, Authentifizierungs- und Autorisierungsmanipulationen, Zugriffe auf Daten über Objektreferenzen absichern[36]. Ebenso müssen die beteiligten Systeme auf Netzwerkebene durch eine geeignete Netzwerk- und Firewall-Architektur sowie ein konsequent umgesetztes Patch-Management geschützt werden.

6.9. Spezielle Pflichten des Telemedienanbieters

Weitreichende Pflichten zur technisch-organisatorischen Ausgestaltung eines Dienstes ergeben sich für einen Telemedienanbieter auch aus § 13 Abs. 4 TMG. Der Diensteanbieter hat danach durch technische und organisatorische Vorkehrungen sicherzustellen, dass

1. der Nutzer die Nutzung des Dienstes jederzeit beenden kann,
2. die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht oder in den Fällen des § 13 Abs. 4 Satz 2 („soweit einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen“) gesperrt werden,
3. der Nutzer Telemedien gegen Kenntnisnahme Dritter geschützt in Anspruch nehmen kann,
4. die personenbezogenen Daten über die Nutzung verschiedener Telemedien durch denselben Nutzer getrennt verwendet werden können,
5. Daten nach § 15 Abs. 2 TMG nur für Abrechnungszwecke zusammengeführt werden können (vgl. Kapitel 4.1.1.3) und
6. Nutzungsprofile nach § 15 Abs. 3 TMG nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden können.

Hieran erkennt man den Willen des Gesetzgebers, dass durch die Nutzung entstehende personenbezogene Daten in der Regel umgehend nach der Beendigung des Dienstes gelöscht werden müssen (vgl. Nr. 2), es sei denn, sie werden für Abrechnungszwecke

[36] Ausführliche Informationen zu diesem Themenfeld finden sich z. B. bei den „OWASP Top 10“ - Stand 2013 (abrufbar unter www.owasp.org) oder beim BSI Baustein „B 5.21 Webanwendungen“ - Stand 2013 (abrufbar unter www.bsi.bund.de/ DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b05/b05021.html).

benötigt (vgl. Nr. 5). Nicht erfasst hiervon werden Inhaltsdaten, die für die App selber erforderlich sind (z. B. Kalendereinträge bei einer Kalender-App).
Aber auch die Absicherung der Kommunikation etwa durch Einsatz von (SSL-) Verschlüsselung wird durch das Gesetz gefordert (vgl. Nr. 3). Dies gilt insbesondere, wenn personenbezogene Daten über das Internet übertragen werden.
Nr. 4 ist vor allem für Anbieter wichtig, die mehrere Dienste anbieten (etwa über eine gemeinsame App oder über mehrere Apps). Diese Daten müssen getrennt verwendet werden, so dass vermieden wird, dass in den Datenbanken gemeinsame Profile über die Nutzungen entstehen. Und hat der Betreiber des Dienstes (in der Regel der App-Anbieter) sich entschieden, Profile über seine Nutzer im Rahmen des § 15 Abs. 3 TMG zu erstellen (vgl. Kapitel 4.1.1.2.2), dann muss dieses nicht nur unter Pseudonym und mit Einräumung eines Widerspruchsrechts erfolgen, sondern auch durch den Betreiber verhindert werden, dass die Pseudonyme aufgedeckt werden.

Nach § 13 Abs. 6 TMG schließlich ist dem Nutzer die Weitervermittlung zu einem anderen Diensteanbieter anzuzeigen. Das bedeutet, dass der Nutzer erkennen können muss, wenn etwa über einen Link oder eine andere Verknüpfung ein Dienst von Dritten aufgerufen wird.

7. Erhöhter Schutzbedarf

Verarbeitet eine App Daten mit erhöhtem Schutzbedarf, bspw. besondere Arten personenbezogener Daten i. S. d. § 3 Abs. 9 BDSG, also Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben, sind als Konsequenz zusätzliche Sicherheitsmaßnahmen erforderlich. Diese Maßnahmen sind gem. der Anlage zu § 9 BDSG je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien zu treffen.

