Sächsischer Landtag
6. Wahlperiode

DRUCKSACHE 6/2562

Schutz des Persönlichkeitsrechts im öffentlichen Bereich

17. Tätigkeitsbericht

des

Sächsischen Datenschutzbeauftragten

Berichtszeitraum: 1. April 2013 bis 31. März 2015

Dem Sächsischen Landtag

vorgelegt zum 31. März 2015

gemäß § 30 des Sächsischen Datenschutzgesetzes

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

Vorbemerkung zum Sprachgebrauch in diesem Bericht:

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

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

AmtshilfeRLUmsG	Gesetz zur Umsetzung der Amtshilferichtlinie sowie zur Änderung steuerlicher Vorschriften - Amtshilferichtlinie-Umsetzungsgesetz vom 26. Juni 2013 (BGBl. I. S. 1809)
AO	Abgabenordnung in der Fassung der Bekanntmachung vom 1. Oktober 2002 (BGBl. I S. 3866; 2003 I S. 61), zuletzt geändert durch Art. 3 des Gesetzes vom 28. Juli 2015 (BGBl. I S. 1400)
ATDG	Antiterrordateigesetz vom 22. Dezember 2006 (BGBl. I S. 3409), zuletzt geändert durch Art. 1 des Gesetzes vom 18. Dezember 2014 (BGBl. I S. 2318)
AZRG	Ausländerzentralregistergesetz vom 2. September 1994 (BGBl. I S. 2265), zuletzt geändert durch Art. 2 des Gesetzes vom 8. Juli 2014 (BGBl. I S. 890)
BArchG	Bundesarchivgesetz vom 6. Januar 1988 (BGBl. I S. 62), zuletzt geändert durch Art. 4 Abs. 38 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154)
BDSG	Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Art. 1 des Gesetzes vom 25. Februar 2015 (BGBl. I S. 162)
BeamtStG	Beamtenstatusgesetz vom 17. Juni 2008 (BGBl. I S. 1010), zuletzt geändert durch Art. 15 Abs. 16 des Gesetzes vom 5. Februar 2009 (BGBl. I S. 160)
BGB	Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003, BGBl. I S. 738), zuletzt geändert durch Art. 16 des Gesetzes vom 29. Juni 2015 (BGBl. I S. 1042)
BKAG	Bundeskriminalamtgesetz vom 7. Juli 1997 (BGBl. I S. 1650), zuletzt geändert durch Art. 7 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1324)

BRAO	Bundesrechtsanwaltsordnung in der im Bundesgesetzblatt Teil III, Gliederungsnummer c, veröffentlichten bereinigten Fassung, zuletzt geändert durch Art. 3 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1332)
BStatG	Bundesstatistikgesetz vom 22. Januar 1987 (BGBl. I S. 462, 565), zuletzt geändert durch Art. 13 des Gesetzes vom 25. Juli 2013 (BGBl. I S. 2749)
BZRG	Bundeszentralregistergesetz in der Fassung der Bekanntmachung vom 21. September 1984 (BGBl. I S. 1229, 1985 BGBl. I S. 195), zuletzt geändert durch Art. 2 Abs. 4 des Gesetzes vom 21. Januar 2015 (BGBl. I S. 10)
EGGVG	Einführungsgesetz zum Gerichtsverfassungsgesetz in der im Bundesgesetzblatt Teil III, Gliederungsnummer 300-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Art. 20 des Gesetzes vom 29. Juni 2015 (BGBl. I S. 1042)
E-Privacy-Richtlinie	Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG) vom 12. Juli 2002 (ABl. EG Nr. L 201 S. 37-47)
EStG	Einkommensteuergesetz in der Fassung der Bekanntmachung vom 8. Oktober 2009 (BGBl. I S. 3366, 3862), zuletzt geändert durch Art. 5 des Gesetzes vom 28. Juli 2015 (BGBl. I S. 1400)
EUV/AEUV	Vertrag über die Europäische Union / Vertrag über die Arbeitsweise der Europäischen Union
GG	Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949, zuletzt geändert durch Art. 1 des Gesetzes vom 23. Dezember 2014 (BGBl. I S. 2438)
GO RAK Sachsen	Geschäftsordnung der Rechtsanwaltskammer Sachsen (mit Wahlordnung), beschlossen in der Kammerversammlung vom 31. März 2000, geändert durch Beschluss Kammerversammlung vom 22. März 2002, 28. März 2003, 24. September 2004, 27. März 2009, 18. März 2011, 23. März 2012 und 25. März 2013
IHKG	Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern in der im Bundesgesetzblatt Teil III, Gliederungsnummer 701-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Art. 17 des Gesetzes vom 25. Juli 2013 (BGBl. I S. 2749)

JGG	Jugendgerichtsgesetz in der Fassung der Bekanntmachung vom 11. Dezember 1974 (BGBl. I S. 3427), zuletzt geändert durch Art. 7 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1332)
KFRG	Gesetz zur Weiterentwicklung der Krebsfrüherkennung und zur Qualitätssicherung durch klinische Krebsregister (Krebsfrüherkennungs- und -registergesetz) vom 3. April 2013 (BGBl. I S. 617)
KomWO	Kommunalwahlordnung vom 5. September 2003 (SächsGVBl. S. 440), zuletzt geändert durch die Verordnung vom 29. November 2013 (SächsGVBl. S. 842)
LJHG	Landesjugendhilfegesetz in der Fassung der Bekanntmachung vom 4. September 2008 (SächsGVBl. S. 578), zuletzt geändert durch Art. 2 des Gesetzes vom 11. Juni 2010 (SächsGVBl. S. 182)
OWiG	Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 602), zuletzt geändert durch Art. 4 des Gesetzes vom 13. Mai 2015 (BGBl. I S. 706)
OWiZuVO	Ordnungswidrigkeiten-Zuständigkeitsverordnung vom 16. Juni 2014 (SächsGVBl. S. 342)
PStG	Personenstandsgesetz vom 19. Februar 2007 (BGBl. I S. 122), zuletzt geändert durch Art. 3 des Gesetzes vom 28. August 2013 (BGBl. I S. 3458)
RiStBV	Richtlinien für das Strafverfahren und das Bußgeldverfahren vom 1. Januar 1977, zuletzt geändert mit Wirkung vom 1. August 2015 durch Bekanntmachung vom 21. Juli 2015 (BAnz AT 31. Juli 2015 B1)
SächsArchivG	Archivgesetz für den Freistaat Sachsen vom 17. Mai 1993 (SächsGVBl. S. 449), zuletzt geändert durch das Gesetz vom 18. Dezember 2013 (SächsGVBl. 2014 S. 2)
SächsBeWoG	Sächsisches Betreuungs- und Wohnqualitätsgesetz vom 12. Juli 2012 (SächsGVBl. S. 397)
SächsBG	Sächsisches Beamtengesetz vom 18. Dezember 2013 (SächsGVBl. S. 970, 971), erlassen als Art. 1 des Gesetzes zur Neuordnung des Dienst-, Besoldungs- und Versorgungsrechts im Freistaat Sachsen (Sächsisches Dienstrechtsneuordnungsgesetz)
SächsBhVO	Sächsische Beihilfeverordnung vom 16. September 2014 (SächsGVBl. S. 530, 567)

SächsDSG	Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz) vom 11. Dezember 1991 (SächsGVBl. S. 401), geändert durch Gesetz vom 7. April 1997 (SächsGVBl. S. 350), geändert durch Gesetz vom 25. August 2003 (SächsGVBl. S. 330), zuletzt Neufassung vom 14. Dezember 2006 (SächsGVBl. S. 530), 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), zuletzt geändert durch die Verordnung vom 4. April 2015 (SächsGVBl. S. 374)
SächsFischG	Sächsisches Fischereigesetz vom 9. Juli 2007 (SächsGVBl. S. 310), zuletzt geändert durch das Gesetz vom 29. April 2012 (SächsGVBl. S. 254)
SächsFischVO	Sächsische Fischereiverordnung vom 4. Juli 2013 (SächsGVBl. S. 569)
SächsGemO	Sächsische Gemeindeordnung in der Fassung der Bekanntmachung vom 3. März 2014 (SächsGVBl. S. 146), zuletzt geändert durch Art. 18 des Gesetzes vom 29. April 2015 (SächsGVBl. S. 349)
SächsHSFG	Sächsisches Hochschulfreiheitsgesetz in der Fassung der Bekanntmachung vom 15. Januar 2013 (SächsGVBl. S. 3), zuletzt geändert durch Art. 11 des Gesetzes vom 29. April 2015 (SächsGVBl. S. 349)
SäHO	Sächsische Haushaltsordnung in der Fassung der Bekanntmachung vom 10. April 2001 (SächsGVBl. S. 153), zuletzt geändert durch Art. 1 des Gesetzes vom 29. April 2015 (SächsGVBl. S. 349)
SächsJG	Sächsisches Justizgesetz vom 24. November 2000 (SächsGVBl. S. 482; 2001 S. 704), zuletzt geändert durch Gesetz vom 9. Juli 2014 (SächsGVBl. S. 405)
SächsKAG	Sächsisches Kommunalabgabengesetz in der Fassung der Bekanntmachung vom 26. August 2004 (SächsGVBl. S. 418; 2005 S. 306), zuletzt geändert durch Art. 6 des Gesetzes vom 28. November 2013 (SächsGVBl. S. 822)
SächsKitaG	Gesetz über Kindertageseinrichtungen in der Fassung der Bekanntmachung vom 15. Mai 2009 (SächsGVBl. S. 225), zuletzt geändert durch Art. 7 des Gesetzes vom 29. April 2015 (SächsGVBl. S. 349)

SächsKomPrüfVO-Doppik	Sächsische Kommunalprüfungsverordnung-Doppik vom 25. Oktober 2011 (SächsGVBl. S. 604)
SächsMeldVO	Sächsische Meldeverordnung vom 13. Dezember 2006 (SächsGVBl. S. 540; 2010 S. 35), zuletzt geändert durch Art. 2 des Gesetzes vom 30. März 2015 (SächsABl. S. 290)
SächsMG	Sächsisches Meldegesetz in der Fassung der Bekanntmachung vom 4. Juli 2006 (SächsGVBl. S. 388), zuletzt geändert Art. 2 des Gesetzes vom 6. Dezember 2011 (SächsGVBl. S. 638)
SächsPolG	Polizeigesetz des Freistaates Sachsen in der Fassung der Bekanntmachung vom 13. August 1999 (SächsGVBl. S. 466), geändert durch Art. 45 des Gesetzes vom 5. Mai 2004 (SächsGVBl. S. 148, 171), zuletzt geändert durch Art. 1 des Gesetzes vom 17. Dezember 2013 (SächsGVBl. S. 890)
SächsPsychKG	Sächsisches Gesetz über die Hilfen und die Unterbringung bei psychischen Krankheiten in der Fassung der Bekanntmachung vom 10. Oktober 2007 (SächsGVBl. S. 422), zuletzt geändert durch Art. 1 des Gesetzes vom 7. August 2014 (SächsGVBl. S. 446)
SächsStatG	Sächsisches Statistikgesetz vom 17. Mai 1993 (SächsGVBl. S. 453), zuletzt geändert durch Art. 13 des Gesetzes vom 6. Juni 2002 (SächsGVBl. S. 168)
SächsStudDatVO	Verordnung zur Verarbeitung personengebundener Daten der Studienbewerber, Studenten und Prüfungskandidaten für statistische und Verwaltungszwecke der Hochschulen (Sächsische Studentendatenverordnung) vom 19. Juli 2000 (SächsGVBl. S. 390)
SächsStVollzG	Sächsisches Strafvollzugsgesetz vom 16. Mai 2013 (SächsGVBl. S. 250)
SächsVerf	Verfassung des Freistaates Sachsen vom 27. Mai 1992 (SächsGVBl. S. 243), zuletzt geändert durch das Gesetz vom 11. Juli 2013 (SächsGVBl. S. 502)
SächsVersG	Sächsisches Versammlungsgesetz vom 25. Januar 2012 (SächsGVBl. S. 54), zuletzt geändert durch Art. 4 des Gesetzes vom 17. Dezember 2013 (SächsGVBl. S. 890)
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)

SBO	Schulbesuchsordnung vom 12. August 1994 (SächsGVBl. S. 1565), zuletzt geändert durch die Verordnung vom 4. Februar 2004 (SächsGVBl. S. 66)
SchulG	Schulgesetz für den Freistaat Sachsen in der Fassung der Bekanntmachung vom 16. Juli 2004 (SächsGVBl. S. 298), zuletzt geändert durch Art. 2 des Gesetzes vom 19. Mai 2010 (SächsGVBl. S. 142)
SGB I	Erstes Buch Sozialgesetzbuch - Allgemeiner Teil - (Art. 1 des Gesetzes vom 11. Dezember 1975, BGBl I S. 3015), zuletzt geändert durch Art. 2 des Gesetzes vom 18. Dezember 2014 (BGBl. I S. 2325)
SGB II	Zweites Buch Sozialgesetzbuch - Grundsicherung für Arbeitsuchende - in der Fassung der Bekanntmachung vom 13. Mai 2011 (BGBl. I S. 850, 2094), zuletzt geändert durch Art. 5 des Gesetzes vom 24. Juni 2015 (BGBl. I S. 974)
SGB III	Drittes Buch Sozialgesetzbuch - Arbeitsförderung - (Art. 1 des Gesetzes vom 24. März 1997, BGBl. I S. 594, 595), zuletzt geändert durch Art. 3 des Gesetzes vom 16. Juli 2015 (BGBl. I S. 1211)
SGB IV	Viertes Buch Sozialgesetzbuch - Gemeinsame Vorschriften für die Sozialversicherung - in der Fassung der Bekanntmachung vom 12. November 2009 (BGBl. I S. 3710, 3973; 2011 I S. 363), zuletzt geändert durch Art. 1 des Gesetzes vom 15. April 2015 (BGBl. I S. 583)
SGB V	Fünftes Buch Sozialgesetzbuch - Gesetzliche Krankenversicherung (Art. 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477, 2482), zuletzt geändert durch Art. 1 und 2 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1368)
SGB VII	Siebtes Buch Sozialgesetzbuch - Gesetzliche Unfallversicherung (Art. 1 des Gesetzes vom 7. August 1996, BGBl. I S. 1254), zuletzt geändert durch Art. 4 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1368)
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. 5 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1368)
SGB IX	Neuntes Buch Sozialgesetzbuch - Rehabilitation und Teilhabe behinderter Menschen - (Art. 1 des Gesetzes vom 19. Juni 2001, BGBl. I S. 1046, 1047), zuletzt geändert durch Art. 1a des Gesetzes vom 7. Januar 2015 (BGBl. 2015 II S. 15)

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. 10 des Gesetzes vom 11. August 2014 (BGBl. I S. 1348)
SGB XI	Elftes Buch Sozialgesetzbuch - Soziale Pflegeversicherung - (Art. 1 des Gesetzes vom 26. Mai 1994, BGBl. I S. 1014, 1015), zuletzt geändert durch Art. 7 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1368)
SGB XII	Zwölftes Buch Sozialgesetzbuch - Sozialhilfe - (Art. 1 des Gesetzes vom 27. Dezember 2003, BGBl. I S. 3022, 3023), zuletzt geändert durch Art. 9 des Gesetzes vom 21. Juli 2014 (BGBl. I S. 1133)
SigG	Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Art. 4 Abs. 111 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154)
StDÜV	Verordnung über die elektronische Übermittlung von für das Besteuerungsverfahren erforderlichen Daten (Steuerdaten-Übermittlungsverordnung) vom 28. Januar 2003 (BGBl. I S. 139), zuletzt geändert durch Art. 6 des Gesetzes vom 1. November 2011 (BGBl. I S. 2131)
StGB	Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Art. 1 des Gesetzes vom 21. Januar 2015 (BGBl. I S. 10)
StPO	Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Art. 2 Abs. 3 des Gesetzes vom 21. Januar 2015 (BGBl. I S. 10)
StVG	Straßenverkehrsgesetz in der Fassung der Bekanntmachung vom 5. März 2003 (BGBl. I S. 310, 919), zuletzt geändert durch Art. 4 des Gesetzes vom 8. Juni 2015 (BGBl. I S. 904)
StVO	Straßenverkehrs-Ordnung vom 6. März 2013 (BGBl. I S. 367), zuletzt geändert durch Art. 1 der Verordnung vom 22. Oktober 2014 (BGBl. I S. 1635)
TKG	Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Art. 5 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1324)
TMG	Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), zuletzt geändert durch Art. 2 Abs. 16 des Gesetzes vom 1. April 2015 (BGBl. I S. 434)

TSG	Gesetz über die Änderung der Vornamen und die Feststellung der Geschlechtszugehörigkeit in besonderen Fällen (Transsexuellengesetz) vom 10. September 1980 (BGBl. I S. 1654), zuletzt geändert durch Art. 1 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 1978)
VerpflG	Verpflichtungsgesetz vom 2. März 1974 (BGBl. I S. 469, 547), zuletzt geändert durch § 1 Nr. 4 des Gesetzes vom 15. August 1974 (BGBl. I S. 1942)
VwV Personalakten	Verwaltungsvorschrift Personalakten vom 3. Dezember 1996 (SächsABl. 1997 S. 145), geändert durch die VwV vom 20. Juli 1999 (SächsABl. S. 866), zuletzt enthalten in der VwV vom 12. Dezember 2013 (SächsABl.SDr. S. S848)
VwV-SäHO	Verwaltungsvorschriften des SMF zur Sächsischen Haushaltsordnung vom 27. Juni 2005 (SächsABl.SDr. S. S226), geändert durch die VwV vom 25. März 2015 (SächsABl. S. 515), zuletzt enthalten in der VwV vom 12. Dezember 2013 (SächsABl.SDr. S. S848)
VwVfG	Verwaltungsverfahrensgesetz in der Fassung der Bekanntmachung vom 23. Januar 2003 (BGBl. I S. 102), zuletzt geändert durch Art. 3 des Gesetzes vom 25. Juli 2013 (BGBl. I S. 2749)
VZG 1983	Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz 1983) vom 25. März 1982 (BGBl. I S. 369)
WoGG	Wohngeldgesetz vom 24. September 2008 (BGBl. I S. 1856), zuletzt geändert durch Art. 9 Abs. 5 des Gesetzes vom 3. April 2013 (BGBl. I S. 610)
WRV	Die Verfassung des Deutschen Reichs (Weimarer Reichsverfassung) in der im Bundesgesetzblatt Teil III, Gliederungsnummer 401-2, veröffentlichten bereinigten Fassung
ZensG 2011	Zensusgesetz 2011 vom 8. Juli 2009 (BGBl. I S. 1781)

Sonstiges

BAMF	Bundesamt für Migration und Flüchtlinge
BfDI	Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGBl.	Bundesgesetzblatt

BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BMI	Bundesministerium des Innern
BMJV	Bundesministerium der Justiz und für Verbraucherschutz
BND	Bundesnachrichtendienst
BR-Drs.	Bundesrats-Drucksache
BSG	Bundessozialgericht
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestags-Drucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Amtliche Sammlung der Entscheidungen des Bundesverfassungsgerichts
BZSt	Bundeszentralamt für Steuern
DSK	Konferenz der Datenschutzbeauftragten des Bundes und der Länder - Datenschutzkonferenz (findet halbjährlich statt)
ELSTAM	Elektronische Lohnsteuerabzugsmerkmale
EU	Europäische Union
EUV/AEUV	Vertrag über die Europäische Union / Vertrag über die Arbeitsweise der Europäischen Union
IHK	Industrie- und Handelskammer
INPOL	Polizeiliches Informationssystem des Bundes u. der Länder
JVA	Justizvollzugsanstalt
KDN	Kommunale DatenNetz GmbH
KISA	Kommunale Informationsverarbeitung Sachsen
LfV	Landesamt für Verfassungsschutz des Freistaates Sachsen

LG	Landgericht
LKA	Landeskriminalamt Sachsen
LSF	Landesamt für Steuern und Finanzen
LSG	Landessozialgericht
LT-Drs.	Landtags-Drucksache
MDK	Medizinischer Dienst der Krankenversicherung
MiStra	Anordnung über Mitteilungen in Strafsachen
NVwZ	Neue Zeitschrift für Verwaltungsrecht
m. w. N.	mit weiteren Nachweisen
OLG	Oberlandesgericht
OVG	Sächsisches Oberverwaltungsgericht
PD	Polizeidirektion
RAK	Rechtsanwaltskammer
RiStBV	Richtlinien für das Strafverfahren und das Bußgeldverfahren
SAB	Sächsische Aufbaubank
SächsABl.	Sächsisches Amtsblatt
SächsGVBl.	Sächsisches Gesetz- und Verordnungsblatt
SID	Staatsbetrieb Sächsische Informatik Dienste
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
SVN	Sächsisches Verwaltungsnetz
VG	Verwaltungsgericht
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 Global denken, lokal handeln

Aus mehrfachen Richtungen heraus ist im Berichtszeitraum deutlich geworden, dass dieses Motto auch für den Datenschutz gilt. Der Globalisierungsdruck in der Informationsverarbeitung hat die Europäische Union dazu gebracht, den Rechtsrahmen bei der Verarbeitung von personenbezogenen Informationen neu zu gestalten (siehe 3.1). Auch wenn dies eine Initiative ist, die nur für den europäischen Raum direkt gilt, wirkt sie sich mittelbar global aus, denn international tätige Unternehmen haben natürlich bei ihrer Geschäftstätigkeit in der EU diesen Rechtsrahmen zu beachten. Ich hoffe, dass dieses Vorhaben das gesetzte Ziel erreichen kann. Der vor uns liegende Arbeitsumfang ist groß. Parlamente, Exekutive, Aufsichtsbehörden, Betroffene und Unternehmen haben sich auf viele neue Regelungen einzustellen und den damit verbundenen Aufwand zu bewältigen. Auch die Judikative wird nach meiner Einschätzung ihren Teil leisten müssen. Erfahrungsgemäß lassen europäische Regelungen einen Spielraum, der im Nachhinein verbindlich geklärt werden muss.

Ist die Europäische Datenschutzreform eher ein Thema, das Fachkreise, Lobbyisten und Aktivisten interessiert, hat die sogenannte „Snowden-Affäre“ 2013 große mediale Wellen geschlagen. Schlagartig ist uns der Umfang und die Tiefe geheimdienstlicher Überwachung vor Augen geführt worden, die auch vor verbündeten Staaten nicht Halt macht. Auch wenn nach US-amerikanischem Recht Edward Snowdens Whistleblowing von Strafe bedroht ist, gebührt ihm Dank dafür, dass er den Vorhang weggezogen hat vor einem sonst im Dunkeln liegenden Bereich und damit auf eine Gefahr aufmerksam gemacht hat, die auch demokratisch verfasste Staaten betrifft. In diesen werden normalerweise Geheimdienste in ein Geflecht an rechtlichen Regelungen und Kontrollmechanismen eingebunden, um den durch ihre Funktionsweise tiefgreifenden Eingriff in die Grundrechte einzudämmen und auszugleichen. Bei den veröffentlichten Informationen kann man sich zu Recht die Frage stellen, ob dies noch funktioniert, ob nicht sogar die, die zur Kontrolle berufen sind, ihnen aus Unvermögen oder sogar willentlich freie Hand lassen. Hier sind wir (die Bundesrepublik Deutschland) gerufen, nach innen und nach außen tätig zu werden. Auch wenn das vorrangig die zögerlich vorgehende Bundesebene betrifft, kann auch Sachsen etwas tun. Ich habe mich im Juli 2013 an den Sächsischen Ministerpräsidenten mit Vorschlägen gewandt, die ich gleichlautend auch in einer Pressemitteilung veröffentlicht habe:

Vorzunehmende Maßnahmen aus Sicht des Sächsischen Datenschutzbeauftragten sind

1. eine eingehende Untersuchung, inwieweit sächsische Bürger, Behörden und Unternehmen und deren Kommunikation und gespeicherte Daten vor rechtsstaatswidrigen Zugriffen geschützt sind,

2. die Erprobung und der Einsatz von technischen Maßnahmen zur Datensicherheit, insbesondere zur durchgängigen Verschlüsselung bei der Übertragung und Speicherung von Daten,

3. die Förderung von lokalen Cloud-Diensten, die sächsischen Einrichtungen und Unternehmen eine sichere Verarbeitung der Daten erlauben,

4. der Einsatz und die Förderung von Softwareprodukten und Diensten, die im Hinblick auf Datensicherheit wegen ihrer transparenten Programmierung tatsächlich prüfbar sind,

5. die Stärkung behördlicher Informatikdienste, der Beauftragten für Informationssicherheit und der Beauftragten für den Datenschutz in den Behörden

6. eine deutliche Schwerpunktsetzung auf Informationssicherheit und Datenschutz bei den Behörden allgemein,

7. der Ausbau der Spionageabwehr in Sachsen und die Intensivierung der proaktiven Beratung behördlicher Einrichtungen, Unternehmen, Universitäten in Bezug auf Informationssicherheit,

8. eine verbesserte Vermittlung und Beratung zum Selbstdatenschutz, auch durch Bildungseinrichtungen.

Einiges davon ist umgesetzt. Sachsen hat ein neues E-Government-Gesetz beschlossen, das wesentlich auch auf IT-Sicherheitsfragen Bezug nimmt (siehe 5.9.6, 5.11.1, 5.12.2, 7.7, 14.2). Die damit verbundenen Anforderungen werden derzeit in der sächsischen Verwaltung sowohl auf Landes- als auch auf kommunaler Ebene angegangen. Anderes ist eine Daueraufgabe. Die in Punkt acht erwähnte Bildungsaufgabe richtet sich nicht nur an Andere, sondern gilt auch für meine Behörde. Ich sehe darin einen Schwerpunkt für meine Arbeit in der kommenden Zeit (siehe 7.1).

Der Vollständigkeit halber möchte ich erwähnen, dass die vorgeschlagenen Maßnahmen nicht nur aus der Bedrohung durch spionierende Geheimdienste egal welcher Couleur herrühren, sondern genauso durch die ständig wachsende Internetkriminalität bedingt sind, die Bürger und Unternehmen betrifft.

Abschließend möchte ich mich bei denen bedanken, die mich bei meiner Arbeit unterstützt haben. Die Exekutive bezieht mich frühzeitig in Planungen von datenschutzrechtlich relevanten Vorhaben ein. Auch wenn das nicht immer begeistert geschehen mag, ist es doch hilfreich, bereits im Vorfeld datenschutzrechtliche Anforderungen zu berücksichtigen, die später nur mit erheblichem Mehraufwand umgesetzt werden können. Dem Parlament gebührt in zweifacher Hinsicht Dank. Die Abgeordneten von Koalition und Opposition sind offen für Datenschutzanliegen und beziehen den Sächsischen Datenschutzbeauftragten aktiv in ihre parlamentarische Arbeit ein. Ich komme dem gern nach. Die Verwaltung des Sächsischen Landtages kümmert sich in vielfacher Weise (bei Beachtung unserer Unabhängigkeit) organisatorisch um uns. Dies ist nicht immer einfach wegen der unterschiedlichen Aufgabengebiete, wird aber im Beurteilungsdeutsch „zur vollsten Zufriedenheit“ gewährleistet. Letztendlich gilt mein Dank denen, die uns Hinweise geben, die sich in den Verwaltungen und Unternehmen um die Lösung von Datenschutzproblemen bemühen, die sich Rat suchend und gebend an uns wenden (dafür beachte 14.1). Ohne sie wäre unsere Arbeit nicht erfolgreich.

2 Parlament

In diesem Jahr nicht belegt.

3 Europäische Union / Europäische Gemeinschaft

3.1 Reform der Rechtsgrundlagen der Datenverarbeitung in der Europäischen Union

Im Berichtszeitraum setzte sich auf EU- wie auf deutscher Ebene die intensive Diskussion über die Entwürfe einer Datenschutzgrundverordnung (DGVO) sowie einer Richtlinie für den Strafverfolgungs- und -vollstreckungsbereich (RL) fort. Beide Entwürfe waren Anfang 2012 durch die EU-Kommission vorgelegt worden. Der DGVO kommt dabei eine überaus wichtige Rolle zu. Sie soll zukünftig unmittelbar in allen Mitgliedsstaaten gelten und den Datenschutz in den meisten Bereichen der öffentlichen Verwaltung regeln. Über die dringende Notwendigkeit einer Anpassung des geltenden, noch auf der Datenschutz-Richtlinie aus dem Jahre 1995 beruhenden Rechts der Mitgliedsstaaten an die seitdem eingetretene technische und gesellschaftliche Entwicklung und die wesentlichen Inhalte beider Gesetzentwürfe hatte ich bereits in meinem vorhergehenden Tätigkeitsbericht (16/3.1) berichtet.

Auch im Berichtszeitraum habe ich mich in vielen Arbeitsgruppen und Einzelgesprächen an der Meinungsbildung in der deutschen Datenschutzkonferenz sowie am Austausch mit der EU-Kommission und den Abgeordneten des Europäischen Parlaments beteiligt. Auch öffentlich habe ich mich mit meinen Kollegen aus der Datenschutzkonferenz mehrfach zu diesen großen Reformvorhaben geäußert. Gemeinsam haben wir insbesondere eine Reihe weiterer Entschließungen[1] verfasst und veröffentlicht. Wir haben dabei von Anfang an das Ziel der EU-Kommission unterstützt, einen „modernen, stabilen, kohärenten und umfassenden Datenschutz-Rechtsrahmen für die Europäische Union“, d. h. für deren ca. 500 Millionen Einwohner, bereitzustellen. Dies halte ich insbesondere vor der Tatsache, dass der Datenschutz seit Lissabon (2009) in den Primärverträgen der Union (vgl. Art. 8 EUV i. V. m. der Europäischen Grundrechtecharta; Art. 16 AEUV) - also quasi in der EU-Verfassung - niedergelegter Bestandteil der EU-Grundrechtsordnung ist, für zwingend geboten. Mit beiden Gesetzentwürfen wird über die künftige Machtverteilung zwischen dem Individuum und den staatlichen, kommunalen, universitären, Sozialversicherungs- etc. Kollektiven nicht nur in den EU-Mitgliedsstaaten entschieden. Welche Regelungen etwa für die Übermittlung personenbezogener Daten an Stellen außerhalb der EU gelten sollen, ist nicht nur im nicht-öffentlichen, sondern auch im öffentlichen Bereich von zentraler Bedeutung.

Die Bedeutung neuer, der rasanten technischen Entwicklung angepasster Rechtsgrundlagen für die Verarbeitung personenbezogener Daten in den Mitgliedsstaaten kann nicht

[1] „Zur Struktur der Europäischen Datenschutzaufsicht“ vom 27./28.3.2014 sowie „Datenschutz-Grundverordnung darf keine Mogelpackung werden!“ vom 18./19.3.2015, vgl. auch 16/17.1.8, 17.1.14, 17.1.19; jeweils abrufbar unter www.datenschutz.sachsen.de unter Öffentlicher Bereich/Datenschutzkonferenzen.

hoch genug eingeschätzt werden. Die vernetzte und allgegenwärtige Datenverarbeitung hat unser Leben grundlegend verändert. Die Folgen dieser Entwicklung sind noch nicht abschließend erkennbar. Noch immer stellen sich neue rechtliche und ethische Fragen. Sowohl der EU- wie auch der nationale Gesetzgeber hinken dabei leider der technischen Entwicklung mittlerweile um Jahrzehnte hinterher. Die dringenden Datenschutzfragen, die sich auch im öffentlichen Bereich ergeben haben (z. B. die Nutzung von „Big Data“ durch Sicherheitsbehörden und Nachrichtendienste), lassen sich mit dem heutigen rechtlichen und tatsächlichen Instrumentarium nicht befriedigend lösen. Zu diesem Thema gehört auch, dass die staatlichen Datenschutzbehörden in den Mitgliedsstaaten seit Jahrzehnten personell nicht in die Lage versetzt werden, die Datenschutzgrundrechte der Menschen wirkungsvoll zu schützen.

In den letzten zwei Jahren kam die Meinungsbildung auf der Ebene der Regierungen der Mitgliedsstaaten, im Rat der Europäischen Union, allerdings über lange Zeit nur zäh voran. Eine offenbare Beschleunigung scheint jedoch derzeit, gegen Ende des Berichtszeitraums, im ersten Quartal 2015, unter lettischer Präsidentschaft stattzufinden. So, wie die Dinge derzeit aussehen, werden die sog. Trilog-Verhandlungen zwischen der EU-Kommission, dem Europäischen Parlament und dem Rat, an deren Ende beschlussfähige abgestimmte Fassungen beider Gesetzentwürfe stehen sollen, voraussichtlich noch Mitte 2015 beginnen können. Damit würden voraussichtlich Ende 2015 oder spätestens Anfang 2016 beide Gesetze beschlossen werden und nach einer zweijährigen Übergangsfrist dann Ende 2017 bzw. Anfang 2018 in Kraft treten können.

Für mich ist es von außerordentlicher Bedeutung, dass die DGVO im Vergleich zum geltenden Rechtsstand - der im Wesentlichen durch die Richtlinie 95/46/EG geprägt ist - einen besseren, mindestens aber gleichwertigen Grundrechtsschutz gewährleistet. Die Reform des EU-Datenschutzrechts darf nicht dazu führen, hinter das geltende Datenschutzniveau zurückzufallen. Die sich aus Art. 8 der Europäischen Grundrechtecharta und Art. 16 Abs. 1 AEUV ergebenden Grundprinzipien des Datenschutzes dürfen nicht zur Disposition stehen. Gerade in Zeiten von Big Data, globaler Datenverarbeitung, einer „informationsbasierten Wirtschaft“ und nicht zuletzt staatlicher Zugriffe auf die riesigen Datenmengen - ich denke, um nur ein Beispiel zu benennen, an die orwellsche Überwachung unseres Verhaltens durch auch ausländische Nachrichtendienste wie die US-amerikanische *National Security Agency* oder das britische *General Communications Headquarters* - sind die informationelle Selbstbestimmung des Einzelnen und seine weiteren Datenschutzgrundrechte, die bisher geltenden Prinzipien der Datenverarbeitung, die Verantwortlichkeit des Datenverarbeiters sowie insgesamt die Rechtmäßigkeit, insbesondere die Verhältnismäßigkeit, der Datenverarbeitung ebenso wichtig wie eine starke Datenschutzaufsicht und wirksame Sanktionen.

Im Berichtszeitraum musste ich jedoch immer wieder beobachten, dass die im Rat der Europäischen Union versammelten Regierungen der Mitgliedsstaaten zentrale Inhalte des Kommissionsentwurfs in Frage stellten. Dies betraf insbesondere Kapitel II der DGVO (Grundsätze der Datenverarbeitung). Dort sollten nach dem Willen der Regierungen - und den meisten voran der deutschen Bundesregierung - erhebliche Interpretationsspielräume eröffnet werden, mit denen zentrale Datenschutzgrundsätze ausgehebelt werden können. Nur beispielhaft möchte ich hier einige der Forderungen des Rats aufführen: So setzte sich der Rat für eine unangemessen restriktive Auslegung des Begriffs des personenbezogenen Datums ein, wonach Kennnummern, Standortdaten, Online-Kennungen oder IP-Adressen nicht notwendigerweise als personenbezogene Daten anzusehen wären. Damit wären weite Bereiche der für die Grundrechte gefährlichen Datenverarbeitung vom Anwendungsbereich der DGVO ausgenommen. Auch sollten personenbezogene Daten nach den Vorstellungen des Rates einerseits ohne jede weitere Rechtsgrundlage zu anderen Zwecken als dem ursprünglichen Erhebungszweck verarbeitet werden dürfen, wenn der neue Zweck mit dem ursprünglichen Zweck noch vereinbar ist. Andererseits sollten noch darüber hinausgehende Zweckänderungen schon dann erlaubt sein, wenn der Datenverarbeiter hieran ein überwiegendes berechtigtes Interesse hat. Durch das Zusammenspiel dieser beiden Möglichkeiten könnten Zweckänderungen in einem derart weiten Umfang zulässig werden, dass das für den Datenschutz elementare Prinzip der Zweckbindung praktisch nicht mehr gälte. Dies würde die Entscheidungsfreiheit und die Transparenz für den Einzelnen weitgehend einschränken. Des Weiteren hat der Rat das Prinzip der Datensparsamkeit, das Kommission und Parlament erfreulicherweise ausdrücklich als eines der Grundprinzipien des Datenschutzes in Art. 5 Abs. 1 Buchst. c DGVO verankert hatten, aus dem Text gestrichen - ein fatales Zeichen zugunsten einer noch weiter ausufernden Verarbeitung personenbezogener Daten. Schließlich wollte der Rat u. a. die Verarbeitung personenbezogener Daten zu Forschungszwecken derart weitgehend privilegieren, dass ein angemessener Ausgleich mit dem Recht auf informationelle Selbstbestimmung des Betroffenen kaum noch möglich wäre. Mit seinen Vorschlägen fiel der Rat im Berichtszeitraum nicht nur hinter die Entwürfe der EU-Kommission und die Änderungsvorschläge des Europäischen Parlaments zurück, sondern bereitete sogar den Weg zu einer Verschlechterung des derzeitigen Datenschutzniveaus. Das ist mit dem erklärten politischen Ziel der Reform, der Verbesserung des Datenschutzes, nicht zu vereinbaren.

Auch was die nicht unmittelbar geltende, sondern durch nationales Recht umzusetzende Richtlinie für den Strafverfolgungs- und -vollstreckungsbereich angeht, bin ich in Sorge. Der Entwurf soll den derzeit noch geltenden - und übrigens in Deutschland nach sieben Jahren immer noch nicht umgesetzten (!) - Rahmenbeschluss 2008/977/JI des Rates, der nur die grenzüberschreitende polizeiliche und staatsanwaltliche Datenverar-

beitung regelt, ersetzen und den Strafverfolgungs- und -vollstreckungsbereich auf das Niveau der „alten“ EG-Richtlinie 95/46/EG heben. Zwar enthält der Richtlinienentwurf einige positive Ansätze: So soll u. a. die Einwilligung des Betroffenen als Rechtfertigungsgrund für eine Datenverarbeitung ausgeschlossen werden. Die Informationspflichten gegenüber dem Betroffenen bei offenen wie verdeckten Datenerhebungen sollen deutlich gestärkt werden. Die Löschungspflichten sollen noch stärker als bisher verfahrensrechtlich abgesichert werden. Doch insgesamt erreicht die Richtlinie nicht das Schutzniveau der DGVO. Daher ist jede Ausweitung des Anwendungsbereichs der Richtlinie problematisch. Und genau hier hat der Rat - und insbesondere die deutsche Bundesregierung - angesetzt. So spricht sich u. a. die Bundesregierung für eine deutliche Erweiterung des Anwendungsbereichs der RL aus. Insbesondere soll auch die Datenverarbeitung der Polizei zu Gefahrenabwehrzwecken unter die RL fallen. Dabei steht sogar im Raum, auch die Datenverarbeitung der Ordnungsverwaltungen, also z. B. der kommunalen Bußgeldstellen, unter die RL fallen zu lassen. Ich lehne eine solche Aufweichung und damit Verminderung des von der EU-Kommission entworfenen Schutzniveaus ab. Auch stellt die Bundesregierung (und hinter ihr die Länder) generell praktisch jegliche Regelungswirkung der RL in Frage. „Bestehende Verfahrensregeln“ für die Strafverfolger dürften durch Datenschutzregeln „nicht geändert oder eingeschränkt werden“. Was, bitte, soll dann überhaupt eine „Datenschutzreform“, die mit dem Ziel angetreten ist, die Schutzrechte für die Betroffenen im Strafverfolgungs- und -vollstreckungsbereich EU-weit auf einem angemessenen Niveau zu harmonisieren? Eigentlich macht die Bundesregierung damit ja die Ansage, die von der EU-Kommission geöffnete Akte am besten gleich wieder zuzumachen und es beim derzeitigen, von mir als sehr löchrig kritisierten Rahmenbeschluss für den Bereich der inneren Sicherheit zu belassen. Erfreulicherweise bestehen aber das Europäische Parlament und die EU-Kommission darauf, die DGVO und die RL nur als „Paket“ zu beschließen. Diesem Anliegen wünsche ich viel Erfolg.

4 Medien

In diesem Jahr nicht belegt.

5 Inneres

5.1 Personalwesen

5.1.1 Personenbezogene Daten für das Rechnungsprüfungsamt

Zuweilen besteht in Kommunalverwaltungen Unklarheit darüber, ob Mitteilungen über die Teilnahme an Schulungen und Gehaltsdaten einzelner Beschäftigter an das kommunale Rechnungsprüfungsamt datenschutzrechtlich zulässig sind.

Die Gemeindeordnung und die Sächsische Kommunalprüfungsverordnung-Doppik weisen dem Rechnungsprüfungsamt und seinen Prüfern eine hohe Verantwortung und Unabhängigkeit zu. Der Prüfer ist bei seinen Aufgaben zu unterstützen, er kann alle Auskünfte und Unterlagen verlangen sowie eigene Erhebungen vornehmen, die zur Erfüllung seiner Aufgaben erforderlich sind (§ 5 Abs. 3 SächsKomPrüfVO-Doppik).

Neben der Prüfung des Jahresabschlusses und des Gesamtabschlusses (§ 104 SächsGemO) und der Prüfung der Eigenbetriebe (§ 105 SächsGemO) werden weitere Aufgaben geregelt. So werden weitere sogenannte freiwillige Aufgaben des Rechnungsprüfungsamtes aufgeführt, die es von selbst (auf eigene Initiative) wahrnehmen kann (§ 106 Abs. 2 SächsGemO). Dazu gehört unter Nummer 1 die Prüfung der Organisation und Wirtschaftlichkeit der Verwaltung.

Die Kommunalverwaltung hat zu prüfen, ob die an sie gerichteten Forderungen des Rechnungsprüfungsamtes zur Weitergabe personenbezogener Daten aus einer gesetzlich normierten Aufgabenstellung resultieren. Soweit das auf die konkret genannte Aufgabe des Rechnungsprüfungsamtes zutrifft, hat die Verwaltung den Prüfer bei seiner Arbeit in allem zu unterstützen, was einer sachgemäßen und zügigen Erledigung der Prüfung dient. Die Mitarbeiter der Verwaltung sind verpflichtet, dem Prüfer wahrheitsgemäß und umfassend Auskünfte zu erteilen und Unterlagen zur Einsicht zu geben, die zur Erfüllung seiner Prüfungsaufgabe objektiv erforderlich und notwendig sind. Auch Gesundheits- und Sozialdaten sowie Daten, die durch das Steuergeheimnis oder allgemein datenschutzrechtlich zu schützen sind, unterliegen diesem Einsichtnahmerecht, wenn die Einsichtnahme zur Erfüllung der Prüfaufgabe objektiv erforderlich ist (vgl. Quecke/Schmid, Kommentar Gemeindeordnung, § 103 Rdnr. 79, 84 f.). Beschäftigtendaten sind nicht ausgenommen.

Hinzuweisen ist in diesem Zusammenhang auf den Bezug zur VwV Personalakten, die den kommunalen Gebietskörperschaften zur Anwendung empfohlen wird. Die VwV Personalakten verweist unter Buchst. E, II zur Erteilung von Auskünften oder die Herausgabe von Personalakten u. a. auf § 95 SäHO. Danach sind Unterlagen, die der Rechnungshof zur Erfüllung seiner Aufgaben für erforderlich hält, diesem auf Verlangen

innerhalb einer bestimmten Frist zu übersenden oder seinen Beauftragten vorzulegen; die erbetenen Auskünfte sind zu erteilen. Diese streng genommen für die überörtliche Prüfungsbehörde geltende Regelung kann durchaus auch in Bezug auf die örtliche Prüfung durch das Rechnungsprüfungsamt bei der Auslegung der Mitwirkungspflichten herangezogen werden.

