Sächsischer Landtag
6. Wahlperiode

DRUCKSACHE 6/10549

Schutz des Persönlichkeitsrechts im öffentlichen Bereich

18. Tätigkeitsbericht

des

Sächsischen Datenschutzbeauftragten

Berichtszeitraum: 1. April 2015 bis 31. März 2017

Dem Sächsischen Landtag

vorgelegt zum 31. März 2017

gemäß § 30 des Sächsischen Datenschutzgesetzes

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

Vorbemerkung zum Sprachgebrauch in diesem Bericht:

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

Herausgeber: Der Sächsische Datenschutzbeauftragte
Andreas Schurig
Bernhard-von-Lindenau-Platz 1 Postfach 12 07 05
01067 Dresden 01008 Dresden
Telefon: 0351/4935-401
Fax : 0351/4935-490

Besucheranschrift: Devrientstraße 1
01067 Dresden

Herstellung: Parlamentsdruckerei

Vervielfältigung erwünscht.

Inhaltsverzeichnis

Abkürzungsverzeichnis

Vorschriften

Nachstehend werden Gesetze und andere Vorschriften nach der alphabetischen Reihenfolge der *amtlichen, in Ausnahmefällen auch nichtamtlichen Abkürzung, ersatzweise der amtlichen Kurzbezeichnung* aufgeführt.

AO	Abgabenordnung in der Fassung der Bekanntmachung vom 1. Oktober 2002 (BGBl. I S. 3866; 2003 I S. 61), zuletzt geändert durch Art. 6 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745)
BDSG	Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Art. 7 des Gesetzes vom 30. Juni 2017 (BGBl. I S. 2097)
BeamtStG	Beamtenstatusgesetz vom 17. Juni 2008 (BGBl. I S. 1010), zuletzt geändert durch Art. 2 des Gesetzes vom 8. Juni 2017 (BGBl. I S. 1570)
BewachV	Bewachungsverordnung in der Fassung der Bekanntmachung vom 10. Juli 2003 (BGBl. I S. 1378), zuletzt geändert durch Art. 1 der Verordnung vom 1. Dezember 2016 (BGBl. I S. 2692)
BGB	Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Art. 1 des Gesetzes vom 20. Juli 2017 (BGBl. I S. 2787)
BKAG	Bundeskriminalamtgesetz vom 7. Juli 1997 (BGBl. I S. 1650), zuletzt geändert durch Art. 2 des Gesetzes vom 1. Juni 2017 (BGBl. I S. 1354)
BMG	Bundesmeldegesetz vom 3. Mai 2013 (BGBl. I S. 1084), geändert durch Art. 11 Abs. 4 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745)
BZRG	Bundeszentralregistergesetz in der Fassung der Bekanntmachung vom 21. September 1984 (BGBl. I S. 1229, 1985 BGBl. I S. 195), zuletzt geändert durch Art. 1 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2732)

GewO	Gewerbeordnung in der Fassung der Bekanntmachung vom 22. Februar 1999 (BGBl. I S. 202), zuletzt geändert durch Art. 1 des Gesetzes vom 20. Juli 2017 (BGBl. I S. 2789)
GG	Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Art. 1 des Gesetzes vom 13. Juli 2017 (BGBl. I S. 2347)
GO	Geschäftsordnung des Sächsischen Landtags 6. Wahlperiode vom 12. November 2014 (SächsABl. S. 1497)
KKG	Gesetz zur Kooperation und Information im Kinderschutz vom 22. Dezember 2011 (BGBl. I S. 2975), zuletzt geändert durch Art. 20 Abs. 1 des Gesetzes vom 23. Dezember 2016 (BGBl. I S. 3234)
NachwG	Nachweisgesetz vom 20. Juli 1995 (BGBl. I S. 946), zuletzt geändert durch Art. 3a des Gesetzes vom 11. August 2014 (BGBl. I S. 1348)
PaßG	Paßgesetz vom 19. April 1986 (BGBl. I S. 537), zuletzt geändert durch Art. 2 des Gesetzes vom 7. Juli 2017 (BGBl. I S. 2310)
PAuswG	Personalausweisgesetz vom 18. Juni 2009 (BGBl. I S. 1346), zuletzt geändert durch Art. 4 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745)
Richtlinie (EU) 2016/680	Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates
SächsAGBMG	Sächsisches Gesetz zur Ausführung des Bundesmeldegesetzes vom 9. Juli 2014 (SächsGVBl. S. 76), zuletzt geändert durch Art. 2 des Gesetzes vom 26. Oktober 2016 (SächsGVBl. S. 504)
SächsArchivBenVO	Sächsische Archivbenutzungsverordnung vom 24. Februar 2003 (SächsGVBl. S. 79)
SächsDSG	Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz) vom 25. August 2003 (SächsGVBl. S. 330), zuletzt geändert durch Art. 17 des Gesetzes vom 29. April 2015 (SächsGVBl. S. 349)

SächsEGovG	Gesetz zur Förderung der elektronischen Verwaltung im Freistaat Sachsen (Sächsisches E-Government-Gesetz) vom 9. Juli 2014 (SächsGVBl. S. 398), geändert durch die Verordnung vom 4. April 2015 (SächsGVBl. S. 374)
SächsGemO	Sächsische Gemeindeordnung in der Fassung der Bekanntmachung vom 3. März 2014 (SächsGVBl. S. 146), zuletzt geändert durch Art. 2 des Gesetzes vom 13. Dezember 2016 (SächsGVBl. S. 652)
SächsJG	Sächsisches Justizgesetz vom 24. November 2000 (SächsGVBl. S. 482; 2001 S. 704), zuletzt geändert durch Art. 7 des Gesetzes vom 15. Dezember 2016 (SächsGVBl. S. 630)
SächsJStVollzG	Sächsisches Jugendstrafvollzugsgesetz vom 12. Dezember 2007 (SächsGVBl. S. 558), zuletzt geändert durch Art. 2 des Gesetzes vom 16. Mai 2013 (SächsGVBl. S. 250)
SächsKAG	Sächsisches Kommunalabgabengesetz in der Fassung der Bekanntmachung vom 26. August 2004 (SächsGVBl. S. 418; 2005 S. 306), zuletzt geändert durch Art. 1 des Gesetzes vom 26. Oktober 2016 (SächsGVBl. S. 504)
SächsPolG	Polizeigesetz des Freistaates Sachsen in der Fassung der Bekanntmachung vom 13. August 1999 (SächsGVBl. S. 466), zuletzt geändert durch Art. 1 des Gesetzes vom 17. Dezember 2013 (SächsGVBl. S. 890)
SächsPresseG	Sächsisches Gesetz über die Presse vom 3. April 1992 (SächsGVBl. S. 125), zuletzt geändert durch Art. 2 des Gesetzes vom 17. Dezember 2013 (SächsGVBl. S. 896)
SächsSchulG	Sächsisches Schulgesetz in der Fassung der Bekanntmachung vom 16. Juli 2004 (SächsGVBl. S. 298), zuletzt geändert durch Art. 1 des Gesetzes vom 26. April 2017 (SächsGVBl. S. 242)
SächsStVollzG	Sächsisches Strafvollzugsgesetz vom 16. Mai 2013 (SächsGVBl. S. 250)
SächsSWG	Sächsisches Sicherheitswachtgesetz vom 12. Dezember 1997 (SächsGVBl. S. 647), zuletzt geändert durch Art. 9 des Gesetzes vom 18. Dezember 2013 (SächsGVBl. S. 970)
SächsUHaftVollzG	Sächsisches Untersuchungshaftvollzugsgesetz vom 14. Dezember 2010 (SächsGVBl. S. 414), geändert durch Art. 3 des Gesetzes vom 16. Mai 2013 (SächsGVBl. S. 250)

SächsVerf	Verfassung des Freistaates Sachsen vom 27. Mai 1992 (SächsGVBl. S. 243), zuletzt geändert durch Gesetz vom 11. Juli 2013 (SächsGVBl. S. 502)
SächsVSG	Gesetz über den Verfassungsschutz im Freistaat Sachsen (Sächsisches Verfassungsschutzgesetz) vom 16. Oktober 1992 (SächsGVBl. S. 459), zuletzt geändert durch Art. 3 des Gesetzes vom 17. Dezember 2013 (SächsGVBl. S. 890)
SchfHwG	Schornsteinfeger-Handwerksgesetz vom 26. November 2008 (BGBl. I S. 2242), zuletzt geändert durch Art. 1 des Gesetzes vom 17. Juli 2017 (BGBl. I S. 2495)
SGB I	Erstes Buch Sozialgesetzbuch – Allgemeiner Teil – (Art. I des Gesetzes vom 11. Dezember 1975, BGBl. I S. 3015), zuletzt geändert durch Art. 5 des Gesetzes vom 14. August 2017 (BGBl. I S. 3214)
SGB V	Fünftes Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung (Art. 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477, 2482), zuletzt geändert durch Art. 4 des Gesetzes vom 14. August 2017 (BGBl. I S. 3214)
SGB VIII	Achtes Buch Sozialgesetzbuch – Kinder und Jugendhilfe – in der Fassung der Bekanntmachung vom 11. September 2012 (BGBl. I S. 2022), zuletzt geändert durch Art. 3 des Gesetzes vom 20. Juli 2017 (BGBl. I S. 2780)
SGB X	Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – in der Fassung der Bekanntmachung vom 18. Januar 2001 (BGBl. I S. 130), zuletzt geändert durch Art. 2 Abs. 6 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2739)
SGB XI	Elftes Buch Sozialgesetzbuch – Soziale Pflegeversicherung – (Art. 1 des Gesetzes vom 26. Mai 1994, BGBl. I S. 1014, 1015), geändert durch Art. 9 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2757)
SGB XII	Zwölftes Buch Sozialgesetzbuch – Sozialhilfe – (Art. 1 des Gesetzes vom 27. Dezember 2003, BGBl. I S. 3022, 3023), zuletzt geändert durch Art. 2 des Gesetzes vom 17. August 2017 (BGBl. I S. 3214)
StGB	Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Art. 1 des Gesetzes vom 17. August 2017 (BGBl. I S. 3202)

StPO	Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Art. 1 des Gesetzes vom 27. August 2017 (BGBl. I S. 3295)
StVG	Straßenverkehrsgesetz in der Fassung der Bekanntmachung vom 5. März 2003 (BGBl. I S. 310, 919), zuletzt geändert durch Art. 6 des Gesetzes vom 17. August 2017 (BGBl. I S. 3202)
TMG	Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), zuletzt geändert durch Art. 2 des Gesetzes vom 1. September 2016 (BGBl. I S. 3352)
ÜSchuldStatG	Gesetz über die Statistik der Überschuldung privater Personen (Überschuldungsstatistikgesetz) vom 22. Dezember 2011 (BGBl. I S. 3083)
Verordnung (EU) 2016/679	Datenschutz-Grundverordnung – Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, die ab 25. Mai 2018 vollständig in Kraft tritt

Sonstiges

a. F.	alte Fassung
AG	Arbeitsgruppe
ASD	Allgemeiner Sozialer Dienst
BfDI	Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BR-Drs.	Bundesrats-Drucksache
BSG	Bundessozialgericht
BSGE	Bundessozialgerichtsentscheidung

BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
BVerwGE	Bundesverwaltungsgerichtsentscheidung
DSK	Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder – Datenschutzkonferenz (findet halbjährlich statt)
EU	Europäische Union
IVO	Integriertes Vorgangsbearbeitungssystem für die Landespolizei
JVA	Justizvollzugsanstalt
KSV	Kommunaler Sozialverband Sachsen
LfV	Landesamt für Verfassungsschutz des Freistaates Sachsen
LKA	Landeskriminalamt Sachsen
LT-Drs.	Landtags-Drucksache
n. F.	neue Fassung
m. w. N.	mit weiteren Nachweisen
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
SächsABl.	Sächsisches Amtsblatt
SächsGVBl.	Sächsisches Gesetz- und Verordnungsblatt
SächsVerfGH	Sächsischer Verfassungsgerichtshof
SMF	Sächsisches Staatsministerium der Finanzen
SMI	Sächsisches Staatsministerium des Innern
SMJus	Sächsisches Staatsministerium der Justiz

SMK	Sächsisches Staatsministerium für Kultus
SMS	Sächsisches Staatsministerium für Soziales
SMUL	Sächsisches Staatsministerium für Umwelt und Landwirtschaft
SMWA	Sächsisches Staatsministerium für Wirtschaft, Arbeit und Verkehr
SMWK	Sächsisches Staatsministerium für Wissenschaft und Kunst
StA	Staatsanwaltschaft
SVN	Sächsisches Verwaltungsnetz
VwV	Verwaltungsvorschrift

Verweise im Text auf Ausführungen in früheren Tätigkeitsberichten des Sächsischen Datenschutzbeauftragten sind durch Angabe der Nummer des jeweiligen Tätigkeitsberichtes sowie der jeweiligen Abschnitt-Nr. – getrennt durch einen Schrägstrich – gekennzeichnet (z. B. 4/5.1.2.6).

1 Datenschutz im Freistaat Sachsen

1.1 Datensparsamkeit versus Datenreichtum

In letzter Zeit hört man in Deutschland im Rahmen der Digitalisierungsdebatte neue wohlklingende Schlagwörter vorrangig aus Politikermund wie „Datenreichtum“, „Datenschatz“ oder „Datensouveränität“. Daten sind das „Öl“ oder der „Rohstoff des 21. Jahrhunderts“. Ziel ist nicht einfach das Sammeln von Daten („Big Data“), sondern das Auswerten („Smart Data“). Datensparsamkeit dagegen verhindert Fortschritt und reduziert Entwicklungschancen. Wohlweislich wird dabei vermieden, darauf hinzuweisen, dass es sich bei den Daten oft um Informationen über Personen handelt, die in ihrer Summe weitreichende Persönlichkeitsprofile zulassen. Erstaunlich ist dabei, dass die europäische und globale Entwicklung dem deutlich entgegenläuft. Erst letztes Jahr hat die Europäische Union eine Datenschutzreform verabschiedet, die die Datenminimierung als zentralen Verarbeitungsgrundsatz benennt. Einige global agierende Konzerne entdecken den Datenschutz („privacy“) als Verkaufsvorteil und versuchen zumindest, dies auch in ihren Geschäftsmodellen zu verankern. Immer mehr erkennen, dass es für Geschäftsmodelle, bei denen Informationen über Menschen verarbeitet werden, essentiell auf das Vertrauen der Betroffenen ankommt. Im Gegensatz zur analogen Welt ist die digitale deutlich undurchschaubarer. Dies betrifft sowohl die verwendeten Mittel als auch die ablaufenden Prozesse. Nicht umsonst redet man zum Beispiel von der Cloud, die eben wolkig und undurchsichtig ist. Wer digitale Dienste nutzt, muss Vertrauen in die Sicherheit der Systeme und in die Versicherungen des Anbieters haben. Die Mittel, dieses Vertrauen zu erzeugen, sind Transparenz seitens der Anbieter, Überprüfung und Zertifizierung ihrer Dienste und Produkte sowie Kontrolle durch Aufsichtsinstitutionen, alles wesentliche Bestandteile der neuen EU-Datenschutzreform. Dass die Erzeugung dieses Vertrauens sowohl im Interesse der Unternehmen als auch der Nutzer ist, ist leider nicht allen Beteiligten an der Umsetzung der Datenschutzreform hinreichend klar. Wer aus einer falsch verstandenen Fortschrittsgläubigkeit mit dem Ziel „Schranken abzubauen“ Datenschutz erschweren und beseitigen will, verhindert gerade eine Entwicklung, die technische und gesellschaftliche Entwicklung akzeptiert und mit Grundwerten verbindet.

Das dabei noch viele Fragen offen sind, wird bei der aktuellen Umsetzung der Datenschutzreform deutlich. Nachdem im Berichtszeitraum der europäische Gesetzgebungsprozess abgeschlossen worden ist, stand die Umsetzung in nationales Recht an. Ein erster Schritt auf der Bundesebene ist erfolgt, vieles ist in Bund und Ländern noch zu tun. Darüber hinaus wird auch die direkte Vorbereitung in den datenverarbeitenden Stellen immer drängender. Hinweise dafür werden von den Datenschutzaufsichtsbehörden herausgegeben und finden sich auch im Weiteren in diesem Tätigkeitsbericht.

Die Neuregelungen werden erhebliche Auswirkungen auf meine Organisationsstruktur, meine Befugnisse und Aufgaben haben. Letztere werden sich enorm ausweiten; je nach Zählart kommt man auf 50 bis 60 neue Aufgaben für meine Behörde. Hieraus resultiert ein erheblicher Personalmehrbedarf. Meine Behörde verfügt derzeit, Anfang 2017, über fast die gleiche Anzahl von Stellen (21) wie zur Anfangszeit ihres Bestehens (1993 19 Stellen), obwohl sich die Aufgaben seither – von der 2007 durch den Gesetzgeber zugewiesenen, zuvor den Regierungspräsidien obliegenden, Aufsicht über die nicht-öffentlichen Stellen (Unternehmen, Vereine etc. in Sachsen) über einige andere neue Aufgaben bis zu dem sich neuerdings abzeichnenden „Gemeinsamen Kompetenz- und Dienstleistungszentrums“ der Länder Berlin, Brandenburg, Sachsen, Sachsen-Anhalt und Thüringen, enorm ausgeweitet haben. Gleiches gilt – als Zeichen eines gestiegenen Datenschutzbewusstseins zu begrüßen – für die stark gewachsene Anzahl der Bürgeranfragen. Ich bin aber deshalb derzeit nicht in der Lage, meine gesetzlichen Aufgaben vollumfänglich und mit der eigentlich notwendigen Breite und Tiefe zu erfüllen. Dies ist ein konkreter Nachteil für die sächsischen Bürger und Unternehmen. Ich hoffe, dass dies im Rahmen der Umsetzung der Datenschutzreform gelöst werden kann.

Wie immer an dieser Stelle möchte ich meinen Dank gegenüber der Landtagsverwaltung äußern. Den positiven Ausführungen in meinem Bericht ist nichts hinzuzufügen. Auch die Zusammenarbeit mit Parlament und Staatsregierung gestaltet sich in bewährter Weise. Dies kommt insbesondere der Qualität und der Zügigkeit der Umsetzung der EU-Datenschutzreform in Sachsen zugute.

1.2 Datenschutz-Grundverordnung und JI-Richtlinie der Europäischen Union in Kraft getreten – eine neue Zeitrechnung im Datenschutzrecht

Am 25. Mai 2016 ist die

> „*Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)*“

und am 5. Mai 2016 die

> „*Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Er-*

mittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016“

in Kraft getreten. Mit diesen beiden EU-Gesetzen ist ein seit Anfang 2012, mit Vorarbeiten seit 2008, im Zusammenwirken der EU-Kommission, des Europäischen Parlaments und des Rates entworfenes Datenschutz-Reformpaket abgeschlossen worden. Ab dem 25. Mai 2018 wird die Datenschutz-Grundverordnung unmittelbar und direkt in allen Mitgliedsstaaten der EU anwendbar sein. Bis zum 6. Mai 2018 muss die JI-Richtlinie in allen Mitgliedsstaaten, also auch in Sachsen, in nationales Recht umgesetzt worden sein.

Meine Beteiligung

Ich habe von Anfang an auf nationaler Ebene – in der deutschen Datenschutzkonferenz der staatlichen Datenschutzbeauftragten von Bund und Ländern – sowie auf internationaler Ebene – im direkten Kontakt mit der EU-Kommission, Mitgliedern des Europäischen Parlaments sowie der Bundesregierung – an der Reform mitgewirkt.

Eine neue Datenschutzarchitektur

Mit der Datenschutz-Grundverordnung und der JI-Richtlinie werden die bisherige Datenschutz-Richtlinie 95/46/EG, die den Rahmen für die Verarbeitung personenbezogener Daten im größten Teil der öffentlichen Verwaltung und im gesamten nichtöffentlichen Bereich vorgegeben hatte, sowie der Rahmenbeschluss 2008/977/JI, der Gleiches für die grenzüberschreitende Datenverarbeitung im polizeilichen und justiziellen Bereich bewirkt hatte, vollständig ersetzt. Damit wird das Datenschutzrecht auf EU-Ebene grundlegend neu geordnet und eine neue datenschutzrechtliche Architektur in der Union geschaffen.

Datenschutzbehörden künftig auf unionsrechtlicher Grundlage

Mit beiden Rechtsvorschriften wird erstmals in der Bundesrepublik Deutschland und der übrigen Union eine Verwaltung, namentlich die Datenschutz-Aufsichtsbehörden, auf EU-rechtlicher Grundlage bestehen und verfahren. Meine Befugnisse, meine Aufgaben und meine Verfahrensweise werden im Bereich der Datenschutz-Grundverordnung grundsätzlich nur noch auf Unionsrecht beruhen. Nationales Recht, in meinem Fall also bundesdeutsches und sächsisches Recht, wird insofern nur noch als Ausführungsrecht eine Rolle spielen. Anderes gilt für die Datenverarbeitungsvorschriften (z. B. die Erhebungs- oder Löschungsvorschriften nach dem Sozialgesetzbuch), die nach der

Datenschutz-Grundverordnung grundsätzlich weiter durch den nationalen Gesetzgeber gestaltet werden können.

Das Verfahren im Berichtszeitraum

Nachdem die Verhandlungen im Lauf des Jahres 2015 deutlich an Fahrt aufgenommen hatten, traten die Beteiligten – Kommission, Parlament und Rat – zum Ende des Jahres 2015 in die abschließenden sogenannten Trilog-Verhandlungen ein. Der luxemburgische Ratsvorsitz hatte hierzu einen konsolidierten Text erstellt. Zuletzt wurde im Wesentlichen noch über die „besonders sensiblen Daten“ (Art. 9), die sogenannten Datenportabilität (Art. 18), die Meldung von Datenschutzverletzungen (Art. 31, 32), die betrieblichen und behördlichen Datenschutzbeauftragten (Art. 35), die Abberufung eines Mitglieds der Datenschutzaufsichtsbehörde (Art. 48 Abs. 4) sowie über Fragen der Haftung (Art. 77) und Geldbußen (Art. 79) verhandelt. Mit dem 15. Dezember 2015 konnten die Trilog-Verhandlungen zu einem Ende gebracht werden.

Neuerungen durch die Datenschutz-Grundverordnung

Mit der Datenschutz-Grundverordnung werden zum einen die subjektiven Datenschutzrechte natürlicher Personen gestärkt und neue Verfahren zum Schutz der Datenschutz-Grundrechte eingeführt, zum anderen der freie Verkehr personenbezogener Daten in der Union erleichtert.

Datenverarbeitungen, die die betroffene Person tatsächlich oder vermeintlich belasten, werden objektiv aus mehreren Gründen zunehmen und damit auch die Zahl der Beschwerden, die von den Aufsichtsbehörden zu bearbeiten sind. Erstens wird durch das Marktortprinzip (Art. 3) die Zahl der von der Datenschutz-Grundverordnung erfassten Datenverarbeitungsvorgänge – vor allem im Internet – erheblich zunehmen. Zweitens wird darüber hinaus die Digitalisierung aller Lebensbereiche zu einer Vervielfachung der Verarbeitung von personenbezogenen Daten führen.

1.3 Datenschutz-Grundverordnung – Behördliche Datenschutzbeauftragte

Die Datenschutz-Grundverordnung sieht in Art. 37 innerbetriebliche und behördliche Datenschutzbeauftragte vor. Für öffentliche Stellen – *Verantwortliche* (Art. 4 Nr. 7) – sind Datenschutzbeauftragte zukünftig verpflichtend zu berufen, Art. 37 Abs. 1 Buchstabe a der Verordnung (EU) 2016/679.

Somit haben auch abweichend von derzeitigen Verwaltungsfestlegungen wie der VwV Schuldatenschutz nicht nur Schulen ab einer bestimmten Größe, sondern alle Schulen einen Datenschutzbeauftragten zu bestellen. In der Verwaltungspraxis werden Bestellungen Datenschutzbeauftragter nicht selten erstmals außerhalb des staatlichen Verwaltungsbereichs, bei vielen kommunalen Stellen, vorzunehmen sein. Zusätzlich haben auch alle Datenverarbeitungsauftragnehmer als *Auftragsverarbeiter* (Art. 4 Nr. 8) öffentlicher Stellen einen Datenschutzbeauftragten zu bestellen, vgl. hierzu Art. 37 Abs. 1 der Verordnung (EU) 2016/679 und dessen Wortlaut am Anfang.

Wie nach der bisherigen Rechtslage nach dem Sächsischen Datenschutzgesetz können interne und externe Datenschutzbeauftragte bestellt werden (Art. 37 Abs. 6 der Verordnung (EU) 2016/679). Gegenüber der gegenwärtigen Rechtslage, was Zuverlässigkeit und Sachkunde betrifft, präzisiert der Verordnungstext, dass der Datenschutzbeauftragte „auf der Grundlage seiner beruflichen Qualifikation und insbesondere seines Fachwissens“, das er „auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt“ – Bezug genommen wird zudem auf die Aufgaben nach Art. 39 der Verordnung (EU) 2016/679 –, benannt werden soll. Eine ausdrückliche Kontrollbefugnis, was personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterfallen, betrifft, enthält die Datenschutz-Grundverordnung selbst nicht, vgl. § 11 Abs. 3 Satz 2 SächsDSG. Aber die bestellten Personen üben ihr Amt weiterhin weisungsfrei (Weisungsfreiheit) aus und dürfen wegen der Erfüllung ihrer Aufgaben nicht abberufen und benachteiligt werden (Benachteiligungsverbot), Art. 38 Abs. 3 Satz 1 und 2 der Verordnung (EU) 2016/679. Die Weisungsfreiheit bedingt, was die Rechtsstellung angeht, auch weiterhin, dass der Datenschutzbeauftragte in seiner Tätigkeit keinen kommunikativen Dienstwegen unterworfen ist. Verantwortlich ist der Datenschutzbeauftragte in seiner Funktion zwar auch weiterhin lediglich gegenüber der Amtsspitze, vgl. Art. 38 Abs. 3 Satz 3 der Verordnung (EU) 2016/679. Wegen der Weisungsfreiheit betrifft dies aber dienstrechtliche Fragen bzw. die notwendige Information und Beratung gemäß Art. 39 der Verordnung (EU) 2016/679. Die Weisungsfreiheit bedingt jedoch aufgrund der Geheimhaltungs- und Vertraulichkeitspflicht des Art. 38 Abs. 5 der Verordnung (EU) 2016/679 zum Schutz Betroffener, was Berichtsbefugnisse und Berichtspflichten angeht, auch weiterhin eine Verschwiegenheitspflicht, personenbezogene Einzelheiten und Identitäten betreffend, gegenüber der Amtsspitze.

Meiner Behörde sind, ohne dass diese explizit ein Register der Datenschutzbeauftragten zu führen hätte, weiterhin die Kontaktdaten des Datenschutzbeauftragten mitzuteilen. Der Verantwortliche und der Auftragsverarbeiter, die öffentliche Stelle und bisherige Auftragsdatenverarbeiter, haben zudem die „Kontaktdaten“, wozu Namensangaben, dienstliche Adressen, Raumnummern und angebotene Telefon- und E-Mail-Kommuni-

kationsmöglichkeiten zählen, um den Datenschutzbeauftragten erreichen zu können, zu veröffentlichen, vgl. Art. 37 Abs. 7 der Verordnung (EU) 2016/679.

Hervorzuheben ist, dass die Aufgaben des Datenschutzbeauftragten gegenüber der gegenwärtigen Rechtslage geändert werden. Die Aufgaben sind in Art. 39 der Verordnung (EU) 2016/679 aufgeführt. Datenschutzbeauftragte haben nicht mehr, wie bisher in § 11 Abs. 4 Nr. 3 SächsDSG geregelt, das Verfahrensverzeichnis zu führen. Das künftige Verzeichnis von Verarbeitungstätigkeiten wird stattdessen gemäß Art. 30 Abs. 1 der Verordnung (EU) 2016/679 durch den Verantwortlichen selbst geführt. Zudem ist das Verzeichnis nach Art. 30 Abs. 4 der Verordnung (EU) 2016/679 nur noch meiner Behörde auf Anfrage zur Verfügung zu stellen. Ein § 11 Abs. 4 Nr. 5 oder § 31 Abs. 2 SächsDSG vergleichbares Einsichtsrecht für jedermann wird es künftig nicht mehr geben.

Auch ist künftig nur noch der Rat des Datenschutzbeauftragten bei einer *Datenschutz-Folgenabschätzung* durch den Verantwortlichen (siehe dazu 1.4) einzuholen, Art. 35 Abs. 2 der Verordnung (EU) 2016/679. Eine § 11 Abs. 4 Nr. 4 SächsDSG vergleichbare Pflicht zur Durchführung der Vorabkontrolle besteht hingegen künftig nicht mehr. Der Datenschutzbeauftragte hat jedoch gemäß Art. 39 Abs. 1 Buchstabe c der Verordnung (EU) 2016/679 die Durchführung der Datenschutz-Folgenabschätzung zu „überwachen“.

Wie bisher ist der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden und bei der Erfüllung seiner Aufgaben zu unterstützen, Art. 38 Abs. 1 der Verordnung (EU) 2016/679. Es ist sicherzustellen, dass seine anderen Aufgaben und Pflichten nicht zu einem Interessenkonflikt mit seiner Tätigkeit als Datenschutzbeauftragter führen, vgl. Abs. 6 der Vorschrift.

Nachdem es gemäß Art. 39 Abs. 1 der Verordnung (EU) 2016/679 zu seinen Aufgaben gehört, den Verantwortlichen, Auftragnehmer und Beschäftigte hinsichtlich ihrer Pflichten u. a. nach der Datenschutz-Grundverordnung zu beraten, die Verarbeitung zu überwachen und Mitarbeiter zu schulen, ist nach meiner Überzeugung nicht davon auszugehen, dass sich der Arbeitsumfang verringern wird. Hervorzuheben ist nämlich neben der Zusammenarbeit mit der Aufsichtsbehörde – Buchstabe d – als Aufgabe auch noch die neuartige Festlegung, dass der Datenschutzbeauftragte „Anlaufstelle“ für die Aufsichtsbehörde sein soll, Art. 39 Abs. 1 Buchstabe e der Verordnung (EU) 2016/679. Wegen der Aufgabenverdichtung sind die Verantwortlichen und Auftragsverarbeiter pflichtig, sicherzustellen, dass der Datenschutzbeauftragte in angemessenem Umfang

von anderen Aufgaben freigestellt wird bzw. genügend Ressourcen zur Aufgabenerledigung zur Verfügung gestellt bekommt, vgl. Art. 38 Abs. 2 der Verordnung (EU) 2016/679.

1.4 Datenschutz-Grundverordnung – Datenschutz-Folgenabschätzung und vorherige Konsultation

Die bisher in § 10 Abs. 4 SächsDSG vorgesehene Vorabkontrolle wird durch die „Datenschutz-Folgenabschätzung“ (Art. 35) und die „vorherige Konsultation“ (Art. 36) der Datenschutz-Grundverordnung ersetzt.

Anders als die Vorabkontrolle nach dem bisherigen Recht wird die Datenschutz-Folgenabschätzung durch den Verantwortlichen – Art. 4 Nr. 7 der Verordnung (EU) 2016/679 – selbst durchgeführt, Art. 35 Abs. 1 der Verordnung (EU) 2016/679. Ihr Mindest-Inhalt ist in Art. 35 Abs. 7 der Verordnung (EU) 2016/679 festgelegt worden.

Die Datenschutz-Folgenabschätzung ist durchzuführen, wenn sich aus einer Abschätzung der Risiken der Verarbeitungsvorgänge („Schwellwertanalyse“) ein voraussichtlich hohes Risiko, bezogen auf den Schutz personenbezogener Daten, ergibt. Wird festgestellt, dass ein Verarbeitungsvorgang vermutlich kein hohes Risiko aufweist, dann ist dieses Ergebnis für den konkreten Verarbeitungsvorgang mit Angabe der Gründe zu dokumentieren. Artikel 35 selbst benennt in Absatz 3 nur einige Faktoren, die wahrscheinlich zu einem hohen Risiko führen. Aufbauend auf den Leitlinien der Artikel-29-Datenschutzgruppe werden die Datenschutzaufsichtsbehörden eine nicht-abschließende Liste veröffentlichen, die Verarbeitungstätigkeiten aufführt, bei denen eine Datenschutz-Folgeabschätzung durchzuführen ist, vgl. Art. 35 Abs. 4 der Verordnung (EU) 2016/679. Zur Durchführung der Schwellwertanalyse werden künftig Hinweise der Aufsichtsbehörden zur Verfügung gestellt werden.

Eine Datenschutz-Folgenabschätzung ist *vor* der Aufnahme der zu betrachtenden Verarbeitungsvorgänge durchzuführen. Zu beachten ist, dass auch bereits bestehende Verarbeitungsvorgänge unter die Pflicht einer Datenschutz-Folgenabschätzung fallen können. Da eine Datenschutz-Folgenabschätzung meist nicht kurzfristig erstellt werden kann, ist sie rechtzeitig, vorzugsweise im Zusammenhang mit einem Datenschutz- und Informationssicherheitskonzept nach § 5 Abs. 1 SächsEGovG, auf den Weg zu bringen. Dabei kann das sogenannte „Standard-Datenschutzmodell“ (siehe dazu 14.3) Anwendung finden.

Eine Datenschutz-Folgenabschätzung ist kein einmaliger und dann abgeschlossener Akt, sondern kann als Verfahrensmethode und Maßstab eines fortwährenden Beobach-

tungsprozesses begriffen werden. Sollten sich auf Seiten des Verantwortlichen Veränderungen und neue Risiken ergeben, die in der untersuchenden Betrachtung bisher nicht berücksichtigt wurden, so ist die Ausarbeitung zu überprüfen und ggf. anzupassen. Um dies zu gewährleisten, sind geeignete personell-organisatorische Vorkehrungen zu treffen, zum Beispiel mittels eines eingerichteten Datenschutz-Managements.

Wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, ist meine Behörde vor der Verarbeitung zu konsultieren, Art. 36 Abs. 1 der Verordnung (EU) 2016/679. Das Verfahren ist im Wesentlichen in Art. 36 Abs. 2 der Verordnung (EU) 2016/679 geregelt. Komme ich zu der Auffassung, dass die geplante Verarbeitung nicht im Einklang mit dieser Verordnung steht, unterbreite ich dem Verantwortlichen – und ggf. dem Auftragsverarbeiter – innerhalb eines Zeitraums von bis zu acht Wochen nach Erhalt des Ersuchens um Konsultation entsprechende schriftliche Empfehlungen und kann meine in Art. 58 der Verordnung (EU) 2016/679 genannten Befugnisse ausüben. Diese Frist kann unter Berücksichtigung der Komplexität der geplanten Verarbeitung um weitere sechs Wochen verlängert werden. Welche Informationen des Verantwortlichen für die vorherige Konsultation seitens der Aufsichtsbehörden zur Bearbeitung Verwendung finden sollen, regelt Art. 36 Abs. 3 der Verordnung (EU) 2016/679.

1.5 Datenschutz-Grundverordnung – Datenverarbeitung im Auftrag

Die nach § 7 SächsDSG bestehende Sonderregelung für eine Verarbeitung personenbezogener Daten im Auftrag behält die Datenschutz-Grundverordnung bei. Allerdings legt insbesondere Art. 28 der Verordnung (EU) 2016/679 den Auftragnehmern künftig mehr Verantwortung und mehr Pflichten auf.

Datenschutzrechtlich wird der per Auftrag und weisungsgebunden eingesetzte Dienstleister – der *Auftragsverarbeiter* – im Rahmen der (weisungsgebundenen) Verarbeitung für den Auftraggeber nicht als *Dritter* betrachtet. Die normierte Fiktion schließt daher, wie bisher, die Anwendung der Übermittlungsvorschriften aus.

Anders als bisher (siehe dazu 17/14.6.) wird künftig auch eine Auftragsverarbeitung durch Dienstleister außerhalb des EU-/EWR-Raums zulässig sein, wenn die zusätzlichen Anforderungen der Art. 44 ff. der Verordnung (EU) 2016/679 für Verarbeitungen in Drittstaaten eingehalten werden.

Künftig sollen jedoch ausdrücklich nur Auftragnehmer beauftragt werden, die hinreichend Garantien dafür bieten, dass sie geeignete technische und organisatorische Maßnahmen für einen ausreichenden Datenschutz haben, sodass die Verarbeitung im Einklang mit der Datenschutz-Grundverordnung erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet ist, vgl. Art. 28 Abs. 1 der Verordnung (EU) 2016/679.

Wie bisher muss mit dem Auftragnehmer im Regelfall ein Vertrag über die weisungsgebundene Tätigkeit geschlossen werden, der schriftlich oder künftig auch in elektronischer Form abgefasst sein kann, Art. 28 Abs. 3 und 9 der Verordnung (EU) 2016/679. Für den notwendigen Inhalt des Vertrags gilt weitestgehend das Gleiche wie bisher. Ein wichtiger Bestandteil wird jedoch vor allem die Darstellung der erforderlichen Maßnahmen zur Sicherheit der Verarbeitung nach Art. 32 der Verordnung (EU) 2016/679.

Es ist eine der Aufgaben der Aufsichtsbehörden, für solche Verträge zur Auftragsverarbeitung als Muster sog. Standardvertragsklauseln festzulegen, sowohl für Auftragsverhältnisse innerhalb EU/EWR wie auch für Auftragsverhältnisse in Drittstaaten. Entsprechende Ausarbeitungen werden gegenwärtig noch vorbereitet.

Will der Auftragsverarbeiter Subunternehmen als weitere Auftragsverarbeiter bei der Erbringung der vereinbarten Dienstleistung einsetzen, so bedarf dies der vorherigen (schriftlichen oder elektronischen) Genehmigung durch den Verantwortlichen. Später beabsichtigte Änderungen bei den eingesetzten Subunternehmen muss der Auftragsverarbeiter dem Auftraggeber als Verantwortlichen vorher mitteilen, wobei der Verantwortliche dann bei Bedarf Einspruch gegen die geplante Einbeziehung des neuen Subunternehmens einlegen kann, Art. 28 Abs. 2 der Verordnung (EU) 2016/679 – vgl. auch Absatz 4 der Vorschrift.

Verstößt ein Auftragsverarbeiter gegen die Pflicht zur weisungsgebundenen Verarbeitung, indem er die Daten des Auftraggebers eigenmächtig für eigene Zwecke oder Zwecke Dritter verarbeitet, gilt er insoweit selbst als Verantwortlicher – mit allen rechtlichen Folgen, z. B. auch zur Erfüllung der Betroffenenrechte, Art. 28 Abs. 10 der Verordnung (EU) 2016/679. Neu hinzugekommen sind auch spezielle Haftungsregelungen für Auftragsverarbeiter bei Datenschutzverletzungen. Demnach drohen Auftragsverarbeitern bei Verstößen auch Schadensersatzforderungen von Betroffenen, vgl. auch Art. 82 Abs. 1 der Verordnung (EU) 2016/679.

Des Weiteren besteht für Auftragsverarbeiter die neue Pflicht, künftig auch ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 der Verordnung (EU) 2016/679 für alle Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätig-

keiten der Verarbeitung zu führen. Zudem hat er, wenn er für eine öffentliche Stelle tätig wird, gemäß Art. 37 Abs. 1 der Verordnung (EU) 2016/679 in jedem Fall einen Datenschutzbeauftragten zu bestellen.

Die bisher in § 7 Abs. 5 SächsDSG vorgenommene Einordnung aller Wartungsarbeiten als Auftragsdatenverarbeitung wird es künftig so nicht mehr geben. Nur im Falle einer Notwendigkeit oder Möglichkeit des Zugriffs auf personenbezogene Daten durch IT-Wartungs- oder Fernwartungs-Dienstleister – z. B. bei der Prüfung von Speicher-Dumps, bei Support-Arbeiten in Systemen des Auftraggebers usw. – handelt es sich im Hinblick auf die weite Definition einer Verarbeitung in Art. 4 Nr. 2 der Verordnung (EU) 2016/679 – z. B. das Auslesen, Abfragen, Verwenden von Daten – ebenfalls um eine Form bzw. Teiltätigkeit einer Auftragsverarbeitung.

Nach Art. 33 Abs. 2 der Verordnung (EU) 2016/679 muss ein Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten nach Bekanntwerden unverzüglich dem Verantwortlichen melden.

Ebenso sind die umfassenden Bußgeldvorschriften des Art. 83 Abs. 4, 5 und 6 der Verordnung (EU) 2016/679 zu berücksichtigen: Diese können bei Verstößen durchaus auch bei einem Auftragsverarbeiter zur Anwendung kommen, speziell z. B. bei Verstößen des Auftragsverarbeiters gegen seine Verpflichtungen aus Art. 28 Abs. 2 bis 4 der Verordnung (EU) 2016/679.

1.6 Datenschutz-Grundverordnung – Die Einwilligung

Nach der neuen Datenschutz-Grundverordnung kann Datenverarbeitung neben gesetzlichen Rechtsgrundlagen auf eine Einwilligung gestützt werden, Art. 6 Abs. 1 der Verordnung (EU) 2016/679. Die Einwilligung folgt nicht mehr dem Sächsischen Datenschutzgesetz, sondern der Datenschutz-Grundverordnung. Allerdings dürfen Konkretisierungen bereichsspezifisch erfolgen, soweit die Verordnung dies zulässt.

Art. 4 Nr. 11 der Verordnung (EU) 2016/679 enthält die Begriffsbestimmung zur Einwilligung, die vom bisherigen Recht des § 4 SächsDSG abweicht. Eine Neuerung ist danach, dass eine unmissverständliche Willensbekundung, einverstanden zu sein, genügt. Auch konkludente Handlungen sind denkbar. Und das bedeutet auch, dass Einwilligungen nicht mehr schriftlich zu erfolgen haben, selbst Gesten oder mündliche Bekundungen sind ausreichend, vgl. den Wortlaut von Art. 4 Nr. 11 der Verordnung (EU) 2016/679. Allerdings ist in dem Zusammenhang auch auf die Nachweispflicht des *Verantwortlichen*, dass eingewilligt worden ist, hinzuweisen, Art. 7 Abs. 1 der Verordnung (EU) 2016/679. In der Praxis werden Behörden daher zweckmäßigerweise weiter-

hin eine schriftliche Erklärung des Einwilligenden einzuholen bestrebt sein, da die Nicht-Nachweisbarkeit gravierende Folgen, was die Annahme der Rechtmäßigkeit der Datenverarbeitung auf Einwilligungsgrundlage angeht, haben kann. Dem Erwägungsgrund 32 der Datenschutz-Grundverordnung ist zusätzlich zu entnehmen, dass für die Erteilung von Einwilligungen ein aktives Verhalten der betroffenen Personen erforderlich ist und eine Einwilligungsmöglichkeit auf elektronischem Wege ohne Hindernisse grundsätzlich besteht (z. B. per E-Mail), dagegen Stillschweigen, bereits markierte Vorlagen oder Untätigkeit der betroffenen Personen keine Einwilligung darstellen.

Die Begriffsdefinition des Art. 4 der Verordnung (EU) 2016/679 legt zudem fest, dass es sich um eine freiwillige Erklärung für einen bestimmten Fall unter der Voraussetzung der Informiertheit der einwilligenden betroffenen Person handeln muss, Art. 4 Nr. 11 der Verordnung (EU) 2016/679.

Im Hinblick auf die Freiwilligkeit ist auf Erwägungsgrund 43 der Datenschutz-Grundverordnung hinzuweisen, wonach keine gültige Rechtsgrundlage besteht, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, und es deshalb „unwahrscheinlich“ ist, dass die Einwilligung freiwillig gegeben wurde. Insbesondere soll dies gelten, wenn es sich bei dem Verantwortlichen um eine Behörde handelt. Gleichwohl wird in dem Erwägungsgrund diese Aussage auf die konkreten Einzelfallumstände bezogen. Soweit eine Einwilligung nicht gesetzlich ausdrücklich vorgesehen ist, werden damit die Möglichkeiten der Datenverarbeitung von öffentlichen Stellen weiter eingeschränkt sein und sich zunehmend auf einen Bereich, der nicht einem Über-Unterordnungsverhältnis zuzurechnen ist, bzw. auf Zusatzleistungen seitens öffentlicher Stellen gegenüber betroffenen Personen zu beschränken haben. Generell ist nach Erwägungsgrund 42 zu beachten, dass Freiwilligkeit der Einwilligung eine Verweigerungs- und Widerrufsmöglichkeit ohne Nachteile bedingt.

Erwägungsgrund 33 relativiert die eigentlich erforderliche Konkretisierung des Zwecks, den „bestimmten Fall“ nach Art. 4 Nr. 11 der Verordnung (EU) 2016/679, bei der Einwilligung bei Forschungsvorhaben unter Einhaltung ethischer Standards, indem eine Eingrenzung auf bestimmte Bereiche der Forschung genügen soll. Öffentliche Stellen wie Universitäten, Institute und Universitätskliniken können sich hierauf berufen.

In Bezug auf die Informiertheit gemäß Art. 4 Nr. 11 der Verordnung (EU) 2016/679 ist bei Datenerhebungen zudem auf Art. 13 der Verordnung (EU) 2016/679 hinzuweisen, der Festlegungen zur Informationspflicht des Verantwortlichen enthält.

Art. 7 der Verordnung (EU) 2016/679, in dem die Bedingungen der Einwilligung festgelegt werden, regelt die schon erwähnte Nachweispflicht in Absatz 1, ein neu-

artiges explizites Gebot, ausdrückliches Ersuchen um Einwilligung von anderen Textinhalten inhaltlich zu trennen und textlich verständlich abzusetzen (Absatz 2), eine Hinweispflicht auf den durchführbaren Widerruf jederzeit für die Zukunft, dass der Widerruf für die Zukunft gilt und eine Hinweispflicht des Verantwortlichen gegenüber der betroffenen Person darauf (Absatz 3) sowie ein Kopplungsverbot, die Einwilligung nicht in Abhängigkeit zu Verträgen oder der Erbringung von Dienstleistungen zu bringen. Auch diese Qualifizierung des Gebots der Freiwilligkeit – Art. 4 Nr. 11 – in Abs. 4 des Art. 7 der Verordnung (EU) 2016/679 stellt eine Neuerung dar. Keine Freiwilligkeit der Einwilligung läge danach vor, wenn die Erfüllung eines Vertrages von einer Einwilligung abhängig gemacht wird. Rechtswidrigkeit der Datenverarbeitung wäre die Folge.

Bezogen auf Absatz 2 ist bei Vertragsregeln zu beachten, dass anders als nach der bisherigen Rechtsprechung des BGH (Urteil vom 16. Juli 2008 – VIII ZR 348/06; Urteil vom 11. November 2009 – VIII ZR 12/08) es nicht mehr ausreichend sein soll, dass betroffene Personen auf inkludierte Vertragsklauseln verwiesen werden, die fiktiv erteilte Erklärungen enthalten, Erwägungsgrund 32 der Datenschutz-Grundverordnung.

Relevant im Schul- und Bildungsbereich sein kann Art. 8 der Verordnung (EU) 2016/679, insbesondere wenn im Schulbereich Lern-Medien und Internetplattformen in Anspruch genommen werden sollen, vgl. zu Medien hierzu die ausführliche Betrachtung unter 7.3. Art. 8 der Verordnung (EU) 2016/679 enthält besondere Regeln für die Einwilligung von Kindern bei sogenannten „informationsgesellschaftlichen Diensten“. Danach ist es für eine Einwilligung erforderlich, dass es sich um einen mindestens 16-Jährigen oder eine Erklärung der Elternsorgeberechtigten handelt. Zudem ist eine ordnungsgemäße Einwilligung durch technische Maßnahmen sicherzustellen.

Art. 9 der Verordnung (EU) 2016/679 legt in Bezug auf die Verarbeitung besonderer Kategorien personenbezogener Daten – besonders schützenswerte Daten – Ausnahmebereiche nach der Datenschutz-Grundverordnung fest, wonach für die Verarbeitung solcher Daten eine ausdrückliche Einwilligung erforderlich ist. Konkludente Handlungen sind danach ausgeschlossen, vgl. Art. 9 Abs. 2 Buchstabe a der Verordnung (EU) 2016/679. Im Falle der Unmöglichkeit der Einwilligung bei Eintreten besonderer Umstände zum Schutz lebenswichtiger Interessen der betroffenen Personen kann auf eine Einwilligung verzichtet werden, Art. 9 Abs. 2 Buchstabe c der Verordnung (EU) 2016/679. Letztlich sollen besonders schutzwürdige Daten verarbeitet werden dürfen, wenn eine Stiftung oder eine Vereinigung ohne Gewinnerzielungsabsicht geeignete datenschutzrechtliche Garantien in Bezug auf Mitglieder oder Kontaktpersonen

sicherstellt und eine Offenlegung gegenüber Dritten nicht ohne Einwilligung erfolgt, Art. 9 Abs. 2 Buchstabe d der Verordnung (EU) 2016/679.

Bezogen auf Art. 9 Abs. 2 Buchstabe a der Verordnung (EU) 2016/679 wären danach z. B. gesetzliche Regelungen zur Patientendatenverarbeitung nach dem Sächsischen Krankenhausgesetz mit der Festlegung der Schriftlichkeit der Einwilligung im Einklang mit der Verordnung.

Einwilligungen, die nicht den Verordnungsanforderungen genügen, sind unwirksam und können nicht als Rechtsgrundlage für eine Datenverarbeitung herangezogen werden.

Bei Verstößen – einschließlich der Bedingungen für die Einwilligung – kann nach Maßgabe von Art. 83 Abs. 5 Buchstabe a der Verordnung (EU) 2016/679 eine Geldbuße verhängt werden. Schadensersatzansprüche der betroffenen Person kommen zudem in Betracht, vgl. Art. 82 der Verordnung (EU) 2016/679.

Bestehende Einwilligungen sind durch die öffentlichen Stellen auf ihre Wirksamkeit zu überprüfen, vgl. hierzu die Ausführungen unter 1.7.

1.7 Datenschutz-Grundverordnung – Zur Fortgeltung willenserklärungsabhängiger Rechtsverhältnisse nach altem Recht: Einwilligungen, Auftragsdatenverarbeitung, Datenschutzbeauftragte, Datengeheimnis

Mit Wirksamwerden der Datenschutz-Grundverordnung stellt sich auch die Frage, inwieweit auf Grundlage alten Rechts bestehende Datenverarbeitungsverhältnisse fortgelten. Soweit gesetzliche und bereichsspezifische Regelungen weiterbestehen, können auch Datenverarbeitungen fortgesetzt werden. Eine andere Problemlage ergibt sich bei Rechtsinstrumenten, die in die Datenschutz-Grundverordnung aufgenommen worden und dort abschließend geregelt sind und altes Recht verdrängt haben. Die Frage stellt sich insbesondere bei erteilten Einwilligungen, Verträgen der Auftragsdatenverarbeitung und der Bestellung behördlicher Datenschutzbeauftragter sowie bei Verpflichtungen auf das Datengeheimnis.

Bei der Einwilligung kommt es darauf an. Entscheidend wird im Wesentlichen sein, ob die alte Willenserklärung, die im Verfahren angesichts bestimmter rechtlicher und tatsächlicher Umstände abgegeben worden ist, der Einwilligung, die erneuert oder neu abgegeben würde, entspricht. Die Einwilligung bezieht sich auf eine konkrete Datenverarbeitung unter tatsächlichen Bedingungen. Erwägungsgrund 171 der Datenschutz-Grundverordnung eröffnet die Möglichkeit der Fortgeltung der Wirksamkeit der Ein-

willigung, die Grundlage einer begonnenen Datenverarbeitung sein soll. Danach ist es nicht erforderlich, dass die betroffene Person zu einer gleichartigen fortgesetzten Datenverarbeitung, zu der sie gemäß altem Recht eingewilligt hat, erneut einwilligt, wenn die Art der bereits erteilten Einwilligung den Bedingungen der Datenschutz-Grundverordnung entspricht. Eine zurückliegend wirksam erteilte Einwilligung nach altem Recht gilt dann bis auf weiteres für unbestimmte Zeit fort.

Erwägungsgrund 42 der Datenschutz-Grundverordnung hebt bei Einwilligungen darauf ab, dass eine vom Verantwortlichen vorformulierte Einwilligungserklärung in verständlicher und leicht zugänglicher Form, in einer klaren und einfachen Sprache zur Verfügung gestellt wird, keine missverständlichen Inhalte aufweist und die betroffene Person mindestens darüber informiert worden ist, wer der Verantwortliche ist und zu welchen Zwecken ihre personenbezogenen Daten verarbeitet werden sollen. Diese Bedingungen werden bei Alt-Einwilligungen gemäß der Vorschrift zur informierten Einwilligung nach § 4 Abs. 3 SächsDSG regelmäßig noch erfüllt sein. Zu beachten ist darüber hinaus aber auch Art. 7 Abs. 3 Satz 3 der Verordnung (EU) 2016/679, was die Hinweispflicht auf die Wirkung des Widerrufs für die Zukunft anbelangt. Außerdem ist Art. 13 der Verordnung (EU) 2016/679, wonach umfassende Informationspflichten bestehen, die bei Erhebung personenbezogener Daten bei betroffenen Personen vorgesehen sind, einzuhalten.