Bei Apps aus dem Gesundheitsbereich werden regelmäßig Gesundheitsdaten verarbeitet. Dies können Daten über den physischen und psychischen Gesundheitszustand des Nutzers sein, aber auch Angaben zu einzelnen Krankheiten, deren ärztliche Begleitung sowie einzunehmende Medikamente. Ggf. können auch sogenannte Fitness-Apps, die Werte über den Blutdruck, das Gewicht oder Ausdauer eines Nutzers speichern, darunter fallen. Um sicherzustellen, dass die Daten mit erhöhtem Schutzbedarf vor unberechtigtem Zugriff geschützt sind, sind sowohl auf dem Endgerät des Nutzers als auch - falls die Daten zum Anbieter oder an andere berechtigte Dritte übermittelt werden - für den Übertragungsweg und den Speicherort Sicherungsmaßnahmen zu ergreifen. So ist der Zugriff auf die App - und damit auf die dort gespeicherten besonderen Daten - mit einer gesonderten Authentifizierung zu versehen, die dem Schutzbedarf entspricht (vgl. Kapitel 6.2 zu

Zugangsdaten). Die auf dem Endgerät gespeicherten Daten sind verschlüsselt abzulegen, um sie im Falle eines Geräteverlustes vor dem Zugriff Unbefugter zu schützen.
Werden die Daten zwischen der App und einem (berechtigten) Dritten übermittelt, ist die Datenübertragung entsprechend des Schutzbedarfes zu gestalten (vgl. Kapitel 6.3 zur sicheren Datenübertragung).

Generell gilt, dass bei der Bereitstellung von Apps, die Daten erhebt und verwendet, welche der Geheimhaltungspflicht des § 203 StGB (etwa Ärzte, Anwälte) unterliegen und bei der eine Offenbarung (etwa an Betreiber des App-Stores, der App-Infrastruktur oder Vertreiber des Betriebssystems) und damit ein Straftatbestand nicht ausgeschlossen werden kann, eine gesonderte Einwilligung (ggf. Schweigepflichtentbindungserklärung) der Nutzerin bzw. des Nutzers einzuholen ist.

8. Konsequenzen unzulässigen Datenumgangs

Die Datenschutzaufsichtsbehörden sind gem. § 38 Abs. 5 BDSG befugt, Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anzuordnen. Eine solche Anordnung kann bei Nichtbefolgung mittels eines Zwangsgeldes erzwungen werden. Führt dies nicht zum Erfolg, so kann ein Datenumgang oder der Einsatz einzelner Verfahren untersagt werden. In bestimmten Fällen kann daneben die Begehung einer Ordnungswidrigkeit oder sogar einer Straftat im Raum stehen: Datenschutzrechtliche Bußgeldtatbestände sind insbesondere in § 16 TMG und § 43 BDSG aufgezählt und können mit einer Geldbuße bis zu 50.000 Euro, zum Teil sogar bis zu 300.000 Euro geahndet werden. In § 44 BDSG wird geregelt, in welchen Fällen eine Straftat vorliegt, die mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft wird.
Adressat aufsichtsrechtlicher Maßnahmen ist jeweils die verantwortliche Stelle, während Adressat der Ordnungswidrigkeitenvorschriften jeweils diejenige natürliche Person ist, welche den Verstoß begangen hat. Allerdings kommt unter bestimmten, in § 30 des Ordnungswidrigkeitengesetzes (OWiG) geregelten Voraussetzungen auch eine Geldbuße gegen Unternehmen als solche in Betracht. Voraussetzung hierfür ist - vereinfacht gesprochen - ein Versäumnis einer Leitungsperson, infolge dessen es im Unternehmen zu einer (z. B. datenschutzrechtlichen) Ordnungswidrigkeit gekommen ist. Häufiger Anwendungsfall hiervon ist das sog. Organisationsverschulden, auch in der Form einer mangelhaften Aufsicht: Die Geschäftsleitung ist grundsätzlich dafür verantwortlich, dass das Unternehmen im Zuge seiner wirtschaftlichen Betätigung alle geltenden einschlägigen Anforderungen der Rechtsordnung einhält, somit auch diejenigen des Datenschutzrechts. Die Geschäftsleitung muss hierfür, insbesondere durch geeignete Organisation

und Aufsicht im Unternehmen, Sorge tragen. Ist insoweit einer Leitungsperson ein (organisatorisches) Versäumnis vorzuwerfen, kann eine Geldbuße gegen das Unternehmen in Betracht kommen.