5.1.2 Ehegatteneinkünfte im Beihilfeverfahren

Ein Petent wies mich darauf hin, dass in einem Merkblatt des Landesamts für Steuern und Finanzen ein (vollständiger) Steuerbescheid als Voraussetzung für die Gewährung von Beihilfe für den Ehegatten angesehen wird. Ich bat das LSF um Stellungnahme, wofür über den Gesamtbetrag der Einkünfte hinausgehende Angaben benötigt werden, da gemäß § 12 Abs. 1 SächsDSG Daten nur dann erhoben werden dürfen, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist.

Das LSF verwies in seiner Antwort auf § 4 Abs. 2 Satz 1 SächsBhVO. Dieser verlangt jedoch ausdrücklich lediglich den Gesamtbetrag der Einkünfte (nach § 2 Abs. 3 EStG).

Nachdem ich mit einem erneuten Schreiben das LSF von meiner Rechtsauffassung überzeugen konnte, wurde das Merkblatt entsprechend geändert.

5.1.3 Beschäftigtendatenverarbeitung zur Prüfung der Eignung von Bediensteten

Im letzten Berichtszeitraum wandten sich Bedienstete einer JVA an meine Behörde. Gegenstand war ein Schreiben des SMJus an die Anstaltsleitung, das Vorkehrungen seitens der Einrichtung vorsah, um möglichen „Grenzverletzungen“ zwischen Bediensteten des allgemeinen Vollzugsdienstes und Gefangenen vorzubeugen bzw. in diesen Fällen Maßnahmen ergreifen zu können. Hintergrund waren in der Vergangenheit vorgekommene Beziehungen und Verhältnisse zwischen Vollzugsbediensteten und Gefangenen gewesen. Z. T. war eine mediale Resonanz zu Vorkommnissen dieser Art zu verzeichnen.

Mit dem ministeriellen Schreiben wurde der Anstalt ein Maßnahmenbündel auferlegt, eine „Risikoanalyse und Prüfung der Eignung von Bediensteten“, eine „regelmäßige Analyse der sozialen Beziehungen von Bediensteten und Gefangenen im Stationsbereich (Frühwarnsystem)“ und eine „Fortbildung, kollegiale Beratung und Supervision für die Bediensteten der JVA…“ zu verfolgen. Ich teilte dem Ministerium mit, dass eine Beschäftigtendatenverarbeitung gemäß § 37 SächsDSG bzw. bei Beamten gemäß den personalaktenrechtlichen Bestimmungen des Sächsischen Beamtengesetzes zulässig sei. Daneben enthält das Beamtengesetz Festlegungen zu Fragen der Eignung und Befähi-

gung, die durch einschlägige Verordnungen ergänzt werden. Ich betonte dem Ministerium gegenüber, dass eine Verarbeitung der Daten der Bediensteten in geregelten Verfahren zu erfolgen habe.

Bedenken erhob ich zum einen, da mir unklar erschien, wie die Risikoanalyse und Prüfung der Eignung von Bediensteten anhand einer von der obersten Dienstbehörde vorgegebenen Checkliste vonstattengehen sollte, wie die erhobenen Daten verwendet und ob und wie die erhobenen Daten in der Personalakte verarbeitet werden können sollten. Ebenso hatte ich Zweifel an einer Verarbeitung außerhalb der Personalakte. Ein Problem schienen mir auch die relativ ungeregelten und - aus datenschutzrechtlicher Sicht - problematischen kaum zu umreißenden gefühlsbezogenen Einschätzungen im Beziehungsbereich zu sein, die nach den ministeriellen Ausführungen ausdrücklich im Hinblick auf die Analyse der sozialen Beziehungen im Stationsbereich eine Rolle spielen sollten. Auch sollten Informationen der Gefangenen zu Bediensteten genutzt werden, wogegen ich wegen der planmäßigen und verdeckten Datenerhebung über Bedienstete bei Dritten Bedenken geltend machte.

In einem Gespräch und in einer ersten Stellungnahme teilte mir das Ministerium mit, dass die besagte Checkliste zur „Risikoanalyse und Prüfung der Eignung von Bediensteten“ ausschließlich als Gedankenstütze für den verantwortlichen Vorgesetzten anzusehen und von diesem zu verwenden sei. Zur Wahrung der datenschutzrechtlichen Bestimmungen sollten die in der Checkliste aufgeführten Fragen grundsätzlich ohne Aufzeichnung von personenbezogenen Daten ausgewertet werden.

Auch wurde mir zugesichert, dass die vorgesehene Analyse der sozialen Beziehungen von Bediensteten und Gefangenenstationsbereich ausschließlich dem fachlichen Austausch im „Team“ dienen solle, keinesfalls aber einer Bewertung oder gar dienstrechtlichen Beurteilung einzelner Bediensteter. Auch dabei sollte - so stellt es das Ministerium gegenüber der Anstalt klar - auf die Erhebung personenbezogener Daten verzichtet werden. Soweit personenbezogene Daten in der Besprechung anfallen sollten, sollten diese nach deren jeweiligem Ende unverzüglich auf datenschutzkonforme Weise gelöscht werden.

Die oberste Dienstbehörde verhielt sich bedacht. Aufgrund eines weiteren klarstellenden Schreibens des Ministeriums an die Anstalt mit den Stellungnahmen und Versicherungen mir gegenüber entsprechenden Inhalts konnte ich den Vorgang abschließen.

5.1.4 Grenzen der Auftragsdatenverarbeitung - Vorgesehene Privatisierung im Beschaffungswesen

Das Landespolizeipräsidium beteiligte mich in meiner Beratungsfunktion für öffentliche Stellen (§ 30 Abs. 4 SächsDSG). Infolge des Gutachtens eines Beratungsunternehmens erwog die Polizeiverwaltung die Privatisierung der Beschaffung von Dienst- und Schutzkleidung bei der sächsischen Polizei. Auch das Justizressort bekundete wegen seiner Justizvollzugsbeamten Interesse. Das Landespolizeipräsidium übersandte mir die entsprechenden Vertrags- und Vergabeunterlagen, nach denen die Belieferung der Bediensteten mit Dienstkleidung durch einen externen Dienstleister durchgeführt werden sollte. Gegenstand der Auftragsvergabe war die Übernahme, Lagerung und vorrangige Auslieferung von Vorräten an Dienstkleidung sowie der Einkauf der Ware. Ferner sollte ein automatisiertes Verfahren mit einer von dem Dienstleister betriebenen Bestellplattform eingerichtet werden. Über ein Online-Verfahren und einen individuellen Account sollte den einzelnen Bediensteten der Zugang zu den Anwendungen eröffnet werden, die die Abwicklung von Bestellungen, Retouren, Reklamationen, Beschwerden, Umtausch sowie die Rücknahme, Vernichtung oder Verwertung von Dienstkleidung ermöglichen sollten. Zur Durchführung des Verfahrens sollte der Auftragnehmer jeweils Name, Vorname, Dienststelle und die dienstliche E-Mail-Adresse und Konfektionsgröße sowie im Falle von Privatbestellungen die Kontoverbindung und die Bankleitzahl als personenbezogene Daten der Bediensteten verarbeiten dürfen. Die Stammdaten sollten von der Polizeiverwaltung zur Verfügung gestellt werden. Das Online-Verfahren sollte aus Sicherheitsgründen nicht über das Internet, sondern ausschließlich über das SVN realisiert werden.

Der Freistaat Sachsen ist Träger der Aufgabe, seine Bediensteten mit angemessener Dienstkleidung auszustatten. Unter anderem § 136 SächsBG regelt, dass die Beamten des uniformierten Polizeivollzugsdienstes freie Dienstkleidung erhalten. Entsprechendes gilt für Beamte des Justizvollzugsdienstes (§ 143 SächsBG). Es stellte sich die zu beantwortende datenschutzrechtliche Frage, ob ein Auftragnehmer an der hoheitlichen Aufgabe in der vorgesehenen Weise beteiligt werden konnte und in welchem Umfang er befugt sein können sollte, für die öffentliche Stelle die Beschäftigtendaten im Zusammenhang mit der Beschaffung der Dienstkleidung zu verarbeiten.

Ich hatte mich in der Vergangenheit bereits mehrfach mit der Frage auseinanderzusetzen gehabt, inwieweit sich öffentliche Stellen Verwaltungshelfern als „Werkzeug“ bei der Erledigung öffentlich-rechtlicher - auch hoheitlicher - Aufgaben bedienen können. Aufgrund der beamtengesetzlichen Bestimmungen und der Bindung der Verwaltung an die gesetzlich ihr übertragene Aufgabenerfüllung bin ich - wie in anderen ver-

gleichbaren Fällen - davon ausgegangen, dass das Verfahren datenschutzrechtlich nur als Auftragsdatenverarbeitung gemäß § 7 SächsDSG umgesetzt werden darf. Bei einer Auftragsdatenverarbeitung würde der Auftragnehmer und Dienstleister nur eine technische Unterstützungsleistung im Hinblick auf die vorzunehmende personenbezogene Datenverarbeitung erbringen, wäre nur nach den Weisungen der Polizeiverwaltung befugt, personenbezogene Daten zu verarbeiten und der Auftraggeber, die Polizeiverwaltung, wäre weiterhin datenschutzrechtlich verantwortlich, als datenverarbeitende Stelle zu betrachten und würde weiterhin den Inhalt der Daten bestimmen (vgl. § 7 SächsDSG). Rechtlich wäre im Fall einer Auftragsdatenverarbeitung die Weitergabe von Informationen durch den Auftraggeber an den Auftragnehmer nicht als Übermittlung von Beschäftigtendaten anzusehen gewesen, sondern würde wie eine Weitergabe innerhalb der organisatorischen Stelle der Polizeiverwaltung betrachtet. Andernfalls würde es sich um eine Datenübermittlung handeln. Die Übermittlung von Beschäftigtendaten an nichtöffentliche Stellen ist hingegen gesetzlich beschränkt und wäre im konkreten Rechtsfall nur zulässig gewesen, soweit eine Rechtsvorschrift eine Übermittlung vorsieht oder der Betroffene einwilligt (vgl. § 37 Abs. 3 SächsDSG).

Bei der Frage der rechtlichen Einordnung, wie der Austausch personenbezogener Daten mit dem Dienstleister zu bewerten war, war die Auftragsdatenverarbeitung gegenüber der Funktionsübertragung abzugrenzen. Schutzfunktion der gesetzlichen Regelungen zur Auftragsdatenverarbeitung des § 7 SächsDSG ist, sicherzustellen, dass den Betroffenen gegenüber, die Behörde, die ihre personenbezogenen Daten ursprünglich erhoben und verarbeitet hat, in ihrer datenschutzrechtlichen Verantwortung bleibt. Behörden sollen sich ihrer Verantwortung nicht dadurch entledigen können, dass sie die Datenverarbeitung auslagern. Eine „Flucht ins Privatrecht“ soll es nicht geben. Obwohl der Anwendungsbereich des § 7 SächsDSG eigentlich relativ eng auf *unterstützende technische Hilfsdienstleistungen* eingegrenzt ist, wird die Vorschrift seitens der Behörden zum Teil sehr weit ausgelegt. Dies geschieht vor allem dadurch, dass das Auftragsverhältnis, das der Anwendung des § 7 SächsDSG zugrunde liegt, häufig nicht nur auf die Datenverarbeitung im engen technischen Sinne bezogen wird, sondern auch auf eine inhaltliche Aufgabenübertragung. Damit wird die Norm seitens der Exekutive allerdings zu einer allgemeinen Rechtsgrundlage für Outsourcing und Aufgabenübertragung auf Dritte umgeformt, obwohl sie vom Wortlaut und Zweck her eine ganz andere Fallgestaltung regeln soll. Der Auftrag hat sich auf die eigentliche technische Abwicklung der Datenverarbeitung nach einem vorgegebenen Algorithmus zu beziehen, nicht auf die Übertragung von Aufgaben oder Teilaufgaben, bei denen nicht alle vorzunehmenden Verarbeitungsschritte von vornherein festgelegt sind. Auch die Weisungen des Auftraggebers im Sinne der Vorschrift haben sich auf die Datenverarbeitung selbst und nicht etwa auf eine inhaltliche Aufgabenerledigung zu beziehen. Das klassische Beispiel für Auftrags-

datenverarbeitung bleibt damit die Nutzung externer Rechenzentren oder Speicherkapazitäten, sofern ausschließlich rechentechnische Vorgänge nach vorgegebenen Algorithmen ausgelagert werden.

Vorstellbar wäre, übertragen auf den Ausgangsfall, daher gewesen, dass der Dienstleister die Bestellungen zu Dienstkleidung lediglich für Behörden speichert und für diese „durchleitet".

Soweit Aufgaben oder auch Teilbereiche der Aufgabenerfüllung auf eine andere öffentliche oder nicht-öffentliche Stelle übertragen werden sollen und die damit verbundene elektronische Datenverarbeitung nur Annex zur eigentlichen Aufgabenverlagerung ist, ist zu beachten, dass angesichts der verfassungsrechtlich geforderten Bindung der Verwaltung an Recht und Gesetz eine funktionale Tätigkeit nur durch den Gesetz- und Verordnungsgeber bestimmt werden kann, wobei gleichzeitig der Umfang der funktionalen Tätigkeit des Auftragnehmers zu begrenzen und die zuständige Stelle für deren Aufgaben zu bestimmen ist. Soll die inhaltliche Wahrnehmung von Aufgaben vollständig oder in Teilbereichen auf andere Stellen übertragen werden, scheiden als rechtliche Grundlage hingegen die Bestimmungen über die Auftragsdatenverarbeitung aus, auch wenn der Auftragnehmer keine eigenen Entscheidungsspielräume hat und bei der inhaltlichen Auftragserfüllung vollständig von Weisungen des Auftraggebers abhängig ist. Eine Weisungsbindung an den Auftraggeber reicht nicht aus, da verfassungsrechtlich die Zuständigkeit für die Aufgabenerledigung durch Rechtsvorschrift definiert ist und die auf die bloße Datenverarbeitung als Hilfsfunktion zur Aufgabenerfüllung gerichtete Vorschrift des § 7 SächsDSG eine gesetzliche Festlegung nicht zu ändern geeignet ist.

In Bezug auf die beamtengesetzlichen Dienstkleidungsvorschriften war nach meiner Überzeugung davon auszugehen, dass Verantwortung und Aufgabenwahrnehmung beim Freistaat Sachsen und seinen Behörden verbleiben sollten. Jedenfalls eröffneten das Sächsische Beamtengesetz bzw. die ergänzenden Rechtsverordnungen keinen Raum, um nicht-öffentliche Stellen bzw. Dritte zu beleihen.

Die mir übersandten Vertrags- und Vergabeunterlagen sahen demgegenüber vor, dass die Belieferung von Dienstkleidungsträgern „eigenverantwortlich" durchgeführt werden sollte. Ausweislich einer Antwort der Staatsregierung zu einer Kleinen Anfrage im Sächsischen Landtag - LT-Drs. 5/14390 - ging das SMI von einer „Privatisierung" bzw. „Vollprivatisierung" des Beschaffungswesens im Polizeibereich aus. Eine Auftragsdatenverarbeitung, so teilte ich es dem Polizeipräsidium mit, wäre nach den dargestellten Grundsätzen noch vorstellbar gewesen, wenn es sich bei dem Dienstleister lediglich um einen Verwaltungshelfer gehandelt hätte, der - anders als ein Beliehener - nur tech-

nische Aufgaben vollzogen hätte. Dabei wäre der Helfer lediglich „Werkzeug“ der Behörde und bei der Erledigung hoheitlicher Aufgaben tätig. Der Leistungsumfang des Auftragnehmers war aber nicht mehr nur als technische Unterstützung anzusehen gewesen. Insbesondere fiel auf, dass der Dienstleister auch nach außen hin eigenverantwortlich tätig werden sollte, d. h., dass er auch als eigene Rechtsperson und nicht als Helfer der staatlichen Behörden auftreten sollte, etwa dann, wenn Dienstkleidung von Zulieferern aufgekauft werden sollte. Allein die Weitergabe von Erklärungen der Behörde im Namen der Behörde und die Entgegennahme von Erklärungen für die Behörde hätte noch den Schluss erlauben können, dass die Aufgabe weiterhin vom Freistaat Sachsen wahrgenommen werden sollte. Bereits die Wortwahl „Privatisierung“ und „Vollprivatisierung“ in der Antwort zu der Kleinen Anfrage seitens der Staatsregierung zeigte, dass mehr gewollt war, dass man - so war es meine Überzeugung - die Aufgabe zu verlagern bzw. sich ihr zu entledigen versuchte. Im Ergebnis ging ich daher von einer Funktionsübertragung aus. Damit wäre auch eine Übermittlung personenbezogener Daten der Bediensteten verbunden gewesen (vergleiche oben), die aber nach meiner Überzeugung nicht erforderlich gewesen war. Eine nicht erforderliche Datenverarbeitung wäre nach § 37 SächsDSG unzulässig gewesen. Begleitend kam hinzu, dass eine Rechtsvorschrift, die eine Aufgabenverlagerung vorsah, nicht existierte. Damit war das Verfahren in der vorgesehenen Weise - bei gegenwärtiger Rechtslage - nicht ordnungsgemäß umsetzbar.

Nachdem ich mein Prüfergebnis dem Landespolizeipräsidium mitgeteilt hatte, teilte mir die Behörde mit, dass sie das Vorhaben nicht weiterverfolgen werde.

5.1.5 Videodatenverarbeitung im Beschäftigungsverhältnis

Die Videoüberwachung und Videoaufzeichnung öffentlich zugänglicher Bereiche durch öffentliche Stellen zum Schutz der Liegenschaften, zum Schutz von Personen oder zur Abwehr von Vandalismus, Diebstählen oder sonstigen Eigentumsdelikten ist in § 33 SächsDSG geregelt. Bei der Kontrollpraxis meiner Behörde ist eine deutliche Zunahme von Videobeobachtungsmaßnahmen festzustellen. Aber auch in den nicht-öffentlich zugänglichen Bereichen der Behörden wird zunehmend videografiert. Die Videobeobachtung nicht-öffentlich zugänglicher Räume - zum Beispiel eines Serverraums oder eines städtischen Kassenbereichs - ist nicht in § 33 SächsDSG geregelt. Die Datenverarbeitung ist dann auf die allgemeinen Verarbeitungsbestimmungen des zweiten Abschnitts des Sächsischen Datenschutzgesetzes zu stützen.

In beiden Fällen - bei öffentlich und bei nicht-öffentlich zugänglichen Bereichen - ist es nicht primäre Absicht, mit optisch-elektronischen Einrichtungen Beschäftigte zu beobachten, ihr Verhalten aufzuzeichnen oder sie zu kontrollieren. Gleichwohl findet eine

Videobeobachtung dieser Personengruppe statt und es ist zu beachten, dass die Videodatenverarbeitung der Beschäftigten nur in beschränktem Umfang und nach transparenten und klaren Regeln zulässig ist. Zu beachten ist in diesem Zusammenhang auch, dass in einigen Bereichen, wie in Sozial-, Sanitär- und Umkleideräumen ein Videografieren aus Persönlichkeitsrechts- und Verhältnismäßigkeitsgesichtspunkten von vorneherein ausgeschlossen ist.

Die Dienststelle ist grundsätzlich befugt, eine Videobeobachtung einzurichten. Die Zulässigkeit der Maßnahme erfordert aber zunächst ein Vorliegen der gesetzlichen Datenverarbeitungsvoraussetzungen (§§ 33, 12 ff. SächsDSG). Zusätzlich muss der Eingriff in die Persönlichkeitsrechte der Beschäftigten verhältnismäßig sein. Um eine Videobeobachtung durchführen zu dürfen, hat die öffentliche Stelle auch - so empfehle ich es regelmäßig - mit der Personalvertretung eine Dienstvereinbarung abzuschließen. Ohnehin hat die Personalvertretung bei Videobeobachtung nach dem Sächsischen Personalvertretungsgesetz mitzubestimmen. Dienstvereinbarungen haben nach dem Sächsischen Datenschutzgesetz normative Wirkung (§ 37 Abs. 1 SächsDSG). Auf sie kann - soweit die Festlegungen darin im Einklang mit höherrangigem Recht stehen - personenbezogene Datenverarbeitung gestützt werden.

Zu berücksichtigen ist, dass die Videoüberwachung und Videoaufzeichnung alle beeinträchtigt, die den überwachten Bereich betreten, unabhängig davon, ob die Betroffenen Anlass für einen Verdacht geben oder nicht. Derartige verdachtslose Eingriffe mit großer Streubreite haben eine hohe Eingriffsintensität.

Unter 17.2.1 empfehle ich eine Musterdienstvereinbarung zum datenschutzgerechten Gebrauch.

5.2 Personalvertretung

In diesem Jahr nicht belegt.

5.3 Einwohnermeldewesen

5.3.1 Unterbliebene Vernichtung von Meldescheinen

Ein Betroffener informierte mich darüber, dass eine Stadtverwaltung ihrer Verpflichtung gemäß § 18 Abs. 1 SächsMeldVO, Meldescheine - die gesetzlich vorgesehenen Vordrucke für An- und Abmeldungen - längstens bis zum Ablauf des dritten auf die Abgabe des Meldescheins folgenden Kalenderjahres gesondert aufzubewahren und danach zu vernichten, nicht nachgekommen sei. Um den Sachverhalt datenschutzrechtlich zu prüfen, bat ich die betroffene Meldebehörde um Stellungnahme.

Die Stadtverwaltung teilte mir mit, dass sie mit einer verbreiteten Einwohnermeldeamt-Software arbeite und im Zuge der ständig fortschreitenden Informationstechnik der Verwaltungsprozesse auf verordnungsrechtlicher Grundlage die Meldescheine elektronisch in einer sogenannten „E-Akte“ speichern würde. In diesem Verfahren könne bei dem entsprechenden elektronischen Dokument auch eine Frist für die Aufbewahrung von Daten angegeben werden. Diese Eingabe sei durch die Stadtverwaltung erfolgt.

Allerdings hatte die Stadt dennoch bei der informationstechnischen Umsetzung der Löschfristen Schwierigkeiten. Die Löschung der elektronisch gespeicherten Original-Meldescheine bereitete nämlich technische Probleme aufgrund der Programmierung und Konfiguration der einzurichtenden Schnittstelle. Die Stadt versicherte, dem Softwareanbieter einen Auftrag zur Lösung des Problems erteilt zu haben und dieser werde im Zuge der Umstellung der Einwohnersoftware mit aktualisierten Modulen, u. a. zur Dokumentenarchivierung und Dokumentenlöschung, diesen Mangel beseitigen.

Ich wies die Stadt darauf hin, dass diese als Auftraggeber für die Einhaltung des Sächsischen Datenschutzgesetzes und anderer Vorschriften über den Datenschutz verantwortlich sei (§ 7 Abs. 1 Satz 1, Abs. 5 SächsDSG). Dies gelte auch, wenn sie der Verpflichtung gemäß § 18 Abs. 1 SächsMeldVO bisher aus technischen Gründen nicht nachgekommen sei und ein Softwareunternehmen diese Gründe im Innenverhältnis gegenüber dem Auftraggeber zu vertreten habe bzw. keine gesetzeskonforme Softwarelösung zur Verfügung zu stellen in der Lage sei. Ich forderte die Stadtverwaltung auf, den melderechtlichen Verstoß innerhalb von zwei Monaten zu beheben. Ein fortgesetzter rechtswidriger Zustand entgegen § 18 Abs. 1 SächsMeldVO wäre meinerseits gemäß § 29 SächsDSG zu beanstanden gewesen.

Mittlerweile teilte mir die Stadtverwaltung mit, dass die Löschung der Meldescheine gemäß § 18 SächsMeldVO abschließend erfolgt sei.

5.3.2 Einschränkung der Widerspruchsrechte eines Betroffenen im Rahmen der Anmeldung durch ein Einwohnermeldeamt

Ein Betroffener wandte sich an mich und bat um datenschutzrechtliche Prüfung der Rechtmäßigkeit der Verkürzung seiner Widerspruchsrechte durch die Meldebehörde. Der Betroffene teilte mir mit, dass er bei der Anmeldung beim Einwohnermeldeamt alle auf dem behördlichen Vordruck vorgesehenen gesetzlichen Widerspruchsmöglichkeiten angekreuzt habe. Auf dem Ausdruck der Anmeldebestätigung waren hingegen die Kreuze in den Feldern „Übermittlung der Daten an Presse, Rundfunk, und andere Medien zum Zwecke der Veröffentlichung von Alters- und Ehejubilaren“, „Weitergabe der Daten an öffentlich-rechtliche Religionsgesellschaften, wenn der Ehegatte oder ein Eltern-

teil eines minderjährigen Kindes dieser zwar angehört, die Person oder das Kind jedoch nicht“, „Erteilung einfacher Melderegisterauskünfte zu erkennbaren Zwecke der Direktwerbung“ und „Widerspruch gegen die Datenübermittlung an das Bundesamt für Wehrverwaltung“ unberücksichtigt geblieben.

Die Stadtverwaltung - so teilte mir es der Betroffene mit - habe ihm auf Nachfrage schriftlich mitgeteilt, dass die Übermittlungssperren nicht eingetragen worden seien, die nicht auf ihn zutreffen würden.

Ich forderte die betreffende Meldebehörde zur Stellungnahme auf. Die Stadtverwaltung teilte mir daraufhin mit, dass das Einwohnermeldeamt nur „sinnvolle Widersprüche“, d. h. auf die jeweilige Person zutreffende Übermittlungssperren in das Melderegister eintragen würde.

Diese geübte Verwaltungspraxis entsprach nicht den gesetzlichen Bestimmungen (§ 23 Abs. 1 Nr. 4 SächsMG). Die Vorschrift bestimmt, dass der Betroffene gegenüber der Meldebehörde nach Maßgabe des Gesetzes ein Recht auf Widerspruch gegen die Übermittlung bzw. Veröffentlichung seiner Daten hat (vgl. § 30 Abs. 2 Satz 3, § 32 Abs. 4 Satz 4, § 33 Abs. 4 Satz 1 SächsMG). Die Behörde ist an die Vorgaben des jeweiligen Betroffenen gebunden. Eine Überprüfung gesetzlich vorgesehener Widerspruchsentscheidungen des Betroffenen ist nach dem Sächsischen Meldegesetz nicht vorgesehen. Die Meldebehörde hatte demzufolge aufgrund der geltend gemachten Widersprüche die Übermittlungssperren sämtlich einzutragen und diese so lange zu berücksichtigen gehabt, bis sie vom Betroffenen zurückgenommen werden oder dieser aus der Gemeinde weggezogen ist.

Ich wies die Stadtverwaltung abschließend auf die Rechtslage hin und gehe davon aus, dass der Wille der Bürger zukünftig ordnungsgemäß Beachtung findet.

5.3.3 Übermittlung von Meldedaten gemäß § 29 SächsMG trotz Vorliegens eines Offenbarungsverbotes gemäß § 5 TSG

Eine Gemeinde wandte sich mit der Bitte um datenschutzrechtliche Prüfung eines Vorgangs im Zusammenhang mit dem Offenbarungsverbot nach dem Transsexuellengesetz an mich. Die Stelle teilte mir mit, dass ein Betroffener mit Bescheid aus dem Jahr 1997 aufgefordert worden sei, Wohngeld zurückzuzahlen. Der Aufhebungs- und Rückforderungsbescheid sei rechtskräftig, unanfechtbar und vollstreckbar. Die Verjährungsfrist betrage 30 Jahre. Vollstreckungsversuche in den vergangenen Jahren seien erfolglos verlaufen. Die Forderung sei mehrmals befristet niedergeschlagen worden.

Im Jahr 2005 habe die zuständige Vollstreckungsbehörde zur Beitreibung des Wohngeldes ein Amtshilfeersuchen an die zuständige Meldebehörde gerichtet. Da der Vollstreckungsbehörde Informationen vorlagen, dass der betroffene Schuldner nicht unter der genannten Wohnanschrift gemeldet sei, sei die Meldebehörde um die Übermittlung der Daten zur Person des Betroffenen gebeten worden. Das angefragte Einwohnermeldeamt habe der Vollstreckungsbehörde daraufhin mitgeteilt, dass die betroffene Person eine Änderung ihres Vornamens durchgeführt habe und unter der genannten Adresse als weibliche Person gemeldet sei. Aufgrund der meldebehördlichen Auskunft seien nun gegen die Frau Vollstreckungsmaßnahmen eingeleitet worden. Im Jahr 2006 sei erneut ein Ersuchen um Amtshilfe zur Vollstreckung des Wohngeldes an die gemeindliche Stadtkasse übersandt worden. Die Vollstreckungsmitteilung der Stadt ergab, dass die Frau die Zahlung verweigere und sich dabei auf das Offenbarungsverbot des § 5 TSG berufe.

Der Behörde liege ein Schreiben der Schuldnerin vor, in welchem die betroffene Frau mit einer Strafanzeige wegen des Verstoßes gegen das Sächsische Datenschutzgesetz drohe.

§ 5 Abs. 1 TSG regelt, dass die zur Zeit der Entscheidung der Namensänderung bisher geführten Vornamen ohne Zustimmung des Antragstellers nicht offenbart oder ausgeforscht werden dürfen, es sei denn, dass besondere Gründe des öffentlichen Interesses dies erfordern oder ein rechtliches Interesse glaubhaft gemacht wird.

Für die Meldebehörde gilt das Offenbarungsverbot des § 5 Abs. 1 TSG unmittelbar. Sie hat für die betroffene Person von Amts wegen eine Auskunftssperre einzutragen, wenn sie vom zuständigen Standesbeamten eine Mitteilung über die Änderung des Vornamens eines Transsexuellen erhält. Konsequenz des Vorliegens der Auskunftssperre ist, dass eine Melderegisterauskunft an Private (§§ 32 und 32a SächsMG) unzulässig ist, es sei denn, dass nach Anhörung des Betroffenen eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen, welche für ihn oder eine andere Person erwachsen kann (§ 34 Abs. 1 SächsMG), ausgeschlossen werden kann. Die Übermittlungsverbote des § 34 SächsMG erfassen damit also lediglich die Melderegisterauskünfte an Private.

Trotz des Vorliegens eines Offenbarungsverbotes gemäß § 5 TSG ist eine Übermittlung der Meldedaten an Behörden und sonstige öffentliche Stellen gemäß § 29 SächsMG melderechtlich zulässig. Aufgabe der zuständigen Vollstreckungsbehörde ist im vorliegenden Fall die Durchsetzung der Rückzahlung ungerechtfertigt erbrachter staatlicher Leistungen. Zum Schutz des Betroffenen sieht § 29 Abs. 6 SächsMG aber auch für die öffentlichen Stellen, welche Meldedaten empfangen haben, in den Fällen des § 34

Abs. 1 und 2 SächsMG besondere Pflichten vor. Sie sind verpflichtet, sorgfältig zu prüfen, ob durch eine weitere Verarbeitung oder Nutzung der übermittelten Meldedaten, insbesondere der Datenweitergabe an Dritte, schutzwürdige Interessen des Betroffenen gefährdet werden könnten. Eine Verarbeitung oder Nutzung der übermittelten oder weitergegebenen Daten ist nur zulässig, wenn die Beeinträchtigung schutzwürdiger Interessen des Betroffenen ausgeschlossen werden kann.

Von einer Beeinträchtigung schutzwürdiger Interessen der betroffenen Person war bei dem streitigen Vorgang nicht auszugehen, da sich die Vollstreckungsbehörde mit den empfangenen Meldedaten an die betroffene Person selbst - und nicht an Dritte gewandt hatte. Eine Beeinträchtigung schutzwürdiger Interessen könnte jedoch nur dann nicht ausgeschlossen werden, wenn nicht zweifelsfrei feststeht, dass es sich bei der in Rede stehenden Person um den Adressaten des von der Vollstreckungsbehörde angeführten Bescheides handelt.

Unberücksichtigt blieb meinerseits die Frage, ob als Voraussetzung für die Vollstreckung der im Bescheid aufgeführte ehemalige Vorname der betroffenen Person in den aktuellen Vornamen zu ändern gewesen war. Dabei handelte es sich aber um ein vollstreckungsrechtliches und nicht um ein datenschutzrechtliches Problem.

5.4 Personenstandswesen

5.4.1 Rechtmäßigkeit der Ablehnung der Akteneinsichtnahme in einen Registereintrag des Standesamtes

Im Berichtszeitraum wurde ich seitens eines Betroffenen um Prüfung gebeten, ob die Ablehnung der Akteneinsichtnahme in ein Gutachten des LKA Sachsen durch ein Standesamt ordnungsgemäß sei. Bei dem Dokument handelte es sich um ein Gutachten des Kriminalwissenschaftlichen- und -technischen Instituts des LKA Sachsen. Dieses untersucht im Rahmen der Amtshilfe für die Behörden des Freistaates Sachsen, u. a. für Standesämter, ausländische Identitätsdokumente. Als Ergebnis dieser Untersuchung wird den anfragenden Behörden ein Gutachten des LKA zur Echtheit von Urkunden und anderen Dokumenten übersandt.

Ich habe den Vorgang datenschutzrechtlich geprüft. Im Ergebnis wurde festgestellt, dass die standesamtliche (teilweise) Versagung der Einsichtnahme in die Akten, die zur Person des Betroffenen geführt werden, aus datenschutzrechtlicher Sicht unzulässig war.

In seiner Stellungnehme hatte mir das Standesamt mitgeteilt, dass die negative Bescheidung der Akteneinsichtnahme auf den Vorschriften des Personenstandsgesetzes (§§ 61, 62 PStG) und des Verwaltungsverfahrensgesetzes (§ 29 Abs. 1 und 2 VwVfG) beruhe.

Das Standesamt führte dazu aus, dass für die Einsichtnahme in einen Registereintrag sowie Auskunft aus den und Einsicht in die Sammelakte die Vorschriften der §§ 61 ff. PStG gelten würden. Dieser Vorschrift würden jedoch nicht sog. „Hilfsmittel“, wie das in Rede stehende Gutachten des LKA unterfallen, weil dieses nicht unmittelbar der Beurkundung eines Personenstandsfalles dienen würde. Es sei zu differenzieren, ob Unterlagen, die für Zwecke der Beurkundung eines Personenstandsfalles erhoben worden sind, Bestandteil der Sammelakte sind (wie z. B. die ausländische Urkunde) oder ob Unterlagen vorhanden sind, die die Echtheit der genannten Urkunde zum Gegenstand haben.

Die dargestellte Unterscheidung beruhte offenkundig auf § 48 der früheren, jetzt nicht mehr gültigen Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden. Der dort ehemals niedergelegte Grundsatz sah vor, dass Übermittlungen aus den Sammelakten nur hinsichtlich solcher Angaben und Unterlagen gestattet sind, die „für die Zwecke der Beurkundung des Personenstandsfalls“ erhoben worden sind. Diese Beschränkung lässt sich aus dem seit 2007 geltenden Personenstandsgesetz oder der Verordnung zur Ausführung des Personenstandsgesetzes vom 22. November 2008 nicht mehr ableiten. § 6 PStG lässt sich eher das Gegenteil entnehmen: Da in Sammelakten (alle) Dokumente aufbewahrt werden, die einzelne Beurkundungen in den Personenstandsregistern „betreffen“ und Einsicht in eben diese Sammelakten genommen werden kann, wird sich die Einsichtnahme auch auf alle Dokumente beziehen, die im Zusammenhang mit der einzelnen Beurkundung stehen, unabhängig davon, ob sie „zum Zwecke“ oder „aus Anlass“ in die Sammelakte gelangt sind. Für die unbeschränkte Einsichtnahme spricht auch, dass § 48 der alten Dienstanweisung weder in das neue Gesetz noch in die Ausführungsverordnung übernommen wurde. Hätte der Gesetz- bzw. Verordnungsgeber eine entsprechende Unterscheidung gewollt, wäre diese in das Gesetz, die Verordnung oder die Verwaltungsanweisungen zur Aktenführung übernommen oder neu formuliert worden.

Zur Anwendbarkeit von § 29 VwVfG führte das Standesamt aus, dass, wenn die Unterlagen der genannten Art nicht unter die Vorschriften der §§ 61 und 62 PStG fielen, § 29 VwVfG anzuwenden sei. Hilfsweise wurde ausgeführt, dass, selbst wenn die genannten Unterlagen unter die §§ 61 und 62 PStG fallen würden, § 29 Abs. 2 VwVfG ergänzend anzuwenden sei, da ansonsten eine Regelungslücke im Personenstandsgesetz entstehen würde.

Dieser Rechtsauffassung habe ich mich nicht angeschlossen. Aus den oben dargestellten Gründen geht hervor, dass alle Dokumente Bestandteil der Sammelakte sind und damit dem Einsichtnahmerecht unterfallen. Und aus § 62 Abs. 1, 2 PStG ergibt sich, dass einer Person, auf die sich der Registereintrag bezieht, auf Antrag Einsicht in die Akte zu

gewähren ist. Gesetzliche Beschränkungen des Einsichtnahmerechts sind ausschließlich in den Fällen der §§ 63, 64 PStG vorgesehen. Die Regelungen des Personenstandsgesetzes sind abschließend. Das Verwaltungsverfahrensgesetz kommt im vorliegenden Fall nicht zur Anwendung.

Etwaige Überlegungen wonach die Behörde zur Gestattung der Akteneinsicht nicht verpflichtet sein könnte, soweit das Bekanntwerden des Inhaltes der Akten dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder soweit die Vorgänge nach einem Gesetz oder ihrem Wesen nach, namentlich wegen der berechtigten Interessen der Beteiligten oder dritten Personen, geheim gehalten werden müssten, gingen vor dem Hintergrund weiterer mir mitgeteilter Informationen des LKA ins Leere. Nach Mitteilung des LKA würden schützenswerte oder geheime Informationen nicht in die Echtheits-Expertisen aufgenommen werden.

Die Verkürzung der Einsichtnahme durch das Standesamt in die Akten, die zur Person des Betroffenen geführt werden, war nach allem datenschutz- und personenstandsrechtlich unzulässig.

Nach Abschluss der Prüfung des Vorganges forderte ich das zuständige Standesamt auf, dem Betroffenen die beantragte Akteneinsichtnahme unverzüglich zu gewähren. Dies wurde mir durch die Behörde zugesichert.

5.5 Kommunale Selbstverwaltung

5.5.1 Bürgerbeschwerden in Gemeinden

Oft stelle ich fest, dass der Umgang mit Bürgerbeschwerden den Gemeinden Schwierigkeiten bereitet. Als Ursache ist nicht selten das Unvermögen der Verantwortlichen auszumachen, die Bürgerbeschwerde als eine Petition nach § 12 SächsGemO zu erkennen und entsprechend zu bearbeiten.

Durch persönliche Vorsprache beim Ordnungsamt seiner Gemeinde beschwerte sich ein Bürger über die betriebene Pferdehaltung auf seinem Nachbargrundstück. Die Gemeinde leitete die Beschwerde an das zuständige Landratsamt sowie an den Eigentümer des betreffenden Nachbargrundstücks weiter. Dem Bürger wurde eine Abgabenachricht erteilt, die lediglich den Hinweis auf die Abgabe an das Landratsamt enthielt. Die Gemeinde begründete dieses Vorgehen zunächst mit dem Verweis auf das für die Beschwerde anzuwendende Privatrecht, später mit einem Handeln nach dem Verwaltungsverfahrensgesetz. Ebenso wurden später im Fall einer an das Landratsamt gerichteten Dienstaufsichtsbeschwerde personenbezogene Daten durch die zur Stellungnahme aufgeforderte Gemeinde an eine Privatperson weitergegeben.

In dem Verfahren erkannte ich zwei Verstöße gegen § 16 Abs. 1 Nr. 1 SächsDSG, einmal in Verbindung mit § 12 SächsGemO.

Bei der beim Ordnungsamt der Gemeinde eingereichten Beschwerde handelte es sich rechtlich um eine Eingabe nach § 12 SächsGemO. Danach hat jeder Einwohner das Recht, sich einzeln oder in Gemeinschaft mit anderen in Gemeindeangelegenheiten mit Bitten oder Beschwerden (Petitionen) an die Gemeinde zu wenden. Ihm ist in angemessener Frist, spätestens nach sechs Wochen, ein begründeter Bescheid zu erteilen. Eine Petition ist jeder formlose Antrag - außerhalb formaler Rechtsmittel- und Gerichtsverfahren - etwas Bestimmtes zu tun oder zu unterlassen (vgl. Quecke/Schmid u. a., Gemeindeordnung für den Freistaat Sachsen, Kommentar, § 12 Rdnr. 1, 9). Die Gemeinde stellte bei der Prüfung des Beschwerdeinhalts der Eingabe ihre Unzuständigkeit fest. Die Weiterleitung an das zuständige Landratsamt entsprach pflichtgemäßem Handeln der unzuständigen Stelle, den Vorgang mit der entsprechenden Unterrichtung an den Einreicher abzugeben (Quecke/Schmid u. a., a. a. O. § 12 Rdnr. 24). Bei Unzuständigkeit der Gemeinde für die Belange der Eingabe ist die Eröffnung eines eigenen Verwaltungsverfahrens und damit die Feststellung der Beteiligung nach § 13 VwVfG des Eigentümers des die Beschwerde betreffenden Nachbargrundstücks mit der Pferdehaltung verwehrt. Die Übermittlung der Beschwerde an diesen war demgemäß nach § 16 Abs. 1 Nr. 1 SächsDSG unzulässig, da sie nicht zur Aufgabenerfüllung erforderlich war. Die rechtswidrige Übermittlung der Eingabe durch die Gemeinde führte darüber hinaus zur Einbeziehung eines weiteren Unbeteiligten und zu Unannehmlichkeiten in dessen sozialen Lebensbereich.

Eine Dienstaufsichtsbeschwerde ist, ähnlich der Petition, ein nichtförmlicher Rechtsbehelf zur Rüge des Verhaltens von öffentlich Bediensteten. Die Dienstaufsichtsbeschwerde veranlasst interne Ermittlungen der Dienstaufsicht, sie setzt kein Verwaltungsverfahren in Gang. Die Übermittlung des Inhalts der Dienstaufsichtsbeschwerde durch die Gemeinde und den Namen des Einreichers an eine die Dienstaufsichtsbeschwerde betreffende Privatperson war in dem mir vorliegenden Fall für die Aufgabenerfüllung - Prüfung auf Pflichtverletzung von Gemeindebediensteten - nicht erforderlich. Die Datenübermittlung war nach § 16 Abs. 1 Nr. 1 SächsDSG unzulässig. Als Folge der unzulässigen Übermittlung der Dienstaufsichtsbeschwerde an die Privatperson war der Beschwerdeführer Rechtsverfolgung ausgesetzt, die mit finanziellen Nachteilen für ihn verbunden sein konnten.

Ich habe die Gemeinde wegen der unzulässigen Übermittlungen personenbezogener Daten beanstandet. Die Gemeinde wies mir danach eine Belehrung der Bediensteten der Gemeinde und deren Verpflichtung nach § 6 SächsDSG nach. Darüber hinaus bestellte die Gemeinde einen externen behördlichen Datenschutzbeauftragten.

5.5.2 Weitergabe von Adressen von Gemeinde- und Kreisräten

Eine Kreisverwaltung fragte nach der Zulässigkeit der Weitergabe personenbezogener Daten von Kreisräten und in Ausschüssen mitarbeitenden sachkundigen Bürgern. Es bestünde Unklarheit beim Umgang mit Anfragen von Bürgern zur Erreichbarkeit der Betroffenen.

Die Weitergabe personenbezogener Daten von Gemeinde- und Kreisräten begegnet datenschutzrechtlich keinen Bedenken, soweit diese sich auf die in § 51 Abs. 1, 3 KomWO bestimmten Daten (u. a. Familiennamen, Vornamen, Geburtsjahr, Beruf oder Stand und Wohnanschrift der Gewählten) beschränken und im Zuge des Wahlverfahrens gemäß § 53 KomWO veröffentlicht wurden.