Es ist durch die öffentlichen Stellen, die eine Datenverarbeitung, die auf Einwilligungen gestützt worden ist, begonnen haben, daher von Fall zu Fall zu entscheiden, ob zurückliegende Einwilligungen den Regelungen der Datenschutz-Grundverordnung genügen würden. In Zweifelsfällen wird aus Gründen der Rechtssicherheit die Einwilligung zu wiederholen und nach der Datenschutz-Grundverordnung erneut einzuholen sein.

Im Unterschied zur Einwilligung finden sich zur Auftragsdatenverarbeitung keine Hinweise zur Fortgeltung in den Erwägungsgründen. Die Fortgeltung des alten Rechtsinstruments ist nicht vorgesehen. Altes Recht ist ab dem 25. Mai 2018, dem vollständigen Wirksamwerden der Datenschutz-Grundverordnung, außer Kraft. Aber Auftragsdatenverarbeitungsverhältnisse bestehen auf vertraglicher Grundlage. Und Verträge sind nach deutschem Recht einzuhalten, *pacta sunt servanda*. Allerdings handelt es sich letztendlich um eine von beiden Parteien nicht zu vertretende Vertragsstörung, die sich mit der neuen Rechtslage eingestellt hat, wenn die Vertragsparteien bei einer vertragsgemäßen Fortsetzung der Datenverarbeitungsverhältnisse, die einem nicht mehr wirksamen Rechtsinstrument entspricht, gegen öffentliches Ordnungsrecht – EU-Recht – verstoßen. Das alte Rechtsinstitut der Auftragsdatenverarbeitung – jetzt Auftragsverarbeitung – ist, was Rechte, Pflichten und Verhältnisse des Auftragsverarbeiters

gegenüber dem Auftraggeber als Verantwortlichem betrifft, materiell-rechtlich nach den Normativen der Datenschutz-Grundverordnung verändert, vgl. 1.5. Bestehende alte Formularverträge, wie die meiner Dienststelle, verweisen inhaltlich zudem neben der Vorschrift des § 7 SächsDSG zur Auftragsdatenverarbeitung regelmäßig auf weitere Bestimmungen, die außer Kraft gesetzt sind, wie z. B. Schutzziele nach § 9 SächsDSG, die mit der Datenschutz-Grundverordnung nicht mehr vollständig kongruent sein werden. Hinzuweisen ist daher in diesem Zusammenhang auf Erwägungsgrund 171 – zweiter Satz –, wonach Verarbeitungen, die zum Zeitpunkt der Anwendung dieser Verordnung bereits begonnen haben, innerhalb von zwei Jahren nach dem Inkrafttreten der Verordnung mit ihr in Einklang gebracht werden „sollten“. Zu berücksichtigen ist zudem auch die Schriftlichkeit bzw. Dokumentationspflicht nach Art. 28 Abs. 9 der Verordnung (EU) 2016/679, was denknotwendig einschließt, dass auch Änderungen des Vertrags entsprechend zu dokumentieren sind. Damit im Einklang stehend, sehen die Verträge – zivilrechtlich – regelmäßig vor, dass Änderungen des Vertrags nur wirksam werden sollen, wenn sie schriftlich erfolgen.

Als Ergebnis des Ganzen bleibt danach festzuhalten, dass Verantwortliche als datenverarbeitende Stellen nach der Datenschutz-Grundverordnung pflichtig sind, gemäß den Bestimmungen der Verordnung Auftragsverarbeitung zu organisieren und dass, solange alte Verträge der Auftragsdatenverarbeitung fortbestehen und die Auftragsverarbeitung nicht in diesem Sinne ordnungsgemäß durchgeführt werden kann, öffentliche Stellen auch pflichtig sind, die entsprechenden Verträge anzupassen oder zu beenden. Auf welche Weise dies erfolgt, ob mit einer einvernehmlichen Vertragsänderung oder etwa im Wege einer außerordentlichen Kündigung aus wichtigem Grund, ist eine zivilrechtliche Frage, die im Einzelfall zu bewerten und zu entscheiden ist, vgl. auch § 313 Abs. 1 BGB.

In jedem Fall sind bestehende Auftragsdatenverarbeitungsverhältnisse auf die neue Rechtslage hin zu überprüfen, vgl. Erwägungsgrund 171.

Bei der Bestellung der Datenschutzbeauftragten kann nach meiner Überzeugung das alte Rechtsverhältnis in jedem Fall nicht erhalten bleiben. Nach bisherigem Recht durchgeführte Bestellungen sind regelmäßig unter ausdrücklicher Bezugnahme auf die entsprechenden Rechtsnormen und ab 25. Mai 2018 nach dann nicht mehr wirksamem Recht erfolgt. Zurückliegende Bestellungen sind nicht nur deklaratorisch in Bezug auf die Aufgabe, sondern formell-inhaltlich erfolgt. § 11 SächsDSG z. B. ist Rechtsgrund der Bestellung. Zudem ist, wie unter 1.3 dargestellt, inhaltlich der Aufgaben- und Befugnisbereich des Datenschutzbeauftragten verändert worden, was bei einer Nichtanpassung der Alt-Bestellungen in dienst-, arbeits- und vertragsrechtlicher Hinsicht zu nicht überschaubaren rechtlichen Fragen zu führen geeignet ist. Die Bestellung der

Datenschutzbeauftragten bei öffentlichen Stellen ist nach der neuen Rechtslage auch nicht mehr nur fakultativ, sondern obligatorisch vorzunehmen. Zur Herstellung vertragsrechtlicher bzw. dienstrechtlicher Rechtssicherheit rate ich daher auch, die Bestellungen der Datenschutzbeauftragten anzupassen oder zum Ende des 24. Mai 2018 zu widerrufen und ggf. im Gegenzug Bestellungen zum 25. Mai 2018 nach der Datenschutz-Grundverordnung unter Beachtung der zivil- und dienstrechtlichen Besonderheiten vorzunehmen. Ebenso würde man in Anbetracht der veränderten Aufgaben zweckmäßigerweise die Verträge mit externen Dienstleistern und Datenschutzbeauftragten modifizieren. Wenn auch Art. 37 ff. der Verordnung (EU) 2016/679 keine schriftliche Bestellung verlangen, wird bei internen Bestellungen weiterhin nach § 50 BeamtStG bzw. nach § 2 Abs. 2 NachwG zu verfahren sein und die Aufnahme der Bestellung bzw. die vorgenommene Anpassung in die Personalakte erfolgen müssen. Im Übrigen wird bei externen Bestellungen vertraglich oder mit Verwaltungsvereinbarung die Einsetzung und Aufgabenübertragung bei öffentlichen Stellen – bereits aus Gründen der ordnungsgemäßen Haushaltsführung – schriftlich zu dokumentieren sein. Angeraten wird meinerseits auch, die Bestellungen in der bisher empfohlenen Weise unter Nennung der konkreten Aufgaben und bei interner Übertragung unter Freistellung des Beschäftigten von sonstigen Aufgaben bzw. der Einräumung eines Zeitanteils vorzunehmen und auf die Vorschriften der Datenschutz-Grundverordnung zu verweisen. Nach altem Recht bestellten behördlichen Datenschutzbeauftragten sollte so mit einem erneuernden Akt ebenfalls in Bezug auf ihren Rechtsstatus Gewissheit verschafft werden.

Eine Verpflichtung auf das Datengeheimnis entfällt nach der Datenschutz-Grundverordnung, auch wenn sich eine gewisse Entsprechung zum bisherigen Datengeheimnis in Art. 29 der Verordnung (EU) 2016/679 findet. Die eingetretene materiell-rechtliche Unwirksamkeit für die Zukunft, ab 25. Mai 2018, hat keine weiteren Folgen. Es ist seitens der personalverwaltenden Stellen noch zu prüfen, ob und wann Dokumente zur Verpflichtung auf das Datengeheimnis aus Personalakten entfernt werden können und sollen.

Der im Kontext beachtenswerte Erwägungsgrund 171 im gesamten Wortlaut lautet folgendermaßen: „Die Richtlinie 95/46/EG sollte durch diese Verordnung aufgehoben werden. Verarbeitungen, die zum Zeitpunkt der Anwendung dieser Verordnung bereits begonnen haben, sollten innerhalb von zwei Jahren nach dem Inkrafttreten dieser Verordnung mit ihr in Einklang gebracht werden. Beruhen die Verarbeitungen auf einer Einwilligung gemäß der Richtlinie 95/46/EG, so ist es nicht erforderlich, dass die betroffene Person erneut ihre Einwilligung dazu erteilt, wenn die Art der bereits erteilten Einwilligung den Bedingungen dieser Verordnung entspricht, sodass der Verantwortliche die Verarbeitung nach dem Zeitpunkt der Anwendung der vorliegenden Verord-

nung fortsetzen kann. Auf der Richtlinie 95/46/EG beruhende Entscheidungen bzw. Beschlüsse der Kommission und Genehmigungen der Aufsichtsbehörden bleiben in Kraft, bis sie geändert, ersetzt oder aufgehoben werden.“

2 Parlament

Mitunter treten Mitglieder des Landtags oder Vertreter eines Staatsministeriums mit der Frage an mich heran, inwieweit das Recht auf informationelle Selbstbestimmung Dritter der Beantwortung von Abgeordnetenschreiben – gemeint sind nicht die formalisierten parlamentarischen Fragerechte gemäß Art. 51 SächsVerf, sondern informelle Abgeordnetenschreiben – entgegensteht. Mit Abgeordnetenschreiben wenden sich Mitglieder des Landtags direkt an ein Staatsministerium, um Informationen zu erfragen und Auskünfte zu erlangen.

Um zu klären, welcher rechtliche Rahmen für die Beantwortung solcher Schreiben durch ein Staatsministerium zu beachten ist, bedarf es zunächst einer Einordnung des Abgeordnetenschreibens innerhalb der Informationsbeziehungen zwischen Parlament und Staatsregierung.

Direkt an ein Staatsministerium gerichtete Abgeordnetenschreiben gehören nicht zu den formell geregelten Ausformungen des Fragerechts der Abgeordneten, das für die Kontrollfunktion des Parlaments von zentraler Bedeutung ist. Art. 51 Abs. 1 Satz 1 SächsVerf bestimmt, dass Fragen einzelner Abgeordneter oder parlamentarische Anfragen die Staatsregierung oder ihre Mitglieder im Landtag und in seinen Ausschüssen nach bestem Wissen unverzüglich und vollständig zu beantworten haben. Näheres regelt nach Art. 51 Abs. 3 SächsVerf die Geschäftsordnung des Landtags. In Abschnitt IX. der Geschäftsordnung des 6. Sächsischen Landtags (GO) finden sich Bestimmungen zum Verfahren bei der Befragung der Staatsminister nach der Aktuellen Stunde in Plenum, zur Fragestunde im Rahmen von Sitzungen des Landtags, zur Aktuellen Stunde, zu Großen Anfragen sowie zu Kleinen Anfragen. Diese Ausformungen des Fragerechts unterfallen Art. 51 SächsVerf; sie sind in der Geschäftsordnung formell geregelt und ziehen nach ständiger Rechtsprechung des Sächsischen Verfassungsgerichtshofes eine Pflicht der Staatsregierung zur Beantwortung nach sich, die sich direkt aus Art. 51 SächsVerf ergibt. Die Antwort der Staatsregierung oder ihrer Mitglieder erfolgt in diesen Fällen gemäß Art. 51 Abs. 1 SächsVerf „im Landtag“ und „in seinen Ausschüssen“. Die Fragen und ihre Antworten sind als Teil des Plenarprotokolls oder als sonstige Landtagsdrucksachen in aller Regel öffentlich zugänglich und stehen nicht nur dem Fragesteller allein zur Verfügung.

Das Abgeordnetenschreiben wird im Gegensatz zu den genannten Frageformen in der Geschäftsordnung „verfahrenstechnisch“ nicht geregelt, es findet aber an einer Stelle – in § 56 Abs. 3 Satz 3 GO – Erwähnung. Diese Erwähnung des Abgeordnetenschreibens in der Geschäftsordnung des Landtags und der lange parlamentarische Brauch der

Ausübung des Informationsrechts der Abgeordneten (auch) über dieses Instrument lassen keine Zweifel an der Zulässigkeit des Abgeordnetenschreibens. Wenn sich diese nicht aus Art. 51 SächsVerf ergibt, was insofern zweifelhaft wäre, als das Verfahren für das Abgeordnetenschreiben in der Geschäftsordnung gerade nicht formell geregelt ist und die Antwort nicht „im Landtag“ oder „in seinen Ausschüssen“ erfolgt, sondern direkt an den anfragenden Abgeordneten gerichtet wird, so wird sich die Befugnis des Abgeordneten zu direkten Anfragen bei Staatsministerien jedenfalls aus der Ausübung seines freien Mandats nach Art. 39 Abs. 3 SächsVerf herleiten lassen.

Abgeordnetenschreiben sind danach nicht als formelle Anfrage im Sinne von Art. 51 SächsVerf anzusehen. Eine Pflicht zur Beantwortung durch die Staatsregierung und ihre Mitglieder oder Beauftragten ergibt sich mithin nicht aus Art. 51 Abs. 1 SächsVerf; die Beschränkung der Antwort richtet sich damit auch nicht nach Art. 51 Abs. 2 SächsVerf. Vielmehr liegt ihre Beantwortung durch die Exekutive in deren Ermessen. Hinsichtlich des „Ob“ einer Antwort dürfte bei Fragen von Abgeordneten, die auf den Verantwortungsbereich der Staatsregierung zielen, allerdings in aller Regel eine Ermessensreduzierung auf null anzunehmen sein und eine entsprechende Verpflichtung der Staatsregierung bestehen. Bezüglich des „Wie“, d. h. des Inhalts der Antwort hätte die Staatsregierung bei einer evtl. Verarbeitung personenbezogener Daten allerdings einfachgesetzliche, den Schutz potentiell Betroffener bezweckende Übermittlungsvorschriften zu beachten. Die einschlägige Bestimmung ist dabei § 16 SächsDSG.

Die Antwort auf Abgeordnetenschreiben stellt keine fachspezifische Aufgabe einer Behörde dar – sie gehört für Stellen der Staatsregierung vielmehr, wie etwa die Erteilung von Auskünften an die Presse oder die Löschung nicht mehr erforderlicher personenbezogener Daten, zum Kanon allgemeiner Aufgaben der Verwaltung. Eine Übermittlung zum Zweck der Beantwortung eines Abgeordnetenschreibens dient damit nicht der Erfüllung eigener Aufgaben im Sinne von § 16 Abs. 1 Nr. 1 SächsDSG. Einschlägig ist § 16 Abs. 1 Nr. 2 SächsDSG, wobei das berechtigte Interesse des Abgeordneten in aller Regel gegeben sein dürfte (s. o.). Die Abwägung zwischen dem Interesse des Abgeordneten an der erfragten Information und dem Geheimhaltungsinteresse des Betroffenen hat nun über die Berücksichtigung des schutzwürdigen Interesses des Betroffenen nach § 16 Abs. 1 Nr. 2 SächsDSG zu erfolgen.

Dabei können für personenbezogene Auskünfte auf Abgeordnetenschreiben die vom Sächsischen Verfassungsgerichtshof für Auskünfte im Rahmen von Art. 51 SächsVerf entwickelten Abwägungsgrundsätze herangezogen werden: Das Informationsinteresse des Abgeordneten und das Geheimhaltungsinteresse des Dritten sind unter Berücksichtigung der Bedeutung der Pflicht zur erschöpfenden Beantwortung parlamentarischer Anfragen für die Funktionsfähigkeit des parlamentarischen Systems gegeneinander ab-

zuwägen. Da sowohl das Grundrecht auf informationelle Selbstbestimmung als auch der parlamentarische Informationsanspruch auf der Ebene des Verfassungsrechts angesiedelt sind, müssen sie im konkreten Fall einander so zugeordnet werden, dass beide so weit wie möglich ihre Wirkungen entfalten (SächsVerfGH, Urteil vom 20. April 2010 – Vf. 54-I-09, S. 24). Diese Bewertung hat die Staatsregierung einzelfallbezogen anhand der jeweiligen Gesamtumstände vorzunehmen (vgl. SächsVerfGH, a. a. O.).

Kommt die Staatsregierung bzw. das angefragte Staatsministerium in der Einzelfallabwägung zum Ergebnis eines Vorrangs des Schutzes des oder der Betroffenen, muss eine Übermittlung unterbleiben. In der Regel wird das Ministerium dies in seiner Antwort auf das Abgeordnetenschreiben mitteilen und begründen. Nicht personenbezogene bzw. -beziehbare, insbesondere pseudonymisierte Auskünfte dürften selbstverständlich erteilt werden.

Ergibt die Abwägung im Einzelfall ein Übergewicht des Interesses des Abgeordneten an der Information, ist eine Übermittlung grundsätzlich zulässig. Allerdings schreibt § 16 Abs. 3 SächsDSG für diesen Fall eine Anhörung des Betroffenen vor der Übermittlung vor. Schwerwiegende öffentliche oder private Belange – § 16 Abs. 3, 2. Halbsatz SächsDSG – dürften vor Übermittlungen auf Abgeordnetenschreiben einer Anhörung nicht entgegenstehen. Der Abgeordnete hat stets die Möglichkeit, sein Informationsrecht über eine formelle Anfrage, insbesondere die Kleine Anfrage nach § 56 GO zu befriedigen, wobei es nicht zu Anhörungen/Unterrichtungen der von Datenübermittlungen betroffenen Dritten käme. Einen Anspruch auf Geheimhaltung seiner Anforderungen personenbezogener Daten im Wege des einfachen Abgeordnetenschreibens hat der Abgeordnete nicht. Gleiches gilt für die Unterrichtung der Betroffenen nach einer erfolgten Übermittlung (§ 16 Abs. 3 SächsDSG). Sollte der Betroffene auf die Anhörung vor der Übermittlung dieser widersprechen (§ 22 SächsDSG), müsste die Staatsregierung bzw. das Staatsministerium prüfen, ob den vorgebrachten persönlichen Gründen Vorrang gegenüber dem Interesse der Behörde, ein Abgeordnetenschreiben zu beantworten, einzuräumen ist. Eine Übermittlung ist in der Regel zulässig, wenn sie zumindest auch im öffentlichen Interesse erfolgt. Die Beantwortung von Abgeordnetenschreiben, die in Ausübung des freien Mandats an die Exekutive gerichtet werden, liegt auch im öffentlichen Interesse. Über die Anhörung und Unterrichtung wäre der Betroffene zudem in der Lage, die Übermittlung gerichtlich überprüfen zu lassen.

3 Europäische Union

In diesem Jahr nicht belegt. Bitte beachten Sie die Punkte 1.1 bis 1.7 dieses Tätigkeitsberichts.

4 Medien

4.1 Datenschutz als ein Teil der Medienbildung – Abschlussbericht der AG Digitale Medien

Digitale Medien gehören selbstverständlich zum Alltag der meisten Menschen. Glaubt man mittelfristigen Zukunftsprognosen und verfolgt die dynamischen Entwicklungen, die die Digitalisierung mit sich bringt, ist es allerhöchste Zeit, sich dem Themenfeld Digitale Medien in umfassender Weise nachhaltig zu widmen. Nur so können die Menschen mit den technischen Errungenschaften Schritt halten, diese mündig und selbstbewusst in ihr Leben einbinden und selbst gestalten. Digitales Grundwissen der Bürger ist eine Voraussetzung für die Erhaltung des Wirtschafts- und Wissenschaftsstandorts Sachsen.

Gemäß eines Beschlusses des Plenums des Landespräventionsrates luden der Sächsische Datenschutzbeauftragte und der Sächsische Landespräventionsrat die ihnen bekannten, im Bereich der Digitalen Medienbildung aktiven Institutionen im Freistaat Sachsen zur Mitarbeit in der AG Digitale Medien des Landespräventionsrates ein. Über einen Zeitraum von einem Jahr sollten gemeinsam konkrete Bedürfnisse der Bürger, Anforderungen aus Perspektive der Institutionen und bestehende Maßnahmen im Themenbereich digitaler Medien ermittelt und diskutiert werden.

Die Arbeitsgruppe verfolgte hierbei folgende Ziele:

- Erstellung einer IST-Analyse der durch die beteiligten Institutionen aktuell geleisteten Arbeiten im Handlungsfeld Prävention und digitale Medien,
- Ermittlung von Schnittstellen und möglichen Redundanzen,
- Erhebung weiterer Präventionserfordernisse in Bezug auf digitale Medien.

Die Analyse sollte aufzeigen, mit welchen Bedürfnissen und Fragen bezüglich der digitalen Medien die sächsischen Bürger an die einzelnen Institutionen herantreten und welche Aktivitäten behördlicherseits bereits angeboten und durchgeführt werden. Hierbei sollte Bedarf offengelegt werden, der derzeit noch keine oder wenig Berücksichtigung findet. Prävention soll im Hinblick auf digitale Medien im Lebensverlauf der Bürger verbindlich verankert werden. Entsprechend ist es notwendig, die Bildungspro-

zesse generationsübergreifend an dem Konzept des lebenslangen Lernens auszurichten, um eine umfassende Medienbildung zu gestalten.

Das Ergebnis der Tätigkeit der Arbeitsgruppe sind ein Bericht (http://www.lpr.sachsen.de/download/landespraeventionsrat/20170410_Bericht_final_AG_Digitale_Medien.pdf) und die vorgelegten 15 Handlungsempfehlungen, vgl. Anhang unter 17.2.1.

Die Bildung zu digitalen Medien ist eine große Herausforderung, die ein abgestimmtes und koordiniertes Handeln aller Akteure dieses Themenfeldes erfordert. Der Landespräventionsrat plant auf der Grundlage des Berichts gemeinsam mit den betroffenen Ressorts, das Ziel einer gelungenen Bildung zu digitalen Medien weiter zu verfolgen und dafür die Arbeit der derzeit temporären Arbeitsgruppe fortzuführen.

Vgl. auch 7.1 zu Datenschutz als ein Teil der Medienbildung und Digitalisierung in der Schule.

5 Inneres

5.1 Personalwesen

5.1.1 Nutzung von Zeiterfassungsdaten für Controlling-Zwecke

Ein Staatsministerium informierte mich über Pläne, zukünftig die Wirtschaftlichkeitskennzahlen mit einer speziellen Software in einem großen nachgeordneten Bereich genauer zu ermitteln. Zu diesem Zweck sollten die tatsächlichen Anwesenheitszeiten der Bediensteten der Aufgabenbereiche mithilfe einer Schnittstelle zum elektronischen Zeiterfassungs- und Zutrittskontrollsystem genutzt werden, um zusammen mit Vorgangszahlen Leistungsmessdaten zu gewinnen, die auch den Behördenleitungen zur Verfügung gestellt werden sollten.

Das Fachministerium teilte mir in diesem Zusammenhang mit, dass die anderen am Leistungsvergleich beteiligten Länderverwaltungen entsprechende Wirtschaftlichkeitskennzahlen bereits so ermitteln würden. Dies konnte in einer Umfrage durch mich nicht verifiziert werden. Im Gegenteil: Keine einzige der von mir kontaktierten Datenschutzbehörden der Länder bestätigte die Nutzung von Zeiterfassungsdaten für die vorgesehenen Controlling-Zwecke.

Der Vorgang hatte für mich grundsätzliche Bedeutung. Der Zulässigkeit der vorgesehenen Nutzung stand entgegen, dass die einschlägige Rahmendienstvereinbarung zur Nutzung des Zeiterfassungs- und Zutrittskontrollsystems die zulässigen Nutzungsmöglichkeiten der entsprechenden Daten abschließend aufzählt; eine Verwendung für Controlling-Zwecke ist davon aber nicht umfasst. Eine Erweiterung der genannten Zwecke ist nur mit Zustimmung des Hauptpersonalrats zulässig. Diese Regelungen könnten geändert und erweitert werden, wie es das Staatsministerium insofern folgerichtig bedeutete. Allerdings müsste eine Änderung der Dienstvereinbarung auch mit den gesetzlichen Bestimmungen in Einklang zu bringen sein.

Mittels Schnittstelle sollten auch sehr kleine oder einzelne Beschäftigtengruppen erfasst und weiterverarbeitet werden. Eine Zuordnung der Daten zu einzelnen Beschäftigten war aufgrund der Bezüge der Informationen und erkennbaren Organisationseinheiten nicht auszuschließen, auch wenn ansonsten pseudonyme Informationen, Daten ohne Klarnamen, ausgewertet werden sollten. Sofern Beschäftigtendaten aber nicht anonymisiert werden, ist § 37 Abs. 6 SächsDSG anwendbar, wonach Daten von Beschäftigten, die zur Verhaltens- oder Leistungskontrolle erhoben werden, nur zu diesem Zweck verarbeitet werden dürfen. Arbeitszeitdaten werden zur Verhaltenskontrolle erhoben und verarbeitet. Primärer Zweck der Verarbeitung der Arbeitszeitdaten ist neben der Sicherstellung der arbeitszeitrechtlichen Bestimmungen die Einhaltung der dienstrechtlich und arbeitsvertraglich geregelten Dienst- und Arbeitszeiten. Zwar eröffnet § 13 Abs. 3

SächsDSG, dass Daten gespeichert und genutzt werden können, wenn dies der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung, der Durchführung von Organisationsuntersuchungen, der Prüfung und Wartung von automatisierten Verfahren der Datenverarbeitung sowie statistischen Zwecken der speichernden Stelle dient. Diese Zwecke lagen nach meiner Überzeugung aber eben gerade nicht vor bzw. die zweckändernde Datenverarbeitung war nicht erforderlich oder unverhältnismäßig. Weder handelt es sich um die Wahrnehmung von Aufsichts- und Kontrollbefugnissen im Sinne der Vorschrift, noch handelt es sich insbesondere um "Organisationsuntersuchungen", die zu einem bestimmten Zeitpunkt durchgeführt und dann abgeschlossen werden, sondern um kybernetische Informationen, die aus den Beschäftigtendaten immer wiederkehrend gewonnen werden sollen. Controlling bedeutet die Gewinnung von standardisierten (betriebswirtschaftlichen) Informationen für Zwecke der Führung und einer gewissen betriebswirtschaftlichen Transparenz. Gegen das Prinzip, das im öffentlichen Verwaltungssektor wirtschaftswissenschaftlich nur bedingt trägt, ist dem Grunde nach auch nichts einzuwenden. Allerdings hat die Beschäftigtendatenverarbeitung grundsätzlich informationell abgeschottet zu erfolgen. Das gilt auch insoweit, dass das vorgesehene Verfahren mit seiner Schnittstelle, die originär eben nur zu Verhaltens- und nicht zur Leistungskontrolle verarbeiteten Arbeitszeitdaten mit weiteren Informationen verbinden soll, die dazu dienen, Leistungsmesszahlen zu gewinnen, die nicht nur sehr granular sein sollen, sondern auch einzelne Beschäftigte zu betreffen geeignet sind. Ein so weitgehendes Controlling ist nach meiner Überzeugung nicht erforderlich, um den vorgeblichen Zweck zu erreichen. Unabhängig von dem Controlling ist es der Personalverwaltung eröffnet, notwendige personelle Entscheidungen in Bezug auf personelle Ressourcen, Fehlzeiten und Erledigungen zu treffen. Inwieweit die Erweiterung des Verfahrens den betreffenden Verwaltungsbereich unmittelbar produktiv ertüchtigt, ist nach den mir vorgelegten Unterlagen nicht dargetan worden und zwingend.

Ich habe mich daher nur mit der Nutzung von aus den Arbeitszeitdaten gewonnenen statistischen und anonymen Informationen für das Verfahren einverstanden erklärt. Kleinere Organisationseinheiten betreffende Arbeitszeitinformationen müssten hochgerechnet werden, um keine Rückschlüsse auf einzelne Bedienstete zuzulassen. Entsprechendes teilte ich dem Hauptpersonalrat auf Anfrage mit.

5.1.2 Abgleich der IBAN von Bediensteten zum Zwecke der Korruptionsprävention

Im Berichtszeitraum wurde ich von einem Landkreis gebeten, zu prüfen, ob und inwieweit ein Abgleich der dem Personalreferat aus den Gehaltsabrechnungen bekannten IBAN (International Bank Account Number) der Landkreisbediensteten mit den IBAN

von Sozialleistungsdaten des angegliederten „Jobcenters“ rechtmäßig wäre. Hintergrund war, dass bekannt geworden war, dass ein Landkreisbediensteter neben seinem Arbeitsentgelt auch ihm nicht zustehende Sozialleistungen nach SGB II bezog, also ein Fall des Sozialleistungsmissbrauchs.

Den Abgleich sollte das Rechnungsprüfungsamt des Landkreises im Auftrag (§ 7 SächsDSG) des Personalreferats durchführen. Dadurch erhoffte sich die Landkreisverwaltung, etwaige weitere Missbrauchsfälle aufdecken zu können. Konkrete Anhaltspunkte für weitere Missbrauchsfälle lagen nicht vor. Im Falle eines Treffers, also einer Doppelung, sollten weitere Ermittlungen angestellt werden, um festzustellen, ob der betreffende Landkreisbedienstete tatsächlich unrechtmäßig Zahlungen nach SGB II erhält. Rechtsgrundlage sollte § 106 Abs. 2 Nr. 2 SächsGemO (Prüfung der Vergaben vor dem Abschluss von Lieferungs- und Leistungsverträgen) sein, wonach u. a. auch die vorbeugende Korruptionsprävention zu den Aufgaben der örtlichen Rechnungsprüfung zählen kann.

Ich habe den Landkreis in dieser Angelegenheit, in der es um den Schutz von Beschäftigtendaten im öffentlichen Dienst gemäß § 37 SächsDSG ging, wie folgt beraten: Die IBAN ist ein personenbezogenes Datum i. S. v. § 3 Abs. 1 SächsDSG, denn durch sie kann, wenn der Kontoinhaber eine natürliche Person ist, diese eindeutig identifiziert werden. Zweifelhaft erscheint mir jedoch bereits, ob es sich bei dem beabsichtigten Datenabgleich überhaupt um eine Maßnahme der vorbeugenden Korruptionsbekämpfung (und nicht um Ermittlungen „ins Blaue“ hinein) handelt und mithin § 106 Abs. 2 Nr. 2 SächsGemO eine taugliche Rechtsgrundlage für diese Verarbeitung personenbezogener Daten (Vorbehalt des Gesetzes) sein kann. Im Ergebnis kann dies aber offengelassen werden, da jedenfalls das Personalreferat nicht befugt ist, Beschäftigtendaten i. S. v. § 37 SächsDSG zu anderen Zwecken als der „Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen“ oder dann zu verarbeiten, wenn ein „Gesetz, ein Tarifvertrag oder eine Dienstvereinbarung“ dies vorsieht, § 37 Abs. 1 SächsDSG (sogenannte enge Zweckbindung des Beschäftigtendatenschutzes). Auch die Voraussetzungen von § 37 Abs. 3 SächsDSG, wonach eine Übermittlung von Beschäftigtendaten nur zulässig ist, wenn eine Rechtsvorschrift dies vorsieht oder der Betroffene eingewilligt hat oder die Voraussetzungen einer Veröffentlichung vorliegen, sind nicht gegeben. Diesen strengen Vorgaben zum Beschäftigtendatenschutz kann sich der Landkreis auch nicht dadurch entziehen, indem er sich die Befugnis einer funktional anderen Stelle, hier des Rechnungsprüfungsamts, im Wege der Auftragsdatenverarbeitung quasi aneignet. Eine solche Aufweichung der Zweckbindung des § 37 SächsDSG und der Zuständigkeitsregelungen dürfte nur der Gesetzgeber vornehmen.

Der Landkreis hat daraufhin von seinem Vorhaben Abstand genommen.

5.1.3 Videodatenverarbeitung in Bewerbungsverfahren und im Beschäftigungsverhältnis

Neue Medientechnik erlaubt Kommunikation und Datenverarbeitungswege, die für den öffentlichen Verwaltungssektor neuartig ist. Z. T. wird nach meiner Kenntnis, im nichtöffentlichen Bereich, aber auch im Bereich öffentlicher Hochschulen Videotechnik eingesetzt, um Abschnitte des Bewerbungsverfahrens, wie z. B. (Vor-)Auswahlgespräche durchzuführen. Verbreitet ist hierbei u. a. der Microsoft-Dienst „Skype“.

Bei einer Video-Kommunikation handelt es sich nach meiner Überzeugung um eine automatisierte Datenverarbeitung gemäß § 3 Abs. 5 SächsDSG. Auch IP-gestützte Kommunikation von personenbezogenen Daten fällt hierunter und eingesetzte Verfahren wie Skype sind als elektronische programmgesteuerte Datenverarbeitungssysteme, unabhängig vom Inhalt, automatisierte Verfahren. Verantwortliche Stelle ist nach § 3 Abs. 3 SächsDSG die Stelle, die die Bewerbungsgespräche mit dem Verfahren durchführt.

Das Führen von Bewerbungsgesprächen über derartige Anbieterpräsenzen würde zudem ein Verfahren darstellen, das nach § 10 Abs. 4 Nr. 3 SächsDSG der Vorabkontrolle durch den Datenschutzbeauftragten unterliegt. Danach ist eine Vorabkontrolle erforderlich, wenn die Verarbeitung von Beschäftigtendaten durchgeführt wird. Bewerberinformationen sind auch Beschäftigtendaten, vgl. den Wortlaut von § 37 Abs. 1 SächsDSG.

Es handelt sich auch um neue Technologien, die, sofern Personaldaten offenbart werden, besondere Risiken im Hinblick auf die betroffenen Bewerber bergen. Zum einen handelt es sich um Peer to Peer-Kommunikationstechnik, die informationssicherheitstechnisch zu untersuchen sein wird. Zum anderen speichern Anbieter wie Skype ggf. gemäß ihren Nutzungsbedingungen Inhalte der Gespräche auf zentralen Serveranlagen, zumindest kurzzeitig. Soweit Anbieter für sich in Anspruch nehmen Inhalte zu speichern, zu übertragen, zu kopieren oder weiter zu verteilen, ist im Hinblick auf das Risiko in Bezug auf Beschäftigtendaten und die Vertraulichkeit des Bewerbungsgespräches die Zulässigkeit eines Einsatzes in Frage zu stellen.

Der Dienstherr bzw. Arbeitgeber ist gemäß § 37 SächsDSG zur Erhebung und Verarbeitung personenbezogener Daten der Bewerber befugt. Eine Berechtigung von Anbietern wie Skype, selbst Daten gleichzeitig zu verarbeiten, ergibt sich aus der Zustimmung der Nutzer zu den Nutzungsbedingungen der Dienste. Falls Bewerber von potentiellen Dienstherrn und Arbeitgebern veranlasst werden, Nutzungsbedingungen zuzustimmen, wenn sie die entsprechende Beschäftigung haben möchten, und kein alternatives Bewer-

bungsgespräch angeboten wird, ist fraglich, ob von einer Freiwilligkeit der Einwilligung in das Videotelefonat im Verhältnis zum potentiellen Dienstherrn und Arbeitgeber sowie zum Anbieter ausgegangen werden kann.

Im letzten Tätigkeitsbericht war ich bereits auf Videografie im Beschäftigungsverhältnis eingegangen und hatte auch in Bezug auf den Abschluss von Dienstvereinbarungen Empfehlungen ausgesprochen, vgl. auch 17/5.1.5. Dienstvereinbarungen bieten wegen ihrer normativen Wirkung den Vorteil, dass sich damit das Problem der Freiwilligkeit bei ansonsten einzuholenden Einwilligungen, nicht stellt. Die Freiwilligkeit wird man im Beschäftigungsverhältnis bei derartigen eingreifenden Maßnahmen seitens des Arbeitgebers und Dienstherrn als eingeschränkt ansehen müssen. Allerdings entscheiden auch immer wieder Gerichte dahingehend, dass sie eine entsprechende Einwilligung für zulässig halten. In einer aktuelleren Entscheidung aus dem letzten Berichtszeitraum entschied das Verwaltungsgericht Saarlouis (VG vom 29. Januar 2016 – Az. 1 K 1122/14) in Sachen Videoüberwachung in einer Apotheke. Das Gericht hat die Einwilligungserklärungen der Beschäftigten in eine Videoüberwachung der Arbeitsplätze für zulässig und wirksam gehalten.

5.1.4 Weitergehende Nutzung von Beschäftigten- und Studentendaten

Ein Betroffener wies mich darauf hin, dass die Leitung einer großen sächsischen Hochschuleinrichtung Beschäftigte und Studenten der Hochschule über deren dienstliche E-Mail-Adresse zur Teilnahme an bestimmten, ausgewählten allgemeinpolitischen, aber nicht hochschulbezogenen Veranstaltungen aufrufen würde. Verwiesen wurde seitens eines Betroffenen unter anderem auf eine letzte Mail-Aussendung an Bedienstete und Studenten, mit der auf Veranstaltungen im Oktober 2016 hingewiesen wurde. Der genaue Wortlaut der Mail wurde mir zugeleitet.

Gemäß § 37 SächsDSG dürfen Daten von Beschäftigten nur verarbeitet werden, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder ein Gesetz, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht. Auch die E-Mail-Adressdaten der Studenten sind zu universitären Zwecken eingerichtet.

Nachdem es sich auch bei dienstlichen E-Mail-Adressen zwar nur um eingeschränkt schutzwürdige Daten, aber auch um Beschäftigtendaten handelt und zudem zusätzlich Studenten betroffen waren, bat ich um Stellungnahme zum Sachverhalt und wie die

Nutzung der E-Mail-Adressen zu dem streitigen Zweck dienstlich gerechtfertigt sein sollte.

Die Hochschule äußerte sich nach mehreren Monaten dahingehend, dass der Rektor lediglich „eine sachliche Information über eine Veranstaltung“ versandt habe, aber eine Verpflichtung zur Teilnahme bzw. eine Werbung nicht erfolgt sei. Die Aussendung habe im Wesentlichen dem Aufruf an die Beschäftigten und Studenten gedient, „sich ihrer Rolle als Individuen in einer demokratischen Gesellschaft bewusst zu werden“. Zudem habe die Zielrichtung der Veranstaltung einen überparteilichen Charakter gehabt. Man sehe die Information des Rektors über die Veranstaltung von dessen Befugnissen als „Leiter einer staatlichen international zusammengesetzten und orientierten Wissenschaftseinrichtung gedeckt“. Einen Teilnahmedruck habe man nicht erzeugen wollen. Das Schreiben schloss mit der Bemerkung, dass „es sich um die zunächst letzte Mail dieser Art, die über diese Kommunikationskanäle an die Beschäftigten und Studierenden versendet wurde“ gehandelt habe.

Die Veranstaltung, auf die der Rektor zuletzt hinwies, bezog sich auf eine zeitaktuelle gesellschaftspolitische Thematik, die allgemein streitig diskutiert wird. Unterstützt wurde sie von zahlreichen Vereinen und Parteien, die sich wiederum politisch gegen konkrete gegensätzlich positionierte Parteien bzw. Zusammenschlüsse wandten. Auch wurde das Angebot eines „Sammelpunkts“ im Universitätsbereich zum gemeinsamen Gang in die Innenstadt gemacht. Insoweit konnte die Hochschule nach meiner Überzeugung die in sie geweckten Zweifel an einer Einhaltung der Neutralitätspflicht, verbunden mit der Ausnutzung der Hochschulressourcen und einer zweckwidrigen Verwendung der dienstlichen und studentischen E-Mail-Adressen nicht entkräften.

In mehreren gerichtlichen Entscheidungen sind in letzter Zeit ähnliche Fälle behandelt worden (BVerfG, Urteil vom 16. Dezember 2014 – 2 BvE 2/14, BVerfG, Beschluss vom 7. November 2015 – 2 BvQ 39/15, OVG Münster, Urteil vom 4. November 2016 – 15 A 2293/15, BVerwG, Urteil vom 13. September 2017 – 10 C 6.16). Das Oberverwaltungsgericht schreibt in seiner Entscheidung: „Soweit ein Amtsinhaber am politischen Meinungskampf zwischen den politischen Parteien teilnimmt, muss zur Wahrung der Chancengleichheit dieser Parteien sichergestellt sein, dass ein Rückgriff auf die mit dem Amt verbundenen Mittel und Möglichkeiten unterbleibt. Nimmt der Amtsinhaber für sein Handeln die Autorität des Amtes oder die damit verbundenen Ressourcen in spezifischer Weise in Anspruch, ist es im Verhältnis zu den politischen Parteien dem Neutralitätsgebot unterworfen. … Amtsautorität wird dabei in Anspruch genommen, wenn der Amtsinhaber sich durch amtliche Verlautbarungen etwa in Form offizieller Publikationen, Pressemitteilungen oder auf offiziellen Internetseiten seines

Geschäftsbereichs erklärt. … Dass der Amtsinhaber außerhalb seiner amtlichen Funktionen am politischen Meinungskampf teilnimmt und in den Wahlkampf eingreift, ist dagegen nicht ausgeschlossen. Ob die Äußerung unter spezifischer Inanspruchnahme der Autorität des Regierungsamtes oder der mit ihm verbundenen Ressourcen stattgefunden hat, ist nach den Umständen des jeweiligen Einzelfalles zu bestimmen."

Auch ein Amtsträger hat das Recht, für ein ihm wichtiges Anliegen einzutreten, aber er hat auch die sich aus seinem Amt ergebenden Schranken zu beachten.

5.2 Personalvertretung

5.2.1 Online-Wahl zur Personalvertretung

Vertreter einer sächsischen öffentlichen Stelle mit einer sehr hohen Beschäftigtenanzahl traten mit meiner Behörde wegen Wahlen zum Gesamtpersonalrat und von örtlichen Personalräten in Kontakt. Die Wahlvorstände verfolgten die Überlegung, die Wahlen online über eine Firma durchzuführen. Die Wählerverzeichnisse sollten zu diesem Zweck an die Firma übermittelt werden. Per E-Mail sollte der für die Beauftragung vorgesehene Dienstleister individuelle Internetverknüpfungen an die Wahlberechtigten versenden, die auf diese Weise dann hätten online abstimmen können. Die Firma hätte in der Folge automatisiert das Wahlergebnis ermittelt. Nach Angaben des Unternehmens sei sichergestellt gewesen, dass die Wahl geheim geblieben wäre und technisch keine Verbindung zwischen dem Wähler und seiner Wahlentscheidung zugänglich gemacht worden wäre. Das Unternehmen reklamierte für sich, vom BSI zertifiziert worden zu sein. Mit dem Verfahren wäre die Datenverarbeitung des Wahlverfahrens an eine externe Stelle ausgelagert worden und neben der datenschutzrechtlichen Problematik der Übermittlung der personenbezogenen Daten der Wahlberechtigten und der Datenverarbeitung des Wahlvorgangs selbst, hätte die Schwierigkeit bestanden, wie bei dem vorgesehenen Verfahren ein revisionsfähiges transparentes Wahlverfahren hätte sichergestellt werden können.

In der Folge trat ich sodann an die für Personalvertretungsrecht zuständige Aufsichtsbehörde heran, was ich auch dem behördlichen Datenschutzbeauftragten der Stelle so anempfahl.

Die Behörde teilte der öffentlichen Stelle den aktuellen Verfahrensstand einer vorgesehenen Änderung der Sächsischen Personalvertretungswahlverordnung mit und dass es keine Rechtsgrundlage für die Durchführung von Online-Personalratswahlen gebe. Ergänzend wies die Behörde darauf hin, dass eine Online-Wahl nicht nur anfechtbar, sondern von den Verwaltungsgerichten möglicherweise darüber hinaus als nichtig angesehen werden könnte. Die Rechtsprechung sei nämlich dann ausnahmsweise von einer

Nichtigkeit ausgegangen, wenn in so hohem Maß gegen allgemeine Grundsätze jeder ordnungsgemäßen Wahl verstoßen worden war, dass selbst der Anschein einer ordnungsgemäßen Wahl nicht mehr vorliegt. Eine Nichtigkeit der Wahl mit der Folge, dass ein Personalrat nie bestanden habe, könnte ggf. von jedem Beschäftigten und jederzeit geltend gemacht werden

Danach nahmen die zuständigen Wahlvorstände der öffentlichen Stelle von der Umsetzung des Verfahrens Abstand.

5.3 Einwohnermeldewesen

5.3.1 Veröffentlichung von Alters- und Ehejubiläen in kommunalen Amtsblättern

Es ist in vielen Gemeinden üblich, dass Bürgermeister bzw. deren Vertreter ältere Menschen zu ihren Ehrentagen aufsuchen, um diesen ihre Glückwünsche persönlich zu überbringen. Die Mandatare schätzen die Möglichkeiten ihres Amts zur Kontaktpflege zur Wählerschaft. Zusätzlich werden Informationen zu Alters- und Ehejubilaren über die amtlichen Blätter der Gemeinden verbreitet.

Jedoch erreichten mich im letzten Berichtszeitraum wieder verstärkt Anfragen und Beschwerden von Betroffenen, die mit einer Veröffentlichung ihrer Daten nicht einverstanden waren und nachfragten, ob das Handeln der Gemeinde datenschutzrechtlich ordnungsgemäß sei. Hintergrund des Ganzen sind maßgebliche Änderungen des Melderechts.

Auf meine Nachfragen hin teilten mir die Gemeinden häufig mit, dass die Betroffenen, deren Namen und Geburtstage und Hochzeitstage als Altersjubilare und Ehejubilare verbreitet würden, selbst großen Wert auf die persönliche Gratulation und die Veröffentlichung im Gemeindeblatt legten, da diese als eine Anerkennung und Ehrung empfunden werde. Die Enttäuschung der Jubilare sei dagegen groß, wenn Veröffentlichungen unterblieben. Das mag tatsächlich die Sicht einiger Menschen sein, aber nicht wenige Betroffene sehen das wiederum anders und allein entscheidend ist letztendlich die Gesetzeslage.

Nach altem Recht waren die Meldebehörden gemäß § 33 Abs. 2 Sächsisches Meldegesetz tatsächlich zum einen befugt, Namen, Doktorgrad, Anschriften, Tag und Art des Jubiläums von Alters- und Ehejubiläen intern weiterzugeben und selbst zu veröffentlichen, aber auch an Presse, Rundfunk oder andere Medien „zum Zwecke der Veröffentlichung“ zu übermitteln. Altersjubilare waren Einwohner, die den 70. oder einen spä-

teren Geburtstag hatten, Ehejubilare Einwohner, die die goldene Hochzeit oder ein späteres Ehejubiläum begingen.

Mit Inkrafttreten der im November 2015 die vorgenannte Vorschrift ablösenden Bestimmung des § 50 BMG darf die Meldebehörde gemäß Absatz 2 auf Verlangen von Mandatsträgern und von Presse oder Rundfunk Auskunft aus dem Melderegister über Alters- oder Ehejubiläen von Einwohnern erteilen, es sei denn, diese haben von ihrem Widerspruchsrecht gegen diese Übermittlung gemäß § 50 Abs. 5 BMG Gebrauch gemacht. Die Befugnis zur Datenweitergabe umfasst Familienname, Vorname, Doktorgrad, Anschrift sowie Datum und Art des Jubiläums. Als Altersjubiläen, zu denen Informationen übermittelt werden dürfen, gelten nach neuem Recht nur noch der 70. Geburtstag und jeder fünfte darauffolgende Geburtstag sowie ab dem 100. Geburtstag jeder jährliche Geburtstag. Als Ehejubiläen gelten nach neuem Recht das 50. und jedes danach folgende Ehejubiläum.

So kann man festhalten, dass die Melderegisterdaten zu Alters- und Ehejubiläen an die Bürgermeister für eine persönliche Gratulation der Jubilare unter Beachtung der Einschränkungen nach § 50 Abs. 2 BMG weiterzugeben, zulässig ist. Möchte der Bürgermeister den Einwohnern zu weiteren Jubiläen, als den in § 50 Abs. 2 BMG abschließend genannten, gratulieren, könnten die notwendigen Daten durch die Meldebehörde auf Grundlage von § 37 Abs. 1 BMG übermittelt werden, soweit man gewisse Eigenpräsentationszwecke des Bürgermeisters als von den gemeindlichen Aufgaben umfasst ansieht. Das betrifft allerdings nur den Bürgermeister und dessen Verwaltung selbst.

Die gesetzliche Regelung des § 50 Abs. 2 BMG regelt im Unterschied zu der alten Regelung nach dem Sächsischen Meldegesetzes lediglich die Weitergabe- bzw. Übermittlung an die erlaubten Empfänger. Chronologisch nachfolgende Datenverarbeitungsphasen durch diese Stellen werden von der Regelung des Bundesmeldegesetzes hingegen gar nicht erfasst, hat der Bund doch auch keine Gesetzgebungsbefugnis für die Datenverarbeitung sächsischer Gemeinden bzw. richtet sich die Datenverarbeitung anderer Stellen nach dem Bundesdatenschutzgesetz. Das bedeutet auch, dass die empfangenden Stellen sich bei Veröffentlichungen der Jubiläumsdaten auf gesonderte bereichsspezifische Vorschriften stützen müssten. Der Verweis auf § 50 Abs. 2 BMG, den Empfang der Daten, genügt nicht. Weder werden Presse- noch Medienunternehmen ohne ausdrückliche Einwilligung Betroffener entsprechende Veröffentlichungen vorzunehmen befugt sein, noch ermächtigt die Sächsische Gemeindeordnung den Bürgermeister oder die Gemeinde selbst, die behördenintern weitergegebenen Melderegisterdaten als Jubiläumsdaten im Amtsblatt zu veröffentlichen.

Mir mitgeteilte Beschwerden zu einer gegenteiligen Praxis (weiterhin) veröffentlichender Gemeinden sind meinerseits als begründet zu betrachten gewesen.

Keine Einwände gegen eine Veröffentlichung von Jubiläumsdaten als Interesse und Angelegenheit der örtlichen Gemeinschaft bestehen nur insoweit, als Jubilare selbst den Gemeinden *schriftlich* gegenüber per Einwilligung erklären, dass sie (weiterhin) eine Veröffentlichung ihrer Ehrentage im Gemeindeblatt wünschen. Hierfür könnten die Gemeinden auch ein Formblatt vorhalten, welches in den örtlichen Amtsblättern verbreitet wird. Für die Einwilligungserklärung sind die Verfahrens- und Formvorschriften des § 4 Abs. 3 bis 5 SächsDSG einzuhalten.

Die betroffenen Personen, die keine Gratulation durch den Bürgermeister bzw. eine Veröffentlichung ihrer Jubiläumsdaten wünschen, haben das Recht, der Weitergabe ihrer Daten gemäß § 50 Abs. 2 BMG zu widersprechen. Die Praxis zeigt immer wieder, dass den Betroffenen ihr Widerspruchsrecht gemäß § 50 Abs. 5 BMG nicht bekannt ist. Hervorzuheben ist daher, dass die Meldebehörde verpflichtet ist, Betroffene auf das bestehende Widerspruchsrecht bei der Anmeldung nach § 17 Abs. 1 BMG sowie mindestens einmal jährlich durch ortsübliche Bekanntmachung hinzuweisen. Auf Anfragen hin versicherten mir jedenfalls die entsprechenden Kommunen, dass diese jährliche Bekanntmachung im örtlichen Gemeindeblatt auch durchgeführt werde.

5.3.2 Einführung eines elektronischen Systems für die Erhebung der Fremdenverkehrs- und Kurbeiträge

Im letzten Berichtszeitraum wandten sich Petenten und Tourismusvereine an meine Behörde. Gegenstand war die geplante Einführung eines gemeindeübergreifenden elektronischen Meldesystems für die Erhebung der Kurtaxe und die Ausgabe einer regionalen Gästekarte in verschiedenen sächsischen Regionen.

Hierzu wurde das Verfahren zur Abrechnung der Gästeabgabe bzw. Kurtaxe verändert – eine elektronische Lösung sollte das handschriftliche Ausfüllen von Meldescheinen zukünftig überflüssig machen und so nicht nur die Verfahren zur Meldung und Abrechnung zwischen Beherbergungsstätten und Kommunalverwaltungen optimieren, sondern gleichzeitig auch Nutzungsmöglichkeiten für das Tourismusmarketing eröffnen.

In den mir vorliegenden Stellungnahmen von zwei beteiligten Tourismusverbänden wurde mir mitgeteilt, dass diese im Rahmen der jeweils regionalen Einführungsprojekte lediglich eine koordinierende Funktion eingenommen hätten. Ziel sei es gewesen, die Vereinheitlichung der von den Orten ausgegebenen Kur- und Gästekarten zu einer gemeinsamen regionalen Gästekarte herbeizuführen.

Über das einzuführende elektronische System sollte das Verfahren zur Meldung und Abrechnung der Fremdenverkehrs- und Kurbeiträge durchgeführt werden. Laut der technischen Beschreibung wurden die Daten des Gastes in einer Erfassungsmaske im System durch den Beherberger elektronisch erfasst. Nach dem Ausdruck des elektronischen Meldescheins und dessen handschriftlicher Unterzeichnung durch den Gast erhalte dieser eine Gästekarte. Die Gästekarte sei zum einen die Quittung für den bezahlten Fremdenverkehrs- und Kurbeitrag und zum anderen habe sie eine Ausweisfunktion für kostenlose Eintritte oder ermäßigte Leistungen als Gegenleistung für die bezahlte Gebühr. Die durch den Beherberger elektronisch erfassten Personendaten des Gastes würden in einem System gespeichert und der Kommunalverwaltung zur Rechnungsstellung der Kurtaxe gegenüber dem Beherbergungsbetrieb zur Verfügung gestellt. Eine zusätzliche Speicherung der Daten durch den Beherberger erfolge nicht. Nur ein Ausdruck des Meldescheins verbliebe beim Beherberger für dessen eigene Unterlagen. Gäste würden auf dem ausgedruckten Meldeschein auf die elektronische Speicherung und Verarbeitung der Daten hingewiesen.