9. Besonderheiten / Hinweise

9.1. Bezahlvorgänge

Mit Hilfe einiger Apps können heute schon Smartphones zum Bezahlen verwendet werden. Der Bezahlvorgang wird dabei in elektronischer Form und in der Regel kontaktlos abgewickelt. Technisch realisiert wird der kontaktlose Bezahlvorgang z. B. durch die Near Field Communication (NFC). Unterschieden werden kann zwischen zwei Betriebsmodi:

- Das Smartphone kommuniziert über eine App mit einem NFC-Lesegerät, z. B. einem Händlerterminal. In diesem Fall übernimmt das Smartphone die Rolle einer kontaktlosen Smartcard (Card Emulation Modus). Die notwendigen kritischen Operationen (Authentifizierung, Schlüsselberechnung, Speicherung von PIN u. a.) werden dabei auf einem sicheren Element auf dem Smartphone (regelmäßig im NCF-Bauteil oder in der SIM-Karte) durchgeführt.
- Wie im ersten Fall übernimmt das Smartphone die Rolle der Smartcard. Jedoch werden die kritischen Operationen vollständig in der App durchgeführt und das NFC-Bauteil nur zur Übertragung der Daten genutzt (Host Card Emulation Modus).
- Beim Read/Writer-Modus vertauschen sich die Rollen und das Smartphone wird zum NFC-Lesegerät. Mit einer Smartcard lassen sich (kontaktlos) am Smartphone Bezahlvorgänge durchführen.

Bei der Verwendung von Apps als Zahlungssoftware sind verschiedenste Regelungen aus den Bereichen des Telekommunikationsgesetzes (TKG), des Telemediengesetzes (TMG), des Bundesdatenschutzgesetzes (BDSG), des Zahlungsdiensteaufsichtsgesetzes (ZAG), des Kreditwesengesetzes (KWG), des Bürgerlichen Gesetzbuchs (BGB), und der EU-Richtlinien (z. B. Payment Services Directive) zu beachten.

Der Datenumgang ist dem Diensteanbieter im gesetzlichen Rahmen des § 28 Abs. 1 S. 1 Nr. 1 BDSG gestattet. Der Diensteanbieter kann danach personenbezogene Daten der Nutzer (z. B. Name, Kontoverbindungsdaten, Preis, Kaufsache) nur erheben, speichern, verändern oder übermitteln, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Nutzer erforderlich ist. Ein darüber hinausgehender Datenumgang durch den Diensteanbieter ist nur im Umfang einer zuvor einzuholenden Einwilligung der Nutzer zulässig.

Für die im Rahmen eines Zahlungsvorgangs erhobenen personenbezogenen Daten gilt eine strenge Zweckbindung. Die Verwendung der erhobenen Daten zu Zwecken der Direktwerbung ist nur unter den Voraussetzungen des § 28 Abs. 3 BDSG zulässig.

Die Verwendung von Nutzungsdaten zur Erstellung von Nutzungsprofilen zu Zwecken der Marktforschung (Analyse des Nutzerverhaltens) oder zu Werbezwecken ist ohne Einwilligung nur unter den Voraussetzungen des § 15 Abs. 3 TMG zulässig (vgl. Kapitel 4.1.1.2.2).