Eine spätere Weitergabe kann in diesen Fällen nach § 16 i. V. m. § 13 Abs. 2 Nr. 2 SächsDSG erfolgen, da die Daten dann als „allgemein zugängliche“ Daten im Sinne des Sächsischen Datenschutzgesetzes zu bewerten sind.

Anders verhält es sich mit personenbezogenen Daten von in Ausschüssen von Gemeinden oder des Kreistages mitarbeitenden sachkundigen Einwohnern. Diese unterliegen dem Recht auf informationelle Selbstbestimmung. Die Weitergabe ihrer Daten ist nur mit der Einwilligung der Betroffenen zulässig.

Soweit eine Gemeinde- oder Kreisverwaltung personenbezogene (dienstliche) E-Mail-Adressen für die Gemeinde- bzw. Kreisräte mit einem geschützten und sicheren Zugang einrichtet, ist diese Lösung datenschutzrechtlich zu begrüßen. Diese können der Öffentlichkeit gegenüber auch bekanntgegeben werden. Auch amtliche E-Mail-Adressen für weitere Ehrenämter, wie z. B. für sachkundige Einwohner können durch die bestellenden kommunalen Gebietskörperschaften eingerichtet werden. Bei diesen Ehrenämtern rate ich, soweit es sich nicht um Gemeinde- oder Kreisräte handelt, eine Einrichtung wegen der Häufigkeit und Dauer der Nutzung nur im Einvernehmen vorzunehmen und für eine Bekanntgabe der E-Mail-Adresse eine Einwilligung der Betroffenen einzuholen, um eventuellen Unstimmigkeiten und Missverständnissen vorzubeugen.

5.5.3 Erhebung einer Kurtaxe in der Landeshauptstadt

Nach dem sächsischen Kommunalabgabenrecht sind Kurorte, Erholungsorte und sonstige Fremdenverkehrsgemeinden befugt, für Fremdenverkehrseinrichtungen und Veranstaltungen eine Kurtaxe zu erheben. Die Landeshauptstadt Dresden beschloss eine Satzung über die Erhebung einer Kurtaxe (Kurtaxsatzung) die am 1. Februar 2014 in Kraft trat. Danach sollten alle Besucher der Stadt, die in Dresden übernachten und Einwohner

der Stadt Dresden deren erster Wohnsitz in einer anderen Gemeinde liegt, kurtaxpflichtig sein. Ausgenommen sein sollten die Stadt besuchende Personen bei privaten Übernachtungen, Verwandtenbesuchen, Krankenhausaufenthalten und Pflegeeinrichtungen sowie Kinder bis zur Volljährigkeit. Nicht kurtaxpflichtig sein sollten darüber hinaus Personen, die überwiegend beruflich veranlasst die Stadt besuchen und Personen, die erkrankungsbedingt keine Möglichkeit zur Inanspruchnahme von Einrichtungen zu Fremdenverkehrszwecken und entsprechenden Veranstaltungen haben.

Die Beherbergungsunternehmen waren nach der Satzung verpflichtet, Namen, Wohnanschrift und die Daten der An- und Abreise auf Meldescheinen einzutragen, die dann jeweils von den Gästen zu unterschreiben gewesen und für die Stadtverwaltung zur Einsichtnahme und Kontrolle zu verwahren waren. Ferner war vorgesehen, dass die Betreiber der Unterkünfte die Kurtaxe von den Gästen einziehen. Mit dem ganzen Verfahren war daher für die Beherbergungsbetriebe, aber auch für die Gäste, die Befreiungen oder Anträge auf Rückerstattung der Kurtaxe stellen wollten, ein nicht unerheblicher Aufwand verbunden, der - naturgemäß - eine umfangreiche und durchaus auch - berücksichtigt man die Gesundheitsinformationen - tiefgehende Datenverarbeitung nach sich zog.

Ein Beherbergungsunternehmen wandte sich an meine Behörde und bat um Überprüfung der Rechtmäßigkeit des Verfahrens zur Erhebung der Kurtaxe. Dem Grunde nach war das Verfahren nach der Satzung datenschutzrechtlich formal nicht zu beanstanden, auch wenn Zweifel in Hinblick auf einen gerichtsfesten Bestand der Satzung blieben. Medienberichten zufolge blieb allerdings ein nicht geringer Anteil der Rückerstattungsanträge bei der Stadt zunächst unerledigt.

Im Oktober 2014 erklärte das OVG dann in einer Entscheidung die Kurtaxsatzung der Landeshauptstadt für unwirksam. Daraufhin konnte eine Rückerstattung bezahlter Kurtaxe - datensparsam - lediglich auf der Grundlage nur eines entsprechenden Zahlungsnachweises ohne weitergehende Nachweise und Belege vorgenommen werden, da die Kurtaxsatzung der Landeshauptstadt nicht mehr als rechtliche Grundlage zur Erhebung und Verarbeitung personenbezogener Daten herangezogen werden konnte. Auch erhobene und bei der Stadt geführte Gesundheitsinformationen, die wegen ihrer erhöhten Sensibilität (vgl. § 4 Abs. 2 SächsDSG) in besonderer Weise persönlichkeitsrechtlich belasten, waren nach Wegfall der Satzung damit nicht mehr erforderlicherweise weiter zu speichern. Soweit die Landeshauptstadt vortrug, dass alle Daten - also auch die weitergehenden Gesundheitsinformationen der Rückerstattungsantragsteller - zum Ausschluss des Vorbringens von Rückzahlungsansprüchen aufzubewahren gewesen sind, war das aus meiner Sicht nicht mehr nachzuvollziehen. Und auch Kopien von Schwerbehindertenausweisen waren nach dem Urteil des OVG als unrechtmäßig erhoben und

daher nach meinem Rechtsstandpunkt zu sperren bzw. zu löschen gewesen (§ 20 Abs. 1 SächsDSG). Auch eine vorgetragene Erforderlichkeit für eine weitere Speicherung der Informationen unter Verweis auf § 3 Abs. 1 SächsKAG i. V. m. § 88 AO für eine eventuelle zukünftige Nutzung für andere abgabenrechtliche Verwaltungsverfahren überzeugte mich nicht. Eine Datensammlung auf Vorrat zu unbestimmten oder nicht bestimmbaren Zwecken ist verfassungsrechtlich prekär. Zu klären war letztlich noch, wie mit Fällen, in denen Rückerstattungsanträge bestandskräftig abgelehnt worden sind, verfahren werden sollte. Bis zum Ende des Berichtszeitraums konnten nicht mehr alle offenstehenden Fragen geklärt werden.

5.5.4 Straßenzustandserfassung mittels Kameras

Im Berichtszeitraum wandte sich der behördliche Datenschutzbeauftragte einer Stadt mit der Bitte um Beratung an meine Behörde. Die Stadtverwaltung beabsichtigte, im gesamten Stadtgebiet eine Straßenzustandserfassung durch Messfahrzeuge mit Kameras durchzuführen. Erwartungsgemäß würden bei dem Vorhaben sehr große Datenmengen anfallen. Es war daher zu klären, welche datenschutzorganisatorischen Vorkehrungen zu treffen waren.

In einer gemeinsamen Beratung mit der Stadtverwaltung wurden weitere Einzelheiten des Projekts offengelegt. Beauftragt werden sollte ein Privatunternehmen, das mit Fahrzeugen mit hochauflösenden Kameras, die auf die Straßenflächen gerichtet werden, ausgerüstet ist. Parallel sollten an den Wagen angebrachte Laserscanner zum Einsatz kommen, die die Straßenoberfläche abtasten, um die Daten dreidimensional zu erfassen. GPS-Empfänger waren für die Zuordnung der zugehörigen Koordinaten zu den erfassten Informationen vorgesehen. Die Kameraaufnahmen sollten nicht als Videoaufnahmen, sondern mit Einzelfotos erfolgen. Dennoch war die extensive Straßenzustandserfassung datenschutzrechtlich von nicht unerheblicher Bedeutung. Denn aufgrund des Umfangs des Vorhabens und der Kameraeinstellungen konnte nicht ausgeschlossen werden, dass auch in signifikanter Weise personenbezogene Daten, Einzelpersonen, Aufnahmen von Privatgrundstücken, Kfz-Kennzeichen u. v. a. miterfasst werden würden. Allerdings sollten die personenbezogenen Daten - anders als bei Google-Streetview - weder veröffentlicht noch zu anderen Zwecken als zur Straßenzustandserfassung genutzt werden. Ich bat die Stadt dennoch darum, vorsorglich die vertraglich zugesicherte Zweckbindung noch einmal gegenüber dem Auftragnehmer hervorzuheben und eine Weitergabe anfallender personenbezogener Daten durch das Unternehmen an andere Stellen mit Verweis auf die vertragliche Regelung auszuschließen sowie eine Verpflichtung auf das Datengeheimnis nach dem Bundesdatenschutzgesetz seitens des Auftragnehmers nachzufordern (vgl. § 5 BDSG).

Die Datenverarbeitung des Privatunternehmens richtete sich nach meiner Überzeugung nach dem Bundesdatenschutzgesetz. Es handelte sich nicht um eine Auftragsdatenverarbeitung für die Stadt, da die Firma die Daten für eigene Geschäftszwecke erhob, um sie in messtechnische Angaben umzusetzen (vgl. § 7 SächsDSG). Die Erhebung der Bilddaten erfolgte dabei als notwendiger technischer Zwischenschritt, um die geometrischen Verhältnisse der Straßenflächen zur Anfertigung der Messdaten vollständig zu erfassen.

Soweit der Auftragnehmer die vereinbarte Leistung erbracht haben sollte, so riet ich der Stadt, sollten bei diesem unverzüglich noch vorhandene personenbezogene Daten gelöscht werden. Sofern mit der Übergabe der Vertragsleistung verbundene personenbezogene Daten an die Stadt weitergegeben werden sollten, sei eine Nutzung seitens der Stadt für andere Zwecke als für die Straßenzustandserfassung - z. B. für Ordnungsbehörden - auszuschließen. Spätestens einen Monat nach Übergabe seien sämtliche erhaltenen personenbezogenen Daten zu löschen.

Da bereits in der Tagespresse und im städtischen Amtsblatt das Vorhaben allgemein bekannt gemacht worden war, empfahl ich, die Öffentlichkeit gesondert auf die dabei unbeabsichtigt anfallende zeitweise Verarbeitung personenbezogener Daten in einer weiteren Veröffentlichung in der Tagespresse und im Amtsblatt hinzuweisen und auch gleichzeitig über den Beginn und das Ende der Straßenzustandserfassung zu informieren. Dabei sollte erklärt werden, dass zufällig anfallende personenbezogene Daten weder von der beauftragten Firma noch von Stellen der Stadtverwaltung weitergenutzt werden und bei der Firma unmittelbar nach Übergabe des Ergebnisses der Straßenzustandserfassung, beim Straßen- und Tiefbauamt nach Prüfung der vollständigen Übergabe der vereinbarten Leistung nach dem Monat komplett gelöscht werden. Die Stadt versicherte mir entsprechend zu verfahren.

5.5.5 Rasant am Ziel vorbei

Ein Petent teilte mir mit, dass er von einer kommunalen Ordnungsbehörde eine schriftliche Verwarnung mit Verwarngeld wegen einer Geschwindigkeitsübertretung im Straßenverkehr erhalten habe. Doch weise weder die auf dem Beweisfoto abgebildete Person irgendeine Ähnlichkeit mit ihm auf, noch könne er sonst irgendeinen Bezug zu sich erkennen. Unerklärlich sei ihm auch, wie das Ordnungsamt überhaupt auf seine Person und an seine Adresse gekommen ist.

Meine Ermittlungen ergaben, dass sich die betreffende Ordnungsbehörde nicht an geltende datenschutzrechtliche Vorgaben gehalten und eine Schlüssigkeitsprüfung unterlassen hatte.

Aufgrund eines Geschwindigkeitsverstoßes, dessen „Blitzfoto“ einen offensichtlich männlichen Fahrer zeigte, wurde der Halterin des Fahrzeugs ein Zeugenfragebogen zugesandt. Auf dieses Schreiben reagierte die Halterin längere Zeit nicht. Da sie andernorts wohnte, wandte sich die Ausgangsbehörde mittels Amtshilfe an die für die Halterin örtlich zuständige Ordnungsbehörde. Deren Mitarbeiter suchten daraufhin den Wohnort der Halterin zu acht verschiedenen Terminen auf, wobei sie die Halterin niemals antrafen. Am letzten dieser Vorortttermine zeigten sie jedoch das Foto einem Nachbarn der Halterin, wobei dieser angab, dass es sich um den Sohn der Halterin handele und den Ordnungshütern den Namen und die Anschrift des Petenten nannte. Diese Informationen übermittelten die Bediensteten dann an die Ausgangsbehörde zurück, die den Petenten sodann als Beschuldigten anschrieb.

Damit verstieß die Ordnungsbehörde gegen den einschlägigen Erlass des SMI vom 18. November 1999 (Az.: 31-55/114), wonach der Fahrer in erster Linie durch Anfragen bei den Melde- bzw. Pass- und Personalausweisregisterbehörden zu ermitteln ist. Eine Nachbarschaftsbefragung darf wegen der damit verbundenen Gefahr der Diskriminierung im Nachbarschaftskreis nur als letztes Mittel angewandt werden. Die Ordnungsbehörde argumentierte nun pseudo-datenschützerisch: Eine Melderegisterauskunft würde, insbesondere bei Mehrfamilienhäusern, zu einer übermäßigen Datenerhebung führen und sei deshalb unterblieben. Das ist falsch: Abgesehen davon, dass diese Argumentation nur bei großen Mehrfamilienhäusern ansatzweise verfängt, sind verwaltungsinterne Ermittlungen, bei denen die Gefahr einer möglichen Schädigung des Rufs des Betroffenen (besonders wenn sich später herausstellt, dass die Anschuldigungen fehlerhaft oder unwahr waren) minimal ist, stets persönlichkeitsrechtsfreundlicher. Informationen zu unbeteiligten Dritten sind im Übrigen nach Abschluss der Fahrzeugführerfeststellung zu vernichten, da sie zur Aufgabenerfüllung nicht mehr erforderlich sind (vgl. § 20 Abs. 2 Nr. 2 SächsDSG). Damit ist ein „übermäßiger Eingriff in die Rechte unbeteiligter Dritter“ per se ausgeschlossen.

Im konkreten Fall waren die beim auskunftsfreudigen Nachbarn erhobenen Angaben wohl zudem noch völlig unschlüssig. Denn die Geburtsjahre der Betroffenen (Halterin und Petent) schlossen mit absoluter Sicherheit aus, dass es sich um ein Mutter-Sohn Verwandtschaftsverhältnis hätte handeln können. Der Ordnungsbehörde war dies egal: Sie sah darüber hinweg und ermittelte eifrig gegen den Petenten.

Ich habe die beteiligten Behörden gerügt und aufgefordert, sich zukünftig an die geltenden Vorschriften zu halten.

5.6 Baurecht; Wohnungswesen

In diesem Jahr nicht belegt.

5.7 Statistikwesen

5.7.1 Die Beteiligung des Sächsischen Datenschutzbeauftragten bei Erlass von Statistiken gemäß § 8 Abs. 3 SächsStatG

Nach § 8 SächsStatG können Gemeinden zur Wahrnehmung ihrer Aufgaben Kommunalstatistiken durchführen. Sie werden ermächtigt, Kommunalstatistiken durch Satzung anzuordnen. Dies gilt für Landkreise und sonstige kommunale Körperschaften entsprechend.

Bei der Vorbereitung der Satzung ist neben dem Statistischen Landesamt auch der Sächsische Datenschutzbeauftragte - zwingend - zu beteiligen.

Aus gegebenem Anlass darf ich in diesem Zusammenhang darauf hinweisen, dass eine Beteiligung der dort genannten Stellen nach dem eindeutigen Wortlaut des Absatzes 3 der Vorschrift bereits bei der *Vorbereitung* der Satzung, also mithin im Stadium des Satzungsentwurfs, und nicht erst bei der Durchführung der auf der verabschiedeten Satzung sodann durchgeführten Primärbefragungen zu erfolgen hat (zur Art und Weise der Beteiligung siehe bereits die Ausführungen in 5/5.7.4).

Ich bitte, die für den Satzungserlass zuständigen Mitarbeiter ggf. nochmals ausdrücklich auf dieses Beteiligungsrecht hinzuweisen, damit in Zukunft die Einbindung meiner Behörde tatsächlich rechtzeitig erfolgt.

5.7.2 Löschung von Datenbeständen mit Hilfsmerkmalen beim Zensus 2011

Ich bin von einem Kollegen davon in Kenntnis gesetzt worden, dass im Hinblick auf laufende Gerichtsverfahren zur Klärung der kommunalen Einwohnerzahlen dort von der Fortführung der Löschung der vorhandenen Hilfsmerkmale seitens des dortigen Statistischen Landesamtes abgesehen worden war, zumindest bis eine gerichtliche Entscheidung des zuständigen Verwaltungsgerichts über die Vorlage der Daten vorliegt. Zu dieser Problematik gab es wohl auch bereits im April 2014 eine Diskussion innerhalb der Statistischen Ämter des Bundes und der Länder sowie deren Dienstaufsichten.

Entsprechende Anfragen seitens sächsischer Verwaltungsgerichte zur Bereitstellung einwohnerrelevanter Daten an das Statistische Landesamt in Sachsen gab es nach dessen Auskunft vom November 2014 nicht, sodass alle Daten mit Personenbezug entsprechend den gesetzlichen Vorgaben des § 19 ZensG 2011 gelöscht worden sind: Nach

Auffassung des Statistischen Landesamtes war die Überprüfung der Erhebungs- und Hilfsmerkmale auf ihre Schlüssigkeit und Vollständigkeit spätestens Ende März 2014 abgeschlossen, sodass dann keine Rechtsgrundlage mehr für ein weiteres Vorhalten der Daten bestand.

5.8 Archivwesen

5.8.1 Anbietung von Sozialdaten an das Archiv nur unter Beachtung der maßgeblichen Schutzfristen

Mit der Frage, ob nach sächsischem Recht auch Akten, die dem Sozialgeheimnis nach § 35 SGB I unterliegen, dem zuständigen Archiv angeboten werden dürfen, hat sich ein behördlicher Datenschutzbeauftragter an mich gewandt.

Zur Rechtslage:

§ 71 Abs. 1 Satz 3 SGB X stellt klar, dass auch Sozialakten dem Archiv anzubieten sind bzw. von der Archivbehörde übernommen werden dürfen. Insoweit regelt § 5 Abs. 2 SächsArchivG, dass (soweit Bundes- oder Landesrecht nichts anderes bestimmt) sich die Anbietungspflicht auch auf Unterlagen erstreckt, die dem Datenschutz oder dem Geheimschutz unterliegen (siehe § 2 Abs. 4 BArchG), sowie auf Unterlagen, die personenbezogene Daten enthalten, welche nach Bundes- oder Landesrecht gesperrt, gelöscht oder vernichtet werden müssten oder könnten (vgl. § 84 Abs. 6 SGB X).

Die archivrechtliche Abgabepflicht geht also auch für Unterlagen nach § 35 SGB I der Löschung dieser Akten vor (so Rombach in Hauck/Noftz, § 71 Rdnr. 61). Für die besonderen Sozialdaten des § 76 SGB X ist § 76 Abs. 2 Nr. 2 Alternative 3 SGB X zu beachten.

Die Übermittlungsbefugnis für die Durchführung der Anbietung von Sozialdaten setzt allerdings nach § 71 Abs. 1 Satz 3 SGB X voraus, dass die in § 5 BArchG bzw. die in den jeweiligen Landesarchivgesetzen entsprechend (!) geregelten *Schutzfristen* nicht unterschritten werden.

Die Schutzfristen nach § 5 BArchG und § 10 SächsArchivG:

§ 5 BArchG regelt in seinem Absatz 3, dass Unterlagen nach § 35 SGB I erst 60 Jahre nach Entstehen benutzt werden dürfen. Nach Absatz 5 der Vorschrift kann diese Frist um höchstens 30 Jahre verlängert werden, soweit dies im öffentlichen Interesse liegt. Eine Verkürzung von Schutzfristen auf Einwilligungsgrundlage in Bezug auf Sozialdaten ist indes in § 5 BArchG nicht vorgesehen.

§ 10 Abs. 1 Satz 3 SächsArchivG sieht vor, dass für Archivgut, das Rechtsvorschriften des Bundes über die Geheimhaltung unterliegt, die Schutzfristen des § 5 BArchG entsprechend gelten. Mit dieser Regelung findet sich der Verweis auf die Anwendung des § 5 BArchG und den dort genannten Schutzfristen für Archivgut nach § 35 SGB I. Ein gleiches Schutzniveau wegen Gleichlaut der Schutzfristen wäre somit gegeben.

Nicht eindeutig geklärt ist damit allerdings, ob § 10 Abs. *4* SächsArchivG auf Sozialdatenarchivgut keine Anwendung mehr findet. Dies ist insoweit fraglich, als § 10 Abs. 4 SächsArchivG *pauschal* auf den gesamten § 10 Abs. 1 SächsArchivG verweist, sodass fraglich ist, ob auch im Bereich des sozialdatenschutzrechtlichen Archivguts eine Lockerung der Schutzfristen per *Einwilligung* - wie es nach § 10 Abs. 4 SächsArchivG ausdrücklich erlaubt ist - möglich wäre, eine Lockerung, die allerdings, wie bereits erwähnt, § 5 BArchG für Sozialakten gerade *nicht* vorsieht, womit folglich das Sächsische Archivgesetz hinter dem Schutzniveau des § 5 BArchG zurückbliebe und eine Übermittlung von Sozialdatenakten an das Archiv damit also wiederum ausgeschlossen wäre.

Zu der letztlich entscheidungserheblichen Frage des Verhältnisses von § 10 Abs. 1 Satz 3 zu § 10 Abs. 4 SächsArchivG bat ich das SMI um Stellungnahme. Das Ministerium teilte mir mit, dass nach seiner Auffassung § 10 Abs. 1 Satz 3 SächsArchivG die maßgebliche Vorschrift sei und § 10 Abs. 4 SächsArchivG insoweit nicht zur Anwendung komme. Mit dieser Auslegung findet sich der Verweis auf die Anwendung des § 5 BArchG und den dort genannten Schutzfristen für Archivgut, das dem § 35 SGB I unterliegt. Ein gleiches Schutzniveau wegen Gleichlaut der Schutzfristen ist somit nach Auffassung des SMI gegeben und folglich eine Anbietung von Unterlagen, die § 35 SGB I unterliegen, an das zuständige Archiv zulässig.

Ich habe dieses Ergebnis dem anfragenden Datenschutzbeauftragten so mitgeteilt. Allerdings werde ich bei der nächsten Änderung des Sächsischen Archivgesetzes im Rahmen des Gesetzgebungsverfahrens auf eine normenklare Bereinigung der Vorschrift drängen.

5.9 Polizei

5.9.1 Neuregelung der Bestandsdatenauskunft im Polizeigesetz des Freistaates Sachsen

Am 24. Januar 2012 hatte das Bundesverfassungsgericht (Az.: 1 BvR 1299/05) erkannt, dass die in § 113 Abs. 1 Satz 2 TKG geregelten Pflichten der Telekommunikationsdiensteanbieter (TK-Diensteanbieter) zur Herausgabe von Zugangssicherungscodes (z. B. Passwörter, PIN’s etc.) an Ermittlungsbehörden und andere öffentliche Stellen nicht mit dem Grundrecht auf informationelle Selbstbestimmung vereinbar waren. Ge-

rügt wurde vor allem, dass die einschlägigen Vorschriften nicht verhältnismäßig und zu weitreichend ausgestaltet waren. Dadurch war nicht sichergestellt, dass die Zugangscodes nur dann verlangt werden dürfen, wenn die gesetzlichen Voraussetzungen dafür vorliegen. Die entsprechenden Regelungen durften deshalb nur noch bis spätestens zum 30. Juni 2013 angewendet werden. Des Weiteren erkannte das Gericht, dass § 113 TKG nicht auf dynamische IP-Adressen anwendbar war, da das Bestimmen des Anschlussinhabers zu einem Eingriff in das Fernmeldegeheimnis führte. Der in der Vergangenheit üblichen Gesetzesauslegung des § 113 TKG durch die Strafverfolgungsbehörden und der darauf beruhenden Verfolgung von Urheberrechtsverstößen seitens der Musik- und Filmindustrie wurde damit ein Riegel vorgeschoben.

Der Bundesgesetzgeber beschloss daraufhin am 21. März 2013 das „Gesetz zur Änderung des Telekommunikationsgesetzes und zur Neuregelung der Bestandsdatenauskunft“ (BGBl I S. 1602), mit dem u. a. ein Richtervorbehalt bei Abfragen von Zugangssicherungscodes durch Bundesbehörden (§ 100j Abs. 3 StPO) sowie Benachrichtigungspflichten im Anschluss an Auskunftsverfahren (§ 100j Abs. 4 StPO) eingeführt worden sind. Das Gesetz trat am 1. Juli 2013 in Kraft.

In Sachsen bestand nach der Entscheidung des Gerichts ebenfalls Anpassungsbedarf am Polizeigesetz, am Verfassungsschutzgesetz und am Versammlungsgesetz. In die Entwürfe der Änderungsvorschriften wurde ich frühzeitig eingebunden. Meine Anregungen wurden dabei meist aufgegriffen.

So wurde u. a. § 42 SächsPolG neu gefasst (SächsGVBl. 2013, S. 890). Die Vorschrift regelt nunmehr unter Bezugnahme auf den geänderten § 113 TKG, unter welchen Voraussetzungen der TK-Diensteanbieter eine Auskunft zu erteilen hat. Für Zugangscodes/-daten wurde dabei zur Voraussetzung gemacht, dass die zugehörigen Endgeräte der Beschlagnahme unterliegen müssen. Für die polizeiliche Tätigkeit wurde die Anfrage unter einen allgemeinen Richtervorbehalt gestellt (§ 42 Abs. 4 SächsPolG). Auch wurde eine Benachrichtigungspflicht beschlossen (§ 42 Abs. 5 SächsPolG). Die Gesetzesänderungen traten am 31. Dezember 2013 in Kraft.

Ich werde kontrollieren, wie die Vorschriften in der Praxis umgesetzt werden.

5.9.2 Die automatisierte Kennzeichenerfassung in Sachsen

Im Berichtszeitraum habe ich mir u. a. die durch die sächsische Polizei eingesetzten automatisierten Kennzeichenerfassungssysteme (AKES) praktisch vorführen lassen. Für die kompetente Vorführung und freundliche Aufnahme danke ich den beteiligten Polizeibediensteten.

Rechtsgrundlage für die automatisierte Kennzeichenerfassung im Freistaat Sachsen ist § 19a SächsPolG. Diese Vorschrift wurde 2011 im Rahmen des „Gesetzes zur Änderung des Polizeigesetzes des Freistaates Sachsen und anderer Gesetze“ in das Polizeigesetz eingefügt und trat am 4. Oktober 2011 in Kraft (SächsGVBl. 2011 S. 370). Im Gesetzgebungsverfahren hatte ich Bedenken unter anderem gegen die Gesetzgebungskompetenz des Freistaats Sachsen, die ich mit Blick auf die Teile der Vorschrift, die m. E. nicht auf Gefahrenabwehr, sondern auf Strafverfolgung zielen, beim Bund sah, geäußert. Damit ist insbesondere § 19a Abs. 1 Satz 1 Nr. 2 SächsPolG gemeint, wonach einer der Zwecke der automatisierten Kennzeichenerfassung die Sicherstellung gestohlener oder sonst abhanden gekommener Kraftfahrzeuge oder Kraftfahrzeugkennzeichen sein soll. Die Fahndung ist jedoch dem strafrechtlichen Ermittlungsverfahren und damit der konkurrierenden Gesetzgebungskompetenz des Bundes nach Art. 74 Abs. 1 Nr. 1 GG zuzuordnen, von welcher der Bundesgesetzgeber abschließend Gebrauch gemacht hat. Weiterhin hatte ich unter Heranziehung der Zahlen aus Hessen, welche eine Trefferquote von lediglich 0,03% auswiesen, Zweifel an der Geeignetheit automatisierter Kennzeichenerfassung geäußert. Und ich hielt den Teil, der die Maßnahme in einem 30 Kilometer breiten Grenzstreifen entlang der Außengrenzen des Freistaates Sachsen erlaubt und damit sämtliche wesentlichen Fernstraßen - insbesondere die von Chemnitz nach Görlitz parallel zur Grenze verlaufende Autobahn A4 - und Städte flächendeckend erfasst, nicht für vereinbar mit den vom BVerfG in seiner Entscheidung vom 11. März 2008 (Az.: 1 BvR 2074/06 und 1 BvR 1254/07) gesetzten Voraussetzungen, dass es keine „flächendeckende“ Überwachung geben darf. Trotz der - auch von anderen Sachverständigen geäußerten - Bedenken wurde das Gesetz nur unwesentlich verändert beschlossen.

Im März 2013 ließ ich mir daraufhin im Fortbildungszentrum der Polizei in Bautzen das in Sachsen verwendete System praktisch vorführen. Es besteht im Wesentlichen aus einer Kameraeinheit, welche bis zu drei Fahrspuren gleichzeitig erfassen kann, und einer Auswerteeinheit. Bei der Verfahrensbeschreibung wurde mir erklärt, dass die Geräte vor allem ein Fahndungshilfsmittel seien. Auf dem Bildschirm der Auswerteeinheit seien die Umrisse der durch die Kamera aufgenommenen Kraftfahrzeuge sichtbar. Dabei würden die gelesenen Kennzeichen mit dem zur Verfügung stehenden Fahndungsbestand abgeglichen und im Trefferfall akustisch und optisch angezeigt. Zum Abruf der Vergleichsdaten (aus INPOL und dem Schengener Informationssystem) und Einspeisung in das Gerät seien nur bestimmte Mitarbeiter der Polizeidirektion berechtigt. Diese Dateien stelle der SID zur Verfügung. Aufgezeichnet würden im Trefferfall allerdings nur das Kfz-Kennzeichen sowie der Ort und die Zeit der Aufnahme. Die Treffer würden auf der Dienststelle aus dem Gerät gelesen. Im Freistaat seien ab dem 15. Februar 2013 landesweit fünf Geräte im Einsatz, je ein Gerät pro Polizeidirektion. Im Nichttrefferfall

würden die Aufnahme sowie das ausgelesene Kennzeichen nur kurzzeitig angezeigt und anschließend sofort gelöscht und stünden damit nicht mehr zur Verfügung. Im Trefferfall würden die Daten für ein eventuell folgendes Gerichtsverfahren eigens ausgelesen und als PDF-Datei gespeichert.

Das System wurde mir zunächst im Schulungsraum und nachfolgend auf dem Gelände vorgeführt. Hierzu fuhren zwei Kraftfahrzeuge der Polizei, deren Kennzeichen vorher manuell in das System eingegeben worden waren, an den aufgestellten Kameras vorbei. Zwei unterschiedliche Kameras, eine mittels Stativ, die andere am Fahrzeug angebracht, kamen zum Einsatz. Trotz guter Lichtverhältnisse wurden die Kennzeichen in weniger als 40% der Fahrten als Trefferfälle erkannt. Man erklärte hierzu, dass der hier eingesetzte Rechner bereits als „problembehaftet“ bekannt sei und alle ordnungsgemäß funktionierenden Geräte aktuell in den Polizeidirektionen im Einsatz seien. So habe etwa das Gerät der Polizeidirektion Görlitz in einem Einsatz zuverlässig funktioniert und vier Treffer angezeigt.

Am 30. Oktober 2013 veröffentlichte das SMI zudem statistische Informationen über den Zeitraum zwischen dem 15. Februar und 29. August 2013. Die AKES-Geräte seien auf den BAB 4, 9, 14 und 72 sowie auf den Bundesstraßen 2, 87 und 95 wie folgt zum Einsatz gekommen:

Anzahl	Ort	**Monat des Jahres 2014**	**Anzahl je Monat**	**Einsatzstunden**	**Grund der Maßnahme § 19a Abs. l Satz 1 Nr. … SächsPolG**
68	BAB 4	Februar	5	130	2, 3, 5
		März	15	361	2, 3, 5
		April	14	281	2, 3, 5
		Mai	9	197	2, 3, 5
		Juni	17	378	2, 3, 5
		Juli	8	162	2, 3, 5
6	BAB 72	April	1	3,5	5
		Mai	3	11	5
		Juni	1	4	5
	BAB 9, BAB 14, B 2, B 87, B 95	April	8	11,25	2, 3, 5
		Mai	2	3	2, 3, 5

Wie viele Kfz dabei gescannt wurden, sei statistisch nicht erfasst worden. Insgesamt sei es zu 464 Treffermeldungen gekommen, wovon 72 „Echttreffer“ gewesen seien. System- bzw. umweltbedingt, beispielsweise aufgrund schlechter Lichtverhältnisse oder

verschmutzter Kennzeichentafeln, könne die von der Kamerakomponente erkannte Zeichenkette von der auf der Kennzeichentafel tatsächlich befindlichen abweichen und demzufolge zu Scheintreffern führen. Weitere Scheintreffer könnten z. B. entstehen, wenn nur die Kennzeichentafel selbst (wegen Verlusts) zur Fahndung ausgeschrieben worden sei. In diesem Fall löse die noch am Fahrzeug befindliche zweite Kennzeichentafel eine Treffermeldung aus. Die 72 „Echttreffer“ unterteilten sich wie folgt: 31 Verstöße gegen das Pflichtversicherungsgesetz, drei Unterschlagungen von Kfz, 27 Diebstähle von Kfz, fünf Diebstähle von Kennzeichen, vier Diebstähle/Tankbetrug, zwei Feststellungen vermisster Personen. Bei diesen 72 Echttreffern seien alle Kfz angehalten und die Identität der Insassen festgestellt worden.

Die nach dem Besuch des Fortbildungszentrums veranlasste Prüfung der übergebenen Unterlagen (IuK-Sicherheitskonzept vom 7. Februar 2013; Technisches Betriebskonzept; CatchKen Handbuch für die Polizei Sachsen vom 20. Februar 2013) ist noch nicht abgeschlossen. Gleiches gilt für die Errichtungsanordnung zum IT-Verfahren „Mobiles automatisiertes Kennzeichenerfassungssystem - AKES“ (Neufassung: Februar 2015). Daher steht die abschließende Bewertung der technisch-organisatorischen Ausgestaltung des Systems nach § 9 SächsDSG noch aus.

An meinen grundsätzlichen Bedenken gegen den Einsatz von automatisierten Kennzeichenerfassungsgeräten hat sich dagegen bis heute nichts geändert. Dies habe ich auch dem BVerfG, das mich im Berichtszeitraum um eine Stellungnahme zu drei anhängigen Verfassungsbeschwerden gegen die automatisierte Kennzeichenerfassung in den Ländern Hessen, Bayern und Baden-Württemberg gebeten hat, mitgeteilt.

5.9.3 Einsatz von Kameras bei friedlichen Veranstaltungen

Die rechtlichen Bedingungen des Einsatzes von Kameras bei Demonstrationen und anderen öffentlichen Veranstaltungen habe ich bereits in 15/5.9.6 beschrieben. Im Nachgang zu einer am 13. Februar 2014 in Dresden stattgefundenen angemeldeten Demonstration trat ein Bürger an mich heran, weil er Persönlichkeitsrechte der Teilnehmer verletzt sah. Er hatte einen Polizeibeamten beobachtet, wie er bei einer friedlich verlaufenden Demonstration eine Handkamera mit Stativ auf die Teilnehmer richtete. Da er keinen plausiblen Grund für das Anfertigen von Videoaufnahmen feststellen konnte, fragte er bei einem in der Nähe stehenden Beamten des Kommunikationsdienstes nach, erhielt aber nur unzureichende Auskunft. Ich schrieb daraufhin den Präsidenten der Polizeidirektion Dresden an, um den Sachverhalt aufzuklären. Gleichzeitig äußerte ich die Bitte, die Beamten besser zu schulen. Er antwortete mir, dass das Geschehen durch die vorliegenden Angaben nicht konkret zuordenbar sei, es aber auch zu keiner Aufzeichnung von Videomaterial gekommen sei. Des Weiteren teilte er mir mit, dass er den Einsatz

von Aufzeichnungstechnik im Rahmen friedlicher Versammlungs- und Veranstaltungslagen explizit untersagt habe. Auch die Anregung, die Kommunikationsteams für Auskunftsersuchen der Teilnehmer besser zu schulen, wurde aufgenommen.

Für diese Klarstellungen und die weiteren Maßnahmen danke ich. Ich gehe davon aus, dass künftig mitgeführte Kameras im Rahmen friedlicher Veranstaltungen nicht mehr auf die Teilnehmer gerichtet werden.

5.9.4 Neue gesetzliche Regelung zu Bild- und Tonaufnahmen bei Versammlungen und sonstigen Veranstaltungen

Mit dem Gesetz zur Änderung des Polizeigesetzes des Freistaates Sachsen, zur Änderung des Sächsischen Verfassungsschutzgesetzes und zur Änderung des Sächsischen Versammlungsgesetzes sowie zur Änderung weiterer Gesetze vom 17. Dezember 2013 hat der Sächsische Landtag die Bestimmungen für Bild- und Tonaufnahmen bei Versammlungen nach dem Versammlungsgesetz sowie bei öffentlichen Veranstaltungen und Ansammlungen, die nicht dem Versammlungsgesetz unterfallen, neu geregelt bzw. ergänzt.

Über dieses Gesetzgebungsverfahren wurde ich frühzeitig informiert und hatte mehrfach Gelegenheit zu Anmerkungen und Stellungnahmen.

Die Änderungen stellen u. a. klar, dass die Polizei Bild- und Tonaufnahmen von Teilnehmern bei oder im Zusammenhang mit öffentlichen Versammlungen nur offen und nur dann anfertigen darf, wenn die anderen, bereits in früheren Fassungen des § 12 SächsVersG enthaltenen Voraussetzungen vorliegen. Eine verdeckte, heimliche Anfertigung von Aufnahmen ist nach den Vorschriften des Versammlungsgesetzes damit unzulässig. Dies gilt für öffentliche Versammlungen in Räumen ebenso wie für öffentliche Versammlungen unter freiem Himmel und Aufzüge.

Zu begrüßen ist auch die Straffung von § 12 Abs. 2 SächsVersG, wonach nun Bildaufnahmen nach Beendigung der öffentlichen Versammlung oder zeitlich und sachlich damit unmittelbar im Zusammenhang stehender Ereignisse nur noch aufbewahrt werden dürfen, soweit sie für die Verfolgung von Straftaten von Teilnehmern benötigt werden. Die früher mögliche Aufbewahrung zur Gefahrenabwehr wurde - auch mangels Relevanz in der Praxis - gestrichen.

Übersichtsaufnahmen von öffentlichen Versammlungen unter freiem Himmel und Aufzügen dürfen nach dem neu eingefügten § 20 Abs. 2 SächsVersG nur offen und nur dann angefertigt werden, wenn und soweit dies wegen der Größe der Versammlung

oder Unübersichtlichkeit der Versammlungslage zur Lenkung und Leitung eines Polizeieinsatzes im Einzelfall erforderlich ist. Zu begrüßen ist die Klarstellung im Gesetzestext, dass eine Identifikation von Personen oder Aufzeichnung der Übertragung bei Übersichtsaufnahmen nicht stattfindet.

Datenschutzrechtliche Prüfvorgänge zeigten mir, dass die Dienststellen der sächsischen Polizei in Bezug auf Bild- und Tonaufnahmen bei öffentlichen Versammlungen verantwortungsvoll handeln und das Bewusstsein, dass das Versammlungsgrundrecht des Art. 8 GG von zentraler Bedeutung für die demokratische Teilhabe an Willensbildungsprozessen ist, ausgeprägt ist. Erwähnenswerte Vorfälle, bei denen durchgreifende Bedenken gegen Bildaufnahmen einzelner Situationen bei öffentlichen Versammlungen bestanden hätten, gab es im Berichtszeitraum nicht. Unsicherheiten - auf Seiten der Polizei wie auch seitens der Petenten - waren allenfalls bei der Frage festzustellen, ob und wie Bildaufnahmetechnik durch Beamte mitgeführt und bereitgehalten werden darf, ohne dass bei den Versammlungsteilnehmern der Eindruck entstehen muss, dass bereits Aufnahmen gefertigt werden (vgl. auch Beitrag 5.9.3). Auf die Bitte einer Polizeidirektion habe ich meine Bereitschaft erklärt, für Erläuterungen und Gespräche zu diesem Punkt zur Verfügung zu stehen.

5.9.5 Nutzung von Facebook durch die Polizei zur Nachwuchswerbung, Öffentlichkeitsarbeit und Öffentlichkeitsfahndung

Im Herbst 2013 trat das SMI - Landespolizeipräsidium - mit der Bitte an mich heran, zu prüfen, ob und ggf. inwieweit die Nutzung von *social networks* (deutsch unzutreffend, aber verbreitet übersetzt mit „sozialen Netzwerken“) durch die Polizei datenschutzrechtlichen Bedenken begegnet. Das SMI teilte mir mit, dass es - dem politischen Willen zur gezielten Nutzung solcher Kommunikationsformen entsprechend - eine Plattform bei Facebook für die Nachwuchswerbung und Öffentlichkeitsarbeit, aber auch zur Öffentlichkeitsfahndung, errichten und nutzen wolle. Die Nutzung von Facebook sei insbesondere deshalb von Interesse, weil dadurch Personengruppen erreicht werden könnten, für die die klassischen Medien eine nur noch untergeordnete oder gar keine Rolle mehr spielen.

Ich habe dem SMI meine grundsätzlichen Bedenken gegen Facebook dargelegt und in der Folgezeit dazu beizutragen versucht, dass eine eventuelle Facebook-Nutzung so datenschutzfreundlich wie möglich gestaltet wird.

I. Grundsätzliche Bedenken gegen den Kooperationspartner Facebook

Facebook ist ein soziales Netzwerk, das von der Facebook Inc. mit Sitz in Menlo Park (Kalifornien/USA) betrieben wird. Vertragspartner der europäischen Nutzer ist dagegen die Facebook Ltd. in Irland, eine Tochter des erstgenannten Unternehmens. Aufgrund dieser Konstruktion können deutsche Datenschutzaufsichtsbehörden Facebook nicht wirksam kontrollieren. Für die Facebook Ltd. gilt das sehr unternehmensfreundliche irische Datenschutzrecht, welches der Aufsicht der eher schwachen irischen Datenschutzbehörde unterliegt.

Facebook wird aufgrund seines Geschäftsmodells „Daten als Ware“ zu der Gruppe der „Datenschutzignoranten“ gezählt. Das Unternehmen missachtet derart massiv deutsche datenschutz- und telemedienrechtliche Bestimmungen, dass die Aufzählung der einzelnen Verstöße kaum übersichtlich dargestellt werden kann. Hier nur eine kleine Auswahl: Notwendige Einwilligungen bei der Datenübermittlung ins Nicht-EU-Ausland oder bei dem Setzen von Cookies (§ 4c Abs. 1 Nr. 1 BDSG, Art. 5 Abs. 3 E-Privacy-Richtlinie) werden nicht eingeholt oder genügen nicht den Anforderungen nach § 4a BDSG, § 13 Abs. 2, 3 TMG. Die Rechte der Betroffenen auf Auskunft, Berichtigung, Sperrung oder Löschung ihrer Daten werden teilweise völlig, jedenfalls aber weitgehend verweigert und unangemessen behindert (§ 35 Abs. 2 BDSG, §§ 5, 6, 13 Abs. 1 TMG). Facebook verstößt des Weiteren auch außerhalb datenschutzspezifischer Normen gegen deutsches Recht. Die allgemeinen Geschäftsbedingungen enthalten mehrfach überraschende, verbraucherschädigende und aus sonstigen Gründen unwirksame Klauseln nach den §§ 305 ff. BGB. Auch der Minderjährigenschutz nach den §§ 106 ff. BGB findet keine Berücksichtigung.