In Beherbergungsstätten gilt eine besondere Meldepflicht. Gemäß § 29 Abs. 2 BMG hat die beherbergte Person am Tag der Ankunft einen besonderen Meldeschein handschriftlich zu unterschreiben, der die in § 30 Abs. 2 BMG aufgeführten Daten enthält. Diese Daten sind das Datum der Ankunft und der voraussichtlichen Abreise, Familiennamen, Vornamen, Geburtsdatum, Staatsangehörigkeiten, Anschrift, Zahl der Mitreisenden und ihre Staatsangehörigkeit, Seriennummer des anerkannten und gültigen Passes oder Passersatzpapiers bei ausländischen Personen.

Gemäß § 30 Abs. 3 BMG kann durch Landesrecht bestimmt werden, dass für die Erhebung von Fremdenverkehrs- und Kurbeiträgen weitere Daten auf dem Meldeschein erhoben werden.

Mit § 10 SächsAGBMG hat der Freistaat Sachsen von dieser Möglichkeit Gebrauch gemacht. Hiernach können Gemeinden durch Satzung zusätzlich zu den in § 30 Abs. 2 BMG genannten Daten weitere, für die Erhebung der Kurtaxe nach § 34 SächsKAG erforderliche Daten auf dem Meldeschein erheben. Für Gemeinden, die dem Anwendungsbereich der *Verordnung des Sächsischen Staatsministeriums der Finanzen über die Erhebung der Kurtaxe in den sächsischen Staatsbädern* (Kurtaxordnung) unterfallen, kann das SMF die entsprechenden Daten durch Rechtsverordnung bestimmen. Die Verwendung von Meldescheinen, die die Muster des nach § 11 Nr. 1 SächsAGBMG zu bestimmenden Meldescheins entsprechend ergänzen, ist in den betreffenden Gemeinden zulässig.

Ich stehe auf dem Standpunkt, dass das Verfahren in § 30 BMG und in § 10 SächsAGBMG abschließend geregelt ist. Die Verwendung der Meldescheine und das Meldeverfahren sind dort gesetzlich vorgeschrieben und müssen unverändert vollständig eingehalten werden.

Allerdings hat das SMI nach mir erteilter Auskunft eben gerade darauf verzichtet, Vordrucke für besondere Meldescheine vorzusehen, dies um automatisierte Verfahren in der oben dargestellten Weise formfrei zu lassen und so zu ermöglichen.

Bei gegenwärtigem Rechtsstand in Sachsen sind lediglich die nach dem Bundesmeldegesetz vorgesehenen Daten (§ 30 Abs. 2 BMG) in irgendeiner Weise zu erheben. Formularfestlegungen kann die Gemeinde, um eine einheitliche Datenverarbeitung sicherzustellen, selbst vornehmen. Damit wäre die Gemeinde bei gegenwärtigen Rechtsstand auch dazu befugt, in der vorgesehenen Weise zu verfahren, ohne gegen Melderecht zu verstoßen.

Nach den mir zugegangenen Informationen nutzen die Gemeinden zur Erfassung der Daten gemäß § 29 Abs. 2 i. V. m. § 30 Abs. 2 BMG das elektronische System eines Anbieters. Die jeweiligen Verträge zur Auftragsdatenverarbeitung würden zwischen dem Auftragnehmer und der jeweiligen Gemeinde geschlossen. Jede Gemeinde werde als Mandant in einem nur für sie zugänglichen System angelegt und erhielte auf die elektronischen Meldesysteme der weiteren beteiligten Gemeinden, die sich an der Einführung einer regionalen Gästekarte beteiligen, keinen Zugriff. Auch hätten weder die Tourismusverbände noch die sich beteiligten Gewerbetreibenden Einsichts- bzw. Zugriffsrechte auf das von den Gemeinden genutzte elektronische Verfahren.

Gemäß § 7 Abs. 1 SächsDSG kann eine öffentliche Stelle, soweit gesetzlich nichts anderes bestimmt ist, einen anderen mit der Verarbeitung personenbezogener Daten beauftragen (Datenverarbeitung im Auftrag). Für die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz ist der Auftraggeber verantwortlich, d. h. die jeweilige Gemeinde.

Der Auftraggeber hat den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen personellen, technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei Gegenstand und Umfang der Datenverarbeitung, die notwendigen zusätzlichen personellen, technischen und organisatorischen Maßnahmen sowie etwaige Unterauftragsverhältnisse festzulegen sind. Der Auftraggeber ist verpflichtet, sich von der Einhaltung der getroffenen Festlegungen beim Auftragnehmer zu überzeugen. Der Auftraggeber hat dem

Auftragnehmer die erforderlichen Weisungen zu erteilen. Die Datenverarbeitung ist nur im Rahmen des Auftrags und der Weisungen zulässig (§ 7 Abs. 2 SächsDSG).

Ich werde kontrollieren, wie die Vorschriften und die festgelegten Maßnahmen im laufenden Praxisbetrieb umgesetzt werden.

Auch habe ich darauf hingewiesen, dass die Regelungen für ein elektronisches Meldeverfahren in die jeweilige Kurtaxensatzung der beteiligten Gemeinden aufzunehmen sind. Ich empfahl, ein Meldescheinmuster für das automatisierte Verfahren und ein empfohlenes Muster für die herkömmliche Erfassung der Meldedaten durch den Beherberger der Satzung als Anlage beizufügen.

5.3.3 Mitwirkungspflicht des Wohnungsgebers

Zuweilen besteht bei Wohnungsgebern Unklarheit darüber, welche Mitwirkungspflichten sie bei der An- oder Abmeldung ihrer Mieter gegenüber dem Einwohnermeldeamt haben.

Seit dem 1. November 2015 sind Wohnungsgeber nach § 19 BMG verpflichtet, den Mietern den Einzug oder Auszug schriftlich oder elektronisch zu bestätigen.

Mit der *Allgemeinen Verwaltungsvorschrift zur Durchführung des Bundesmeldegesetzes* (BMGVwV) konkretisiert der Gesetzgeber die unbestimmten Rechtsbegriffe des § 19 BMG. Hiernach ist Wohnungsgeber, wer einem anderen eine Wohnung tatsächlich zur Benutzung überlässt, unabhängig davon, ob dem ein wirksames Rechtsverhältnis zugrunde liegt. Wohnungsgeber ist zum Beispiel der Eigentümer oder Nießbraucher, der die Wohnung vermietet, oder die vom Eigentümer mit der Vermietung der Wohnung beauftragte Person oder Stelle. Wohnt eine Person zur Untermiete, ist für diese der Hauptmieter Wohnungsgeber.

Der Wohnungsgeber oder eine von ihm beauftragte Person hat nach dem Einzug oder Auszug der meldepflichtigen Person schriftlich mit Unterschrift oder gegenüber der Meldebehörde nach § 19 Abs. 4 BMG elektronisch innerhalb der in § 17 Abs. 1 oder 2 BMG genannten Fristen zu bestätigen.

Nach § 19 Abs. 3 BMG soll die Bestätigung des Wohnungsgebers als Daten Name und Anschrift des Wohnungseigners, Art des meldepflichtigen Vorgangs mit Einzugs- oder Auszugsdatum, Anschrift der Wohnung sowie Namen der meldepflichtigen Personen enthalten.

In Anlage 2 BMGVwV ist eine Wohnungsgeberbestätigung als Muster dargestellt. Entsprechend dieser Anlage werden die in § 19 Abs. 3 BMG genannten Daten konkretisiert. So meint der Gesetzgeber mit Name den jeweiligen Vor- und Familiennamen. Und Zusatzangaben zur Wohnung, z. B. Stockwerks- oder Wohnungsnummer, sind anzugeben.

Unabhängig von der Pflicht des Vermieters bleiben Mieter weiterhin verpflichtet, sich bei einem Wohnungswechsel innerhalb von zwei Wochen bei der zuständigen Meldebehörde anzumelden, § 17 Abs. 1 BMG.

Der Wohnungsgeber ist berechtigt von der Meldebehörde Informationen zu beziehen, ob sich sein Mieter an- bzw. abgemeldet hat. Die Meldebehörde wiederum ist befugt, Informationen über aktuelle oder vorherige Mieter beim Vermieter nachzufragen.

5.3.4 Weitergabe der neuen Wohnanschrift vom Vorvermieter an die Meldebehörde

Ein Betroffener wandte sich an mich und bat um datenschutzrechtliche Prüfung der Rechtmäßigkeit der Weitergabe der neuen Wohnanschrift vom Vormieter an die Meldebehörde.

Der Betroffene teilte mir mit, dass er umgezogen sei. Eine Abmeldung am alten Wohnort habe er nicht vorgenommen, jedoch räumte er ein, dass die Anmeldung am neuen Wohnort etwas verspätet erfolgt sei.

Von der Meldebehörde des alten Wohnortes habe er sodann einen Brief erhalten, in dem ihm die fehlende Abmeldung vorgeworfen und Bußgeld angedroht worden sei. Auf telefonische Nachfrage bei der Meldebehörde habe man ihm mitgeteilt, dass ein Brief der Kommune an seine alte Wohnanschrift nicht zugestellt werden konnte. Daraufhin habe die Meldebehörde den ehemaligen Vermieter kontaktiert und von diesem das Auszugsdatum und die neue Wohnanschrift des Betroffenen erfahren. Nach Ansicht des Betroffenen könne jedoch nur der Vermieter bei der Meldebehörde Informationen zu seinen Mietern erfragen und nicht umgekehrt.

Wer eine Wohnung bezieht, hat sich gemäß § 17 Abs. 1 BMG innerhalb von zwei Wochen nach dem Einzug bei der zuständigen Meldebehörde anzumelden. Eine separate Abmeldung für den Auszug ist in diesem Fall nicht notwendig. Jedoch muss sich derjenige, der aus einer Wohnung auszieht und keine neue Wohnung im Inland bezieht, innerhalb von zwei Wochen nach dem Auszug bei der zuständigen Meldebehörde gemäß § 17 Abs. 2 BMG abmelden. Kommt der Meldepflichtige seiner Meldepflicht

innerhalb dieser Zweiwochenfrist nicht nach, so begeht er eine Ordnungswidrigkeit nach § 54 Abs. 2 Nr. 1 BMG.

Da die Meldebehörde des alten Wohnortes Kenntnis vom Auszug des Betroffenen erhalten hatte und nach der genannten Zwei-Wochen-Frist weder eine Anmeldung vom Bezug einer neuen Wohnung durch die Meldebehörde des neuen Wohnortes erhielt, noch eine Abmeldung durch den Betroffenen selbst erfolgte, ging die Meldebehörde von einer Ordnungswidrigkeit nach § 54 Abs. 2 Nr. 1 BMG aus. Da der entsprechende Schriftverkehr nicht zugestellt werden konnte, nahm die Meldebehörde des alten Wohnortes Kontakt mit dem Vorvermieter (Wohnungsgeber) auf.

§ 19 BMG regelt die Mitwirkungspflichten des Wohnungsgebers (Vermieters) bei An- und Abmeldungen. Hiernach kann sich der Wohnungsgeber (Vermieter) durch Rückfrage bei der zuständigen Meldebehörde davon überzeugen, dass sich die meldepflichtige Person an- oder abgemeldet hat (§ 19 Abs. 1 Satz 3 BMG). Gemäß § 19 Abs. 5 BMG kann auch die zuständige Meldebehörde vom Wohnungsgeber Auskunft über Personen verlangen, welche bei ihm wohnen oder gewohnt haben. Die Auskunftspflicht des Wohnungsgebers bezieht sich auf diejenigen Angaben, zu denen er aufgrund seiner vorhandenen Unterlagen oder aufgrund seiner Erinnerung in der Lage ist.

5.3.5 Verpflichtung auf das Meldegeheimnis

Auch das neue bundesgesetzliche Bundesmeldegesetz sieht eine Verpflichtung auf das Meldegeheimnis vor. Die Verpflichtung auf die Einhaltung des Meldegeheimnisses erfolgt nunmehr gemäß § 7 BMG. Von Gemeinden bin ich angefragt worden, ob meine Behörde ein entsprechendes Formular als Arbeitshilfe zur Verfügung stellen könne. Dem bin ich gerne nachgekommen. Das Formular, das auch auf meiner Internetpräsenz zur Verfügung gestellt wird, ist im Anhang unter 17.2.2 abgedruckt. Die Verpflichtungen auf das Meldegeheimnis nach altem Recht sind durch die Meldebehörden anzupassen bzw. zu ersetzen.

5.3.6 Melderegisterauskünfte zu Kindern und Minderjährigen

Eine Meldebehörde teilte mir mit, dass sie Melderegisterauskunftsanträge zu Kindern und Minderjährigen negativ bescheidet. Die Auskunftsbestimmungen des Bundesmeldegesetzes sind Befugnisnormen für die öffentlichen Stellen. Antragsteller haben Anspruch auf ordnungsgemäße Bescheidung und gleichmäßige Behandlung. Gesetzlich besteht aber kein Anspruch auf Auskunft. Die Bestimmung zur einfachen Melderegisterauskunft unterscheidet jedoch nicht im Hinblick auf das Lebensalter der registrierten Personen oder ob es sich um Kinder oder Erwachsene handelt, § 44 BMG. Das habe ich der Behörde so mitgeteilt.

Tatsächlich werden in Bezug auf Kinder in der Praxis häufige und zahlreiche Abfragen durchgeführt, so z. B. bei Unterhaltsfragen, wenn ein ehemaliger Ehepartner in Erfahrung zu bringen trachtet, ob der Partner mit seiner neuen Freundin gemeinsame Kinder zu versorgen hat. Zwar sind bis zur Vollendung des 18. Lebensjahres im Familienverbund Daten im Melderegister gespeichert, aber derartige Auskunftsanträge sind nicht selten abzulehnen, da das Gesetz derartige erweiterte Auskünfte für Private nicht vorsieht. Die eingangs erwähnte einfache Melderegisterauskunft ist hingegen, ergeben sich keine sonstigen Hinderungsgründe, auch in Bezug auf Kinder, gegenüber anfragenden Privatpersonen zu beauskunften.

Auch seitens öffentlicher Stellen, die gemäß ihrer Aufgabenerledigung weitere Meldedaten zu beziehen befugt sind, erfolgen ebenso häufig Anfragen zu Kindern, nicht selten auch in Unterhaltsangelegenheiten, so wenn von Seiten eines Gerichts nachgefragt wird, wie viele Kinder sich in einem Haushalt befinden. Inhaltlich sind die Auskünfte dennoch nur von eingeschränktem Nutzen, ergeben sich aus dem Melderegister zwar Informationen, wie die zu gesetzlichen Vertretern der Kinder, aber viele Bezüge eben nicht, so etwa die biologische Abstammung der Kinder. In Zweifelsfällen sollten die Bediensteten der Meldebehörden wegen der Zweckmäßigkeit des Auskunftsersuchens bei der anfragenden Stelle rückfragen.

5.3.7 Stichprobenartige Überprüfung der Einwilligungen bei Melderegisterbehörden wegen einfacher Melderegisterauskünfte durch Werbe- und Adresshandelsunternehmen

Gemäß § 44 Abs. 3 Satz 6 BMG haben die Meldebehörden wegen der einfachen Melderegisterauskunft durch Auskunft verlangende Werbe- oder Adresshandelsunternehmen das Vorliegen der für Auskünfte dieser Branchen nach dem Gesetz notwendigen Einwilligungserklärungen der Betroffenen stichprobenhaft zu überprüfen, vgl. auch Satz 2 bis 5 der Vorschrift. Die Regelung wurde im parlamentarischen Verfahren zu einem sehr späten Zeitpunkt eingefügt, als (scheinbares) Zugeständnis an Kritiker, um zu demonstrieren, dass Interessen der Betroffenen durch die Parlamentarier gewahrt werden. Tatsächlich ist sie unzweckmäßig und geht ins Leere. Weder beschreiten Werbeindustrie und Adresshandel den Weg, sich über einfache Melderegisterauskünfte im nennenswerten Umfang Daten zu verschaffen, noch willigen Betroffene ein, dass ihre Melderegisterdaten für Adresshandel und durch Werbefirmen genutzt werden können sollen. Die einfache Melderegisterauskunft ist für die genannten Branchen angesichts der für Adressen üblichen Marktpreise und gezielter neuartiger Beschaffungsmöglichkeiten, z. B. über Internetaktionen einfach nicht wirtschaftlich.

Eine Abfrage an Meldebehörden durch meine Dienststelle bestätigte meine bisherigen Einschätzungen. Die Meldebehörden teilten mir mit, dass entsprechende Einwilligungen Betroffener gar nicht vorlägen. Meine auch in der Vergangenheit immer wieder vorgebrachte Kritik, dass vielmehr – die nach neuem Recht gemäß § 50 Abs. 3 BMG – gesetzlich erlaubten Gruppenauskünfte an Adressbuchverlage, die eine Massendatenverarbeitung betreffen, von der Einwilligung und nicht von Widerspruchserklärungen der Betroffenen, die aus rechtlicher Unkenntnis zumeist nicht vorliegen, abhängig gemacht werden sollten, blieb ungehört.

Allen betroffenen meldepflichtigen Personen möchte ich raten, die gesetzlich bestehenden Widerspruchsmöglichkeiten gegen Datenübermittlungen zu erwägen. Die Meldebehörden haben die Einwohner diesbezüglich aufzuklären und zu beraten, vgl. auch 5.3.1. Bisher wegen Widerspruchs nach dem alten Sächsischen Meldegesetz eingetragene Widersprüche werden seitens der sächsischen Meldebehörden weiterhin berücksichtigt; die Übermittlungssperren bleiben bestehen.

5.3.8 Anträge auf Einrichtung einer Auskunftssperre nach § 51 Abs. 1 BMG

Immer wiederkehrend wenden sich Personen an mich, die darlegen, als Personen gefährdet zu sein und die Einrichtung einer Auskunftssperre, die ihnen von der Meldebehörde versagt wurde, verlangen. Auskunftssperren können auf Antrag oder von Amts wegen eingetragen werden. Eine Auskunftssperre kann aber – auch nach neuer Rechtslage – nur in den Fällen erfolgen, in denen „Tatsachen“ vorliegen, „die die Annahme rechtfertigen“, dass dem Betroffenen durch Melderegisterauskünfte „eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen erwachsen kann“. Nicht selten bitten mich dabei auch Angehörige bestimmter Berufsgruppen um datenschutzrechtliche Prüfung der Ablehnung des Antrages auf Einrichtung einer Auskunftssperre durch deren Meldebehörde.

Die tatbestandlichen Gewährungsvoraussetzungen nach § 51 Abs. 1 BMG sind nach dem Wortlaut aber eben nicht erfüllt, soweit in den entsprechenden Anträgen lediglich eine abstrakte Gefahrenlage durch eine mögliche Melderegisterauskunft dargestellt werden kann. Diese Rechtsauffassung hat das Bundesverwaltungsgericht mit Urteil vom 14. Februar 2017 (BVerwG – 6 B 49.16) bestätigt. Das Gericht führt dazu aus: „§ 51 Abs. 1 BMG fordert für die Eintragung einer Auskunftssperre im Melderegister, dass Tatsachen vorliegen, die die Annahme rechtfertigen, dass der betroffenen oder einer anderen Person durch eine Melderegisterauskunft eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen erwachsen kann. Nach dem Gesetzeswortlaut hängt das Vorliegen einer Gefahr i. S. d. § 51 Abs. 1 BMG für eine Person von deren individuellen Verhältnissen ab; die Überschreitung der maßgeblichen

Gefahrenschwelle lässt sich nur in Bezug auf eine konkrete Person durch Darlegung ihrer Verhältnisse belegen. Zu den individuellen Verhältnissen gehört auch die berufliche Tätigkeit der betroffenen Person (vgl. BVerwG, Beschluss vom 7. März 2016 – 6 B 11.16 [ECLI: DE: BVerwG:2016:070316B6B11.16.0] – juris Rdnr. 6). Allein die berufliche Tätigkeit und damit die Zugehörigkeit zu einer Berufsgruppe kann hiernach eine Gefahr im Sinne des § 51 Abs. 1 BMG allerdings nur in seltenen Ausnahmefällen begründen. Dazu muss die Gefahrenschwelle, die das Vorliegen eines schwerwiegenden Grundes verlangt (vgl. BVerwG, Urteil vom 21. Juni 2006 – 6 C 5.05 – BVerwGE 126, 140 Rdnr. 17), allein durch die berufstypischen Risiken überschritten werden, denen sich die betroffene Berufsgruppe ausgesetzt sieht. Das setzt hinreichend dichte Tatsachenfeststellungen voraus, aus denen sich abstrakt das Vorliegen einer Gefahr für alle Angehörigen dieser Berufsgruppe ergibt. Denn die Gefahrenschwelle liegt bei einer abstrakten Gefahr nicht niedriger als im Falle der individuellen Prognose einer konkreten Gefahr. Das ergibt sich aus den Zwecken des Melderegisters, der Melderegisterauskunft sowie dem Ausnahmecharakter der Auskunftssperre gemäß § 51 BMG. Für die Annahme einer abstrakten Gefahr, die für eine Eintragung einer Auskunftssperre nach § 51 Abs. 1 BMG allein aufgrund der Zugehörigkeit zu einer Berufsgruppe ausnahmsweise ausreicht, ist erforderlich, dass Tatsachen festgestellt werden, die eine Gefahrenprognose rechtfertigen, dass aufgrund von in Einzelfällen verwirklichten Gefährdungen der Schluss gezogen werden kann, dass alle Angehörigen der Berufsgruppe sich in einer vergleichbaren Gefährdungslage befinden. Hierzu reicht die Feststellung einzelner Vorfälle nicht aus. Die Vorfälle müssen in einer Anzahl und Häufigkeit auftreten, dass der Schluss berechtigt ist, jeder Angehörige der jeweiligen Berufsgruppe sei einer berufstypischen Gefährdung ausgesetzt. Eine derartige berufsgruppentypische Gefährdungslage dürfte in aller Regel nur durch statistische Angaben oder Ergebnisse repräsentativer Umfragen belegt werden können.“

Soweit eine Gefahr für alle Angehörigen einer beruflichen oder gesellschaftlichen Gruppe generell nicht bejaht werden kann, z. B. bei Bediensteten von Sozialbehörden, Polizisten, privaten Personenschützern oder politischen Mandatsträgern, sind in den Anträgen konkrete Tatsachen, die eine Gefahr zu begründen geeignet sind, anzuführen bzw. von den Meldebehörden von Amts wegen heranzuziehen.

In allen anderen Fällen hat die Eintragung einer Auskunftssperre zu unterbleiben.

5.4 Personenstandswesen

5.4.1 Änderung des Personalausweisgesetzes und des Passgesetzes

Im letzten Berichtszeitraum änderte der Gesetzgeber das Personalausweisgesetz und das Passgesetz. Abweichend vom alten Rechtsstand werden die Personalausweise im Scheckkartenformat standardmäßig mit einem integrierten elektronischen Identitätsnachweis ausgegeben. Mit der Online-Funktion sollen sich Bürger online ausweisen können, einkaufen oder sich gegenüber Behörden authentifizieren. Bis dahin hatte die Anwendung kaum jemand benötigt und genutzt. Die Bundesregierung teilte mit, dass der Ausweis seit 2010 an 45 Millionen Bürger ausgegeben worden sei und nur ein Drittel die Online-Funktion aktiviert habe, was bislang auch freiwillig durchzuführen war. Durch die Gesetzesänderungen sollen die Online-Ausweisfunktionen aus Regierungssicht erweitert und leichter anwendbar werden. Ob dies so gelingt, ist m. E. fraglich, zumal alternative Identifikationsmöglichkeiten im privatwirtschaftlichen Sektor bereits etabliert sind.

Neben der e-ID hat der Gesetzgeber im Personalausweisgesetz und im Passgesetz vorgesehen, dass zusätzlich zu Polizeibehörden die deutschen Geheimdienste zukünftig weitgehend ungeregelt in automatisierten Verfahren auf die Daten in den Meldebehörden zuzugreifen befugt sein sollen, einschließlich der biometrischen Passbilder, vgl. u. a. § 25 Abs. 2 PAuswG. Der automatisierte Abruf, der ohne eine Protokollierung und Kenntnis bei den Meldeämtern erfolgen können soll, wird die Kontrolle darüber, welche Geheimdienste welche Daten abrufen, erschweren. Wenn auch eine zentrale biometrische Datenbank nach dem Personalausweis- und Passrecht ausgeschlossen bleibt, teile ich zudem die Bedenken von Bürgerrechtlern, wonach der fortgeschrittene Ausbau des Abrufs biometrischer Daten immer mehr dazu zu führen geeignet ist, dass biometrische Informationen für Behörden Erkennungsmerkmal zu einzelnen Personen im öffentlichen Raum werden.

Die vor der abschließenden Parlamentsberatung erfolgte Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder „Novellierung des Personalausweisgesetzes vom 24. Januar 2017“ konnte den Gesetzgebungsprozess in den entscheidenden Fragen nicht beeinflussen, vgl. 17.1.12.

5.5 Kommunale Selbstverwaltung

5.5.1 Lichtbildabgleich durch die Bußgeldstellen zur Fahrerermittlung

Im Berichtszeitraum erreichten mich erneut Beschwerden wegen durch kommunale Bußgeldstellen vorgenommener Lichtbildabgleiche zur Fahrerermittlung im Zuge der

Bearbeitung von Verkehrsordnungswidrigkeiten. Ich verweise zur rechtlichen Bewertung im Wesentlichen auf meine Ausführungen in 13./9.1.3.

In den mir erneut bekannt gewordenen Fällen sandten die Bußgeldstellen bei sog. negativem Plausibilitätsabgleich (z. B. Halter männlich, Fahrer eine Frau) zunächst richtigerweise dem Fahrzeughalter einen Zeugenfragebogen zur Fahrerermittlung zu. Die Halter machten jedoch von ihrem Auskunfts- bzw. Zeugnisverweigerungsrecht nach den §§ 52 bis 55 StPO Gebrauch. Die Bußgeldstellen ersuchten daraufhin bei den Meldebehörden um Übermittlung von Name und Anschrift von Familienmitgliedern des Halters und die Übersendung der von diesen Familienmitgliedern hinterlegten Lichtbilder. Anschließend glichen sie sofort das Beweisfoto mit dem übermittelten Foto ab.

Diese Verfahrensweise widerspricht aber den Regelungen des *Erlasses des SMI zur Einsichtnahme des Polizeivollzugsdienstes und der Bußgeldbehörden in des Personalausweis- und Passregister wegen eines Bildabgleiches bei Verfahren wegen Verkehrsordnungswidrigkeiten* vom 18. November 1999, zuletzt geändert am 1. Juli 2005, AZ 31-055/14. Zwar gibt Nr. 1.2 des o. g. Erlasses durchaus das Recht, nach erfolgloser Anhörung des Halters die Meldedaten der Familienangehörigen bei den Meldebehörden nach § 34 Abs. 1 BMG zu ermitteln. Allerdings sind diese zunächst als Zeugen zu hören. Der Anhörungsbogen muss dabei folgenden Hinweis enthalten:

> ‘*Hinweis: Nach dem gegenwärtigen Stand der Ermittlungen sind Sie Zeuge und möglicher Betroffener im Verfahren wegen o. g. Ordnungswidrigkeit. Sofern Sie innerhalb einer Frist von einer Woche keine Angaben zum verantwortlichen Fahrzeugführer machen, kann das Beweisfoto mit Ihrem im Pass- und Personalausweisregister hinterlegtem Foto verglichen werden.*’

Erst nach Verstreichen der gesetzten Frist oder der Ausübung des Zeugnisverweigerungsrechtes ist die Anforderung des im Pass- und Personalausweisregister hinterlegten Lichtbildes zum Abgleich mit dem Beweisfoto rechtlich zulässig (§ 22 Abs. 2 Satz 2 Nr. 1 bis 3 PaßG und § 24 Abs. 2 PAuswG). Die Regelung folgt dem Grundsatz, dass Daten zunächst direkt beim Betroffenen zu erheben sind (vgl. § 12 Abs. 2 SächsDSG). Der befragte Zeuge kann so die Datenerhebung verhindern, indem er die ggf. im Verwarnungsgeldverfahren eingeräumte Möglichkeit, das Verwarnungsgeld zu bezahlen, nutzt oder den verantwortlichen Fahrer benennt.

Meine Ermittlungen ergaben weiterhin, dass noch vor dem (rechtswidrigen) Lichtbildabgleich Ermittlungen am Wohnort des Betroffenen stattgefunden hatten. Dies oder gar eine Befragung der Nachbarschaft darf aufgrund der Schwere des Grundrechtseingriffes

jedoch erst erfolgen, wenn der (rechtmäßige) Lichtbildabgleich ergebnislos verlaufen ist. Dies ist ebenfalls in dem o. g. Erlass vorgeschrieben.

Ich habe die betroffenen Behörden auf die korrekte Anwendung des Erlasses des SMI hingewiesen und für die datenschutzrechtlichen Belange sensibilisiert. Auch habe ich dafür gesorgt, dass die im o. g. Erlass vorgegebenen Hinweise in die Anhörungsbögen aufzunehmen sind. Aufgrund der guten Zusammenarbeit bei der Aufklärung der Vorfälle und der Zusicherung, die Verfahrensfehler abzustellen, habe ich von Beanstandungen abgesehen. Allerdings habe ich das SMI um Prüfung aufsichtsrechtlicher Schritte gebeten. Dieses beauftragte im November 2016 die Landesdirektion Sachsen, die Bußgeldstellen im Rahmen der Fachaufsicht erneut über die korrekte Verfahrensweise zu belehren.

5.5.2 Darf die Presse von einer Stadtverwaltung erstmals erfahren, wer gegen Asylbewerber demonstriert hat?

Nicht nur im Hinblick auf die mangelhafte Ersterfassung von Asylbewerbern bin ich im Rahmen der Massenimmigration des Jahres 2015 mit datenschutzrechtlichen Fragen befasst worden. Auch im Hinblick auf damit zusammenhängende Themen habe ich verschiedentlich Kommunen beraten. Einen beispielhaften Fall, in dem es um das Verhältnis zwischen presserechtlichem Auskunftsanspruch und Datenschutz für die beteiligten Einwohner geht, möchte ich hier schildern.

Eine Stadtverwaltung hatte mich telefonisch und dringend um Beratung zu folgendem Fall gebeten: „Vor der Tür“ stünden Journalisten einer größeren deutschen Zeitschrift, die Fragen zu drei Personen, die im Zusammenhang mit Protesten gegen eine Asylbewerber-Gemeinschaftsunterkunft aufgefallen seien, verlangten. Die Stadt wisse nicht genau, ob und was sie der Presse insofern über diese Personen, die gemeldete Einwohner der Stadt seien, sagen dürfe.

Ich habe die Stadtverwaltung wie folgt beraten: Presserechtlich ergibt sich ein Auskunftsanspruch der Presse aus § 4 Abs. 2 SächsPresseG. Dagegen steht § 4 Abs. 2 Nr. 1 SächsPresseG, wonach die Auskunft verweigert werden darf, wenn und soweit „Vorschriften über die Geheimhaltung“ entgegenstehen. Eine solche Vorschrift stellt § 7 BMG dar, wonach es Personen, die bei Meldebehörden oder anderen Stellen, die im Auftrag der Meldebehörden handeln, verboten ist, personenbezogene Daten unbefugt zu verarbeiten, d. h. hier zu übermitteln (Meldegeheimnis). Es handelt sich beim Meldegeheimnis um ein besonderes Amtsgeheimnis und damit über eine „Vorschrift über die Geheimhaltung“ i. S. v. § 4 Abs. 2 Nr. 1 SächsPresseG. Daher wären Auskünfte zu bisher der Presse nicht namentlich bekannten Einwohnern der Stadt unzulässig. Dagegen

können die Journalisten, wie jeder andere auch, eine einfache Melderegisterauskunft nach § 44 BMG zu ihnen bereits namentlich bekannten Personen erhalten. Voraussetzung ist lediglich, dass die Personen, zu denen eine Melderegisterauskunft beantragt wird, eindeutig identifizierbar sind, § 44 Abs. 3 BMG. Hier entscheiden die Umstände des Einzelfalls. Handelt es sich um gebräuchliche Namen, die mehrfach in der Meldedatei vorhanden sind, muss die Presse die betroffenen Personen durch die Angabe des Geburtsdatums oder einer Anschrift eindeutig identifizieren.

Angesichts der Tatsache, dass gegen die angefragten Personen zum Zeitpunkt der Presseanfrage auch ein staatsanwaltschaftliches Ermittlungsverfahren lief, habe ich der Stadtverwaltung insofern zusätzlich zur Zurückhaltung geraten.

5.5.3 Umfangreiche Datenerhebung im Rahmen des Bieterverfahrens eines kommunalen Grundstücksverkaufs

Eine Gemeinde führte zum Verkauf eines Baugrundstücks ein Bieterverfahren für interessierte Erwerber durch. Ein Betroffener fühlte sich durch den Umfang der dabei vorgesehenen Datenverarbeitung in seinem Grundrecht auf Datenschutz beeinträchtigt.

In der Ausschreibung zum Bieterverfahren wurden klare Vorgaben gemacht, was das Bieterangebot enthalten sollte. Gefordert waren das Gebot sowie ein ausgefülltes Antragsformular, das über die Internetseite der Gemeinde zur Verfügung gestellt wurde. Weiterhin war der Einsendetermin genannt und der Hinweis, dass in der Regel der Kaufinteressent mit dem höheren Gebot bevorzugt werden würde. Im Antragsformular wurden Angaben zur antragstellenden Person, nämlich Name, Vorname, Anschrift, Telefon- und Faxnummer, E-Mail-Adresse, Anzahl der Kinder verlangt Darüber hinaus sollten Angaben zum Vorhabenträger und zum Bauvorhaben, der Schaffung von Wohnungen oder Gewerbeflächen erfolgen und ob Stell- oder Tiefgaragenparkplätze vorgesehen sind, gemacht werden. Auch war eine Finanzierungserklärung beizufügen. Auch das hierfür vorgesehene Formblatt konnte von der Internetseite heruntergeladen werden.

Angaben bzw. Regeln für die Durchführung des Bieterverfahrens, wie beispielsweise eine Bewertungsmatrix, Vorgaben für eine spätere Nutzung des Objektes etc., waren nicht bekannt gemacht worden.

Der Petent fragte nach durchgeführter Entscheidung über den Verkauf, ob die Datenerhebung durch die Gemeinde zulässig gewesen sei. Er habe nur einen lapidaren Zweizeiler als Absage erhalten, dass andere Bieter mehr geboten hätten. Eine Auskunft auf seine Nachfrage nach dem Höchstgebot bzw. der zu Grunde gelegten Bewertungsmatrix für die Entscheidung sei ihm ohne Angabe von Gründen verweigert worden.

Grundsätzlich hat der Gemeinderat die Entscheidungen über Vermögensveräußerungen zu treffen, § 28 Abs. 1 SächsGemO. Nach § 41 SächsGemO kann der Gemeinderat durch die Hauptsatzung beschließende Ausschüsse bilden und ihnen bestimmte Aufgaben zur dauernden Erledigung übertragen.

Für die Veräußerung von Grundstücken durch Gemeinden gibt es aus rechtlicher Sicht keine klaren Vorgaben für ein Bieterverfahren. Unter Beachtung von § 72 Abs. 2 SächsGemO (Allgemeine Haushaltsgrundsätze), § 90 SächsGemO (Veräußerung von Vermögen) und den Regelungen der *Verwaltungsvorschrift über die Veräußerung kommunaler Grundstücke* (VwV kommunale Grundstücksveräußerung) liegt es im Ermessen der Gemeinde, wie sie das Bieterverfahren durchführt. D. h. die Gemeinde kann festlegen, welche Kriterien sie ihrer Zuschlagserteilung zu Grunde legt. Bezogen auf die Informationen, die von den Bietern abverlangt werden, sind auch nur erforderliche personenbezogene Daten zu erheben.

Auch wenn die Grundsätze des Vergaberechts nicht ohne weiteres auf ein Bieterverfahren der Gemeinde übertragen werden kann (vgl. BGH, Urteil vom 22. Februar 2008 – V ZR 56/07), sollte die Gemeinde jedoch die Regeln für die Durchführung eines Bieterverfahrens detailliert und so konkret wie möglich festlegen, und zwar in schriftlicher Form. Im Rahmen des Bieterverfahrens entsteht zwischen dem Bieter und der Gemeinde ein vorvertragliches Vertrauensverhältnis. Dieses verpflichtet die Gemeinden zur Gleichbehandlung der Teilnehmer, Transparenz des Verfahrens und Rücksichtnahme. Das gilt auch außerhalb des Anwendungsbereichs des allgemeinen Vergaberechts (BGH, Urteil vom 12. Juni 2001 – X ZR 150/99).

Die Sitzungen des Gemeinderates (nach § 37 SächsGemO) und die Sitzungen des Grundstücksverkehrsausschusses (nach Hauptsatzung i. V. m. § 37 SächsGemO) sind öffentlich, soweit diese über Gegenstände verhandeln und beschließen, sofern nicht das öffentliche Wohl oder berechtigte Interessen Einzelner eine nichtöffentliche Verhandlung erfordern. Jedoch sind auch Beschlüsse, die in nichtöffentlichen Sitzungen gefasst wurden, in öffentlichen Sitzungen bekannt zu geben, sofern nicht das öffentliche Wohl oder berechtigte Interessen Einzelner entgegenstehen. Als berechtigte Interessen Einzelner kommen alle rechtlich geschützten oder anerkannten Individualinteressen in Betracht, insbesondere persönliche oder wirtschaftliche Verhältnisse.

Der Erwerberkaufpreis und der Nutzungszweck des Grundstückes ist namens- und identitätsbezogen bekanntzugeben, da sich aus diesem Bekanntwerden nichts ergibt, was im Interesse der Parteien vor der Öffentlichkeit geheim zu halten wäre und bei Verkaufsangelegenheiten der Gemeinde der Öffentlichkeitsgrundsatz regelmäßig über-

wiegt. Gegen eine Herausgabe der zugrunde gelegten Entscheidungsregeln und -maßstäbe bestanden ohnehin keine datenschutzrechtlichen Vorbehalte.

Auf die Nachfrage des betroffenen Bieters, welche Daten zu seiner Person anlässlich des Verfahrens gespeichert worden sind und wie diese ausgewertet wurden, war gemäß § 18 SächsDSG seitens der Gemeinde kostenfrei und ohne unzumutbare Verzögerung Auskunft zu erteilen gewesen.

5.5.4 Herausgabe von elektronischen Fundsachen an den Finder

An mich wurde die Frage herangetragen, ob ein Finder nach Vorliegen der zivilrechtlichen Voraussetzungen die Herausgabe von Mobiltelefonen, Smartphones oder anderen elektronischen Speichermedien verlangen kann oder ob dies aus datenschutzrechtlichen Gründen verwehrt werden muss.

Nach § 973 Abs. 1 BGB erwirbt der Finder mit dem Ablauf von sechs Monaten nach der Anzeige des Fundes bei der zuständigen Behörde das Eigentum an der Sache, wenn kein Empfangsberechtigter dem Finder bekannt geworden ist oder sein Recht bei der zuständigen Behörde angemeldet hat.

Handelt es sich bei der Fundsache um Mobiltelefone, USB-Speicherstifte, Laptops und sonstige Datenträger, die noch personenbezogene Daten enthalten, ist der Herausgabeanspruch gegen die Gemeinde aus dem öffentlich-rechtlichen Verwahrverhältnis, den der Finder zugleich mit dem Eigentumsübergang nach § 973 BGB erhält, datenschutzrechtlich überlagert, denn mit Ablieferung der Fundsache beim gemeindlichen Fundamt wird dieses datenschutzrechtlich verantwortliche öffentliche Stelle für die auf der Fundsache gespeicherten Daten.

In der Herausgabe der Fundsache durch die Gemeinde mitsamt der auf dieser gespeicherten unkörperlichen personenbezogenen Daten des ehemaligen Eigentümers an den Finder (natürliche Person) ist eine Datenübermittlung an eine nicht-öffentliche Stelle zu sehen.

Mangels einschlägiger speziellerer Regelungen im Sinne des § 2 Abs. 4 SächsDSG wäre diese Datenverarbeitung einer Gemeinde als verantwortlicher Stelle nur unter den Voraussetzungen des § 16 Abs. 1 i. V. m. § 12 Abs. 4 und § 13 Abs. 2 SächsDSG zulässig.

An diesen Voraussetzungen wird es aber regelmäßig mangeln. Weder ist die Herausgabe der Fundsache mitsamt den auf dieser gespeicherten Daten zur Aufgabenerfüllung

der Fundbehörde gemäß § 16 Abs. 1 Nr. 1 SächsDSG erforderlich, noch liegen die Voraussetzungen von § 12 Abs. 4 und § 13 Abs. 2 SächsDSG vor. Darüber hinaus kann auch ein schutzwürdiges Interesse des ehemaligen Eigentümers am Unterbleiben der Übermittlung gemäß § 16 Abs. 1 Nr. 2 SächsDSG nicht ausgeschlossen werden.

Daher sind vor einer Herausgabe der Fundsache an den Finder die auf dieser gespeicherten personenbezogenen Daten des ehemaligen Eigentümers zu löschen. Sollte eine Löschung nicht möglich bzw. Aufwand und Kosten, die dem Finder aufgebürdet werden können, für die Löschung unverhältnismäßig groß sein, oder kann aufgrund technischer Hindernisse mit angemessenen Aufwand nicht geklärt werden, ob auf dem Gerät noch schutzwürdige Daten gespeichert sind, ist dieses Gerät datenschutzgerecht zu entsorgen.

Nach meiner Überzeugung ist der Schutz des Datenschutzgrundrechts des betroffenen Verlierers und ursprünglichen Eigentümers höher zu bewerten als der Vollzug des Eigentumserwerbs an der körperlichen Sache. Sofern durch eine Löschung der Daten kein gefahrenbefreiter Zustand hergestellt werden kann, ist die Herausgabe öffentlich-rechtlich gehindert.

5.5.5 Drohnenüberflüge und Videoaufnahmen durch Gemeinden

Im letzten Berichtszeitraum wandte sich ein Betroffener an mich und teilte mit, dass ihm zur Kenntnis gelangt sei, dass die städtische Verwaltung einer sächsischen Großstadt bei einer Veranstaltung Drohnenüberflüge und Videoaufnahmen durchgeführt habe.

Meine Anfrage an die Stadt und eine Vorortkontrolle ergaben, dass das Ordnungsamt der Gemeinde eine Befliegung und Videoaufnahmen beauftragt hatte, um für dieselbe Veranstaltung im nächsten Jahr Rettungs- und Einsatzwege sowie die mit freien Verkehrswegen und die mit einer kritischen Anzahl von Menschen zusammenhängende Frage straßenrechtlicher Sondergenehmigungen zur Verkaufsstandvergabe planen zu können.

Bei den Videoaufnahmen war eine konkrete Verletzung der Rechte des Betroffenen nicht feststellbar gewesen. Gesichter waren nicht erkennbar. Die Auflösung war zu grob. Allerdings hätten aufgrund der Qualität der Aufnahmen einzelne Personen aufgrund besonderer Kleidung oder Umstände bei einigen Videoaufnahmen wiedererkannt werden können. Auf eine zeitliche Zuordnung der durch Videoaufnahmen erfassten Personen auf den Verkehrswegen war durch den Auftragnehmer verzichtet worden.

Ein schriftlicher Vertrag der Stadt mit dem Dienstleister zu der Überfliegung lag allerdings nicht vor. Der Auftrag wurde mündlich erteilt. Schon formell waren daher die Voraussetzungen einer Auftragsdatenverarbeitung im Sinne von § 7 SächsDSG nicht eingehalten. Zudem konnte der Auftragnehmer frei und ohne engere Vorgaben seine Luftaufnahmen zusammentragen. Demgegenüber hätte eine Auftragsdatenverarbeitung vorausgesetzt, dass der Auftragnehmer die Videoaufnahmen nach konkreten Weisungen anfertigt. So war von einer Datenerhebung durch eine nicht-öffentliche Stelle auszugehen, § 6b BDSG.

Die Sondervorschrift des § 33 SächsDSG erfordert nicht die Verarbeitung *personenbezogener* Daten, vgl. auch den Wortlaut von § 33 Abs. 2 SächsDSG. Die Verarbeitung von Daten genügt. Öffentlichen Stellen rate ich zur Auftragsdatenverarbeitung, möglichst unter Verzicht auf die Erhebung personenbezogener Daten, den Einsatz von mit Videoaufnahmegeräten ausgerüsteten Drohnen durch Auftragnehmer zur eigenen Aufgabenerfüllung mit einer Verfahrensbeschreibung vorzubereiten und den Zweck und sämtliche gesetzlichen Voraussetzungen zu dokumentieren. Die Videografie durch den Auftragnehmer sollte auf Grundlage eines konkreten Befliegungsplans anhand einer Kartierung festgelegt werden, ebenso der Einsatz der konkreten Technik, die Datenqualität, Auflösung der Aufnahmen, Flughöhe, Flugbedingungen und -dauer, um damit eine weisungsgebundene Datenverarbeitung des Auftragnehmers sicherzustellen und dass möglichst keine Personen identifiziert werden können. Die Daten sind an die Gemeinde als Auftraggeber zu übergeben bzw. nach Auftragserfüllung und Auswertung zu löschen. Je nach Dauer und Einsatzaufwand sollten entsprechende Ankündigungen der Maßnahme als Bekanntmachungen im amtlichen Gemeindeblatt und ggf. in Tageszeitungen erfolgen, vgl. § 33 Abs. 3 SächsDSG.

5.5.6 Informationsfreiheitssatzungen der Gemeinden und Datenschutz

Der Freistaat Sachsen verfügt bisher über kein Informationsfreiheitsgesetz. Einige Gemeinden sind dazu übergegangen, Informationsfreiheitssatzungen zu erlassen.

In Ermangelung bereichsspezifischer gesetzlicher Grundlagen kann eine entsprechende Normsetzung auf Grundlage von § 4 Abs. 1 SächsGemO erfolgen. Nach der Vorschrift können die Gemeinden zur Regelung ihrer Angelegenheiten, also für den weisungsfreien Bereich, Satzungen erlassen. Die Rechtsetzungskompetenz für die weisungsfreien Selbstverwaltungsangelegenheiten ist Ausfluss des verfassungsrechtlich durch Art. 28 Abs. 2 Satz 1 GG garantierten gemeindlichen Selbstverwaltungsrechts. Die gemeindeordnungsrechtliche Vorschrift kommt damit grundsätzlich als Rechtsgrundlage in Betracht. Die allgemeine Satzungsbefugnis ermächtigt nach der ständigen Rechtsprechung

des Bundesverwaltungsgerichts allerdings nur zu Regelungen, die nicht in Rechte Dritter eingreifen. Grundrechtseingriffe bedürfen einer besonderen gesetzlichen Ermächtigung in Form eines parlamentarischen Gesetzes, vgl. BVerwG, Urteil vom 16. Oktober 2013 – 8 CN 1.12. Dementsprechend können z. B. Abwägungen von widerstreitenden Grundrechten nicht in einer auf der Generalklausel beruhenden Satzung gestützt werden. Bei entsprechenden Satzungen ist demzufolge darauf zu achten, dass Grundrechtseingriffe durch eine entsprechende Gestaltung der Ausschlussgründe verhindert werden.

Gewährung von Informationsfreiheit ist – naheliegenderweise – geeignet, sowohl, was personenbezogene Daten, die vom Recht auf informationelle Selbstbestimmung geschützt sind (Art. 2 Abs. 1 i.V. m. Art. 1 Abs. 1 GG), als auch was Betriebs- und Geschäftsgeheimnisse (Art. 12 Abs. 1, Art. 14 Abs. 1 GG), die häufig personenbezogene Daten enthalten, betrifft, einen gegen den Willen der betroffenen Grundrechtsträger gerichteten Grundrechtseingriff darzustellen. Da der Eingriff allein aufgrund der kommunalrechtlichen Generalklausel zum Satzungserlass nicht gerechtfertigt werden kann, haben gemeindliche Informationsfreiheitssatzungen personenbezogene Daten ebenso wie Betriebs- und Geschäftsgeheimnisse umfassend vor einer behördlichen Offenbarung zu schützen. Bei Auskunftsbegehren, die sich auch gegen einzelne Betroffene richten, kann daher das Ortsrecht nicht formelle Gesetze abändern. Damit bleibt es auch bei allgemeinen Bestimmungen wie § 16 SächsDSG oder bereichsspezifischen Regelungen, die eine Übermittlung an nicht-öffentliche Stellen nur unter den normierten Voraussetzungen zulassen oder wenn der Betroffene eingewilligt hat, vgl. § 4 Abs. 1 Nr. 2 SächsDSG. Entsprechend hat die kommunale Rechtsetzung inhaltlich ausgestaltet zu sein.

Die Satzungen müssen meiner Behörde nicht zugeleitet werden. Kommunale Satzungen werden aber der Rechtsaufsichtsbehörde angezeigt, § 4 Abs. 3 Satz 3 SächsGemO. Bei bisher mir bekanntgewordenen gemeindlichen Satzungen konnte ich bisher keine Rechtsfehler ausmachen.

5.5.7 Ratsinformationssysteme und der Zugang zu Sitzungsunterlagen und Niederschriften

Zurückliegend hatte ich mich mehrfach zu der Zulässigkeit der Verarbeitung personenbezogener Daten in Stadtratsunterlagen bzw. Sitzungsvorlagen geäußert, vgl. auch 12/5.5.6, 12/5.5.9, 14/5.5.4, 15/5.5.3.

Vielfach gehen Gemeinden dazu über, nicht nur, wie es die Sächsische Gemeindeordnung vorsieht, über anstehende Beratungen und Beschlussfassungen zu informieren, sondern die Tagesordnungen der Sitzungen mitsamt den Vorlagen und den Nieder-

schriften mittels Internetpräsenz nicht nur den Gemeinderäten, sondern auch einer breiten Öffentlichkeit zugänglich zu machen. Was die Stadtratsvorlagen betrifft, gibt es hierfür keine gesetzliche Stütze, auch nicht, was die Inhalte öffentlicher Sitzungen anbelangt. § 36 Abs. 3 Satz 1 SächsGemO sieht lediglich vor, dass der Bürgermeister den Gemeinderat schriftlich oder in elektronischer Form mit angemessener Frist einberuft, ihm rechtzeitig die Verhandlungsgegenstände mitteilt und die für die Beratung erforderlichen Unterlagen beifügt, soweit nicht das öffentliche Wohl oder berechtigte Interessen Einzelner entgegenstehen. Allerdings bestehen gegen die Zugänglichmachung der Informationen dann allein datenschutzrechtlich keine Einwände, wenn keine personenbezogenen Daten Betroffener verarbeitet werden. Nach dem Gesetz ist sogar die Beschränkung der Gemeinderäte selbst vorgesehen, wenn berechtigte Interessen Einzelner entgegenstehen, siehe den Wortlaut von § 36 Abs. 3 Satz 1 SächsGemO – am Ende. Und da in den kommunalen Vertretungskörperschaften und Ausschüssen, in Personalvorgängen, bei Beschwerden von Bürgern, Vertrags- und Steuerangelegenheiten regelmäßig auch personenbezogene schützenswerte und vertrauliche Angelegenheiten Gegenstand sind, bedeutet das, dass die Gemeinden als datenverarbeitende Stellen sämtliche vorgesehenen Inhalte vor einer Veröffentlichung im Internet zu prüfen haben und personenbezogene Inhalte unkenntlich oder von dem Angebot auszunehmen haben, um Datenschutzverletzungen auszuschließen. Vgl. zu Beschlussfassungen im Übrigen auch 5.5.8, zu Niederschriften auch 14/5.5.2.