Bei Bankkontodaten handelt es sich um besonders sensible Daten, deren Kenntnisnahme durch unberechtigte Dritte eine Meldepflicht nach § 42a BDSG nach sich zieht. Die Sicherung der Bankkontodaten durch technisch-organisatorische Maßnahmen, insbesondere einem sicheren Übertragungsweg kommt daher besondere Bedeutung zu.

Bei der Entwicklung von Bezahl-Apps sollte darauf geachtet werden, dass ein Bezahlvorgang nicht ohne Kenntnis und aktive Mitwirkung der Nutzer stattfinden kann. Die Informationen sollten insbesondere Name und Anschrift des Vertragspartners und den zu entrichtenden Preis enthalten. Ferner sollte die App eine nachvollziehbare Authentifizierung und Protokollierung bereitstellen.[37] Wird beim Einsatz einer Bezahlfunktion eine rein softwarebasierte Berechnung und Speicherung der kritischen Nutzerdaten (Authentifizierung, Schlüsselspeicher) eingesetzt, ist die Sicherheit dieser Daten nach dem Stand der Technik zu gewährleisten.

9.2. Nutzung alternativer Quellen zum Bezug von Apps

Apps finden zu einem überwiegenden Teil über App-Stores der großen Anbieter wie Apple, Microsoft oder Google Verbreitung. Apple bzw. Microsoft sehen für ihre Mobilgeräte, die das Betriebssystem iOS bzw. Windows Phone verwenden, außer der Nutzung des eigenen App-Stores keine weitere Möglichkeit zum Erwerb von Apps vor. Die Verwendung von Software aus alternativen Quellen ist lediglich nach Überwindung technischer Zugangshinderungen möglich (sog. „Jailbreak“). Im Gegensatz dazu bietet Google für Android-Mobilgeräte die Möglichkeit, Apps von anderen Quellen als dem Play Store zu erwerben. Damit können Apps z. B. von Webseiten heruntergeladen und auf den Endgeräten installiert werden. Neben einzelnen Apps können für Android auch ganze alternative App-Stores aus dem Internet geladen und installiert werden.[38]

[37] Weitere Informationen zum Mobile Payment finden Sie in der Veröffentlichung zum 3. Verbraucherdialog Rheinland-Pfalz „Mobile Payment“, Empfehlungen der Arbeitsgruppe Zahlungssicherheit (http://www.datenschutz.rlp.de/downloads/misc/mobile_payment/Empfehlungen_der_AG_Zahlungssicherheit.pdf) und Schütte, NFC? Aber sicher, DuD 2014, 20 ff.

[38] Ein Beispiel für einen alternativen Non-Profit App-Store, der auf Free und Open Source Software spezialisiert ist und nach eigenen Angaben keine Nutzungsdaten erhebt, ist F-Droid (https://www.f-droid.org).

Bei der Auswahl eines Distributionswegs handelt ein App-Anbieter datenschutzfreundlich, wenn er neben App-Stores, bei denen der Bezug von Apps mit einer Registrierung und weiteren Datensammlungen verbunden ist, den Endnutzern weitere Möglichkeiten zum Erwerb von Apps bietet. Gleiches gilt für die Auswahl von App-Stores, die eine Registrierung unter einem Pseudonym ermöglichen sowie für Angebote, für deren Bezahlung nicht die Angaben von Kreditkarteninformationen erforderlich ist, sondern stattdessen Prepaid-Karten verwendet werden können.

Des Weiteren ist es empfehlenswert, dass die Nutzerin bzw. der Nutzer der App beim Download der App aus dem App-Store erkennen können sollte, ob es sich um eine nichtmanipulierte Version der App handelt. Wünschenswert wäre daher die Generierung von Hashwerten etc. als Fingerprint durch die App, die es sicherheitsbewussten Nutzern erlauben würde, diese mit den entsprechenden Werten auf z. B. der Webseite des Entwicklers zu vergleichen. Dazu ist es notwendig, dass ein geeigneter Algorithmus zur Erzeugung des Fingerprints verwendet wird.