II. Die Nutzung sozialer Netzwerke zu Strafverfolgungszwecken sowie zur Öffentlichkeitsfahndung

Die Öffentlichkeitsfahndung zu Strafverfolgungszwecken ist in den §§ 130 ff. StPO eigens geregelt. Diese Vorschriften kommen grundsätzlich auch als Rechtsgrundlage für Öffentlichkeitsfahndungen im Internet in Betracht, wenn diese auch mit Blick auf den Verhältnismäßigkeitsgrundsatz nur eingeschränkt zur Anwendung kommen können. Ausschreibungen zur Öffentlichkeitsfahndung zwecks der Aufenthaltsermittlung eines Beschuldigten oder eines Zeugen sind bereits gemäß § 131a Abs. 3 StPO auf Straftaten von erheblicher Bedeutung (entsprechend § 98a Abs. 1 StPO) beschränkt; zudem muss der Beschuldigte dringend tatverdächtig sein und die Aufenthaltsermittlung auf andere Weise erheblich weniger Erfolg versprechend oder wesentlich erschwert sein.

Mit Blick auf die gesondert zu berücksichtigende Verhältnismäßigkeit ist die Öffentlichkeitsfahndung im Internet mithin nur bei besonders schwerwiegenden Straftaten in Betracht zu ziehen. Ich habe das SMI darauf hingewiesen, dass die Erforderlichkeit in jedem Einzelfall streng zu prüfen ist und Art, Umfang und Dauer auf das dann noch rechtlich zulässige Maß zu beschränken sind. Zusätzlich muss Anlage B RiStBV, wonach Fahndungsaufrufe auf speziellen Seiten - etwa der Polizei - zu bündeln sind, beachtet werden. Vor diesem Hintergrund und auch aufgrund der Gefahr der unkontrollierten Weitergabe von Daten sollte die Bereitstellung von Daten mit Personenbezug daher ausschließlich auf polizeieigenen Servern erfolgen. Auch muss u. a. die Weitergabe sowie der automatisierte Abruf von personenbezogenen Daten aus dem Internet durch „Web-Crawler“ etc. verhindert werden. Schließlich müssen sachdienliche Hinweise ausschließlich außerhalb der durch das soziale Netzwerk vorgegebenen Kommunikationsstrukturen entgegengenommen werden. Da eine Kommentierung auf Facebook technisch nicht vermieden werden kann, diese in rechtlicher Hinsicht allerdings höchst bedenklich ist, sind die Kommentierungen auf der Facebook-Seite der Polizei ständig zu beobachten und ggf. zu löschen. Auf der außerhalb von Facebook gelegenen Fahndungswebseite der Polizei muss zudem darauf hingewiesen werden, dass eine Verbreitung des Links, aber keine Kommentierung desselben gewünscht ist.

Was eventuell gewünschte verdeckte Ermittlungen innerhalb von Facebook angeht, habe ich darauf hingewiesen, dass mir keine Rechtsgrundlage, die dies erlauben würde, ersichtlich ist.

III. Öffentlichkeitsarbeit

Im Hinblick auf die Nutzung von Facebook zur Öffentlichkeitsarbeit wies ich auf die Geltung des Kunsturhebergesetzes und die Notwendigkeit der Einwilligung von in Porträtaufnahmen abgebildeten Personen hin.

IV. Umsetzung durch das SMI

Meine Hinweise sind vom SMI offen aufgenommen worden. Das SMI hat mir im Februar 2015 ein weitgehend abgeschlossenes Konzept zur Nutzung von sozialen Netzwerken auch zur Öffentlichkeitsfahndung vorgelegt. Das Konzept entsprach hinsichtlich der Verlinkung auf polizeieigene Server und der Vermeidung von Kommunikation auf Facebook weitgehend meinen Forderungen. Die Einbindung erfolgt in technischer Hinsicht derart, dass lediglich ein Hinweis mit kurzer Beschreibung des Sachverhalts enthalten ist und mittels angefügtem Link eine Weiterleitung auf die polizeieigene Seite erfolgt.

Im Februar 2015 unterrichtete mich das SMI erneut über den Stand seiner Vorbereitungen. Im Hinblick auf die Öffentlichkeitsfahndung warte man noch auf die anstehende Änderung der Richtlinien für das Straf- und Bußgeldverfahren. Sobald diese erfolgt seien, werde man mir erneut Gelegenheit zur Stellungnahme geben. Dahingegen soll der Wirkbetrieb hinsichtlich der Öffentlichkeitsarbeit bereits zuvor aufgenommen werden.

V. Resümee

Vorerst abschließend darf ich feststellen, dass das SMI einen wachen Blick für die Gefahren, die dem Persönlichkeitsrecht aus einer Facebook-Nutzung drohen, hat. Es ist meinen Anregungen - Verlinkung auf polizeieigene Server, keine Kommunikation auf Facebook - gefolgt. Dafür danke ich ihm ausdrücklich.

Derzeit sind jedoch weder alle rechtlichen noch die tatsächlichen Grundlagen für die Facebook-Nutzung durch die sächsische Polizei abgeschlossen. Ich werde dieses Vorhaben, insbesondere seine dann konkrete praktische Durchführung, daher weiter beobachten und begleiten.

5.9.6 Unverschlüsselte E-Mail-Kommunikation der Polizei mit Dritten

Im Berichtszeitraum hatte ich mich wiederholt mit der Frage zu beschäftigen, ob und ggf. unter welchen Voraussetzungen die Polizei unverschlüsselte E-Mails an Dritte, d. h. Private, Kommunen etc., versenden darf.

Ein Fall wurde mir von einem betrieblichen Datenschutzbeauftragten aus einem anderen Bundesland berichtet. Danach hatte sein Unternehmen von einer sächsischen Polizeidirektion in einem Ermittlungsverfahren eine unverschlüsselte und auch nicht elektronisch signierte E-Mail erhalten. Diese E-Mail habe neben Angaben zum Tatvorwurf auch personenbezogene Daten (Name, Geburtsdatum) enthalten. Meine anschließenden Ermittlungen haben diesen Sachverhalt bestätigt.

Der betroffenen Polizeidirektion habe ich daraufhin Folgendes mitgeteilt: Personenbezogene Daten dürfen per E-Mail an Personen oder Stellen außerhalb des sächsischen Polizeidatennetzes oder des SVN wenn überhaupt nur verschlüsselt übermittelt werden. Dies ergibt sich seit dem Inkrafttreten des Sächsischen E-Government-Gesetzes am 9. August 2014 aus dessen § 2 Abs. 1, der auch für die Vollzugspolizei gilt.

Grundsätzlich ist die Übermittlung personenbezogener Daten per E-Mail an Personen oder Stellen außerhalb des sächsischen Polizeidatennetzes oder des SVN auch durch Ziff. 7 der Benutzerrichtlinie für die Nutzung von E-Mail (Anlage 2 der Rahmendienst-

vereinbarung Nutzung Internet-Dienste vom 8. Juli 2003) ausdrücklich verboten. Zum einen sind E-Mails eine nicht-formelle Form der Kommunikation, bei der nicht garantiert werden kann, dass die Nachricht den Empfänger rechtzeitig, inhaltlich korrekt, vollständig, unverfälscht oder überhaupt erreicht (s. auch Ziff. 1 Abs. 1 und Ziff. 4 Abs. 1 der Sicherheitsrichtlinie zum Betrieb der nicht-formellen Kommunikation mittels Exchange/Outlook im Polizeivollzugsdienst des Freistaates Sachsen vom 1. Juli 2014 - nfKom-SiRL). Schwerer wiegt jedoch die Tatsache, dass E-Mails ohne großen Aufwand durch Dritte mitgelesen, abgefangen, umgeleitet, verändert, ausgedruckt oder aufbewahrt werden können. In diesem Sinne ähneln sie Postkarten in der „analogen“ Welt.

Die Übermittlung personenbezogener Daten per E-Mail ist danach nur ausnahmsweise zulässig, namentlich dann, wenn sie zwingend zur Aufgabenerfüllung erforderlich ist, etwa da eine ganz besondere Eilbedürftigkeit besteht, die nicht durch Übermittlung per Fax, durch Kurier oder unter Hinzuziehung einer anderen Polizeidienststelle abgewendet werden kann, und spezielle Verschlüsselungssysteme verwendet werden (siehe Ziff. 4 nfKom-SiRL). Ziff. 32a der VwV Dienstordnung sieht ergänzend vor, dass die elektronische Kommunikation nur für Nachrichten zulässig ist, die keine schützenswerten Daten enthalten. Mit anderen Worten: Genauso wenig wie die Polizei per Postkarte personenbezogene Daten übermitteln darf, darf sie es per E-Mail tun.

Der Präsident der betroffenen Polizeidirektion versicherte mir, dass es in seiner Behörde nicht allgemein üblich sei, den Schriftwechsel in Ermittlungsverfahren per E-Mail zu führen. Ich habe ihn daraufhin jedoch trotzdem gebeten, seine Bediensteten erneut über das grundsätzliche Verbot der unverschlüsselten Übermittlung von E-Mails mit personenbezogenen Daten zu belehren und mir dies nachzuweisen.

Wegen einer weiteren, ähnlichen Petition hatte ich mich schließlich außerdem an das SMI gewandt. Der Landespolizeipräsident hat mein Anliegen positiv aufgenommen und Anfang 2015 sämtliche bereits geltenden Vorschriften zum datenschutzgerechten Umgang mit E-Mails in der Polizei in einem Erlass (Az.: 36-055/365 - „Grundsätzliche Maßnahmen zur Gewährleistung des Schutzes personenbezogener Daten im Rahmen der polizeilichen elektronischen Kommunikation“) zusammengefasst. Danach hat in der Vollzugspolizei ausnahmslos nunmehr Folgendes zu gelten:

A. Nutzung von Secure Mail-Gateway (SMGW)

Für den Versand von E-Mails an außerhalb des SVN/KDN befindliche Adressaten („dies können auch Kommunen sein, wenn sie keinen KDN-Anschluss nutzen“) steht für den Polizeibereich seit dem 2. Februar 2015 die Teilkomponente Secure Mail-Gateway (SMGW) zur Verfügung. Diese wird als Bestandteil der Basiskomponente Elektro-

nische Signatur und Verschlüsselung vom SID bereitgestellt. Für den Transport im Internet können über das SMGW die Nachrichten auf Anwendungsprogrammebene (Inhaltsverschlüsselung über S/MIME) verschlüsselt werden. Die hiermit zur Verfügung gestellten Verschlüsselungstools sind als Standard zu nutzen: E-Mails mit personenbezogenen Daten i. S. d. § 3 Abs. 1 SächsDSG mit Zielrichtung Internet sind zu verschlüsseln. Zu den Einzelheiten der Nutzung wird auf den einführenden Erlass des SMI vom 14. Januar 2015 (Az.: 32-0272.00/104) mit Handlungsanleitung verwiesen.

B. Sonderfall: Versendung „personenbezogener Daten mit besonders hoher Schutzwürdigkeit“:

Für personenbezogene Daten mit besonders hoher Schutzwürdigkeit, namentlich für sensitive und heikle personenbezogene Daten i. S. v. § 4 Abs. 2 SächsDSG, ist allerdings die durch das SMGW bewirkte Verschlüsselung nicht ausreichend. Derartige Daten dürfen grundsätzlich nicht in Netze außerhalb des SVN ohne die erforderliche Ende-zu-Ende-Verschlüsselung per E-Mail versendet werden. Wie bei einem E-Mail-Versand eine nach o. g. Grundsätzen erforderliche Inhalts-/Ende-zu-Ende-Verschlüsselung konkret bewerkstelligt werden kann, ist im Detail mit dem jeweiligen Beauftragten für Informationssicherheit der Dienststelle zu klären. Sofern die erforderliche Verschlüsselung nicht gewährleistet werden kann, ist auf andere, dem hohen Schutzbedarf entsprechende Kommunikationsmittel (z. B. klassisches Telefax, Übermittlung per Post, durch Kurier) zurückzugreifen.

C. Weitere Anforderungen an die E-Mail-Kommunikation: Absenderangabe/Signatur

a) Generell gilt: E-Mails werden an ihrem Ende mit einem Textbaustein versehen, aus dem sich die Bezeichnung und Anschrift der Behörde sowie Vor- und Nachname, Funktions-, Amts- oder Dienstbezeichnung, Referat, Referatsbezeichnung und Telekommunikationsverbindungen des Unterzeichners ergeben (E-Mail-Signatur). (Näheres unter Nr. 31 e VwV Dienstordnung vom 6. September 2010).

b) Für in Richtung Internet ausgehende E-Mails wird zur Vertrauensbildung und Erhöhung des Schutzes bei dem Adressaten darüber hinaus festgelegt, dass die „fortgeschrittene elektronische Signatur“ gemäß § 2 Nr. 2 SigG zu verwenden ist. Eine derartige Signatur wird im SMGW über die Funktion „[Sign]“ ermöglicht. Diese Signatur gemäß § 2 Nr. 2 SigG ermöglicht es, die Authentizität und Unverfälschtheit der durch sie signierten Daten zu prüfen; es erfolgt ein Austausch von digitalen Zertifikaten/Schlüsseln. Auf den bereits erwähnten Einführungserlass SMGW vom 14. Januar 2015 (Az.: 32- 0272.00/104) mit Handlungsanleitung wird verwiesen.

D. Verwaltungsvorschriften und Dienstvereinbarungen:

a) Sicherheitsrichtlinie zum Betrieb der nicht formellen Kommunikation mittels Exchange/Outlook im Polizeivollzugsdienst des Freistaates Sachsen nfKom-Sicherheitsrichtlinie (nfKom-SiRL) vom 1. Januar 2012,

b) Rahmendienstvereinbarung des SMI - Landespolizeipräsidium - und dem Hauptpersonalrat der Polizei Sachsen über die Nutzung von internetbasierten Diensten im Polizeivollzugsdienst Sachsen (Nutzung Internet-Dienste) vom 8. Juli 2003,

c) Verwaltungsvorschrift der Sächsischen Staatsregierung zur Regelung des Dienstbetriebes für die Behörden des Freistaates Sachsen (VwV Dienstordnung vom 6. September 2010, insbes. Ziff. 32).

Für diese Zusammenfassung bin ich dem Landespolizeipräsidenten dankbar. Ich gehe nach alledem davon aus, dass in der Polizei künftig keine unverschlüsselten E-Mails mehr versandt werden.

5.9.7 Zielgerichtete Ermittlungen statt undifferenzierter Erhebungen

Ermittlungen zur Strafverfolgung dürfen sich nur gegen solche Personen richten, gegen die ein Anfangsverdacht (§ 152 Abs. 2 StPO) vorliegt. Entsprechendes gilt für die vorbeugende Straftatenbekämpfung oder die Gefahrenabwehr. Stets müssen konkrete *tatsächliche Anhaltspunkte*, z. B. für das Vorliegen einer strafbaren Handlung, die Erhebung personenbezogener Daten rechtfertigen können. Dabei darf die Schwelle für das zulässige Tätigwerden mitunter durchaus niedrig sein, z. B. bei sog. Initiativermittlungen nach Nr. 6 RiStBV, die bereits dann zulässig sind, wenn „nach kriminalistischer Erfahrung die wenn auch geringe Wahrscheinlichkeit besteht, dass eine verfolgbare Straftat begangen worden ist“. Eine solch niedrige Schwelle widerspricht jedoch nicht dem Prinzip - dem Vorhandensein tatsächlicher Anhaltspunkte -, sondern bekräftigt es.

So selbstverständlich diese Feststellung auch anmutet, in der Praxis werde ich immer wieder mit Fragestellungen konfrontiert, bei denen dieses Prinzip zunächst verletzt scheint. Bereits in 14/8.9 hatte ich im Zusammenhang mit einem „Reihengentest nach § 81h StPO in Dresden und Umgebung zur Suche nach einem Sexualverbrecher“ im Jahr 2009 darauf hingewiesen, dass nur diejenige Ermittlungsmethode zulässig ist, die von einem Anfangsverdacht ausgehend weitere Daten erhebt und verdichtet. Um eine rechtsstaatlich unzulässige Vorratsdatensammlung handelt es sich dagegen, wenn Sicherheitsbehörden lediglich auf der Grundlage von Vermutungen, mögen diese auch naheliegen, zunächst Daten aller in Betracht kommenden Personen erheben, um diese dann nach bestimmten Kriterien zu analysieren.

So klein der Unterschied erscheinen mag, hat er doch gewaltige Auswirkungen: In dem einen Fall entstehen bei den Strafverfolgungsbehörden in der Regel ausschließlich Datensammlungen zu Personen, die einen Anfangsverdacht gesetzt haben. In dem anderen Fall entstehen dagegen Datensammlungen auch zu unbescholtenen Personen, zu denen bestenfalls eine größer werdende Gruppe von Personen, bei denen sich nach und nach ein Anfangsverdacht herauskristallisiert, hinzukommt. Letztere Vorgehensweise wirft nicht nur die Frage der unzulässigen Erhebung von Daten zu Personen, die keinen Anfangsverdacht gesetzt haben, sondern auch die Frage auf, was mit den Daten dieser Personen geschieht, wenn sie sich auch im weiteren Verlauf der Ermittlungen nicht als relevant erweisen. Aus einer Reihe von Gründen werden diese Daten nämlich praktisch nicht vor Abschluss der Ermittlungen gegen sämtliche Tatverdächtigen wieder gelöscht; stattdessen bleiben sie in den polizeilichen Dateien, wo sie nicht hingehören. Löschungsanträge - denen stattgegeben werden müsste - werden kaum gestellt werden, da die Betroffenen in der Regel von den gegen sie geführten Ermittlungen nichts wissen (können).

Auch im Berichtszeitraum wurde ich wieder mit einer solchen Frage konfrontiert: Im Herbst 2013 teilte mir eine Polizeibehörde ihr Vorhaben mit, Daten über eine bestimmte, identifizierbare Personengruppe in der Bevölkerung zu erheben und im Weiteren zu ermitteln, ob sich innerhalb dieser Bevölkerungsgruppe bestimmte typische Straftaten nachweisen lassen. Zur Bestimmung dieser Bevölkerungsgruppe, d. h. zur Erhebung der Daten, waren ganz allgemeine Merkmale vorgesehen, die für sich genommen alles andere als einen Anfangsverdacht zu begründen in der Lage waren.

Ich teilte der Polizeibehörde daraufhin mit, dass anstelle der breit angelegten Datenerhebung anhand ganz allgemeiner Merkmale bereits zu Beginn Daten nur über solche Personen erhoben werden dürfen, die einen - ggf. niedrigschwelligen - konkreten Anfangsverdacht gesetzt haben. Von diesen Personen ausgehend, darf die Ermittlungsbehörde dann im Zuge ihrer Ermittlungen den Kreis der Tatverdächtigen erweitern.

Die Polizeibehörde hat meine Hinweise beachtet. Ich hoffe, dass die Strafverfolgungsbehörden künftig von sich aus jede Form der Vorratsdatensammlung als solche erkennen und davon Abstand nehmen werden.

5.9.8 Kontrolle der Anti-Terror-Datei

Im November 2014 habe ich die Nutzung der „Anti-Terror-Datei“ (ATD) durch das LKA kontrolliert. Meine Kontrolle, etwa was die Zugriffsberechtigungen oder den Grund der Speicherungen anging, ergab keine ersichtlichen Verstöße gegen den Datenschutz.

Wegen des engen Sachzusammenhangs kontrollierte ich zur gleichen Zeit auch die Nutzung der o. g. Datei durch das LfV. Wegen meiner grundsätzlichen Bedenken gegen (immer) neue Befugnisse für die Sicherheitsbehörden und die Nachrichtendienste weise ich auf meinen Kontrollbericht zum LfV (siehe 5.10.2) hin.

5.9.9 Umgang mit sichergestellten Gegenständen und Daten im Strafverfahren

Ein Datenschutzbeauftragter einer sächsischen Polizeidirektion (PD) teilte mir folgenden, in Ermittlungsverfahren nicht seltenen Sachverhalt mit und bat um Beratung:

Die PD führe ein Ermittlungsverfahren wegen des illegalen Anbaus von Betäubungsmitteln gegen einen namentlich bekannten Beschuldigten. Bei der Durchsuchung seiner Wohnung seien neben Cannabispflanzen und -produkten auch ein Laptop sichergestellt (§ 94 StPO) worden. Im Zuge der weiteren Ermittlungen sei festgestellt worden, dass der Laptop gestohlen worden war. Der frühere Besitzer habe dies auch angezeigt und verlange nunmehr seinen Laptop zurück. Die PD habe von den darauf gespeicherten Daten eine Kopie angefertigt, so dass der Rechner dem ursprünglichen Besitzer zurückgegeben werden könne. Dem Beschuldigten könne nicht nachgewiesen werden, dass er auch den Diebstahl begangen hat. Die Dateien auf dem Rechner seien von unterschiedlichen Personen angelegt worden. Außerdem sei versucht worden, die Daten des ursprünglichen Besitzers zu löschen. Leider könne technisch nicht unterschieden werden, welche Daten welchem Nutzer zuzuordnen sind. Insbesondere sei auch eine zeitliche Zuordnung (vor dem Diebstahl/nach dem Diebstahl) nicht eindeutig möglich. Der Beschuldigte mache keine Angaben, insbesondere auch nicht zur Identifikation „seiner“ Dateien, verlange aber „seine“ auf dem Rechner befindlichen Dateien zurück.

Ich habe die PD im Hinblick auf die Fragen, wem der Laptop mit welchem Datenbestand zurückzugeben ist und ob der Beschuldigte ein Recht auf die Rückgabe bestimmter Dateien hat, wie folgt beraten:

Grundsätzlich sind nach § 94 StPO sichergestellte Beweisgegenstände, hier der Laptop und die darauf gespeicherten Dateien, zurückzugeben, wenn sie für Zwecke des Strafverfahrens nicht mehr benötigt werden (vgl. Nr. 75 Abs. 1 RiStBV). Mit dem Anfertigen einer Kopie des gesamten Datenbestandes (Backup) sind die verfahrensrelevanten Daten gesichert worden, so dass der Laptop grundsätzlich an den letzten Gewahrsamsinhaber, hier also den Beschuldigten, zurückzugeben wäre. Auf das Eigentum oder den Besitz an der Sache kommt es nicht an. Grundsätzlich ist der Zustand wiederherzustellen, der vor der Sicherstellung bestand.

Allerdings gibt es von diesem Grundsatz Ausnahmen:

Die Rückgabe des Laptops scheidet dann aus, wenn feststeht, dass der Gegenstand durch unrechtmäßiges oder strafbares Verhalten in den Besitz des letzten Gewahrsamsinhabers gelangt ist (vgl. Karlsruher Kommentar, StPO, 7. Aufl., § 94 Rdnr. 24). Stehen der Herausgabe an den letzten Gewahrsamsinhaber offensichtlich begründete Ansprüche eines Dritten entgegen, hier des früheren Besitzers, so werden die Sachen an diesen zurückgegeben (Nr. 75 Abs. 3 Satz 1 RiStBV). Hierbei ist allerdings sicherzustellen, dass die auf dem Speichermedium (Festplatte) befindlichen Dateien nachfolgender Nutzer vollständig gelöscht worden sind. Da nach Auskunft der PD die Dateien des ursprünglichen Besitzers nicht wiederhergestellt werden konnten, der Rechner aber datenmäßig auf null gebracht werden konnte, war die Festplatte des Laptops somit gelöscht oder auf die Werkseinstellungen zurückgesetzt an den ursprünglichen Besitzer zurückzugeben.

Die Rückgabe der auf dem Laptop gespeicherten Dateien scheidet ebenfalls dann aus, wenn feststeht, dass die Dateien durch unrechtmäßiges oder strafbares Verhalten in den Besitz des Beschuldigten gelangt sind. Dies ist hier allerdings fraglich. Der Rechner ist nach dem Diebstahl „neu aufgesetzt“ worden und die Dateien des ursprünglichen Besitzers sind nicht wiederherstellbar. Somit können keine offensichtlich begründeten Ansprüche des ursprünglichen Besitzers einer Herausgabe der Dateien an den Beschuldigten entgegenstehen.

Sollte der Rechner nach dem Diebstahl noch von anderen Personen benutzt worden sein, was allerdings nur theoretisch möglich und nicht erwiesen war, sodass sich eventuell auch deren Daten zum Zeitpunkt der Sicherstellung auf dem Laptop befunden hätten, stünden deren (Persönlichkeits-)Rechte einer Herausgabe an den Beschuldigten jedenfalls nicht entgegen, da hier gerade nicht positiv feststand, dass sie unrechtmäßig in den Besitz des Beschuldigten gelangt waren. Begründete Ansprüche Dritter, auch soweit sie auf Datenschutzrechten beruhen, waren nicht ersichtlich. Somit blieb es hier bei dem Grundsatz, dass die Daten an den letzten Gewahrsamsinhaber, somit den Beschuldigten, zurückzugeben sind. Da somit der gesamte Datenbestand, der sich zum Zeitpunkt der Sicherstellung auf dem Laptop befunden hat, betroffen ist, musste der Beschuldigte auch keine Angaben zum Auffinden „seiner“ Dateien machen.

Unterliegen nach § 94 StPO sichergestellte Gegenstände, hier etwa bestimmte Dateien des Beschuldigten, dem Verfall (§ 73 StGB) oder der Einziehung (§ 74 StGB), können diese nach den §§ 111b, 111c und 111e StPO sichergestellt oder beschlagnahmt werden und sind dann nicht zurückzugeben. Dies könnte etwa auf Dateien zutreffen, welche

Listen mit Kunden oder Lieferanten des Beschuldigten enthalten oder auf Bilddateien, welche Personen mit Cannabispflanzen zeigen.

Auf der Sicherungskopie der PD dürfen nur die Dateien gespeichert werden, die als Beweismittel für das konkrete Strafverfahren erforderlich sind (§ 483 Abs. 1 StPO, vgl. BVerfG, Beschluss vom 12. April 2005 - 2 BvR 1027/02). Die darüberhinausgehenden Datenbestände sind zu löschen.

5.10 Verfassungsschutz

5.10.1 Neue gesetzliche Regelung zur Vernichtung von Akten im Landesamt für Verfassungsschutz

Nachdem ich Ende 2012 Vernichtungen von Akten bzw. Aktenteilen, die angeblich für den parlamentarischen Untersuchungsausschuss zur Aufklärung behördlicher Aktivitäten im Zusammenhang mit dem sog. Nationalsozialistischen Untergrund (NSU) von Bedeutung waren oder hätten sein können, im LfV kontrolliert und die Ergebnisse Anfang 2013 in einem Bericht an den Sächsischen Landtag (LT-Drs. 5/11033) vorgestellt hatte, wurde mein Vorschlag einer Neuregelung der Vernichtung von Akten im LfV aufgegriffen und in einem Gesetzgebungsverfahren im Berichtszeitraum umgesetzt.

Die alte Rechtslage sah in § 7 Abs. 2 SächsVSG eine Löschpflicht für in Dateien gespeicherte Daten vor, wenn die Speicherung unzulässig oder die Kenntnis der Daten für die Aufgabenerfüllung nicht mehr erforderlich war. § 7 Abs. 4 SächsVSG a. F. bestimmte, dass Akten, in denen personenbezogene Daten gespeichert waren, zu vernichten waren, wenn die gesamte Akte zur Aufgabenerfüllung nicht mehr benötigt wurde. Bis zu diesem Zeitpunkt sollten einzelne in der Akte gespeicherte personenbezogene Daten, deren Kenntnis für die Aufgabenerfüllung des LfV nicht mehr erforderlich war, gesperrt werden.

Die frühere Regelung zur Vernichtung von Akten, die sich eng an den Wortlaut von § 20 Abs. 2 SächsDSG angelehnt hatte, war schwer mit einem effektiven Grundrechtsschutz der von Speicherungen betroffenen Personen in Einklang zu bringen. Dies lag - neben dem Fehlen einer klaren Definition des Begriffs der Akte - nicht zuletzt an der Besonderheit von Vorgängen und Akten im LfV. Während eine klassische Verwaltungsbehörde Vorgänge von einem definierten Anfang (Antrag, Ereignis) über ein Verwaltungsverfahren bis zu einem definierten Abschluss (Einstellung, Entscheidung, Verwaltungsakt) bearbeitet, führt das LfV auch Sachakten zu Beobachtungsobjekten oder Bestrebungen, die regelmäßig personenbezogene Daten enthalten. Mögen die Beobachtungsvorgänge zwar zu einem bestimmten Zeitpunkt beginnen, so ist ein Abschluss schwer zu prognostizieren und bei langlebigen extremistischen Phänomenen unabseh-

bar. In diesen Fällen muss(te) im Hinblick auf das Grundrecht auf informationelle Selbstbestimmung eine Löschung personenbezogener Daten auch in Akten möglich sein, bevor die gesamte Akte zur Aufgabenerfüllung nicht mehr benötigt wird. Lediglich eine Sperrung in Form eines Sperrvermerks, der zwar eine Nutzung der Daten verbietet, aber einer u. U. auf Jahrzehnte hinaus möglichen Kenntnisnahme der Informationen nicht entgegensteht, schützte das Grundrecht der Betroffenen nur unzureichend.

Aus diesem Grund habe ich angeregt, den Gleichlauf von Löschungen personenbezogener Daten in Dateien und Löschungen personenbezogener Daten in Akten gesetzlich festzulegen. Eine Unterscheidung zwischen Akten und Aktenteilen sollte obsolet werden.

Mit dem Gesetz zur Änderung des Polizeigesetzes des Freistaates Sachsen, zur Änderung des Sächsischen Verfassungsschutzgesetzes und zur Änderung des Sächsischen Versammlungsgesetzes sowie zur Änderung weiterer Gesetze vom 17. Dezember 2013 wurde § 7 Abs. 4 SächsVSG neu gefasst und sieht nun in seinem Satz 1 vor, dass die nicht in Dateien gespeicherten personenbezogenen Daten gemäß Absatz 2 zu löschen sind. Die Regelung erfasst damit personenbezogene Daten, die nicht in Dateien gespeichert - für diese gilt weiterhin § 7 Abs. 2 SächsVSG -, sondern in Papier- oder digitalen (aber nicht elektronisch auswertbaren) Akten enthalten sind.

Damit ist ein effektiver Grundrechtsschutz für Betroffene gewährleistet, ohne dass das LfV in der Erfüllung seiner gesetzlichen Aufgaben unangemessen beeinträchtigt wird.

5.10.2 Kontrolle der Anti-Terror-Datei

Im November 2014 habe ich die Nutzung der „Anti-Terror-Datei“ (ATD) durch das LfV und das LKA kontrolliert. Meine Kontrollen, etwa was die Zugriffsberechtigungen oder den Grund der Speicherungen anging, ergaben bei beiden Behörden keine ersichtlichen Verstöße gegen den Datenschutz.

Diese Kontrollen nehme ich jedoch gerne zum Anlass, hier auch einmal Grundsätzliches zur Schaffung (immer) neuer Befugnisse für die Nachrichtendienste und die Sicherheitsbehörden zu sagen. Die ATD ist nur ein Beispiel dafür, dass der Gesetzgeber - sprich: bestimmte Politiker - aus rein politischen Gründen neue Datenverarbeitungsbefugnisse schaffen, ohne den Rat der Fachleute (aus den Sicherheitsbehörden, den Nachrichtendiensten sowie den Datenschutzbehörden) ausreichend zu berücksichtigen und auch ohne die absehbare Beurteilung durch das BVerfG in sein Kalkül mit einzubeziehen. Im Besonderen gibt der Bundesgesetzgeber den staatlichen Datenschutzbehörden nicht die zur Kontrolle all dieser neuen Befugnisse erforderliche Personalausstattung an die Hand

- und das, obwohl er weiß, dass das BVerfG gerade auf eine ausreichende datenschutzrechtliche Kontrolle großen Wert legt.

Errichtet wurde die ATD aufgrund des Antiterrordateigesetzes als Verbunddatei der Polizei- und Verfassungsschutzbehörden von Bund und Ländern. Ausweislich der amtlichen Begründung bezweckte diese, „angesichts der Bedrohungen durch den internationalen Terrorismus den Informationsaustausch zwischen Polizeien und Nachrichtendiensten weiter zu verbessern“ (BT-Drs. 16/2950 S. 1). Im Kern enthielt der Gesetzentwurf Vorschriften über die Speicherung und Verwendung von Daten in einer „gemeinsamen standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern“ (§§ 1 bis 6 ATDG), des Weiteren Vorschriften, die die datenschutzrechtliche Verantwortung und Kontrolle (§§ 8 bis 12 ATDG) betrafen, und schließlich - auf Betreiben des Bundesrats - eine Evaluierungsvorschrift[1] und die Befristung des Gesetzes, namentlich das Außerkrafttreten mit Ablauf des 30. Dezember 2017.

Am 26. April 2007 erhob ein Beschwerdeführer vor dem BVerfG Verfassungsbeschwerde gegen das Antiterrordateigesetz. Unmittelbar wandte er sich gegen die §§ 1 bis 6 ATDG, mittelbar auch gegen die §§ 8 bis 12 ATDG.

Mit Urteil vom 24. April 2013[2] erkannte das BVerfG schwerwiegende verfassungsrechtliche Mängel des Antiterrordateigesetzes. So beanstandete es im Kern, dass die §§ 1 bis 6 ATDG den hinsichtlich des Rechts auf informationelle Selbstbestimmung (Datenschutz) gesteigerten verfassungsrechtlichen Anforderungen nicht gerecht wurden, nicht stets hinreichend bestimmt waren und nicht stets dem Übermaßverbot entsprachen. Im Hinblick auf den Ausgleich der zahlreichen und tiefgreifenden Eingriffsbefugnisse in die Rechte der Betroffenen hielt das Gericht insbesondere wegen des Umstands, dass den Betroffenen praktisch kein Auskunftsrecht zusteht, eine wirksame Aufsicht durch dafür geeignete staatliche Behörden, namentlich die Datenschutzbehörden, für wesentlich und erforderlich. Wörtlich führte das BVerfG dazu aus:

„*Die Gewährleistung einer wirksamen Aufsicht setzt zunächst sowohl auf Bundes- wie auf Landesebene mit wirksamen Befugnissen ausgestattete Aufsichtsinstanzen - wie nach geltendem Recht die Datenschutzbeauftragten - voraus. Weiter ist erforderlich, dass Zugriffe und Änderungen des Datenbestandes vollständig protokolliert werden. Dabei muss durch technische und organisatorische Maßnahmen sichergestellt werden, dass die Daten den Datenschutzbeauftragten in praktikabel auswertbarer Weise zur Verfügung stehen und die Protokollierung hinreichende Angaben für die Zuordnung zu dem zu kontrollierenden Vorgang enthält.*“ (Abs. 215)

[1] Vgl. Bericht der Bundesregierung vom 7. März 2013 (BT-Drs. 17/12665).
[2] BVerfGE 133, 277.

Zur Häufigkeit von Kontrollen durch die Datenschutzbehörden führte das BVerfG weiter aus:

„*Angesichts der Kompensationsfunktion der aufsichtlichen Kontrolle für den schwach ausgestalteten Individualrechtsschutz kommt deren regelmäßiger Durchführung besondere Bedeutung zu und sind solche Kontrollen in angemessenen Abständen - deren Dauer ein gewisses Höchstmaß, etwa zwei Jahre, nicht überschreiten darf - durchzuführen. Dies ist bei ihrer Ausstattung zu berücksichtigen.*“ (Abs. 217)

All dies war jedoch bereits 2006 bekannt und absehbar gewesen; die Stellungnahmen des damaligen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit hatten insofern an Deutlichkeit nichts zu wünschen übrig gelassen. Der Gesetzgeber hätte sich seine Niederlage vor dem BVerfG also ersparen können, wenn er auf den Rat der Fachleute gehört hätte.

Der Bundesgesetzgeber hat daraufhin mit dem am 14. Dezember 2014 beschlossenen und am 1. Januar 2015 in Kraft getretenen neuen § 10 Abs. 1, 2 ATDG u. a. die Kontrollbefugnisse der Datenschutzbeauftragten von Bund und Ländern neu geregelt. Danach darf bzw. muss auch ich „die von den Ländern in die Antiterrordatei eingegebenen Datensätze“ spätestens alle zwei Jahre kontrollieren.

Weiter nicht berücksichtigt hat der Gesetzgeber allerdings den mit regelmäßigen Kontrollen nicht nur der Antiterrordatei, sondern auch der verwandten Dateien der Polizeien und Nachrichtendienste verbundenen Mehraufwand in den staatlichen Datenschutzbehörden. Auch meine Behörde wird mit solchen Kontrollen, die aus verfassungsrechtlichen Gründen unerlässlich sind, zusätzlich belastet, ohne dass ich bisher das dazu nötige zusätzliche Personal erhalten habe.

Meine nächste Kontrolle der ATD wird - gemäß den Anforderungen des BVerfG - spätestens im November 2016 stattfinden.

5.11 E-Government

5.11.1 E-Government-Gesetz zur Veröffentlichung von Amtsblättern im Internet

Ich habe mich in der Vergangenheit oft mit der Zulässigkeit der Veröffentlichung von kommunalen Dokumenten im Internet beschäftigt (14/5.5.2, 15/5.5.6, 16/5.5.1). Das Sächsische E-Government-Gesetz (SächsEGovG) vom 9. Juli 2014 enthält nun in § 4 klare Vorgaben, unter welchen Voraussetzungen amtliche Mitteilungs- und Verkündungsblätter auch im Internet veröffentlicht werden dürfen. Dies setzt zunächst eine ent-

sprechende Regelung in einer Satzung voraus. In dieser ist auch eine Regelung zu treffen, welche Form als die authentische anzusehen ist.

Weiterhin ist jedoch sicherzustellen, dass in der elektronischen Fassung der Publikation 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 müssen als solche erkennbar gemacht werden und den Zeitpunkt der Änderung erkennen lassen. Dies wird die kommunale Verwaltungspraxis vor einige Herausforderungen stellen. Leider wurde § 4 SächsEGovG trotz meiner mehrfachen Anregung nicht in den Handlungsleitfaden zum Sächsischen E-Government-Gesetz aufgenommen.

5.12 Landessystemkonzept / Landesnetz

5.12.1 Einsatz von zusätzlichen Schutzmaßnahmen im Sächsischen Verwaltungsnetz (SVN)

Seit dem Jahr 1999 betreibt der Freistaat Sachsen ein eigenes Behördennetzwerk, welches sich mittlerweile auch in alle Kommunen erstreckt und sorgt somit für eine moderne Infrastruktur und kurze Wege in der Kommunikation mit dem Bürger und zwischen den Behörden. Ich begleite diese Entwicklungen in einem derart wichtigen Segment natürlich mit besonderem Augenmerk, auch weil über die Kommunikationsstränge die Daten der Bürger und Beschäftigten verteilt werden.

„The Times They Are a-Changin'“ - das gilt natürlich auch und besonders für die Technik. Das SVN soll in den kommenden Jahren in die Version 2.0 überführt werden. Und mit den nunmehr fest etablierten Informationssicherheitsbeauftragten in den Ressorts und den Kommunen gibt es jetzt eine weitere Stimme, die beim Thema Datenschutz und Informationssicherheit mitbestimmen wollen. Dabei ziehen Datenschutz und Informationssicherheit stets am selben Strang, nur nicht immer in die gleiche Richtung. Beim Einsatz von Logdaten zur Erkennung und Auswertung von potenziellen Angriffen oder beim Thema Ende-zu-Ende-Sicherheit für E-Mails (diese können aufgrund der Verschlüsselung nicht gescannt werden) gibt es von Zeit zu Zeit unterschiedliche Auffassungen.

Es gibt zurzeit erste Überlegungen für die Weiterentwicklung des Netzes und hierbei spielen Datenschutz und Informationssicherheit eine wichtige Rolle bei der Ausgestaltung der Zielvorgaben. Die nachfolgenden Festlegungen wurden dazu mit der Staatsregierung abgestimmt.

Meine Behörde wird für alle direkt in den Infrastrukturen des SVN 2.0 entstehenden Daten vor Abschluss der Verträge die Erforderlichkeit prüfen. Die Anbieter sind entsprechend dem Sächsischen Datenschutzgesetz zu verpflichten. Sie haben rechtzeitig ein Datenschutzkonzept vorzulegen. Die darin getroffenen Festlegungen sind durch den Freistaat Sachsen regelmäßig auf Einhaltung zu überprüfen. Fachdaten der Behörden, Einrichtungen und Kommunen sind jeweils vom Dateneigner entsprechend abzusichern.

Der Informationssicherheit kommt nach den Erkenntnissen über die Geheimdiensttätigkeiten der letzten zwei Jahre und den Angriffen auf Regierungsnetze eine besondere Bedeutung zu. Durch die Bereitstellung einer entsprechenden Infrastruktur soll diesen Erkenntnissen Rechnung getragen werden. Informationsübermittlungen durch die Anbieter außerhalb der EU sind unzulässig, die gesamte Administration der Komponenten und Dienste soll in Sachsen bzw. in Deutschland erfolgen.

Dies sind wesentliche, vertragsrelevante Aspekte, deren Einhaltung von den Anbietern über geeignete Verpflichtungen und Nachweise abgefordert werden. Wie im aktuellen SVN, gehört dazu auch der Einsatz sicherheitsüberprüften Personals für die Betriebsaufgaben. Eine sehr wesentliche Investition in den zukünftigen Schutz sächsischer Daten ist die Anforderung, die Infrastruktur entsprechend den Empfehlungen des BSI abzusichern und moderne Verschlüsselungsalgorithmen zu nutzen.

Nach Vergleich mit anderen Landesnetzen, den Erfahrungen des SVN und den Rückmeldungen der Ressorts wird für das gesamte SVN 2.0 das Schutzniveau gemäß BSI *Normal* festgelegt. Höhere Schutzbedarfe werden bei Erforderlichkeit und Angemessenheit in zu identifizierenden Teilbereichen umgesetzt.

Das SVN 2.0 soll auch weitere, jeweils den Angriffsvektoren angemessene Schutzmechanismen ermöglichen, die über die Arbeitsgruppe Informationssicherheit zu konkretisieren sind. Die Anpassung dieser Mechanismen muss jederzeit und kurzfristig möglich sein.

5.12.2 Verschlüsselung

Eine sorgfältig implementierte und konfigurierte Verschlüsselung ist in Zeiten der scheinbar schrankenlosen Datensammlung und -auswertung eine der wenigen technischen Maßnahmen, um die Vertraulichkeit sensibler personenbezogener oder anderer schützenswerter Daten tatsächlich noch wirksam gewährleisten zu können.

Aus diesem Grund, aber auch unter dem Eindruck der im April 2014 bekannt gewordenen „Heartbleed“-Verletzbarkeit tausender Webserver weltweit (https://de.wikipedia.

org/wiki/Heartbleed), habe ich das Thema in die maßgeblichen IT-Arbeitskreise des Freistaates Sachsen getragen. Dass diese Schwachstellen keinen Bogen um Sachsen machen und an vielen Stellen Handlungsbedarf besteht, ist den Verantwortlichen in den meisten Fällen klar. Aber - solange nichts passiert, gehen wie so oft andere Aufgaben im Tagesgeschäft aufgrund der verfügbaren Ressourcen vor.

In der Folge wurde ein sogenanntes Kernteam „Verschlüsselung“ eingesetzt, dessen vordringliche Aufgabe darin bestand, zunächst den Handlungsbedarf zu verdeutlichen, um danach Lösungsvorschläge zur Verbesserung der Situation zu unterbreiten.

So hat dann auch die Analyse der Ausgangslage - hier insbesondere die automatisierte Bewertung der Verschlüsselungszertifikate und -algorithmen auf Webservern - deutlich gemacht, dass zum damaligen Zeitpunkt auf ca. 70% der geprüften Websites zum Teil gravierende Zertifikatsfehler bestanden.