Erfolgt die Veröffentlichung von Sitzungsunterlagen, die allein den Gemeinderäten zur Verfügung gestellt worden sind, wiederum durch die Mandatare selbsttätig, wird eine solche Eigenmacht nach der gegebenen Rechtslage in Sachsen regelmäßig als rechtswidrig zu erkennen sein, vgl. Beschluss des OVG Bautzen vom 8. Juli 2016 – 4 B 366/15. Im letzten Berichtszeitraum hatte das Oberverwaltungsgericht zu einer Veröffentlichung von Stadtratsunterlagen durch einen Gemeinderat entschieden, dass durch die modernen Informations- und Kommunikationstechniken vielfältige Möglichkeiten bestünden, personenbezogene Daten zielgerichtet auszuwerten und zu verarbeiten und eine unzulässige Veröffentlichung im Internet und mangelnde Datensicherheit der in den Ratsinformationssystemen verarbeiteten und gespeicherten personenbezogenen Daten eine Gefährdung des Rechts auf informationelle Selbstbestimmung der Betroffenen ergebe. Im konkreten Fall hatte die Stadt neben dem Betreff, Beschlussvorschlag und lediglich eine kurze Zusammenfassung des Sachverhalts zur Information der Einwohner im Internet bereitgestellt, die einen geringeren inhaltlichen Gehalt aufwies, als die Sitzungsunterlagen und Anlagen, deren Veröffentlichung durch den Gemeinderat die Gemeinde zu verhindern trachtete. In seiner Entscheidung wies das Gericht zudem auf die Verschwiegenheitspflicht der Gemeinderäte nach § 19 Abs. 2 Satz 1 SächsGemO hin, zu der diese über geheimzuhaltende Angelegenheiten verpflichtet sind. Deren

Geheimhaltung ist ihrer Natur nach erforderlich, da Offenbarungen dem Gemeinwohl bzw. den schutzwürdigen Interessen einzelner Personen zuwiderlaufen. Bei internen Angelegenheiten der Gemeindeverwaltung besteht parallel zudem gesetzliche Amtsverschwiegenheit. Letztendlich betrachtet das Oberverwaltungsgericht, dessen Rechtsauffassung ich in der Sache vollumfänglich teile, die Sitzungsunterlagen als „rein interne Papiere der Verwaltung“ und sieht eine Befugnis einzelner Gemeinderäte zur Veröffentlichung verwaltungsinterner Schriftstücke bzw. kompletter Sitzungsunterlagen als nicht gegeben an. Der Zweck der Sitzungsunterlagen bestehe „allein in der Verwendung innerhalb des Stadtrats“, der „Unterrichtung innerhalb des Stadtrats“ und „der Vorbereitung von Abstimmungen im Stadtrat“.

Grundsätzlich erhöhen Informationsangebote im Internet zu den Gemeinderatsangelegenheiten aber auch die Transparenz der Entscheidungen, die das persönliche Lebensumfeld der Bürger in der gemeindlichen Öffentlichkeit betreffen und sind daher auch als zweckmäßig zu betrachten. Neben der Frage, welche Informationen der Öffentlichkeit angeboten werden sollten – vgl. oben –, sind aber derartige Verfahren, die zumeist gleichzeitig die Aufgabenerledigung der ehrenamtlichen Räte durch Recherche- und Archivfunktionen unterstützen und verbessern sollen, informationssicherheitstechnisch sicher auszugestalten.

Entscheidet die Vertretungskörperschaft der Gemeinde Tagesordnung, Sitzungsvorlagen und Niederschriften öffentlicher Sitzungen in das Internet einzustellen, so sind hierfür eine entsprechende Beschlussfassung des Rates und ggf. ergänzende Festlegungen, die auch in der Geschäftsordnung getroffen werden können, notwendig. So sind Vorgänge, die aufgrund berechtigter Interessen Betroffener in nichtöffentlicher Sitzung zu behandeln sind, ohne Einwilligung nicht im öffentlich zugänglichen Teil eines Ratsinformationssystems zu platzieren. Auch sollten die Gemeinderäte im Rahmen ihrer Verpflichtung auf ihre Rechte und Pflichten auf den ordnungsgemäßen Umgang mit dem Ratsinformationssystem hingewiesen werden.

Des Weiteren sollten Tagesordnungen und Sitzungsvorlagen bzw. Zusammenfassungen zu den Themen inhaltlich so bearbeitet sein, dass Personenbezug ausgeschlossen ist. Auch ist zu raten bereits bei der Erstellung der Vorlagen von verantwortlichen Beschäftigten festzulegen, ob die Dokumente in den öffentlichen Teil des Ratsinformationssystems eingestellt werden sollen oder nur verwaltungsintern und Gemeinderäten zugänglich gemacht werden sollen. Zu Beschlussfassungen, siehe ausführlich 5.5.8. Auch eine Veröffentlichung von Niederschriften öffentlicher Sitzungen sieht die Sächsische Gemeindeordnung nicht vor, lediglich ein Einsichtnahmerecht für Einwohner. Soweit Niederschriften oder Zusammenfassungen der Sitzungen publiziert werden sollen, wäre nach der gegenwärtigen Rechtslage daher ebenso auf einen datenschutzgerechten Inhalt

zu achten. So sind personenbezogene Angaben in veröffentlichten Fassungen von Niederschriften zu vermeiden, vgl. 14/5.5.2. Auch ist davon abzusehen, Wortprotokolle und Protokollierungen des Abstimmungsverhaltens einzelner Ratsfrauen oder Ratsherren in das Internet einzustellen.

Im Hinblick auf Zugriffs- und Einsichtsrechte ist sicherzustellen, dass das Ratsinformationssystem personenbezogene Informationen, die in nichtöffentlicher Sitzung behandelt worden sind, nur Beschäftigten zugänglich gemacht werden, die im Rahmen ihrer Aufgabenerfüllung auch an den jeweiligen Vorgängen zu beteiligen sind. Die Zugriffs- und Einsichtsrechte sind generell nach Schreib- und Leserechten zu differenzieren und in einem Berechtigungs- und Rollenkonzept niederzulegen. Gemeinderäten kann nach sächsischem Gemeinderecht ein Zugriff auf sämtliche Vorlagen, auch nichtöffentlicher Sitzungen des Rates und der sonstigen Ausschüsse und Gremien, eröffnet werden, auch wenn sie diesen Ausschüssen nicht angehören, § 42 Abs. 4 SächsGemO. Mitglieder von Ausschüssen, die hingegen nicht Gemeinderatsmitglieder sind, dürfen nur Zugriff auf Unterlagen und Niederschriften nichtöffentlicher Sitzungen des Ausschusses haben, denen sie selbst angehören. Mitarbeiter von Fraktionen, können im Einklang mit § 35a Abs. 4 SächsGemO Zugang erhalten.

Ratsinformationssysteme, die im Übrigen regelmäßig vorabkontrollpflichtig sein werden, vgl. § 10 Abs. 4 SächsDSG, sind aufgrund der Art und des Umfangs der Datenverarbeitung Gegenstand von Dienstanweisungen und ggf. Dienstvereinbarungen, in denen Mandatare und Beschäftigte über die einzuhaltenden technisch-organisatorischen Maßnahmen zu informieren sind.

Ein Augenmerk ist in technisch-organisatorischer Hinsicht in besonderer Weise auf Zugriffe auf das Verfahren von außerhalb des Netzwerks zu legen, um mittels Firewall und Verschlüsselungstechnik einen kontrollierten Zugang und eine gesicherte Datenkommunikation in das lokale Netzwerk absichern zu können. Entsprechende Maßnahmen sind bei der Einbindung von E-Mail-Diensten zu ergreifen. Bei Ratsinformationssystemen größerer Gemeinden bieten sich, was den nichtöffentlichen und internen Bereich angeht, Authentifikationsmittel wie Chip- und Signaturkartensysteme an.

Soweit Gemeinderäte mit eigener Hardware von außerhalb auf das Ratsinformationssystem zugreifen und Daten lokal speichern, sollte die Gemeindeverwaltung eine Sicherheitsprüfung durch die Administratoren anbieten, um Sicherheitsmängel auszuschließen. Auf der privaten Hardware sollte dem technischen Standard entsprechende Sicherheitssoftware zum Einsatz kommen. Soweit schutzwürdige Informationen auf Computersystemen außerhalb der Verwaltung gespeichert werden, sollten die verant-

wortlichen Gemeinderäte verpflichtet werden, die Daten in geeigneter Weise gegen unbefugten Zugriff zu sichern. Zweckmäßig ist, eine Verschlüsselung von aus dem Ratsinformationssystem übertragenen Daten auf externen Trägern durchzuführen. Letztlich ist, wenn Gemeinderäte ihre ehrenamtliche Tätigkeit beenden, sicherzustellen, dass die auf heimischen Computersystemen gespeicherten vertraulichen Informationen unverzüglich und unumkehrbar gelöscht werden. Der Export von Inhalten die besonders hohen Schutzgrad aufweisen, ist zu unterbinden.

Was die Veröffentlichung personenbezogener Daten der Gemeinderäte, Mandatare in Gremien und deren Zusammensetzung im Ratsinformationssystem selbst betrifft, werden über die wahlgesetzlichen Kandidateninformationen hinausgehende Daten, wie Portraitabbildungen oder private Anschriften- und Kommunikationsdaten nur bei Vorliegen einer schriftlichen Einwilligung zulässig veröffentlicht werden dürfen. Das Kunsturhebergesetz ist bei der Veröffentlichung von Abbildungen zu beachten. Ich rate allerdings generell zur Einrichtung von Gemeinde-E-Mail-Adressen und der Kommunikation über das Rathaus um eine gewisse Chancengerechtigkeit aufrechtzuerhalten, dies daher, da nicht wenige politisch engagierte Personen im Freistaat Sachsen Aggressionen und Einschüchterungen ausgesetzt sind.

5.5.8 Veröffentlichung von Gemeinderatsbeschlüssen, die personenbezogene Daten enthalten, auf der kommunalen Webseite

Häufig werde ich um Auskunft darüber ersucht, ob die Veröffentlichung von Gemeinderatsbeschlüssen, die personenbezogene Daten enthalten, gegen datenschutzrechtliche Bestimmungen verstößt, zum Beispiel bei Veräußerungen der Gemeinde.

Einerseits sind die Gemeinden gemäß § 37 SächsGemO angehalten, Sitzungen des Gemeinderates grundsätzlich öffentlich durchzuführen, sofern nicht das öffentliche Wohl oder berechtigte Interessen Einzelner eine nichtöffentliche Verhandlung fordern. Die in nichtöffentlichen Sitzungen gefassten Beschlüsse sind in öffentlichen Sitzungen bekanntzugeben.

Jedoch bedürfen die Beschlüsse des Gemeinderates weder der öffentlichen Bekanntmachung noch der ortsüblichen Bekanntgabe. Wird der Beschluss in öffentlicher Sitzung gefasst bzw. bekanntgegeben, ist er zu diesem Zeitpunkt auch „bekanntgegeben“, ohne dass es einer weiteren nochmaligen Veröffentlichung bedarf. Ein zusätzlicher Veröffentlichungsakt wird vom Gesetzeswortlaut nicht vorgeschrieben (vgl. Quecke/ Schmid/Menke/Rehak/Wahl/Vinke/Blazek/Schaffarzik, Rdnr. 43 zu § 37 SächsGemO). Unstreitig ist jedoch, dass es wegen der kommunalpolitischen Bedeutung zweckmäßig

ist, wenn über die Ergebnisse z. B. im Amts- oder Mitteilungsblatt der Gemeinde berichtet wird.

Viele sächsische Gemeinden stellen im Ansinnen, Bürgerfreundlichkeit, mehr Transparenz der Verwaltung und eine Verbesserung der Informationen und Teilhabe der Einwohner am kommunalpolitischen Geschehen herzustellen, ihre Amts- und Mitteilungsblätter auf ihre Internetseiten oder z. T. über besondere Online-Ratsinformationssysteme zur Verfügung.

Meine Behörde hat sich bereits in der Vergangenheit immer wieder mit der Zulässigkeit der Veröffentlichung kommunaler Dokumente im Internet beschäftigt (siehe 14/5.5.2, 15/5.5.6, 16/5.5.1). Das Sächsische E-Government-Gesetz enthält in § 4 klare Vorgaben, unter welchen Voraussetzungen amtliche Mitteilungs- und Verkündungsblätter auch im Internet veröffentlicht werden dürfen. Auf kommunaler Ebene ist ergänzend eine entsprechende Rechtsetzung mit einer Satzung erforderlich. Darin ist auch festzulegen, welche Form, die Papier- oder elektronische Fassung, als die authentische anzusehen ist. Bei einer elektronischen Fassung ist zudem sicherzustellen, dass personenbezogene Daten unkenntlich gemacht werden, wenn der Zweck ihrer Veröffentlichung erledigt ist und eine fortdauernde Veröffentlichung das Recht der betroffenen Person auf informationelle Selbstbestimmung unangemessen beeinträchtigen würde. Derartige Änderungen sind als solche erkennbar zu machen und haben den Zeitpunkt der Änderung erkennen zu lassen. Ich begrüße in dem Zusammenhang sehr die ministeriellen Bemühungen, den einheitlichen Vollzug des E-Government-Gesetzes durch Umsetzungshinweise zu gewährleisten und die Behörden damit in ihrer Rechtsanwendung zu unterstützen. Eine Ergänzung der Hinweise zu der gesetzlich zugrundeliegenden Vorschrift des § 4 SächsEGovG zur Veröffentlichung möchte ich, in Anbetracht erwartbarer praktischer Schwierigkeiten der öffentlichen Stellen, anraten.

Zu bedenken ist bei einer Veröffentlichung im Internet generell, dass die Daten weltweit einem unbeschränkten Personenkreis zur Verfügung gestellt werden. Moderne Informations- und Kommunikationstechniken bieten vielfältige Möglichkeiten, personenbezogene Daten zielgerichtet auszuwerten und zu verarbeiten. Durch eine Veröffentlichung im Internet kann sich eine Gefährdung des Rechts auf informationelle Selbstbestimmung ggf. auch erst aus einer möglichen weiteren Verknüpfung von Angaben einzelner Personen mit Informationen aus anderen Datenbeständen ergeben. Die Gemeinden sollten dies stets bei ihren Entscheidungen, Daten im Internet zu veröffentlichen, berücksichtigen, sorgfältig und einzelfallbezogen abwägen und entsprechende datenschutzorganisatorische und technische Maßnahmen ergreifen.

Der Zweck einer Veröffentlichung von Gemeinderatsbeschlüssen ist erfüllt, wenn die Einwohner die Möglichkeit eröffnet bekommen haben, Kenntnis von den Beschlüssen und der Tätigkeit des Gemeinderates zu nehmen. Als zeitliche Vorgabe hierfür könnte daher auch für im Internet zugängliche Informationen der Zeitraum herangezogen werden, in dem das aktuell gedruckte amtliche Gemeindeblatt in den Gemeinden ausliegt. Hinzuweisen ist auch noch darauf, dass den Einwohnern die Möglichkeit zu gewähren ist, Einsicht in die Niederschriften der Ratssitzungen zu nehmen, die die Niederschriften der Beschlüsse in ihrem Wortlaut enthalten, § 40 Abs. 1 SächsGemO.

Auf meine Anregung hin haben die betroffenen Gemeinden alle Beschlüsse, die nicht das laufende Kalenderjahr betreffen, löschen lassen. Den Gemeinden empfahl ich weiter, das Verfahren in Bezug auf eine elektronische Veröffentlichung der kommunalen amtlichen Mitteilungs- oder Verkündungsblätter in ihre Bekanntmachungssatzungen aufzunehmen. Dabei kann auch der Zeitraum der elektronischen Veröffentlichung festgelegt werden. Nach der Unkenntlichmachung der personenbezogenen Daten in den Beschlüssen oder auch der Gesamtausgabe der elektronischen Amts- oder Mitteilungsblätter, kann ein Hinweis erfolgen, dass benötigte Druckausgaben künftig in den Räumen der Gemeinde, z. B. der Verwaltungsbibliothek oder dem Archiv zur Einwohnerinformation als Präsenzexemplare zur Verfügung gestellt werden können.

5.6 Baurecht; Wohnungswesen

In diesem Jahr nicht belegt.

5.7 Statistikwesen

5.7.1 Zulässige Kopplung von Zuwendungsbescheiden an die verpflichtende Teilnahme an der Datenübermittlung nach ÜSchuldStatG

Die Überschuldungsstatistik ist eine zentral vom Statistischen Bundesamt durchgeführte Erhebung bei den Schuldnerberatungsstellen, um Informationen zur Situation von Personen bereitzustellen, die sich in finanziellen Schwierigkeiten befinden. Grundlage für die Durchführung der Überschuldungsstatistik ist das Überschuldungsstatistikgesetz.

Die Erteilung der Auskunft durch die Schuldner- oder Insolvenzberatungsstellen zur Durchführung der Überschuldungsstatistik an das Statistische Bundesamt ist nach § 7 Abs. 1 ÜSchuldStatG freiwillig. Soweit personenbezogene Daten betroffen sind, ist die Auskunftserteilung durch die Schuldner- oder Insolvenzberatungsstelle an das Statistische Bundesamt nach Absatz 2 der Vorschrift auch nur zulässig, wenn die betroffene Person in die Übermittlung ihrer Daten eingewilligt hat.

Im Berichtszeitraum erreichte mich die Anfrage einer Schuldnerberatungsstelle, ob die Praxis des SMS, die Zuwendungsbescheide an die verpflichtende Teilnahme an der Datenübermittlung nach dem Überschuldungsstatistikgesetz zu koppeln, rechtmäßig sei. Zudem wollte die Beratungsstelle wissen, wie sie zu verfahren hätte, wenn der zu Beratende die Einwilligung zur Datenübermittlung verweigere.

Die Datenübermittlung an das Statistische Bundesamt erfolgt, wie bereits erwähnt, freiwillig. Allerdings hat der Bundesgesetzgeber den Ländern in der damaligen Gesetzesbegründung zu § 7 Abs. 1 ÜSchuldStatG (BT-Drs. 17/7418) das Recht eingeräumt, den Schuldner- und Insolvenzberatungsstellen Vorgaben zu machen. Dieses Vorgabenrecht deckt aus meiner Sicht die verpflichtende Teilnahme im Zusammenhang mit den Zuwendungsbescheiden. Die Freiwilligkeit wird hierbei nicht per se eingeschränkt, sondern nur im Zusammenhang mit der Gewährung einer Leistung. Das Interesse des Freistaates an der Datenübermittlung besteht darin, dass der Freistaat bei einer statistisch relevanten Datenmenge Abfragen aus der Bundesstatistik durchführen kann, was wiederum Relevanz für politische Entscheidungen hat.

Die Frage, ob eine Übermittlung auch bei fehlender Einwilligung zulässig ist, lässt sich mit § 7 Abs. 2 ÜSchuldStatG beantworten. Allerdings ist dabei zu prüfen, ob es sich bei dem Datensatz um personenbezogene Daten handelt, also gemäß § 3 Abs. 1 BDSG um Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren Person. Die Abfrage sachlicher und persönlicher Verhältnisse ist unstreitig. Da bei dem Formular keine Namen, Anschriften und exakte Geburtsdaten übermittelt werden, ist keine Bestimmtheit gegeben. Die Bestimmbarkeit der Person ist von mehreren Faktoren abhängig. Zum einen von dem den Datensatz pseudonymisierenden und von der Beratungsstelle zu vergebenen Aktenzeichen. Dies darf keinen direkten Bezug zum Namen oder Geburtsdatum enthalten. Zum anderen können, je nach Grad der Einmaligkeit und des Herausstechens der Daten sowie der Größe der Gemeinde, die Daten durchaus zu personenbezogenen Daten werden. Die wäre z. B. gegeben, wenn in einer kleinen Gemeinde nur ein 12-Personenhaushalt wohnt. Dann wäre der Bezug durch die abgefragten Daten „Haushaltsgröße“ und „Gemeindeschlüssel“ zu der Person herstellbar.

Die, im Einzelfall eventuell schwierige, Abwägung, ob es sich im konkreten Fall um personenbezogene Daten handelt oder nicht, obliegt der datenübermittelnden Stelle. Sollte im Einzelfall die Überzeugung entstehen, dass es sich bei den zu übermittelnden Daten um personenbezogene Daten handelt, ist eine Einwilligung einzuholen. Wird die Einwilligung verweigert, hat eine Datenübermittlung zu unterbleiben. Ein Verlangen seitens des SMS, die Übermittlung dennoch durchzuführen, wäre rechtswidrig und da-

mit nichtig. Allerdings ist jährlich die Anzahl der Widersprüche gegen die Datenübermittlung dem Statistischen Bundesamt mitzuteilen.

Die Einwilligung darf aber auch nur dann eingeholt werden, wenn es sich um personenbezogene Daten handelt, da die Übermittlung andernfalls auch ohne Einwilligung zulässig und im Falle einer Zuwendung auch verpflichtend wäre.

Ansonsten wird dem Betroffenen ein Wahlrecht suggeriert, welches er in Wahrheit gar nicht besitzt.

5.8 Archivwesen

5.8.1 Erhebung personenbezogener Daten bei der Archivnutzung

Mir wurde die Frage gestellt, ob die Archivverwaltung berechtigt sei, Angaben zur Person, die Archivgut nutzen möchte, erfragen, also im datenschutzrechtlichen Sinne erheben zu dürfen.

Hintergrund der Anfrage war, dass im Rahmen der letzten Novellierung des Sächsischen Archivgesetzes die Vorschrift des § 9 dahingehend geändert worden ist, dass auf die Glaubhaftmachung eines berechtigten Interesses als Zugangsvoraussetzung für die Nutzung verzichtet wird und nunmehr jedermann Archivgut nutzen darf.

Die Erhebung personenbezogener Daten in Bezug auf den Nutzer halte ich dennoch weiterhin für zulässig, da die Archivverwaltung weiterhin im Einzelfall prüfen muss, ob Gründe entgegenstehen, die – ausnahmsweise – einer Nutzung durch den – konkreten – Antragsteller entgegenstehen und dem konkreten Antragsteller gegenüber eine Nutzung genehmigt, versagt oder widerrufen werden muss.

Insoweit können sich die Archivverwaltungen auch weiterhin auf den nach wie vor gültigen § 2 SächsArchivBenVO, insbesondere dessen Absatz 2, stützen, der die Erhebung bestimmter personenbezogener Daten des Antragstellers vorsieht.

5.9 Polizei

5.9.1 Keine illegalen Gesprächsaufzeichnungen bei der sächsischen Polizei

Im Berichtszeitraum wurde ich durch Medienberichte auf eine angeblich massenhafte und für Betroffene nicht nachvollziehbare Speicherung von Telefongesprächen bei der Thüringer Polizei aufmerksam. Dort sollten nicht nur Gespräche über die Notrufnummer „110“, sondern auch Telefonate innerhalb von Polizeibehörden und mit externen Teilnehmern, u. a. Rechtsanwälten, Justizbeamten oder Journalisten, aufgezeichnet worden sein. Weiterhin sollten auch heimliche Mitschnitte von Gesprächen in Polizei-

dienststellen möglich gewesen sein. Diese Veröffentlichungen nahm ich zum Anlass einer schriftlichen Kontrolle, ob eventuell ähnliche Gesprächsaufzeichnungen im sächsischen Polizeidienst stattfinden.

In seinem ausführlichen Antwortschreiben teilte mir der Landespolizeipräsident mit, dass in Sachsen die über die Kurzwahl „110“ eingehenden Notrufe automatisch aufgezeichnet würden. Bei Notrufen, welche über eine allgemein bekannte Einwahlrufnummer der örtlichen Polizeidirektion erfolgten, würde die Aufzeichnung des Anrufes manuell durch den Disponenten in der Leitstelle verfügt. Beide Vorgänge würden nach § 43 Abs. 1 SächsPolG i. V. m. der Errichtungsanordnung für den Betrieb von Einsatzleittechnik in den Leitstellen der Polizei Sachsen als zulässig erachtet. Darüber hinaus fände keine Speicherung von Telefonaten statt.

Da diese Regelungen aber aufgrund ihres allgemeinen Charakters für die Aufzeichnung von Notrufen nicht optimal sind, sagte das SMI zu, auf eine gesetzliche Regelung zur Speicherung von Notrufen im Freistaat Sachsen hinzuwirken. Hierauf hatte ich bereits anlässlich früherer Kontrollverfahren hingewiesen. Aus meiner Sicht ist eine spezielle gesetzliche Regelung, auch im Hinblick auf eindeutige Regelungen zur Erhebung, Aufbewahrung und Löschung dieser Daten, sehr zu begrüßen.

Auch zu der Möglichkeit des unbemerkten Abhörens der Raumgespräche hat sich der Polizeipräsident geäußert. Zwar gibt es bei den eingesetzten Telekommunikationsanlagen grundsätzlich die Möglichkeit der Direktannahme von Gesprächen (Leistungsmerkmal „Direktantworten“), wodurch das Mikrofon aktiviert wird und ein Mithören der Gespräche im Raum möglich wäre. Dennoch ist dies nicht mit den angeblichen Umständen in Thüringen vergleichbar. Zum einen ist diese Funktion durch den Mitarbeiter problemlos jederzeit deaktivierbar, zum anderen wird der Umstand, dass das Mikrofon eingeschaltet ist, durch eine leuchtende Lampe am Telefonapparat angezeigt. Um dennoch weitestgehend die Möglichkeit der ungewollten Überwachung durch diese Funktion auszuschließen, werden die Polizisten und Zivilbediensteten in die Funktionsweise dieses Leistungsmerkmals eingewiesen und auf ihr Widerspruchsrecht zur Nutzung dieser Funktion hingewiesen. Ferner ist die Einrichtung des Leistungsmerkmals in Besprechungs- und Aufenthaltsräumen untersagt. Die getroffenen Maßnahmen erschienen mir als geeignet, die ungewollte Aufzeichnung von Gesprächen im Raum wirksam zu verhindern.

Ich habe mithin keine Anhaltspunkte für systematische Datenschutzverletzungen bei der Nutzung von Fernsprechtechnik bei der sächsischen Polizei feststellen können.

5.9.2 Regelanfrage von Gewerbeämtern an die Polizei zu Mitarbeitern im Bewachungsgewerbe

Das LKA Sachsen fragte mich, unter welchen Voraussetzungen kommunale Gewerbeämter Daten zur Zuverlässigkeitsbeurteilung von Personal zur Bewachung von Erstaufnahmeeinrichtungen bei anderen Behörden, insbesondere der Polizei, erheben dürfen.

Hintergrund war der 2015 gestiegene Bedarf an Personal zur Bewachung von Erstaufnahmeeinrichtungen für Asylbewerber. Die zur Bewachung eingesetzten Personen, darunter EU-Ausländer sowie Personen aus den Herkunftsländern der Asylantragsteller, sollten vor ihrem Dienstantritt auf ihre Zuverlässigkeit überprüft werden. Dem LKA Sachsen war die Zuständigkeit für derartige Auskunftsersuchen im Zuge einer Verfahrensvereinheitlichung im Februar 2016 von den Polizeidirektionen übertragen worden.

Die Gesetzeslage stellt sich wie folgt dar: Gemäß § 34a Abs. 4 GewO dürfen nur solche Personen in einem Bewachungsunternehmen beschäftigt werden, die die dafür erforderliche Zuverlässigkeit besitzen. Anhaltspunkte für eine Unzuverlässigkeit sind nach § 34 Abs. 1 Satz 4 GewO etwa die Mitgliedschaft in einem verfassungswidrigen Verein oder einer solchen Partei, die mangelnde wirtschaftliche Leistungsfähigkeit, Steuerschulden, die Verletzung sozialversicherungsrechtlicher Verpflichtungen, die Verurteilung wegen einer gewerbebezogenen Straftat oder die Begehung einer gewerbebezogenen nicht geringfügigen Ordnungswidrigkeit. Nach § 9 Abs. 1 Satz 2 BewachV hat die Behörde zur Überprüfung der Zuverlässigkeit eine unbeschränkte Auskunft nach § 41 Abs. 1 Nr. 9 BZRG einzuholen. Diese umfasst neben den rechtskräftigen Entscheidungen von Strafgerichten, auch bestimmte Entscheidungen von Verwaltungsbehörden sowie unter Umständen auch Suchvermerke. In Frage stand, ob und gegebenenfalls unter welchen Voraussetzungen ein Gewerbeamt zusätzlich nach § 11 GewO befugt ist, weitere Auskünfte, hier aus kriminalpolizeilichen Akten, oder eine Stellungnahme der örtlichen Polizeidirektion zu erheben. § 11 Abs. 1 Satz 1, Satz 2 Nr. 1 GewO erlaubt es, personenbezogene Daten, insbesondere auch solche aus bereits abgeschlossenen oder sonst anhängigen gewerberechtlichen Straf- oder Bußgeldverfahren zu erheben, sofern dies zur Zuverlässigkeitsbeurteilung erforderlich ist.

Ich habe dem LKA mitgeteilt, dass § 11 GewO m. E. als allgemeine Bestimmung neben den speziellen Vorschriften für das Bewachungsgewerbe angewendet werden kann. Damit ist es m. E. zulässig, personenbezogene Daten auch aus Polizeiakten zur Zuverlässigkeitsbeurteilung heranzuziehen. Allerdings erlaubt § 11 GewO keine Regelabfrage, sondern nur eine im begründeten Einzelfall durchzuführende Anfrage.

SMI und SMWA haben daraufhin in gleichgerichteten Erlassen an ihre nachgeordneten Behörden ausdrücklich darauf hingewiesen, dass Abfragen nach § 11 GewO bei der Polizei nur vorgenommen werden dürfen, wenn die Erhebung der Daten zur Beurteilung der Zuverlässigkeit im Einzelfall erforderlich ist. Eine Regelabfrage auf der Grundlage von § 11 GewO ist damit ausgeschlossen.

5.9.3 Veröffentlichung personenbezogener Daten im Facebook-Profil „Polizei Sachsen“

Im Sommer 2015 beschäftigte mich ein Beitrag, der auf dem Facebook-Profil „Polizei Sachsen“ veröffentlicht worden war.

In der Meldung der Polizei wurde über die Aufklärung einer Diebstahlsserie berichtet und mitgeteilt, dass der mutmaßliche Täter gefasst worden sei. Erwähnt wurden das Alter und die Nationalität des Mannes sowie der Umstand, dass dieser kurze Zeit zuvor einen Sportwettbewerb gewonnen habe. Die Kommentare, die von Besuchern des Profils „Polizei Sachsen“ abgegeben wurden, bewegten sich zwischen Unverständnis über die Darstellung der Polizei und offen fremdenfeindlichen Äußerungen. Einem Kommentar, der darauf aufmerksam machte, dass in der Meldung personenbezogene Daten verwendet worden seien, durch deren Zusammenspiel die Identität des Betroffenen offenbart worden sei, widersprach die „Polizei Sachsen“.

Aufgrund der in dem Beitrag genannten Informationen war es allerdings in der Tat möglich, durch eine oberflächliche Internetrecherche binnen weniger Minuten die Identität des Mannes festzustellen. Es handelte sich daher zweifelsohne um die Veröffentlichung personenbezogener Daten. Ich richtete unverzüglich ein Schreiben an das SMI, das für das Facebook-Profil „Polizei Sachsen“ verantwortlich zeichnet, und bat um eine rasche Löschung des Beitrages nebst Kommentaren. Dieser Bitte kam das Ministerium umgehend nach.

In der Auswertung des Vorgangs teilte das SMI mit, dass es meine Auffassung, es habe sich um eine rechtswidrige Veröffentlichung personenbezogener Daten gehandelt, teile und die Mitarbeiter der polizeilichen Pressestellen in Zukunft weitergehend belehren werde, um datenschutzrechtliche Verstöße dieser Art zu vermeiden.

Wegen der Erheblichkeit des Verstoßes gegen datenschutzrechtliche Vorschriften habe ich die ohne Rechtsgrundlage erfolgte Veröffentlichung personenbezogener Daten aus einem laufenden Ermittlungsverfahren förmlich beanstandet. Besonders bemerkenswert an dem Vorfall war der Umstand, dass die Polizei nach langen Gesprächen über die Nutzung von Facebook für Zwecke der Öffentlichkeitsarbeit eigentlich sensibilisiert

war für die Gefahren und Risiken bei Aktivitäten in sozialen Netzwerken, insbesondere bei einem notorischen Datenschutzignoranten wie Facebook. In den Datenschutzhinweisen des Facebook-Profils „Polizei Sachsen“ selbst wird zutreffend darauf hingewiesen, dass nicht ersichtlich sei, in welchem Umfang, an welchem Ort und für welche Dauer die Daten gespeichert würden, inwieweit Facebook bestehenden Löschungspflichten nachkomme, welche Auswertungen und Verknüpfungen mit den Daten vorgenommen würden und an wen die Daten weitergegeben würden, was im Ergebnis auch der Grund dafür ist, dass die sächsische Polizei von Fahndungsaufrufen auf Facebook absieht.

Ich hoffe – gemeinsam mit dem SMI –, dass sich eine Veröffentlichung personenbezogener Daten auf Facebook durch die sächsische Polizei nicht wiederholen wird.

5.9.4 Wie weiter mit Daten mit theoretisch möglichem NSU-Bezug?

Das LKA Sachsen bat mich im Berichtszeitraum um Beratung zu den im Polizeibereich vorhandenen, gesetzmäßig mittlerweile zu löschenden, aber seit 2011 auf Bitten des 1. Untersuchungsausschuss („Neonazistische Terrornetzwerke in Sachsen“) des Landtages nicht gelöschten Daten und nicht vernichteten Akten, die in irgendeinem Zusammenhang mit dem „Nationalsozialistischen Untergrund“ (NSU) stehen könnten. Mitte 2012 habe die Polizei dazu ein erstes Löschmoratorium beschlossen, das seitdem ständig verlängert worden sei. Nach diesem sollen personenbezogene Daten und Unterlagen von Personen, die in Verbindung mit dem NSU stehen könnten, mit einem Sperrvermerk versehen werden. Ein solcher Sperrvermerk verhindere die Löschung der Einträge im „Polizeilichen Auskunftssystem Sachsen“ („PASS“) und die Vernichtung der Papierakten, obwohl dies gemäß § 49 SächsPolG i. V. m. § 20 SächsDSG nach bestimmten Kriterien (Zeitablauf, weitere Relevanz für die polizeiliche Aufgabenerfüllung) zu geschehen habe. Bei diesen Datensätzen sei zum Teil unklar, ob auch nur theoretisch Bezüge zum NSU bestünden und sie für die Arbeit des Untersuchungsausschuss auch nur von theoretischer Relevanz sein könnten. Das LKA teilte mir u. a. weiter mit, dass die Unterlagen auch bei den Justizbehörden vorhanden sind.

Das LKA habe, was den im PASS gespeicherten, zu löschenden, jedoch automatisiert durch Sperrvermerk gesicherten Datenbestand angeht, ein Verfahren zur Migration dieser Daten in eine separierte, in sich abgeschlossene Datei entwickelt. Damit wären Zugriffsmöglichkeiten auf so wenig wie möglich Personen beschränkt. Gleichzeitig könnten die Daten in PASS endlich gelöscht werden.

Des Weiteren habe das LKA, was die Papierakten angeht, organisiert, dass, sobald in PASS eine Löschung verfügt wird, automatisch eine Mitteilung an die aktenführende

Stelle (z. B. den mit der Sache befassten Sachbearbeiter im Polizeirevier) zur Vernichtung der Papierakte geht. Mit der Löschung aus PASS würden somit auch die Papierakten vernichtet werden. Zwischen den elektronischen Akten und den Papierakten sei aber keine vollkommene Übereinstimmung gegeben. Auch die bei den Justizbehörden vorhandenen Akten, die nach Zusicherung des SMJus im Hinblick auf eine eventuelle Anforderung durch den Untersuchungsausschuss noch vorgehalten würden, seien nicht völlig deckungsgleich mit den Ermittlungsakten der Polizei. Ein manueller Abgleich der Unterlagen sei aufgrund des Umfangs der Daten und Unterlagen aus organisatorischer und personeller Sicht nicht möglich.

Ich habe dem LKA mitgeteilt, dass das Löschmoratorium rechtlich umso prekärer wird, je mehr Zeit seit dem Zeitpunkt der Löschungsverpflichtung abläuft. Zusammen mit dem Untersuchungsausschuss, dem SMI und dem SMJus werde ich über das weitere Vorgehen beraten.

5.9.5 Inanspruchnahme von Medien zur Öffentlichkeitsfahndung nach Personen

Nach Maßgabe bundeseinheitlicher Richtlinien muss der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz auch bei der Öffentlichkeitsfahndung nach Personen beachtet werden. Danach hat die Polizei stets zu prüfen, ob zunächst Medien von geringer Breitenwirkung, z. B. eine nur lokal verbreitete Zeitung, in Anspruch genommen werden können. Nach geltender Erlasslage in Sachsen beginnt daher die Öffentlichkeitsfahndung nach einer Person regelmäßig mit der Veröffentlichung von Fahndungsinformationen in den regionalen Printmedien. Entscheidend dafür, welches Veröffentlichungsmedium durch die Polizei gewählt wird, sind die Umstände des Einzelfalls. Nach einem regional tätigen Täter muss nicht überregional gefahndet werden. Die gleichzeitige Veröffentlichung durch die Medien in deren Online-Diensten ist durch die Polizei grundsätzlich zu untersagen, da dies eine zu einem solch frühen Zeitpunkt noch nicht zulässige Internetfahndung darstellte.

Im Berichtszeitraum ist es nun wiederholt vorgekommen, dass sich bestimmte Zeitungen nicht an die Vorgaben der Polizeidirektionen bzw. an die zugrundeliegenden richterlichen Beschlüsse, die Veröffentlichung von Fahndungsaufrufen zunächst auf lokale Printmedien zu beschränken, hielten, und stattdessen die Fahndungsinformationen unverzüglich auf ihren (überregional, ja weltweit abrufbaren) Internetseiten und Facebook-Profilen veröffentlichten. Dies unterläuft die entsprechenden Festlegungen zur Inanspruchnahme von Publikationsorganen und die Nutzung des Internets zur Öffentlichkeitsfahndung und entsprechende sächsische Verwaltungsvorschriften.

Das SMI hat sich von Anfang an offen für die Lösung des Problems gezeigt. Ich habe zahlreiche Gespräche mit den Vertretern des SMI sowie zusammen mit diesen mit Pressevertretern geführt und dabei mögliche Lösungswege erörtert. Insbesondere habe ich der Polizei vorgeschlagen, Zeitungen, die sich in der Vergangenheit nicht an entsprechende Vorgaben gehalten haben, von der Verteilerliste zu nehmen. Ich halte dies für presserechtlich gerechtfertigt und rechtsstaatlich geboten. Leider konnte sich das SMI – mit aus seiner Sicht nicht abwegigen Argumenten – meiner Sichtweise bisher nicht anschließen.

Ich bleibe bei meiner Bitte, die Einrichtung von getrennten Verteilern für allgemeine polizeiliche Presseinformationen und Öffentlichkeitsfahndungen ernsthaft zu prüfen, wenn die Praxis einzelner Printmedien, die Fahndungsersuchen unmittelbar auch auf ihren Webseiten und in sozialen Netzwerken im Internet zu veröffentlichen, fortgeführt wird.

5.10 Verfassungsschutz

5.10.1 Rechtswidrige Datenübermittlungen zwischen LfV und einer sächsischen Hochschule und einer sächsischen Forschungseinrichtung

Im Berichtszeitraum wandte sich ein Petent an mich, der vermutete, dass Mitteilungen des LfV an zwei seiner früheren Arbeitgeber zur Beendigung des jeweiligen Beschäftigungsverhältnisses geführt hätten. Gewissheit hatte er in dieser Frage auch nicht über ein Auskunftsersuchen nach § 9 SächsVSG erlangen können, auf welches hin ihn das LfV zwar über bestimmte Speicherungen informiert hatte, in dem Übermittlungen an andere Stellen aber nicht erwähnt worden waren.

Im Laufe meiner datenschutzrechtlichen Kontrolle bestätigte mir das LfV, dass es in der Vergangenheit Kontakte zu den beiden zeitweiligen Beschäftigungsstellen des Petenten gehabt und dabei Auskünfte über ihn übermittelt hatte. Bei den Stellen handelte es sich um eine sächsische Hochschule (öffentliche Stelle) und eine nicht-öffentliche Forschungseinrichtung (nicht-öffentliche Stelle). Während Speicherungen zum Petenten durch das LfV gesetzlich gedeckt und nicht zu beanstanden waren, musste ich hinsichtlich der Übermittlungen Versäumnisse und Gesetzesverstöße feststellen, die zu handfesten, existenziell bedrohlichen Konsequenzen für den Petenten führten, ohne dass er irgendwann in die Lage versetzt worden wäre, Rechtsschutz erlangen zu können. Die mündlichen Übermittlungen fanden in den Jahren 2009, 2010 und 2012 statt.

Sachverhalt und datenschutzrechtliche Prüfung stellten sich mir wie folgt dar:

Einige Monate nach zwei Gesprächen zwischen der Hochschulleitung und dem LfV hatte sich die Hochschule mit einem schriftlichen Mitwirkungsersuchen (§ 2 Abs. 2 Nr. 4 SächsVSG) an das LfV gewandt, über die bevorstehende Entscheidung über die Weiterbeschäftigung des Petenten informiert und um schriftliche Mitteilung evtl. entgegenstehender Gründe gebeten. Das Gesetz setzt in derartigen Fällen voraus, dass der Betroffene über Zweck und Verfahren der Überprüfung einschließlich der Verarbeitung der erhobenen Daten durch die anfragende Stelle unterrichtet wird (§ 2 Abs. 3 Satz 1 SächsVSG). Tatsächlich wurde der Petent jedoch in keiner Weise informiert – weder unterrichtete die Hochschule ihn von ihrem Ersuchen an das LfV noch vergewisserte sich das LfV über das Vorliegen der gesetzlich geforderten Unterrichtung. Die auf das Ersuchen der Hochschule folgenden Gespräche zwischen Hochschulleitung und LfV fanden vertraulich statt. Das LfV übermittelte dabei seine Erkenntnisse weder schriftlich – die Dienstvorschrift bestimmte die schriftliche Übermittlung aber als Regelfall und die Hochschule hatte um schriftliche Antwort gebeten – noch dokumentierte es die Besprechungen mit der von der Dienstvorschrift bestimmten Genauigkeit.

Das LfV teilte mir dazu mit, dass das Mitwirkungsersuchen der Hochschule seinerzeit nicht als solches erkannt worden sei und räumte Ungenauigkeiten bei der Dokumentation ein; im Übrigen seien die Übermittlungen an die Hochschulleitung aber gesetzlich gedeckt gewesen.

Nach einigen Gesprächen zwischen der Hochschulleitung und dem LfV wurde dem Petenten – nach anderslautenden Signalen im Vorfeld für ihn überraschend – mitgeteilt, dass seine Weiterbeschäftigung an der Hochschule nicht möglich sei. Sein Arbeitsplatz war dahin. Der Petent zog mit seiner Familie daraufhin in eine andere sächsische Stadt und fand eine Stelle in einer nicht-öffentlich organisierten Forschungseinrichtung. Allerdings wurde dem LfV seine neue Anstellung bekannt. Es teilte der dortigen Leitung daraufhin mit, weshalb der Petent an der Hochschule nicht mehr weiterbeschäftigt worden war. Auch diese Übermittlung erfolgte nicht schriftlich; auch sie wurde nicht in dem Maße dokumentiert, wie es die Dienstvorschrift erfordert hätte. Etwa einen Monat nach dem Gespräch zwischen dem LfV und der Forschungseinrichtung meldete letztere telefonisch an das LfV, dass das Beschäftigungsverhältnis mit dem Petenten beendet worden sei.

In der datenschutzrechtlichen Kontrolle räumte das LfV ein, dass es irrtümlich davon ausgegangen sei, dass die Forschungseinrichtung eine öffentliche Stelle im Sinne des § 12 Abs. 1 SächsVSG gewesen sei. Tatsächlich aber handelte es sich um eine nicht-öffentliche Stelle. Die gesetzlichen Voraussetzungen für eine Übermittlung personenbe-

zogener Daten an eine nicht-öffentliche Stelle nach § 12 Abs. 3 SächsVSG hätten allerdings nicht vorgelegen, weshalb diese Übermittlung ohne Rechtsgrundlage erfolgt sei.

Ich habe das LfV wegen der aus meiner Sicht – und zumindest teilweise mit der Auffassung des LfV übereinstimmenden Einschätzung – rechtswidrigen Übermittlungen von Angaben über den Petenten an die Hochschule und die Forschungseinrichtung förmlich beanstandet. Den Petenten habe ich, nicht ohne das LfV zuvor darüber zu informieren, von den Übermittlungen und meiner rechtlichen Bewertung des Vorgehens des LfV unterrichtet.

Das LfV sagte zu, Übermittlungen des LfV aus den letzten Jahren an Hochschulen und nicht-öffentliche Stellen zu überprüfen.

Einen unerwarteten Verlauf nahm das mit der Beanstandung eigentlich abgeschlossene Kontrollverfahren mit der Stellungnahme des SMI, das als oberste Aufsichtsbehörde über das LfV Adressat der förmlichen Beanstandung nach § 29 SächsDSG gewesen war. Differenzen in der Bewertung von objektiven Versäumnissen und Verfahrensfehlern durch das LfV konnten bis zuletzt nicht ausgeräumt werden. Hinweise aus dem Ministerium auf die Bedeutung des Informationsaustausches zwischen dem LfV und anderen staatlichen Stellen sowie darauf, dass es notwendig sei, „dass das LfV Sachsen als verlässlicher und vertrauensvoller Gesprächspartner auftritt“ geben Anlass, auf Folgendes hinzuweisen. Eine enge Ausrichtung an Recht und Gesetz bei der Wahrnehmung fachaufsichtlicher Aufgaben ist vor allem und gerade im Bereich oftmals verdeckter (Grund-)Rechtseingriffe von rechtsstaatlich elementarer Bedeutung. Voraussetzungen, unter denen personenbezogene Daten verarbeitet, insbesondere übermittelt werden dürfen, werden allein durch das Gesetz bestimmt. Es ist zwar zutreffend, dass insbesondere der Austausch zwischen den Nachrichtendiensten und mit Sicherheitsbehörden zwingend erforderlich ist. Je weiter aber (öffentliche) Stellen als Empfänger personenbezogener Daten, die das LfV übermittelt, vom Aufgabenbereich des Schutzes der inneren Sicherheit entfernt sind, desto größer muss die Zurückhaltung der Verfassungsschutzbehörden hinsichtlich der Weitergabe personenbezogener Daten an diese Stellen sein. Der Grund hierfür liegt in dem enormen Missverhältnis zwischen möglichen Konsequenzen der Übermittlung für den Betroffenen einerseits und andererseits der fehlenden Möglichkeit, Rechtsschutz zu erlangen, da der Betroffene regelmäßig nicht über solche Übermittlungen informiert wird.

Die mittlerweile abgeschlossene Prüfung von Übermittlungen an Hochschulen und nicht-öffentliche Stellen durch das LfV in den letzten Jahren ergab, dass solche Informationen relativ selten vorgenommen worden waren. Zwar erschien auch in anderen Fällen die Dokumentation der Übermittlungen verbesserungswürdig, Regelverletzungen

in einem Ausmaß wie im hier vorgestellten Fall seien aber nicht noch einmal festgestellt worden. Meine stichprobenhafte Prüfung bestätigte diesen Befund.

Das LfV nahm den Fall zum Anlass, Änderungen an der einschlägigen Dienstvorschrift vorzunehmen, die das Risiko von Fehlern bei der Übermittlung personenbezogener Daten weiter reduzieren sollen.

5.11 E-Government

In diesem Jahr nicht belegt.

5.12 Landessystemkonzept / Landesnetz

5.12.1 Grundverschlüsselung - der neue Normalfall

Das Sächsische Verwaltungsnetzwerk (SVN) erbringt seit Jahren einen ganzen Katalog an Leistungen für die sächsische Landesverwaltung und die kommunalen Einrichtungen. Dabei wurde seitens der Verantwortlichen gern – auch um den Unterschied zur Zeit vor dem SVN herauszustellen – auf Veranstaltungen und in Präsentationen der Satz gebraucht: „Das SVN ist sicher“.

Nun ist Sicherheit ohnehin ein relativer Begriff, der immer einer weitergehenden Erläuterung bedarf. Allzu oft ist diese Aussage leider missverstanden worden und hat in der Folge dazu geführt, dass Verfahrensverantwortliche die eigenen technischen und organisatorischen Maßnahmen nicht mit der gebotenen Sorgfalt ausgestaltet haben.

Sicherheit im bisherigen SVN war vor allem dadurch ausgeprägt, dass sich abgeschlossene Benutzergruppen bilden konnten (Landes- und Kommunalverwaltung), zwischen denen definierte verfahrenstechnische Übergänge oder insgesamt Übergänge in Verfahren des Bundes sowie für alle ein gesicherter Zugang zum Internet bereitgestellt wurde. Darüber hinaus waren Leistungen im SVN vor allem durch „Service Level Agreements“ (SLA) gesicherte Leistungen, die vor allem der *Ausfall*sicherheit zuzurechnen sind und im Sinne einer Schutzzielbetrachtung nach § 9 SächsDSG dem Schutzziel *Verfügbarkeit* unterfallen.

Auch wenn das Angriffs- und Schadpotential durch klare Begrenzung der Benutzergruppen deutlich reduziert werden konnte, stellt dies allein keine angemessene Maßnahme dar, um zum Beispiel dem Schutzziel der Vertraulichkeit bei Übertragung oder Verarbeitung besonders schutzwürdiger personenbezogener Daten zu genügen. Seitens der SVN-Verantwortlichen wurde dazu auch immer wieder darauf hingewiesen, dass höhere Anforderungen innerhalb von Fachverfahren durch eigene – zusätzliche – Maß-

nahmen umgesetzt werden müssen. Dies ist bei manchen Entscheidern nicht immer in der Klarheit angekommen oder in der Praxis umgesetzt worden, wenn allein der oben zitierte Satz zur Sicherheit im SVN als Maßstab herangezogen wurde.

So ergaben sich im Berichtszeitraum immer wieder Fälle, in denen unzulässiger Weise sensitive Daten unverschlüsselt (z. B. per E-Mail) übertragen wurden.

Wenn hierzu im Bereich E-Mail-Übertragung im Berichtszeitraum in Teilbereichen der sächsischen Verwaltung ein Fortschritt erreicht werden konnte, ist dies ausschließlich der eingesetzten Software zu verdanken, mit der für den Versand von Nachrichten von Server zu Server eine so genannte Transport-Verschlüsselung per Standard Einzug gehalten hat. Das erlaubt aufgrund anderer fortbestehender Risiken zwar dennoch nicht grundsätzlich den Versand besonders schutzwürdiger personenbezogener Daten per E-Mail, hebt aber dennoch das Schutzniveau für E-Mails zwischen Einrichtungen der sächsischen Landesverwaltung an. Hierzu zahlt sich auch aus, dass in der Landesverwaltung frühzeitig auf Verfahrensvereinheitlichung gesetzt wurde, wodurch sich gleichzeitig in der Kommunalverwaltung ein wesentlich weniger homogenes Bild ergibt.

Grundsätzlich obliegt die Gewährleistung der Vertraulichkeit (wie auch der anderen Schutzziele nach § 9 SächsDSG) immer den Verfahrensverantwortlichen, also nicht automatisch dem SVN bzw. seinen Betreibern. Unter meiner Mitwirkung wurde im Zuge der Neuausschreibung des Nachfolgers (SVN2) besonderes Augenmerk darauf gelegt, das Grundniveau der Vertraulichkeit deutlich anzuheben. Erfreulicherweise ist es gelungen, diese sog. Grundverschlüsselung zwischen Behördenstandorten als wesentlichen Eckpunkt des neuen Verwaltungsnetzwerkes festzuschreiben. Auch wenn in darüberhinausgehenden Fällen, in denen es eine direkte Verschlüsselung zwischen zwei Kommunikationsteilnehmern erforderlich macht, auch weiterhin zusätzliche Schutzmaßnahmen unabdingbar sind (z. B. die Inhaltsverschlüsselung / Ende-zu-Ende-Verschlüsselung), werden von dieser nun beschlossenen Grundverschlüsselung alle Verwaltungsverfahren ganz grundsätzlich profitieren, wenn die Gewährleistung der Vertraulichkeit von Behördengrenze zu Behördengrenze als ausreichend betrachtet wird.

5.13 Ausländerwesen

In diesem Jahr nicht belegt.

5.14 Wahlrecht

In diesem Jahr nicht belegt.

6 Finanzen

6.1 Einsatz privater Speichermedien (Handy) bei der Sachverhaltsaufklärung

Im Berichtszeitraum wandte sich ein Petent mit dem Vortrag an mich, dass sein zuständiges Finanzamt ihm die Aufwendungen für sein dienstlich genutztes Telefon nur zur Hälfte anerkannt habe. Zum Beleg fügte der Petent eine Kopie des Schreibens des Sachbearbeiters des Finanzamts bei, in dem wörtlich geschrieben stand:

„*6. Darüber hinaus werden die Aufwendungen für das dienstlich genutzte Telefon trotz Arbeitgeberbescheinigung nur zu 50 % anerkannt, weil nur für diese Nummer ein WhatsApp-Konto besteht. Auf diesem WhatsApp-Konto wurde als Profilbild ein Foto Ihres Kindes verwendet. Allein dies spricht gegen eine allein ausschließlich dienstliche Verwendung des Telefons. Zudem waren auch am Wochenende Online-Zeiten zu verzeichnen. Erfahrungsgemäß wird ein WhatsApp-Konto sogar zumeist für private Kommunikation verwendet.*“

Auf meine Ermittlungen hin teilte mir das Finanzamt mit, dass der zuständige Bedienstete mittels seines privaten Mobiltelefons und in der WhatsApp-Kontakte-Datei des Bediensteten Ermittlungen zu dem Steuerpflichtigen angestellt habe.