9.3. Apps für Jugendliche und Kinder

Kinder und Jugendliche haben häufig nur ein geringes Verständnis und Wissen in Bezug auf den Umfang und die Sensibilität der Daten, die bei der Verwendung einer App übertragen und möglicherweise an Dritte weitergegeben werden. Daher tragen Anbieter und Entwickler bei App-Angeboten, die sich speziell an die Zielgruppe Minderjähriger richten, besondere Verantwortung im Umgang mit deren Daten.

Zu unterscheiden ist generell weiterhin zwischen dem Datenumgang auf Basis gesetzlicher Erlaubnistatbestände und dem Datenumgang auf Basis einer Einwilligung. In beiden Situationen sind jedoch das besondere Interesse Minderjähriger und deren Einsichtsfähigkeit in die Wertung der datenschutzrechtlichen Zulässigkeit einzubeziehen. Hinsichtlich der Einsichtsfähigkeit stellt das Datenschutzrecht nicht auf die Geschäftsfähigkeit (vgl. §§ 104 ff. BGB) ab und legt keine verbindliche Altersgrenze fest, ab der diese Fähigkeit bei Kindern und Jugendlichen generell angenommen werden könnte. Entscheidend ist vielmehr in Anknüpfung an die Berechtigung und Mündigkeit zur Ausübung des Grundrechts auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, ob ein Kind oder Jugendlicher in der Lage ist, die Konsequenzen des Umgangs mit seinen Daten zu überblicken. Diese Beurteilung kann nur für den Einzelfall erfolgen, da sie abhängig ist vom jeweiligen Entwicklungsstand des Minderjährigen und der beabsichtigten Verwendung der Daten.

Sofern der Minderjährige selbst nicht über die notwendige Einsichtsfähigkeit und geistige Reife verfügt, sind deshalb regelmäßig die Erhebung und Verwendung Daten

Minderjähriger nur nach Einwilligung durch die Erziehungsberechtigten rechtmäßig. Bei unter 14-jährigen wird im Allgemeinen die Fähigkeit zur Abschätzung der Tragweite einer Einwilligung in die Verarbeitung der eigenen Daten - insbesondere unter Berücksichtigung der komplexen Datenverarbeitungsprozesse, die der Verwendung von Apps zugrunde liegen - abzulehnen sein. App-Anbieter müssen deshalb bei App-Angeboten, die an die Zielgruppe der unter 14-jährigen gerichtet sind, in diesen Fällen sicherstellen, dass die Einwilligung der Eltern zur Datenverarbeitung vorliegt. In der Praxis wird die Einwilligung der Eltern teilweise durch Bestätigung eines Aktivierungslinks abgefragt, der an die E-Mail Adresse der Eltern versandt wurde. Problematisch an dieser Methode ist jedoch, dass nicht sichergestellt werden kann, dass die Bestätigung des Links tatsächlich durch die Eltern erfolgt ist. Anbieter sind angehalten, effektive Mechanismen zur Altersverifikation und Beteiligung der Eltern zu entwickeln und Missbrauch konsequent zu reglementieren. Generell sind Hinweise und Informationen zur Datenverarbeitung in angemessener und verständlicher Sprache zu formulieren, die sich an den Fähigkeiten der Zielgruppe orientiert, so dass Kinder und Jugendliche die Auswirkung und Konsequenzen der Nutzung begreifen können. Das Einwilligungsrecht der Eltern geht graduell auf das Kind über, d. h. der Entscheidungsspielraum der Eltern nimmt in dem Maß ab, in dem die Einsichtsfähigkeit des Kindes zunimmt.

Unabhängig von der datenschutzrechtlichen Bewertung ist bereits fraglich, ob das einer App-Nutzung durch beschränkt geschäftsfähige Minderjährige im Alter zwischen 7 und 14 Jahren zugrundeliegende Rechtsgeschäft ohne die Zustimmung der Eltern gemäß §§ 104 ff. BGB rechtsverbindlich zustande kommen kann.