Unter meiner Mitwirkung sind die unter Kapitel 17.2.2 aufgeführten Handlungsempfehlungen erarbeitet und in der Zwischenzeit von allen relevanten Arbeitskreisen bestätigt worden. Sie sind also, entsprechend einer ebenso verabschiedeten Zeitplanung, nunmehr in die Praxis umzusetzen.

Im Kern bedeutet dies, die Webseiten künftig durchgängig verschlüsselt anzubieten, wobei nur noch anerkannt sichere Verschlüsselungsverfahren eingesetzt werden dürfen. Aber auch hinsichtlich des sicheren internen E-Mail-Versandes konnte eine durchgängige Transportverschlüsselung erreicht werden. Es entstanden Handlungsanleitungen zur E-Mail-Konfiguration, aber auch zur Härtung der typischerweise eingesetzten Webserver. Eine ausführliche Anleitung für die weitverbreitete Apache-Implementation habe ich extern beauftragt (siehe 17.2.3).

Die gestiegenen Anforderungen an die wirksame Gewährleistung von Vertraulichkeit werden erfreulicherweise auch durch die Aufnahme der Verschlüsselung in § 2 Abs. 1 Satz 2 SächsEGovG deutlich: „Für die elektronische Kommunikation sind Verschlüsselungsverfahren anzubieten und grundsätzlich anzuwenden“.

Verschlüsselung ist aus meiner Sicht im Bewusstsein der IT-Entscheidungsträger angekommen. Es ist kein „nice-to-have“-Baustein mehr, den man sich je nach Kassenlage leisten kann oder eben nicht. Mit anderen Worten: Verschlüsselung wird zu einem maßgeblichen Qualitätskriterium im künftigen Nachfolger des derzeitigen Sächsischen Verwaltungsnetzwerkes.

Ich werde die Umsetzung der sich aus den vorab genannten Handlungsempfehlungen und dem Sächsischen E-Government-Gesetz ergebenden Maßnahmen auch im kommenden Berichtszeitraum aufmerksam verfolgen.

5.13 Ausländerwesen

5.13.1 Einsicht in Akten der Ausländerbehörden

Nachdem mich die Problematik verweigerter oder beschränkter Einsicht in Akten der Ausländerbehörden früher des Öfteren zu Beiträgen in Tätigkeitsberichten veranlasst hatte (vgl. 14/5.12.2), stelle ich fest, dass mich auf diesem Gebiet im Berichtszeitraum weniger Petitionen erreicht haben. Meine Erfahrungen zeigen, dass die Ausländerbehörden offenbar sensibler und überwiegend betroffenenfreundlich agieren, wobei den Beteiligten bewusst ist, dass es sich dabei nicht um Kulanz, sondern um die Umsetzung gesetzlicher Vorgaben handelt.

Gleichwohl möchte ich zwei Fälle aus dem Berichtszeitraum erwähnen, die exemplarisch für Schwierigkeiten bei der Gewährung von Akteneinsicht stehen:

In einem Fall wurde auf Antrag des Rechtsanwalts eines Ausländers Einsicht in dessen Ausländerakte gewährt, wobei der Akte vor der Einsichtnahme sieben Seiten, die einen Ausdruck aus INPOL enthielten, sowie zwei weitere Seiten, die den Ausdruck aus dem Ausländerzentralregister enthielten, entnommen worden waren. Die Verweigerung der Einsicht in diese Aktenbestandteile begründete die Ausländerbehörde mit § 12 Abs. 5 BKAG, wonach für Auskünfte aus INPOL das Bundeskriminalamt zuständig sei, sowie mit § 34 Abs. 1 AZRG, wonach für Auskünfte aus dem Ausländerzentralregister das Bundesamt für Migration und Flüchtlinge (BAMF) als Registerbehörde nach § 1 Abs. 1 Satz 1 AZRG die Zuständigkeit besitze. Die Ausländerbehörde hielt die Vorschriften des § 12 Abs. 5 BKAG und des § 34 Abs. 1 AZRG, nach denen Sie mangels Zuständigkeit keine Einsicht gewähren dürfe, für vorrangig gegenüber etwaigen Ansprüchen nach § 29 VwVfG und § 18 SächsDSG.

Ich habe daraufhin die Ausländerbehörde auf die Rechtslage hingewiesen:

Die einzelne Ausländerbehörde ist nicht Adressat der Vorschriften des Bundeskriminalamtgesetzes sowie des Ausländerzentralregistergesetzes. Sie ist weder das BKA noch die Registerbehörde des Ausländerzentralregisters (BAMF) - nur diese Behörden werden in den genannten Gesetzen aber zur Auskunftserteilung verpflichtet und zu bestimmten Beschränkungen der Auskunft befugt. Die Ausländerbehörde, die im laufenden Verwaltungsverfahren nach § 29 VwVfG Auskunft zu erteilen bzw. Akteneinsicht zu gewähren und außerhalb eines Verfahrens bzw. verfahrensunabhängig die Rechte des

Betroffenen nach § 18 SächsDSG zu erfüllen hat, kann sich nicht auf Auskunftsbeschränkungen in Gesetzen berufen, deren Adressat sie nicht ist.

Dass § 12 Abs. 5 BKAG und § 34 Abs. 1 AZRG gegenüber § 29 VwVfG und § 18 SächsDSG spezieller sind, ist zutreffend, hat aber lediglich Auswirkungen auf Auskunftsansprüche Betroffener gegenüber dem BKA zu in INPOL gespeicherten Daten bzw. gegenüber dem BAMF zu Daten, die im Ausländerzentralregister gespeichert sind. Diese Ansprüche könnten wegen des Vorrangs spezieller Vorschriften nicht auf § 19 BDSG (der bezüglich Bundesbehörden dem § 18 SächsDSG entspricht) gestützt werden.

Der Anspruch des Ausländers zielt aber gerade auf die in der Ausländerbehörde zu seiner Person gespeicherten Daten, wozu die für das Verfahren eingeholten Angaben aus INPOL selbstverständlich ebenso gehören wie der Ausdruck aus dem Ausländerzentralregister, nachdem diese in die Ausländerakte aufgenommen worden waren. Die Ausländerbehörde hat diesen Anspruch - je nach Zusammenhang (s. o.) - ausschließlich nach Maßstab des § 29 VwVfG bzw. des § 18 SächsDSG zu erfüllen.

Die von der Ausländerbehörde in diesem Verfahren unzutreffend als vorrangig angesehenen Regelungen entfalten auch keine „Fernwirkung“ in dem Sinne, dass dritte Stellen, die Auskünfte, Abdrucke oder Auszüge aus den Datenbanken erhalten, bei ihrem behördlichen Umgang mit diesen Daten den Anforderungen und Beschränkungen unterlägen, die das BKA nach § 12 Abs. 5 BKAG und die Registerbehörde nach § 34 AZRG zu beachten hat.

Ebenso wenig ist eine Zustimmung des BKA bzw. des BAMF für eine Akteneinsicht des Betroffenen in seine Ausländerakte erforderlich. § 18 Abs. 7 SächsDSG macht lediglich die Auskunft über Datenübermittlungen an Strafverfolgungs- und Sicherheitsbehörden (so auch § 19 Abs. 3 BDSG) von der Zustimmung dieser Behörden abhängig. Soweit sich die Auskunftserteilung auf die Herkunft von Daten bezieht, die der Ausländerbehörde von anderen (Sicherheits-)Behörden übermittelt worden sind, sieht das Gesetz kein Zustimmungserfordernis vor. Der Gesetzgeber ging offenbar davon aus, dass Daten, die eine Strafverfolgungs- oder Sicherheitsbehörde an eine Behörde außerhalb des Sicherheitsbereichs übermittelt, nicht in gleicher Weise geheimhaltungsbedürftig sind (vgl. Mallmann in Simitis, Kommentar zum BDSG, 7. Aufl., § 19 Rdnr. 74). Ausreichend sind hier die Beschränkungen in den für die dritten Behörden maßgeblichen Auskunftsregelungen.

Die Beschränkungen der Auskunft bzw. Akteneinsicht, die die Ausländerbehörde vornehmen kann bzw. muss, ergeben sich danach allein aus den Vorschriften des § 29 Abs. 2 VwVfG bzw. § 18 Abs. 5 SächsDSG.

Die Ausländerbehörde im Beispielfall konnte sich leider nicht dazu durchringen, meiner Auffassung zu folgen, gewährte aber umfassend und uneingeschränkt Einsicht auch in die zuvor zurückgehaltenen Aktenbestandteile, nachdem die zwischenzeitlich eingeschaltete Landesdirektion Sachsen als ausländerrechtliche Aufsichtsbehörde die Zustimmung des BKA und des BAMF (Registerbehörde für das Ausländerzentralregister) eingeholt hatte. Im Rahmen seiner Äußerung schloss sich das BKA übrigens meiner Einschätzung an, dass der INPOL-Ausdruck mit Aufnahme in die Ausländerakte Bestandteil dieser Akte wird und damit ausschließlich den Einsichtsbestimmungen für Ausländerakten unterfällt.

Ich hoffe, dass die Ausländerbehörde bei künftigen Akteneinsichtsgesuchen diese nur anhand der für sie einschlägigen gesetzlichen Bestimmungen prüft und keine Vorschriften mehr anwendet, deren Adressat sie nicht ist.

Dass auch bei der Anwendung von § 29 VwVfG als der (einzigen) einschlägigen Vorschrift für Akteneinsichten im laufenden aufenthaltsrechtlichen Verfahren Beschränkungen der Einsicht möglich und zulässig sind, zeigt der zweite Fall:

In einem aufenthaltsrechtlichen Verfahren hatte sich auch das Generalkonsulat des Herkunftsstaats des Ausländers geäußert, in seinem Schreiben aber um „Vertraulichkeit“ und ausdrücklich darum gebeten, das Schreiben Dritten nicht zugänglich zu machen.

Der auf Einsicht auch in dieses Schreiben gerichtete Antrag des Rechtsanwalts des Ausländers - in die restlichen Teile der Akte war Einsicht gewährt worden - wurde im Ergebnis abgelehnt. Anders als im zuvor geschilderten Fall, in dem ein Registerauszug und ein Ausdruck aus einem polizeilichen Auskunftssystem standardmäßig zur Akte genommen worden waren, ohne dass dabei Auskunftssperren oder ähnliches vermerkt waren, hatte hier der Verfasser des Schreibens, die konsularische Vertretung eines auswärtigen Staates, konkret den Wunsch nach vertraulicher Behandlung geäußert. Zwar war auch dieses Schreiben Bestandteil der Ausländerakte geworden, allerdings hatte die Ausländerbehörde - in Abstimmung mit dem SMI - in Anwendung des § 29 VwVfG die Ablehnung der Einsicht auf einen Ausnahmetatbestand des § 29 Abs. 2 VwVfG gestützt.

Die Ablehnung der Einsicht wurde mit drohenden Nachteilen für das Wohl des Bundes bei Bekanntwerden der Zugänglichmachung des Schreibens sowie mit Art. 33 des Wie-

ner Übereinkommens über konsularische Beziehungen und der dort statuierten Unverletzlichkeit konsularischer Schriftstücke begründet. Zwar lag auch unter den Umständen des Einzelfalls die Gewährung der Akteneinsicht im gesetzmäßigen Ermessen der Behörde. Diese durfte aber nach § 29 Abs. 2 VwVfG drohende Beeinträchtigungen des Wohls des Bundes bei der Abwägung des öffentlichen Interesses an der Geheimhaltung gegenüber dem Interesse des Ausländers an der Einsicht in das Konsulatsschreiben berücksichtigen. Dass damit außenpolitische Rücksichtnahmen zu der Entscheidung führten, keine Einsicht zu gewähren, war vertretbar und ist daher datenschutzrechtlich nicht zu beanstanden gewesen.

Allerdings habe ich die Ausländerbehörde und das SMI auch darauf hingewiesen, dass nach deutschem Verwaltungsrecht die Behörde in diesem Fall verpflichtet ist, den Betroffenen zur Wahrung seines rechtlichen Gehörs *in anderer Weise* über den wesentlichen Inhalt der Akten zu unterrichten (vgl. Kopp/Ramsauer, Kommentar zum VwVfG, § 29 Rdnr. 27).

Das konkrete aufenthaltsrechtliche Verfahren konnte übrigens mit einer alle Beteiligten zufriedenstellenden Entscheidung abgeschlossen werden; die Ablehnung der Einsicht in das Schreiben des Generalkonsulats hatte keine nachteiligen Konsequenzen für den Betroffenen.

5.13.2 Adressmittlungsverfahren zur Versendung von Anschreiben an ausländische Staatsangehörige

Im Berichtszeitraum trat das SMI mit der Frage an mich heran, in welcher Weise es Adressdaten ausländischer Staatsangehöriger zur Versendung von *nicht zur Aufgabenerfüllung erforderlicher*, gleichwohl politisch erwünschter Anschreiben nutzen dürfe. Es bestünden Zweifel, ob die gesetzlichen Grundlagen eine solche Nutzung der in den Ausländerdateien der unteren Ausländerbehörden, d. h. der Landkreise und kreisfreien Städte, gespeicherten Daten durch es erlaubten.

Ich habe dem SMI daraufhin mitgeteilt, dass ich seine Zweifel teile. Zugleich aber habe ich darauf hingewiesen, dass ich keine Bedenken gegen ein Adressmittlungsverfahren, also ein Verfahren, bei dem das SMI den unteren Ausländerbehörden frankierte, aber nicht adressierte Briefumschläge samt nicht personalisierten Anschreiben übergibt, habe. Die unteren Ausländerbehörden dürfen die Umschläge sodann mit den aus der Ausländerdatei A oder dem Ausländerzentralregister erhobenen Adressdaten versehen und versenden.

5.14 Wahlrecht

In diesem Jahr nicht belegt.

5.15 Sonstiges

In diesem Jahr nicht belegt.

6 Finanzen

6.1 Kirchensteuerabzugsverfahren

Einige Aufregung verursachten im Berichtszeitraum die Mitteilungen von Banken oder Sparkassen an ihre Kunden, dass sie das Merkmal „Zugehörigkeit oder Nicht-Zugehörigkeit zu einer Religionsgesellschaft“ von der Steuerverwaltung erhalten haben und für Zwecke der Abführung (oder Nichtabführung) der Kirchensteuer nutzen. Die Banken oder Sparkassen hatten dies im Sinne der Transparenz ihrer Datenverarbeitung datenschutzfreundlich ihren Kunden mitgeteilt.

Den verhältnismäßig vielen Petenten, die in dieser Übermittlung ihrer Religionszugehörigkeit bzw. -nichtzugehörigkeit durch die Steuerverwaltung an die kontoführende Stelle einen Verstoß gegen den Datenschutz sahen, konnte ich fernmündlich oder schriftlich stets Folgendes mitteilen:

Ab 2009 wurde die Besteuerung von Kapitalerträgen (Zinsen, Dividenden, Veräußerungsgewinnen etc.) durch die Einführung der sogenannten Abgeltungssteuer, einer besonderen Form der Erhebung der Einkommensteuer *und damit auch der Kirchensteuer*, gesetzlich neu geordnet. Wurde bisher Einkommenssteuer auf Kapitalerträge durch Angabe in der Einkommenssteuererklärung erst im Rahmen der Veranlagung durch das Finanzamt erhoben, wurde sie mit der Neuregelung gleich an der Quelle, d. h. bei dem kontoführenden Kreditinstitut (der Bank oder Sparkasse) einbehalten und von dort an die Finanzverwaltung abgeführt. Im Zuge der Neuregelung wurde übrigens der Steuersatz der Abgeltungssteuer auf höchstens 25% (bisher bis zu 45%) begrenzt. Hierauf wurde und wird - neben dem Solidaritätszuschlag - auch die Kirchensteuer (in Sachsen 9%) erhoben. Die steuermindernde Wirkung des Sonderausgabenabzugs für die Kirchensteuer wurde mit berücksichtigt, d. h. sie ist in der Tarifformel eingepreist. Mit dem Einbehalt der Kirchensteuer konnte das Kirchenmitglied bisher seine Bank beauftragen. Dazu musste es dieser seine Religionszugehörigkeit mitteilen. Die Bank behielt die Kirchensteuer daraufhin gleich mit ein. Andernfalls musste der Steuerpflichtige seine Kapitalerträge zur Festsetzung der Kirchensteuer im Rahmen seiner Einkommenssteuererklärung angeben.

Ab 2015 erhält die Bank oder Sparkasse nunmehr das Religionsmerkmal elektronisch durch die Finanzverwaltung verschlüsselt mitgeteilt. Dies ist vergleichbar mit dem Verfahren beim Lohnsteuerabzug, bei dem der Arbeitgeber die Religionszugehörigkeit des Arbeitnehmers ebenfalls elektronisch mitgeteilt bekommt (Verfahren ELSTAM). Damit wird die Erhebung der Kirchensteuer auf Kapitalertragssteuer in die Philosophie des Kapitalertragssteuer-Erhebungsverfahrens vollständig eingebunden (vgl. § 51a Abs. 2c und e EStG i. d. F. des Amtshilferichtlinie-Umsetzungsgesetzes).

Die gesetzliche Grundlage für diese Übermittlungen, namentlich § 51a Abs. 2c EStG, begegnet keinen datenschutzrechtlichen Bedenken. Sie ist verhältnismäßig und mit dem Grundgesetz vereinbar. Zwar wird das Recht, nicht verpflichtet zu sein, seine religiöse Überzeugung zu offenbaren, durch Art. 4 Abs. 1 GG (Glaubensfreiheit) in Verbindung mit Art. 136 Abs. 3 WRV gewährleistet. Es ist jedoch spätestens seit dem Volkszählungsurteil des BVerfG (BVerfGE 65, 1 ff.) anerkannt, dass Art. 136 Abs. 3 Satz 2 WRV durch ein behördliches Fragerecht zu (hauptsächlich) steuerlichen oder statistischen Zwecken eingeschränkt werden darf:

„*Die Verpflichtung zu wahrheitsgemäßen Angaben (§ 5 Abs. 1 Nr. 1 VZG 1983 in Verbindung mit § 10 Abs. 3 BStatG) über die rechtliche Zugehörigkeit oder Nichtzugehörigkeit zu einer Religionsgesellschaft (§ 2 Nr. 1 VZG 1983) verstößt nicht gegen das Grundrecht der Beschwerdeführer auf Bekenntnisfreiheit (Art. 4 Abs. 1 GG). Zur Bekenntnisfreiheit gehört nicht nur das Recht, seine religiöse Überzeugung zu bekennen, sondern auch zu schweigen, wie dies durch Art. 140 GG in Verbindung mit Art. 136 Abs. 3 der Weimarer Reichsverfassung (WRV) besonders anerkannt ist. Diese negative Bekenntnisfreiheit wird aber durch den Vorbehalt des Art. 136 Abs. 3 Satz 2 WRV eingeschränkt, der es den Behörden gestattet, nach der Zugehörigkeit zu einer Religionsgesellschaft zu fragen, wenn davon Rechte und Pflichten abhängen oder eine gesetzlich angeordnete statistische Erhebung dies erfordert. Eine solche zulässige Ausnahme liegt hier vor, da es sich um eine gesetzlich angeordnete statistische Erhebung für Bundeszwecke (Art. 73 Nr. 11 GG) handelt.*“ (BVerfGE 65, 1, 39)

So wird auch etwa die nach § 49 Abs. 1 EStG vorgesehene Eintragung der Religionszugehörigkeit oder -nichtzugehörigkeit auf der Lohnsteuerkarte und die darin liegende Offenbarung durch die in Art. 137 Abs. 6 WRV enthaltene Garantie einer geordneten Besteuerung gerechtfertigt (vgl. BVerfG, NVwZ 2001 S. 909).

Auch die technisch-organisatorischen Maßnahmen, die der Gesetzgeber für die Gewährleistung des Datenschutzes vorgeschrieben hat, begegneten keinen Bedenken. So ist u. a. vorgeschrieben, dass dem Abzugsverpflichteten (der Bank oder Sparkasse) das Religionsmerkmal als sechsstellige Kennzahl geliefert wird. Mit ihr kann die Bank oder Sparkasse die einbehaltene Kirchensteuer an diejenige Religionsgemeinschaft weiterleiten, der der Kunde konkret angehört. Die Verarbeitung des Religionsmerkmals erfolgt zudem in einer gesicherten Umgebung, d. h. für die Mitarbeiter der Bank ist die Religionszugehörigkeit des Kunden nicht einsehbar, sie wird nicht in seinen Kundenstammdaten ausgewiesen. Gehört der Kunde keiner steuererhebenden Religionsgemeinschaft an oder hat er nach § 51a Abs. 2e EStG der Weitergabe seines Religionsmerkmals an

die Bank oder Sparkasse widersprochen, wird der Bank oder Sparkasse ein neutraler Nullwert übermittelt.

Ein Verstoß gegen den Datenschutz lag damit in keinem der an mich herangetragenen Fälle vor.

Ein amtlich vorgeschriebenes Formular für den Widerspruch hält das Bundeszentralamt für Steuern bereit (www.bzst.de). Das Kirchenmitglied ist dann jedoch verpflichtet, im Folgejahr die für die Berechnung der Kirchensteuer notwendigen Angaben im Rahmen seiner Veranlagung gegenüber der Steuerbehörde zu machen.

6.2 Regelmäßige Übermittlung von Einkommensdaten durch die Steuerverwaltung an die Industrie- und Handelskammern

Ein Gewerbetreibender wandte sich an mich und trug vor, dass seine IHK ganz offensichtlich über Daten aus seiner Einkommenssteuererklärung verfüge. Er sah darin einen Verstoß gegen den Datenschutz, konkret gegen das Steuergeheimnis nach § 30 AO. Ich konnte dem Petenten mitteilen, dass das Finanzamt durchaus auf gesetzlicher Grundlage bestimmte Einkommensdaten an die IHK übermitteln und die IHK diese Daten auch erheben darf.

Rechtsgrundlagen hierfür sind § 31 Abs. 1 AO:

„§ 31 Mitteilung von Besteuerungsgrundlagen
(1) Die Finanzbehörden sind verpflichtet, Besteuerungsgrundlagen, Steuermessbeträge und Steuerbeträge an Körperschaften des öffentlichen Rechts einschließlich der Religionsgemeinschaften, die Körperschaften des öffentlichen Rechts sind, zur Festsetzung von solchen Abgaben mitzuteilen, die an diese Besteuerungsgrundlagen, Steuermessbeträge oder Steuerbeträge anknüpfen. Die Mitteilungspflicht besteht nicht, soweit deren Erfüllung mit einem unverhältnismäßigen Aufwand verbunden wäre. Die Finanzbehörden dürfen Körperschaften des öffentlichen Rechts auf Ersuchen Namen und Anschriften ihrer Mitglieder, die dem Grunde nach zur Entrichtung von Abgaben im Sinne des Satzes 1 verpflichtet sind, sowie die von der Finanzbehörde für die Körperschaft festgesetzten Abgaben übermitteln, soweit die Kenntnis dieser Daten zur Erfüllung von in der Zuständigkeit der Körperschaft liegenden öffentlichen Aufgaben erforderlich ist und überwiegende schutzwürdige Interessen des Betroffenen nicht entgegenstehen.
(2) …
(3) …“

sowie § 9 IHKG:

„§ 9
(1) …
(2) Die Industrie- und Handelskammern … sind berechtigt, zur Feststellung der Kammerzugehörigkeit und zur Festsetzung der Beiträge der Kammerzugehörigen Angaben zur Gewerbesteuerveranlagung, wie sie auch zur Feststellung der Kammerzugehörigkeit im Sinne von § 2 Abs. 1 erforderlich sind, sowie die nach § 3 Abs. 3 erforderlichen Bemessungsgrundlagen bei den Finanzbehörden zu erheben.
(3) Die in den Absätzen 1 und 2 genannten Daten dürfen von den Industrie- und Handelskammern und ihren Gemeinschaftseinrichtungen verwendet werden, soweit dies zur Erfüllung der ihnen nach diesem Gesetz übertragenen Aufgaben erforderlich ist. Andere als die in Satz 1 genannten Daten dürfen sie nur erheben und verwenden, soweit eine andere Rechtsvorschrift dies erlaubt oder anordnet.
(4) …
(5) …
(6) …“

Das für den Petenten zuständige Finanzamt war mithin verpflichtet, der IHK die zur Festsetzung des IHK-Beitrages des Petenten erforderlichen Besteuerungsgrundlagen, Steuermessbeträge und Steuerbeträge mitzuteilen. Denn die IHK ist Körperschaft des öffentlichen Rechts und knüpft bei ihrer Beitragsfestsetzung an die Besteuerungsgrundlagen (Einkommen, bestimmte Einkunftsarten und die Höhe dieser Einkünfte, Gewinn, Ertrag, Vermögensangelegenheiten und ihr Wert, Umsatz, Gewerbeertrag, Gewerbekapital u. Ä.), Steuermessbeträge oder Steuerbeträge des Petenten an. Das Finanzamt darf der IHK jedoch selbstverständlich nur die zur Beitragsfestsetzung *erforderlichen* Angaben übermitteln, nicht darüber hinausgehende Angaben. Die für den Petenten zuständige IHK durfte ihrerseits diese Angaben auch erheben (§ 9 Abs. 2 IHKG).

Der Gesetzgeber wollte also die IHK in den Stand versetzen, die Beiträge für ihre Mitglieder aufgrund der von den Finanzämtern übermittelten Angaben festzusetzen. Einen Verstoß gegen den Datenschutz konnte ich in diesem und gleichen Fällen, die an mich herangetragen wurden, nicht erkennen.

6.3 Unrichtige Verarbeitung des Heiratsdatums führte zu falscher Steuerklasse

Im Berichtszeitraum teilte mir ein im öffentlichen Dienst beschäftigter Petent mit, dass er in seiner Bezügemitteilung entdeckt habe, neuerdings in der Lohnsteuerklasse IV ge-

führt zu werden. Er habe jedoch bereits vor Jahren die für ihn und seine Ehefrau viel günstigere Lohnsteuerklassenkombination III/IV beantragt und bis vor kurzem auch gehabt. Eine Änderung hätten weder er noch seine Ehefrau beantragt. Die neue Lohnsteuerklassenkombination habe für ihn über Monate hinweg, in denen er sich um eine Rückkehr zu der Kombination III/IV bemüht habe, zu einer deutlich höheren Lohnsteuervorauszahlung, d. h. zumindest zu einem Zinsschaden, geführt. Das zuständige Finanzamt habe ihm derweil erklärt, dass sich in das automatisierte Verarbeitungsverfahren ein Fehler eingeschlichen habe, der jedoch weder durch das Finanzamt noch die Meldebehörde veranlasst worden sei.

Hierzu muss man wissen: Mit Wirkung zum 1. Januar 2013 wurden die Lohnsteuerkarten aus Papier durch ein elektronisches Datenaustauschverfahren ersetzt. Dieses sieht auf der Grundlage der „Verordnung über die elektronische Übermittlung von für das Besteuerungsverfahren erforderlichen Daten“ (StDÜV) den elektronischen Austausch von steuerlich relevanten Daten, insbesondere von Angaben zum Wohnort, Familienstand oder auch einem nach Beantragung erfolgten Steuerklassenwechsel vor. Diese Daten werden durch die Meldebehörde (Gemeinde) sowie das jeweils zuständige Finanzamt an das BZSt übermittelt. Das BZSt speichert diese Daten und stellt sie als elektronische Lohnsteuerabzugsmerkmale (ELSTAM) für die Arbeitgeber, hier also den Arbeitgeber des Petenten, zum Abruf bereit.

Meine Ermittlungen ergaben nun, dass der Petent vor einiger Zeit sein bei seiner Meldebehörde unrichtig eingetragenes Heiratsdatum berichtigen ließ (§ 19 SächsDSG) - ein völlig normaler Vorgang. Dadurch wurde jedoch automatisch ein aktualisierter Datensatz des Petenten an das BZSt übermittelt. Da in dem betreffenden Zeitraum die entsprechende BZSt-Datenbank fehlerhaft programmiert war, wurde dem Petenten der Status eines Neuverheirateten und damit die für diese standardmäßig vorgesehene Steuerklassenkombination IV/IV zugeteilt. Der Fehler sei, so das zuständige sächsische Finanzamt, jedoch zwischenzeitlich behoben worden.

Da das BZSt als Bundesbehörde nicht in meine Kontrollzuständigkeit fällt, habe ich den Vorgang schließlich an die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit abgegeben.

Gerne nehme ich diesen Vorgang jedoch zum Anlass, darauf hinzuweisen, dass die Generierung unrichtiger Datensätze in automatisierten Verfahren zu Schadensersatzansprüchen des Betroffenen gegen die öffentliche Verwaltung führen kann. Anspruchsgrundlage hierfür können - bei Ansprüchen gegen sächsische öffentliche Stellen - neben den „klassischen“ Amtshaftungsansprüchen auch der betroffenenfreundlich formulierte § 23 SächsDSG sein. Dieser setzt kein Verschulden, also weder Fahrlässigkeit noch

Vorsatz, der öffentlichen Stelle voraus und ist weder der Höhe nach noch auf automatisierte Verarbeitungen begrenzt.

6.4 Antragstellung bei der SAB nach der Richtlinie Hochwasserschäden 2013

Die Sächsische Aufbaubank ist gesetzlich mit der Bewilligung und Auszahlung staatlicher Fördermittel beauftragt. Einem hohen Verwaltungsaufwand begegnet die Behörde mit einem für die Verfahren spezifischen Internet-Angebot auszufüllender Formulare, die über die Seite der Bank bezogen werden können. Bereits in der Vergangenheit erreichten mich Nachfragen zur datenschutzrechtlichen Zulässigkeit von Nachfragen und Forderungen der SAB an den Antragsteller.

Neu war hingegen der Hinweis eines Antragstellers, die SAB verwende bei der Antragstellung nach der *Richtlinie Hochwasserschäden 2013* den Vordruck für eine Einwilligungserklärung in die unverschlüsselte elektronische Übersendung von Daten. Im Text des Einwilligungsformulars wurde der Antragsteller zunächst auf die Risiken unverschlüsselter elektronischer Datenübermittlung hingewiesen. Gleichzeitig wurde er ermuntert, dennoch auf der elektronischen Übermittlung seiner Daten per E-Mail zu „bestehen“ und das Risiko fehlerhafter Übermittlung ab dem Zeitpunkt des Verlassens der elektronischen Nachricht der technischen Infrastruktur der SAB zu übernehmen.

Die SAB ist als öffentliche Stelle pflichtig, nach dem Stand der Technik Maßnahmen zu treffen, die eine personenbezogene Datenverarbeitung gemäß den Anforderungen des § 9 Abs. 1, 2 SächsDSG gewährleisten. Die gesetzliche Verantwortung ist nicht disponibel bzw. kann nicht durch Einwilligung der Betroffenen abgeschwächt werden oder entfallen. Eine unverschlüsselte elektronische Übermittlung personenbezogener Daten per E-Mail erfüllt die im Gesetz genannten Anforderungen an eine zulässige elektronische Verarbeitung personenbezogener Daten regelmäßig nicht.

Die SAB teilte mir in ihrer Stellungnahme mit, dass ihr grundsätzlich angebotenes und vorgesehenes Verfahren zur Verschlüsselung des E-Mail-Verkehrs zwischen der SAB und den Antragstellern weitgehend auf Unverständnis stoße und nicht angenommen werde. Die entsprechende Einwilligungserklärung mit dem monierten Inhalt werde aber nicht mehr verwendet, da das Formular inhaltlich den Anschein erweckt habe, dass das Verfahren eine unverschlüsselte E-Mail-Beantragung erfordere, so dass eine Freiwilligkeit der Einwilligung in den unverschlüsselten E-Mail-Verkehr nicht erkennbar gewesen sei. Daher sei das Formular aus dem Internet entfernt worden. Das Angebot, eine

Einwilligungserklärung für unverschlüsselten E-Mail-Verkehr zwischen der SAB und dem Antragsteller anzubieten, wolle die SAB jedoch beibehalten.

Ich habe die SAB darauf hingewiesen, dass bei einer Mittelbeantragung per E-Mail, an einem sicheren Verfahren mit Verschlüsselung festzuhalten sei und der sicheren Kommunikation Vorrang zu geben ist. Wünscht ein Antragsteller abweichend davon ausdrücklich, das vorgesehene Verschlüsselungsverfahren nicht zu nutzen, sind bei der sodann einzufordernden Einwilligungserklärung für einen unverschlüsselten E-Mail-Verkehr mit der SAB die datenschutzrechtlichen Vorgaben nach § 4 Abs. 3 bis 5 SächsDSG einzuhalten.

7 Kultus

7.1 Handlungsfeld: Datenschutz als ein Teil der Medienbildung

In unserer Informationsgesellschaft hat die Medienbildung ein außerordentliches Gewicht erlangt. Der Umgang mit modernen Medien steht mittlerweile in unserer sich rapide entwickelnden Zeit auf einer Stufe mit den althergebrachten Grundfertigkeiten Lesen, Schreiben und Rechnen. Idealerweise werden die Schüler durch eine gelungene Medienbildung dazu in die Lage versetzt, 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. Im Berichtszeitraum arbeitete ich daher verstärkt an der Frage, wie der Datenschutz als ein Teil der Medienbildung nachhaltig und systematisch in die Schullandschaft des Freistaates Sachsen integriert werden kann. In Kooperation mit den für Medienbildung zuständigen Referaten des Kultusministeriums, der Sächsischen Bildungsagentur, des Sächsischen Bildungsinstitutes und den Medienpädagogischen Zentren der Sächsischen Bildungsagentur führte ich eine Reihe von Schulungen zu Medienbildung und Datenschutz in der Schule durch. Beispielhaft seien die Schulungen in Beruflichen Schulzentren genannt, bei denen neben den Rechtsgrundlagen und Grundprinzipien des allgemeinen und schulischen Datenschutzrechts auch Lösungen angeboten wurden, wie die Vermittlung von Themen, z. B. die Funktionsbedingungen des digitalen Zeitalters, die Sensibilisierung für die Risiken, die Vermittlung der Datenschutzrechte und der Möglichkeiten, sich im Netz selbst helfen zu können, im Unterricht erfolgen kann.

In den zurückliegenden Jahren wurden auf Bundes- und Länderebene zunehmend Anstrengungen zur Förderung der Medienbildung unternommen - in der Politik, in der Wissenschaft und selbstverständlich auch in den Schulen.

Dazu gehören die Beschlüsse der Kultusministerkonferenz, die 1995 zur Medienpädagogik Stellung genommen hat, 2012 zur Medienbildung und 2013 zur Verbraucherbildung und die im September 2015 eine Fachtagung zur Umsetzung des Beschlusses über die schulische Medienbildung in den Ländern durchführen wird. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder plädierte bereits 2008 und 2011 dafür, die Sensibilisierung für den Schutz personenbezogener Daten als wesentliche Bildungsaufgabe und ein Element der Medienbildung der allgemeinen und beruflichen Bildung zu begreifen. Zur Unterstützung und im Hinblick auf den dringenden Handlungsbedarf haben die Datenschutzbeauftragten der Länder gemeinsam das Jugendportal www.Youngdata.de freigeschaltet.

Der Freistaat Sachsen hat als eines von wenigen Bundesländern die wichtige und richtige grundlegende Entscheidung getroffen, dem Schulfach Informatik in der Sekundarstufe einen festen Platz in der Stundentafel zu geben. Innerhalb des Faches Informatik werden bereits jetzt datenschutzrechtliche Aspekte mit zumeist technischem Ansatz vermittelt. Fachübergreifend haben Bezüge des Datenschutzes in den Fächern Gesellschaftskunde, Ethik und Deutsch Berücksichtigung gefunden. Dort ist die Vermittlung der Themen wie der „Gläserne Bürger“ oder das „Recht auf informationelle Selbstbestimmung“ Bestandteil der Lehrpläne.

Die Anforderungen der schulischen Medienbildung fanden auch Eingang in die Ausgestaltung der schulischen Infrastruktur und Ausstattung. Die sächsischen Lernplattformen MeSAX und LernSAX gelten bundesweit als Vorbilder. Datenschutzthemen wurden Bestandteil in der Lehreraus- und -fortbildung, in curricularen Vorgaben und natürlich auch in unzähligen Schulprojekten oder dem jährlich stattfindenden „Safer Internet Day“.

Medienbildung ist keine zu erledigende Aufgabe. Medienbildung ist ein Prozess, der zahlreiche Handlungsfelder umfasst. Der Datenschutz ist didaktisches Handlungsfeld der Medienbildung und gleichzeitig eine Anforderung an deren Ausgestaltung. Medienbildung geht permanent mit der Verarbeitung personenbezogener Daten einher. Dabei handelt es sich um die personenbezogenen Daten sowohl der Lehrer als auch der Schüler. Diese Verarbeitung der personenbezogenen Daten durch die Schulen bedarf einer in rechtlicher und technischer Hinsicht sicheren Infrastruktur und einer Ausstattung, in der Lehrer künftig in Chats oder virtuellen Lernräumen Wissen vermitteln und Nachrichten sicher sowohl mit der Schulverwaltung, aber auch mit den Eltern und Schülern austauschen können.

Die Aus- und Fortbildung der Lehrer soll diese in die Lage versetzen, das Thema Datenschutz in der erforderlichen Breite und Tiefe den Schülern vermitteln zu können. Um die Lehrer bei der Vermittlung der datenschutzrechtlichen Themen fachlich zu unterstützen, bietet sich das Angebot von vorbereitetem Lehrmaterial in Modulform an.

Eine breit angelegte Bildungsoffensive Medienbildung im Zusammenspiel mit dem von der Kultusministerkonferenz empfohlenen Bildungsmonitoring kann eine gute Grundlage für die Weiterentwicklung der Medienbildung sein, die dafür sorgt, dass im Freistaat Sachsen Lehrende und Lernende gleichermaßen gut und erfolgreich in unserer digitalisierten Zeit bestehen können. Was den Teil des Datenschutzes angeht, ist es mir ein wichtiges Anliegen diesen Prozess zu unterstützen.

7.2 Verbesserungsbedürftige Schulordnungen

Bereits seit geraumer Zeit befinde ich mich mit dem SMK in Kontakt, um die verschiedenen Schulordnungen zu harmonisieren.

Die diversen Schulordnungen sehen zum Teil nicht nachvollziehbare und uneinheitliche Datenerhebungen vor. Zum Teil werden die Staatsangehörigkeit sowie „Telefonnummern und Notfalladressen“ verpflichtend erhoben. Kontaktdaten wie Rufnummern und weitere Adressen wird man nur auf freiwilliger Grundlage zu verlangen berechtigt sein. Auch das Datum „Religionszugehörigkeit“ wird nicht auf die Wahrnehmung des entsprechenden Unterrichts beschränkt. Bei der Unterrichtsplanung spielt wegen der Wahlfreiheit der Fächer katholische Religion, evangelische Religion und Ethikunterricht für die Schüler die Religionszugehörigkeit eigentlich keinerlei Rolle. Weiterhin wird (nur) an Berufsfachschulen ein Status als „Spätaussiedler“ erwähnt. Erhoben werden kann darüber hinaus Art und Grad einer Behinderung sowie chronische Krankheiten, aber nur teilweise mit der erforderlichen Einschränkung „soweit sie für die Ausbildung von Bedeutung sind“.

Im Berichtszeitraum wurde ich vom SMK zum Entwurf einer Verordnung zur Änderung der Schulordnung Grundschulen und der Schulgesundheitspflegeverordnung (SOGS-E) angehört.

Neben grund- und förderschulrechtlichen Hinweisen wies ich das SMK auf die grundsätzliche Problematik der Verarbeitung des Datums des „Migrationshintergrundes“ hin. Die Erhebung personenbezogener Daten im Zusammenhang mit einem „Migrationshintergrund“, die bei den Schularten versucht wird, ist aus datenschutzrechtlicher Sicht kritisch zu bewerten.

Gründe dafür sind:

1. Die Daten zu einem Migrationshintergrund fallen ggf. als besonders zu schützende Daten unter die Regelungen des § 4 Abs. 2 SächsDSG. Die Vorschrift bestimmt, dass die Verarbeitung personenbezogener Daten, aus denen die rassische oder ethnische Herkunft hervorgeht, nur zulässig ist, wenn aus Gründen eines wichtigen öffentlichen Interesses eine Rechtsvorschrift dies ausdrücklich vorsieht oder zwingend voraussetzt. Ein wichtiges öffentliches Interesse ist aber weder begründet worden, noch ist der unbestimmte Begriff per Gesetz definiert worden.

   Auch der vorgelegte Entwurf der Grundschulverordnung enthielt keine Datenerhebungs- und Datenverarbeitungsbefugnis für Informationen im Zusammenhang mit

einem „Migrationshintergrund“. Um Inhalt, Umfang und Tiefe der Datenverarbeitung hinreichend zu bestimmen, hätten die für die Ermittlung/Beurteilung eines „Migrationshintergrundes“ erforderlichen Daten in § 3 Abs. 6 SOGS-E konkret genannt und abschließend aufgezählt werden müssen.

2. Die Formulierung „mit Migrationshintergrund“ entsprach nicht dem Grundsatz der Normenklarheit, da es sich bei der Formulierung um einen unbestimmten Rechtsbegriff handelte und damit nicht hinreichend geregelt wird, welche Kinder tatsächlich gemeint sind. Der mit dem Mikrozensus 2005 auch im Bereich der amtlichen Statistik genutzte Begriff diente der Beschreibung einer Bevölkerungsgruppe, die aus seit 1949 eingewanderten Personen und deren Nachkommen besteht. Eine andere Definition wurde für den Bereich der Bundesagentur für Arbeit in der Migrationshintergrund-Erhebungsverordnung vom 29. September 2010 getroffen.

   Hinzu kommt, dass bei einer flächendeckenden Erhebung der Daten von Kindern mit sogenannten „Migrationshintergrund“ gravierend gegen die datenschutzrechtlichen Grundsätze der Datensparsamkeit, der Erforderlichkeit und der Verhältnismäßigkeit verstoßen wird, da nur ein kleiner Anteil dieser Personengruppe tatsächlich Adressat der Bildungsberatung und der weiteren Angebote (Vorbereitungsklasse, Vorbereitungsgruppen oder zusätzlichem Unterricht im Fach Deutsch als Zweitsprache) sein sollen. Nur diese schulbezogenen Gründe könnten aber Grund für eine Erhebung des Datums sein.

   Da der Begriff „mit Migrationshintergrund“ aus den vorgenannten Gründen ungeeignet ist, schlug ich dem SMK vor, die Formulierung der vormals geltenden Fassung der Verordnung: „Für Kinder mit Deutsch als Zweitsprache, die einer besonderen Sprachförderung bedürfen…“ weiter zu nutzen bzw. ggf. zu ergänzen.

Diesem Vorschlag folgte das zuständige Ministerium nicht, mit der Begründung, dass die Belegung des Faches nur eine von verschiedenen Integrationsmaßnahmen darstelle und deshalb zu kurz greifen würde. Welche weiteren Integrationsmaßnahmen dies wären, ließ das SMK allerdings offen. Stattdessen teilte mir das SMK in seiner Erwiderung mit, dass Schüler mit Migrationshintergrund gemäß einer zwischen dem SMK und dem Statistischen Landesamt abgestimmten Definition jene Schüler seien, die zwei- oder mehrsprachig aufwachsen oder die selbst oder deren Eltern (bzw. ein Elternteil) oder Großeltern nach Deutschland zugewandert seien, ungeachtet ihrer gegenwärtigen Staatsangehörigkeit und ungeachtet des Aufenthaltsstatus (eine zeitliche Begrenzung gebe es nicht). Gleichzeitig wurde darauf hingewiesen, dass es sich um eine freiwillige Angabe handeln würde und keine Verarbeitung personenbezogener Daten darstelle, aus denen die rassische oder ethnische Herkunft hervorgehen würde.