Ich habe daraufhin dem Finanzamt mitgeteilt, dass ich die Benutzung privater Mobiltelefone zu dienstlichen Zwecken unter Verarbeitung personenbezogener Daten von Steuerpflichtigen als problematisch ansehe. Für die (auch nur vorübergehende) Speicherung der Daten des Petenten im Nummernverzeichnis des privaten Mobiltelefons und in der WhatsApp-Kontakte-Datei des Bediensteten ist die erforderliche gesetzliche Grundlage nicht ersichtlich. Auch stellt sich – unabhängig vom Einzelfall – die Frage, wie gewährleistet werden kann, dass die Daten Steuerpflichtiger nach Erfüllung der Aufgabe, hier der Sachverhaltsermittlung gemäß § 88 AO, wieder gelöscht werden. Unter Löschung ist die rückstandsfreie nicht-mehr-Zuordenbarkeit der personenbezogenen Daten des Steuerpflichtigen in einem Speichermedium zu verstehen.

Die Verarbeitung personenbezogener Daten durch öffentliche Stellen stellt nach völlig herrschender Auffassung, u. a. des Bundesverfassungsgerichts und des Bundesfinanzhofs, einen Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG; Art. 33 SächsVerf) dar, die in jedem Fall einer Rechtsvorschrift oder der Einwilligung des Betroffenen als Grundlage bedarf. Selbst wenn man – was ich nicht tue – hier § 88 AO als gesetzliche Rechtsgrundlage für die Verarbeitung, hier: Speicherung, der personenbezogenen Daten des Petenten in dem privaten

Mobiltelefon des Bediensteten ansähe, wären Anlass, Art und Ausmaß solcher Speicherungen regelungsbedürftig. Eine Regelung, etwa durch Verwaltungsvorschrift, unter welchen Voraussetzungen private Sachmittel zur Sachverhaltsaufklärung genutzt werden dürfen, ist jedoch, soweit mir ersichtlich, nicht vorhanden. Damit bleibt insbesondere die Frage offen, nach welcher Zeit dort eingespeicherte personenbezogene Daten von Steuerpflichtigen wieder gelöscht werden und wie dies kontrolliert werden kann.

Ferner und lediglich ergänzend halte ich die Nutzung privater Sachmittel, die über mehr und andere Merkmale als die dienstlich bereitgestellten Sachmittel verfügen, im Hinblick auf die damit verbundene Umgehung des Willens des Haushaltsgesetzgebers für problematisch.

Aus alledem folgte, dass ich das Finanzamt aufgefordert habe, ab dem 1. Mai 2016 keine privaten Speichermedien wie Smartphones etc. zur Sachverhaltsaufklärung mehr einzusetzen. Da ich annehmen musste, dass die hier kritisierte Vorgehensweise auch in anderen Finanzämtern des Freistaates Sachsen praktiziert wird, habe ich dem Finanzamt anheimgestellt, das LSF und eventuell das SMF einzubeziehen.

Das LSF hat mir daraufhin bestätigt, dass in dem betreffenden Finanzamt ab dem 1. Mai 2016 keine privaten Speichermedien zur Sachverhaltsaufklärung mehr eingesetzt werden. Es sei veranlasst worden, dass sämtliche personenbezogenen Daten des Petenten einschließlich seines Profilbilds auf dem privaten Mobiltelefon des zuständigen Bediensteten vollständig gelöscht worden sind. Der Fall sei außerdem zum Anlass genommen worden, sämtliche sächsischen Finanzämter nochmals darauf hinzuweisen, dass keine privaten Speichermedien zur Sachverhaltsaufklärung eingesetzt werden dürfen. Insofern ist mir eine interne Anweisung des LSF vorgelegt worden.

Aus diesen Gründen durfte ich davon ausgehen, dass eine Wiederholung eines solchen Falles künftig ausgeschlossen ist. Ich habe daher von einer förmlichen Beanstandung des SMF abgesehen.

7 Kultus

7.1 Datenschutz als ein Teil der Medienbildung und Digitalisierung in der Schule

Eine gelungene Medienbildung soll die Schüler dazu in die Lage versetzen, mit den Herausforderungen der modernen Medien kompetent umzugehen, auch um die Gefahren, die durch deren Nutzung entstehen können, möglichst überschaubar zu halten. Datenschutz ist ein Bestandteil dieser Bildungsaufgabe.

Bereits im letzten Tätigkeitsbericht beschäftigte ich mich mit diesem Thema. Im aktuellen Berichtszeitraum unterstützte ich das für Medienbildung zuständige Referat des SMK bei der Erstellung der Konzeption „Medienbildung und Digitalisierung in der Schule“. Bildung zu digitalen Medien ist eine Herausforderung, die ein abgestimmtes und koordiniertes Handeln aller Akteure dieses Themenfeldes erfordert. Es freut mich daher, dass das zuständige Ressort als eine Grundlage des Konzeptes den Bericht der AG Digitale Medien des Landespräventionsrates zu Grunde gelegt hat, vgl., 4.1.

Mit diesem Konzept erfolgen die pädagogischen, didaktischen und technisch-infrastrukturellen Festlegungen der schulischen Bildung zu digitalen Medien.

Das für mich vorrangige Thema Datenschutz als Teil der Medienbildung berührt die Lehrkräfte hierbei in zweierlei Hinsicht. Zum einen nutzen die Lehrer digitale Medien als didaktisches Mittel. In dieser Rolle ist der Lehrer als Teil einer öffentlichen Stelle an die sächsischen Gesetze, Verordnungen und Verwaltungsvorschriften gebunden. In einer zweiten ebenso wichtigen Funktion ist die Lehrkraft als „Befähiger“ der Schüler zur Nutzung digitaler Medien tätig. In diesem Bereich beschäftigt er sich z. B. mit der Lebenswirklichkeit der Schüler und den Wirkmechanismen des Internets. Beide Rollen setzen bei Lehrern jedoch gänzlich unterschiedliches datenschutzrechtliches Wissen voraus. Um Lehrer und Schüler in die Lage zu versetzen, selbstbestimmt, kritisch und verantwortungsbewusst die digitalen Medien zu nutzen, ist Datenschutz als ein Teil der Medienbildung sowohl für Schüler als auch für Lehrer verbindlich, nachhaltig und systematisch in den Bildungsgang zu integrieren.

Vor dem Hintergrund der nach meiner Überzeugung ansonsten nicht zureichenden Berücksichtigung medienpädagogischer Inhalte in Aus- und Fortbildung der pädagogischen Fachkräfte und der fehlenden Vermittlung medienpädagogischer Grundlagen in den entsprechenden Studiengängen, stimmt es mich einigermaßen optimistisch, dass im Berichtszeitraum eine gute Zusammenarbeit meiner Behörde mit der TU Dresden, der Professur für Didaktik der Informatik der Fakultät Informatik und der Professur für

Medienpädagogik der Fakultät Erziehungswissenschaften, entstehen konnte. Dabei fanden medienpädagogische und datenschutzrechtliche Aus- und Weiterbildungen von Lehramts-Studenten und Teilnehmern im berufsbegleitenden Studium statt.

Ich hoffe, dass die Kooperation mit der Technischen Universität weiter ausgebaut wird und die Inhalte zukünftig auch den Studenten anderer pädagogischer Studiengänge, auch an anderen Hochschuleinrichtungen, zugänglich gemacht werden.

Um die sächsischen Schüler auf die persönlichen und beruflichen Anforderungen unserer digital geprägten Zeit gut vorzubereiten, ist die Vermittlung einer umfassenden Medienbildung erforderlich. Diese geht mit dem Einsatz und der Nutzung moderner Medien im Unterricht einher. Im Berichtszeitraum fanden zu diesen Fragen Vorträge und Seminare statt. Die Schule bleibt auch bei der Nutzung moderner Lernmedien verantwortliche Stelle für die Datenverarbeitung und -nutzung. Hinsichtlich der Fragen des Schuldatenschutzes bestehen oft erhebliche Unsicherheiten. Die Lehrer müssen die datenschutzrechtlichen Möglichkeiten und Grenzen der Nutzung der modernen Medien im Unterricht kennen, um zu erkennen, wie der Einsatz im Unterricht datenschutzkonform erfolgen kann. Die Begründung und der Ausbau schuldatenschutzrechtlicher Aus- und Fortbildungsangebote ist in diesem Zusammenhang ein anzustrebendes Ziel.

Nicht weniger notwendig ist, neben der Vermittlung der Schuldatenschutzinhalte, die Ausbildung von Lehrern und Lehramtsanwärtern zu der Frage, wie Schülern die Themen des Datenschutzes erfolgreich vermittelt werden können. Zu diesem Thema wurde anlässlich einer Veranstaltung zum 23. Sächsischen Schulinformatiktag an der Fakultät Informatik der TU Dresden referiert. Ziel ist dabei, die Schüler in Sachsen auf die persönlichen und beruflichen Anforderungen des Informationszeitalters vorzubereiten. Datenschutz aus technischer und rechtlicher Sicht bietet eine Vielzahl an Möglichkeiten für Schüler, sich inhaltlich auseinanderzusetzen. Datenschutz als Bildungsaufgabe bedeutet, neben verfassungsrechtlichen Fragestellungen, die Vermittlung von Funktionsbedingungen des digitalen Zeitalters und eine Sensibilisierung für die Risiken und die Möglichkeiten, sich sicherheitstechnisch selbst behelfen zu können. Am Ende sollte Schülern bewusst sein, in Bezug auf neue Medien nicht nur über Rechte und Möglichkeiten zu verfügen, sondern auch über Pflichten. Und sie sollten die Erkenntnis gewinnen, dass es ein Gewinn für alle ist, rücksichtsvoll und respektvoll mit personenbezogenen Daten und Bildern anderer umzugehen.

Auch zu diesem Thema sollten den Lehrern verstärkt Aus- und Fortbildungsangebote offeriert werden.

7.2 Fragebögen im Unterricht

Im Berichtszeitraum wandten sich besorgte Eltern mit der Bitte an mich, die Zulässigkeit eines im Unterricht verwendeten Fragebogens datenschutzrechtlich zu überprüfen.

Hintergrund der Anfrage war, dass einem Schüler der vierten Klasse von der Klassenleiterin ein Fragebogen mit dem Titel „Weiterführende Schule“ zur Beantwortung vorgelegt worden ist. Im Fragebogen wurde unter anderem abgefragt, auf welche Schule das Kind gern gehen würde und weshalb dieser Wunsch bestünde. Anstoß nahmen die anfragenden Eltern an den Fragen „Meine Eltern wünschen sich für mich diese Schule.“, „Weißt Du, warum sie sich das wünschen? Wenn ja, warum?“, „So fühle ich mich, wenn ich an die weiterführende Schule denke:“ und „Darauf freue ich mich/habe ich vielleicht Angst:“.

Für die anfragenden Eltern war es nicht nachvollziehbar, in welchem Zusammenhang die genannten Fragen in einem Arbeitsblatt der Klassenstufe 4 mit der Umsetzung des Bildungs- und Erziehungsauftrages der Grundschule bzw. der Erfüllung des Lehrplanes stehen.

Da von der Schule hierzu keine überzeugenden Antworten gegeben worden seien, vertraten die Eltern die Auffassung, dass derartige an 10-jährige Schüler gerichtete Fragen lediglich den Zweck verfolgten, über die Schüler „Gesinnungsschnüffelei“ in Bezug auf das Elternhaus zu betreiben.

Ich prüfte diesen Vorgang, konnte jedoch keinen Datenschutzverstoß festzustellen.

Im schulischen Bereich erfolgt die Verarbeitung personenbezogener Daten zum Zwecke der Schulverwaltung oder zur Umsetzung des Bildungs- und Erziehungsauftrages der Grundschule.

Unterricht findet dialogisch statt. Dabei werden vielfältige personenbezogene Informationen zu einzelnen Schülern im Unterricht von Lehrern und Mitschülern miterfasst. Ein kommunikativer Gedankenaustausch bewegt sich im Rahmen eines pädagogisch notwendigen und auch rechtlich anerkannten schulischen Spielraums bei der Erziehung, Unterrichtsgestaltung und Leistungsbewertungen der Schüler. Dass hierbei auch häufig persönlichkeitsrechtsrelevante Informationen offenbart werden, macht die Informationsflüsse, auch wenn sie personenbezogen sind, nicht datenschutzrechtswidrig, vgl. u. a. die Überlegungen in 17/7.4 zur Bekanntgabe von Noten im Klassenverband. So werden Informationen, auch bei schriftlichen Aufgabenstellungen und Prüfungen in Schulen in ständiger Übung von den Lehrkräften ausgewertet.

Eine Speicherung der Inhalte, das Anlegen von Kopien etc., erfolgt bei dem Unterricht regelmäßig nicht, auch wenn die Beiträge der Schüler zeitweise von den Lehrkräften verwahrt werden sollten, vgl. § 3 Abs. 2 Nr. 1 SächsDSG. Gespeichert werden gegebenenfalls bei den Lehrkräften Auswertungen, Ergebnisse und Leistungseinschätzungen. Die Informationen im vorliegenden Vorgang wurden zum Zweck der unmittelbaren pädagogischen Arbeit der Lehrkraft verarbeitet. Die Schule teilte mir mit, dass sie keine Datensammlung von zusätzlichen Informationen bei der Schulübergangsphase zu den betroffenen Schülern und Elternsorgeberechtigten anlegt und angelegt hat, als die Informationen, die für den Besuch der weiterführenden Schule materiell-gesetzlich vorgesehen sind. Nach Angaben der Schule verblieben die Fragebögen vielmehr im Sachunterrichtsordner der Schüler und wurden auch nicht von der unterrichtenden Lehrkraft im Unterricht eingesammelt.

Personenbezogene Daten wurden seitens der öffentlichen Stelle – bezogen auf den Fragebogen des betroffenen Schülers – damit nicht gespeichert. Begründet worden ist die Unterrichtsmaßnahme als Übung zur Selbstreflexion im Zusammenhang mit dem Schulübergang.

Meine Kontrolle ergab, dass im Lehrplan der 4. Klasse im Unterrichtsfach Sachkunde und dort im Lernbereich 1 „Zusammen leben und lernen“ das Thema „Kennen von Bildungswegen nach Abschluss der Grundschule“ explizit aufgeführt ist. Die Lehrkraft ist nach den Erläuterungen des Lehrplanes dazu angehalten, mit den Schülern Bildungsinteressen, -angebote und -bedingungen abzuwägen und auf die Selbstsicht und -einschätzung der Schüler einzugehen.

Mit dem Lehrplan und den Freiräumen zu dessen Umsetzung, konnten daher die Daten, die die Schullaufbahn und die persönliche Meinungsbildung der Schüler betreffen, im Rahmen eines aufgabenbezogenen Unterrichts grundsätzlich thematisiert werden.

Demzufolge war nicht von einem Datenschutzverstoß auszugehen.

7.3 Digitales Lernen an sächsischen Schulen

Der Einsatz digitaler Lehr- und Lernmedien ist aus dem heutigen Schulalltag nicht mehr wegzudenken. Im Gegenteil: Digitale Medien werden als nützliches Hilfsmittel in der schulischen Praxis künftig weiter an Bedeutung gewinnen.

Die Zwecke des Einsatzes sogenannter Online-Lernmedien an der Schule sind vielfältig. Mit ihnen wird ein einfacher Zugang zu digitalen Lehr- und Lerninhalten ermöglicht und die Lernbegleitung der Schüler erleichtert. Ein reichhaltiges Angebot an digitalen

Inhalten und Anwendungen bieten zahllose Möglichkeiten für eine zeitgemäße Vermittlung des Unterrichtsstoffs.

Didaktische Möglichkeiten und Komfortabilität dürfen allerdings nicht vergessen lassen, dass mit der Nutzung digitaler Lehr- und Lernmedien regelmäßig Schüler- und Lehrerdaten webbasiert verarbeitet werden. Die Systeme stellen zumeist ein Kontingent personalisierter Benutzerkonten zur Verfügung. Schule bzw. der verantwortlichen Lehrkraft wird eine Teiladministration eröffnet, mit der Zugriffsrechte für die einzelnen Nutzer festgelegt und die Funktionalitäten ausgewählt werden können, die im Unterricht genutzt werden sollen, z. B. Lerninhalte, Diskussionsforen oder Übungsaufgaben.

Sei es durch die personalisierte Anmeldung der Nutzer oder der Speicherung des Nutzerverhaltens, es werden hierbei personenbezogene Daten verarbeitet. Gespeichert wird z. B. wann welcher Nutzer auf welche Seite zugegriffen oder ob und mit welchem Ergebnis er sich an einem Test beteiligt hat. Die Nutzung der Lehr- und Lernmedien bedingt wegen des Umfangs, der Tiefe und des Ausmaßes der Datenverarbeitung im Hintergrund auch die Gefahr der Erstellung von Persönlichkeitsprofilen oder angereicherten Informationen über bestimmte Schüler und Lehrkräfte. Daher sind besondere datenschutzrechtliche und -organisatorische Anforderungen vor und während der Nutzung der digitalen Lehr- und Lernmedien zu beachten.

Für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten beim Einsatz digitaler Lehr- und Lernmedien ist die jeweilige Schule als datenverarbeitende Stelle (§ 3 Abs. 3 SächsDSG) zuständig.

Gemäß § 58 Abs. 1 SächsSchulG steht das gesamte Schulwesen in der Verantwortung des Landes Sachsen, welches insbesondere die Schulen berät und unterstützt, die Qualität der Arbeit gewährleistet und die Fach- und Dienstaufsicht sowie die Rechtsaufsicht wahrnimmt. Demgegenüber obliegt den Schulträgern gemäß § 23 Abs. 2 SächsSchulG die sachliche Ausstattung und ordnungsgemäße Unterhaltung. Daraus ergibt sich, dass das Land Sachsen die inhaltliche, pädagogische Ausrichtung einer Schule zu verantworten hat, während der Schulträger die sachliche Ausstattung der jeweiligen Schulgebäude und Schulanlagen sowie deren Organisation gewährleistet. Dient der Einsatz digitaler Lernmedien der Unterstützung der Unterrichtsziele der Schule, wie z. B. dem Erlernen des Lesens, ist dessen Einsatz damit auch dem Verantwortungsbereich der Schule zuzurechnen. Gemäß § 23 SächsSchulG kann der Schulträger zwar für die Anschaffung des Leseprogramms zuständig sein, sollte diese Anschaffung jedoch im Hinblick darauf, dass die Nutzung des Programms unmittelbar mit der Verarbeitung personenbezogener

Daten zu pädagogischen Zwecken verbunden ist, in enger Abstimmung mit der Schule tätigen.

Die Verarbeitung personenbezogener Daten ist zulässig, wenn entweder eine Rechtsvorschrift die Verarbeitung zulässt oder der Betroffene eingewilligt hat, § 4 Abs. 1 SächsDSG. Rechtsgrundlagen für die Verarbeitung personenbezogener Schülerdaten auch in Online-Lernmedien sind zunächst das Schulgesetz und dazu erlassene Schulordnungen (z. B. Schulordnung Grundschulen). Ergänzend dazu kommen z. B. die Verwaltungsvorschrift Schuldatenschutz und das Sächsische Datenschutzgesetz zur Anwendung.

Die verpflichtende Verwendung eines Lehrmediums kann nur durch oder aufgrund Gesetzes vorgeschrieben werden. Eine gesetzliche Grundlage in diesem Sinne liegt derzeit und auch mit der Novelle des Schulgesetzes, welches zum 1. August 2018 in Kraft tritt, nicht vor. Mit § 38b des neuen Schulgesetzes wird E-Learning zwar geregelt, aber lediglich, dass Schüler an allen Schularten bei Vorlage eines von der Schulkonferenz beschlossenen pädagogischen Konzeptes innerhalb und außerhalb der Schule zeitweilig über elektronische Medien und mittels Lern- und Kommunikationsplattformen unterrichtet werden können. E-Learning soll nach Vorstellung des Gesetzgebers Ausnahme bleiben. Satz 2 der Vorschrift legt beispielhaft fest, in welchen besonderen Ausnahmefällen E-Learning genutzt werden kann. Dies sollen die Unterrichtung von Schülern, die längerfristig erkrankt sind, die selbst oder mit ihren Eltern beruflich reisen oder für die Förderung individueller besonderer Begabungen und bei sonderpädagogischem Förderbedarf der Fall sein. Mit der Eingrenzung für E-Learning, besteht für einen flächendeckenden Einsatz außerhalb der genannten oder anderer maßstäblich vergleichbarer Sonderfälle keine Rechtsgrundlage.

Aus diesem Grund und auch weil digitale Lehrmedien zur Aufgabenerfüllung der Schule nicht als zwingend erforderlich anzusehen sind, wären sie datenschutzrechtlich nur auf Grundlage einer freiwillig erteilten Einwilligung zulässig, was gleichzeitig die Schwierigkeit mit sich bringt, dass bei Versagung der Einwilligung eine gleichmäßige Beschulung nicht stattfinden kann und dann wiederum von dem Vorhaben Abstand genommen werden müsste.

Bei der Formulierung der Einwilligung wäre darauf zu achten, dass Betroffene nachvollziehen können, welche personenbezogenen Daten, zu welchem Zweck, in welcher Art und Weise verarbeitet und ggf. an welche weiteren Stellen übermittelt werden, vgl. § 4 Abs. 3 SächsDSG als sogenannter informierten Einwilligung. Für den Fall, dass die Schule die Daten an den Anbieter übermittelt, was auch erfolgen kann, indem die Schule die Stammdaten der Schüler in einem Internetportal anlegt, empfehle ich auch

diese Übermittlung in die Einwilligung mit aufzunehmen. In der Einwilligung ist darüber zu informieren, welche Auswertungsmöglichkeiten die Anwendung bietet und welche Konsequenzen das Nutzerverhalten ggf. haben kann. In der Einwilligung ist ausdrücklich auf deren Freiwilligkeit und das bestehende Widerrufsrecht hinzuweisen. Die Einwilligung ist schriftlich einzuholen. Um die Einwilligung entsprechend den gesetzlichen Vorgaben nach § 4 Abs. 3 bis 5 SächsDSG formulieren zu können, ist es erforderlich, dass die Schule sich mit den Datenverarbeitungsprozessen des Anbieters vertieft auseinander setzt.

Die meisten Online-Lernplattformen funktionieren letztendlich als gemeinsames Verfahren oder als Verbunddatenverarbeitung, bei denen der technische Betrieb über den Anbieter gewährleistet wird. Die Schule ist daher, soweit sie die Informationen über die Online-Lernplattform auswertet und nutzt, für die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich, selbst wenn sie z. B. Stammdaten an den Anbieter und Plattformbetreiber übermittelt, die dieser einspeist oder verwaltet. Verantwortliche datenverarbeitende Stellen haben gemäß § 9 SächsDSG alle angemessenen personellen, technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine den Vorschriften dieses Gesetzes entsprechende Datenverarbeitung zu gewährleisten. Dazu gehört auch, dass Online-Lernangebote mit der gebotenen Sorgfalt im Hinblick auf die Zuverlässigkeit des Anbieters bei der Verarbeitung personenbezogener Daten ausgewählt werden. Die öffentliche Stelle sollte bei der Auswahl des Anbieters u. a. darauf achten, dass dieser den europäischen Datenschutznormen unterfällt. Die schul- und datenschutzrechtlichen Regelungen für die Verarbeitung und Nutzung personenbezogener Daten setzen zudem voraus, dass deren Verarbeitung für die Aufgabenwahrnehmung durch die Schule erforderlich sein muss. Dies gilt für jedes einzelne personenbezogene Datum, welches in dem Lernprogramm verarbeitet wird. Daher ist strikt auf die Grundsätze der Datenvermeidung und Datensparsamkeit und zum Beispiel auch auf die Einhaltung von Löschfristen zu achten.

Regelmäßig werden in den Verfahren unterschiedliche Arten von Daten verarbeitet. Dazu gehören Stammdaten, optionale Daten, Nutzungsdaten und weitere Daten wie pädagogische Prozessdaten (Forendiskussion; Wiki-Einträge; Glossar (Datenbank); Lernobjekte (Aufgaben, Tests) etc.) oder statistische Daten ohne Personenbezug. Viele Online-Lernmedien stellen erheblich mehr Möglichkeiten zur Datenauswertung zur Verfügung, als für die Aufgabenwahrnehmung erforderlich sind. Das Verfahren ist daher so einzurichten, dass ausschließlich die zur Aufgabenerfüllung der Schule erforderlichen Daten erhoben und verarbeitet werden.

Bei dem Einsatz von digitalen Lernmedien ist neben der Verarbeitung von Schülerdaten auch von einer Verarbeitung von Beschäftigtendaten der Bediensteten des Schulträgers und auch der staatlichen Lehrkräfte auszugehen. Eine Dienstvereinbarung zur Beschäftigtendatenverarbeitung gemäß § 37 Abs. 1 SächsDSG sollte abgeschlossen werden, um den Einsatz entsprechender Verfahren normativ abzusichern. Regelungsgegenstand sollten Angaben zu Art, Umfang und Zweck der Datenverarbeitung sein, ebenso wie beschränkende Festlegungen zu Auswertungen der Nutzungsdaten von Lehrkräften.

Nähere Informationen enthält die *Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder für Online-Lernplattformen im Schulunterricht*, die auf meiner Internetpräsenz unter Öffentlicher Bereich/Informationen/Arbeitshilfen abgerufen werden kann.

Je nach vertraglicher Gestaltung des Rechtsverhältnisses zwischen dem Anbieter des Verfahrens und der zuständigen Stelle wird zu entscheiden sein, ob es sich um eine Datenverarbeitung im Auftrag gemäß § 7 SächsDSG handelt oder ob die Nutzung eines Programms, z. B. auf der Grundlage einer Schulträgerlizenz angeschlossenen Schulen bereitgestellt wird. Datenverarbeitung im Auftrag bedeutet, dass eine öffentliche Stelle einen Auftragnehmer mit der Verarbeitung personenbezogener Daten weisungsgebunden beauftragt. Voraussetzung dafür wäre, dass die Schule als verantwortliche Stelle den Inhalt der Daten vorgibt und bestimmt. Dazu müsste sie festlegen, wer die Daten auf welche Weise verarbeitet und nutzt. Sie müsste, gegenüber dem Auftragnehmer ein Weisungsrecht in Bezug auf die Datenverarbeitung und -nutzung haben und sich vertraglich Kontrollrechte einräumen. Nur so wären die Vorgaben zur Regelung der Datenverarbeitung im Auftrag gemäß § 7 SächsDSG einzuhalten. Entsprechend wären die allgemeinen Geschäftsbedingungen externer Dienstleister unter Beachtung der hier dargestellten Grundsätze zu überprüfen und ggf. vertraglich abzuändern. Mit dem Auftragnehmer wäre ein entsprechender Vertrag zu schließen. Die Voraussetzungen der Auftragsdatenverarbeitung bei Lizenzvereinbarungen zur Nutzung einer Schulträgerlizenz sehe ich regelmäßig als nicht gegeben an. Es kommt jedoch auf den Einzelfall an. Auch, soweit allgemeine Geschäftsbedingungen, die die Datenverarbeitung betreffen, als nicht abänderbar vorgegeben werden, wird genau zu prüfen sein, ob die Schule die Datenverarbeitung des Online-Lernangebots bestimmen kann und eine Auftragsdatenverarbeitung zu bejahen ist.

Als verantwortliche Stelle hat die Schule sicherzustellen, dass gemäß § 9 SächsDSG alle angemessenen personellen, technischen und organisatorischen Maßnahmen getroffen werden, die erforderlich sind, um eine ordnungsgemäße Datenverarbeitung zu gewährleisten. Die rechtliche Prüfung der Zulässigkeit des Einsatzes des Verfahrens hat der behördliche Datenschutzbeauftragte der datenverarbeitenden Stelle durchzuführen.

Vor dem Einsatz des digitalen Lehr- und Lernmediums ist dessen vorgesehener Einsatz in einer Nutzerordnung bzw. einer Arbeits- und Dienstanweisung festzulegen. Außerdem sind die Lehrkräfte und Administratoren entsprechend zu schulen und die Schüler entsprechend zu unterweisen. Die von der Schule zu erstellenden Nutzungsbedingungen, das Verfahrensverzeichnis und die sonstigen getroffenen technischen und organisatorischen Maßnahmen unterliegen der datenschutzrechtlichen Prüfung des Datenschutzbeauftragten. Die datenschutzrechtlichen Fragen sind neben den pädagogischen und didaktischen Aspekten eine entscheidende Anforderung an digitale Lernmedien.

7.4 Datenübermittlung einer Schule an das Jugendamt

Im Berichtszeitraum hatte ich die Rechtmäßigkeit einer Datenübermittlung der Schule an das zuständige Jugendamt im Zusammenhang mit einer vermuteten Kindeswohlgefährdung zu prüfen.

Der Petent, Elternteil eines Schulkindes, gab an, dass es außerhalb der Schule zu einem tätlichen Vorfall mit dem eigenen Kind gekommen sei. Dieser Vorfall soll von Seiten der Grundschullehrerin angesprochen worden sein, was im Ergebnis schulseitig zu einer Kontaktaufnahme des Jugendamts geführt habe. Die Eltern vermuteten in der Übermittlung von Informationen zu dem Vorfall durch die Schule an das Jugendamt, ohne dass sie zuvor hierüber informiert worden seien, einen datenschutzrechtlichen Verstoß.

Ich bat die Schule um Stellungnahme zum Sachverhalt. Diese teilte mir mit, dass die Klassenleiterin an einem Tag äußerliche Verletzungen an dem Kind festgestellt habe. Das Kind habe sich ihr hilfesuchend anvertraut und berichtet, dass es wegen schulischer Probleme geschlagen und des Hauses verwiesen worden sei. Das Kind habe sich geängstigt und geäußert, sich den Kindseltern entziehen zu wollen. Weiter teilte die Schule neben vielen weitergehenden Details zum Vorgang mit, dass das Kind bereits zuvor gegenüber der Lehrerin und auch gegenüber Mitschülern bedeutet habe, dass es von seinen Eltern wegen negativer schulischer Leistungen Misshandlungen erfahren habe. Nach Rücksprache mit der Beratungslehrerin habe die Klassenleiterin daraufhin die Eltern wegen körperlicher Züchtigungen angesprochen, was keine Veränderungen ergeben habe.

Von den aktuellen Verletzungen und den Äußerungen sei die Klassenleiterin schockiert gewesen und habe den Schulleiter wegen des Verdachts einbezogen. Auch diesem gegenüber habe das Kind bekräftigt, dass es körperlicher Gewalt seitens seiner Eltern ausgesetzt gewesen sei. Der Schulleiter habe sich mit der Bitte um Beratung an eine Mitarbeiterin des Jugendamtes gewandt, um zu erfahren, welche Schritte von Seiten der

Schule einzuleiten seien. Nach einer Information sei die zuständige Mitarbeiterin des Jugendamtes daraufhin umgehend in der Schule erschienen und habe weitere Maßnahmen in die Wege geleitet. Die Grundschullehrerin sei vom Schulleiter nochmals gebeten worden, den Vorfall zu schildern und die Auffälligkeiten in der Vorsituation dem Jugendamt mitzuteilen. Dazu sei ein Vermerk gefertigt und dem Jugendamt übermittelt worden. Als Zweck der Datenübermittlung gab die Schule an, eine akut bestehende Gefahr für den anvertrauten Schüler abwenden zu wollen und damit die gesetzlichen Pflichten bei Vorliegen einer Gefährdung des Kindeswohls zu erfüllen. Als gesetzliche Grundlage wurde Art. 6 Abs. 2 Satz 1 und 2 GG angegeben.

Meine Kontrolle der Rechtmäßigkeit der Datenübermittlung ergab keinen Verstoß gegen datenschutzrechtliche Normen.

Die Rechtsgrundlagen für die Übermittlung von personenbezogenen Daten durch die Schule im Zusammenhang mit einer Gefährdung des Kindeswohls sind das Schulgesetz und das Gesetz zur Kooperation und Information im Kinderschutz (KKG). § 50a Abs. 1 SächsSchulG regelt, dass die Schule die erforderlichen Maßnahmen nach dem Gesetz zur Kooperation und Information im Kinderschutz einleiten soll, wenn Lehrern an Schulen in öffentlicher und freier Trägerschaft in Ausübung ihrer beruflichen Tätigkeit gewichtige Anhaltspunkte für eine Gefährdung des Wohls eines Kindes oder eines Jugendlichen bekannt werden.

§ 4 KKG regelt die Beratung und Übermittlung von Informationen durch Geheimnisträger bei Kindeswohlgefährdung. Die Vorschrift sieht ein abgestuftes behördliches Handeln vor. Zunächst sollen die genannten Personengruppen Eltern beraten und motivieren, Hilfen nach dem SGB VIII anzunehmen, Absatz 1. Bei weiterer Erforderlichkeit sollen sie die Möglichkeit haben, zu Fragen der Gefährdung des Kindeswohls in einem konkreten Fall Beratung durch den öffentlichen Träger einzuholen, ohne die Identität der Betroffenen in diesem Stadium offenbaren zu müssen, Absatz 2. Erst danach, wenn dies keinen Erfolg verspricht, soll das Jugendamt über eine mögliche Gefährdung des Kindeswohls informiert werden.

Das Verfahren wurde nach meiner Einschätzung dennoch eingehalten. Im vorliegenden Fall hatte die Schule bereits vor dem letzten tätlichen Angriff gemäß § 4 Abs. 1 KKG wegen der dargestellten Anhaltspunkte für eine Kindeswohlgefährdung mit der Mutter als Personensorgeberechtigter eine Aussprache durchgeführt. Die weiteren äußeren Verletzungen des Kindes und dessen weitere Angaben veranlassten den Schulleiter telefonische Beratung beim zuständigen Jugendamt gemäß § 4 Abs. 2 KKG zu suchen.

Aufgrund der Angaben und sichtbaren körperlichen Verletzungen des Kindes konnte die Schule von Anhaltspunkten einer Gefährdung des Kindeswohls ausgehen. Zu dem Zweck, das Wohl des Kindes zu schützen, durfte die Schule daher das Jugendamt über den Fall informieren und die erforderlichen Daten übermitteln. Auch die Entscheidung, auf eine vorherige Information über die Übermittlung zu verzichten, war nach meiner Überzeugung angesichts der Einschätzung einer Eilbedürftigkeit aufgrund akuter sichtbarer äußerer Verletzungen als nicht fehlerhaft zu beurteilen.

7.5 Elektronisches Klassenbuch

Ich erhalte zunehmend Anfragen von Schulen zur Zulässigkeit von sogenannten elektronischen Klassenbüchern. Das Klassenbuch besteht aus einem Klassentagebuch und aus einem Notenbuch. Das Klassentagebuch wird für Eintragungen zum erteilten Unterricht und für tägliche Aufzeichnungen über Schülerversäumnisse genutzt. Das Notenbuch dient der Erfassung aller erteilten Noten. Gemäß II.3.1 Schulformular-VwV (*Verwaltungsvorschrift des Staatministeriums für Kultus zur Verwendung von Vordrucken für die schulische Verwaltung*) sind jedoch beide im Format DIN A4 zu führen. Dies schließt nach meiner Auffassung eine rein elektronische Führung des Notenbuchs aus. Diese Auffassung vertritt das von mir um Stellungnahme gebetene SMK ebenfalls. Bis jetzt nicht geäußert hat sich die Behörde leider zu der ebenfalls gestellten Frage, ob die gesetzliche Vorschrift des § 12 Abs. 1 SächsEGovG, wonach staatliche Behörden, also auch Schulen in Trägerschaft des Freistaates Sachsen, grundsätzlich die elektronische Vorgangsbearbeitung und Aktenführung einzusetzen haben, ein anderes Ergebnis bedingt.

8 Justiz

8.1 Übersendung von Austrittsmitteilungen zu Gefangenen durch eine Justizvollzugsanstalt

Ich erhielt Kenntnis von einem Fall, in dem eine sächsische JVA dem Absender einer an einen ehemaligen Gefangenen gerichteten Postsendung eine Austrittsmitteilung übersandt hatte. Als die Sendung in der JVA eintraf, war der Gefangene schon entlassen worden und kein Gefangener mehr.

Die mit Hilfe eines automatisierten Verfahrens erstellte Austrittsmitteilung enthielt personenbezogene Angaben zu Name, Vorname, Geburtsdatum, Staatsangehörigkeit, Geburtsland und Geschlecht des ehemaligen Gefangenen. Darüber hinaus informierte sie über den genauen Termin seiner Entlassung und seine „Austrittsadresse“. Eine Einwilligung in die Übermittlung dieser Daten hatte er nicht gegeben.

Weil die Austrittsmitteilung automatisiert erstellt worden war, lag die Vermutung nahe, dass nicht nur im konkreten Fall einem Absender einer an einen zwischenzeitlich entlassenen Gefangenen gerichteten Postsendung ausführliche Austrittsmitteilungen übersandt wurden. Ich informierte deshalb das SMJus über den Fall und teilte mit, dass ich die Übermittlung der oben genannten Angaben über ehemalige Gefangene an Absender von Postsendungen, die an diese Gefangenen in der JVA adressiert worden waren, für unzulässig halte.

§ 96 Abs. 5 SächsStVollzG bestimmt, unter welchen Voraussetzungen die JVA nichtöffentlichen Stellen Auskünfte zu Inhaftierung, evtl. bevorstehender Entlassung und Entlassungsadresse eines Gefangenen erteilen kann bzw. zu erteilen hat. Eine an den Gefangenen in der JVA adressierte Postsendung berechtigt die Anstalt danach keinesfalls, dem Absender der Postsendung eine Austrittsmitteilung einschließlich der oben genannten personenbezogenen Angaben zu übermitteln, wenn der Gefangene vor Erhalt der Postsendung entlassen wurde. Vorsorglich wies ich darauf hin, dass auch nicht von einer „mutmaßlichen Einwilligung“ des entlassenen Gefangenen in die Übermittlung dieser Daten ausgegangen werden kann. Hielte man die Übermittlungsvorschriften des Sächsischen Strafvollzugsgesetzes nach der Entlassung des Betroffenen nicht für anwendbar, weil es dann an der Gefangeneneigenschaft fehlt und der Vollzug der Freiheitsstrafe beendet ist (vgl. § 1 SächsStVollzG), könnte eine Übermittlung personenbezogener Daten an nicht-öffentliche Stellen allenfalls nach § 16 SächsDSG in Betracht kommen. Allerdings lägen in oben beschriebenen Konstellationen auch dessen Voraussetzungen nicht vor. Ein Hinweis an den Absender der Postsendung, dass der Betroffene

aus der JVA entlassen wurde, wäre nach alldem ausreichend und datenschutzrechtlich nicht zu beanstanden.

Das SMJus teilte meine Auffassung und wies die sächsischen Justizvollzugsanstalten darauf hin, dass die §§ 96 Abs. 5 SächsStVollzG, 88 Abs. 1 und 2 SächsUHaftVollzG, 88 Abs. 5 SächsJStVollzG und 97 Abs. 5 SächsSWG abschließend regelten, unter welchen Voraussetzungen nicht-öffentlichen Stellen Auskünfte zu Inhaftierung, evtl. bevorstehender Entlassung und Entlassungsadresse eines Gefangenen erteilt werden dürften. Insbesondere bedürfe es eines schriftlichen Antrages der nicht-öffentlichen Stelle, in der das berechtigte Interesse derselben an der erbetenen Auskunft glaubhaft dargelegt wird.

Der Fall zeigt, dass auch und gerade bei häufig vorkommenden Datenverarbeitungstätigkeiten die Bedingungen des Einzelfalls entscheidend sind. Übermittlungen an nicht-öffentliche Stellen sind in aller Regel nur unter strengeren Voraussetzungen zulässig als Mitteilungen im Behördenverkehr. Ein Grund hierfür wird gerade in diesem Fall deutlich, wenn man bedenkt, dass durchaus Konstellationen vorstellbar sind, in denen es einem (ehemaligen) Gefangenen nicht recht sein dürfte, dass private Dritte von seiner ersten Wohnanschrift nach Haftentlassung erfahren.

8.2 Übermittlung personenbezogener Daten von Kostenschuldnern durch die Landesjustizkasse an Finanzämter ohne Rechtsgrundlage

Mit einer Beschwerde über die Landesjustizkasse (LJK) Chemnitz wandte sich eine Petentin an mich und berichtete davon, dass sie von dem für sie zuständigen Finanzamt darüber informiert worden sei, dass sie der LJK Geld schulde. Weil die Forderung zu diesem Zeitpunkt bereits beglichen gewesen sein soll, war der Petentin unverständlich, weshalb die LJK dem Finanzamt unzutreffende Informationen übermittelt hatte.

Im Lauf der datenschutzrechtlichen Kontrolle erklärte das OLG Dresden, das die Aufsicht über die LJK führt und dem die LJK meine Schreiben regelmäßig vorlegt, dass die LJK ein Aufrechnungsersuchen an das Finanzamt übersandt habe, dessen Grundlagen sich in den §§ 387 ff. BGB fänden. Da ich die Grundlage für die Übermittlung personenbezogener Daten durch die LJK erfragt hatte, war diese Auskunft nicht zufriedenstellend – die §§ 387 ff. BGB bestimmen lediglich, unter welchen Umständen Forderungen im Verhältnis von Gläubiger und Schuldner miteinander verrechnet werden können. Auf meine Nachfrage teilte das OLG Dresden mit, dass eine Verwaltungsvorschrift zur Sächsischen Haushaltsordnung Rechtsgrundlage für das Aufrechnungsersuchen gewesen sei. Auch diese Erklärung konnte ich nicht akzeptieren, weil die Über-

mittlung personenbezogener Daten als Grundrechtseingriff einer gesetzlichen Grundlage bedarf und deshalb nicht aufgrund einer Verwaltungsvorschrift vorgenommen werden darf, im Übrigen enthielt weder die Verwaltungsvorschrift noch die in Bezug genommene Bestimmung der Sächsischen Haushaltsordnung auch nur ansatzweise eine Befugnis zur Übermittlung personenbezogener Daten.

Im Schriftwechsel mit dem OLG Dresden stellte sich dann heraus, dass die LJK den jeweils örtlich zuständigen Finanzämtern in Sachsen regelmäßig mitteilte, wenn Forderungen gegen Kostenschuldner offen und fällig waren. Für den Fall, dass der Kostenschuldner eine Forderung gegen den Freistaat Sachsen hat, etwa in Form eines Steuererstattungsanspruchs, wurde das Finanzamt um Erklärung der Aufrechnung ersucht. Im Laufe des Prüfvorgangs hat das OLG Dresden die LJK gebeten, vorerst von der Übersendung von Aufrechnungsersuchen an die Finanzämter abzusehen.

Das zwischenzeitlich durch das OLG Dresden informierte SMJus vertrat gegenüber dem OLG Dresden die Auffassung, dass im Fall der Petentin für die Übermittlung personenbezogener Daten durch die LJK Chemnitz an das Finanzamt zum Zweck der Aufrechnung mit etwaigen Steuererstattungsansprüchen keine rechtliche Grundlage bestanden habe.

Ich habe gegenüber dem SMJus als oberster Aufsichtsbehörde förmlich beanstandet, dass die LJK über Jahre hinweg ohne Rechtsgrundlage personenbezogene Daten von Kostenschuldnern an Finanzämter zum Zweck der Aufrechnung mit etwaigen Steuererstattungsansprüchen übermittelt hat. Weder §§ 387 ff. BGB noch die Verwaltungsvorschrift zur Sächsischen Haushaltsordnung erlaubten der LJK derartige Übermittlungen. Auch § 14 SächsDSG konnte nicht als Grundlage für die Übermittlungen herangezogen werden, da es an der „Erforderlichkeit“ der Übermittlungen für die Aufgabenerfüllung der LJK und der Finanzämter fehlte. Beide Stellen waren und sind auch ohne – nur auf Verdacht gestellte – Aufrechnungsersuchen der LJK in der Lage und mit Befugnissen ausgestattet, ihre gesetzlichen Aufgaben zu erfüllen.

Bedenklich war das Vorgehen der LJK auch vor dem Hintergrund eines Vorgangs aus dem Jahr 2013/2014, über den ich im letzten Tätigkeitsbericht (17/8.7: Übermittlung von Gläubigerdaten durch die LJK an die Steuerbehörden) informiert hatte. Zwischen meiner Behörde und dem SMJus bestand damals im Ergebnis Einigkeit, dass Übermittlungen personenbezogener Daten durch die LJK an Steuerbehörden zum Zweck der Prüfung evtl. bestehender Gegenforderungen einer spezifischen Rechtsgrundlage bedürfen, die es damals nicht gab und die auch heute noch nicht existiert. Das Staatsministerium hatte seinerzeit das OLG Dresden unterrichtet und gebeten, von dem ursprünglich geplanten Verfahren Abstand zu nehmen.

Im Hinblick darauf, dass die LJK und das OLG Dresden in Kenntnis des zurückliegenden Vorgangs und entgegen der damaligen rechtlichen Bewertung die regelmäßige Übermittlung von Kostenschuldnerdaten an Finanzämter praktizierten und als vertretbar einschätzten, konnte ich nicht von der förmlichen Beanstandung absehen.

Der Datenschutzverstoß wog auch dadurch besonders schwer, dass Übermittlungen von Daten zu Kostenschuldnern – unabhängig von der Frage der rechtlichen Unzulässigkeit – in zahlreichen Fällen nicht einmal sachdienlich gewesen sein dürften; in Konstellationen nämlich, in denen keine Forderungen des jeweiligen Kostenschuldners gegen die Finanzverwaltung bestanden. Die Finanzämter erlangten so Kenntnis von personenbezogenen Vorgängen der LJK, obwohl diese Kenntnis von keinerlei Nutzen und für ihre Aufgabenerfüllung nicht einmal dienlich war.

Die LJK hat die gerügte rechtswidrige Praxis eingestellt; derzeit richtet sie Aufrechnungsersuchen an Finanzämter nur in den Fällen, in denen sie – z. B. aus der Vermögensauskunft von Kostenschuldnern – positiv Kenntnis von tatsächlich bestehenden Steuererstattungsansprüchen des betreffenden Schuldners hat. Zur rechtlichen Bewertung dieser Vorgehensweise stehe ich aktuell im Austausch mit dem SMJus.

8.3 Zuverlässigkeitsüberprüfung durch eine JVA nach unwirksamer Einwilligung

Der Inhaber eines kleinen Ein-Mann-Unternehmens schrieb mich an und bat um eine Einschätzung zum Vorgehen einer sächsischen Justizvollzugsanstalt bei der Prüfung, ob das Unternehmen geeignet sei, einen Strafgefangenen im Rahmen eines freien Beschäftigungsverhältnisses anzustellen.

Die JVA hatte dem Petenten den Vordruck einer Einverständniserklärung vorgelegt, in der sie auf Folgendes hinwies: „Bei den zuständigen Behörden werden, im Rahmen der Prüfung der Geeignetheit eines Unternehmens zur Arbeit mit Gefangenen des offenen Vollzugs, Auskünfte über dieses Unternehmen eingeholt. Die dabei erlangten Erkenntnisse werden nur im weiteren Verfahren verwertet.“ Der Petent erklärte sich mit dieser Überprüfung einverstanden und schickte den unterschriebenen Vordruck an die JVA zurück.

In der Folge erfuhr der Petent, dass der Strafgefangene, der bei ihm beschäftigt werden wollte, eine negative Antwort auf seinen Antrag erhalten hatte. Die JVA begründete die Ablehnung des Antrags gegenüber dem Strafgefangenen damit, dass Anfragen beim Gewerbeamt, bei der Staatsanwaltschaft und der Polizei ergeben hätten, dass Bedenken gegen die Zuverlässigkeit des Petenten bestünden.

Ich bat die JVA um Nennung der Rechtsgrundlage, auf der Informationen insbesondere bei Polizei und Staatsanwaltschaft eingeholt worden waren. Daneben wies ich darauf hin, dass die dem Petenten vorgelegte Einverständniserklärung in keiner Hinsicht den rechtlichen Anforderungen an eine wirksame Einwilligung in die Überprüfung einer natürlichen Person entsprechen dürfte, da sie sich ausdrücklich (nur) auf die Einholung von Auskünften über das Unternehmen bezog, dessen Geeignetheit zur Arbeit mit Gefangenen des offenen Vollzugs geprüft werden soll.

Die JVA teilte mit, dass die Angaben über den Petenten auf Grundlage der von ihm erteilten Einwilligung erhoben worden seien. Die Anfragen bei Staatsanwaltschaft und Polizei hätten sich auf das Unternehmen bezogen – dabei ist anzumerken, dass der Name des Ein-Mann-Unternehmens aus der Berufsbezeichnung und dem Namen des Petenten bestand. In Anbetracht dieser Sachlage sei ein weiterer Hinweis darauf, dass sich die Überprüfung auf die Person des Petenten bezieht, nicht erforderlich gewesen. Die JVA sehe es auch nicht als notwendig an, darauf hinzuweisen, bei welchen Stellen Informationen erhoben werden sollten. Somit sei die Datenerhebung auf der Grundlage von § 97 Abs. 2 i. V. m. Abs. 1 SächsStVollzG und § 12 Abs. 4 Nr. 2 SächsDSG zulässig gewesen.

Weil diese Ausführungen hinsichtlich der Anforderungen an Einwilligungserklärungen aus datenschutzrechtlicher Sicht völlig inakzeptabel waren, habe ich neben der JVA zugleich auch das SMJus über meine Einschätzung informiert:

Grundsätzlich ist eine Verarbeitung personenbezogener Daten Dritter, d. h. anderer Personen als Gefangener, durch die JVA auf Grundlage einer wirksamen Einwilligung des Dritten zulässig. Eine Datenerhebung auf Einwilligungsbasis wäre nach § 97 Abs. 1 Satz 2 SächsStVollzG i. V. m. § 12 Abs. 4 Nr. 2 SächsDSG möglich. Allerdings muss die Einwilligung des Betroffenen den gesetzlichen Anforderungen entsprechen. Insbesondere muss der Betroffene erkennen können, bei welchen bestimmten Stellen konkret Informationen über ihn erhoben werden sollen.

Die JVA erwähnte in ihrem Anschreiben und dem Vordruck der Einverständniserklärung die Einholung von Auskünften über das „Unternehmen“. Die „bei den zuständigen Behörden“ erhobenen Angaben würden „nur im weiteren Verfahren“ verwendet werden. Es war für Unterzeichner der Erklärung gerade nicht erkennbar, bei welchen konkreten Stellen Informationen eingeholt werden sollen. Unterzeichner wurden auch nicht darüber aufgeklärt, dass – gerade bei Kleinbetrieben oder, wie im Ausgangsfall, bei „Ein-Mann-Unternehmen“ – die JVA Daten zur Person erhebt. Die Argumentation, die Anfragen bei Polizei und Staatsanwaltschaft hätten sich nicht auf den Petenten als Privatperson bezogen, sondern erkennbar einen ausschließlichen Bezug zum Unter-

nehmen gehabt, war absurd. Speicherungen in Dateien der Polizei und der Staatsanwaltschaft, insbesondere über Tatverdächtige/Beschuldigte, beziehen sich stets auf natürliche Personen. Schließlich konnte dem Vordruck der JVA keineswegs entnommen werden, dass personenbezogene Daten bei Staatsanwaltschaft und Polizei erhoben werden; der Hinweis auf die Einholung von Auskünften über das Unternehmen bei den zuständigen Behörden schafft insoweit nicht ansatzweise die für eine wirksame Einwilligung erforderliche Klarheit beim Betroffenen.

Das SMJus teilte meine Auffassung und wies in Abstimmung mit meiner Dienststelle neben der betroffenen JVA auch die anderen sächsischen JVA auf die Sach- und Rechtslage im Rahmen der Prüfung der Eignung von Beschäftigungsstellen gemäß § 23 Abs. 1 SächsStVollzG und einer damit verbundenen Erhebung personenbezogener Daten Dritter hin. Danach ist die Einholung von Auskünften zu den betroffenen Unternehmen aus allgemein zugänglichen Informationsquellen, insbesondere dem Handelsregister oder dem Register beim Gewerbeaufsichtsamt gemäß § 14 Abs. 5 Satz 2 GewO ausreichend und – soweit personenbezogene Daten erhoben werden – auf der Grundlage von § 97 Abs. 2 i. V. m. Abs. 1 Satz 2 SächsStVollzG, § 12 Abs. 4 Nr. 8 SächsDSG auch ohne die Einwilligung der betroffenen Dritten zulässig. Soweit im Einzelfall einer Eignungsprüfung weitere, über die aus allgemein zugänglichen Informationsquellen erhältlichen hinausgehende personenbezogene Daten erforderlich sind, müssen diese beim Betroffenen direkt oder bei Dritten auf Grundlage einer wirksamen Einwilligung des Betroffenen erhoben werden. Bei der Erhebung personenbezogener Daten Dritter auf der Grundlage einer Einwilligung müssen wirksame, den rechtlichen Anforderungen entsprechende Einwilligungserklärungen verwendet werden. Insbesondere müssen Betroffene erkennen können, bei welchen Stellen konkrete Informationen über sie erhoben und welchen Personen bzw. Stellen diese erlangten Erkenntnisse vermittelt werden sollen. Zudem muss der Betroffene unter Darlegung der Rechtsfolgen darauf hingewiesen werden, dass die Einwilligung verweigert und mit Wirkung für die Zukunft widerrufen werden kann.

Die unzulässig über den Petenten erhobenen Angaben wurden bei der JVA gelöscht; die Verwendung des Vordrucks zur Einwilligung, wie er dem Petenten vorgelegt worden war, ist nicht mehr zulässig.