9.4. Apps öffentlicher Stellen

Die vorliegende Orientierungshilfe des Düsseldorfer Kreises wurde für den nicht-öffentlichen Bereich erstellt. Der Düsseldorfer Kreis ist ein informeller Zusammenschluss der Aufsichtsbehörden im nichtöffentlichen Bereich. Handelt es sich bei den Akteuren[39] um öffentliche Stellen, so gelten die Vorschriften des TMG auch für diese. Daneben ist eine Orientierung an den dargestellten Grundsätzen und rechtlichen Ausführungen möglich. Die Zulässigkeit der Erhebung und Verwendung personenbezogener Daten durch Behörden und andere öffentliche Stellen richtet sich allerdings nach den für diese Stellen maßgeblichen Datenschutzregelungen. Für den öffentlichen Bereich gelten insbesondere die jeweiligen Landesdatenschutzgesetze (es sei denn, es handelt sich um Stellen gem. § 1 Abs. 2 Nr. 1 und Nr. 2 BDSG) oder vorrangig zu beachtende bereichsspezifische Datenschutzvorschriften. Die Einhaltung dieser Regelungen ist jeweils genau zu prüfen und sicherzustellen.

[39] Denkbar ist auch eine Konstellation, bei der es sich bei dem App-Anbieter um eine öffentliche Stelle, bei dem App-Entwickler oder einem weiteren Akteur jedoch um eine nicht-öffentliche Stelle handelt.

Anlagen

Anlage 1 - Wortlaut des neugefassten § 40 SächsDSG

§ 40 Kostenerhebung

(§ 40 neu gefasst durch Artikel 17 des Gesetzes vom 29. April 2015, SächsGVBl. S. 349, 358)

(1) Der Sächsische Datenschutzbeauftragte kann für Amtshandlungen und sonstige öffentlich-rechtliche Leistungen nach dem Bundesdatenschutzgesetz die in der Anlage festgelegten Kosten (Gebühren und Auslagen) erheben. Die Kosten fließen dem Freistaat Sachsen zu.

(2) Kosten für Kontrollen nach § 38 Absatz 1 Satz 1 des Bundesdatenschutzgesetzes werden nur erhoben, wenn ein Verstoß gegen das Bundesdatenschutzgesetz oder eine andere Bestimmung über den Datenschutz festgestellt wird. Kontrollen oder Beratungen einfacher Art sowie die Beratung nicht-öffentlicher Stellen ohne Gewinnerzielungsabsicht sind kostenfrei.

(3) Die Höhe der Gebühr ist nach dem Verwaltungsaufwand und nach der Bedeutung der Angelegenheit für die Beteiligten zu bemessen.

(4) Der Sächsische Datenschutzbeauftragte entscheidet in eigener Verantwortung über die Ermäßigung oder Befreiung von Kosten, soweit dies aus Gründen der Billigkeit oder aus öffentlichem Interesse geboten ist. Im Übrigen finden § 2 Absatz 1 Satz 1 und Absatz 2 bis 4, § 9 Absatz 1, §§ 10, 12 bis 23 und 26 des Verwaltungskostengesetzes für den Freistaat Sachsen in der Fassung der Bekanntmachung vom 17. September 2003 (SächsGVBl. S. 698), das zuletzt durch Artikel 31 des Gesetzes vom 27. Januar 2012 (SächsGVBl. S. 130) geändert worden ist, in der jeweils geltenden Fassung, entsprechend Anwendung.

Anlage 2 - Wortlaut der Anlage zum neugefassten § 40 SächsDSG

Anlage zu § 40

(Anlage angefügt durch Artikel 17 des Gesetzes vom 29. April 2015, SächsGVBl. S. 349, 358)

Folgende Kosten werden erhoben:

1.	Kontrollen nach § 38 Absatz 1 Satz 1 des Bundesdatenschutzgesetzes je angefangene halbe Stunde und eingesetztem Bediensteten	
	a) bei Kontrollen ohne besondere Prüfintensität	40 Euro
	b) bei örtlichen Kontrollen oder solchen mit besonderer Prüfintensität	60 Euro
2.	Heranziehung zur Erteilung datenschutzrechtlicher Auskünfte durch Verwaltungsakt	150 bis 1 500 Euro
3.	Anordnungen nach § 38 Absatz 5 Satz 1 des Bundesdatenschutzgesetzes	150 bis 1 500 Euro
4.	Untersagungen nach § 38 Absatz 5 Satz 2 des Bundesdatenschutzgesetzes	250 bis 2 500 Euro
5.	Abberufungen nach § 38 Absatz 5 Satz 3 des Bundesdatenschutzgesetzes	150 bis 1 500 Euro
6.	Beratungen nach § 38 Absatz 1 Satz 2 des Bundesdatenschutzgesetzes je angefangene halbe Stunde und eingesetztem Bediensteten	50 Euro*
7.	Genehmigung der Datenübermittlung in Drittstaaten nach § 4c Absatz 2 des Bundesdatenschutzgesetzes	1 500 bis 15 000 Euro
8.	Prüfung von Verhaltensregeln nach § 38a des Bundesdatenschutzgesetzes	1 000 bis 5 000 Euro
9.	Bearbeitungen von Meldungen nach § 4d Absatz 1 des Bundesdatenschutzgesetzes	
	a) Erstmeldung (je Verfahren)	50 Euro
	b) Änderungs- oder Abmeldungen (je Verfahren)	25 Euro

*) Der Umfang der Leistung und die voraussichtliche Höhe der Gebühr sind dem Kostenschuldner vorher mitzuteilen.

Anlage 3 - „Mindestlohngesetz und Datenschutz“

Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. bis 19. März 2015 in Wiesbaden

Die Umsetzung des Mindestlohngesetzes wirft eine Reihe von datenschutzrechtlichen Problemen auf, die einer Klärung bedürfen.

Unter anderem haftet ein Unternehmen dafür, wenn ein Subunternehmer - und ggf. auch dessen Subunternehmer - den Beschäftigten nicht den Mindestlohn zahlt; außerdem kann ein hohes Bußgeld verhängt werden, wenn der Auftraggeber weiß oder fahrlässig nicht weiß, dass Auftragnehmer den Mindestlohn nicht zahlen. Da das Mindestlohngesetz nicht bestimmt, wie die Überprüfung durch den Auftraggeber konkret zu erfolgen hat, sichern sich - wie Industrie- und Handelskammern berichten - zahlreiche Unternehmen vertraglich durch umfangreiche Vorlagepflichten und Einsichtsrechte in Bezug auf personenbezogene Beschäftigtendaten beim Subunternehmer (z. B. Lohnlisten, Verdienstbescheinigungen usw.) ab. Dies ist in Anbetracht der schutzwürdigen Interessen der Beschäftigten weder datenschutzrechtlich gerechtfertigt noch im Hinblick auf die soziale Zielrichtung des Mindestlohngesetzes erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, bei der in Aussicht genommenen Überprüfung des Mindestlohngesetzes stärker auf die Belange des Datenschutzes zu achten. Auch im Interesse einer unbürokratischen Lösung sollte der Gesetzgeber klarstellen, dass eine schriftliche Erklärung des Auftragnehmers ausreicht, um die Voraussetzungen des Mindestlohngesetzes einzuhalten. Dies kann eventuell durch Vertragsstrafenregelungen, Übernahme des Haftungsrisikos durch Bankbürgschaften sowie vertragliche Zustimmungsvorbehalte für den Fall der Beauftragung weiterer Subunternehmer durch den Auftragnehmer abgesichert werden. Aus Datenschutzsicht sind allenfalls stichprobenartige Kontrollen von geschwärzten Verdienstbescheinigungen hinnehmbar. Bei einer Novellierung des Gesetzes, sollte der Gesetzgeber darüber hinaus klarstellen, dass Zugriffe des Auftraggebers auf personenbezogene Beschäftigtendaten des Auftragnehmers unzulässig sind.

Stichwortverzeichnis