Anhand der nachfolgend durch das SMK übersandten Definition des Migrationshintergrundes des Statistischen Landesamtes wurden allerdings die Ungenauigkeiten der zugrunde liegenden Definition und unterschiedlichen Nutzung des Datums deutlich. Während das SMK davon ausgeht, dass die Herkunft der Eltern für das Vorliegen eines Migrationshintergrundes nicht relevant sei, stellt das Statistische Landesamt darauf ab, ob der Schüler oder dessen Eltern oder Großeltern nach Deutschland zugewandert sind. Für den Kultusbereich sei ausschließlich die vorhandene Mehrsprachigkeit für die angebotene Förderung ausschlaggebend. Meine Erfahrungen aus den sächsischen Schulen zeigen, dass die angegebene Definition zur Feststellung eines Migrationshintergrundes nicht bekannt ist. Da diese aber vor der Aufgabe stehen, entsprechende Daten zu verarbeiten, regte ich erneut an, eine entsprechende Regelung und Definition in die Schulordnungen aufzunehmen.

Im Hinblick auf die Bedeutung der Angelegenheit wies ich das zuständige Fachreferat mehrfach auf den bestehenden Handlungsbedarf in dieser Frage hin. Leider ging das SMK in seinem Schreiben nicht auf meine Forderung ein, den Migrationshintergrund in den Katalog der in den jeweiligen Schulordnungen zu erhebenden Daten aufzunehmen.

Eine Rechtsgrundlage zur Speicherung eines Migrationshintergrundes und dessen präzise Definition in den Schulordnungen fehlen damit. Entsprechende Datenverarbeitungen, soweit sie nicht *unmittelbar* einer geeigneten Integrationsmaßnahme dienen, betrachte ich als rechtswidrig.

7.3 Datenverarbeitung im Rahmen eines Antrags auf Ruhen der Schulpflicht

Im letzten Berichtszeitraum beanstandete ich die Datenverarbeitung durch das Gesundheits- und Jugendamt eines Landratsamtes.

Petenten wiesen mich darauf hin, dass das Gesundheitsamt eines Landkreises umfangreiche Befunddaten aus der Untersuchung zur Schulfähigkeit an eine (damalige) Mittelschule übermittelt hat. Eine daraufhin durchgeführte Kontrolle ergab, dass die Übermittlung von Befunddaten aus Schuluntersuchungen bei dem Gesundheitsamt gängige Praxis gewesen und trotz meiner Hinweise zur ärztlichen Schweigepflicht weiterhin als rechtmäßig angesehen worden ist. In diesem Zusammenhang wurde mir auch mitgeteilt, dass bei Schweigepflichtentbindungserklärungen mit Kindern als Betroffenen die Unterschrift eines Elternteils als ausreichend angesehen wird und das entsprechende Formular daher auch nur eine Unterschrift vorsehe.

In dem in diesem Zusammenhang ebenfalls kontrollierten Jugendamt ist eine Schweigepflichtentbindungserklärung verwendet worden, in der zwar beide Eltern vorgesehen sind, aber neben „Einrichtung/Schule“, „Jugendamt“, „dem Maßnahmeträger“ auch „Sonstige“ von ihrer Schweigepflicht entbunden und „Unterlagen, Einschätzungen, Gutachten u. Ä. zur Entscheidungsfindung bezüglich der laufenden Hilfegewährung gemäß § 27 ff. SGB VIII *zur Verfügung gestellt*“ werden können.

Die während der Kontrolle geäußerten rechtlichen Bedenken gegen deren Verwendung wurden ausdrücklich nicht geteilt.

Das von mir zwischenzeitlich beteiligte SMS teilte hingegen meine rechtlichen Bedenken. Aber auch dies überzeugte das Landratsamt nicht. Es unterstellte vielmehr dem SMS, nur sehr begrenzt mit den praktischen Arbeitsabläufen im Gesundheitsamt und den damit verbundenen Problemen vertraut zu sein.

Die dargestellten Verarbeitungen personenbezogener Daten stellten gravierende Datenschutzverstöße dar. Bei der Erstellung eines amtsärztlichen Zeugnisses nach § 2 Abs. 3 SBO ist sich auf allgemeine Angaben, z. B. „aus gesundheitlichen Gründen“ zu beschränken. Es ist, anders als vom Gesundheitsamt behauptet und auch im vorliegenden Beispiel praktiziert, keine umfangreiche Übermittlung von Gesundheitsdaten vorzunehmen. Gesundheitsdaten dürfen nach dem Sächsischen Datenschutzgesetz als besonders schützenswerte Daten vielmehr nur unter erschwerten Voraussetzungen verarbeitet werden. Gemäß § 4 Abs. 2 SächsDSG ist ihre Verarbeitung u. a. zulässig, wenn aus Gründen eines wichtigen öffentlichen Interesses eine besondere Rechtsvorschrift dies ausdrücklich vorsieht oder zwingend voraussetzt. Die Voraussetzungen des § 4 Abs. 2 SächsDSG waren im vorliegenden Fall nicht erfüllt. Es ist lediglich der Grund des Fernbleibens vom Unterricht, hier z. B. „aus gesundheitlichen Gründen“, zur Gewährleistung der Schulpflicht gemäß § 26 SchulG erforderlich.

Vom Einverständnis des jeweils anderen Elternteils kann gemäß § 1626 BGB nicht generell ausgegangen werden. Es ist anzunehmen, dass es zu umfangreichen Übermittlungen von Gesundheitsdaten ohne wirksame Schweigepflichtentbindungserklärung gekommen ist.

Das durch das Jugendamt verwendete Formular wiederum war wegen seiner Unbestimmtheit unwirksam. Eine Einwilligung muss, um wirksam zu sein, informiert erfolgen. Wer die Einwilligung des Betroffenen einholt, hat diesen gemäß § 4 Abs. 3 SächsDSG zuvor in geeigneter Weise über die beabsichtigte Datenverarbeitung und ihren Zweck sowie die Empfänger vorgesehener Übermittlungen aufzuklären. Davon kann bei einer „zur Verfügung Stellung“ für „Sonstige“ jedoch keine Rede sein. Weder

ist der Adressat der Erklärung zum Zeitpunkt der Unterschrift bestimmbar, noch lässt ein „zur Verfügung stellen“ eindeutige Rückschlüsse zu, ob es sich um eine Erhebung oder Übermittlung durch das Jugendamt handeln soll. Auch ist eine Möglichkeit, die Entbindung bzw. Einwilligung auf bestimmte Ärzte bzw. Stellen und bestimmte Unterlagen zu begrenzen, nicht vorgesehen.

Nach meiner Beanstandung wurde mir zugesichert, dass die festgestellten Datenschutzverstöße abgestellt werden und mir auf Nachfrage die - nunmehr datenschutzgerecht überarbeiteten - Formulare zugesandt.

Ich habe dies alles zum Anlass genommen, sämtliche Landratsämter anzuschreiben und um Übersendung der verwendeten Formulare zu bitten. Leider ist das beanstandete Landratsamt kein Einzelfall. Vielmehr werden in nahezu sämtlichen Landkreisen unwirksame Einwilligungserklärungen verwendet. Ich habe mich mit dem Vorschlag an das SMS gewandt, bei der Erstellung von entsprechenden Mustern behilflich zu sein.

7.4 Bekanntgabe von Zensuren im Klassenverband

Ein Elternteil wandte sich an mich, dessen Kind berichtete, dass die Zensuren vor der Klasse vorgelesen worden seien. Mir wurde die Ansicht entgegengehalten, dass ein generelles Vorlesen der Zensuren aus datenschutzrechtlichen Gründen nicht erlaubt sei, da die Bewertung einer Schülerleistung zu den zu schützenden personenbezogenen Daten der Schüler gehöre. Ferner wurde der Standpunkt vertreten, dass die Nennung der Bewertung einer Schülerleistung in Verbindung mit dem zugehörigen Schüler vor der Klasse nur in einem engen Rahmen, zum Beispiel als besondere Würdigung im positiven Sinn, zulässig sei. Ein regelmäßiges Vortragen der Bewertungen, insbesondere auch der schlechten Zensuren sei hingegen nicht statthaft, dies auch vor dem Hintergrund, dass z. B. einer - ungewollten - Herabwürdigung von Schülern vorzubeugen sei. Um einen pädagogischen Anreiz zu schaffen, sei ein Notenspiegel ausreichend. Die Schulleitung hingegen vertrat die Meinung, dass es sich nicht um die Weitergabe von personenbezogenen Daten handele, sondern um eine schulinterne Bekanntgabe. Sie verwies auf die pädagogische Funktion im Klassenverband und darauf, dass der Schüler seine Leistungen im Klassenverband vergleichend einordnen können müsse.

Ich teilte dem Betroffenen mit, dass nach meiner Überzeugung die Nennung der Zensuren einzelner Schüler im Rahmen der Verhältnismäßigkeit und bei pädagogischer Notwendigkeit im Rahmen des Bildungsauftrags der Schule statthaft sei. Ferner vertrat ich den Standpunkt, dass die Bekanntgabe von Zensuren vor der Klasse im Einzelfall durch den Lehrer in eigener pädagogischer Verantwortung zu entscheiden sei. Maßgebend sei

hierbei für die Lehrkraft, ob die Nennung pädagogisch zweckmäßig bzw. notwendig sei. Ob die Bekanntgabe im Unterricht vor der Klasse oder etwa in Einzelgesprächen mit den Schülern vorzunehmen ist, mag zudem auch abhängig von der jeweiligen Klassendynamik sein. Auch wenn es eine ausdrückliche Verpflichtung zur Bekanntgabe von Zensuren vor der Klasse nicht gibt, ist unter dem Gesichtspunkt der Gleichmäßigkeit und Fairness von Bewertungen sowohl gegenüber den Schülern als auch gegenüber den Elternsorgeberechtigten eine Notwendigkeit anzuerkennen, dass eine notwendige Transparenz, was Einschätzungen des Lehrers und den Leistungsstand in der Klasse betrifft, hergestellt wird.

Bei seiner einzelfallbezogenen Entscheidung wird der Lehrer nach gesetzmäßigem Ermessen im besonderen Gewaltverhältnis der Schule zum Schüler abzuwägen haben, ob es aufgrund der konkreten Klassensituation und aus pädagogischer Sicht erforderlich ist, die Noten entweder vor der Klasse oder im Einzelgespräch bekanntzugeben oder ob datenschutzfreundlicher vorgegangen werden kann. So ist auch zu überlegen, inwieweit bei schriftlichen Leistungskontrollen ein Klassenspiegel genügen mag. Bei mündlichen Leistungskontrollen wird es hingegen eher regelmäßig erforderlich sein, die Bewertung der jeweiligen Einzelleistung anderen Schülern gegenüber zu offenbaren, da nur auf diese Weise die Schüler nachzuvollziehen in der Lage sein werden, was und inwieweit der Lehrer positiv oder negativ gewichtet und das eigene Leistungsvermögen dazu in Relation zu setzen. Dies wird ebenso für Gesamtnoten und deren Zusammensetzung gelten, denn nur durch eine transparente Nachvollziehbarkeit der Bewertung in Bezug auf Einzel- und Gesamtleistungen wird eine Maßstäblichkeit in der Bewertung des Lehrers vermittelt werden können.

Soweit eine Lehrkraft unter Berücksichtigung der oben genannten Ausführungen die Bekanntgabe vor der Klasse für erforderlich hält, hat diese in einer Art und Weise zu erfolgen, dass auch schlechte Schüler gegenüber den Mitschülern nicht zurückgesetzt werden, d. h. dass keine unbilligen und für die Schüler nicht zumutbaren Entäußerungen durch Lehrkräfte erfolgen dürfen. Die Lehrkräfte sind trotz und gerade wegen des besonderen Gewaltverhältnisses, dem die Schüler im Schulverhältnis unterworfen sind, gerade nicht frei in ihrem Handeln. Ihnen ist auch die Sorge für die Schüler anvertraut. So sind (ehr-)verletzende Entäußerungen, Häme und Erniedrigungen im Zusammenhang mit schwachen Schülerleistungen Überschreitungen, die auch datenschutzrechtlich Verstöße darstellen können. Nicht ausgeschlossen sind gleichwohl auch als unangenehm empfundene oder berührende sachliche Offenbarungen in Bezug auf den Leistungsstand des einzelnen Schülers.

Zu der Bekanntgabe des Zensurenspiegels und des Klassendurchschnitts hatte ich mich bereits im fünften Tätigkeitsbericht geäußert und diesen für zulässig angesehen (vgl.

5/7.3). Was Offenbarungen außerhalb des Klassenverbandes und in der Öffentlichkeit betrifft, hatte ich mich zu der Unzulässigkeit bereits im neunten Tätigkeitsbericht geäußert (vgl. 9/7.6).

7.5 Berufspotentialanalyse durch „Praxisberater“ - Informationsaustausch zwischen Arbeitsverwaltung und Schulen zu Zwecken der Berufs- und Studienorientierung

Der Presse konnte ich im Berichtszeitraum entnehmen, dass ein vom SMK zusammen mit der Bundesagentur für Arbeit entwickeltes Projekt „Praxisberater“ begonnen hatte. In Sachsen beteiligten sich 50 der 281 Oberschulen daran. Das Vorhaben sah vor, dass ein Profil der einzelnen Schüler gebildet werden sollte, das einer Beratung zur Berufs- und Studienorientierung durch sogenannte „Praxisberater“ dienen sollte.

Um die Erforderlichkeit und Zulässigkeit der Erhebung von Daten der Schüler in diesem Zusammenhang zur Erfüllung der gesetzlichen Aufgaben der Schulen zu überprüfen, bat ich das SMK um Stellungnahme. Von Interesse waren neben der Verarbeitung der Schülerdaten die Gestaltung der Einwilligungserklärung und der geplante Datenaustausch zwischen Arbeitsverwaltung und Schule. Auf Grundlage der mir daraufhin übersandten Unterlagen und geführter Gespräche war meine Behörde imstande, eine rechtliche Einordnung der Informationsflüsse und des Verfahrens des Projektes vorzunehmen. Die beteiligten Praxisberater selbst, die von der Bundesagentur für Arbeit beauftragt werden, sind wegen ihrer vertraglichen Bindung als Teil der Arbeitsverwaltung anzusehen gewesen und unterliegen damit - wie die (Bundes-)Arbeitsverwaltung selbst auch - nicht dem Sächsischen Datenschutzgesetz und meiner Kontrollbefugnis. Eine Rechtsgrundlage für einen Austausch von Potentialdaten zu Schülern zwischen dem Praxisberater als Teil der Arbeitsverwaltung, der Schulleitung, Lehrern und Eltern fehlte jedoch.

Die Kultusverwaltung versicherte mir, dass bei der Berufspotentialanalyse ausschließlich unter der Voraussetzung des Vorliegens der Einwilligung der Eltern und ggf. der Schüler Daten aus dem Projekt heraus an die Schule übermittelt werden würden. Auch bei Vorliegen der Einwilligungserklärung finde kein allgemeiner mündlicher oder schriftlicher Informationsaustausch zwischen den Schulen und dem Praxisberater bzw. den Schülern statt.

In dem Prozess führt der Praxisberater eine Potentialanalyse durch, bei der Stärken oder Handlungsbedarf in den Bereichen „Sozialkompetenz“, „Methodenkompetenz“, „personalen Kompetenz“ und „arbeitspraktischer Basiskompetenz“ des Schülers ermittelt wer-

den. Darauf folgt eine persönliche Auswertung zwischen dem Praxisberater, dem Schüler und ggf. den Elternsorgeberechtigten. Der persönliche Auswertungsbogen verbleibt mit einem Exemplar beim Praxisberater. Ein zweites Exemplar erhält der Schüler und dessen Elternsorgeberechtigten zur persönlichen Verwendung.

Bei erfolgter Einwilligung kann auf der Grundlage des persönlichen Auswertungsbogens in einem weiteren Schritt ein sogenannten „Entwicklungsplan“ gemeinsam mit der Schule erarbeitet werden. Erst in diesem Fall werden erhobene personenbezogene Daten der Schüler aus der Potentialanalyse an die Schule übermittelt. Bei der Erarbeitung des Entwicklungsplans werden die Ergebnisse der Potentialanalyse des Schülers gemeinsam mit dem Praxisberater, den Erziehungsberechtigten und dem Klassenlehrer um Ziele und Maßnahmen ergänzt.

Wie bereits angemerkt, mangelt es allerdings an einer Erhebungsbefugnis der Potentialdaten seitens der Schule. Deswegen habe ich mit dem SMK für die Übermittlung der Daten an die Schule eine gesonderte weitere Einwilligungserklärung erarbeitet. Dabei war insbesondere drauf zu achten gewesen, dass die Schüler zum überwiegenden Teil noch nicht volljährig sind. In diesen Fällen ist die Einwilligung der gesetzlichen Vertreter, in der Regel der Eltern, erforderlich. Bei 14-jährigen oder älteren minderjährigen Schülern, die im datenschutzrechtlichen Sinn einwilligungsfähig sind, rate ich dazu, zwei Einwilligungen einzuholen, die des Schülers und die der Elternsorgeberechtigten.

Die Unterzeichnung der Einverständniserklärung zur Teilnahme am Projekt „Praxisberater an Schulen“ und die Einwilligung zur Weitergabe von personenbezogenen Daten sind freiwillig und können jederzeit mit Wirkung für die Zukunft widerrufen werden. Sollte von dieser Widerrufsmöglichkeit Gebrauch gemacht werden, werden die erhobenen personenbezogenen Daten durch den Praxisberater, ggf. den Klassenlehrer, ggf. den Berufsberater der Agentur für Arbeit, unverzüglich gelöscht bzw. vernichtet. Eine (weitere) Teilnahme an der Maßnahme ist bei Widerruf der Einwilligung zur Weitergabe von personenbezogenen Daten an den Berufsberater der Agentur für Arbeit allerdings nicht möglich.

Wichtig war eine Regelung zur Löschung der im Projekt erhobenen Daten. Zugesichert wurde mir, dass die Daten nach Ablauf von zwei Jahren nach Ende der Teilnahme an der Maßnahme bzw. mit Verlassen der Schule gelöscht werden. Da die Maßnahme am Ende der Klassenstufe 8 endet, werden die Daten damit spätestens am 31. Juli des jeweiligen Jahres in der Klassenstufe 10 gelöscht.

Ich werde das Verfahren der Berufspotentialanalyse gemäß § 27 SächsDSG stichprobenartig kontrollieren.

7.6 Veröffentlichung personenbezogener Daten über die Schuldatenbank des Freistaates Sachsen via Internet

Eine Elternvertreterin teilte mir mit, dass ihr Name im Zusammenhang mit ihrer Funktion als stellvertretender Elternratsvorsitzenden ohne ihr Einverständnis in der über das Internet verbreiteten „Schuldatenbank Sachsen“ veröffentlicht worden sei, und bat mich um Unterstützung bei der Entfernung ihres Namens aus dieser Datenbank.

Ich habe diesen Hinweis zum Anlass genommen, das Schulportal wegen der Veröffentlichung personenbezogener Daten von Eltern- und Schülervertretern insgesamt datenschutzrechtlich zu prüfen. Hierfür wurde die für die Datenbank zuständige Stelle, das SMK um Stellungnahme gebeten. Ich erhielt die Auskunft, dass es von Anfang an beabsichtigt gewesen sei, die personenbezogenen Daten nur mit Einwilligung der jeweiligen Vertreter im Internet zu veröffentlichen. Die Schulleiter aller sächsischen Schulen in öffentlicher Trägerschaft waren von der Kultusverwaltung angehalten, die Einwilligung der Eltern- und Schülervertreter vor Veröffentlichung der personenbezogenen Daten einzuholen. Die Erhebung der Daten der Eltern- und Schülervertreter der Schule erfolgt nach Information der Kultusverwaltung in der Sächsischen Schulverwaltungssoftware (SaxSVS) an der Schule. Die Daten seien dann in der Sächsischen Schuldatenbank/ Schulporträt der jeweiligen Schule übertragen worden. Bei der automatisierten Einspeisung der Daten sei der Fall, dass die Einwilligung der Eltern- und Schülervertreter nicht vorliegt, fehlerhafter Weise bisher nicht vorgesehen gewesen.

Um Veröffentlichungen personenbezogener Daten in der Sächsischen Schuldatenbank/ Schulporträt ohne vorliegende Einwilligungserklärung in Zukunft zu vermeiden, wurde mir eine Änderung des Verfahrens seitens des SMK zugesichert.

Zukünftig habe die Schule beim Eintragen in SaxSVS auszuwählen zwischen

- Elternsprecher ohne Einwilligung oder
- Elternsprecher mit Einwilligung bzw.
- Schülersprecher ohne Einwilligung/ohne Einwilligung der Erziehungsberechtigten oder
- Schülersprecher mit Einwilligung/Einwilligung der Erziehungsberechtigten.

In der Exportdatei für die für das Internet vorgesehene Sächsische Schuldatenbank/ Schulporträt sollen dann nur noch die Daten mit dem Merkmal „mit Einwilligung“ enthalten sein.

Eine Einwilligungserklärung für die Internetveröffentlichung soll den Schulleitern im Downloadbereich des Schulportals zur Verfügung gestellt werden. Zusätzlich wurden alle Schulleiter öffentlicher Schulen sowie die Sächsische Bildungsagentur über die vorgesehene Einwilligungserklärung und über die veränderte Verfahrensweise bei der Erfassung in SaxSVS eigens informiert.

Für die Entfernung des Namens der Betroffenen und anfragenden Elternvertreterin aus der Datenbank konnte diese auf der Internetseite „Schuldatenbank Sachsen“ unter „Hilfe und Kontakt“ das Kontaktformular für Anfragen und Hilfe nutzen und die Löschung ihrer namensbezogenen Nennung als Elternvertreterin ihrer Schule verlangen.

7.7 E-Mail-Adressen für Lehrer

Bereits seit geraumer Zeit befinde ich mich mit dem SMK in Kontakt, damit dieses Ressort seinen Bediensteten im Schuldienst (und nicht zuletzt den schulischen Datenschutzbeauftragten) ermöglicht, rechtskonform per dienstlicher E-Mail zu kommunizieren

Die Verwaltungsvorschrift Schuldatenschutz untersagt seit 2007 den unverschlüsselten Versand personenbezogener Daten via E-Mail. Dennoch vermochte es die Schulverwaltung bisher nicht, dafür Sorge zu tragen, dass allen Lehrern dienstliche E-Mail-Adressen zur Verfügung gestellt werden, mit denen auch mit Personen außerhalb der Schulverwaltung kommuniziert werden kann. Dies ist bisher allein der Schulleitung vorbehalten. Lehrer, die beispielsweise mit Eltern elektronisch kommunizieren wollen, verwenden in der behördlichen Praxis daher überwiegend private E-Mail-Adressen. Nachdem nun auch § 2 Abs. 1 SächsEGovG grundsätzlich eine verschlüsselte Kommunikation fordert, sollte unverzüglich in Bezug auf die Einrichtung dienstlicher E-Mail-Adressen samt angepasster Verschlüsselungstechnik Abhilfe geschaffen werden.

8 Justiz

8.1 Jugendsünden - längst getilgt und doch verwertet

Mit einer sächsischen Staatsanwaltschaft diskutierte ich im Berichtszeitraum ein Problem, das nicht häufig, aber immer wieder auftaucht und dem aufgrund seiner Auswirkungen auf die Betroffenen eine besondere Bedeutung zukommt. Dabei handelt es sich um die Beachtung der Konsequenzen der gesetzlichen Tilgungsbestimmungen für Eintragungen im Bundeszentralregister. Es ist Ausdruck eines rechtsstaatlichen Grundprinzips und des Gedankens der Resozialisierung, dass verurteilte Rechtsverstöße nach bestimmten Fristen aus dem „staatlichen Gedächtnis“ gelöscht werden und die betroffenen Personen - auch und vor allem im Rechtsverkehr - wieder als unbescholten und nicht vorbestraft gelten. Dass es in der Praxis trotz klarer gesetzlicher Regelungen immer wieder zu widersprüchlichen Maßnahmen und Anwendungsschwierigkeiten kommt, belegen bereits Beiträge in früheren Tätigkeitsberichten (15/8.1; 13/8.4).

Der hier vorgestellte Fall nahm seinen Ausgang schon vor dem Berichtszeitraum, als gegen den Petenten ein Ermittlungsverfahren wegen Betruges eingeleitet worden war. Dazu hatte eine Anzeige einer dritten Person im Jahr 2011 bei dem Dienstherrn des Petenten, der im öffentlichen Dienst tätig war, geführt, wonach der Petent bei seiner Bewerbung um eine Stelle im öffentlichen Dienst im Jahr 1992 verschwiegen hätte, im Jahr 1980 zu einer kurzen Freiheitsstrafe verurteilt worden zu sein.

Der Petent hatte sich allerdings 1991, noch vor seiner Bewerbung, bei der Staatsanwaltschaft erkundigt, ob er noch als vorbestraft gelte und dies angeben müsse. Dort sei ihm mitgeteilt worden, dass die Strafe verbüßt, die Eintragung im Zentralregister gelöscht sei und er sich als nicht vorbestraft bezeichnen dürfe. Das Führungszeugnis des Petenten im Jahr 1992 wies keine Eintragungen auf.

Das Ermittlungsverfahren wegen Einstellungsbetruges wurde gleichwohl durch die Staatsanwaltschaft betrieben und Ende 2011 mit einer Anklage am Amtsgericht abgeschlossen. In der Anklageschrift wurde dem Petenten vorgeworfen, dass er bei seiner Bewerbung im Jahr 1992 die zum damaligen Zeitpunkt mehr als zwölf Jahre zurückliegenden Ermittlungen gegen ihn, das im Jahr 1980 gegen ihn ergangene Urteil und die dabei verhängte Haftstrafe bewusst verschwiegen hatte.

Für den Petenten folgten aus der Anklage keine strafrechtlichen Konsequenzen, das Amtsgericht hatte - allerdings aus Gründen der Verjährung - die Eröffnung des Hauptverfahrens abgelehnt, das Landgericht bestätigte diese Entscheidung.

Ich bat die Staatsanwaltschaft um Auskunft, inwieweit im Ermittlungsverfahren die Vorschriften der §§ 51 und 53 BZRG berücksichtigt worden waren - § 51 Abs. 1 BZRG lautet: „Ist die Eintragung über eine Verurteilung im Register getilgt worden oder ist sie zu tilgen, so dürfen die Tat und die Verurteilung dem Betroffenen im Rechtsverkehr nicht mehr vorgehalten und nicht zu seinem Nachteil verwertet werden“. § 53 Abs. 1 BZRG: „*Der Verurteilte darf sich als unbestraft bezeichnen und braucht den der Verurteilung zugrunde liegenden Sachverhalt nicht zu offenbaren, wenn die Verurteilung nicht in das Führungszeugnis […] aufzunehmen oder zu tilgen ist*.“

In ihrer Antwort vertrat die Staatsanwaltschaft die Auffassung, dass § 51 Abs. 1 BZRG der Verwendung der Erkenntnisse aus dem Verfahren aus den Jahren 1979/1980 nicht entgegengestanden hätte, da die Ausnahmeregelung des § 52 Abs. 1 Nr. 4 BZRG gegriffen hätte und die Tat durch die Anzeige eines Dritten bekannt geworden wäre. § 52 Abs. 1 BZRG enthält Abweichungen zum Grundsatz des Verwertungsverbots nach § 51 Abs. 1 BZRG (s. o.); nach § 52 Abs. 1 Nr. 4 BZRG darf die frühere Tat abweichend von § 51 Abs. 1 BZRG u. a. berücksichtigt werden, wenn der Betroffene die Einstellung in den öffentlichen Dienst beantragt, falls die Einstellung sonst zu einer erheblichen Gefährdung der Allgemeinheit führen würde.

Das Recht, nach § 53 Abs. 1 BZRG eine frühere Verurteilung zu verschweigen, umfasse nach Ansicht der Staatsanwaltschaft nicht das Recht, die Frage nach Ermittlungsverfahren wahrheitswidrig zu beantworten, selbst dann nicht, wenn es nur Ermittlungen gab, die zu der Verurteilung führten, die verschwiegen werden darf.

Diesen Auffassungen musste ich entschieden entgegentreten.

Das grundsätzliche Verwertungsverbot des § 51 Abs. 1 BZRG gilt selbstverständlich auch im strafrechtlichen Ermittlungsverfahren und für Staatsanwaltschaften; es betrifft jede getilgte Verurteilung nebst zugrundeliegender Tat, ganz gleich, woher die Kenntnis darüber stammt. Strafverfolgungsbehörden gehören nicht zum Adressatenkreis von § 52 Abs. 1 Nr. 4 BZRG, sie befinden in einem Ermittlungsverfahren nicht über Anträge auf Einstellung in den öffentlichen Dienst. § 52 Abs. 1 Nr. 4 BZRG hätte möglicherweise im Rahmen des Einstellungsverfahrens im Jahr 1992 durch den Dienstherrn des Petenten zur Anwendung gebracht werden können, keinesfalls aber in einem strafrechtlichen Ermittlungsverfahren im Jahr 2011 durch die Staatsanwaltschaft.

Dass die Vorschrift des § 53 Abs. 1 BZRG nur für Verurteilungen, nicht aber für diesen Verurteilungen vorausgehende Ermittlungsverfahren gelte, ist ein gravierender - und für Betroffene fataler - Irrtum über die Anwendung der Vorschrift. Die Bestimmung spricht ausdrücklich davon, dass der „*Verurteilte […] sich als unbestraft bezeichnen [darf] und*

den der Verurteilung zugrunde liegenden Sachverhalt nicht zu offenbaren [braucht]“. Wie dieser klare Gesetzeswortlaut in einem strafprozessualen Ermittlungsverfahren zu Ungunsten des Betroffenen auf eine Erlaubnis des Verschweigens lediglich der Verurteilung reduziert werden kann, war unter keinem Gesichtspunkt nachzuvollziehen. Das Verschweigensrecht des § 53 Abs. 1 BZRG erfasst, ebenso wie das Verwertungsverbot des § 51 Abs. 1 BZRG, den gesamten geschichtlichen Vorgang, der Gegenstand der Urteilsfindung war, und jede Verurteilung, durch die auf Strafe erkannt worden ist. Das umfasst zwingend auch die zur Anklage und später zur Verurteilung führenden Ermittlungen und Feststellungen. Die - umstrittene - Frage, ob Ermittlungen berücksichtigt werden dürfen, die nicht zu einer Verurteilung geführt haben, stellte sich in diesem Fall nicht.

Die in der Anklageschrift der Staatsanwaltschaft aufgeführten Anschuldigungen, die sich auf wahrheitswidrige Angaben des Petenten zu früheren gegen ihn geführten Ermittlungen, anhängigen Verfahren und gegen ihn verhängte Strafen bezogen, waren angesichts der längst vollzogenen Tilgung der Eintragung aus dem Jahr 1980 in Verletzung der datenschutzrechtlichen Vorschrift des § 51 Abs. 1 BZRG und unter grober Verkennung der Bestimmung des § 53 Abs. 1 BZRG erhoben worden, was ich der Staatsanwaltschaft mitteilte.

Die Staatsanwaltschaft sagte daraufhin zu, meine Ausführungen zu §§ 52 Abs. 1 Nr. 4 und 53 Abs. 1 BZRG bei zukünftigen Verfahren zu berücksichtigen.

8.2 Vordrucke für Schweigepflichtentbindungen in sozialgerichtlichen Verfahren

Regelmäßig erreichen mich Anfragen von Personen, die in sozialgerichtlichen Verfahren vom Gericht Vordrucke für Erklärungen zur Entbindung von Geheimhaltungs- und ärztlichen Schweigepflichten erhalten und von der großen Zahl der darin aufgeführten Behörden und sonstigen Stellen sowie Mitglieder medizinischer Berufsgruppen irritiert sind.

In derartigen Fällen weise ich die Petenten stets auf die Unzuständigkeit des Sächsischen Datenschutzbeauftragten für die Kontrolle richterlicher Handlungen zur Sachaufklärung hin (§ 27 Abs. 4 SächsDSG). Eine Prüfung der Zulässigkeit von Schweigepflichtentbindungserklärungen, die in einem am Sozialgericht anhängigen Verfahren unterzeichnet werden sollen, steht mir im Hinblick auf die Unabhängigkeit des Richters und die dementsprechende gesetzliche Beschränkung meiner Zuständigkeit nicht zu.

Allerdings sehe ich es als legitim an, im Rahmen der Ausübung meiner Beratungsfunktion nach § 30 Abs. 4 SächsDSG auch Gerichte über Verständnisschwierigkeiten von Betroffenen zu informieren, die diese mit einem durch das Gericht standardmäßig verwendeten Vordruck haben und mit denen sie an mich herantreten. Dies habe ich auch im Berichtszeitraum getan.

Aus den mich in dieser Problematik erreichenden Schreiben von Betroffenen ist ersichtlich, dass deren Unbehagen aus der global formulierten Entbindung von Geheimhaltungs- und Schweigepflichten verschiedenster Stellen und medizinischer Leistungserbringer erwächst. Der Gedanke, mit einer Unterschrift Krankenkasse, MDK, Agentur für Arbeit und derzeitige und frühere Arbeitgeber, Sozialhilfeträger, Unfallversicherungen, Rentenversicherungsträger u. a. von deren Geheimhaltungspflicht zu entbinden, verunsichert dabei ebenso wie die Vermutung, neben Ärzten auch Psychologen und Therapeuten global von deren Schweigepflicht zu befreien. Es zeigt sich - zumindest in den Äußerungen mir gegenüber -, dass gerade Betroffene mit wechselhafter Erwerbsbiographie und/oder verschiedenen zurückliegenden Krankheiten befürchten, dass mit der Unterzeichnung der Geheimhaltungs- und Schweigepflichtentbindungserklärung sämtliche Ereignisse, an denen die genannten Stellen und Berufsgruppen beteiligt waren, offenbart würden.

Ein Problem liegt meiner Erfahrung nach darin begründet, dass die Vordrucke nach einer umfangreichen Aufzählung von Stellen und Leistungserbringern die Möglichkeit bieten, im Einzelfall von Hand einzufügende und genau zu bezeichnende Stellen und Leistungserbringer von der Entbindung von Geheimhaltungs- und Schweigepflichten auszunehmen. Dadurch entsteht häufig der Eindruck, dass grundsätzlich - ohne oder mit nur begrenzter Nutzung dieser Beschränkung - Daten von sämtlichen im Vordruck genannten Stellen und Berufsgeheimnisträgern erhoben werden dürfen und an das Sozialgericht übermittelt werden.

Eine weitere Schwierigkeit besteht in einer immer wieder zu beobachtenden Scheu der Petenten, „amtliche“ Vordrucke zu verändern, bestimmte Passagen oder Listen zu streichen, zu kürzen oder mit eigenen Anmerkungen zu ergänzen.

Dass die Vordrucke der Schweigepflichtentbindungserklärungen auch die Beschränkung auf die durch das „Gericht zur Aufklärung des Sachverhalts für erforderlich gehaltenen Unterlagen“ enthalten und mithin von vornherein einen Großteil der im Vordruck genannten Stellen und Leistungserbringer als Übersender von Unterlagen gar nicht in Betracht kommen, ist den Betroffenen in aller Regel ebenso wenig bewusst wie die - im Vordruck ausdrücklich erwähnte - Möglichkeit, die Entbindung auf bestimmte Behörden bzw. Stellen oder Ärzte, Psychologen, Psychotherapeuten, medizinische Ein-

richtungen oder medizinische Unterlagen zu beschränken. Letzteres setzte allerdings den, wie oben beschrieben oft fehlenden „Mut“ voraus, vom Gericht übersandte Vordrucke zu verändern.

Die Betroffenen, die sich an mich wenden, sehen sich ganz überwiegend in einer Situation, in der sie eine Vielzahl von Stellen und Personen, die über u. U. unangenehme oder intime Angaben über sie verfügen, von deren gesetzlicher Geheimhaltungs- oder Schweigepflicht entbinden sollen, wobei sie im Zeitpunkt der Unterschrift nicht wissen, an welche der genannten Stellen in welchem Umfang welche Informationen übermitteln werden.

Gegenüber dem Landessozialgericht habe ich in einer beratenden Äußerung meine Auffassung erläutert:

Der Gesetzgeber hat sich für einen Vorrang des Schutzes von Sozial- und Patientengeheimnis gegenüber einer ungehinderten Sachaufklärung durch das Gericht entschieden - mit u. U. unangenehmen Folgen für Verfahrensbeteiligte, die geheimhaltungs- oder schweigeverpflichtete Stellen oder Personen nicht entbinden und dadurch im Rechtsstreit unterliegen. Eine aufgrund dieser Rechtslage für die Sachaufklärung notwendige Schweigepflichtentbindungserklärung sollte dann aber so gestaltet sein, dass auch der rechtsunkundige Unterzeichner ohne weiteres erkennen kann, welche Stelle(n) und Personen er im Einzelfall für das konkrete Verfahren von der Schweigepflicht entbindet.

Vordrucke, die eine Auswahl der im konkreten gerichtlichen Verfahren erforderliche(n) Stelle(n) unter den allgemein für eine Entbindung von der Geheimhaltungspflicht in Betracht kommenden Stellen leicht ermöglichen, etwa im Wege des „Ankreuzens“, wären dabei ebenso betroffenenfreundlich wie eine Aufnahme einer Alternative zur globalen Entbindung von der Schweigepflicht, bei der der Prozessbeteiligte lediglich einzelne namentlich bezeichnete medizinische Leistungserbringer von ihrer Schweigepflicht entbindet.

Meiner Einschätzung nach dürften entsprechende Modifizierungen am Vordruck das Verständnis und die Akzeptanz der Schweigepflichtentbindungserklärungen vor allem bei den betroffenen Verfahrensbeteiligten, aber auch bei den von der Schweigepflicht zu entbindenden Leistungserbringern erhöhen und die derzeit zu beobachtende Unsicherheit abbauen.

8.3 Auskunft für Gerichtsvollzieher bei der Polizei

Die Staatsregierung informierte mich im Berichtszeitraum über ihre Absicht, das Sächsische Justizgesetz u. a. um einen Auskunftsanspruch für Gerichtsvollzieher vor bestimmten Maßnahmen der Zwangsvollstreckung zu erweitern. Hintergrund waren gestiegene Zahlen von Übergriffen gegen Gerichtsvollzieher bei der Ausübung ihrer Tätigkeit, wobei es zunehmend nicht nur zu verbalen, sondern auch körperlichen Angriffen gekommen sein soll.

Nach der bisherigen Rechtslage, darin waren sich das SMJus und ich uns einig, gab es für ein Auskunftsbegehren der Gerichtsvollzieher gegenüber der Polizei keine gesetzliche Grundlage, die aber aufgrund der Eingriffsqualität einer solchen Datenübermittlung erforderlich ist.

Mit der Befugnis, vor Vollstreckungsmaßnahmen, die zu einem schwerwiegenden Eingriff bei dem Schuldner führen und daher ein hohes Konfliktpotenzial aufweisen, im Einzelfall bei der örtlich zuständigen Polizeidienststelle anzufragen, ob dort personengebundene Hinweise zu einer Gefährlichkeit oder Gewaltbereitschaft des Schuldners vorliegen, soll der Gerichtsvollzieher in die Lage versetzt werden, vor Vollstreckungsmaßnahmen ggf. geeignete Schutzvorkehrungen zu treffen und etwa um polizeiliche Begleitung zu ersuchen.

Das federführende Justizressort hat mich sehr zeitig über die Pläne informiert und die fachliche Auseinandersetzung zur Umsetzung des Vorhabens gesucht.

Meine trotz allem Verständnis für die Risiken der Gerichtsvollziehertätigkeit von Beginn an geäußerten grundsätzlichen Bedenken gegen das Vorhaben im Hinblick auf Geeignetheit und Erforderlichkeit eines gesetzlichen Auskunftsanspruchs der Gerichtsvollzieher habe ich in der Diskussion über die Gestaltung der gesetzlichen Bestimmung zurückgestellt; Schriftwechsel und Gespräche verliefen unvoreingenommen und sehr konstruktiv. Einige meiner Anregungen wurden aufgegriffen, andere nicht.

Ich begrüße, dass der Wortlaut der Datenerhebungsbefugnis der Gerichtsvollzieher im neu geschaffenen § 42a SächsJG letztendlich nicht auf den Begriff der „personenbezogenen Daten“ abstellt, sondern sich auf „personengebundene Hinweise“ bezieht. Personengebundene Hinweise sind Anmerkungen über die Gefährlichkeit oder Gewaltbereitschaft, die die Polizei bei Vorliegen bestimmter Umstände ohnehin zu Eintragungen von Personen speichert, weil diese u. U. für polizeiliche Einsätze relevant sind. Damit erübrigen sich Abwägungen und Entscheidungen der Polizei, welche Informationen in welchem Umfang bei Anfragen von Gerichtsvollziehern übermittelt werden dürfen. Die

Erhebungsbefugnis der Gerichtsvollzieher beschränkt sich auf ein einzelnes Merkmal, das zuvor - bei Vorliegen bestimmter Umstände - schon durch die Polizei festgestellt worden ist.

Erfreulich ist auch die Aufnahme einer engen Zweckbindung und der vom sonstigen Akteninhalt gesonderten Aufbewahrung der polizeilichen Auskunft in die gesetzliche Bestimmung. Letzteres ist von Bedeutung, weil auch andere am Vollstreckungsverfahren Beteiligte als der Schuldner Einsicht in die Akten des Gerichtsvollziehers beanspruchen können. Polizeiliche Erkenntnisse bzw. eine polizeiliche Wertung über einen anderen Verfahrensbeteiligten sind dabei als „verfahrensfremde“ Informationen ohne Bedeutung und dürfen mithin nicht von der Einsicht umfasst sein.

Auch die Dauer der Aufbewahrung der Auskunft von zwei Jahren erscheint angemessen.

Leider blieb es bei der Bestimmung von Vollstreckungsmaßnahmen, die zu einem schwerwiegenden Eingriff bei dem Schuldner führen, bei der Aufzählung von Regelbeispielen im nunmehr in Kraft getretenen § 42a Abs. 2 SächsJG. Meinem Vorschlag, die Anlässe, wegen derer ein Gerichtsvollzieher bei der Polizei personenbezogene Daten erheben darf, abschließend zu bestimmen, wurde nicht gefolgt. Das Risiko einer unangemessenen Ausweitung der Abfragemöglichkeit wurde offenkundig als hinnehmbar erachtet.

Insgesamt erscheint die Regelung als angemessener Ausgleich zwischen dem Interesse der Gerichtsvollzieher, mit ihrer hoheitlichen Tätigkeit ungefährdet ihrem gesetzlichen Auftrag nachzukommen, und dem Recht betroffener Schuldner auf informationelle Selbstbestimmung.

Die in § 42a Abs. 4 SächsJG gesetzlich vorgesehene Befristung der Abfragebefugnis eröffnet die Möglichkeit, anhand der ebenfalls gesetzlich vorgeschriebenen Evaluierung zu prüfen, ob das mit der Einführung der Bestimmung bezweckte Ziel erreicht wurde. Bereits Ende nächsten Jahres werden wir erfahren, ob die Vorschrift den Praxistest bestanden haben wird.

8.4 Unzureichende Anonymisierung einer veröffentlichten Gerichtsentscheidung

Im Berichtszeitraum wandte sich ein Petent an mich, der sich durch die Art und Weise der Veröffentlichung eines ihn betreffenden Urteils in seinem Recht auf informationelle Selbstbestimmung sowie seinem Steuergeheimnis verletzt sah.

Das Urteil war durch das erkennende Gericht auf mehreren nicht-öffentlichen juristischen Datenbanken veröffentlicht worden. Es enthielt u. a. Angaben zur Art der Erkrankung und dem Sterbemonat der Ehefrau des Petenten, zum Alter seiner Kinder, zur Quadratmeteranzahl seiner Wohnung, dem Zeitpunkt seiner Dissertation sowie der genauen Höhe der festgesetzten Einkommensteuer und des zu versteuernden Einkommens.