Der Fall zeigt, welche Bedeutung der Einhaltung der rechtlichen Vorgaben für eine wirksame Einwilligung zukommt. Betroffene müssen genau wissen, in welche Verarbeitungen ihrer Daten sie einwilligen; die öffentliche Stelle wiederum darf im Rahmen der erteilten Einwilligung rechtssicher agieren. Klare, unmissverständliche Angaben

und genaue Aufklärung sind nicht nur rechtlich geboten, sie erhöhen auch die Akzeptanz der Betroffenen für das behördliche Handeln.

8.4 Auskunft für Gerichtsvollzieher bei der Polizei

Mit dem 2. Gesetz zur Änderung des Sächsischen Justizgesetzes wurde für die Gerichtsvollzieher die Möglichkeit eröffnet, vor schwerwiegenden Vollstreckungsmaßnahmen bei den örtlichen Polizeidienststellen anzufragen, ob dort personengebundene Hinweise über eine Gefährlichkeit oder Gewaltbereitschaft des Schuldners vorliegen (siehe 17./8.3). Zu diesem Zweck können seither personenbezogene Daten des Schuldners an Gerichtsvollzieher übermittelt werden. Die Norm begründet damit eine Datenerhebungsbefugnis für die Gerichtsvollzieher. Sie ist bis zum 31. Dezember 2016 befristet und vor Ablauf dieser Befristung zu evaluieren, um ihre Wirksamkeit und Auswirkungen auf die gerichtsvollzieherische und polizeiliche Praxis zu überprüfen.

Das SMJus hat mich dankenswerterweise bereits früh im Vorfeld an der Formulierung der für die Evaluation sinnvollen Fragen beteiligt. Aus meiner Sicht waren dabei vor allem die tatsächliche Anzahl der Abfragen nach § 42a SächsJG sowie die Häufigkeit von „Treffern“ und nachfolgende Datenübermittlungen von Interesse. Wichtig ist meines Erachtens außerdem, ob und ggf. welche anderen Vollstreckungsmaßnahmen als die in den Regelbeispielen des § 42a SächsJG genannten für Abfragen durch die Gerichtsvollzieher ursächlich waren. Schließlich ist von Interesse, wie sich die Anzahl tätlicher Angriffe auf Gerichtsvollzieher seit Einführung der Abfragemöglichkeit tatsächlich entwickelt hat.

Mit Antwort auf mehrere Kleine Anfragen eines Abgeordneten des Sächsischen Landtages vom 21. Dezember 2016 (LT-Drs. 6/4861 und 6/7156) erläuterte das SMI die Praxis nach § 42a SächsJG. So teilte es mit, dass „grundsätzlich ... alle“ der möglichen 26 „personengebundenen Hinweise für die Eigensicherung von Polizeibediensteten relevant“ seien. Mit Stand von Ende 2016 seien in IVO 576 Gefährlichkeitsabfragen von Gerichtsvollziehern gemäß § 42a SächsJG gespeichert. Zu den Gerichtsvollziehern würden Name und Vorname und ihre Erreichbarkeiten, zu den Betroffenen im Regelfall Name, Vorname, Geburtsdatum und die übermittelten Anschriften, zu den Sachverhalten Zeitpunkt, Anlass und Rechtsgrundlage der Anfrage sowie das Aktenzeichen gespeichert. Darüber hinaus werde der Zeitpunkt der Auskunft dokumentiert. Da die Polizei keine gesonderte Statistik über erfolgte Straftaten gegen Gerichtsvollzieher führe, könne jedoch dazu nichts gesagt werden.

8.5 Meine Zeugnisverweigerungsrechte in Ermittlungsverfahren

Nach den Vorratsdatenspeicherungs-Urteilen des Bundesverfassungsgerichts vom 2. März 2010 (1 BvR 256/08, 1 BvR 263/08 und 1 BvR 586/08) und des Europäischen Gerichtshofs vom 8. April 2014 (C-293/12 und C-594/12), in denen die deutschen Rechtsgrundlagen der Vorratsdatenspeicherung (§§ 113a, 113b TKG a. F. und § 100g StPO a. F.) für nichtig bzw. die EU-Richtlinie zur Vorratsdatenspeicherung für rechtswidrig und ungültig – u. a. wegen fehlender Ausnahmen zur Datenerhebung von Berufsgeheimnisträgern – erklärt worden waren, hatte der Bundesgesetzgeber mit dem „Gesetz zur Einführung einer Speicherfrist und einer Höchstspeicherfrist für Verkehrsdaten“ (BGBl I 2015 S. 2218, in Kraft getreten am 18. Dezember 2015) erneut versucht, eine grundrechtskonforme Vorratsdatenspeicherung in Deutschland einzuführen.

Nach dem neugefassten § 100g Abs. 4 StPO ist die Erhebung und Verwertung von Verkehrsdaten der nach § 53 Abs. 1 Satz 1 StPO zeugnisverweigerungsberechtigten Personen (z. B. Verteidigern des Beschuldigten) verboten, es sei denn, bestimmte Tatsachen begründen den Verdacht, dass diese selbst an der Tat beteiligt sind. Die staatlichen Landesdatenschutzbeauftragten und ihre Mitarbeiter, denen nach § 12 Abs. 3 BDSG ebenfalls ein Zeugnisverweigerungsrecht gemäß § 23 Abs. 4 BDSG zusteht, wurden bei der Neufassung des § 100g StPO dagegen nicht berücksichtigt. Damit besteht zumindest Unklarheit darüber, ob eine Strafverfolgungsbehörde meine und meiner Landeskollegen Verkehrsdaten, über die ich nach dem Bundesdatenschutzgesetz das Zeugnis verweigern darf, nach der aktuellen Fassung der Strafprozessordnung erheben und verwerten darf.

Auf meinen entsprechenden Hinweis antwortete mir das Bundesministerium der Justiz und für Verbraucherschutz, dass von einer Einbeziehung der Datenschutzbeauftragten in den § 100g Abs. 4 StPO abgesehen worden sei, da auch die übrigen Erhebungs- und Verwertungsverbote der Strafprozessordnung keine Sonderregelungen hinsichtlich der Datenschutzbeauftragten enthielten. Die Bundesregierung prüfe aber, ob § 23 Abs. 4 BDSG um daran anknüpfende Beweiserhebungs- und Verwertungsverbote erweitert werden sollte.

Ich werde den Vorgang im Auge behalten.

9 Wirtschaft und Arbeit

9.1 Straßenverkehrswesen

9.1.1 Aufbewahrungsfristen in Führerscheinakten

Nach Änderung des Straßenverkehrsgesetzes – die Neufassung erfolgte bereits 2003 – besteht oft Unklarheit bei Betroffenen, wann die Aufbewahrungsfristen für Dokumente, Urteile und vorgenommene Eintragungen in Akten, die zu ihrer Person bei Fahrerlaubnisbehörden geführt werden, ablaufen.

Die Fahrerlaubnisbehörden erteilen die Erlaubnis zum Führen eines Kraftfahrzeuges auf öffentlichen Straßen, § 2 Abs. 1 StVG. Hierfür stellen sie die Eignung und Befähigung von Personen als Kraftfahrzeugführer und für die Prüfung der Berechtigung zum Führen von Fahrzeugen fest. Den Fahrerlaubnisbehörden dürfen die erforderlichen Daten aus dem Fahreignungsregister durch Abruf im automatisierten Verfahren übermittelt werden (§ 30a Abs. 1 StVG).

Im zentralen Fahreignungsregister, das gemäß § 28 StVG durch das Kraftfahrt-Bundesamt betrieben wird, werden Informationen gespeichert (§ 28 Abs. 1 StVG), die u. a. erforderlich sind, um die Eignung und Befähigung von Personen zum Führen von Kraftfahrzeugen zu beurteilen.

Darüber hinaus werden nach § 28 Abs. 2 StVG Daten im Fahreignungsregister gespeichert über rechtskräftige Entscheidungen der Strafgerichte wegen Straftaten, die in einem Katalog einer ausführenden Rechtsverordnung aufgeführt sind, soweit diese auf Strafe, Verwarnung mit Strafvorbehalt erkennen oder einen Schuldspruch enthalten. Darüber hinaus enthält das Register rechtskräftige Entscheidungen der Strafgerichte, die die Entziehung der Fahrerlaubnis, eine isolierte Sperre oder ein Fahrverbot anordnen.

Zur Beurteilung der Fahreignung holt die Fahrerlaubnisbehörde zu relevanten Eintragungen im Register die jeweiligen Urteile der Gerichte ein. Weiterhin können zur Beurteilung der Fahreignung von Antragstellern Führungszeugnisse nach § 30 Abs. 5 BZRG angefordert werden.

In Bezug auf Tilgungs- und Löschungsfristen ist nachstehendes zu beachten: Nach § 65 Abs. 3 Nr. 2 StVG n. F. findet die Verwertung für Verkehrsordnungswidrigkeiten, Verkehrsstraftaten und Entzuge, welche in der bis zum Ablauf des 30. April 2014 anwendbaren Fassung im früheren Verkehrszentralregister – jetzt Fahreignungsregister – gespeichert wurden, bis zum 30. April 2019 weiterhin ihre Rechtsgrundlage im § 29 StVG StVG a. F. Hier wird zunächst gemäß Absatz 1 geregelt, dass Ordnungswidrigkeiten nach zwei Jahren, Straftaten nach fünf Jahren und die übrigen Vorgänge nach zehn

Jahren getilgt werden. Ausgenommen von der 5-jährigen Tilgungsfrist sind Straftaten nach § 315c Abs. 1 Nr. 1 Buchst. a, §§ 316 und 323a StGB (Alkohol/Drogenfahrten/ Vollrausch) und Entscheidungen, in denen die Entziehung der Fahrerlaubnis nach den §§ 69 und 69b StGB oder eine Sperrfrist nach § 69a Abs. 1 Satz 3 StGB (isolierte Sperre) angeordnet worden ist. Diese Straftaten werden gemäß § 29 Abs. 1 Nr. 3 StVG a. F. nach zehn Jahren getilgt. Gemäß § 29 Abs. 5 StVG a. F. beginnt bei der Versagung oder Entziehung der Fahrerlaubnis wegen mangelnder Eignung, der Anordnung einer Sperre nach § 69a Abs. 1 Satz 3 StGB oder bei einem Verzicht auf die Fahrerlaubnis die 10-jährige Tilgungsfrist erst mit der Erteilung oder Neuerteilung der Fahrerlaubnis, spätestens jedoch fünf Jahre nach der beschwerenden Entscheidung durch Bescheid oder Urteil.

Die gegenseitige Tilgungshemmung bei mehreren eingetragenen Taten ist in § 29 Abs. 6 StVG a. F. geregelt. Sind im Register mehrere Entscheidungen nach § 28 Abs. 3 Nr. 1 bis 9 StVG a. F. über eine Person eingetragen, so ist die Tilgung einer Eintragung vorbehaltlich der Regelungen in den Sätzen 2 bis 6 erst zulässig, wenn für alle betreffenden Eintragungen die Voraussetzungen der Tilgung vorliegen (§ 29 Abs. 6 Satz 1 StVG a. F.). Eine Ablaufhemmung tritt auch ein, wenn eine neue Tat vor Ablauf der Tilgungsfrist nach Absatz 1 begangen wird und bis zum Ablauf der Überliegefrist (Absatz 7) zu einer weiteren Eintragung führt (§ 29 Abs. 6 Satz 2 StVG a. F.). Nach dieser Regelung sind unter Umständen Verurteilungen und Entzüge auch länger als zehn bzw. fünfzehn Jahre oder noch länger durch die Fahrerlaubnisbehörde verwertbar, da sich die jeweiligen Taten gegenseitig an deren Tilgung hemmen.

Die Berechnung der Tilgungs- und Löschungsfristen ist nicht einfach zu verstehen. Ein Beispiel: Für eine Straftat vom 1. November 2003 (Vorsätzliches Fahren ohne Fahrerlaubnis) verhängte das zuständige Gericht eine isolierte Sperrfrist von sechs Monaten nach § 69a StGB. Demnach beträgt zunächst die Tilgungsfrist für diese Tat nach § 29 Abs. 1 Nr. 2a und Nr. 3 StVG a. F. zehn Jahre. Die Tilgungsfrist begann nach § 29 Abs. 5 StVG a. F., auf Grund dessen, dass innerhalb von fünf Jahren keine Erteilung oder Neuerteilung der Fahrerlaubnis erfolgte, am 15. September 2009 und läuft entsprechend der Übergangsvorschriften nach § 65 Abs. 3 Nr. 2 StVG n. F. bis mindestens zum 30. April 2019. Für eine Straftat vom 4. November 2003 (Vorsätzliches Fahren ohne Fahrerlaubnis) verhängte das zuständige Gericht keine isolierte Sperre. Demnach beträgt für diese Tat die Tilgungsfrist nach § 29 Abs. 1 Nr. 2a StVG a. F. zunächst fünf Jahre. Auf Grund der Regelungen des § 29 Abs. 6 StVG a. F. wird die Tat vom 4. November 2003 jedoch durch die Tat vom 1. November 2003 an der Tilgung bis ebenfalls mindestens zum 30. April 2019 gehemmt.

Um die doch komplexe Berechnung der Tilgungs- und Löschfristen verstehen zu können, empfehle ich Betroffenen, einen schriftlichen Antrag auf Akteneinsicht bei der Fahrerlaubnisbehörde gemäß § 18 Abs. 3 SächsDSG zu stellen. Durch die Fahrerlaubnisbehörde ist den Petenten kostenfrei Auskunft über die zu ihrer Person gespeicherten Daten, den Zweck und die Rechtsgrundlage zu geben.

Bei Akteneinsicht erfahren die Betroffenen durch die Fahreignungsbehörden welche eingetragenen Taten im Fahreignungsregister noch verwertbar sind und welche in den Akten befindlichen gerichtlichen Urteile und Beschlüsse somit noch zur Entscheidungsfindung der Fahrerlaubnisbehörde herangezogen werden dürfen.

9.2 Gewerberecht

9.2.1 Datenverarbeitung im Verfahren zur Aufhebung der Bestellung eines Schornsteinfegers

Ein bevollmächtigter Bezirksschornsteinfeger informierte mich, dass im Rahmen eines durch die Landesdirektion Sachsen betriebenen Verfahrens zur Aufhebung seiner Bestellung nach § 12 Abs. 1 Nr. 2 SchfHwG das für ihn zuständige Finanzamt um Mitteilung gebeten wurde, ob neben den, der Behörde bereits vorliegenden, weitere Tatsachen bekannt seien, die seine Unzuverlässigkeit – als Voraussetzung für die Aufhebung – belegen könnten.

Die von mir um Stellungnahme gebetene Landesdirektion war der Auffassung, dass sie hierzu berechtigt sei, konnte mir aber auch auf explizite Nachfrage keine Rechtsgrundlage für die beabsichtigte Datenerhebung nennen. Erst die Befassung der von mir kontaktierten zuständigen Aufsicht, des SMI, mit dem Vorgang konnte die Landesdirektion zu dem Eingeständnis bewegen, dass derartige Abfragen an Steuer- und Finanzbehörden ohne begründete Anhaltspunkte nicht rechtmäßig sind. Anhaltspunkte können beispielsweise dann bestehen, wenn der Handwerker in nicht unerheblichem Ausmaß die mit der Gewerbeausübung verbundenen steuerlichen Mitwirkungs- und Zahlungsverpflichtungen nicht erfüllt hat und aufgrund seines Verhaltens in der Vergangenheit nicht damit zu rechnen ist, dass er zu einer ordnungsgemäßen Erfüllung seiner Berufspflichten zukünftig in der Lage sein wird. Entsprechendes lag hier jedoch nicht vor. Vielmehr sollten erst durch die Anfrage derartige Anhaltspunkte gefunden werden.

Positiv zu betonen ist, dass das befragte Finanzamt dem Verlangen nicht nachgegeben hatte und die Auskunft nicht erfolgt war.

Im Zusammenhang mit dem Vorgang stellte sich heraus, dass nach Aufhebung der Bestellung des Schornsteinfegers eine Kopie der Datensicherung des elektronischen Kehrbuchs in der Landesdirektion verwahrt werden sollte, obwohl gemäß § 19 Abs. 3 SchfHwG das Kehrbuch ausschließlich an den Nachfolger zu übergeben ist. Auch nach einem aufwendigen Schriftwechsel konnte mir die Behörde bis zum Ende des Berichtszeitraums keine Rechtsgrundlage für die Aufbewahrung des elektronischen Kehrbuchs nennen. Ich habe daher die Rechtsaufsicht, das SMI, um Stellungnahme gebeten. Über den Fortgang werde ich berichten

9.3 Kammerwesen

In diesem Jahr nicht belegt.

9.4 Offene Vermögensfragen

In diesem Jahr nicht belegt.

10 Gesundheit und Soziales

10.1 Gesundheitswesen

10.1.1 Verhältnismäßige betriebsärztliche Untersuchungen und Datenerhebungen

Bereits zurückliegend hatte ich mich zu betriebsärztlichen bzw. arbeitsmedizinischen Vorsorgeuntersuchungen geäußert. Dabei stand die Frage, welche Informationen datenschutzrechtlich an die Personalverwaltung weitergeleitet werden können sollten, im Mittelpunkt, vgl. dazu 11/5.1.1.

Im letzten Berichtszeitraum erreichte mich eine Anfrage eines besorgten Beschäftigten zu einer arbeitsmedizinischen Betreuung bzw. im Hinblick auf die Erforderlichkeit von Datenerhebungen mittels Anamnesebögen und Hinweisen auf mehrere G-Untersuchungen. Verwendung fanden seitens des Dienstherrn Anamnesebögen- und Hinweis-Formulare eines Technischen Überwachungsvereins, die für die Beschäftigten einheitlich Fragen nach Suchterkrankungen, schweren seelischen Erkrankungen, Alkohol-, Drogen- und Medikamentengebrauch beinhalteten. Bei den ebenso den Bediensteten zugeleiteten Fragebögen zu den G25-, G37-, G41-Untersuchungen war aus meiner Sicht lediglich der Bogen für die Bildschirmarbeitsplätze, was reguläre Büroangestellte betraf, ohne weiteres nachzuvollziehen. Ob es sich um Pflichtuntersuchungen oder lediglich Angebotsuntersuchungen handelte, war den Anschreiben ebenfalls nicht zu entnehmen.

Der Dienstherr ist in der Lage, auch wenn es sich bei dem Betriebsarzt um keine inkorporierte Stelle, sondern um eine externe nicht-öffentliche Stelle handelt, im Rahmen des Beauftragungsverhältnisses Umfang, Tiefe und Ausmaß der externen betriebsärztlichen Datenverarbeitung zu bestimmen. Insoweit ist eine datenschutzorganisatorische (Mit-)Verantwortung zu bejahen. Betriebsärzte selbst haben sich aber auch an der Erforderlichkeit zu orientieren. So sind u. a. G-Untersuchungen nur Beschäftigten anzubieten, die aufgrund ihrer Tätigkeit hierfür in Betracht kommen. Auch ist mitzuteilen, ob es sich um Pflicht- oder nur um Angebotsuntersuchungen handelt. Bei Anamnesebögen ist auf die Freiwilligkeit bestimmter Angaben hinzuweisen.

Behörden rate ich, zu den betriebsärztlichen Angeboten selbst zu informieren und für rechtliche Rückfragen auskunftsfähig zu sein. Von einer schlichten Weiterleitung von Betriebsarztunterlagen rate ich ab.

10.1.2 eHealth-Beirat

Im letzten Berichtszeitraum, im Juni 2016, bildete der Freistaat Sachsen beim SMS einen eHealth-Beirat.

Das Gremium, in dem ich auch durch Bedienstete meiner Behörde vertreten bin, ist ein beratendes Fachgremium, das sich mit der Digitalisierung im Gesundheitswesen im Freistaat Sachsen auseinandersetzen soll und dem Vertreter der sächsischen berufsständischen Organisationen, Gesundheitsversorger und Behörden angehören.

Zielstellung soll sein, mit Hilfe des Gremiums in geeigneter Weise Initiativen und Projekte zu koordinieren, die zur Verbesserung des digitalen Gesundheitswesens im Freistaat Sachsen beitragen. Zu den konkreten Bereichen sollen sowohl die Befassung mit Förderprojektvorschlägen aus dem Bereich des Europäischen Fonds für regionale Entwicklung (EFRE) als auch strategische Überlegungen zur verbesserten Versorgung im medizinischen Bereich in den Bereichen der Prävention, Diagnose, Therapie, Nachsorge bis hin zur Rehabilitation und Pflege gehören.

Die Mitwirkung meiner Behörde in dem Gremium erfolgt lediglich beratend und tangiert nicht meinen Status als unabhängige Aufsichtsbehörde.

Die Richtlinie des SMS zur nachhaltigen Förderung der Digitalisierung im Gesundheitswesen im Freistaat Sachsen (RL eHealthSax 2017/18), die nach dem Ende des Berichtszeitraums in Kraft getreten ist und in der der eHealth-Beirat als Beratungsgremium Erwähnung findet, bezieht sich inhaltlich auf den verfolgten Zweck.

10.2 Sozialwesen

10.2.1 Datenerhebung der Krankenkasse zur Unterstützung von Versicherten bei Behandlungsfehlern gemäß § 66 SGB V

Ein Klinikum fragte mich an zwecks des Herausgabeverlangens von Behandlungsunterlagen durch Krankenkassen: Diese wenden sich danach immer wieder an Krankenhäuser und weisen in diesem Zusammenhang darauf hin, dass Versicherte Unzufriedenheit mit der Behandlung, entweder in dem angeschriebenen oder aber in einem anderen Krankenhaus geäußert hätten. Es sei vom Versicherer die Vermutung einer fehlerhaften Behandlung geäußert worden und die Krankenkasse um Unterstützung bei der Klärung des Sachverhaltes gebeten worden. Dies soll dann mittels einer Begutachtung durch den Medizinischen Dienst der Krankenversicherung erfolgen. Hierzu werden die Krankenhäuser von den Krankenversicherungen gebeten, Behandlungsunterlagen über den Patienten zur Verfügung zu stellen, beispielsweise Aufnahmebefunde/erhobene Befunde, Epikrisen, OP-Berichte, Aufklärungen. Diese Unterlagen sollen dann direkt an den zuständigen Sachbearbeiter der jeweiligen Krankenkasse übermittelt werden.

Die Krankenkassen legen in der Regel eine Erklärung ihrer jeweiligen Versicherten über die Entbindung von der ärztlichen Schweigepflicht vor, die überwiegend eine konkrete Krankheit bzw. Behandlung sowie einen entsprechenden Behandlungszeitraum benennen.

Demgegenüber habe die Krankenhausgesellschaft Sachsen mit Mitteilung vom 17. August 2015 den Krankenhäusern ausdrücklich davon abgeraten, Unterlagen auf Grundlage von § 66 SGB V herauszugeben. Anderenfalls würden die Krankenhäuser Gefahr laufen, ohne Vorliegen einer gesicherten Befugnisnorm die austarierten datenschutzrechtlichen Regularien zu unterlaufen.

Die Krankenhausgesellschaft Sachsen habe auf zwei Entscheidungen verwiesen, namentlich den Beschluss des Landessozialgerichts Schleswig-Holstein vom 20. März 2015 – L 5 KR 40/15 B ER sowie das Urteil des Hessischen Landessozialgerichts vom 4. Mai 2015 – L 1 KR 381/13. Die wesentlichen Feststellungen aus diesen Entscheidungen ließen sich nach Auffassung der Krankenhausgesellschaft wie folgt zusammenfassen:

- Der Regelung des § 66 SGB V kommt eine eher geringe praktische Bedeutung zu.
- Sowohl Wortlaut als auch Gesetzesbegründung sprechen lediglich von einer Unterstützungshandlung und nicht von einer umfassenden Hilfeleistung, womit der Umfang der Unterstützungsleistung bereits eingeschränkt ist.

- Es geht im Wesentlichen darum, dem Versicherten die für seine Rechtsverfolgung essentiellen Informationen zugänglich zu machen; diese erschöpfen sich in der Regel in der Nennung der Diagnose, der Therapien sowie des Namens des behandelnden Arztes.
- Die Krankenkasse kann nur mit den Beweismitteln unterstützen, die sich aus der Inanspruchnahme von Versicherungsleistungen ergeben, also ihr bekannt und in den Akten dokumentiert sind.

In Anbetracht der Hinweise der Sächsischen Krankenhausgesellschaft hatte das anfragende Klinikum davon abgesehen, den Krankenkassen die Behandlungsunterlagen der Versicherten bei vermuteten Behandlungsfehlern zu übersenden. Vielmehr wurde wohl darauf hingewiesen, dass die Versicherten jederzeit selbst ihre Behandlungsunterlagen direkt beim Krankenhaus einsehen bzw. Kopien der Behandlungsunterlagen anfordern könnten.

Ich konnte die Bedenken des Krankenhauses im Ergebnis nicht teilen und habe – in Bezug auf die meiner Aufsicht unterliegende Krankenkasse – zu dieser Problematik wie folgt Stellung genommen:

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

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

Im Hinblick auf diese Unterstützungsobliegenheit der Krankenkasse normiert § 284 Abs. 1 Nr. 5 SGB V ausdrücklich eine entsprechende Datenerhebungsbefugnis der Krankenkasse. Diese Regelung berechtigt die Krankenkassen, Daten zu erheben und zu speichern, soweit dies für die Unterstützung der Versicherten bei Behandlungsfehlern erforderlich ist. Erheben ist nach der Legaldefinition des § 67 SGB X das Beschaffen

von Daten über den Betroffenen. Dabei ist die Art der (zielgerichteten) Beschaffung unerheblich, sie kann z. B. durch Befragung oder Unterlagenanforderung erfolgen.

Vor diesem Hintergrund halte ich die Krankenkasse für berechtigt, selbst Unterlagen beim betreffenden Behandler – hier Krankenhaus – abzufragen. Wäre die Krankenkasse gehalten, nur mit Beweismitteln zu unterstützen, die ihr – bereits – bekannt sind und sich in ihren Akten befinden, bedürfte es keiner entsprechenden Datenerhebungsbefugnis, dafür wäre eine Datennutzungsbefugnis ausreichend.

So führt das Hessische Landessozialgericht in seinem Urteil vom 4. Mai 2015 – L 1 KR 381/13, ausdrücklich aus: „*Unterstützungsleistungen beschränken sich regelmäßig auf die Verschaffung von Auskünften über die vom Arzt gestellten Diagnosen, die angewandte Therapie, die Namen der Behandler, die Anforderung ärztlicher Unterlagen (Hervorhebung durch U.) einschließlich Röntgen-Aufnahmen etc. von der Behandlung und die Begutachtung durch den Medizinischen Dienst der Krankenversicherung (MDK) nach § 275 Abs. 3 Nr. 4 SGB 5... Dem hat die Krankenkasse vorliegend entsprochen und den Sozialmedizinischen Dienst ein Gutachten nach Beiziehung der relevanten medizinischen Unterlagen erstellen lassen und im Anschluss daran dem Kläger alle Unterlagen zur Verfügung gestellt…*“

Finanzielle Leistungen – namentlich die der Rechtsverfolgung – sollen hingegen nicht nach § 66 SGB V seitens der Krankenkasse geschuldet sein (Kinggreen, SGB V-Komm. § 66 Rdnr. 4 m. w. N.).

10.2.2 Leistungen für ambulant betreute Wohngruppen

Ein Petent wandte sich an mich:

Er hatte als Vertreter seines Vaters einen Antrag auf zusätzliche Leistungen für ambulant betreute Wohngruppen und mithin einen Antrag nach § 38a SGB XI gestellt. Von der zuständigen Pflegekasse seines Vaters war er aufgefordert worden, neben einer Kopie des Mietvertrags auch Angaben zur Anzahl der in der Gemeinschaft lebenden Pflegebedürftigen mitzuteilen. Auch die Mindestangabe zu zwei weiteren Bewohnern mit den Angaben: Name, Vorname, Geburtsdatum, Krankenkasse, Pflegestufe und die Unterschrift dieser Bewohner wollte die Kasse wissen. Der Petent hatte offensichtlich eine schriftliche Bestätigung des Pflegedienstes vorgelegt, dass noch zwei weitere Personen mit einer Pflegestufe in der Wohngemeinschaft lebten.

Das zum Einsatz kommende Formular nach § 38a SGB XI beschäftigte seit einiger Zeit nicht nur meine Behörde, die Problematik war auch Gegenstand im Arbeitskreis Ge-

sundheit und Soziales der unabhängigen Datenschutzbehörden des Bundes und der Länder.

Die Erhebung der leistungsrechtlichen Merkmale durch die Pflegekassen wurde seitens der Datenschutzbehörden unterschiedlich bewertet. Dies wurde auch dem Gesetzgeber bekannt und er schuf aus diesem Grund im Rahmen der Änderung des § 38a SGB XI mit Aufnahme des nun seit 1. Januar 2015 wirksamen Absatzes 2 der Vorschrift eine gesetzliche Ermächtigungsgrundlage für die Datenerhebung und -verarbeitung der Pflegekassen (siehe BT-Drs. 18/2909).

Nach seinem eindeutigen Wortlaut halte ich § 38a Abs. 2 SGB XI für abschließend.

Nach § 38a Abs. 2 Nr. 1 SGB XI ist die Pflegekasse danach berechtigt, eine *formlose Bestätigung des Antragstellers* anzufordern, dass die Voraussetzungen des § 38a Abs. 1 Nr. 1 SGB XI erfüllt sind. Das umfasst auch die formlose Bestätigung, dass mindestens zwei der weiteren Wohngruppenbewohner pflegebedürftig sind.

Eine wie nunmehr gesetzlich normierte nur formlose Bestätigung umfasst meiner Auffassung nach aber darüber hinaus nicht das Recht, weitere personenbezogene Daten dieser Heimbewohner zu erfragen und dies durch Unterschrift bestätigen zu lassen. Insoweit war das bisherige Formular der seit 1. Januar 2015 geltenden Rechtslage anzupassen und die Abfrage dieser Daten zu streichen.

Die Pflegekasse schloss sich meiner Rechtsauffassung an und passte das Formular entsprechend an.

10.2.3 Datenerhebungen aufgrund von Unterhaltspflichten nach dem SGB XII

Zur Prüfung, ob und in welcher Höhe ein Unterhaltsbeitrag für ihren Ex-Ehemann von ihr verlangt werden muss, wurde eine Petentin vom KSV angeschrieben und um Angaben über ihre wirtschaftlichen und persönlichen Verhältnisse gebeten. Hintergrund war, dass der KSV für den geschiedenen Ehemann monatlich Sozialhilfe zahlte. Die Petentin hinterfragte bei mir die Zulässigkeit dieser Datenabfrage.

Hier meine Antwort:

Wenn das Sozialamt Leistungen erbringt, so kann kraft Gesetzes ein sogenannter Forderungsübergang an Unterhaltspflichtige erfolgen. Das heißt, das Sozialamt kann im eigenen Namen die Aufwendungen für den Unterhalt des Sozialhilfeempfängers (Leistungsberechtigter) gegenüber den Unterhaltsverpflichteten geltend machen, §§ 93 bis 95 SGB XII.

Bevor das Sozialamt Sozialhilfe leistet, wird geklärt, ob nahestehende Personen vorrangig unterhaltspflichtig gegenüber dem Leistungsberechtigten sind (sogenannter Nachrang der Sozialhilfe nach § 2 SGB XII).

Es wird dabei unterschieden zwischen gesteigert Unterhaltspflichtigen, normal Unterhaltspflichtigen und nicht Unterhaltspflichtigen. Gesteigert Unterhaltspflichtige müssen einen höheren Unterhalt leisten und können einen geringeren Selbstbehalt beanspruchen. Gesteigert unterhaltspflichtig sind Ehegatten untereinander, auch getrennt lebende und geschiedene Ehegatten.

Neben dem Einkommen ist zur Deckung des ungedeckten Bedarfs auch Vermögen einzusetzen. Zum „Vermögen“ im Sinne des SGB XII gehört das gesamte verwertbare Vermögen. Damit werden alle beweglichen und unbeweglichen Sachen, Forderungen und sonstige Vermögenswerte erfasst, die verwertet werden können. Nicht zur Unterhaltspflicht herangezogen werden kann das so genannte Schonvermögen.

Vor diesem Hintergrund ist das Sozialamt verpflichtet, entsprechende Prüfungen vorzunehmen, das heißt Angaben zu den tatsächlichen Vermögensverhältnissen beim Betroffenen, hier also bei der Unterhaltsverpflichteten, abzufordern.

Das Abfordern einer Vermögensübersicht samt Belegen ist daher zulässig, die Unterhaltspflichtigen haben dem Träger der Sozialhilfe über ihre Einkommens- und Vermögensverhältnisse Auskunft zu geben, soweit die Durchführung dieses Buches es erfordert, so ausdrücklich § 117 SGB XII.

10.2.4 Anvertraute Sozialdaten nach § 65 SGB VIII

Ein Familienvater beantragte Einsicht in Unterlagen beim Jugendamt; konkret ging es ihm um die Einsicht in ein familienpsychologisches Gutachten. Er gab an, das Jugendamt habe ihm auf der Grundlage des § 65 SGB VIII die Einsicht verweigert.

Ich nehme diese Eingabe zum Anlass, erneut (siehe schon 9/10.2.9) auf die Anforderungen des Vorliegens dieser Vorschrift hinzuweisen:

§ 65 SGB VIII lautet – auszugsweise – wie folgt:

§ 65 Besonderer Vertrauensschutz in der persönlichen und erzieherischen Hilfe

(1) Sozialdaten, die dem Mitarbeiter eines Trägers der öffentlichen Jugendhilfe zum Zwecke persönlicher und erzieherischer Hilfe anvertraut worden sind, dürfen von diesem nur weitergegeben werden

….

Insoweit ist bei der Entscheidung über eine Auskunftsgewährung in der Tat auch die Vorschrift des § 65 SGB VIII zu beachten, welche einen besonderen Vertrauensschutz im Bereich der persönlichen und erzieherischen Hilfe normiert. Das besondere Weitergabeverbot des § 65 Abs. 1 Satz 1 Nr. 1 SGB VIII überlagert für seinen Regelungsbereich die allgemeinen Regelungen über die Akteneinsicht nach § 25 SGB X bzw. den datenschutzrechtlichen Auskunftsanspruch nach § 83 SGB X. Insoweit kann diese Vorschrift somit eine Auskunftsverweigerung nach § 83 SGB X begründen.

Allerdings sind die Anforderungen zu beachten, welche an das Vorliegen „anvertrauter" Sozialdaten, wie es § 65 SGB VIII ausdrücklich fordert, zu stellen sind.

§ 65 SGB VIII stellt eine absolute Spezialnorm im Bereich des SGB VIII dar, mit engen Tatbestandsvoraussetzungen und entsprechend strengen Rechtsfolgen: Daten, die tatsächlich (besonders und ganz persönlich, vor allem auch ausdrücklich) nicht dem Träger der öffentlichen Jugendhilfe, sondern einem einzelnen Jugendamtsmitarbeiter anvertraut sind, dürfen nicht weitergegeben werden, auch nicht im internen Dienstverkehr der Behörde (vgl. § 65 Abs. 2 SGB VIII). Solche Daten sind aufgrund dessen gar nicht in der üblichen Weise behördenverfügbar mit der Folge, dass diese Angaben (Daten) in der allgemeinen Sachakte des Jugendamts nichts zu suchen haben.

Daraus folgt, dass die Anforderungen an den Tatbestand des „Anvertrauens" bzw. „Anvertraut-Seins" über das allgemeine, sich bereits aus der Natur der Sache im Bereich des SGB VIII oftmals gesteigerten Vertrauensverhältnisses zwischen Behördenmitarbeiter und Beratenem deutlich hinausgehen.

Die Vorschrift des § 65 SGB VIII käme daher einer ggf. vollständigen Übermittlungssperre im Bereich des SGB VIII gleich und kann daher nur in ganz engen Ausnahmefällen einschlägig sein. Daraus folgt, dass nicht jede Mitteilung des Klienten an den Behördenmitarbeiter im Bereich des SGB VIII als anvertraut bezeichnet werden kann. Vielmehr wird in der Fachliteratur zu Recht gefordert, dass sich der Betroffene gegenüber dem Behördenmitarbeiter speziell mit der Erwartung offenbart hat, dass dieser die Information ausschließlich für sich behält im Sinne eines „das sage ich nur Ihnen und Sie dürfen es keinem weitersagen" und die Fachkraft ausdrücklich oder konkludent zu verstehen gibt, dass sie diese Verschwiegenheit zusichert.

Ob ein derartiges Anvertrauen nur einem ganz konkreten Mitarbeiter des Jugendamtes gegenüber im Sinne des § 65 SGB VIII vorliegen könnte, ist stets im Einzelfall zu prüfen. Bei der Erstellung eines familienpsychologischen Gutachtens gehe ich nicht davon aus.

10.2.5 Unzulässiger Anamnesefragebogen für Krippen-und Kindergartenkinder

Mir ist ein Anamnesefragebogen für Krippen- und Kindergartenkinder vorgelegt worden, der in der Kindertageseinrichtung einer sächsischen Gemeinde zum Einsatz kam und welcher von der Leiterin des Kinderhauses erstellt worden war.

Der betreffende Fragebogen forderte neben personenbezogenen Angaben zu Adressdaten, Geburtsdatum und Staatsangehörigkeit der Eltern und des Kindes noch weitere Angaben, die den Intimbereich der Betroffenen tangierten.

So fanden sich Fragen u. a. zum Geburtsverlauf; hier ein Auszug:

+ Geburtsverlauf:

- *spontan und regelrecht; vorzeitige Wehentätigkeit, Infusion, verzögerte Wehentätigkeit, Infusion;*
- *Kaiserschnitt; Saugglocke; Zangengeburt*
- *Lage des Kindes bei Geburt: regelrechte Schädellage; Steißlage; Anderes/ Weiteres*
- *Wurde Ihr Kind während der Geburt im Geburtskanal gedreht?*
- *War der Vater während der Geburt anwesend?*

Fragen zur Schwangerschaft durften auch nicht fehlen und so sollten die Eltern auch Antworten auf folgende Fragen geben:

+ Schwangerschaft:

- *Gab es über den 4. Monat hinaus Blutungen?*
- *Litt die Mutter an Erkrankungen (chronische Erkrankungen, psychische Erkrankungen, Erkältungen, Schwangerschaftsdiabetes, Schwangerschaftsvergiftung)?*
- *Bestanden Suchterkrankungen/Suchtverhalten der Mutter während der Schwangerschaft (Alkohol, Nikotin, Medikamente, Drogen)? Wenn ja, was und in welcher Menge?*
- *War die Mutter während der Schwangerschaft berufstätig? Wenn ja, was und bis zu welcher Woche?*
- *Kindesvater: Bestanden Suchterkrankungen/Suchtverhalten (Alkohol, Nikotin, Medikamente, Drogen) während der Schwangerschaft der Mutter? Wenn ja, was und in welcher Menge?*
- *Vor der Geburt Ihres Kindes: Gab es vorher bereits eine Schwangerschaft? Wenn ja, wurde diese ausgetragen? Verlief diese normal?*
- *Gab es eine Eileiterschwangerschaft, Totgeburt oder Abtreibung? Wenn ja, was und wie alt war die Mutter?*

Zudem wurden die Erziehungsberechtigten um Abgabe einer Schweigepflichtentbindungserklärung gebeten.

Das Datenschutzrecht erlaubt der Kindertageseinrichtung, für bestimmte Zwecke Daten von Erziehungsberechtigten und vom Kind zu erheben. Die Erhebung ist auf die zur Umsetzung des Betreuungsverhältnisses (=Aufgabe) erforderlichen Daten zu beschränken. Der dem deutschen Datenschutzrecht danach immanente Grundsatz der Erforderlichkeit der Datenerhebung zur Aufgabenerfüllung führt dazu, dass es nicht ausreichend ist, wenn die abgefragten Angaben (Daten) nur nützlich, dienlich oder zweckmäßig sind.

Im Aufnahmevertrag darf vor diesem Hintergrund nach folgenden Angaben gefragt werden:

- Name, Geburtstag und Anschrift des Kindes
- Datum der (noch) bedeutsamen Tetanusimpfungen des Kindes
- Name und Anschrift von Eltern sowie die Telefonnummern, unter denen diese im Notfall zu erreichen sind
- Namen und Geburtstage der Geschwister, wenn die Gebühr der Kindertageseinrichtung von deren Anzahl und Alter abhängt
- Konfession (in einer evangelischen oder katholischen Tageseinrichtung)
- Krankheiten, die der Kindertageseinrichtung bekannt sein müssen, um ggf. angemessen und richtig reagieren zu können (z. B. Diabetes oder Asthma u. Ä.).

All diese Angaben sind für den reibungslosen Ablauf erforderlich und dürfen im Zusammenhang mit dem Aufnahme- bzw. Betreuungsvertrag erhoben werden.

An die Erhebung zusätzlicher Daten im Aufnahme- bzw. Betreuungsvertrag (z. B. Krankenkasse der Eltern, Staatsangehörigkeit von Kindern und deren Eltern, Bildungsstand, Beruf oder Erwerbstätigkeit der Eltern) ist ein strenger Maßstab anzulegen.

Werden solche zusätzlichen Daten erhoben, muss der Träger der Kindertageseinrichtung im Aufnahme- bzw. Betreuungsvertrag konkret begründen, welchen Zweck sie erfüllen sollen und warum gerade diese zusätzlich zu erhebenden Daten erforderlich sind. Beispielsweise kann die Berufstätigkeit ein Kriterium für eine Ganztagesbetreuung sein, worüber dann ein Nachweis verlangt werden darf.

Die im streitgegenständlichen Anamnesebogen abgefragten Angaben gingen weit über das erforderliche und damit zulässige Maß hinaus und waren keinesfalls zur Durch-

führung des Betreuungsvertrages erforderlich. Mithin war auch ihre Speicherung unzulässig.

Offensichtlich teilte die Gemeindeverwaltung hinsichtlich der fehlenden Erforderlichkeit im Anschluss diese Auffassung, da ausweislich eines mir vorgelegten Schreibens der Gemeinde es nun den Eltern freigestellt wurde zu entscheiden, ob sie die Fragen teilweise oder vollständig beantworteten.

Eine entsprechende Datenerhebung auf Einwilligungsgrundlage scheidet indes ebenfalls aus. Denn kraft des verfassungsrechtlichen Grundsatzes des Vorbehaltes des Gesetzes (vgl. Art. 20 Abs. 3, 2. Halbsatz GG i. V. m. der Grundrechtsbindung, Art. 1 Abs. 3 GG, und dem Demokratieprinzip, Art. 20 Abs. 1 GG) dürfen Träger öffentlicher Gewalt (so wie die Gemeinde) nicht in größerem Maße ihnen im Gesetz nicht ausdrücklich zugewiesene Aufgaben mit Hilfe einer lediglich durch Einwilligung der Betroffenen gerechtfertigten Verarbeitung personenbezogener Daten an sich ziehen und erfüllen und dazu durch Verarbeitung personenbezogener Daten in Grundrechte eingreifen.

Insoweit ist auch eine generelle Entbindung von der Schweigepflicht zur Kinderbetreuung nicht erforderlich. Es ist nicht Aufgabe eines öffentlichen Kindergartens zu überprüfen, ob angesprochene Arztvorstellungen seitens der Erziehungsberechtigten eingehalten werden.

Ergebnis: Anamnesebögen und Schweigepflichtentbindungserklärungen kamen daraufhin – so die Mitteilung der Gemeinde – nicht mehr zum Einsatz, bereits ausgefüllte Unterlagen wurden datenschutzgerecht vernichtet.

10.2.6 Erforderlichkeit einer richterlichen Anordnung nach § 73 SGB X im Bereich der Jugendhilfe nach SGB VIII

Ein Landratsamt wandte sich an mich mit der Bitte um Unterstützung in einer Auseinandersetzung mit der Staatsanwaltschaft im Rahmen der Prüfung einer Aussagegenehmigung für eine Mitarbeiterin des Jugendamtes in einem Ermittlungsverfahren wegen Kindesmissbrauchs.

Eine Sozialarbeiterin des ASD hatte im *April* 2016 eine entsprechende Anzeige bei der Polizei erstattet. Zuvor, im *März* 2016, war es zu einer Inobhutnahme der betroffenen Kinder durch das Jugendamt gekommen.

Die Jugendamtsmitarbeiterin war zur Vernehmung bei der Staatsanwaltschaft geladen. Im Vorfeld war bereits seitens des Landratsamts auf das Spannungsverhältnis zwischen der Schweigepflicht von Sozialarbeitern im Strafverfahren und dem Strafverfolgungs-

interesse hingewiesen worden. Problematisch war nach Auffassung des Landratsamts, dass die Staatsanwaltschaft für die Vernehmung vorab keine richterliche Anordnung beantragt hatte, wie dies nach Ansicht der Behörde aber in § 73 Abs. 1 i. V. m. Abs. 3 SGB X vorgesehen sei.

Meine Prüfung kam zu folgendem Ergebnis:

Unstreitig handelt es sich bei den streitgegenständlichen Daten um Sozialdaten, da das Jugendamt die betreffenden Informationen, nämlich Angaben aus der Inobhutnahme der betroffenen Kinder, im Rahmen seiner Aufgabenwahrnehmung erlangt und damit im datenschutzrechtlichen Sinne erhoben hat.

Es geht mithin um Daten, für die das Sozialgeheimnis eingreift, d. h. die besonderen Datenschutzregelungen des SGB, insbesondere die §§ 67 ff. SGB X. Der Begriff des Sozialdatums wird in § 67 Abs. 1 SGB X bestimmt als Einzelangabe über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person, die von einem Sozialleistungsträger im Hinblick auf seine Aufgaben nach dem Sozialgesetzbuch erhoben, verarbeitet oder genutzt wird.

Bei dem Vorgang, als Zeugin Sozialdaten mitzuteilen, handelt es sich im datenschutzrechtlichen Sinne nach der Legaldefinition des § 67 Abs. 6 Nr. 3 SGB X um eine Übermittlung personenbezogener Daten, da die Daten an einen Dritten, nämlich an die Staatsanwaltschaft, weitergegeben werden sollen.

Eine Übermittlung von Sozialdaten bedarf einer ausdrücklich normierten Übermittlungsbefugnis, die sich aus den Sozialgesetzbüchern selbst ergeben muss (BSG, Urteil vom 10. Dezember 2008, BSGE 102, 134). Dies folgt aus § 67d Abs. 1 SGB X. Allein der Hinweis der Staatsanwaltschaft auf ihre Ermittlungsmöglichkeiten nach § 161 StPO genügt im Bereich des Sozialdatenschutzes somit nicht.

Für den Mitarbeiter eines Sozialleistungsträgers besteht, soweit nach § 67d Abs. 1 SGB X eine Datenübermittlung nicht zulässig ist, nach § 35 Abs. 3 SGB I keine Pflicht zum Zeugnis.

Ermächtigungsnorm nach dem SGB:

Nach § 71 SGB X ist eine Übermittlung von Sozialdaten zulässig, wenn sie der Erfüllung besonderer gesetzlicher Pflichten und Mitteilungsbefugnisse dient. Erhält der Sozialleistungsträger Kenntnis von einer bestimmten geplanten schweren Straftat, so ist er zur Mitteilung an die Strafverfolgungsbehörden (StA, Polizei) unter den Voraus-

setzungen des § 138 StGB verpflichtet. Erfährt der Sozialarbeiter von einer vollendeten Straftat, ist er zur Anzeige nach § 71 Abs. 1 Nr. 1 SGB X nicht verpflichtet. Die Mitteilungspflicht dient ausschließlich der Abwehr einer akuten Gefahr, der konkreten Verhinderung von Straftaten, nicht der Strafverfolgung. Unter Umständen genügt zur Gefahrenabwehr eine Information des Gefährdeten. Bei geplanten (schweren) Straftaten besteht keine Anzeigepflicht gegenüber Polizei und Staatsanwaltschaft, wenn eine anderweitige Abwehr, z. B. durch Einwirken auf den möglichen Täter oder durch Warnung des potentiellen Opfers, möglich ist. Um eine anzeigepflichtige Straftat handelt es sich hier indes nicht.

Als weitere Übermittlungsvorschrift ist § 69 Abs. 1 Nr. 1 i. V. m. Abs. 2 SGB X zu beachten.

Als gerichtliches Verfahren im Sinne der Vorschrift wird jedes Verfahren vor einem staatlichen Gericht angesehen, es ist also nicht auf Verfahren der Sozialgerichtsbarkeit beschränkt, in denen es um die Überprüfung der Entscheidung einer SGB-Stelle geht. Auch das staatsanwaltschaftliche Ermittlungsverfahren fasse ich darunter – andernfalls käme auch hier § 69 Abs. 1 Nr. 1 SGB X zur Anwendung.

Die entscheidende Rechtsfrage ist, ob – wie § 69 Abs. 1 Nr. 1 und 2 SGB X dies verlangt – hier das gerichtliche/staatsanwaltschaftliche Verfahren im Zusammenhang mit der Erfüllung einer Aufgabe nach dem Sozialgesetzbuch steht.

Nach § 69 Abs. 1 Nr. 1 2. Alt. SGB X ist die Übermittlung von Sozialdaten auch an andere Stellen zulässig, wenn dies zur Erfüllung der eigenen Aufgabe der übermittelnden Stelle erforderlich ist. Dritte können hier öffentliche oder private Stellen, aber auch Einzelpersonen sein; es muss sich nicht um andere Stellen nach § 35 SGB I oder gleichgestellte Stellen handeln. Betroffen sind z. B. die Fälle, in denen der Sozialleistungsträger an Dritte mit dem Ziel herantreten muss, den Sachverhalt zu klären. Insofern kommt grundsätzlich auch eine Übermittlung von Sozialdaten an die Polizei in Betracht, wenn die Aufgabe nach dem Sozialgesetzbuch nur unter Einschaltung der Polizei erfüllbar ist.

Bei Beantwortung der Frage, wann eine Übermittlung an die Polizei zur Erfüllung der eigenen Aufgabe des Jugendamtes erforderlich ist, wird im Interesse des Vertrauensschutzes ein strenger Maßstab angelegt. Die Einleitung von Strafverfahren ist im Katalog der in § 2 SGB VIII definierten Aufgaben nicht enthalten. Andererseits kann eine Übermittlung von Sozialdaten an die Polizei aber notwendig sein, um die Gefährdung eines Kindes oder Jugendlichen abzuwenden und so erfolgreich Hilfe leisten zu können. Dies ist zum Beispiel denkbar bei der Gefahr der Misshandlung durch die Eltern/sonsti-

ge nahe Angehörige. Dies war aber aufgrund des im vorliegenden Fall erfolgten zeitlichen Ablaufs wohl nicht der Fall: Die Anzeige erfolgte im April 2016, die Inobhutnahme jedoch bereits im März 2016, sodass zum Zeitpunkt der Anzeige nicht mehr von einer entsprechenden Gefährdungslage und mithin nicht mehr von einer entsprechenden Aufgabe des Jugendamts ausgegangen werden konnte.

Nach § 73 Abs. 1 SGB X ist schließlich die Übermittlung von Sozialdaten zulässig, soweit sie zur Durchführung eines Strafverfahrens wegen eines Verbrechens oder wegen einer sonstigen Straftat von erheblicher Bedeutung erforderlich und die Übermittlung durch den Richter angeordnet ist.

Von einer entsprechenden Straftat im Sinne von § 73 Abs. 1 SGB X gehe ich hier aus. Allerdings bedarf es für eine zulässige Übermittlung der richterlichen Anordnung nach Absatz 3 der Vorschrift, die die Staatsanwaltschaft einzuholen hätte.

Insoweit habe ich im Ergebnis die Rechtsauffassung des Landratsamts, dass hier eine richterliche Anordnung nach § 73 SGB X erforderlich ist, geteilt.

10.3 Lebensmittelüberwachung und Veterinärwesen

In diesem Jahr nicht belegt.

10.4 Rehabilitierungsgesetze

In diesem Jahr nicht belegt.

11 Landwirtschaft, Ernährung und Forsten

In diesem Jahr nicht belegt.

12 Umwelt und Landesentwicklung

In diesem Jahr nicht belegt.

13 Wissenschaft und Kunst

In diesem Jahr nicht belegt.

14 Technischer und organisatorischer Datenschutz

14.1 Einsatz von Google Analytics auf einer Webseite der Polizei Sachsen

Durch die Beantwortung einer Kleinen Anfrage eines Abgeordneten durch die Staatsregierung (LT-Drs. 6/1645) wurde ich auf den Einsatz von Google Analytics auf der Webseite der Polizei http://verdaechtig-gute-jobs.de/ aufmerksam. In den Fragen 2 und 3 verwies die Staatsregierung auf einen datenschutzkonformen Einsatz des Webanalysedienstes.

Dies nahm ich zum Anlass, um mich beim SMI genauer zu erkundigen. Insbesondere bat ich um Vorlage eines gültigen Vertrages zur Auftragsdatenverarbeitung für eine Übermittlung der Daten zu Analysezwecken an Google.

Die Rechtsgrundlage für die sogenannte Reichweitenanalyse ergibt sich aus § 15 Abs. 3 TMG, in den letzten beiden Tätigkeitsberichten habe ich ausführlich die Einsatzmöglichkeiten für öffentliche Stellen erläutert (16/14.1) und habe dabei auch auf die fehlende Rechtsgrundlage für den Einsatz von Google Analytics (17/14.3) hingewiesen.