Ich habe gegenüber dem Gericht und dem Petenten wie folgt Stellung genommen: Veröffentlichungen von Gerichtsentscheidungen sind ohne Zweifel eine verfassungsunmittelbare, wichtige Aufgabe der Gerichte. Vorausgesetzt wird dabei aber allerdings die Anonymisierung der in der Entscheidung enthaltenen personenbezogenen Daten. Die Verantwortung für die Erstellung einer herausgabefähigen, d. h. insbesondere anonymisierten Fassung liegt bei der Verwaltung des Gerichts. Eine Übertragung dieser Aufgabe an nicht-öffentliche juristische Datenbanken scheidet bereits deshalb aus, weil bereits in der Übermittlung von noch personenbeziehbaren Angaben an diese eine Verletzung der Persönlichkeitsrechte des Betroffenen begründet wäre.

Im konkreten Fall verstieß die Übermittlung des völlig unzureichend anonymisierten Urteils und seine anschließende Veröffentlichung sowohl gegen das Steuergeheimnis nach § 30 AO als auch gegen § 4 Abs. 1 SächsDSG, wonach die Verarbeitung personenbezogener Daten nur zulässig ist, wenn ein Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat. Die vom Petenten beanstandete Version ermöglichte es Dritten (insbesondere früheren und aktuellen Kollegen), ihn ohne größeren Rechercheaufwand zu identifizieren. Eine rechtliche Grundlage für die Veröffentlichung der in den Urteilsfassungen enthaltenen detaillierten und einen Personenbezug ermöglichenden Angaben zum Petenten bzw. für deren Weitergabe an nicht-öffentliche Stellen zum Zweck der Veröffentlichung war nicht ersichtlich. Die Voraussetzungen von § 16 SächsDSG, wonach die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen zulässig ist, wenn sie zur Erfüllung der Aufgaben der übermittelnden Stellen erforderlich sind, lagen nicht vor, da die detaillierten, personenbeziehbaren Angaben über persönliche, sachliche und steuerliche Verhältnisse des Petenten für das Verständnis der Entscheidung nicht entscheidend waren.

Der Präsident des Gerichts räumte die nicht hinreichende Anonymisierung des Urteils unverzüglich ein und bedauerte sie. Er veranlasste umgehend die Löschung dieser Version der Entscheidung bei den betroffenen juristischen Datenbanken und ließ ihnen eine hinreichend anonymisierte Version des Urteils zukommen. Außerdem nahm er den Vorfall zum Anlass, die Richter und übrigen Bediensteten des Gerichts auf die Notwendigkeit einer strikten Wahrung des Steuergeheimnisses und des Datenschutzes bei der Veröffentlichung von Entscheidungen hinzuweisen.

Wegen der Erheblichkeit des Verstoßes gegen datenschutzrechtliche Vorschriften konnte ich dennoch nach § 29 Abs. 2 SächsDSG nicht von einer Beanstandung absehen.

8.5 Geöffnete Post aus der JVA

Im Berichtszeitraum erreichte mich das Schreiben einer jungen Frau, deren Lebensgefährte in einer sächsischen Justizvollzugsanstalt eine Freiheitsstrafe verbüßte. Sie schilderte darin, dass sie einige Zeit zuvor einen Brief ihres Freundes erhalten habe, der offenkundig schon einmal geöffnet und mit Klebeband über der Risskante wieder verschlossen worden war. Im Briefumschlag habe sich neben dem erwarteten Inhalt auch eine Kopie des aktuellen Führungsberichts der JVA über ihren Freund befunden. Auf ihre Nachfrage habe dieser allerdings angegeben, seinen Führungsbericht bzw. eine Kopie desselben nicht in den Briefumschlag gegeben zu haben.

Im Laufe der datenschutzrechtlichen Kontrolle des Vorgangs stellte sich heraus, dass der Gefangene einen Brief in einem verschlossenen Umschlag an einen Vollzugsbeamten gegeben hatte, der den Umschlag in das Postausgangsfach der Station legte. Am darauffolgenden Morgen hatte ein anderer Vollzugsbeamter den Brief zur Post gegeben und dabei bemerkt, dass der Umschlag beschädigt/offen war. Irgendwann zwischen der Übergabe des verschlossenen, unbeschädigten Briefumschlags an den Vollzugsbeamten und der Übergabe des Schreibens an die Post muss die Kopie des Führungsberichts über den Gefangenen in den Umschlag gelangt sein.

Dass der Gefangene ihn nicht selbst in den Umschlag gegeben haben kann, steht nach den Ermittlungen zum Sachverhalt fest. Er hatte lediglich eine Abschrift des Führungsberichts erhalten, die er nachweislich umgehend an die Strafvollstreckungskammer des für ihn zuständigen Gerichts übersandte. Eine Kopie des Berichts konnte er nicht gefertigt haben, da Gefangene nur auf Antrag weitere Kopien ihres Führungsberichts erhalten können. Ein entsprechender Antrag lag nicht vor; es konnte sich auch kein Bediensteter daran erinnern, eine zusätzliche Kopie gefertigt zu haben.

Die durch die JVA eingeholten dienstlichen Stellungnahmen der Vollzugsbediensteten, die im fraglichen Zeitraum Zugang zu den Aufbewahrungsorten des Briefes hatten, lieferten - wenig überraschend - keine weiteren Erkenntnisse; Manipulationen an der Post oder Briefinhalten seien nicht vorgenommen worden.

Aufgrund der klaren Zugangsberechtigungen für Bedienstete und der ebenfalls klaren Beschränkungen der Gefangenen hinsichtlich der Fertigung von Kopien (Antrag, Nachweis) und des Zugangs zu Stationszimmern und Postmappen (Zugang nur für Bedienstete) konnte im Ergebnis allerdings ausgeschlossen werden, dass eine Person außerhalb

des Kreises der Bediensteten der JVA (zu irgendeinem Zeitpunkt nach Erstellung der Urschrift des Führungsberichts) eine Kopie des Führungsberichts über den Gefangenen gefertigt und in den zuvor verschlossenen, an die Freundin des Gefangenen adressierten Briefumschlag gegeben hat.

Auf die Frage, welche(r) Bedienstete einer öffentlichen Stelle konkret gehandelt hat/haben, kommt es im Rahmen des Beanstandungsverfahrens nach § 29 SächsDSG nicht an, sofern ausgeschlossen ist, dass Personen gehandelt haben, die nicht der öffentlichen Stelle zuzurechnen sind. Dies war aufgrund der geschilderten besonderen Umstände in der JVA der Fall.

In der (heimlichen) Übersendung einer Kopie des Führungsberichts über den Gefangenen an dessen Freundin lag eine Übermittlung personenbezogener Daten an eine Privatperson. Diese Übermittlung war ein schwerwiegender Eingriff in das Grundrecht des Betroffenen auf informationelle Selbstbestimmung und erfolgte ohne gesetzliche Grundlage; die Voraussetzungen des § 96 SächsStVollzG, der die Verarbeitung und Übermittlung personenbezogener Daten im Strafvollzug regelt, lagen offenkundig nicht vor.

Die festgestellte Verletzung einer datenschutzrechtlichen Vorschrift war gravierend. Das Sächsische Strafvollzugsgesetz regelt detailliert, in welchen Fällen öffentliche Stellen und wann - ausnahmsweise - nicht-öffentliche Stellen personenbezogene Daten eines Gefangenen erhalten dürfen oder müssen. Übermittlungen, die unter Verletzung dieser Vorschriften vorgenommen werden, sind unzulässig; sie laufen überdies dem Gedanken der Resozialisierung zuwider und sind geeignet, der Person des betroffenen Gefangenen erheblich zu schaden. Darüber hinaus müssen sie das Vertrauen zumindest des Betroffenen und des Empfängers in eine recht- und gesetzmäßige Justizvollzugsverwaltung erschüttern.

Wegen der Erheblichkeit des Verstoßes gegen datenschutzrechtliche Vorschriften konnte ich nach § 29 Abs. 2 SächsDSG nicht von einer Beanstandung gegenüber dem SMJus absehen.

Das SMJus teilte meine Einschätzung. Bei einer heimlichen Übermittlung von personenbezogenen Daten Gefangener an Dritte handele es sich um einen nicht hinnehmbaren Verstoß gegen die datenschutzrechtlichen Vorschriften der §§ 96 ff. SächsStVollzG. Die Beanstandung wurde zum Anlass genommen, den Leiter der betroffenen Justizvollzugsanstalt zu bitten, die Bediensteten der Anstalt erneut über die datenschutzrechtlichen Vorschriften zu belehren und deutlich auf disziplinar-, ordnungs- und strafrechtliche Konsequenzen der Nichteinhaltung hinzuweisen.

Auch wenn der Fall eher ein individuelles Fehlverhalten eines unbekannt gebliebenen Bediensteten einer JVA schildert, zeigt er, wie schnell und massiv Verstöße gegen datenschutzrechtliche Vorschriften gerade in besonderen Ausprägungen des Verhältnisses zwischen Staat und Bürger grundlegende rechtsstaatliche Prinzipen der Verwaltung verletzen können.

8.6 Externe forensische Sachverständige müssen nach § 6 Abs. 2 SächsDSG auf das Datengeheimnis verpflichtet werden

Durch einen Pressebericht vom 17. März 2014 erfuhr ich, dass die Strafverfolgungsbehörden des Freistaates vor allem im Bereich der Ermittlung von Cyberkriminalität externe Gutachter zur Auswertung beschlagnahmter Datenträger einsetzen.

Aus datenschutzrechtlicher Sicht sind bei der Weitergabe personenbezogener Daten an außerhalb der Ermittlungsbehörde stehende Personen Besonderheiten zu beachten. Um die Einhaltung der datenschutzrechtlichen Vorschriften zu überprüfen, nahm ich Kontakt mit dem Generalstaatsanwalt auf, welcher mir die Herangehensweise bei der Einschaltung externer IT-Sachverständiger erläuterte.

Der Generalstaatsanwalt teilte mir mit, dass externe Dienstleister in strafrechtlichen Ermittlungsverfahren auf der Grundlage von § 161a Abs. 1 Satz 2 StPO i. V. m. §§ 73 bis 76, 78, 80, 82 StPO als forensische IT-Sachverständige im Rahmen eines öffentlich-rechtlichen Auftragsverhältnisses zur Auswertung beschlagnahmter Datenträger beauftragt würden.

Diese Sachverständigen würden durch die örtlichen Polizeibehörden sicherheitsüberprüft und nach § 1 VerpflG auf die gewissenhafte Erfüllung ihrer Obliegenheiten verpflichtet. Damit unterlägen sie auch den gesonderten strafrechtlichen Bestimmungen für Amtsträger. Weiter würden auch die Räumlichkeiten, in denen sie ihre Begutachtungen vornehmen, auf ihre Sicherheit hin überprüft. Um auch die Sicherheit des Übermittlungswegs zu gewährleisten, erfolge der Transport der zu begutachtenden Beweismittel entweder durch die beauftragte Person selbst, durch die Polizei oder aber durch zertifizierte Sicherheitskuriere. Eine darüber hinaus gehende Einzelverpflichtung auf das Datengeheimnis nach § 6 Abs. 2 SächsDSG sei nicht notwendig.

Dem konnte ich nicht voll zustimmen: Das Datengeheimnis in § 6 Abs. 1 Satz 1 SächsDSG soll sicherstellen, dass personenbezogene Daten durch die „für eine öffentliche Stelle tätigen Personen“ nur im Rahmen der gesetzlichen Bestimmungen verarbeitet werden. Dazu werden diese Personen nach § 6 Abs. 2 SächsDSG schriftlich verpflichtet. Unzweifelhaft sind auch externe Sachverständige „für eine öffentliche

Stelle“, namentlich eine Ermittlungsbehörde, „tätig“. Der Anwendungsbereich von § 6 Abs. 1 Satz 1 SächsDSG ist deshalb eröffnet.

Während der nach § 1 VerpflG verpflichtete Sachverständige unter anderem gemäß §§ 203, 353b StGB zur Wahrung von Privatgeheimnissen sowie des Dienstgeheimnisses und besonderer Geheimhaltungspflichten verpflichtet ist, geht das Datengeheimnis aus § 6 Abs. 1 Satz 1 SächsDSG insoweit weiter, als dass bereits jeder unbefugte Verarbeitungsschritt, z. B. ein unbefugtes Nutzen oder Speichern, einen Verstoß darstellt. Auch können personenbezogene Daten als offenkundige Tatsachen i. S. v. § 37 Abs. 2 Satz 1 Nr. 2 BeamtStG von der Verschwiegenheitspflicht ausgenommen sein, dennoch aber dem Datengeheimnis aus § 6 Abs. 1 Satz 1 SächsDSG unterfallen.

Vor diesem Hintergrund wiederholte ich auch gegenüber dem Generalstaatsanwalt meine Aufforderung, externe forensische IT-Sachverständige nach § 6 Abs. 2 SächsDSG auf die Wahrung des Datengeheimnisses zu verpflichten. Um keine Zweifel an einer wirksamen Verpflichtung aufkommen zu lassen, hat der Generalstaatsanwalt den Staatsanwaltschaften diese Vorgehensweise empfohlen.

8.7 Übermittlung von Gläubigerdaten durch die Landesjustizkasse an die Steuerbehörden

Zwischen dem Landesamt für Steuern und Finanzen, dem SMJus, dem OLG sowie der Landesjustizkasse war vereinbart worden, Auszahlungsansprüche von Verfahrensbeteiligten in Strafverfahren, die über 500 Euro hinausgehen, den zuständigen Finanzbehörden zum Zwecke der Prüfung bestehender Gegenforderungen mitzuteilen. Das SMJus teilte mir auf meine Frage nach der Rechtsgrundlage für die Übermittlung dieser personenbezogenen Daten mit, diese würden auf § 14 Abs. 1 SächsDSG gestützt, da die Aufrechnung i. S. v. Nr. 2.2 der VwV zu § 7 SäHO als „wirtschaftlicher als die Auszahlung anzusehen“ sei und insofern erforderlich i. S. d. § 14 Abs. 1 Nr. 1 SächsDSG sei.

Dies überzeugte mich nicht. Zwar konnte ich gut nachvollziehen, dass der Fiskus ein wirtschaftliches Interesse an der Kenntnis solcher Auszahlungsansprüche hat, mit denen dann aufgerechnet werden kann. Möglich erschien mir des Weiteren, dass dadurch ein insgesamt geringerer Mitteleinsatz i. S. v. Nr. 2.2 der VwV zu § 7 SäHO verbunden sein könnte, obwohl mir - vermutlich genauso wie dem SMJus - belastbare empirische Erkenntnisse hierzu nicht zur Verfügung standen und stehen.

Letztlich kam es jedoch hierauf nicht an. Denn eine - hier erforderliche - bereichsspezifische Rechtsgrundlage für die Übermittlung der Gläubigerdaten durch die Justizbehörden an die Finanzverwaltung war nicht ersichtlich. Die Voraussetzungen der §§ 12 ff.

EGGVG i. V. m. der MiStra waren nicht erfüllt. Eine andere bereichsspezifische Mitteilungsbefugnis oder -pflicht (realistisch nur die für Steuer- bzw. Zollstrafsachen einschlägigen Vorschriften, §§ 116, 397 ff. AO, Nr. 266 Abs. 1 RiStBV) war nicht ersichtlich. Einen Rückgriff auf die allgemeinen Datenverarbeitungsvorschriften des Sächsischen Datenschutzgesetzes (§§ 12-17 SächsDSG) hielt und halte ich in Übereinstimmung mit den Justizbehörden angesichts der in aller Regel abschließenden Regelungsnatur der justiziellen Fachgesetze (Strafprozessordnung, Einführungsgesetz zum Gerichtsverfassungsgesetz etc.) für nicht zulässig. Daher ergab sich für mich nach geltendem Recht aus keiner Vorschrift die Befugnis oder gar die Pflicht, Gläubigerdaten zum Zwecke der Prüfung einer Aufrechnungsmöglichkeit an die Finanzverwaltung zu übermitteln.

Selbst wenn man unterstellte, dass § 14 Abs. 1 SächsDSG hier anwendbar wäre, scheiterte die Anwendung daran, dass eine Übermittlung nicht erforderlich ist. Denn „erforderlich“ i. S. v. § 14 Abs. 1 SächsDSG ist eine Übermittlung personenbezogener Daten zur Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers nur dann, wenn ohne sie die öffentliche Stelle, hier die Justiz- oder Finanzbehörde, ihre Aufgaben nicht, nicht vollständig, nicht rechtzeitig, nicht in rechtmäßiger Weise oder nur mit unverhältnismäßig großem Aufwand erfüllen könnte (vgl. Mauersberger in Giesen/ Bannasch/Naumann/Mauersberger/Dehoust, Kommentar zum Sächsischen Datenschutzgesetz, § 14 Rdnr. 13 mit Verweis auf Dehoust a. a. O., § 12 Rdnr. 15). Da jede Datenverarbeitung durch die öffentliche Gewalt grundsätzlich verboten ist und einer ausdrücklichen normenklaren Befugnisnorm bedarf, ist § 14 SächsDSG eng auszulegen. Es genügt daher nicht, dass die Daten zur Aufgabenerfüllung nur „geeignet, nützlich, dienlich oder zweckmäßig“ sind (vgl. Dehoust a. a. O.).

Dass vorliegend Auszahlungsansprüche von Verfahrensbeteiligten in Strafverfahren, die über 500 Euro hinausgehen, generell und anlasslos an die Finanzbehörden zum Zweck der Prüfung bestehender Gegenforderungen übermittelt werden, ist in diesem strengen Sinne nicht erforderlich. Denn die Finanzverwaltung kann ihre Aufgaben auch ohne Kenntnis von Auszahlungsansprüchen von Verfahrensbeteiligten in Strafverfahren erfüllen.

Das SMJus habe ich deshalb gebeten, von der gewählten Verfahrensweise künftig Abstand zu nehmen oder für eine bereichsspezifische Rechtsgrundlage zu sorgen.

9 Wirtschaft und Arbeit

9.1 Straßenverkehrswesen

9.1.1 Verarbeitung personenbezogener Daten bei einer unteren Straßenverkehrsbehörde

Ein Bürger beschwerte sich bei mir über die Verarbeitung seiner personenbezogenen Daten im Zusammenhang mit seinem Antrag auf Befreiung der Pflicht zum Anlegen des Sicherheitsgurts im PKW (§ 46 Abs. 1 Nr. 5 b StVO) durch die untere Straßenverkehrsbehörde. Nach Prüfung der Unterlagen durch die Behörde war festgestellt worden, dass aus der vorgelegten ärztlichen Bescheinigung des Hausarztes die Dauer der Beeinträchtigung, die für die Bearbeitung der Antragstellung erforderlich ist, nicht hervorging. Deshalb wurde, ohne Kontakt mit dem Antragsteller aufzunehmen, der Hausarzt direkt um Informationen gebeten. Gegen die im Anschluss erteilte Bescheinigung legte der Betroffene Widerspruch im Hinblick auf die Befristung ein und wandte sich im Übrigen gegen eine direkte Kontaktaufnahme der Behörde mit seinem Hausarzt. Bei der folgenden Widerspruchsbearbeitung kontaktierte die Behörde den Hausarzt erneut und beschied den Widerspruch positiv.

Die Straßenverkehrsbehörde rechtfertigte das Verfahren als korrektes Vorgehen und zügige Bearbeitung im Interesse des Betroffenen und verwies auf die zulässige Erhebung der personenbezogenen Daten, wenn ihre Kenntnis zur Aufgabenerfüllung erforderlich sei (§ 12 Abs. 1 SächsDSG).

Das Verwaltungsverfahrensrecht sieht vor, dass die Behörde die Berichtigung von Erklärungen oder Anträgen bei dem Beteiligten anregt, wenn diese offensichtlich nur versehentlich oder aus Unkenntnis unterblieben oder unrichtig abgegeben oder gestellt worden sind (§ 25 Abs. 1 VwVfG). Diese Vorgehensweise ist im Einklang mit der datenschutzrechtlichen Regelung, nach der personenbezogene Daten bei Dritten nur erhoben werden dürfen, wenn der Betroffene eingewilligt hat (§ 12 Abs. 4 Nr. 2 SächsDSG). Im Ausgangsfall ließ die Behörde, wie dargestellt, die Rücksprachen mit dem Betroffenen aus.

Eine von einer Behörde zu erwartende bürgerfreundliche Antragsbearbeitung darf nicht zulasten datenschutzrechtlicher Vorgaben erfolgen.

9.1.2 Videoüberwachung und -aufzeichnung im Straßentunnel zur Waldschlößchenbrücke in Dresden

Videoüberwachung ist ein Dauerthema der datenschutzrechtlichen Arbeit. Im Berichtszeitraum stieß ich auf die Problematik der Videoüberwachung in Straßentunneln. Ein

Einwohner bat mich um Stellungnahme zu einer von der Stadt Dresden verantworteten Videoüberwachung und -aufzeichnung des Straßentunnels zur Waldschlößchenbrücke im Gemeindegebiet. Da der Einsatz optisch-elektronischer Einrichtungen gemäß § 33 Abs. 1 und 2 SächsDSG nur unter ganz bestimmten Voraussetzungen und nach einer Abwägung der Grundrechte Betroffener und öffentlichen Interessen erfolgen darf, bat ich die Landeshauptstadt Dresden um Stellungnahme. Meine Nachfragen richtete ich auf die gesetzliche Grundlage der Videoüberwachung und die nach dem Gesetz vorgeschriebene Hinweispflicht (Ausschilderung der Videoüberwachung).

Als bereichsspezifische Rechtsgrundlage für die Videoüberwachung im Straßentunnel zur Waldschlößchenbrücke wurde von Seiten der Stadtverwaltung die „Richtlinie für die Ausstattung und den Betrieb von Straßentunneln RABT 06“, herausgegeben durch die Forschungsgesellschaft für Straßen- und Verkehrswesen (FGSV), angegeben.

In der Stellungnahme vertrat die Stadt die Auffassung, dass gemäß § 2 SächsDSG das Datenschutzgesetz nur einschlägig sei, wenn personenbezogene Daten verarbeitet werden. Die besagte Videoüberwachung diene jedoch der Überwachung des allgemeinen Verkehrsflusses, ohne dass personenbezogene Daten erhoben, gespeichert, verändert, anonymisiert, übermittelt, genutzt, gesperrt oder gelöscht würden. Dieser Rechtsauffassung konnte ich nicht folgen. Zum einen setzt § 33 Abs. 1 SächsDSG als spezielle Norm wegen des Effekts anlass- und verdachtsloser staatlicher Videoüberwachungsmaßnahmen mit großer „Streubreite“ auf die Handlungsfreiheit und das Persönlichkeitsrecht der Menschen keinen unmittelbaren Personenbezug und keine Verarbeitung personenbezogener Daten voraus. So genügen z. B. bereits Übersichtsaufnahmen. Zum anderen sieht die von der Stadt als Grundlage für die Videoüberwachung angeführte Richtlinie unter Nr. 6.2.2 Videoüberwachung vor, dass die erfassten Videobilder des betreffenden Bereichs, welche im Normalfall vierundzwanzig Stunden auf Monitore in einer besetzten Überwachungsstelle übertragen wurden, bei Alarmauslösung auf Grund eines Störfalles oder Unfalles automatisch aufgezeichnet werden, um eine spätere Untersuchung von Ursachen durchführen zu können.

Videoüberwachung greift als Bilddatenverarbeitung signifikant in das allgemeine Persönlichkeitsrecht in seiner Ausprägung als „Recht auf informationelle Selbstbestimmung“ ein. Der Eingriff seitens der öffentlichen Stelle bedarf immer einer normenklaren gesetzlichen Grundlage. Die Stadt teilte mir in ihrer Stellungnahme mit, dass gemäß der Richtlinie für die Ausstattung und den Betrieb von Straßentunneln RABT 06 Punkt 1.2.1, bei Tunneln über 400 Meter Länge sicherzustellen sei, dass die Notrufe und die Videoüberwachung an eine ständig besetzte Stelle übertragen werden müssten. Hieraus ergebe sich kein Ermessensspielraum für die Verwaltung.

Die von der Stadt als bereichsspezifische Rechtsgrundlage für die Videoüberwachung im Straßentunnel zur Waldschlößchenbrücke angegebene „Richtlinie für die Ausstattung und den Betrieb von Straßentunneln RABT 06“ wird durch die Forschungsgesellschaft für Straßen- und Verkehrswesen (FGSV) herausgegeben und ist für die Bürger nicht frei, sondern nur gegen Erwerb des Richtlinientextes zu einem relativ hohen Preis zugänglich. Dennoch wurde sie durch das Bundesministerium für Verkehr, Bau und Stadtentwicklung (BMVBS) mit dem Allgemeinen Rundschreiben Straßenbau Nr. 10/ 2006 als „Ausgabe 2006“ in Verwaltungsvorschriften eingeführt und durch Erlass des SMWA den zuständigen Verwaltungsbehörden bekannt gemacht.

Die Verwaltungsanordnungen und die Richtlinie „RABT 06“ setzen nach meiner Überzeugung damit die Richtlinie 2004/54/EG vom 29. April 2004 über „Mindestanforderungen an die Sicherheit von Tunneln im transeuropäischen Straßennetz“ (sogenannte EU-Tunnelrichtlinie) nicht in nationales Recht um, da es sich hierbei nicht um Rechtsvorschriften i. S. v. § 4 Abs. 1 SächsDSG handelt und die daher auch nicht geeignet sind, Grundrechtseingriffe zu legitimieren. Hierfür wäre eine bereichsspezifische und hinreichend bestimmte gesetzliche Grundlage erforderlich, welche Anlass, Zweck und Ausmaß sowie ggf. die zulässigen Maßnahmen der Datenerhebung, -speicherung und weiteren Datenverarbeitung wie auch Löschfristen abschließend und für alle Bürger transparent regelt.

Trotz der Zweifel an der ordnungsgemäßen Umsetzung in nationales Recht ist es aber nach meiner Ansicht vertretbar, die Videoüberwachung auf die Auffangbestimmung des § 33 SächsDSG in Verbindung mit der geltenden EU-Richtlinie zu stützen. Grundsätzliche datenschutzrechtliche Bedenken hinsichtlich der konkreten Ausgestaltung der Videoüberwachung am Straßentunnel zur Waldschlößchenbrücke bestanden dabei im konkreten Fall nicht. Allerdings sind dann auch sämtliche gesetzliche Anforderungen nach § 33 SächsDSG einzuhalten, u. a. die Hinweispflicht (vgl. § 33 Abs. 3 SächsDSG). Auch zum Zeitpunkt der Kontrolle wurde am Straßentunnel zur Waldschlößchenbrücke nicht auf die Tatsache der Videoüberwachung und die verantwortliche Stelle durch geeignete Maßnahmen hingewiesen. Die Stadt brachte nach meinen Hinweisen Monate später eine Beschilderung an den Zufahrten des Tunnels an.

Das grundsätzliche Problem, ob es sich bei der „Richtlinie für die Ausstattung und den Betrieb von Straßentunneln RABT 06“ um eine rechtmäßige Umsetzung der EU-Rechtsetzung zu „Mindestanforderungen an die Sicherheit von Tunneln im transeuropäischen Straßennetz“ in nationales Recht handelt, werde ich mit meinen Kollegen im Bund und in den Ländern weiterverfolgen. Eine bereichsspezifische normenklare Regelung der Videoüberwachung in Straßentunneln ist nach meiner Überzeugung notwendig und wäre im Interesse der Betroffenen und der Verwaltung.

9.2 Gewerberecht

In diesem Jahr nicht belegt.

9.3 Kammerwesen

9.3.1 Erneut - Besonders bestellte Bevollmächtigte bei den IHK

Im letzten Tätigkeitsbericht (16/9.3.1) berichtete ich über datenschutzrechtliche Unzulänglichkeiten bei einer IHK bei der Prüfung der Eigenschaft des *besonders bestellten Bevollmächtigten* zur Teilnahme an der Vollversammlung durch einen Fragebogen.

Zu Mitgliedern der Vollversammlung können nach § 5 Abs. 2 IHKG auch besonders bestellte Bevollmächtigte von Kammerzugehörigen gewählt werden. Das Nähere über die Ausübung und Durchführung der Wahl ist nach § 5 Abs. 3 IHKG in der Wahlordnung zu regeln. Im Fall der IHK war eine für Wahlbewerber transparente Datenerhebung durch vorher zu erkennende und zu erfüllende Kriterien nicht gegeben.

Im Berichtszeitraum wandte sich eine andere IHK mit der gleichen Thematik an mich. Die dort überarbeitete Wahlordnung enthält eine Beschreibung von Eigenschaften und überprüfbare Kriterien für den besonders bestellten Bevollmächtigten. Bestandteil der Wahlordnung ist als Anlage eine Mustererklärung zur Datenerhebung mit weiteren Hinweisen zu geforderten Eigenschaften des besonders bestellten Bevollmächtigten. Die Datenerhebung beschränkt sich dabei auf das unbedingt erforderliche Maß. Auch die in der Wahlordnung vorgesehene Möglichkeit des Wahlausschusses, die gemachten Angaben durch den Betroffenen vor dem Wahlausschuss erläutern oder bestätigen zu lassen, begegnet keinen datenschutzrechtlichen Bedenken. Die überarbeitete Wahlordnung der IHK ermöglicht eine rechtskonforme und transparente Verarbeitung der personenbezogenen Daten der Bewerber als besonders bestellte Bevollmächtigte.

Die Anfrage der IHK erfolgte auf Veranlassung der Rechtsaufsicht unter Hinweis auf die Ausführungen in meinem 16. Tätigkeitsbericht.

9.3.2 Krankheit im Schatzmeisterbericht

Ein Beschäftigter der Rechtsanwaltskammer gab mir den Hinweis, dass im Bericht des Schatzmeisters der RAK zum Haushaltsjahr 2012 über die ihn betreffende „lang andauernde Erkrankung“ berichtet wurde. Der Bericht wurde als Teil der Materialien zur Kammerversammlung nicht nur an sämtliche Mitglieder der RAK in Papierform versandt, sondern auch im Internet veröffentlicht. Nachdem der Betroffene dies bemängel-

te, wurde der im Internet veröffentlichte Text dahingehend korrigiert, dass der Inhalt in Bezug auf die „lang andauernde Erkrankung“ entfiel.

Die von mir um Stellungnahme gebetene Kammer teilte mir dazu mit, dass es „keinem Zweifel unterliegen“ könne, dass der Schatzmeister im Rahmen seiner Berichterstattung an den Vorstand berechtigt sei, auch über finanzielle Belastungen durch Krankheitsfälle von Mitarbeitern zu berichten. Weiterhin behauptete sie, dass die Übersendung des Schatzmeisterberichts an die Mitglieder „keine Veröffentlichung“ darstellte. Sie bedauerte die Veröffentlichung der beanstandeten Passage im Internet; eine Änderung des Schatzmeisterberichts in Papierform lehnte sie jedoch ab.

Die Auffassung der RAK war aus mehreren Gründen unzutreffend.

Gesundheitsdaten dürfen gemäß § 4 Abs. 2 Nr. 1 SächsDSG nur verarbeitet (also auch veröffentlicht oder übermittelt) werden, wenn eine besondere Rechtsvorschrift dies ausdrücklich vorsieht oder zwingend voraussetzt. Dies war nicht der Fall.

Eine Veröffentlichung der Daten im Internet ist darüber hinaus gemäß § 37 Abs. 2 SächsDSG unzulässig, da diese schon nicht für die Information der Allgemeinheit oder der anderen Beschäftigten erforderlich gewesen war und offensichtlich schutzwürdige Interessen des Betroffenen entgegengestanden haben.

Auch die Übermittlung der Daten an die Kammermitglieder verstößt - neben § 4 Abs. 2 Nr. 1 SächsDSG - gegen § 37 Abs. 3 SächsDSG. Es ist nicht ersichtlich, dass eine Rechtsvorschrift diese vorsieht. Insbesondere ist auch § 87 Abs. 1 BRAO i. V. m. § 6 Abs. 5 GO RAK Sachsen nicht zu entnehmen, dass ein Schatzmeisterbericht (mit Gesundheits- und Beschäftigtendaten) an die Kammermitglieder zu übermitteln wäre.

Die Verarbeitung dieses Inhalts wäre zu begründen gewesen. Die entsprechende Erforderlichkeit im Hinblick darauf, dass ohne die Datenverarbeitung gesetzliche und satzungsgemäße Aufgaben nicht hätten erfüllt werden können, wurde nicht dargetan.

Nachdem ich dementsprechend eine Beanstandung gegenüber der RAK ausgesprochen habe, teilte mir diese mit, nun doch den Schatzmeisterbericht ändern zu wollen. Eine geänderte - datenschutzrechtskonforme - Fassung wurde mir übermittelt.

9.4 Offene Vermögensfragen

In diesem Jahr nicht belegt.

10 Gesundheit und Soziales

10.1 Gesundheitswesen

10.1.1 Einwilligung in die Verarbeitung von Patientendaten

Eine Petentin informierte mich darüber, dass ein städtisches Krankenhaus sie aufgefordert habe, vor ihrer Behandlung alle entsprechenden in ihrem Besitz befindlichen ärztlichen Unterlagen beizubringen. Diese seien daraufhin ohne ihr Einverständnis kopiert worden. Weiterhin seien zwei sie früher behandelnde Ärzte mittels eines Arztbriefes über den aktuellen Befundbericht informiert worden. Auch diese Unterrichtung sei nicht nur ohne ihre Einwilligung geschehen, vielmehr habe sie diese ausdrücklich verweigert.

Kommunale Kliniken ohne eigene Rechtspersönlichkeit sind als Teil der Gebietskörperschaft öffentliche Stellen, die dem Sächsischen Datenschutzgesetz unterliegen (vgl. 12/1.7 Nr. 1). Das Krankenhaus bestätigte nach einem längeren Schriftwechsel schließlich den geschilderten Sachverhalt, sah darin aber zunächst keinen Datenschutzverstoß. Die Klinik wies vielmehr darauf hin, dass nicht mehr festgestellt werden könne, welche Unterlagen kopiert worden seien und behauptete im Übrigen, dass weitere Datenverarbeitungen mit mündlicher Einwilligung der Patientin erfolgt seien. Dies könne auch durch eine anwesende Sekretärin bestätigt werden. Einwilligungen in die Datenverarbeitung öffentlicher sächsischer Stellen haben nach § 4 Abs. 4 SächsDSG aber grundsätzlich schriftlich zu erfolgen. Nachdem ich das Krankenhaus darauf hinwies, dass eine entsprechende Einwilligung schriftlich zu erfolgen habe, um wirksam zu sein, erkannte man schließlich doch einen Verstoß. Da der Sachverhalt aufgrund gegensätzlicher Behauptungen durch mich nicht vollends aufgeklärt werden konnte, habe ich von weiteren Maßnahmen abgesehen.

Wie dieser Fall zeigt, sollte es auch im Interesse der jeweils behandelnden Ärzte sein, Datenübermittlungen nur mit wirksamen schriftlichen Einwilligungen in Form von Schweigepflichtentbindungserklärungen vorzunehmen. Durch die Schriftlichkeit wird auch der Nachweis eines ordnungsgemäßen Vorgehens gemäß den Vorgaben des die Datenverarbeitung bestimmenden Patienten dokumentiert. Ansonsten kann auch eine Strafbarkeit nach § 203 Abs. 1 Nr. 1 StGB nicht ausgeschlossen sein.

10.1.2 Klinische Krebsregister

Im April 2013 ist das Krebsfrüherkennungs- und -registergesetz (KFRG) des Bundes in Kraft getreten. Erstmalig fanden damit die in den neuen Bundesländern schon sehr lange bestehenden klinischen Krebsregister eine gesetzliche Stütze. Die klinischen Krebsregister bleiben aber weiterhin Aufgabe der Bundesländer, die nunmehr gehalten

sind, eine weitgehend lückenlose klinische Krebsregistrierung in ihren Ländern umzusetzen. Auf staatsvertraglicher Grundlage wird das von den Ländern Berlin, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt, Thüringen und Sachsen betriebene Gemeinsame Krebsregister an die neue bundesgesetzliche Rechtslage und an neue Verfahrensstandards angepasst werden müssen. Im Berichtszeitraum sind hierzu bereits erste Gespräche mit meiner Behörde erfolgt. Die Abstimmung des wegen der Schutzwürdigkeit der Gesundheitsdaten datenschutzrechtlich sehr bedeutenden Registerverfahrens unter Einbindung der regionalen klinischen Krebsregister in Sachsen mit meiner Behörde ist noch nicht abgeschlossen. Auch liegt noch kein neuer Entwurf des Staatsvertrags zum Gemeinsamen Krebsregister der vorgenannten Länder vor. Ich werde über die weitere Entwicklung berichten.

Zu verweisen ist in dem Zusammenhang wegen der gesamten organisatorischen Fortentwicklung in dem Bereich auch auf die Entschließung der DSK vom 14. November 2014 zu *Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern* (vgl. 17.1.17).

10.1.3 Folgen der Verarbeitung unrichtiger Informationen - Sperrung und Datenverarbeitungsbeschränkungen

Im Berichtszeitraum erbat ein Betroffener Unterstützung bei der Berichtigung unrichtiger Daten. Aus seiner Sicht waren unzutreffende Informationen, darunter Gesundheitsangaben, unrechtmäßig durch ein städtisches Krankenhaus an eine Polizeidirektion übermittelt worden. Ich bat sowohl das Krankenhaus als auch die Polizeidienststelle um eine entsprechende Stellungnahme.

Meine Kontrolle offenbarte eine gravierende Diskrepanz zwischen den Angaben, welche der *Verbund Gemeindenahe Psychiatrie*, als Teil des städtischen Krankenhauses, an die Polizeidirektion weitergegeben haben wollte und der Darstellung der Polizeibehörde, welche Daten zum Betroffenen ihr tatsächlich übermittelt worden sein sollten.

Aus dem als Abschlussbericht abgelegten Vermerk der Polizei ging hervor, dass Nachfragen bei einer Sozialarbeiterin des Verbundes für Gemeindenahe Psychiatrie ergeben hätten, seit wann der Betroffene dort bekannt gewesen sei. In den Aufzeichnungen wurde zudem wiedergegeben, dass der Betroffene unter einer „Psychose“ leide, sich jedoch nicht behandeln lassen wolle, dass ein Antrag beim Amtsgericht zur Amtsbetreuung nicht gestellt worden sei, da der Betroffene ärztliche Therapie ablehne und dass ein Betreuer nicht bestellt gewesen sei. Bei den Informationen handelte es sich nach meiner Überzeugung um besonders schutzwürdige Gesundheitsdaten (§ 4 Abs. 2 SächsDSG).

Der Verbund Gemeindenahe Psychiatrie teilte mir demgegenüber mit, dass zwischen dem Betroffenen und dem Krankenhaus kein Behandlungsverhältnis bestanden hätte und die im Vermerk der Polizeidirektion dokumentierten Informationen zum Betroffenen tatsächlich so nicht mitgeteilt worden seien. Die handschriftlichen Notizen bei der Psychiatrieeinrichtung zur Anfrage der Polizei belegten lediglich die Erkundigungen der Polizeibehörde wegen einer eventuellen Betreuerbestellung. Die den Vorgang bearbeitende Sozialarbeiterin des Verbundes Gemeindenahe Psychiatrie widersprach zudem, der Polizeidirektion einen medizinischen Befund übermittelt zu haben. Aufzuklären, welche personenbezogenen Daten zur Person des Betroffenen seitens des Krankenhauses der Polizeibehörde gegenüber tatsächlich offenbart wurden, war mir anhand der Aktenlage und widerstreitender Stellungnahmen nicht möglich.

Die Weitergabe von Befunddaten als dem Arzt-Patientengeheimnis unterfallenden Informationen wäre bereits datenschutzrechtlich kritisch gewesen. Bestritten wurde von dem Betroffenen aber auch die Richtigkeit der Einschätzung „Psychose“. Er gab in seiner an mich gerichteten Petition an, dass ihm durch die Speicherung dieser Angabe bei der Polizei Nachteile entstanden seien. Einem Antrag auf Berichtigung des streitigen Befunddatums konnte gemäß § 19 SächsDSG von Seiten des städtischen Krankenhauses nicht entsprochen werden, da der Gegenstand des Antrages auf Berichtigung unrichtiger Daten, der Schlussbericht der Polizeidirektion, nur bei der Polizeibehörde gespeichert und aufbewahrt worden war.

Vor dem Hintergrund, dass die Richtigkeit des übermittelten personenbezogenen Datums, hier die Diagnose „Psychose“, von der betroffenen Person bestritten wurde und der Verbund Gemeindenahe Psychiatrie angab, dieses Datum nicht übermittelt zu haben und kein Behandlungsverhältnis bestanden haben sollte, forderte ich die Polizeidirektion auf, die zur Person des Betroffenen gespeicherten Daten einer angeblichen Diagnose zu sperren (§ 21 Abs. 1 SächsDSG). Gemäß § 21 Abs. 3 SächsDSG sind gesperrte personenbezogene Daten gesondert aufzubewahren. Lässt sich die gesonderte Aufbewahrung aufgrund der Art der Verarbeitung nicht oder nur mit unverhältnismäßigem Aufwand durchführen, sind die Daten mit einem Sperrvermerk zu versehen. Die Polizeibehörde folgte meiner Empfehlung.

Seitens öffentlicher Stellen ist im Falle der Sperrung zu beachten, dass die gesperrten personenbezogenen Daten ohne Einwilligung des Betroffenen nur dann genutzt bzw. verarbeitet werden dürfen, wenn es zur Behebung einer dringenden Beweisnot in gerichtlichen oder Verwaltungsverfahren oder zu Aufsichts- und Kontrollzwecken unerlässlich ist. Personenbezogene Daten, die unzulässig in Akten gespeichert sind oder deren Löschung gemäß § 20 Abs. 4 SächsDSG unterblieben ist, dürfen ohne Einwilligung

des Betroffenen überhaupt nicht mehr genutzt werden. Zu beachten ist ferner, dass gemäß § 21 Abs. 5 SächsDSG ggf. die Empfänger übermittelter Daten nach Maßgabe des § 19 Abs. 2 SächsDSG zu verständigen sind.

Datenschutzrechtlich zu hinterfragen war die durch das städtische Krankenhaus erfolgte Verarbeitung der Daten des Betroffenen. Obwohl zwischen dem Betroffenen und dem städtischen Krankenhaus kein Behandlungsverhältnis bestanden hatte, bewahrte das Krankenhaus Informationen zum Betroffenen auf.

Das Krankenhaus gab dazu an, Informationen zur Prüfung einer eventuell vorliegenden Hilfsbedürftigkeit gemäß dem Sächsischen Gesetz über die Hilfen und die Unterbringung bei psychischen Krankheiten (SächsPsychKG) bereitgehalten zu haben, in deren Ergebnis eine Hilfe durch das städtische Krankenhaus seitens des Betroffenen abgelehnt worden sei. Zum anderen seien Daten des Betroffenen aufgrund eines Akteneinsichtnahmegesuchs und der Bitte um Berichtigung von unrichtigen personenbezogenen Daten nach dem Sächsischen Datenschutzgesetz gespeichert worden. Der Vorgang zu Ansprüchen des Betroffenen aus dem Sächsischen Datenschutzgesetz ist informationell getrennt von dem Vorgang zur Prüfung der Hilfebedürftigkeit zu bearbeiten. Nach jeweils abgeschlossener Prüfung gelten die jeweiligen Fristen zur Aufbewahrung und für die Löschung der Daten.

Auch wenn nicht vollständig aufgeklärt werden konnte, welche personenbezogenen Daten zur Person des Betroffenen tatsächlich vom städtischen Krankenhaus an die Polizeidirektion übermittelt wurden, sprachen viele Umstände dafür, dass durch das städtische Krankenhaus deutlich mehr personenbezogene Daten zur Person des Betroffenen an die Polizei übermittelt wurden als dies in dem handschriftlichen Vermerk des Krankenhauses dokumentiert war. Dass die Polizei erdachte Gesprächsinhalte in den in Rede stehenden Schlussvermerk aufgenommen haben sollte, erschien nach allgemeinen Erfahrungssätzen nicht plausibel.