Das SMI hatte eine Agentur mit dem Hosting der Webseite beauftragt, was legitim ist, aber nicht von den Verpflichtungen aus dem Datenschutzrecht entbindet. Die Agentur hat den Einsatz von Google Analytics weitgehend anhand der Vorgaben des aufgrund der örtlichen Niederlassung von Google Deutschland zuständigen Hamburgischen Datenschutzbeauftragten (Akt. Fassung: https://www.datenschutz-hamburg.de/uploads/media/GoogleAnalytics_Hinweise_fuer_Webseitenbetreiber_in_Hamburg_2017.pdf) ausgerichtet. Danach ist ein beanstandungsfreier Betrieb unter Einhaltung von Voraussetzungen möglich. Diese Hinweise gelten aber nur für private Unternehmen und nicht für öffentliche Stellen.

Eine entscheidende Voraussetzung ist der Abschluss eines Vertrages zur Auftragsdatenverarbeitung. Dieser muss sich für sächsische öffentliche Stellen zwingend auf das Sächsische Datenschutzgesetz beziehen, ein Umstand, der von Google mit dem automatisch bereitgestellten Mustervertrag nicht erfüllt wird, welcher sich dem Bundesdatenschutzgesetz verpflichtet.

In der Konsequenz habe ich eine Abschaltung des Betriebs von Google Analytics und eine Löschung des damit bei Google vorhandenen Nutzerkontos gefordert, da keine Rechtsgrundlage für einen Betrieb gegeben war. Das SMI kam dieser Forderung nach.

14.2 Sicherheitsvorfall bei der Sächsischen Bildungsagentur

Ein Lehramtsstudent hatte sich an mich gewandt wegen eines für ihn nicht erklärlichen Vorfalls. Er nutzt wie alle Lehramtsstudenten des Freistaates Sachsen eine von der Sächsischen Bildungsagentur im Auftrag des SMK betriebene Online-Plattform. In dieser sind – nach einem persönlichen Login – neben den Stammdaten (Name, Anschrift, Telefonnummer, E-Mail-Adresse) auch die Termine und Noten für die zu absolvierenden Prüfungen für ein Lehramt einsehbar.

Der Lehramtsstudent hatte sich seinen Angaben zu Folge mehrmals am Portal mit seinen Zugangsdaten angemeldet und dabei Zugriff auf die Daten einer ihm nicht bekannten Studentin erhalten. Er konnte dies mit Hilfe von Screenshots belegen.

Ich habe mich daraufhin an die Sächsische Bildungsagentur mit der Bitte um Stellungnahme gewandt. Da der Student auf der Wahrung seiner Anonymität gegenüber der Bildungsagentur bestand, konnte ich das Verhalten nur abstrakt schildern.

Die Sächsische Bildungsagentur zeigte sich bemüht, das Verhalten nachbilden zu können und hat nach kurzer Zeit das Fehlerbild reproduzieren können. Demnach prüft die Software nach der Anmeldung lediglich die Zugriffsberechtigung auf das System und gibt nach dieser Prüfung die Daten frei.

Jeder Nutzer des Systems erhält eine UUID (universally unique identifier), welche diesen als eindeutigen Nutzer des Systems ausweist. Diese wird bei der erstmaligen Anmeldung vergeben und ist lediglich in der Adresszeile des Browsers ersichtlich.

Im vorliegenden Fall hat der Lehramtsstudent sich nicht mit der ihm zugewiesenen UUID im Browser angemeldet, sondern sein Login mit der UUID der fraglichen Studentin verwendet. Das System hat nun lediglich geprüft, ob der Nutzer Zugang zum System erhalten darf, was korrekt war. Nicht geprüft wurde, ob die UUID und das Login zueinander passen. Folglich konnte der Student mit seinem Login die Daten der Studentin einsehen.

Wie der Student an die UUID der Studentin gekommen sein mag, darüber kann nur spekuliert werden. Da es für die Beurteilung des Falles aber keine weitere Rolle gespielt hat, habe ich den Studenten dazu auch nicht näher befragt. Möglich, aber unwahrscheinlich, ist eine eigenhändige Manipulation der URL, in dem eine andere UUID einfach ausprobiert wurde. Unwahrscheinlich deshalb, weil diese langen Zahlenketten (in aller Regel 36 Zeichen) nach dem Zufallsprinzip gebildet werden und damit ein Erraten erschwert ist. Viel wahrscheinlicher ist es, dass die UUID im Browserverlauf eines gemeinsam genutzten Computers (z. B. in einer öffentlichen Bibliothek) zufällig auf-

tauchte, nachdem ein nachfolgender Nutzer (hier der Student) die Adresse im Browser eingegeben hat.

Das Systemverhalten war trotz des Umstandes, dass die URL mit der UUID unter normalen Umständen keinem Dritten zur Kenntnis gelangen sollte, ein schwerer Verstoß gegen den Datenschutz und die Informationssicherheit.

Die Bildungsagentur und das zuständige SMK haben auf den Vorfall hinreichend schnell und umfassend reagiert. Gemeinsam mit der Entwicklerfirma wurde eine Programmroutine zum Abgleich der UUID mit dem angemeldeten Nutzer implementiert, welche derartige Vorfälle in Zukunft verhindert. Ich habe angeregt, eine temporäre Abschaltung des Systems bis zur Behebung des Fehlverhaltens zu prüfen und zu dokumentieren. Ebenso habe ich im Rahmen der Prüfung des Verfahrens Mängel bei der Dokumentation festgestellt, welche mittlerweile behoben sind.

Für Nutzer von Online-Systemen mit Anmeldung und dahinter hinterlegten persönlichen Daten empfehle ich bei der Nutzung öffentlich zugänglicher Computer natürlich immer ein Löschen des Browserverlaufs nach der Nutzung oder besser gleich die Nutzung des privaten Modus des Browsers. Unter Umständen bieten die URLs im Browserverlauf eventuell doch die Möglichkeit, ob gewollt oder nicht, mehr über uns Preis zu geben, als wir wollen.

14.3 Weiterentwicklung und Einsatz des Standard-Datenschutzmodells

Die 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat am 9. und 10. November 2016 in Kühlungsborn das Standard-Datenschutzmodell (SDM) in der Version 1.0 zustimmend zur Kenntnis genommen und empfiehlt dessen Erprobung und Anwendung in der Kontroll- und Beratungspraxis für Datenschutzbehörden sowie interne Datenschutzbeauftragte und -interessierte.

Das SDM wurde im Auftrag der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder von einer Arbeitsgruppe der Aufsichtsbehörden entwickelt. In Abstimmung befindet sich derzeit ein Maßnahmenkatalog, welcher künftig Bestandteil des SDM sein wird und in Abhängigkeit der technischen Entwicklung in kürzeren Zyklen überarbeitet werden wird als das SDM selbst.

Das SDM kann als Grundlage für Datenschutzprüfungen und -beratungen im Hinblick auf technisch-organisatorische Maßnahmen genutzt werden, ohne dass dadurch die Unterschiede in den Datenschutzgesetzen der Länder und des Bundes eingeebnet wer-

den und die Unabhängigkeit der Datenschutzaufsicht aufgehoben wird. Vielmehr sollen das Modell und der Katalog Technikern und Juristen einen Weg eröffnen, das gebotene Recht in zweckmäßige und rechtskonforme Technik umzusetzen und dabei eine gemeinsame Sprache zu finden. Das Standard-Datenschutzmodell soll Wirkung sowohl im innerdeutschen als auch im europäischen Datenschutz- und Informationssicherheitsdiskurs entfalten. Dies beinhaltet eine enge Abstimmung mit den Standardisierungsaktivitäten des nationalen IT-Planungsrates (ITPR) als auch eine Orientierung auf die Entwicklungen rund um die Datenschutz-Grundverordnung der EU. Das Modell orientiert sich methodisch am etablierten IT-Grundschutz des BSI und wird im Rahmen der Modernisierung des BSI-Grundschutzes in die Diskussion eingebracht.

14.4 Datenschutz und Informationssicherheit transparent und ohne Aufbau von ‚Herrschaftswissen'

In einem Fall wandte sich eine Behörde im Berichtszeitraum an mich, bei der „Rückgewinnung" von Informationen über Infrastruktur und IT-Verfahren zu unterstützen.

Eigentlich ein Klassiker und gut geeignet als Vorlage für Schulungen zu den Themen Datenschutz und Informationssicherheit. Was war geschehen?

Über viele Jahre hatte der für die IT zuständige Kollege IT-Verfahren aufgebaut und betrieben, Netzwerke konfiguriert, Rechte vergeben. Es ‚funktionierte' augenscheinlich und war somit für die Verwaltungsleitung nicht Gegenstand von anlassbezogenen Auseinandersetzungen. Bis zu dem Tag, an dem das altersbedingte Ausscheiden des verantwortlichen Kollegen in Sichtweite geriet und somit auch die notwendige Frage der Nachfolgeregelung. Idealerweise – wenn auch aufgrund der Organisationsmodalitäten längst nicht der Normalfall – sollte ein Nachfolger vor Ausscheiden eines Wissensträgers mit der Weiterführung dieser Aufgaben betraut werden, um rechtzeitig die notwendige Vertrautheit mit den Details der Informations- und Kommunikationstechnik durch Wissenstransfer sicherzustellen. So zumindest die Theorie. Im vorliegenden Fall war dies nicht möglich und der ausscheidende Mitarbeiter krankheitsbedingt auch nur in zeitlich sehr begrenztem Umfang verfügbar. Unterlagen waren nur bedingt aussagefähig oder fehlten vollständig, eine Korrektur oder nachträgliche detaillierte Darstellung war aufgrund der eingetretenen Situation nicht mehr möglich.

Dabei sollte eigentlich, auch entsprechend des Schutzzieles „Transparenz" nach § 9 SächsDSG, in jeder Einrichtung oder Behörde eine vollständige und aussagekräftige Dokumentation zu den Betriebsprozessen und Verfahren vorliegen, was in der Praxis über die Verfahren hinausgehen sollte, in denen personenbezogene Daten verarbeitet werden. Für diese Gruppe an Verfahren greift ja ohnehin zusätzlich § 10 SächsDSG mit

seinen Vorgaben zum Verzeichnis automatisierter Verarbeitungsverfahren, der Meldepflicht, vor allem aber auch der Vorabkontrolle durch den zuständigen Datenschutzbeauftragten.

Im vorliegenden Fall wurde jedoch schnell deutlich, dass weder die betriebene Infrastruktur noch die darauf aufgesetzten Verfahren in der gebotenen Art und Weise dokumentiert worden waren. Vorabkontrollen waren zu einzelnen Verfahren zwar durchgeführt worden, jedoch ohne dazu im Detail technische Spezifika zu beschreiben.

In der Verwaltungspraxis ist dies leider kein Sonderfall, wie ich bei Prüfungen immer wieder feststellen muss. Personalsituation und Aufgabenverdichtung führen oft zu einer Priorisierung der Sicherstellung laufender Prozesse, ohne das ausreichend Zeit eingeräumt werden kann, diese Prozesse auch angemessen zu dokumentieren oder im Falle von technischen Änderungen auf dem aktuellen Stand zu halten.

Dieses Informationsvakuum beim Ausscheiden eines Wissensträgers nachträglich zu füllen, kann sich zu einer zeitlich aufwändigen und dadurch auch kostspieligen Angelegenheit entwickeln. Im vorliegenden Fall wurde unter meiner Mitwirkung eine entsprechende Fachfirma hinzugezogen, die – in enger Zusammenarbeit mit der Behörde und dem inzwischen neu eingestellten IT Administrator – und mit strukturierter Herangehensweise eine gründliche Inventur der Informations- und Kommunikationslandschaft durchführen musste.

Von einer Beanstandung habe ich in diesem Fall abgesehen. Die Verwaltungsleitung hatte das Versäumnis erkannt und war nach Kräften bemüht, einen ordnungsgemäßen Zustand wiederherzustellen. In diesem Fall war die Lektion gelernt worden. Ganz allgemein steht aber dahinter für jede öffentliche Stelle die Frage, wie vollständig und aktuell das erforderliche IT Know-how beschrieben und ggf. auch auf mehrere Personen verteilt ist, sodass die Kontinuität von Verfahren verantwortungsvoll sichergestellt werden kann. Und das nicht nur im Falle eines eigentlich lange absehbaren altersbedingten Ausscheidens des Wissensträgers.

14.5 Verschlüsselung von Webseiten - Totgesagte leben länger

Wie bereits im letzten Tätigkeitsbericht dargestellt, habe ich schon 2014 in einer Arbeitsgruppe der Landesverwaltung mitgewirkt, die sich die Erarbeitung von Handlungsempfehlungen zur Verbesserung der Sicherheit von Webservern zur Aufgabe gemacht

hatte. Dies war aufgrund der mit dem so genannten Heartbleed[1]-Fehler verbundenen Konsequenzen auch dringend erforderlich geworden.

Die im Endeffekt aufgestellten Handlungsempfehlungen (siehe 17/17.2.2, S. 217) sind von allen relevanten IT-Gremien der sächsischen Landesverwaltung angenommen und beschlossen worden. Umgesetzt wurden diese beschlossenen Maßnahmen bis Ende 2015 jedoch nur teilweise, weshalb eine erneute Erwähnung des Themas auch im aktuellen Tätigkeitsbericht geboten ist. Kritikwürdig bleibt zum einen, dass für die Beantragung von Domänennamen bis heute keine klare organisatorische Regelung getroffen wurde und vor allem für die Beantragung von Event- oder Projektwebseiten praktisch Wildwuchs fortbesteht, was sich in der Praxis häufig in Zertifikatsfehlern auf den zugehörigen Webservern widerspiegelt.

Schwerer wiegt, sowohl aus Informationssicherheits- wie auch aus Datenschutzsicht, dass 2014 beschlossene Sicherheitsparameter bis 2017 entgegen der Beschlusslage nur in geringem Umfang umgesetzt wurden. Beispielsweise wären dazu zu nennen:

- die HTTPS-Verschlüsselung aller Webseiten (bis Ende 2015 zu ca. 70 % umgesetzt)
- per HSTS die Nutzung von HTTPS erzwingen (bis Ende 2015 zu 2 % umgesetzt)
- per Forward Secrecy die nachträgliche Entschlüsselung verhindern (zu 70 % umgesetzt)

Exemplarisch sei hier auch die Abschaltung des vom BSI als unsicher eingestuften RC4 Verschlüsselungsalgorithmus genannt. Obwohl dieser Algorithmus bis Ende 2014 in allen Webservern mit Präsentationen sächsischer Landesverwaltungen lt. Beschlusslage hätte abgeschaltet sein müssen, waren im April 2017 noch immer über 60 Landeswebseiten damit aktiv. Das ist nicht akzeptabel und macht deutlich, dass nicht nur die Beschlüsse, sondern auch deren Umsetzung mit entsprechender Aufmerksamkeit und Wirksamkeit verfolgt werden müssen. Mit der Inbetriebnahme des neuen Verwaltungsnetzwerkes (SVN2) werden bestehende Webseiten in dessen neue Infrastruktur zu überführen sein. Ich befürworte ausdrücklich, dies zum Anlass zu nehmen, bestehende Sicherheitslücken auf Webservern der sächsischen Behörden und Einrichtungen konsequent zu beseitigen.

[1] https:/de.wikipedia.org/wiki/Heartbleed.

15 Vortrags- und Schulungstätigkeit

Am 17. März beging die Behörde des Sächsischen Datenschutzbeauftragten ihr 25-jähriges Bestehen mit einem Festakt im sogenannten „Ständehaus“, dem historischen Landtagsgebäude Sachsens.

In den Redebeiträgen zu der Veranstaltung wurde die Entwicklung des Datenschutzrechts in Sachsen und der Behörde des Sächsischen Datenschutzbeauftragten dargestellt. Deren Rolle, als am Grundrechtsschutz orientierte Institution und ihre unterstützende Beratung im parlamentarischen Betrieb, wurde dabei besonders gewürdigt. Das Thema des Datenschutzes als eines der zentralen Grundrechte und dessen Zukunft, vor allem im Hinblick auf die europarechtliche *Datenschutz-Grundverordnung*, war bei dieser Veranstaltung von zentraler Bedeutung.

Mit der *Datenschutz-Grundverordnung* wird das Datenschutzrecht bis 2018 in Deutschland europaeinheitlich umfassend reformiert (siehe 1.1 bis 1.7). Viele der bisher geltenden Grundsätze aus dem allgemeinen oder bereichsspezifischen Datenschutz werden damit ergänzt bzw. umfassend neu geregelt. Die Datenschutz-Grundverordnung führt zudem Verfahren und Rechtsinstrumente ein, die über die bisher bestehenden gesetzlichen Regelungen hinausgehen. Der Sächsische Datenschutzbeauftragte unterstützt die öffentlichen Stellen bei der Vorbereitung auf den künftigen Rechtsrahmen. Hierzu fanden Veranstaltungen und Vorträge des Sächsischen Datenschutzbeauftragten, z. B. für Vertreter von Kommunalverwaltungen statt. Die Informationsveranstaltungen zu diesem Thema werden in Zukunft noch stark auszubauen sein.

In meiner Rolle als eine grundrechtsschützende Institution, nahm ich an einer Reihe von Veranstaltungen und Podiumsdiskussionen teil, die sich den neuen Herausforderungen an Staat und Verwaltung widmeten. Die Veranstaltung „Digitalisierung und Überwachung – 2 Welten im Konflikt“ und das „Sächsische IT- und Organisationsforum 2016“ seien hier beispielhaft genannt, in denen das Grundrecht auf Datenschutz in seinem Spannungsverhältnis zu neuen Herausforderungen beleuchtet wurde. U. a. Gefahren von Big Data, sicherheitsbehördliche Intensivierung in der Datenverarbeitung und staatliche Überwachungsmaßnahmen konnten bei diesen Gelegenheiten kontrovers diskutiert werden.

Aus der Justizverwaltung wurden im Berichtszeitraum Datenschutzbeauftragte der Justiz (Gerichte, Staatsanwaltschaften, Justizvollzugsanstalten) und ca. 70 Rechtsreferendare aus dem gesamten OLG-Bezirk Sachsen zum Thema Datenschutz fort- bzw. ausgebildet.

Auf Anfrage fanden des Weiteren zu unterschiedlichen Themen des Datenschutzrechts Vorträge z. B. für die Sächsische Landesärztekammer, das Insolvenzverwalter-Forum Leipzig, KPMG Leipzig, den Jüdischen FrauenVerein, die Hochschule Mittweida, den Bund Deutscher Kriminalbeamter und auch vor einer georgischen Delegation im Rahmen eines Studienbesuchs in einem EU-Twinning-Projekt statt.

Die Themen Datenschutz und IT-Sicherheit, Datenschutz und Cybercrime, Datenschutz in Smart Cities und der Datenschutz im 21. Jahrhundert standen auch bei der Fortbildung von mit meiner Behörde kooperierenden Verbänden im Vordergrund. Für die Zielgruppe der IT-Nutzer fanden Veranstaltungen zum (Selbst-)Datenschutz und zur Informationssicherheit bei der Nutzung von Internet und sozialer Netzwerke statt, die neben Erwachsenen auch von Senioren und Schülern gern in Anspruch genommen wurden.

Auch im schulischen Bereich fand im Berichtszeitraum eine Vielzahl von Veranstaltungen statt. Der Schwerpunkt der Vorträge befasste sich inhaltlich mit Datenschutz und digitalen Medien und rechtlichen und technischen Möglichkeiten für Schulen. Dieser Themenbereich war zudem Gegenstand vieler schulinterner Lehrerfortbildungen aber auch z. B. von Fortbildungsveranstaltungen für stellvertretende Schulleiter, die durch Bedienstete meiner Behörde erfolgten.

Gemeinsam mit Partnern aus dem Kultus- und Polizeibereich unterstützte ich anlässlich des Safer-Internet-Day 2015 den datensicheren und geschützten Umgang mit Medien von Kindern und Jugendlichen mit Schülerworkshops. Auch unabhängig von diesem Aktionstag fanden Veranstaltungen für Schüler, die zur Sensibilisierung für die Risiken im Umgang mit den digitalen Medien zum Ziel haben, statt. Beispielhaft werden bei diesen unter anderem die Funktionsbedingungen des digitalen Zeitalters, die bestehenden Datenschutzrechte und Möglichkeiten vorgestellt, sich im Netz selbst helfen zu können sowie Geräte entsprechend zu konfigurieren und zu verschlüsseln.

Im Berichtszeitraum fanden in Zusammenarbeit mit der TU Dresden (Professur für Didaktik der Informatik der Fakultät Informatik und der Professur für Medienpädagogik der Fakultät Erziehungswissenschaften) eine Reihe medienpädagogischer und datenschutzrechtlicher Aus- und Weiterbildungen von Lehramts-Studenten und Teilnehmern im berufsbegleitenden Studium statt. In Kooperation mit der Sächsischen Bildungsagentur, dem Sächsischen Bildungsinstitut und den Medienpädagogischen Zentren der Sächsischen Bildungsagentur führte ich darüber hinaus viele Fortbildungen zu Medienbildung und Datenschutz in der Schule durch. Beispielhaft erwähnt seien die Schulungen in Beruflichen Schulzentren, bei denen neben den Rechtsgrundlagen und Grundprinzipien des allgemeinen und schulischen Datenschutzrechts auch für die Unterrichts-

praxis bedeutsame Themen vermittelt wurden, wie die Sensibilisierung für Datenschutzrisiken, Betroffenenrechte und Möglichkeiten, sich im Netz selbst helfen zu können.

Der Sächsische Datenschutzbeauftragte ist auch Ausbildungsstätte und Station für Rechtsreferendare. Im Berichtszeitraum wurden vier Rechtsreferendare und vier Praktikanten ausgebildet bzw. betreut.

16 Ordnungswidrigkeitenverfahren

In diesem Jahr nicht belegt.

17 Materialien

17.1 Entschließungen der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder

17.1.1 Entschließung zwischen der 89. und 90. Konferenz vom 9. Juni 2015: Gegen den Gesetzentwurf zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten bestehen erhebliche verfassungsrechtliche Bedenken

Mit der Vorlage des „Entwurfs eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ (BR-Drs. 249/15) beabsichtigt die Bundesregierung, eine Vorratsspeicherung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung und der Gefahrenabwehr in Deutschland einzuführen.

Nach Ansicht der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist fraglich, ob dieser Gesetzentwurf den verfassungsrechtlichen und europarechtlichen Anforderungen genügt.

Schon vorherige Regelungen waren vom Bundesverfassungsgericht und vom Europäischen Gerichtshof für unwirksam erklärt worden, weil unzulässig in Grundrechte, insbesondere in das Telekommunikationsgeheimnis und das Recht auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, eingegriffen wurde.

Mit einer Vorratsdatenspeicherung wird massiv in Freiheitsrechte von allen Menschen unabhängig von einem konkreten Verdacht eingegriffen. Deshalb müssen derartige Maßnahmen, die nur als absolute Ausnahme überhaupt zulässig sein können, einer strengen Erforderlichkeits- und Verhältnismäßigkeitsprüfung unterzogen und durch technische, organisatorische und verfahrensrechtliche Vorkehrungen abgesichert werden. Die Konferenz kann nicht erkennen, dass die Regelungen grundrechtlichen Anforderungen genügen. Dies gilt namentlich für die Kommunikation mit Berufsgeheimnisträgern (z. B. Abgeordneten, Ärzten, Rechtsanwälten und Journalisten). Auch die Vorgaben des Europäischen Gerichtshofs sind nicht vollumfänglich berücksichtigt.

Die Bundesregierung hat bisher nicht hinreichend begründet, dass die Speicherung von Standort- und Kommunikationsdaten erforderlich ist, zumal die Gutachten des Max-Planck-Instituts (2011) und des Wissenschaftlichen Dienstes des Deutschen Bundestags (2011) die Wirksamkeit der Maßnahme in Frage gestellt haben. Zudem wurde die gerichtliche Vorgabe, hinsichtlich der Datenarten, deren Speicherfristen und Verwendungszwecken zu differenzieren, nur unzureichend umgesetzt. Ein für derart intensive Grundrechtseingriffe ausreichendes Maß an Bestimmtheit fehlt, wenn unbestimmte Rechtsbegriffe (z. B. angemessenes Verhältnis oder ein besonderes Schwerwiegen einer

Tat) verwendet werden und den Sicherheitsbehörden somit ein weiter Spielraum eröffnet wird.

Der Entwurf sieht keine Evaluierung vor. Neue Maßnahmen mit einem derartigen Eingriffspotential sollten jedoch nach einer bestimmten Frist von unabhängiger Seite auf deren Wirksamkeit wie auch auf die Beeinträchtigung von Grundrechten bewertet werden, um hieraus gesetzgeberische Schlüsse zu ziehen.

Die Konferenz fordert wegen der großen grundrechtlichen Bedeutung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und wegen der Signalwirkung einer deutschen Regelung für Europa, dass der Vorschlag der Bundesregierung in einem ergebnisoffenen Verfahren mit umfassender Öffentlichkeitsbeteiligung erörtert wird.

17.1.2 Entschließung der 90. Konferenz am 30. September und 1. Oktober 2015 in Darmstadt: Verfassungsschutzreform bedroht die Grundrechte

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt die mit dem „Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes“ (BR-Drs. 123/15 und 382/15) beschlossene Verfassungsschutzreform ab. Die vorgesehenen Gesetzesänderungen sind in zentralen Punkten verfassungsrechtlich äußerst bedenklich. Das betrifft insbesondere die praktisch unbegrenzten Befugnisse der Verfassungsschutzbehörden, personenbezogene Daten in umfassenden und zentralen Dateien zu speichern.

Das Gesetz sieht u. a. vor, Aufgaben und Informationen beim Bundesamt für Verfassungsschutz zu zentralisieren. Es erweitert die Verpflichtungen der Verfassungsschutzbehörden, Daten untereinander auszutauschen, erheblich. Zudem ermöglicht es den Austausch mit Polizeibehörden in einem Maß, welches der Rechtsprechung des Bundesverfassungsgerichtes zum informationellen Trennungsprinzip (Urteil vom 24. April 2013, 1 BvR 1215/07) widerspricht. Es schafft weiter die rechtliche Grundlage, das zentrale nachrichtendienstliche Informationssystem (NADIS) von einem reinen Indexsystem zu einem vollumfänglichen Informationssystem auszubauen. Dies geschieht vor allem dadurch, dass nach dem Gesetzeswortlaut zu allen gespeicherten Personen und Objekten zukünftig auch die zugehörigen Dokumente, Bilder, Video- oder Audiomaterial in NADIS gespeichert werden können und sollen. Auf die erheblichen Risiken von Recherchen in solch umfassenden Dateien hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits frühzeitig mit ihrer Entschließung vom 4. November 2010 „Keine Volltextsuche in Dateien der Sicherheitsbehörden“ hingewiesen. Das Bundesamt für Verfassungsschutz erhält schließlich in Konkurrenz zu den Ländern operative Zuständigkeiten auch für nicht länderübergreifende gewaltorientierte

Bestrebungen. Die Verfassungsschutzbehörden der Länder werden faktisch auf die Rolle von Datenlieferanten für das Bundesamt für Verfassungsschutz reduziert.

Es fehlt nach wie vor an einer umfassenden und systematischen Analyse bisheriger Versäumnisse und Vollzugsdefizite. Diese hatte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits mit Beginn der Überlegungen zu einer Reform des Verfassungsschutzes gefordert (Entschließung vom 8. November 2012 „Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben“). Offen bleibt so insbesondere die Frage, ob die Verfassungsschutzbehörden bestehende Befugnisse in der Vergangenheit richtig angewendet haben. Gleichwohl werden nunmehr die Befugnisse der Verfassungsschutzbehörden noch erweitert. Bestehende Defizite der rechtsstaatlichen Kontrolle über die Nachrichtendienste löst das Gesetz ebenfalls nicht. Dabei hat vor allem der Abschlussbericht des NSU-Untersuchungsausschusses des Bundestages ein erhebliches Kontrolldefizit aufgezeigt. Auch hier hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits eine verfassungskonforme Gestaltung der Kontrolle angemahnt (Entschließung vom 9. Oktober 2014 „Effektive Kontrolle von Nachrichtendiensten herstellen!“).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält an ihrer Forderung gegenüber dem Gesetzgeber fest, das Recht der Nachrichtendienste maßvoll und verfassungskonform auszugestalten. Dies ist mit diesem Gesetz misslungen. Das Gesetz stellt einen weiteren Schritt zur Aushöhlung des Rechts auf informationelle Selbstbestimmung dar.

17.1.3 Entschließung der 90. Konferenz am 30. September und 1. Oktober 2015 in Darmstadt: Cloud-unterstützte Betriebssysteme bergen Datenschutzrisiken

Namhafte Hersteller weit verbreiteter Betriebssysteme (z. B. Apple, Google, Microsoft) bieten in zunehmendem Maße neue Versionen dieser Software an, die im Unterschied zu den herkömmlichen Betriebssystemen auf internetbasierte Cloud-Services zurückgreifen. Die Standardeinstellungen dieser neuen Betriebssysteme führen oftmals dazu, dass zunehmend personenbezogene Daten aller Art vom lokalen Endgerät (Personalcomputer, Laptop, Tablet, Smartphone) an die Betriebssystem-Hersteller oder deren Cloud-Dienste übertragen werden. Dadurch erhält der Hersteller Informationen, die es ihm erlauben, das Verhalten der Benutzer nachzuvollziehen und im Detail zu analysieren.

Mit derartigen Betriebssystemen vollziehen die Hersteller einen Paradigmenwechsel, dessen tatsächliche und mögliche Auswirkungen auf den Umgang mit personenbezo-

genen Daten längst nicht allen Anwendern, d. h. Benutzern und für den IT-Einsatz Verantwortlichen, klar sein kann. Die Hersteller schaffen sich den Zugang zu einer Vielzahl personenbezogener Daten, sofern die Standardeinstellungen nicht aktiv durch die Anwender verändert werden. Weitreichende Datenverarbeitungsbefugnisse können nicht dadurch gerechtfertigt werden, dass Nutzern auf Basis von AGB oder datenschutzunfreundlichen Voreinstellungen lediglich ein Opt-Out ermöglicht wird.

Insoweit ist es erforderlich, der Datenherrschaft von Nutzern durch technisch unterstützte Einwilligungslösungen zu entsprechen. Solange nicht unabhängige Dritte die Wirkung der Einstellungen auf den Datenschutz geprüft haben, ist selbst nach deren Änderung häufig unklar, wie weit Datenübertragungen tatsächlich eingeschränkt werden, welche Daten im Detail betroffen sind und zu welchen konkreten Zwecken diese Daten erhoben werden sollen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Hersteller dieser Betriebssysteme auf, die Software mit datenschutzfreundlichen Voreinstellungen auszuliefern. Darüber hinaus sind die Anwender detailliert und fortlaufend darüber zu informieren, welche Daten unter welchen Voraussetzungen zu welchen Zwecken übertragen werden. Nur so können sie einschätzen, ob sie die Software unter den gegebenen Umständen erwerben bzw. verwenden wollen. Zudem müssen Anwender die Möglichkeit haben, auf einfache Weise selbst festzulegen, welche Daten lokal gespeichert bleiben sollen und welche Daten in die Cloud bzw. an den Hersteller übermittelt werden.

Den Benutzern der neuen Betriebssysteme empfehlen die Datenschutzbeauftragten von Bund und Ländern, sich möglichst schon vor dem Kauf detailliert über die Funktionsweise zu informieren und alle Möglichkeiten der datenschutzfreundlichen Einstellungen der Betriebssysteme zu nutzen. Insbesondere die Verantwortlichen im behördlichen und kommerziellen Umfeld sind angehalten vor der Entscheidung für einen Einsatz zu prüfen, ob für ihr Umfeld zugeschnittene Betriebssystemversionen verfügbar sind und ob sie bei der Nutzung der neuen Betriebssysteme ihrer datenschutzrechtlichen Verantwortung als Daten verarbeitende Stelle gerecht werden können.

17.1.4 Entschließung der 91. Konferenz am 6./7. April 2016 in Schwerin: Wahrung der Freiheits- und Persönlichkeitsrechte bei der Bekämpfung des internationalen Terrorismus

Rechtsstaat und Grundrechtsschutz – damit auch Datenschutz – stehen einer effektiven Bekämpfung des Terrorismus nicht entgegen.

Auch nach Brüssel gilt: Datenschutz verhindert nicht, Terroristen und ihre Helfernetzwerke zu erfassen und zu bekämpfen. Das geltende Datenschutzrecht erlaubt deren Daten zu speichern und Informationen wechselseitig auszutauschen. Der Datenschutz kann jedenfalls nicht für etwaige Defizite bei der Nutzung vorhandener Eingriffsbefugnisse sowie für möglicherweise ineffiziente sicherheitsbehördliche Strukturen verantwortlich gemacht werden.

Die häufig reflexartig erhobene Forderung nach weiteren Eingriffsbefugnissen und flächendeckenden Überwachungsmaßnahmen trägt zur Bekämpfung des internationalen Terrorismus nicht bei.

Es kennzeichnet den Rechtsstaat, dass sich jeder in einem fairen Verfahren gegen unberechtigte Verdachtsbehauptungen wehren, Schutz bei Gerichten suchen und auf die Kontrolle der Datenschutzbeauftragten vertrauen darf. Die massenhafte, verdachtsunabhängige Erhebung und Speicherung von Daten widerspricht dem Grundrecht auf Datenschutz.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt ihren mehrfach formulierten Appell[*], dass alle neu erwogenen Maßnahmen zur Bekämpfung des internationalen Terrorismus sich daran messen lassen müssen, ob sie für dessen wirkungsvolle Bekämpfung wirklich geeignet, erforderlich und angemessen sind und damit dem Verfassungsgrundsatz der Verhältnismäßigkeit entsprechen.

[*] - Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. Oktober 2001 in Münster
- Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. Oktober 2006 in Naumburg
- Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München
- Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19. März 2015 in Wiesbaden

17.1.5 Entschließung der 91. Konferenz am 6./7. April 2016 in Schwerin: Datenschutz bei Servicekonten

Der IT-Planungsrat hat sich in einem Beschluss in seiner 17. Sitzung im Juni 2015 für eine flächendeckende Verbreitung so genannter Servicekonten für Bürgerinnen, Bürger und Unternehmen ausgesprochen. Über diese Konten soll es künftig möglich sein, sich einfach für die Inanspruchnahme von Verwaltungsdienstleistungen auf kommunaler, Länder- und Bundesebene zu identifizieren. Dabei soll der neue Personalausweis mit seiner eID-Funktion eine wichtige Rolle spielen. Eine Projektgruppe des IT-Planungsrates erarbeitet zurzeit die rechtlichen und technischen Rahmenbedingungen für Servicekonten.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder nimmt die Aktivitäten des IT-Planungsrates zur Kenntnis, den Zugang zu elektronischen Verwaltungsdienstleistungen zu erleichtern und möglichst medienbruchfrei auszugestalten. Sie weist darauf hin, dass insbesondere die Einrichtung von länderübergreifenden Servicekonten gewichtige verfassungsrechtliche Fragen etwa zum Bund-Länder-Verhältnis und zum Persönlichkeitsrecht aufwerfen. So ist dabei das Verbot einer Vorratsdatenspeicherung zu unbestimmten Zwecken sowie das grundrechtliche Prinzip der informationellen Gewaltenteilung zu beachten. Servicekonten dürfen die gesetzliche Zuständigkeits- und Aufgabenverteilung der öffentlichen Verwaltung nicht unterlaufen.

Hiervon abgesehen müssen jedenfalls die Datenschutzprinzipien der Datensparsamkeit, der Nichtverkettbarkeit und der Transparenz berücksichtigt werden. Für die Integration von Verwaltungsdienstleistungen heißt das insbesondere, dass auch die Schnittstellen zwischen den Systemen so definiert sein müssen, dass nur die für den vorgesehenen Zweck erforderlichen Daten übertragen werden. Dazu sind folgende Rahmenbedingungen einzuhalten:

- Auch künftig muss es möglich sein, ohne Servicekonto Verwaltungsdienstleistungen in Anspruch zu nehmen.
- Die einmalige Inanspruchnahme von Verwaltungsdienstleistungen muss auch ohne dauerhafte Speicherung identifizierender Daten möglich sein. Für diese Zwecke sollten temporäre Servicekonten eingerichtet werden.
- Bürgerinnen und Bürgern muss die Möglichkeit eingeräumt werden, sowohl einzelne im permanenten Servicekonto dauerhaft gespeicherte, personenbezogenen Daten als auch das Konto selbst löschen zu lassen.

- Soweit Daten aus dem Servicekonto übermittelt werden, müssen diese Übermittlungen durch die Bürger im Servicekonto selbst nachvollzogen werden können.
- Für die Erhebung personenbezogener Daten in behördenübergreifenden Servicekonten ist eine Rechtsgrundlage erforderlich, da sie als Aufgabe verwaltungsorganisationsrechtlich einer Stelle zugewiesen werden muss. Der Staat darf personenbezogene Daten zur Erfüllung seiner gesetzlichen Aufgaben grundsätzlich nur auf der Basis einer klaren Rechtsgrundlage verarbeiten. Da zudem die Bedeutung dieser Servicekonten zunehmen wird und absehbar ist, dass den Betroffenen durch die Nutzung dieser Konten erhebliche Vorteile im Sinne von „Digital by Default“ eingeräumt werden sollen, reicht die Einwilligung als Rechtsgrundlage für die Datenerhebung nicht aus.
- Vorbehaltlich weiterer verfassungsrechtlicher Prüfungen ist für die Länder übergreifende Nutzung von Servicekonten eine Rechtsgrundlage erforderlich. Durch die dauerhafte Speicherung identifizierender Daten werden bundesweit nutzbare Servicekonten zu einer digitalen Meldestelle bzw. zu einer zweiten, zentralen Identifizierungsstelle neben den Meldebehörden aufgewertet. Die Rechtsgrundlage muss eindeutige Vorgaben zum Datenumfang, zu Zweckbindungsregelungen, zur Löschung und zur Transparenz der Datenverarbeitung enthalten. Daten der Betroffenen sind alleine zum Betrieb des Serviceportals und zur Erledigung der Verfahren der Nutzer zu verarbeiten. Eine Nutzung dritter Stellen zu anderen Zwecken ist gesetzlich ausdrücklich auszuschließen.
- Bevor Unternehmen verpflichtet werden sollen, die eID-Funktion für Verwaltungsangelegenheiten zu nutzen, ist zu prüfen, ob und unter welchen Voraussetzungen der Einsatz privater digitaler Identifikationsnachweise zu nichtprivaten Zwecken bzw. zur Erfüllung arbeitsvertraglicher Pflichten zulässig ist und inwieweit Arbeitnehmerinnen und Arbeitnehmer hierzu verpflichtet werden können.
- Angesichts des Abhängigkeitsverhältnisses der Arbeitnehmerinnen und Arbeitnehmer im Beschäftigungsverhältnis kann die Nutzung von Servicekonten auf der Basis der privaten eID-Funktion keinesfalls auf der Einwilligungsbasis erfolgen. Auch hierfür ist eine Rechtsgrundlage erforderlich, die die Datenverarbeitung in Servicekonten vollständig erfasst. Bei der Identifizierung eines bevollmächtigten Beschäftigten dürfen nur die für diese Identifizierung erforderlichen Daten erfasst werden.

Sichere, elektronische Identifizierungsmöglichkeiten können zur Datenschutzkonformität von E-Government- und von E-Commerce-Verfahren beitragen. Die unabhängigen Datenschutzaufsichtsbehörden begrüßen daher Maßnahmen, die zur verstärkten

Nutzung der eID-Funktion des neuen Personalausweises beitragen. Dennoch muss den Betroffenen die Möglichkeit gelassen werden, selbst zu entscheiden, ob sie die eID-Funktion freischalten und nutzen wollen. Die Datenschutzkonferenz lehnt daher die angedachte Änderung des Personalausweisgesetzes ab, wonach die eID-Funktion des neuen Personalausweises dauerhaft eingeschaltet wäre und nicht mehr deaktiviert werden könnte. Eine standardmäßige Aktivierung der eID-Funktion wäre allenfalls dann hinnehmbar, wenn den Bürgerinnen und Bürgern ein Opt-In mit Widerrufsmöglichkeit angeboten wird, um die eID-Funktion jederzeit gebührenfrei aktivieren und deaktivieren zu können.

17.1.6 Entschließung der 91. Konferenz am 6./7. April 2016 in Schwerin: Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen!

Die Datenschutzkonferenz tritt für einen effektiven Schutz der Persönlichkeitsrechte der Nutzerinnen und Nutzer von Wearables und Gesundheits-Apps ein. Einer repräsentativen Umfrage zufolge soll bereits knapp ein Drittel der Bevölkerung ab 14 Jahren sogenannte Fitness-Tracker zur Aufzeichnung von Gesundheitswerten und persönlichen Verhaltensweisen nutzen. Am Körper getragene Kleincomputer (sog. Wearables) und auf mobilen Endgeräten installierte Anwendungsprogramme (sog. Gesundheits-Apps) sammeln und dokumentieren auswertungsfähige Körperdaten. In der Regel werden diese Daten über das Internet an Hersteller, Internetanbieter und sonstige Dritte weitergeleitet.

Die digitale Sammlung und Auswertung der eigenen gesundheitsbezogenen Daten können durchaus interessante Informationen für Einzelne bieten, die zu einer besseren Gesundheitsversorgung und einem Zugewinn an persönlicher Lebensqualität beitragen können.

Allerdings stehen diesen Chancen auch Risiken, insbesondere für das Persönlichkeitsrecht, gegenüber. Zahlreiche Wearables und Gesundheits-Apps geben die aufgezeichneten Daten an andere Personen oder Stellen weiter, ohne dass die betroffenen Personen hiervon wissen oder dazu eine bewusste Entscheidung treffen. Darüber hinaus können Bedienungsfehler oder unzureichende technische Funktionalitäten dazu führen, dass Gesundheitsinformationen ungewollt preisgegeben werden. Einige Angebote weisen erhebliche Sicherheitsdefizite auf, so dass auch Unbefugte sich Zugriff auf die Gesundheitsdaten verschaffen können.

Für bestimmte Situationen besteht überdies das Risiko, dass Einzelne aufgrund massiver gesellschaftlicher, sozialer oder ökonomischer Zwänge nicht frei über die Nutzung

derartiger Technologien entscheiden können. Zum notwendigen Schutz von Gesundheitsdaten bei Wearables und Gesundheits-Apps weist die Datenschutzkonferenz auf folgende Gesichtspunkte hin:

- Die Grundsätze der Datenvermeidung und Datensparsamkeit sind zu beachten. Insbesondere Hersteller von Wearables und Gesundheits-Apps sind aufgerufen, datenschutzfreundliche Technologien und Voreinstellungen einzusetzen (Privacy by Design and Default). Hierzu gehören Möglichkeiten zur anonymen bzw. pseudonymen Datenverarbeitung. Soweit eine Weitergabe von Gesundheits- und Verhaltensdaten an Dritte nicht wegen einer medizinischen Behandlung geboten ist, sollten Betroffene sie technisch unterbinden können (lediglich lokale Speicherung).
- Die Datenverarbeitungsprozesse, insbesondere die Weitergabe von Gesundheits- und Verhaltensdaten an Dritte, bedürfen einer gesetzlichen Grundlage oder einer wirksamen und informierten Einwilligung. Sie sind transparent zu gestalten. Für das Persönlichkeitsrecht riskante Datenverwendungen, insbesondere Datenflüsse an Dritte, sollten für die Nutzerinnen und Nutzer auf einen Blick erkennbar sein. Beispielsweise könnte die Anzeige des Vernetzungsstatus die aktuellen Weitergabe-Einstellungen veranschaulichen. Eine solche Verpflichtung zur erhöhten Transparenz sollte gesetzlich verankert werden.
- Einwilligungserklärungen und Verträge, die unter Ausnutzung eines erheblichen Verhandlungsungleichgewichts zwischen Verwendern und den betroffenen Personen zustande kommen, sind unwirksam und liefern keine Rechtsgrundlage für Verarbeitungen. Das gilt namentlich für besonders risikoträchtige Verwendungszusammenhänge, etwa in Beschäftigungs- und Versicherungsverhältnissen.
- Verbindliche gesetzliche Vorschriften zur Datensicherheit, insbesondere zur Integrität und Vertraulichkeit von Daten, können nicht durch Verträge oder durch Einwilligungserklärungen abbedungen werden.
- Wer aus eigenen Geschäftsinteressen gezielt bestimmte Wearables und Gesundheits-Apps in den Umlauf bringt oder ihren Vertrieb systematisch unterstützt, trägt eine Mitverantwortlichkeit für die rechtmäßige Ausgestaltung solcher Angebote. In diesem Sinne Mitverantwortliche haben sich zu vergewissern, dass die Produkte verbindlichen Qualitätsstandards an IT-Sicherheit, Funktionsfähigkeit sowie an Transparenz der Datenverarbeitung genügen.

Die Datenschutzkonferenz fordert den Gesetzgeber auf zu prüfen, ob und inwieweit im Zusammenhang mit Wearables und Gesundheits-Apps die Möglichkeit beschränkt werden sollte, materielle Vorteile von der Einwilligung in die Verwendung von Gesundheitsdaten abhängig zu machen.

17.1.7 Entschließung der 91. Konferenz am 6./7. April 2016 in Schwerin: Stärkung des Datenschutzes in Europa – nationale Spielräume nutzen

Nach vier Jahren intensiver Diskussion ist der Text der Europäischen Datenschutz-Grundverordnung nun zwischen der Europäischen Kommission, dem Europäischen Parlament und dem Rat der Europäischen Union abgestimmt. Mit der Grundverordnung verfügt die EU über ein weiterentwickeltes, einheitliches Datenschutzrecht, das für Unternehmen und Behörden in Deutschland weitgehend Kontinuität gewährleistet. Überall in Europa soll künftig dasselbe Schutzniveau für das Grundrecht auf Datenschutz gelten. Ebenso wird feststehen, dass sich auch außereuropäische Anbieter, die ihre Waren und Dienstleistungen auf dem europäischen Markt anbieten, an das europäische Datenschutzrecht halten müssen.

Wichtige datenschutzrechtliche Prinzipien wie der Grundsatz des Verbots mit Erlaubnisvorbehalt, der Zweckbindungsgrundsatz und der Grundsatz der Datensparsamkeit sind in den Verhandlungen weitgehend erhalten geblieben.

Nach der Einschätzung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder ist es allerdings zur Erhaltung und Verstärkung des bestehenden Datenschutzniveaus auch im Lichte der jüngeren Entscheidungen des Europäischen Gerichtshofs geboten, die in der Grundverordnung enthaltenen Öffnungs- und Konkretisierungsklauseln zu Gunsten des Rechts auf informationelle Selbstbestimmung zu nutzen. Auch die von der Grundverordnung getroffenen Weiterentwicklungen des Datenschutzes wie beispielsweise die Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sowie das Erfordernis von Datenschutz-Folgeabschätzungen müssen wirksam ausgestaltet werden. Die Konferenz fordert deshalb Bundes- und Landesgesetzgeber auf, in allen gesetzgeberischen Bereichen die nationalen Spielräume im Sinne des Grundrechts auf informationelle Selbstbestimmung zu nutzen.

Insbesondere folgenden Regelungen kommt in diesem Zusammenhang hohe Bedeutung zu:

- Schaffung eines Beschäftigtendatenschutzgesetzes, mindestens jedoch Beibehaltung der §§ 3 Abs. 11, 32 BDSG (Art. 88 i. V. m. Erwägungsgrund [EG] 155),
- Beschränkungen für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten (Art. 9 Abs. 4 i. V. m. EG 53, letzte beide Sätze),

- Stärkung der Befugnisse der Aufsichtsbehörden, insbesondere Schaffung von Klagebefugnissen und effektiven Sanktionen auch gegenüber Behörden (Art. 58 und 83 Abs. 7 i. V. m. EG 150, vorletzter Satz),
- jedenfalls im öffentlichen Bereich durch die Nennung der Schutzziele Datensparsamkeit, Vertraulichkeit, Integrität, Verfügbarkeit, Nichtverkettbarkeit, Transparenz und Intervenierbarkeit, um einen einfachen, flexiblen und praxistauglichen technischen und organisatorischen Datenschutz zu konkretisieren (Art. 6 Abs. 2, 25, 32),
- Begrenzung der Zweckänderung bei Videoüberwachung öffentlich zugänglicher Räume durch Private, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist (Art. 6 Abs. 4),
- Beibehaltung der Verpflichtung in § 4f Abs. 1 BDSG einen betrieblichen Datenschutzbeauftragten zu bestellen (Art. 37 Abs. 4).

17.1.8 Entschließung zwischen der 91. und 92. Konferenz vom 20. April 2016: Klagerecht für Datenschutzbehörden – EU-Kommissionsentscheidungen müssen gerichtlich überprüfbar sein

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) fordert den Gesetzgeber auf, umgehend ein eigenständiges Klagerecht für die unabhängigen Datenschutzbehörden vorzusehen. Wenn die unabhängigen Datenschutzbehörden der Auffassung sein sollten, dass eine Entscheidung der EU-Kommission rechtswidrig ist, wären sie gleichwohl an diese gebunden. Sie müssten daher ggf. gegen den rechtsstaatlichen Grundsatz der Gesetzmäßigkeit der Verwaltung verstoßen. Um dies zu verhindern, sind die prozessualen Voraussetzungen dafür zu schaffen, dass die Datenschutzbehörden selbst bestehende Zweifel an der Rechtmäßigkeit einer Kommissionsentscheidung gerichtlich klären lassen können.

Anlass für die obige Aufforderung der Datenschutzkonferenz ist die zwischenzeitliche Vorlage einer Reihe von Dokumenten unterschiedlicher Repräsentanten der US-Administration durch die EU-Kommission am 29. Februar 2016, die für Unternehmen und Behörden Zusagen für den Umgang mit aus der EU übermittelten personenbezogenen Daten enthalten. Im Rahmen eines so genannten EU-US Privacy Shield sollen diese Dokumente Grundlage für eine künftige EU-Kommissionsentscheidung zur Angemessenheit des Datenschutzniveaus in den USA sein und damit als Nachfolgeregelung für die Safe Harbor-Entscheidung dienen. Letztere wurde bekanntlich am 6. Oktober 2015 durch den Europäischen Gerichtshof aufgehoben.

Gegen den „EU-US Privacy Shield“ bestehen jedoch nach Auffassung der Artikel-29-Datenschutzgruppe, dem Zusammenschluss der Datenschutzbehörden der EU-Mitgliedstaaten und des Europäischen Datenschutzbeauftragten, erhebliche Bedenken. Die Artikel-29-Dateschutzgruppe hat zum „EU-US Privacy Shield“ zuletzt am 13. April 2016 detailliert Stellung genommen. Die Datenschutzkonferenz teilt diese umfassende Analyse und unterstützt die darin enthaltene Forderung an die EU-Kommission, vor einer Beschlussfassung substantielle Nachbesserungen vorzunehmen. Die Datenschutzkonferenz ist der Auffassung, dass auch der „EU-US Privacy Shield“ in seiner derzeitigen Form nicht ausreichend ist, das für die Übermittlung personenbezogener Daten in die USA erforderliche „angemessene Datenschutzniveau“ in den USA zu gewährleisten.

Der EuGH stellt in seiner o. g. Entscheidung zur Ungültigkeit von Safe Harbor ausdrücklich klar, dass nach Maßgabe der Datenschutz-Richtlinie der nationale Gesetzgeber für die Datenschutzbehörden Rechtsbehelfe vorzusehen hat, die ihnen bei rechtlichen Zweifeln über eine Angemessenheitsentscheidung die Anrufung nationaler Gerichte ermöglichen, so dass diese den EuGH um eine Entscheidung über die Vereinbarkeit mit den europäischen Grundrechten ersuchen können.

Die Datenschutzkonferenz begrüßt und unterstützt daher ausdrücklich die Bundesratsinitiative der Freien und Hansestadt Hamburg zur zeitnahen Einräumung eines Klagerechts für die Datenschutzaufsichtsbehörden von Bund und Ländern (BR-Drs. 171/16), in der nochmals deutlich gemacht wird, „dass das vom Europäischen Gerichtshof (EuGH in seinem Urteil vom 6.10.2015 (Rechtssache C-362/14) statuierte Klagerecht für Datenschutzaufsichtsbehörden für die Gewährleistung einer effektiven Datenschutzkontrolle von besonderer Bedeutung ist“.

17.1.9 Entschließung[1] zwischen der 91. und 92. Konferenz vom 25. Mai 2016: EU-Datenschutz-Grundverordnung erfordert zusätzliche Ressourcen für Datenschutzbehörden

Am 14. April 2016 hat das Europäische Parlament dem neuen Rechtsrahmen für den Datenschutz in Europa zugestimmt. Wesentlicher Teil des Rechtsrahmens ist die EU-Datenschutz-Grundverordnung, deren Text am 4. Mai 2016 im Amtsblatt der Europäischen Union veröffentlicht wurde. Die Verordnung ist am 25. Mai 2016 in Kraft getreten und zwei Jahre später verbindlich in allen Mitgliedstaaten der Europäischen Union anzuwenden.

[1] Enthaltung Bayern (Bayerischer Landesbeauftragter für den Datenschutz und Bayerisches Landesamt für Datenschutzaufsicht).

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder weist darauf hin, dass mit der EU-Datenschutz-Grundverordnung eine Reihe neuer bzw. erweiterter Aufgaben auf sie zukommen. Hierzu gehören insbesondere:

- Bearbeitung von Beschwerden und Beratung Betroffener sowie datenschutzrechtliche Beratung und Kontrolle von Unternehmen nunmehr unter Beachtung des erweiterten räumlichen Anwendungsbereichs der Verordnung (Marktortprinzip),
- verpflichtende Beratung von Behörden und Unternehmen bei der Datenschutz-Folgenabschätzung, insbesondere im Rahmen der vorherigen Konsultation der Aufsichtsbehörde, sowie Beratung bei der Umsetzung neuer Anforderungen wie Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Privacy By Design, Privacy By Default),
- Aufbau und Anwendung eines Kooperationsverfahrens zwischen Datenschutzbehörden in Europa bei grenzüberschreitenden Datenverarbeitungen (One-Stop-Shop), Verpflichtung zur gegenseitigen Amtshilfe und umfassender Austausch von Informationen zwischen federführenden und betroffenen Aufsichtsbehörden jeweils mit kurzen Bearbeitungsfristen,
- Etablierung eines Kohärenzverfahrens zwischen den Datenschutzbehörden in Europa zur Gewährleistung der europaweit einheitlichen Anwendung der Verordnung, Mitwirkung im Europäischen Datenschutzausschuss,
- europaweit einheitliche Auslegung der Grundverordnung in Bezug auf fehlende Regelungen (z. B. zur Videoüberwachung oder zum Scoring) und neue Anforderungen (z. B. Recht auf transparente Information oder Recht auf Datenübertragbarkeit),
- Erarbeitung von Stellungnahmen und Billigung von branchenspezifischen Verhaltensregeln zur ordnungsgemäßen Anwendung der Verordnung, Erarbeitung von Zertifizierungskriterien, ggf. Durchführung von Zertifizierungen, Erarbeitung von Kriterien für die Akkreditierung von Zertifizierungsstellen, ggf. Durchführung der Akkreditierung,
- Bearbeitung von gerichtlichen Rechtsbehelfen Betroffener gegen Entscheidungen von Aufsichtsbehörden,
- Ausübung neuer bzw. erweiterter Befugnisse der Datenschutzbehörden zur Erteilung von Anordnungen gegenüber den Verantwortlichen nunmehr auch im öffentlichen Bereich sowie Berücksichtigung zusätzlicher Tatbestände für Ordnungswidrigkeiten und eines erweiterten Bußgeldrahmens.

Die Europäische Datenschutz-Grundverordnung verpflichtet die Mitgliedstaaten, die Aufsichtsbehörden zur Gewährleistung ihrer Unabhängigkeit mit den erforderlichen personellen, finanziellen und technischen Ressourcen auszustatten (Art. 52 Abs. 4

DSGVO). Aus Sicht der Datenschutzkonferenz ist es für die Bewältigung der neuen Aufgaben zwingend erforderlich, für die Datenschutzbehörden in Deutschland erweiterte personelle und finanzielle Ressourcen vorzusehen. Dies gilt bereits für die jetzt laufende Vorbereitungsphase, in der die Weichen für eine funktionierende Umsetzung der Datenschutz-Grundverordnung gestellt werden. Die Konferenz appelliert deshalb an die Gesetzgeber in Bund und Ländern, rechtzeitig die haushaltsrechtlichen Vorkehrungen für eine jeweils angemessene, erweiterte Ausstattung der Datenschutzbehörden zu treffen. Nur so lassen sich die zusätzlichen Aufgaben der Datenschutz-Grundverordnung von den Datenschutzbehörden in Deutschland effektiv wahrnehmen.

17.1.10 Entschließung der 92. Konferenz am 9./10. November 2016 in Kühlungsborn: „Videoüberwachungsverbesserungsgesetz“ zurückziehen!

Das Vorhaben des Bundesministeriums des Innern (BMI), durch ein „Videoüberwachungsverbesserungsgesetz“ Änderungen des Bundesdatenschutzgesetzes (BDSG) einzuführen, die künftig privaten Stellen den Betrieb von Videokameras zur Verhinderung von Anschlägen wie in Ansbach und Amokläufen wie in München erleichtern sollen, wird von den unabhängigen Datenschutzbehörden des Bundes und der Länder[1] abgelehnt. Der Gesetzentwurf vermag nicht zu begründen, dass die angestrebte Erleichterung der Videoüberwachung die öffentliche Sicherheit besser gewährleisten kann, als dies gegenwärtig der Fall ist. Auch die Verlagerung der Verantwortung für diese Aufgabe auf die privaten Betreiber von Einkaufszentren und öffentlichem Personennahverkehr lehnen die unabhängigen Datenschutzbehörden des Bundes und der Länder ab. Nach der nicht abschließenden Aufzählung zielt der Gesetzentwurf überwiegend auf Orte, an denen Betroffene ihre Freizeit verbringen. Gerade in diesen Bereichen, in denen sich Menschen typischerweise zur ungezwungenen Kommunikation, Erholung und Entspannung für längere Dauer aufhalten, gilt es das Persönlichkeitsrecht in besonderem Maße zu schützen.

Gleichwohl lässt es die einschlägige Bestimmung des § 6b BDSG bereits gegenwärtig zu, die Sicherheitsbelange von Personen, die sich in öffentlich zugänglichen Bereichen aufhalten, bei der Abwägung zwischen den Rechten Betroffener und den Betreiberinteressen zu berücksichtigen. Im Rahmen der Hausrechtsausübung können auch heute Kameras installiert werden, um Personen von Straftaten an den Objekten abzuhalten. Darüber hinaus kann Videotechnik zur Beweissicherung eingesetzt werden und nach § 6 Abs. 3 Satz 2 BDSG können Videobilder an Polizei-, Ordnungs- und Strafverfolgungsbehörden weitergegeben werden, wenn dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist. Die Be-

[1] Bei Enthaltung der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

gründung des BMI suggeriert, die Datenschutzaufsichtsbehörden verhinderten angesichts der angespannten Sicherheitslage die Durchführung von Videoüberwachung. Dies trifft nicht zu. Tatsächlich werden gerade im Bereich der großen Einkaufszentren, aber auch an Bahnhöfen und in Fahrzeugen des Personennahverkehrs bereits heute zahlreiche Kameras mit ausdrücklicher Billigung der Aufsichtsbehörden betrieben.

Terroristen wie auch irrational handelnde Einzeltäter, vor denen die gesetzliche Regelung schützen soll, nehmen ihren eigenen Tod bei derartigen Anschlägen bewusst in Kauf. Sie werden sich daher von ihren Taten auch nicht durch Videokameras abschrecken lassen.

Hinzu kommt, dass die Betreiber von Videoüberwachungsanlagen bereits heute meistens nicht in der Lage sind, ein Live-Monitoring durchzuführen und die Bilder der vielen Kameras durch ihr eigenes Personal so auszuwerten, dass bei Gefahren direkt und schnell eingegriffen werden kann. In der Praxis bleibt die Bedeutung der Kameras daher auf eine Speicherung auf Vorrat und für die spätere Strafverfolgung beschränkt. Auch die mögliche Erhöhung eines faktisch ungerechtfertigten subjektiven Sicherheitsgefühls könnte Grundrechtseingriffe nicht rechtfertigen. Insoweit ist die Regelung, die von den privaten Betreibern eine stärkere Gewichtung des Schutzes von Leben, Gesundheit oder Freiheit der Betroffenen bei der rechtlichen Abwägung fordert, letztlich gar nicht geeignet, das Ziel der gesetzlichen Regelung zu erreichen.

Die unabhängigen Datenschutzbehörden des Bundes und der Länder betonen mit Nachdruck, dass es nicht die Aufgabe privater Stellen ist, die Sicherheit der Bevölkerung zu gewährleisten. Dies obliegt allein den Sicherheitsbehörden, die über ausreichende landes- und bundesgesetzliche Grundlagen sowohl für die Gefahrenabwehr als auch für die Strafverfolgung verfügen.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Bundesinnenminister auf, den Gesetzentwurf zurückzuziehen.

17.1.11 Entschließung der 92. Konferenz am 9./10. November 2016 in Kühlungsborn: Gemeinsame Prüfung der Falldatei Rauschgift deckt gravierende Mängel auf – Konsequenzen für polizeiliche Datenverarbeitung notwendig

Die Datenschutzbeauftragten des Bundes und der Länder[1] Baden-Württemberg, Bayern, Berlin, Brandenburg, Bremen, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen-Anhalt, Schleswig-Holstein und Thüringen haben parallel die bundesweit geführte „Falldatei Rauschgift“ (FDR) datenschutzrechtlich geprüft.

Die FDR ist eine bundesweite Verbunddatei, in der Informationen über sichergestellte Drogen und Verstöße gegen das Betäubungsmittelgesetz gespeichert werden. Sie wird auf Grundlage des Bundeskriminalamtgesetzes (BKAG) zentral beim Bundeskriminalamt geführt. Die Polizeien aller Länder und die Zollfahndung haben Zugriff auf die Datei und können direkt Daten einspeichern und abrufen. Die Datenschutzbeauftragten haben im Rahmen ihrer Kontrollen sowohl die Struktur der Datei als auch Einzelspeicherungen überprüft.

Die Prüfung hat im Wesentlichen folgende Mängel aufgedeckt:

- Vielfach haben die Behörden nicht ausreichend geprüft, ob die Voraussetzungen des § 2 BKAG (Straftat von länderübergreifender oder erheblicher Bedeutung) und des § 8 Abs. 2 BKAG (Negativprognose) vorliegen.
- Verbreitet fehlt es an einer nachvollziehbaren Dokumentation des Vorliegens der gesetzlichen Speicherungsvoraussetzungen.
- Dementsprechend fanden sich in der bundesweit abrufbaren Datei vielfach Speicherungen, die dem Bereich der Bagatellkriminalität zuzuordnen sind. Auch wurden Personen gespeichert, bei denen kein hinreichender polizeilicher Restverdacht festzustellen war.
- Das Ergebnis des jeweiligen Strafverfahrens war bei vielen Einträgen nicht berücksichtigt – entweder aufgrund organisatorischer Mängel oder weil die nach § 482 Absatz 2 Strafprozessordnung (StPO) notwendige Mitteilung der Staatsanwaltschaft unterblieb.

Die Ergebnisse machen deutlich:

1. Es ist wichtig, die konkrete Zwecksetzung jeder Datei in einer Errichtungsanordnung festzulegen. Die Voraussetzungen, wann welche Daten für den jewei-

[1] Bei Enthaltung Hamburg.

ligen Zweck erforderlich sind und welcher Personenkreis erfasst werden darf, müssen genau definiert werden.
2. Bagatellfälle in Verbunddateien zu speichern, ist auch im Hinblick auf die bundesweite Abrufbarkeit der Daten unverhältnismäßig.
3. In der Praxis ist sicherzustellen, dass in Verbunddateien alle Speichervoraussetzungen, vor allem die Negativprognose, durchgehend und gründlich bezogen auf den jeweiligen Einzelfall dokumentiert werden.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) fordert, nicht nur in der Falldatei Rauschgift die Mängel zu beheben. Vielmehr fordert sie die Einhaltung der grundlegenden Standards für jedwede Speicherung in Verbunddateien der Polizei. Erst recht ist dies erforderlich vor dem Einsatz der neuen Datei zur Betäubungsmittelkriminalität im Polizeilichen Informations- und Analyseverbund (PIAV), die voraussichtlich im kommenden Jahr die FDR ablösen wird. Die Daten aus der FDR dürfen nicht pauschal übernommen werden.

17.1.12 Entschließung zwischen der 92. und 93. Konferenz vom 24. Januar 2017: Novellierung des Personalausweisgesetzes – Änderungen müssen bürger- und datenschutzfreundlich realisiert werden!

Die Bundesregierung plant grundlegende Änderungen des Personalausweisrechts. Nach dem vom Bundeskabinett beschlossenen Gesetzentwurf (BR-Drs. 787/16) werden das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger übergangen und Datenschutz sichernde Standards unterlaufen. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert daher insbesondere folgende datenschutzrechtliche Anforderungen zu berücksichtigen:

- Die obligatorische Aktivierung der eID-Funktion ist dann hinnehmbar, wenn dauerhaft sichergestellt ist, dass daraus keine verpflichtende Nutzung der eID-Funktion des Personalausweises resultiert. Die Entscheidung über die Nutzung der eID-Funktion muss allein bei den Bürgerinnen und Bürgern liegen. Deren Selbstbestimmungsrecht muss gewahrt bleiben.
- An der bisherigen Verpflichtung der Ausweisbehörden, Bürgerinnen und Bürger über die eIDFunktion des Personalausweises schriftlich zu unterrichten, sollte festgehalten werden. Nur durch eine bundesweit einheitliche Vorgabe zu einer solchen Information wird sichergestellt, dass alle Bürgerinnen und Bürger in hinreichend verständlicher Form aufgeklärt werden.
- Vor einer Datenübermittlung aus dem Personalausweis müssen die Bürgerinnen und Bürger Kenntnis über den Zweck der Übermittlung erhalten; zur Wahrnehmung des Rechts auf informationelle Selbstbestimmung müssen die Betroffenen

stets – wie bislang – nachvollziehen können, in welchem konkreten Kontext ihre Identitätsdaten übermittelt werden. Zudem sollte die bisherige Möglichkeit, die Übermittlung einzelner Datenkategorien auszuschließen, beibehalten werden.

- Die Einführung von organisationsbezogenen Berechtigungszertifikaten bei Diensteanbietern wird abgelehnt. Um sicherzustellen, dass Diensteanbieter nur die für den jeweiligen Geschäftsprozess erforderlichen Angaben übermittelt bekommen, sollte an der aktuellen Rechtslage festgehalten werden, nach der der antragstellende Diensteanbieter die Erforderlichkeit der aus der eID-Funktion des Personalausweises zu übermittelnden Angaben nachweisen muss und an den jeweils festgelegten Zweck gebunden ist.
- Berechtigungszertifikate dürfen nur an Diensteanbieter erteilt werden, die Datenschutz und Datensicherheit gewährleisten. Daher sollten antragstellende Diensteanbieter nach wie vor durch eine Selbstverpflichtung die Erfüllung dieser Anforderungen schriftlich bestätigen und nachweisen müssen.
- Die maßgeblichen Regelungen für die mit der Anlegung und Nutzung von Servicekonten einhergehende Erhebung und Verarbeitung von Identitätsdaten aus dem Personalausweis sowie die sicherheitstechnischen Rahmenbedingungen sollten im Personalausweisgesetz getroffen werden.
- Die Voraussetzungen für die Erstellung und Weitergabe von Personalausweisablichtungen sollten gesetzlich konkreter normiert werden. Insbesondere das Prinzip der Erforderlichkeit ist durch eine verpflichtende Prüfung der Notwendigkeit der Anfertigung einer Ablichtung sowie durch eine Positivliste von Erlaubnisgründen zu stärken. Die Einwilligung der Betroffenen als alleinige Voraussetzung birgt die Gefahr, dass in der Praxis Ablichtungen angefertigt werden, obwohl sie nicht erforderlich sind. Zudem dürfte fraglich sein, ob betroffene Personen in eine solche Maßnahme stets informiert und freiwillig einwilligen können.
- Die zum 1. Mai 2021 vorgesehene Einführung eines nahezu voraussetzungslosen Abrufs des Lichtbildes im automatisierten Verfahren durch die Polizeibehörden des Bundes und der Länder sowie die Verfassungsschutzbehörden und Nachrichtendienste wird abgelehnt. Bisher dürfen zur Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten insbesondere die Polizei- und Ordnungsbehörden Lichtbilder automatisiert abrufen, wenn die Personalausweisbehörde nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährdet. Diese gesetzlichen Einschränkungen für das Abrufverfahren sollen nun entfallen. Zudem sollen alle Nachrichtendienste künftig voraussetzungslos Lichtbilddaten abrufen können. Die bisherige Rechtslage ist völlig ausreichend.

17.1.13 Entschließung zwischen der 92. und 93. Konferenz vom 15. März 2017: Einsatz externer Dienstleister durch Berufsgeheimnisträger rechtssicher und datenschutzkonform gestalten!

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Bundesgesetzgeber auf, mit dem derzeit vorliegenden Gesetzentwurf der Bundesregierung „zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen“ (BR-Drs. 163/17) den Einsatz externer Dienstleister durch Berufsgeheimnisträger rechtssicher und datenschutzkonform zu gestalten.

Die Schweigepflicht ist Grundlage des für die Berufsausübung notwendigen Vertrauensverhältnisses. Aber auch Berufsgeheimnisträger können heute nicht mehr wirtschaftlich agieren, ohne die moderne Informations- und Kommunikationstechnik zu nutzen. Kaum ein Anwalt oder Arzt verfügt über das notwendige Spezialwissen, um diese Technik selbst zu warten und vor ständig neuen Bedrohungen abzusichern. Der vorliegende Gesetzentwurf will deshalb eine Praxis legalisieren, die aus Gründen der Praktikabilität längst etabliert ist. Der strafrechtliche Schutz von Privatgeheimnissen soll die Beauftragung externer Dienstleister durch Berufsgeheimnisträger nicht länger erschweren. Im Gegenzug sollen diese Auftragnehmer künftig einer strafrechtlich sanktionierten Verschwiegenheitspflicht unterliegen. Dennoch versäumt es der Gesetzentwurf, insbesondere mit der vorgeschlagenen Formulierung zu § 203 StGB, klare Verhältnisse zu schaffen. Bisher sorgte unter Ärzten – und mitunter sogar Anwälten – der Umstand für Verwirrung, dass das, was datenschutzrechtlich legitim war, noch längst nicht strafrechtlich erlaubt sein musste. Was nach dem Gesetzentwurf nunmehr strafrechtlich erlaubt sein soll, könnte wiederum nach der neuen Europäischen Datenschutz-Grundverordnung mit empfindlichen Bußgeldern in Millionenhöhe sanktioniert werden. Denn es ist weder mit dem Schutzzweck von § 203 StGB vereinbar, noch datenschutzrechtlich zulässig, dass Berufsgeheimnisträger, wie im neuen § 203 StGB vorgesehen, die Verantwortung für die Datenverarbeitung ohne Einwilligung der Betroffenen an externe Dienstleister übertragen. Nicht absehbar ist zudem, ob die Zeugnisverweigerungsrechte und das Beschlagnahmeverbot in einem weiteren Gesetzgebungsverfahren entsprechend weitgehend auf alle denkbaren Dienstleister ausgeweitet werden, die an der Berufsausübung durch Berufsgeheimnisträger mitwirken.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder dringt daher darauf, den Gesetzentwurf nachzubessern und die geplanten straf- und berufsrechtlichen Regelungen mit den datenschutzrechtlichen Vorschriften zu synchronisieren. Es muss Berufsgeheimnisträgern möglich sein, externe Dienstleister zu Rate zu ziehen. Im Sinne der ungestörten Berufsausübung der Berufsgeheimnisträger und des

Rechts auf informationelle Selbstbestimmung der Betroffenen sollten die Pflichten, die den Berufsgeheimnisträger dabei aus unterschiedlichen Rechtsgebieten treffen, aber soweit als möglich gleichlaufend ausgestaltet werden.

17.1.14 Entschließung zwischen der 92. und 93. Konferenz vom 16. März 2017: Gesetzentwurf zur Aufzeichnung von Fahrdaten ist völlig unzureichend!

Die Bundesregierung hat im Januar 2017 einen Entwurf zur Novellierung des Straßenverkehrsgesetzes (BT-Drs. 18/11300) vorgelegt, um die Nutzung automatisierter Fahrfunktionen auf Deutschlands Straßen zu erlauben. Dabei sollen Fahrdaten aufgezeichnet werden, anhand derer bewertet werden kann, zu welchem Zeitpunkt das Auto jeweils durch den Fahrer oder durch eine „automatisierte Fahrfunktion“ gesteuert wurde und wann ein Fahrer die Aufforderung zur Übernahme der Steuerung erhalten hat. Ebenfalls aufgezeichnet werden sollen Daten zu technischen Störungen automatisierter Fahrfunktionen. Mit den Daten soll sich nach einem Unfall klären lassen, ob die Technik und damit der Hersteller oder der Fahrer für einen Unfall verantwortlich war. Welche Daten dies sind und wie das Speichermedium ausgestaltet werden soll, regelt der Gesetzentwurf nicht.

Auf Verlangen der nach Landesrecht für Verkehrskontrollen zuständigen Behörden müssen die Fahrdaten diesen Behörden übermittelt werden. Die Fahrdaten sind auch Dritten zu übermitteln, wenn diese glaubhaft machen können, dass sie die Fahrdaten zur Geltendmachung, Abwehr oder Befriedigung von Rechtsansprüchen aus Unfällen benötigen. Unklar ist, wer die Daten übermitteln muss. Es bleibt ebenfalls unbestimmt, ob ggf. auch die Behörden Fahrdaten übermitteln dürfen.

Im Gesetzesentwurf sind außerdem weder die Zwecke noch die zu übermittelnden Daten hinreichend konkretisiert. Weiterhin geht nicht hervor, wie die Integrität, Vertraulichkeit und Verfügbarkeit bei der Aufzeichnung und Übermittlung der Fahrdaten sichergestellt werden soll.

Sollte der Entwurf in der vorgelegten Form in Kraft treten, besteht in Kraftfahrzeugen mit hoch- oder vollautomatisierter Fahrfunktion die Gefahr elektronischer Fahrtenschreiber, die personenbezogene Profile bilden.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert den Gesetzgeber zu einer dem datenschutzrechtlichen Bestimmtheitsgebot genügenden Novellierung des Straßenverkehrsgesetzes und zur Stärkung der Datenschutzrechte der Fahrer auf.

Sofern man eine Datenverarbeitung überhaupt für erforderlich hält, ist Folgendes zu regeln:

- die abschließende Aufzählung derjenigen Daten, die aufgezeichnet und gespeichert werden dürfen,
- die Bestimmung des für die Verarbeitung Verantwortlichen,
- die Ergänzung einer Übermittlungs-/Zugriffsregelung für den Fahrer/Halter,
- die Konkretisierung der Daten, die den nach Landesrecht zuständigen Behörden zu übermitteln sind,
- die datenschutzgerechte Ausgestaltung des Speichermediums, insbesondere die Festlegung einer angemessenen Speicherdauer anhand der Erforderlichkeit und des Zwecks der Beweisführung für die Haftung,
- eindeutige Festlegungen für die Trennung der Daten von den in den Fahrzeugdatenspeichern der Fahrzeuge gespeicherten Daten,
- die Konkretisierung der Zwecke für die Übermittlung der gespeicherten Daten,
- die Nennung des Adressaten für das Übermittlungsverlangen,
- die abschließende Nennung berechtigter Übermittlungsempfänger und ihrer jeweiligen Verarbeitungsbefugnisse mit im Übrigen strikter Zweckbindung und
- die Konkretisierung des Löschzeitpunkts der übermittelten Daten.

17.1.15 Entschließung zwischen der 92. und 93. Konferenz vom 16. März 2017: Neues Bundeskriminalamtgesetz – Informationspool beschneidet Grundrechte

Der „Entwurf eines Gesetzes zur Neustrukturierung des Bundeskriminalamtgesetzes“ (BT-Drs. 18/11326 und 18/11163; BR-Drs. 109/17) ändert das polizeiliche Datenschutzrecht grundlegend und betrifft Polizeibehörden in Bund und Ländern gleichermaßen. Er beschränkt sich nicht darauf, die Vorgaben des Bundesverfassungsgerichts aus dem Urteil vom 20. April 2016 zum Bundeskriminalamtgesetz und aus der neuen EU-Richtlinie zum Datenschutz im Bereich Justiz und Inneres umzusetzen. Tatsächlich nimmt er sogar wichtige Datenschutzregeln und Verfahrenssicherungen zurück, die der Gesetzgeber nach dem Volkszählungsurteil des Bundesverfassungsgerichts geschaffen hatte.

Der Entwurf ändert den bisherigen Informationsverbund für alle Polizeibehörden grundlegend. Dieser ist nicht mehr nach Dateien untergliedert und führt zu unverhältnismäßig weitreichenden Speicherungen. In dieser Form ist dies weder durch das Urteil des Bundesverfassungsgerichts zum BKAG noch durch die EU-Richtlinie zum Datenschutz im Bereich Justiz und Inneres veranlasst. Das Urteil des Bundesverfassungsgerichts

fordert, den Zweck der jeweiligen Ermittlungsmaßnahmen bei allen weiteren Schritten zu berücksichtigen, bei denen die ermittelten Daten verwendet werden. Nicht im Einklang damit steht es, Verfahrenssicherungen und datenschutzrechtliche Rahmenbedingungen aufzugeben.

Abzulehnen ist insbesondere der vorgesehene Verzicht auf Errichtungsanordnungen. Diese sind bislang Ausgangspunkt sowohl für datenschutzrechtliche Kontrollen als auch die Selbstkontrolle der Polizeibehörden. In ihnen wird festgelegt, zu welchen Zwecken personenbezogene Daten gespeichert sind. Dies ist eine wesentliche verfassungsrechtliche Vorgabe. Die neuen Regeln führen zu umfassenden themenübergreifenden Verknüpfungen und Abgleichen aller gespeicherten Personen. Sie verkürzen die Kontrollmöglichkeiten der Datenschutzaufsichtsbehörden von Bund und Ländern.

Ebenso sind die künftig durch die geplante „Mitziehautomatik“ erheblich längeren Speicherfristen abzulehnen. Die geplante Neuregelung hat zur Folge, dass alte Speicherungen – auch zu Personen, die lediglich im Verdacht standen, eine Straftat begangen zu haben und die nicht verurteilt wurden – bei jedem neuen Speicheranlass ungeprüft weiter fortgeschrieben werden. Dafür soll es schon genügen, wenn die betroffene Person als Zeuge oder Kontaktperson erneut in Erscheinung tritt. Auch dies verstößt gegen das durch die ständige Rechtsprechung des Bundesverfassungsgerichtes bekräftigte Übermaßverbot.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder fordert daher, den Gesetzentwurf in der parlamentarischen Beratung datenschutzkonform zu überarbeiten!

17.1.16 Entschließung der 93. Konferenz am 29./30. März 2017 in Göttingen: Göttinger Erklärung – Vom Wert des Datenschutzes in der digitalen Gesellschaft

Datenschutz ist zurzeit in aller Munde: Mit der Europäischen Datenschutzreform werden ab Mai 2018 in der ganzen Europäischen Union neue einheitliche Regeln gelten. Gegenwärtig sind die Gesetzgeber in Bund und Ländern mit Hochdruck dabei, das nationale Recht an die Europäischen Vorgaben anzupassen. Zugleich schreitet die Digitalisierung der Gesellschaft mit großen Schritten voran, etwa mit dem Internet der Dinge, der Wirtschaft 4.0 und künstlicher Intelligenz, und fordert die Wahrung des Datenschutzes und die Gewährleistung der Persönlichkeitsrechte heraus. Auch der Staat erweitert fortwährend seine Befugnisse zur Verarbeitung personenbezogener Daten, sei es zur Bekämpfung des Terrorismus und zur Gewährleistung der öffentlichen Sicherheit, sei es bei der Digitalisierung staatlicher Dienstleistungen.

Dabei gerät aber leichtfertig eines aus dem Blick: Datenschutz ist ein Grundrecht, wie die Meinungsfreiheit oder die Eigentumsgarantie. Es bindet alle Staatsgewalten unmittelbar, schützt die Menschenwürde und die freie Entfaltung der Persönlichkeit und kann auch Aspekte der Teilhabe und Chancengleichheit betreffen. Alle gesetzlichen Regelungen, sowie die Geschäftsmodelle und Anwendungen auch im Bereich der Wirtschaft, haben dies zu berücksichtigen. Immer häufiger stellen aber Verantwortliche in Politik und Wirtschaft dieses grundrechtlich geschützte Recht auf informationelle Selbstbestimmung implizit oder sogar explizit in Frage. Datenschutz wird als Hindernis diskreditiert.

Dies betrachtet die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder mit großer Sorge. Es befremdet sehr, wenn Mitglieder der Bundesregierung und andere Stimmen in der Politik in letzter Zeit immer wieder betonen, es dürfe kein Zuviel an Datenschutz geben und das Prinzip der Datensparsamkeit könne nicht die Richtschnur für die Entwicklung neuer Produkte sein. Stattdessen wird für eine vermeintliche Datensouveränität geworben, deren Zielrichtung aber im Unklaren bleibt.

Die Konferenz betont, dass Informationen über Personen keine Ware sind wie jede andere und nicht allein auf ihren wirtschaftlichen Wert reduziert werden dürfen. Gerade in Zeiten von Big Data, Algorithmen und Profilbildung bieten die digitalen Informationen ein nahezu vollständiges Abbild der Persönlichkeit des Menschen. Mehr denn je muss daher die Menschenwürde auch im digitalen Zeitalter der zentrale Maßstab staatlichen und wirtschaftlichen Handelns sein. Zu einer menschenwürdigen und freien Entfaltung der Persönlichkeit gehört die freie Selbstbestimmung über das eigene Ich.

„Datensouveränität“ verstanden als eigentumsähnliche Verwertungshoheit kann daher nur zusätzlich zum Recht auf informationelle Selbstbestimmung greifen, dieses jedoch keinesfalls ersetzen.

Die Konferenz fordert daher alle Entscheidungsträger in Politik und Wirtschaft auf, den hohen Wert des Rechts auf informationelle Selbstbestimmung für eine freiheitliche Gesellschaft zu achten und sich nachdrücklich vertrauensbildend für die Persönlichkeitsrechte einzusetzen. Datenschutz stellt kein Hindernis für die Digitalisierung dar, sondern ist wesentliche Voraussetzung für deren Gelingen.

Die Entwicklung datenschutzkonformer IT-Produkte und -Verfahren muss nachhaltig gefördert werden, um den Datenschutz zu einem Qualitätsmerkmal der europäischen Digitalwirtschaft zu machen.

17.1.17 Entschließung der 93. Konferenz am 29./30. März 2017 in Göttingen: Einsatz von Videokameras zur biometrischen Gesichtserkennung birgt erhebliche Risiken

In Pilotprojekten wird derzeit der Einsatz von Videoüberwachungssystemen erprobt, die erweiterte Möglichkeiten der Verhaltensauswertung und der Identifizierung von Beobachteten bieten. Neben der Mustererkennung steht besonders die biometrische Gesichtserkennung im Fokus dieser Projekte. Dies verschärft die ohnehin schon vorhandene Problematik derartiger neuer Überwachungsverfahren, mit denen „abweichendes Verhalten“ erkannt werden soll.[1]

Der Einsatz von Videokameras mit biometrischer Gesichtserkennung kann die Freiheit, sich in der Öffentlichkeit anonym zu bewegen, gänzlich zerstören. Es ist kaum möglich, sich solcher Überwachung zu entziehen oder diese gar zu kontrollieren.

Anders als bei konventioneller Videoüberwachung könnten Passanten mit dieser Technik nicht nur beobachtet und anhand bestimmter Muster herausgefiltert werden, sondern während der Überwachung anhand von Referenzbildern (Templates) automatisiert identifiziert werden. Damit wird eine dauerhafte Kontrolle darüber möglich, wo sich konkrete Personen wann aufhalten oder bewegen und mit wem sie hierbei Kontakt haben. Ermöglicht wird so die Erstellung von umfassenden Bewegungsprofilen und die Verknüpfung mit anderen über die jeweilige Person verfügbaren Daten.

Neben den genannten massiven gesellschaftspolitischen Problemen bestehen auch erhebliche rechtliche und technische Bedenken gegen den Einsatz solcher Überwachungstechniken. Biometrische Identifizierung arbeitet mit Wahrscheinlichkeitsaussagen; bei dem Abgleich zwischen ermitteltem biometrischen Merkmal und gespeichertem Template sind falsche Identifizierungen keine Seltenheit. Beim Einsatz dieser Technik durch Strafverfolgungsbehörden kann eine falsche Zuordnung dazu führen, dass Bürgerinnen und Bürger unverschuldet zum Gegenstand von Ermittlungen und konkreten polizeilichen Maßnahmen werden. Dieselbe Gefahr besteht, falls sie sich zufällig im öffentlichen Raum in der Nähe von gesuchten Straftätern oder Störern aufhalten.

Es gibt keine Rechtsgrundlage für die Behörden von Bund und Ländern für den Einsatz dieser Technik zur Gefahrenabwehr und Strafverfolgung. Die bestehenden Normen zum Einsatz von Videoüberwachungstechnik erlauben nur den Einsatz technischer Mittel für reine Bildaufnahmen oder -aufzeichnungen, nicht hingegen für darüber hinausgehende Datenverarbeitungsvorgänge. Aufgrund des deutlich intensiveren Grundrechtseingriffs,

[1] Siehe auch Entschließung der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum – nicht ohne Datenschutz“.

der durch Videotechnik mit erweiterter Auswertung einhergeht, können die bestehenden gesetzlichen Regelungen nicht analog als Rechtsgrundlage herangezogen werden, da sie für einen solchen Einsatz verfassungsrechtlich zu unbestimmt sind.

Nach der Rechtsprechung des Bundesverfassungsgerichts sind Maßnahmen mit großer Streubreite ein erheblicher Grundrechtseingriff. So verlangt das Bundesverfassungsgericht bereits für das automatisierte Erfassen von KFZ-Kennzeichen zwecks Abgleichs mit dem Fahndungsbestand eine normenklare und verhältnismäßige Rechtsgrundlage, die einen anlasslosen und flächendeckenden Einsatz ausschließt. Da bereits die allgemeine Regelung zur Videoüberwachung nicht zur Erfassung von KFZ-Kennzeichen ermächtigt, muss dies erst recht für die viel stärker in die Grundrechte Betroffener eingreifende Videoüberwachung zwecks Abgleichs biometrischer Gesichtsmerkmale einzelner Personen gelten. Ein Einsatz der Videoüberwachung mit Gesichtserkennung darf daher auf derzeitiger Grundlage auch im Rahmen eines Pilotbetriebs nicht erfolgen.

Der europäische Gesetzgeber hat die enormen Risiken dieser Technik für die Privatsphäre erkannt und die Verarbeitung biometrischer Daten zur Identifizierung sowohl in der ab Mai 2018 wirksamen Datenschutz-Grundverordnung als auch in der bis Mai 2018 umzusetzenden Datenschutz-Richtlinie im Bereich Justiz und Inneres nur unter entsprechend engen Voraussetzungen für zulässig erachtet. Wird über den Einsatz dieser Technik nachgedacht, muss der Wesensgehalt des Rechts auf informationelle Selbstbestimmung gewahrt bleiben und es müssen angemessene und spezifische Regelungen zum Schutz der Grundrechte und -freiheiten der Betroffenen vorgesehen werden. Hierzu gehören u. a. eine normenklare Regelung für die Verwendung von Templates, z. B. von Personen im Fahndungsbestand, für den Anlass zum Abgleich des Templates mit den aufgenommenen Gesichtern sowie zum Verfahren zur Zulassung von technischen Systemen für den Einsatz.

Etwaige gesetzliche Regelungen müssten die vorgenannten verfassungs- und europarechtlichen Bedingungen beinhalten und den mit dieser Technik verbundenen erheblichen Risiken für die Freiheitsrechte der Bürgerinnen und Bürger angemessen Rechnung tragen!

17.2 Sonstiges

17.2.1 Handlungsfelder mit Handlungsempfehlungen der AG Digitale Medien des Landespräventionsrates Sachsen

Erarbeitung einer Landesstrategie Digitale Medienbildung für den Freistaat Sachsen

Mit der Landesstrategie Digitale Medienbildung schafft die Landesregierung einen konzeptionellen Rahmen mit klaren Zielen für die Landespolitik im Bereich der Digitalen Medien. Die Landesstrategie Digitale Medienbildung ist Voraussetzung für eine generationenübergreifende digitale Souveränität jedes Einzelnen – über den Bereich der Schulbildung hinaus.

Einrichtung einer zentralen, ressortübergreifenden Landeskoordinierungsstelle Digitale Medienbildung im Freistaat Sachsen

Die Landeskoordinierungsstelle Digitale Medienbildung entwickelt Handlungsempfehlungen, koordiniert und veröffentlicht die verschiedenen Angebote und Förderprogramme, vernetzt die Akteure, bündelt die Inhalte und legt Synergien offen. Anbieter können bei konkreten Bedarfen vermittelt und medienpädagogische Angebote einer einheitlichen Qualitätsbewertung unterzogen werden.

Dauerhafte Einrichtung eines Beirats Digitale Medienbildung Sachsen

Als Mitglieder des Beirats tauschen sich die im Freistaat Sachsen im Bereich der Medienbildung tätigen Partner/Institutionen über aktuelle Themen und Entwicklungen in regelmäßigen Treffen aus. Das Gremium berät die Landeskoordinierungsstelle Digitale Medienbildung, bestimmt Schwerpunkte zur Ausrichtung und Umsetzung und gibt ein Votum zum Bericht der Landeskoordinierungsstelle Digitale Medienbildung an das Kabinett ab.

Kooperationspartner Wirtschaft, Medien, Kommunen und Wissenschaft und Forschung

Die Sächsische Wirtschaft, die Medien, die Sächsischen Kommunen sowie Wissenschaft und Forschung sind bedeutende Partner für das Thema Medienbildung und arbeiten als Mitglieder im Beirat Digitale Medienbildung Sachsen mit. Zusätzlich sind konkrete Handlungsempfehlungen in Bezug auf die Kooperationen mit den einzelnen Akteuren von der Landeskoordinierungsstelle Digitale Medienbildung zu erarbeiten.

Verankerung medienpädagogischer Inhalte in Aus- und Fortbildung aller pädagogischen Fachkräfte

Medienpädagogische Grundlagen sind in allen pädagogischen Studiengängen verpflichtend und in angemessenem Umfang als eigenständiger Lernbereich zu verankern. Die medienpädagogische und datenschutzrechtliche Weiterbildung von bereits tätigen Pädagogen wird sichergestellt und ist obligatorisch.

Vernetzung der frei tätigen Medienpädagogen

Die Landeskoordinierungsstelle Digitale Medienbildung vernetzt öffentliche Institutionen und praktisch tätige Medienpädagogen und weist auf mögliche Synergien hin. Die stärkere Vernetzung eröffnet den Austausch von Best-Practice-Beispielen und führt dazu, dass landesweit tätige Medienpädagogen ihre zielgruppenspezifischen Angebote besser regional umsetzen können.

Zentrale Veröffentlichung der Förderprogramme zur Medienbildung

Die Landeskoordinierungsstelle Digitale Medienbildung stellt eine digitale Plattform zur Verfügung, die gespeist von den für die Förderung zuständigen Stellen die Ziele und den Umfang der verschiedenen Förderprogramme transparent macht.

Datenschutz als verbindliches Thema der Medienbildung

Um die Menschen in die Lage zu versetzen, selbstbestimmt, kritisch und verantwortungsbewusst die Digitalen Medien zu nutzen, ist der Datenschutz als ein Teil der Medienbildung verbindlich, nachhaltig und systematisch in die Bildungslandschaft des Freistaates Sachsen zu integrieren. Dazu sind konkrete Handlungsempfehlungen von der Landeskoordinierungsstelle Digitale Medienbildung in Zusammenarbeit mit dem Sächsischen Datenschutzbeauftragten zu erarbeiten.

Mediale Teilhabe

Gelungene Medienbildung ist für alle Zielgruppen (Kinder, Erwachsene, Senioren) Voraussetzung für eine erfolgreiche mediale Teilhabe. Daneben kann sie auch eine Grundlage für eine bessere gesellschaftliche Integration schwer erreichbarer Zielgruppen (z. B. Erwachsene mit einem Grundbildungsbedarf, Menschen mit Beeinträchtigung oder Migrationshintergrund) sein. Um beides zu erreichen entwickelt die Landeskoordinierungsstelle Digitale Medienbildung Konzepte und setzt diese mit Partnern der Medienbildung um.

Sensibilisierung zu Chancen und Risiken der digitalen Medien

Öffentlichkeitsarbeit und Informationsvermittlung sind eine wesentliche Aufgabe der Landeskoordinierungsstelle Digitale Medienbildung. Auf Basis der Landesstrategie

Digitale Medienbildung werden geeignete Inhalte (auch anderer bundesweit agierender Institutionen) aufgegriffen, verfügbar gemacht und ggf. in Form von themenspezifischen Kampagnen mit Partnern umgesetzt.

Bereitstellung einer sicheren technischen Infrastruktur

Der Freistaat Sachsen verpflichtet sich ausgehend von den Zielen der Digitalisierungsstrategie, der Strategie für IT- und E-Government und der Landesstrategie Digitale Medienbildung zur Bereitstellung und Nutzung einer sicheren technischen Infrastruktur.

Schulische Medienbildung

Dieses Handlungsfeld bündelt die expliziten Empfehlungen der Arbeitsgruppe für den schulischen Bereich. Darüber hinaus sind auch die vorgenannten Handlungsfelder für den Schulbereich zu berücksichtigen.

- Formulierung der Strategie Medienbildung im Schulbereich und deren verbindliche Verankerung und Umsetzung in den einzelnen Schulformen
- Evaluation der Lehrpläne und deren Umsetzung in den einzelnen Fächern sowie die Evaluation der Lehrpraxis hinsichtlich ausreichender Verortung der Medienbildung und des Datenschutzes. Ableitung von geeigneten Maßnahmen zur Weiterentwicklung von technischen (z. B. Onlinelernplattformen) und pädagogischen (Lehrunterlagen, Übungen) Unterstützungsstrukturen für Lehrer im Bereich der Digitalen Medienbildung
- Evaluation der Studien- und Prüfungsordnung hinsichtlich der verpflichtenden Verortung der Medienbildung und des Datenschutzes in den Lehramtsstudiengängen
- Einsatz von externen Medienpädagogen gemäß des Schulentwicklungsplanes
- Einsatz einer sicheren zentralen Lern- und e-Learning-Plattform (z. B. mit Cloud-Lösungen) mit geprüften Anwendungen als ein sicheres Lernumfeld
- Entwicklung nachhaltig finanzierbarer Konzepte, die es den Kommunen ermöglichen, den in ihrer Trägerschaft befindlichen Schulen eine moderne und zeitgemäße technische Ausstattung zur Verfügung zu stellen, die den Herausforderungen des technischen Fortschritts – als kontinuierliche Anforderung – gewachsen ist. Dabei ist eine Verknüpfung der technischen Ausstattung mit medienpädagogischen und mediendidaktischen Konzepten der jeweiligen Schule sowie der kontinuierlichen Sicherstellung der Administration und des Supports sicherzustellen.

17.2.2 Verpflichtungserklärung zur Einhaltung des Meldegeheimnisses

**Verpflichtung gemäß § 7 des Bundesmeldegesetzes (BMG)
zur Einhaltung des Meldegeheimnisses**

.....
Name der verantwortlichen Stelle

Sehr geehrte(r) Frau/Herr …….....

aufgrund der Ihnen übertragenden dienstlichen Aufgaben verpflichte ich Sie auf die Einhaltung des Meldegeheimnisses gemäß § 7 BMG. Es ist Ihnen nach dieser Vorschrift untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen.

Diese Pflichten bestehen auch nach Beendigung Ihrer Tätigkeit fort.

Verstöße gegen das Meldegeheimnis können mit Freiheits- oder Geldstrafe geahndet werden.

In der Verletzung des Meldegeheimnisses kann zugleich eine Verletzung arbeits- oder dienstrechtlicher Verschwiegenheitspflichten liegen.

Diese Erklärung wird zur Personalakte genommen.

....

Ort, Datum Unterschrift der verantwortlichen Stelle

Über die Verpflichtung auf das Meldegeheimnis und die sich daraus ergebenden Verhaltensweisen wurde ich unterrichtet.

....

Ort, Datum Unterschrift des Verpflichteten

Stichwortverzeichnis

Ergänzende Korrektur zum 18. Tätigkeitsbericht

16 Ordnungswidrigkeitenverfahren

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

- *§ 38 Sächsisches Datenschutzgesetz (§ 38 Abs. 3 Satz 1 SächsDSG),*
- *§ 16 Abs. 2 Nr. 2 bis 5 Telemediengesetz (§ 15 Nr. 2 OWiZuVO i. V. m. § 16 Abs. 2 Nr. 2 bis 5 TMG)*
- *§ 111 Abs. 1 Nr. 1 des Vierten Buches Sozialgesetzbuch – Gemeinsame Vorschriften für die Sozialversicherung – (§ 15 Nr. 3 OWiZuVO i. V. m. § 111 Abs. 1 Nr. 1 SGB IV) und*
- *§ 85 des Zehnten Buches Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – (§ 15 Nr. 4 OwiZuVO i. V. m. § 85 SGB X).*

Im Berichtszeitraum waren im öffentlichen Bereich insgesamt 85 Bußgeldverfahren anhängig. Davon wurden 34 mit einem Bußgeld und eines mit einem Verwarngeld abgeschlossen.

Berichtszeitraum		**01.04.2015 – 31.03.2017**
anhängig gesamt		**85**
davon	mit Bußgeld	34
	mit Verwarnungsgeld	1
	eingestellt/von Verfolgung abgesehen	36
	unzuständig	2
	noch in Bearbeitung	12
Bußgeldsumme in €		**25.655**

Die Zahl der bearbeiteten Bußgeldverfahren als auch die Summe der verhängten Geldbußen bzw. Verwarngelder ist im Vergleich zum vergangenen Berichtszeitraum angestiegen. Die Summe der festgesetzten Geldbußen vergrößerte sich sogar um mehr als das Doppelte.

Mit den bearbeiteten Ordnungswidrigkeitenverfahren wurden

- unbefugte Verarbeitungen (insbesondere in Form der Übermittlung oder Nutzung) nicht offenkundiger personenbezogener Daten (§ 38 Abs. 1 Nr. 1 a SächsDSG),
- unbefugte Abrufe nicht offenkundiger personenbezogener Daten für sich oder einen anderen (§ 38 Abs. 1 Nr. 1 c SächsDSG) und
- unbefugte Erhebungen oder Verarbeitungen nicht allgemein zugänglicher Sozialdaten (§ 85 Abs. 2 Nr. 1 SGB X) geprüft bzw. geahndet.

Die unbefugten Verarbeitungen oder Abrufe nicht offenkundiger personenbezogener Daten (§ 38 Abs. 1 Nr. 1 a und c SächsDSG) gingen zudem, nach entsprechender Verpflichtung gemäß § 6 Abs. 2 SächsDSG, in der Regel mit einer Verletzung des Datengeheimnisses nach § 6 Abs. 1 Satz 1 oder 2 SächsDSG einher (Ordnungswidrigkeitentatbestand des § 38 Abs. 1 Nr. 3 SächsDSG).

Nach wie vor handelt es sich zum Großteil (ca. 85 %) um Ordnungswidrigkeitenverfahren gegen Bedienstete der sächsischen Polizei wegen unbefugter Abrufe personenbezogener Daten aus den der Polizei zur Verfügung stehenden Datenbanken, z. B. zu Bekannten, Freunden oder Kollegen.
Es wurden jedoch auch vermehrt Ordnungswidrigkeitenverfahren gegen Bedienstete anderer Behörden, insbesondere Landratsämter, geführt, die ebenfalls die ihnen zur dienstlichen Aufgabenwahrnehmung zur Verfügung stehenden Datenbanken missbrauchten, z. B. für Kfz-Halterabfragen oder für Abfragen aus dem Bundeszentralregister aus privater Neugier.
Des Weiteren standen Bedienstete von Jobcentern der Bundesagentur für Arbeit, die in den Zuständigkeitsbereich des Sächsischen Datenschutzbeauftragten fallen, unter Verdacht, nicht allgemein zugängliche Sozialdaten ohne dienstlichen Anlass erhoben oder verarbeitet zu haben (Ordnungswidrigkeitentatbestand des § 85 Abs. 2 Nr. 1 SGB X).
Auch bestand gegenüber Bediensteten unterschiedlichster Behörden der Verdacht, nicht offenkundige personenbezogene Daten unbefugt an unberechtigte Dritte übermittelt zu haben.

Der große Anteil an Ordnungswidrigkeitenverfahren gegen sächsische Polizeibeamte zeigt, dass die von mir erhoffte Präventionswirkung durch die, auf meine Anregung hin, intensivierte Belehrung der Polizeidienststellen über den Datenschutz im Zusammenhang mit der Nutzung polizeilicher Datenbanken (vgl. 16/16.1) sowie durch die von mir in der Vergangenheit durchgeführten Ordnungswidrigkeitenverfahren doch nicht eintritt.
Die von mir geschilderte Unsicherheit unter den Polizeibediensteten hinsichtlich der zulässigen Nutzung polizeilicher Datenbanken besteht weiter fort. Häufig wird nach wie vor irriger Weise davon ausgegangen, dass allein aus der technischen Möglichkeit des Zugriffes auf personenbezogene Daten oder aus einem Zugriffsstatus bestimmter Dokumente eine Aussage über die Befugnis der/des einzelnen Beamtin/Beamten zur Verarbeitung dieser Daten abgeleitet werden kann. Ebenso wird oft fälschlicher Weise davon ausgegangen, dass schon allein die Eigenschaft Polizeibeamtin/-beamter zu sein ausreichen würde, um bestimmte Datenabrufe zu rechtfertigen.
Doch selbst wenn Polizeibeamte gem. § 1 SächsPolG generell die Aufgabe haben, vom Einzelnen und dem Gemeinwesen Gefahren abzuwehren, haben sie sich dabei grundsätzlich innerhalb ihrer konkreten Aufgabenzuweisung und Zuständigkeiten zu bewegen. So wie der gesamte Polizeivollzugsdienst nur die personenbezogenen Daten verarbeiten darf, die zur Erfüllung seiner Aufgaben erforderlich sind (§ 43 Abs. 1 Satz 1 SächsPolG), ist auch die/der einzelne Polizeibedienstete nur berechtigt, die zur Erfüllung ihrer/seiner konkreten dienstlichen Aufgabe erforderlichen Daten zu verarbeiten.
Des Weiteren kommt es, wie auch häufig vorgebracht wird, sowohl hinsichtlich der Erfüllung des Tatbestands des § 38 Abs. 1 Nr. 1 Buchst. c) SächsDSG als auch

hinsichtlich des § 38 Abs. 1 Nr. 3 SächsDSG nicht darauf an, ob abgerufene personenbezogene Daten an Dritte weitergegeben worden sind. Die Tatbestände sind erfüllt, wenn die Daten unbefugt für sich selbst oder auch für einen anderen abgerufen werden bzw. diesbezüglich das Datengeheimnis verletzt wird.

Etwa 30% der Verfahren in denen ein Bußgeld festgesetzt wurde, wurden den zuständigen Staatsanwaltschaften mit der Bitte um Weiterleitung an das jeweils zuständige Amtsgericht vorgelegt. In fast allen Fällen, die vor Gericht entschieden wurden, sind den Betroffenen Geldbußen aufgrund ordnungswidrigen Handelns auferlegt worden. Das zeigt, dass die Gerichtsbarkeit im Wesentlichen den Einschätzungen des Sächsischen Datenschutzbeauftragten gefolgt ist.
Meine Beteiligung im Hauptverfahren aufgrund besonderer Sachkunde habe ich im Berichtszeitraum beibehalten. Sowohl bei Abstimmungen mit der Staatsanwaltschaft als auch bei den Hauptverhandlungen nutze ich die Gelegenheit, die Gesichtspunkte vorzubringen, die von meinem Standpunkt aus für die Entscheidung von Bedeutung sind.
Wie auch im vergangenen Berichtszeitraum strebe ich außerdem eine möglichst gleichmäßige Behandlung meiner Belange an. Der Umstand, dass die Zuständigkeit für die Entscheidung über den Einspruch gegen einen Bußgeldbescheid bei den Amtsgerichten am jeweiligen Begehungsort liegt, wirkt sich hinsichtlich einer stringenten Betrachtung bestimmter Aspekte in vergleichbaren Fällen nach wie vor ungünstig aus (vgl. 16/16.1). Eine Kanalisierung in der Justiz wäre, wie von mir bereits mehrfach erwähnt (vgl. auch 5. TB nicht-öffentlicher Bereich 11.2), effizienter und vorteilhafter.
Insgesamt bewirkt der Anstieg an Gerichtsverfahren bei der Bearbeitung von Ordnungswidrigkeitenverfahren im öffentlichen Bereich einen steigenden Bearbeitungsaufwand, größeres Bearbeitungsvolumen und wirkt sich auf die Dauer der Verfahren aus.

Die Ahndung von Ordnungswidrigkeiten im öffentlichen Bereich ist nach wie vor unabdingbar. Die Bediensteten der Behörden und öffentlichen Stellen in Sachsen sind auch zukünftig zu ihrer besonderen Pflichtenwahrung und Vorbildwirkung zu ermahnen. Auch durch bloße Unkorrektheit im Umgang mit behördlichen Informationssystemen kann das Vertrauen der Allgemeinheit in die Zuverlässigkeit der Behörden, und im speziellen die der Polizei, empfindlich geschädigt werden. Der Bürger muss sich darauf verlassen können, dass Daten über ihn, die dem Staat vorliegen – nicht selten sind es sensible Daten – auch nur für staatliche Zwecke, also auf gesetzlicher Grundlage verarbeitet werden.