Ich forderte das städtische Krankenhaus auf, zukünftig durch geeignete innerdienstliche Regelungen sicherzustellen, dass Übermittlungen besonders schutzwürdiger personenbezogener Daten an öffentliche Stellen in Erfüllung der gesetzlichen Aufgaben des Verbundes Gemeindenahe Psychiatrie transparent und revisionsfähig vermerkt werden (vgl. § 9 Abs. 2 SächsDSG).

10.2 Sozialwesen

10.2.1 Herausgabe eines Prüfberichts durch den Medizinischen Dienst der Krankenversicherung an die Staatsanwaltschaft

Ich wurde vom MDK Sachsen um eine datenschutzrechtliche Bewertung des folgenden Sachverhalts gebeten:

Der MDK führt im Rahmen der §§ 114 ff. SGB XI Qualitätsprüfungen bei Pflegeeinrichtungen durch.

In der Folge einer solchen Qualitätsprüfung wurde der nach einer solchen Prüfung zu erstellende Prüfbericht durch eine Staatsanwaltschaft angefordert. Diese ermittelte im Zusammenhang mit einer Körperverletzung gegen Unbekannt, wobei ein Bezug zur Pflegeeinrichtung hergestellt und der Prüfbericht als ermittlungsförderlich angesehen wurde. Die Staatsanwaltschaft nannte dabei als Rechtsgrundlage für die Übermittlung die Vorschrift des § 161 Abs. 1 StPO.

Der MDK fragte nun an, ob eine Herausgabe dieses Berichtes nicht wenigstens einer richterlichen Anordnung nach § 73 Abs. 3 SGB X bedarf, da sonst das Sozialgeheimnis nach § 35 Abs. 1 SGB I verletzt werden könnte.

Ich habe dem MDK mitgeteilt, dass meiner Ansicht nach, wie der MDK in seiner Anfrage bereits richtigerweise angeführt hatte, seine Übermittlungsbefugnis sich alleinig aus dem Sozialgesetzbuch ergeben müsse - dies folgt aus § 67d Abs. 1 SGB X -, wobei zu prüfen war, ob die Vorschrift des § 69 SGB X (Übermittlung für die Erfüllung sozialer Aufgaben) oder die des § 73 SGB X (Übermittlung für die Durchführung eines Strafverfahrens) hier einschlägig ist.

Die Übermittlung nach § 69 SGB X:

Die Übermittlung von Sozialdaten ist nach § 69 Abs. 1 Nr. 2 SGB X zulässig, sofern dies im Rahmen der Durchführung eines mit der Erfüllung einer gesetzlichen Aufgabe der übermittelten Stelle nach dem Sozialgesetzbuch zusammenhängenden gerichtlichen Verfahrens, einschließlich eines Strafverfahrens, geschieht (s. dazu auch 12/10.2.10). Dabei ist festzustellen, dass das hier vorliegende staatsanwaltliche Ermittlungsverfahren unter das Strafverfahren fällt. Im Hinblick auf die Voraussetzung des Zusammenhangs des gerichtlichen Verfahrens mit der Erfüllung einer gesetzlichen Aufgabe im Sinne des Sozialgesetzbuches, reicht jede Aufgabe, die nach § 30 Abs. 1 SGB IV vorgeschrieben oder zugelassen ist, aus. Der erforderliche Zusammenhang ist dabei aus meiner Sicht eher *weit* zufassen.

Im Ergebnis ist darauf abzustellen, ob die Ermittlungen der Staatsanwaltschaft mit einer nicht ordnungsgemäßen Versorgung eines Pflegeheimbewohners zusammenhängen. Denn die Qualitätsprüfung und der daraufhin zu erstellende Bericht sind ja gerade darauf gerichtet, die pflegerisch ordnungsgemäße Versorgung der Pflegeheimbewohner zu begutachten und Missstände aufzudecken. Dabei ist auch der Schutz der Heimbewohner vor Körperverletzungen entscheidend für deren Versorgungssituation. Daher war hier vom MDK festzustellen, ob die Ermittlungen der Staatsanwaltschaft mit dem Verdacht einer nicht ordnungsgemäßen Versorgung in Verbindung standen oder nicht. Ein reines Informationsinteresse der Staatsanwaltschaft an „Randinformationen“ muss hingegen mit Rücksicht auf das Sozialgeheimnis zurücktreten.

Die Übermittlung nach § 73 SGB X:

Die nach § 73 SGB X mögliche Datenübermittlung steht in jedem Fall unter dem im Abs. 3 des § 73 SGB X geregelten Richtervorbehalt (§ 162 StPO). Auch war darauf hinzuweisen, dass § 73 Abs. 1 SGB X nur eine Weitergabe im Zusammenhang mit einem Verbrechen vorsieht, die einfache Körperverletzung nach § 223 StGB den Verbrechensbegriff jedoch nicht erfüllt (zur Abgrenzung von Vergehen und Verbrechen siehe § 12 StGB).

§ 73 Abs. 2 SGB X ist für die Übertragung des Prüfberichts nicht anwendbar, da danach nur bestimmte Daten übertragen werden dürfen, der umfangreiche Prüfbericht aber weit außerhalb dieses Datenkatalogs liegt.

Abschließend ließ sich sagen, dass die Herausgabe des Prüfberichts über den § 73 SGB X nur durch einen richterlichen Beschluss möglich wäre. Die Herausgabe basierend auf § 69 SGB X ist nur dann möglich, wenn ein sinnvoller Zusammenhang zwischen der verfolgten Tat und der Versorgungssituation besteht. Ein reines Informationsinteresse der Staatsanwaltschaft an „Randinformationen“ muss mit Rücksicht auf das Sozialgeheimnis dabei zurücktreten.

10.2.2 Übernahme von Sterbehilfekosten nach § 74 SGB XII

Es erreichte mich die Anfrage einer Petentin im Zusammenhang mit der Beantragung von Sterbekostenhilfe nach § 74 SGB XII für die Bestattung ihres Vaters. Dabei wurde von der Petentin die breite Abfrage von persönlichen Daten, besonders die Einreichung von Miet-, Kredit- und Versicherungsverträgen, als problematisch empfunden.

In dem hierbei zum Einsatz kommenden Fragebogen des betreffenden Sozialleistungsträgers werden neben Unterlagen zum Verstorbenen (so etwa Sterbeurkunde, Kontoauszüge etc.), auch - zur Prüfung der finanziellen Situation der oder des Antragsstellers -

Kopien der bestehenden Versicherungsverträge, der Mietbescheide und der Einkommenslage angefordert. Weiterhin werden Daten wie sonstige monatliche Belastungen des Antragstellers und dessen Einkommen und Vermögen von diesem abgefragt. Falls diese dem Antragsteller bekannt sind, wird auch eine Angabe über mögliche Erben und Angehörige des Verstorbenen gewünscht.

Nach § 74 SGB XII werden die erforderlichen Kosten einer Bestattung staatlicherseits als Sozialleistung nur übernommen, soweit den hierzu Verpflichteten nicht zugemutet werden kann, die Kosten zu tragen. Da die Sonderregelung des § 74 SGB XII die eigenständige Leistungsvoraussetzung der Unzumutbarkeit verwendet, sind neben den wirtschaftlichen Verhältnissen des Verpflichteten zwar auch andere Momente zu berücksichtigen. Eine besondere Bedeutung kommt gleichwohl nach Ansicht des Bundessozialgerichts in seiner Entscheidung (Urteil) vom 29. September 2009 (Az.: B 8 SO 23/08 R) im Rahmen der Prüfung der Zumutbarkeit zunächst den wirtschaftlichen Verhältnissen des Verpflichteten zu. Dies ergibt sich aus § 2 i. V. m. § 19 Abs. 3 SGB XII, wonach u. a. Hilfen in anderen Lebenslagen (§§ 70 - 74 SGB XII) nur geleistet werden, soweit den Leistungsberechtigten die Aufbringung der Mittel aus dem Einkommen und Vermögen nach den Vorschriften des 11. Kapitels des Sozialgesetzbuches Zwölftes Buch nicht zugemutet werden kann (sogenannter Nachranggrundsatz). Anders ausgedrückt: Ist der Bestattungspflichtige bedürftig, kann ihm die Übernahme der Bestattungskosten nicht zugemutet werden; nur bei fehlender Bedürftigkeit kommen sonstige Zumutbarkeitsgesichtspunkte zum Tragen. Bedürftigkeit bzw. Unzumutbarkeit aus anderen Gründen muss insoweit nach Sinn und Zweck der Regelung des § 74 SGB XII zum Zeitpunkt der Fälligkeit der Forderung des Bestattungsunternehmens vorliegen, weil der Leistungsfall die Verbindlichkeit, nicht die erforderliche Bestattung selbst, ist. Soweit es um den Einsatz von Einkommen geht, ist im Hinblick darauf, dass § 74 SGB XII als Hilfe in anderen Lebenslagen dem 9. Kapitel des Sozialgesetzbuches Zwölftes Buch zugeordnet wurde, vorrangig auf die Einkommensgrenze des § 85 SGB XII zu rekurrieren. Sind einsetzbare, aber nicht ausreichende Mittel vorhanden, sind die Bestattungskosten anteilig zu übernehmen.

Sind die Bestattungskosten nicht durch den Nachlass oder sonstige durch den Nachlass zugeflossene Mittel gedeckt oder haben die Kostenpflichtigen keinen realisierbaren Anspruch gegen Dritte - wie zum Beispiel Schadenersatzforderungen gegen Dritte, die den Tod rechtswidrig und schuldhaft verursacht haben (§ 844 BGB, § 10 Abs. 1 StVG) und Versicherungsleistungen aus Anlass des Todesfalles (z. B. Lebens- oder Sterbegeldversicherungen, betriebliche oder sonstige aus Sozialleistungsansprüchen begründete Sterbegelder) sowie auch Ausgleichsansprüche gegen andere Miterben nach § 426 BGB - so ist die Zumutbarkeit gemäß § 19 Abs. 3 SGB XII nach den allgemeinen

Grundsätzen des Sozialhilferechts über Einkommens- und Vermögenseinsatz zu prüfen. Für den Einsatz von Einkommen gelten die Einkommensgrenzen der § 85 ff. SGB XII.

Insoweit ist seitens des Sozialamts eine genaue Einzelfallprüfung der wirtschaftlichen Verhältnisse vorzunehmen, was die Einkommens- und Vermögensverhältnisse wie auch die monatlichen Belastungen (wie z. B. Miete) des Kostenpflichtigen betrifft, sowie Angaben zum Vermögen des Erblassers. Die zuständige Behörde hat dabei auch die Befugnis, sich die Angaben durch entsprechende Nachweise gemäß § 60 SGB I, die mit dem Antrag einzureichen sind, dokumentieren zu lassen.

Hiervon ausgehend habe ich der Petentin daraufhin mitgeteilt, dass keine datenschutzrechtlichen Bedenken meinerseits beim beschriebenen Verfahren erkennbar sind.

10.2.3 Alltagsbilder aus dem Kindergarten

Eine Mutter wandte sich an mich mit der Frage, ob im Kindergarten durch die Betreuer aufgenommene Gruppenbilder/Mehrpersonenbilder den Eltern zur Verfügung gestellt werden können und inwieweit hierfür die Zustimmung der Eltern der anderen abgebildeten Kinder eingeholt werden muss.

Dabei wurde von der Petentin angemerkt, dass bereits eine Einverständniserklärung der Eltern zur Bildaufnahme vorlag, jedoch bei Mehrpersonenaufnahmen der Kindergarten diese Aufnahmen mit Hinweis auf den Datenschutz den Eltern nur zur Einsicht zur Verfügung stellte.

In meiner Bewertung bin ich zu dem Schluss gekommen, dass die Einverständniserklärung angepasst werden müsste, wobei die Eltern der mitabgebildeten Kinder der Herausgabe an andere Eltern ausdrücklich zustimmen müssen. So ist es möglich, sofern diese Zustimmung in Schriftform vorliegt, eine Herausgabe möglich zu machen. Da diese Bilder durch die Eltern möglicherweise veröffentlicht werden, ist die explizite Zustimmung der Eltern aller abgebildeten Kinder in jedem Fall nötig. Auch wurde von mir eine Verpixelung vorgeschlagen, um die Kinder der nicht-zustimmenden Eltern zu schützen, eine Weitergabe aber dennoch möglich zu machen.

10.2.4 Qualitätsprüfung im Pflegeheim nach dem Sächsischen Betreuungs- und Wohngeldqualitätsgesetz

Der Träger eines Pflegeheims fragte mich, ob er im Rahmen einer Prüfung nach dem Sächsischen Betreuungs- und Wohnqualitätsgesetz dazu verpflichtet ist, der zuständigen Kontrollbehörde relevante Unterlagen zu kopieren und zur Mitnahme auszuhändigen.

Das Sächsische Betreuungs- und Wohnqualitätsgesetz gilt für stationäre Einrichtungen im Freistaat Sachsen, die dem Zweck dienen, ältere Menschen, pflegebedürftige Volljährige oder volljährige Menschen mit psychischen Erkrankungen oder mit Behinderungen aufzunehmen, ihnen Wohnraum zu überlassen, Pflege- und Betreuungsleistungen sowie Verpflegung zur Verfügung zu stellen oder vorzuhalten, und die in ihrem Bestand von Wechsel sowie Zahl der Bewohner unabhängig sind sowie entgeltlich betrieben werden.

Zur Qualitätssicherung überwacht die zuständige Behörde - dies ist seit dem 1. Januar 2013 der Kommunale Sozialverband Sachsen - nach § 9 SächsBeWoG die stationären Einrichtungen durch wiederkehrende oder anlassbezogene Prüfungen. Aufzeichnungen, die der Träger nach § 6 Abs. 1 SächsBeWoG zu machen hat, hat dieser dabei grundsätzlich *am Ort der stationären Einrichtung zur Prüfung vorzuhalten*.

Anders als auf den ersten Blick ersichtlich, soll diese Vorschrift den Befugniskatalog der Kontrollbehörde aber nicht auf eine reine Vor-Ort-Kontrolle beschränken. Sie soll vielmehr lediglich sicherstellen, dass die Prüfbehörde nicht an eine ortsfremde Zentrale des Trägers verwiesen wird, der Kommunale Sozialverband Sachsen konnte hierfür auf eine entsprechende Entscheidung des Verwaltungsgerichts Würzburg, Urteil vom 15. Januar 2008 (Az.: W 1 K 07.882) verweisen.

Das Anfertigen von Kopien bestimmter Unterlagen zu deren Auswertung im Rahmen der Überprüfung von Einrichtungen nach dem Sächsischen Betreuungs- und Wohnqualitätsgesetz halte ich dabei für zulässig. Insoweit hat mir die Kontrollbehörde schriftlich dargelegt, in welchen Fällen Bewohnerdokumentationen und Protokolle anderer Prüfinstitutionen in Kopie abgefragt werden. Zudem gibt es eine konkrete Handlungsanweisung für die Mitnahme kopierter Unterlagen, sie ist Bestandteil eines schriftlichen Prüfkatalogs für SGB XI-Einrichtungen, der nach Mitteilung des Kommunalen Sozialverbands Sachsen mit dem SMS abgestimmt ist.

10.2.5 Antragsformular auf Leistungen der Pflegeversicherung

An mich wurde die Bitte herangetragen, ein Antragsformular der meiner Kontrolle unterliegenden Krankenkasse zu prüfen. Bei dem Formular handelte es sich um ein Antragsformular auf Leistungen der Pflegeversicherung, also um Leistungen nach dem Sozialgesetzbuch Elftes Buch.

Bedenken bestanden hinsichtlich des im Antragsformular anzugebenden Namens sowie der Anschrift des Pflegedienstes bzw. des Pflegeheims. Zudem wurde die im Antrag vom Antragsteller abgeforderte Einwilligungserklärung zur Übermittlung des Pflegegut-

achtens an den behandelten Arzt zu dessen Information kritisiert, wie auch die Abfrage einer Einwilligungserklärung für den MDK.

Datenschutzrechtliche Bedenken hinsichtlich der im Formular abgefragten Angabe des Pflegeheimes oder der Behinderteneinrichtungen habe ich im Hinblick auf die vom MDK durchzuführende körperliche Begutachtung nicht. Gleiches gilt für die Angabe des Pflegedienstes, da nach meiner Kenntnis die Abrechnung des Leistungserbringers (Pflegedienst) direkt mit der Pflegekasse erfolgt und damit klargestellt ist, welcher Leistungserbringer nach Wahl des Versicherten mit der Krankenkasse direkt abrechnen darf.

Die im Formular abgefragte Einwilligungserklärung zur Information des Arztes halte ich von der Grundlage des § 67b SGB X für gedeckt.

Die Einwilligungserklärung betreffend den MDK beruht auf § 18 Abs. 4 SGB XI: Nach dieser Vorschrift soll der MDK oder die von der Pflegekasse beauftragten Gutachter, soweit der Versicherte *einwilligt*, die behandelnden Ärzte des Versicherten, insbesondere die Hausärzte, in die Begutachtung einbeziehen und ärztliche Auskünfte und Unterlagen über die für die Begutachtung der Pflegebedürftigkeit wichtigen Vorerkrankungen sowie Art, Umfang und Dauer der Hilfebedürftigkeit einholen. Mit *Einverständnis* des Versicherten sollen auch pflegende Angehörige oder sonstige Personen oder Dienste, die an der Pflege des Versicherten beteiligt sind, befragt werden.

10.2.6 Betreutes Wohnen in Gastfamilien - Erhebungsbogen

Mir wurde ein Erhebungsbogen zur Geeignetheit einer Gastfamilie zur Aufnahme eines erwachsenen Menschen mit Behinderungen zur Kenntnis gegeben.

Das Betreute Wohnen in Gastfamilien ist eine Maßnahme der Eingliederungshilfe nach § 54 SGB XII in Verbindung mit § 55 SGB IX. Erwachsene Menschen mit Behinderung leben in einer Gastfamilie und werden von ihr betreut. Die Gastfamilie erhält dafür ein monatliches Betreuungsgeld, Unterkunfts- und Lebensunterhaltskosten.

Gastfamilien benötigen für die Versorgung des Gastbewohners keine spezielle sozialpädagogische Ausbildung. Selbstverständlich bedarf es jedoch der Prüfung, ob eine Gastfamilie tatsächlich geeignet ist, einen behinderten Menschen aufzunehmen und zu betreuen. Hierfür kommt ein entsprechender Erhebungsbogen zum Einsatz, der eruieren soll, wie der Bewohner in das Familienleben integriert werden kann.

Dabei werden neben allgemeinen Angaben über die Gastfamilie auch Angaben zu Bildung und Beruf erfragt wie auch zu den sozialräumlichen Bedingungen (Wohnsitua-

tion, verfügbarer Raum für den Gastbewohner, Haustiere, Mobilität der Gastfamilie) und Fragen zur Sicherstellung der Teilhabe und eben auch zur Integration des Gastbewohners in das Familienleben (Tagesablauf, Einbeziehung in Aktivitäten der Gastfamilie, auch im Freizeitbereich).

Ich habe im Ergebnis keine Einwände gegen diese Datenabfrage erhoben.

10.2.7 Überprüfung der zweckentsprechenden Mittelverwendung bei einer Kindertageseinrichtung in freier Trägerschaft durch den öffentlichen Träger

Es ist die Anfrage an mich herangetragen worden, ob es zulässig sei, sich von einer Kindertageseinrichtung eines freien Trägers die Arbeits- wie insbesondere auch die Betreuungsverträge vorlegen zu lassen, um im Rahmen eines seitens des öffentlichen Trägers im Einzelfall als notwendig eingestuften Überprüfungsverfahrens eine zweckentsprechende Mittelverwendung des freien Trägers prüfen zu können.

In dem vom freien Träger vorzulegenden Betreuungsvertrag an den öffentlichen Träger sind bestimmte personenbezogene Daten des Kindes und seiner Eltern durch den Mitarbeiter der freien Jugendhilfe festgehalten. Der Träger der öffentlichen Jugendhilfe ist eine in § 61 SGB VIII i. V. m. § 35 SGB I genannte Stelle, da er Leistungsträger ist. Die personenbezogenen Daten des Hilfeempfängers, die der Sozialleistungsträger erheben möchte, sind Sozialdaten nach § 61 SGB VIII, § 67 Abs. 1 SGB X. Insoweit ist zum Schutz des Hilfeempfängers von der Bestimmung des § 35 Abs. 1 Satz 1 SGB I auszugehen, nach der jeder Anspruch darauf hat, dass die ihn betreffenden Daten von den Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden.

Unter Beachtung dieser Vorgaben begegnet die Prüfung der Betreuungs- und Arbeitsverträge keinen datenschutzrechtlichen Bedenken.

Die Befugnis der zuständigen Stelle des betreffenden Trägers der öffentlichen Jugendhilfe, also hier des bei ihm eingerichteten Jugendamtes (§ 69 Abs. 3 SGB VIII), die betreffenden Daten zu erheben, folgt aus § 62 SGB VIII, § 67a SGB X. Danach ist das Erheben von (Sozial-)Daten zulässig, soweit ihre Kenntnis zur Erfüllung einer der Behörde durch Gesetz - hier Sozialgesetzbuch Achtes Buch - zugewiesenen Aufgabe erforderlich ist.

Die Aufgabe, um deren Erfüllung es hier geht, ist die Prüfung der ordnungsgemäßen Mittelverwendung erbrachter Geldleistungen zur Erfüllung einer der in § 2 SGB VIII genannten Aufgaben. Vielfach werden Leistungen wie hier im Bereich der Förderung von Kindern in Tageseinrichtungen von freien Trägern durchgeführt, finanziert von Trä-

gern der öffentlichen Jugendhilfe auf der Grundlage einer mit dem freien Träger abzuschließenden Vereinbarung (§ 77 SGB VIII). In solchen Vereinbarungen sind gemäß § 17 Abs. 5 LJHG leistungsgerechte Entgelte zugrunde zu legen, die den Trägern der freien Jugendhilfe - bei sparsamer und wirtschaftlicher Betriebsführung - die erforderliche Hilfegewährung ermöglichen. Die Vereinbarungen haben den Grundsätzen der Wirtschaftlichkeit, Sparsamkeit und Leistungsfähigkeit zu entsprechen.

Aber auch wenn Leistungen der Jugendhilfe von Trägern der freien Jugendhilfe wahrgenommen werden, bleibt der Träger der öffentlichen Jugendhilfe dem Hilfeempfänger gegenüber für die ordnungsgemäße Gewährung von Sozialleistungen verantwortlich, da nur ihn die gesetzliche Leistungspflicht trifft (§ 17 Abs. 1 Satz 2 LJHG).

Im Bereich der Förderung von Kindern in Kindertagesstätten hat daher das Jugendamt auch die Finanzierung der Leistungsangebote zu gewährleisten. Um dieser Verantwortung gerecht werden zu können, muss das zuständige Jugendamt als Träger der öffentlichen Jugendhilfe die durch den Träger der freien Jugendhilfe erbrachten Leistungen und damit verbundenen Leistungsabrechnungen entsprechend überprüfen können.

Selbstverständlich gilt auch hier, dass die Datenerhebung nur im erforderlichen Umfang zulässig ist.

Die mit der Einsichtnahme in die jeweiligen Verträge verbundene Datenerhebung überschreitet dabei das erforderliche Maß nicht, einer Anonymisierung der Betreuungsverträge bedarf es meiner Auffassung nach, namentlich im Hinblick auf § 15 Abs. 1 Satz 3 und Abs. 5 SächsKitaG, nicht. Insoweit ist zu beachten: Wenn der betreffende Träger der öffentlichen Jugendhilfe (kreisfreie Stadt oder Landkreis) selbst die Leistungen im Bereich der Förderung von Kindern in Kindertagesstätten erbrächte, müssten ebenfalls, um eine interne Aufsicht zu ermöglichen, die entsprechenden Daten dem Jugendamt vorgelegt werden.

Ebenso halte ich es nicht für zwingend, eine Prüfung der Unterlagen ausschließlich in den Räumen des freien Trägers zuzulassen, wobei im Falle der Abfrage von Kopien mit personenbezogenem Inhalt konkrete technische und organisatorische Sicherheitsmaßnahmen zum Schutz vor Einsichtnahme unbefugter Personen zu treffen sind und auch sicherzustellen ist, wie mit den Unterlagen nach Abschluss der Überprüfung verfahren wird.

10.2.8 Übermittlung von psychologischen Gutachten (Jobcenter)

Der Datenschutzbeauftragte eines kommunalen Jobcenters wandte sich mit der Frage an mich, ob ein eingeholtes psychologisches Gutachten vollständig in Kopie an den Betroffenen herausgegeben werden dürfe.

Ich habe diese Anfrage unter Hinweis auf meine Ausführungen in 14/10.2.3 beantwortet, wonach die Überlassung des Gutachtens vom Auskunftsanspruch nach § 83 SGB X umfasst ist. § 83 Abs. 1 Satz 5 SGB X verweist jedoch auch für die Auskunftserteilung auf § 25 Abs. 2 SGB X. Dieser sieht vor, dass - soweit Akten Angaben über gesundheitliche Verhältnisse des Betroffenen enthalten - die Behörde den Akteninhalt durch einen Arzt vermitteln lassen kann. Sie soll es, soweit durch die Akteneinsicht unverhältnismäßige Nachteile für den Betroffenen drohen. Die Regelung gilt entsprechend, wenn Akten Angaben, die Entwicklung und Entfaltung der Persönlichkeit des Betroffenen betreffend, enthalten. In diesem Fall kann bzw. soll die Behörde den Akteninhalt von einem durch seine Vorbildung hierfür geeigneten Bediensteten vermitteln lassen.

Allerdings stellte sich in diesem Zusammenhang die Frage, ob das Jobcenter überhaupt derart sensible Daten, die eine Vermittlung des Akteninhalts erforderlich machen würden, erhalten dürfte. Der Datenschutzbeauftragte des betreffenden Jobcenters hatte mir - selbstverständlich anonymisiert - ein entsprechendes Gutachten zur Verfügung gestellt, das nicht nur die für die Arbeitsvermittlung erforderlichen Fragen beantwortete, sondern auch umfassend zur persönlichen (Lebens-)Situation des Betroffenen in der Vergangenheit Stellung nahm.

Unstrittig war, dass die Jobcenter zur Feststellung der Leistungsfähigkeit des Betroffenen berechtigt sind, medizinische oder psychologische Gutachten einzuholen. Allerdings ist es ausreichend, wenn diese die zur Aufgabenerfüllung erforderlichen Fragestellungen beantworten. Hierbei ist zwar gegen eine kurze Begründung des Ergebnisses nichts einzuwenden, es bedarf jedoch keiner Darstellung der gesamten (ggf. vergangenen und gegenwärtigen) Lebenssituation des Betroffenen.

Ich habe daher vorgeschlagen, die psychologischen Gutachten - ebenso wie die medizinischen - zweigeteilt aufzubauen. Während der Teil, der die der Begutachtung zugrunde liegenden Daten enthält, beim Gutachter verbleibt, wird ein die Ergebnisse zusammenfassender Teil an das Jobcenter übermittelt. Im Ergebnis dürften die Leistungsakten - jedenfalls regelmäßig - keine Daten von derartiger Brisanz mehr enthalten, die eine Vermittlung durch einen Arzt oder Psychologen erforderlich machen würde.

Das anfragende Jobcenter hatte bisher immer das gesamte Gutachten erhalten. Es hat seine Vorgehensweise meinem Vorschlag entsprechend umgestellt.

10.2.9 Anwesenheitslisten in Kindertagesstätten

Im Berichtszeitraum wandten sich mehrere Petenten mit der Frage an mich, wie mit den Bringe- und Abhollisten in Kindertagesstätten zu verfahren sei. Datenschutzrechtliche Bedenken bestanden vor allem dahingehend, dass die Listen auslagen oder ausgehängt waren und somit die Eltern zugleich über Bringe- und/oder Abholzeiten aller anderen Kinder informiert wurden.

Ich habe zu diesen Sachverhalten die folgende Auffassung vertreten:

Grundsätzlich ist die Erhebung der Bringe- und Abholzeit zulässig. Für Einrichtungen in öffentlicher Trägerschaft ergibt sich dies aus § 62 Abs. 1 SGB VIII, wonach Sozialdaten erhoben werden dürfen, wenn dies zur Erfüllung der jeweiligen Aufgabe erforderlich ist.

Die Bringe- und Abholzeiten sind für die Gebührenbemessung relevant. Auch haftungsrechtlich können die Zeiten relevant sein. Eine Erforderlichkeit für die Aufgabenerfüllung war zu bejahen, sodass die Daten zulässigerweise erhoben werden dürfen.

Durch das Auslegen oder Aushängen der Listen erhalten jedoch sämtliche Eltern die Möglichkeit die Bringe- oder Abholzeiten aller in der Kindertagesstätte betreuten Kinder zur Kenntnis zu nehmen. Dies stellt eine Datenübermittlung dar. § 67 Abs. 6 Nr. 3 SGB X definiert die Übermittlung als das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Sozialdaten an einen Dritten durch Weitergabe der Daten an den Dritten oder durch Einsicht oder Abruf des Dritten in hierfür bereitgehaltene Daten. Wenngleich die Daten der Anwesenheitslisten nicht für den Zweck (Kenntnisnahme der Daten durch die anderen Eltern) ausgehängt werden, wird diesen jedoch die Möglichkeit der uneingeschränkten Kenntnisnahme eingeräumt, ohne dass dies von Seiten der Kindertagesstätte noch in irgendeiner Weise beeinflusst werden könnte.

Gemäß § 64 Abs. 1 SGB VIII dürfen Sozialdaten nur zu dem Zweck übermittelt werden, zu dem sie erhoben worden sind. Zweck der Datenerhebung dürfte vorliegend regelmäßig die Gebührenabrechnung sein. Eine Übermittlung der Bringe- und Abholzeiten jedes einzelnen Kindes an alle Eltern, deren Kinder in der jeweiligen Kindertageseinrichtung betreut werden, ist hierfür jedoch nicht erforderlich.

Ich habe daher den Petenten mitgeteilt, dass die Listen möglichst von den Erzieherinnen in der Weise zu führen sind, dass Dritte hierin keine Einsicht nehmen können.

10.2.10 Übermittlung von Rohdaten einer Mietwerterhebung an das Sozialgericht

Im Berichtszeitraum wurde folgende Anfrage eines Landkreises an mich gerichtet:

Die Landkreise und kreisfreien Städte sind u. a. im Rahmen der Grundsicherung für Arbeitsuchende nach dem Sozialgesetzbuch Zweites Buch verpflichtet, die Höhe angemessener Aufwendungen für Unterkunft und Heizung nach einem sogenannten schlüssigen Konzept zu ermitteln. Erforderlich hierzu sind umfangreiche Datenerhebungen bei Vermietern, u. a. von Mieten, Betriebskosten, Heizkosten und Wohnflächen. Diese Datenerhebungen erfolgen vor allem bei kommunalen Trägern und Genossenschaften sowie einzelnen privaten Vermietern. Die erhobenen Daten enthalten keine Namen und Adressen; der kleinste Ortsbezug ist die Gemeinde. Mieterdaten sind in den erhobenen Daten nicht enthalten.

Der betroffene Landkreis war der Auffassung, dass die Rohdatensammlung für eine Mietwertermittlung schutzbedürftige Daten sowie Betriebs- und Geschäftsgeheimnisse von Eigentümern und Unternehmen enthält. Trotz weitgehend anonymer Verarbeitung ließen sich Profile über Preise, Erträge, Bestände, Leerstände und anderes ableiten. Hierbei handele es sich um nicht-öffentliche Wirtschaftsdaten der Unternehmen, die zu deren Schaden Verwendung finden könnten. Folglich käme eine unbeschränkte Einsichtnahme durch Kläger im sozialgerichtlichen Verfahren in die Rohdaten nicht in Betracht.

Im Ergebnis musste ich feststellen, dass diese Sachverhalte nicht in meinen Zuständigkeitsbereich fallen.

Das Sozialgeheimnis des § 35 Abs. 1 SGB I gewährt jedem einen Anspruch darauf, dass die ihn betreffenden Sozialdaten von Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden. Bezüglich des Begriffs der Sozialdaten verweist § 35 Abs. 1 Satz 1 SGB I auf § 67 Abs. 1 Satz 1 SGB X. Danach sind Sozialdaten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), die von einer in § 35 SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch erhoben, verarbeitet oder genutzt werden. Mangels Personenbezug handelt es sich bei den Rohdaten nicht um Sozialdaten i. S. d. § 67 Abs. 1 Satz 1 SGB X. § 35 Abs. 4 SGB I stellt Betriebs- und Geschäftsgeheimnisse Sozialdaten gleich. § 67 Abs. 1 Satz 2 SGB X definiert Betriebs- und Geschäftsgeheimnisse als betriebs- oder geschäftsbezogene Daten, die Geheimnischarakter haben. Geheimnischarakter haben alle Tatsachen, die nur einem beschränkten Personenkreis bekannt sind und an deren Geheimhaltung derjenige, den sie betreffen, ein von

seinem Standpunkt begründetes (schutzwürdiges) Interesse hat (Bieresborn in von Wulffen, SGB X-Kommentar, § 67 Rdnr. 14; Mrozynski, SGB I-Kommentar, § 35 Rdnr. 32 m. w. N.). Es kann sich auch um Daten von juristischen Personen handeln. Erfasst werden juristische Personen des öffentlichen und des privaten Rechts (Bieresborn in von Wulffen, a. a. O., § 67 Rdnr. 15). Betriebs- und Geschäftsgeheimnisse unterfallen daher dem Sozialgeheimnis.

Ob Mieten, Heizkosten und Betriebskosten von Wohnungen Geheimnischarakter haben, ist meines Erachtens zweifelhaft. Zum einen finden sich derartige Daten - soweit vorhanden - in Mietspiegeln, zum anderen sind sie ggf. auch auf andere Weise zugänglich (Internetrecherche etc.). Entsprechendes gilt für Leerstände, die - zugegebener Weise mit etwas Aufwand - ohne weiteres erkennbar sind oder sich auch aus einer Internetrecherche ergeben könnten.

Darüber hinaus war zu berücksichtigen, dass anonymisierte und aggregierte Daten nicht unter die Schutzpflicht fallen (Mrozynski, a. a. O., § 35 Rdnr. 33). Während bei ersteren kein Personenbezug mehr herstellbar ist, handelt es sich bei letzteren um eine Zusammenfassung in Datengruppen, die wiederum bei demjenigen zu Sozialdaten werden können, der über das Mittel zur Individualisierung verfügt. Auch unter diesem Gesichtspunkt unterfallen die Daten nicht dem Sozialdatenschutz. Da Mieterdaten ohnehin nicht enthalten sind, kommen nur vermieterbezogene Daten in Betracht. Da es sich bei den Vermietern in der Regel um (öffentliche) Unternehmen handelt, können diese Daten nicht als Sozialdaten im Sinne des § 67 Abs. 1 Satz 1 SGB X charakterisiert werden.

Im Ergebnis ist daher festzuhalten, dass es sich mangels Bezug zu einer natürlichen Person nicht um Sozialdaten im Sinne des § 67 Abs. 1 Satz 1 SGB X handelt. Entscheidend für die Frage, ob vorliegend Betriebs- und Geschäftsgeheimnisse betroffen sind, ist, ob die erhobenen Daten Geheimnischarakter haben. Wenngleich ich hiervon nicht ausgehen würde, fehlte es mir für die Prüfung an einer hinreichenden Informationsgrundlage.

Ich musste diese Frage jedoch ohnehin unbeantwortet lassen. Denn gemäß § 81 Abs. 1 SGB X kann jemand, der der Auffassung ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Sozialdaten in seinen Rechten verletzt worden zu sein, sich an den jeweils zuständigen Datenschutzbeauftragten wenden. Das Recht ist nach § 81 Abs. 1 SGB X auf personenbezogene Sozialdaten beschränkt. Die Möglichkeit den Datenschutzbeauftragten bezüglich des Umgangs mit Betriebs- und Geschäftsgeheimnissen anzurufen, sollte nach dem Willen des Gesetzgebers nicht eröffnet werden (vgl. BT-Drs. 12/6334 S. 11 f.).

Das Ergebnis wird durch das sächsische Landesrecht bestätigt. Denn § 25 Abs. 1 SächsDSG bestimmt, dass zur Wahrung des Rechts auf Datenschutz und zur Unterstützung bei der Ausübung der parlamentarischen Kontrolle beim Sächsischen Landtag der Sächsische Datenschutzbeauftragte berufen wird. Gemäß § 27 Abs. 1 SächsDSG kontrolliert der Sächsische Datenschutzbeauftragte bei den öffentlichen Stellen die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz. Zweck des Sächsischen Datenschutzgesetzes ist es ausweislich dessen § 1, den Einzelnen davor zu schützen, dass er im Freistaat Sachsen durch Behörden oder sonstige öffentliche Stellen bei der Verarbeitung personenbezogener Daten in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt wird. Das Gesetz ist Ausfluss des aus dem allgemeinen Persönlichkeitsrecht abgeleiteten Grundrechts auf informelle Selbstbestimmung, das unter anderem in Art. 33 SächsVerf seinen Niederschlag gefunden hat.

Obgleich die erhobenen Rohdaten möglicherweise vom Schutz des Sozialgeheimnisses des § 35 SGB I erfasst waren, fiel dieser Sachverhalt nicht in meinen Zuständigkeitsbereich, sodass ich in der Sache keine weitergehende Stellungnahme abgeben konnte.

10.2.11 Verlangen nach vollständiger Vorlage ungeschwärzter Kontoauszüge bei der Gewährung von Wohngeld

Auch in diesem Berichtszeitraum hat mich die Frage nach der Zulässigkeit behördlicher Verlangen nach der Vorlage vollständiger, ungeschwärzter Kontoauszüge im Zusammenhang mit der Gewährung von Sozialleistungen beschäftigt.

Der Petent hatte Wohngeld beantragt. Er hatte angegeben, die Mietzahlungen jeweils bar zu begleichen. Zum Nachweis hierfür hatte er Quittungen des Vermieters über den Erhalt der Barzahlungen vorgelegt. Die Wohngeldbehörde, der bekannt war, dass zwischen dem Petenten und dessen Vermieter ein verwandtschaftliches Näheverhältnis bestand - es handelte sich um Vater und Sohn - bat um lückenlose Vorlage ungeschwärzter Kontoauszüge. Das zunächst äußerst weitreichende Verlangen, wurde später auf einen Zeitraum von drei Monaten beschränkt.

Ich habe die Wohngeldbehörde um Stellungnahme gebeten und unter Berücksichtigung der hierin vorgetragenen Aspekte zum Sachverhalt folgende Auffassung vertreten:

Wohngeld wird als Zuschuss zu den Aufwendungen für den selbst genutzten Wohnraum geleistet, sodass der Wohngeldberechtigte nachzuweisen hat, dass er die vereinbarten Aufwendungen trägt. Aus diesem Grund ist nicht allein auf die mietvertragliche Vereinbarung und/oder den entsprechenden Zufluss beim Vermieter abzustellen. Vielmehr ist nachzuweisen, dass der Haushalt des Antragstellers entsprechend belastet wird.

Nicht zuletzt unter Berücksichtigung dieses Aspektes erachte ich daher die Vorlage lückenloser Kontoauszüge für einen Zeitraum von bis zu drei Monaten als zulässig. Hintergrund ist hierbei, dass die vorgelegten Quittungen nicht in gleicher Weise geeignet sind, die Belastung des Antragstellers mit den Zahlungen zu belegen.

Grundsätzlich soll insoweit eine Einsichtnahme in die Originalkontoauszüge in einem Termin erfolgen und sodann lediglich die leistungserheblichen Buchungen kopiert werden. Im Hinblick auf die räumliche Situation wird den Antragstellern die Möglichkeit angeboten, die Kontoauszüge in Kopie vorzulegen. In diesem Fall wird die Einsichtnahme anhand der Kopien vorgenommen. Nicht für die Leistung relevante Buchungen werden sodann geschwärzt bzw. entsprechende Auszüge datenschutzgerecht vernichtet.

Diese Vorgehensweise, die die betreffende Wohngeldbehörde anwendet, wurde mit mir abgestimmt und begegnet keinen datenschutzrechtlichen Bedenken. Da entsprechendes für die auf den Zeitraum von drei Monaten beschränkte Vorlage der lückenlosen Kontoauszüge galt, ließ sich ein Verstoß gegen datenschutzrechtliche Bestimmungen nicht feststellen.

10.2.12 Plausibilitätsprüfung von Wohngeldanträgen

Aufgrund einer Eingabe war die datenschutzgerechte Durchführung von Plausibilitätsprüfungen bei der Gewährung von Wohngeld nach meinen Beiträgen in 8/10.2.5 und 15/10.2.16 erneut Gegenstand meiner Tätigkeit.

Der Petent, der sich an mich wandte, verfügte über ein Einkommen, das unter dem sozialhilferechtlichen Mindestbedarf lag. Er hatte einen Antrag auf Wohngeld gestellt und diesem alle geforderten Unterlagen beigefügt. Im Nachgang zu seinem Antrag erhielt er ein Schreiben der Wohngeldstelle mit diversen Auskunftsforderungen. Unter anderem wurde er aufgefordert, eine vollständige Aufstellung über seine monatlichen Einnahmen und Ausgaben anzufertigen und dieser entsprechende Belege beizufügen. In dem Schreiben heißt es:

„*Hierzu bitten wir Sie[,] uns mitzuteilen, wie Sie mit den Ihnen derzeitig zur Verfügung stehenden Einnahmen und Ausgaben Ihren Lebensunterhalt bestreiten. Fertigen sie dazu eine vollständige Aufstellung über Ihre monatlichen Einnahmen und Ausgaben (z. B. Kosten für Ernährung; Bekleidung[,] Hygieneartikel; Hausrat- und sonstige Versicherung; Kosten für Strom, Telefon, Handy, Rundfunk- und Fernsehgebühren; Kosten für Bekleidung (sic!), laufende Unterhaltskosten für eine[n] PKW; Kosten für Wasser, Abwasser, Müllgebühren, Essenkehrer, Heizkosten, Kosten für Gebäude- und Haftpflichtversicherung [sic!], ...) an und belegen Sie Ihre Angaben mit entsprechenden*

Nachweisen (z. B. Kopien der Rechnungen, Gebührenbescheide sowie entsprechende Zahlungsnachweise wie z. B. Kopien der Kontoauszüge, …) zu belegen.“

Nach der Rechtsgrundlage für die beabsichtigte Erhebung der vorstehend vom Landratsamt erbetenen Daten befragt, teilte dieses mit, dass meine Ausführungen aus dem 8. und 12. Tätigkeitsbericht zur datenschutzgerechten Ausgestaltung einer sogenannten Plausibilitätsprüfung bekannt seien. Abweichend davon verzichte man im Landkreis auf ein persönliches Gespräch. Ein persönliches Erscheinen des Antragstellers bei der Behörde erachte man aufgrund der territorialen Gegebenheiten sowie der Infrastruktur als unverhältnismäßig.

Diese Aussage verwunderte mich, da die datenschutzgerechte Vorgehensweise in den Jahren 1999/2000 gemeinsam mit dem SMI als oberste Fachaufsichtsbehörde erarbeitet worden war.

Auf Nachfrage teilte das SMI mit, dass es meine letzte Kritik in 15/10.2.16 an der Durchführung der Plausibilitätsprüfungen zum Anlass genommen habe, nochmals im Erlasswege auf die Anforderungen an eine datenschutzgerechte Ausgestaltung der Plausibilitätsprüfungen hinzuweisen. Das Schreiben aus dem Jahr 2012 wurde mir vorgelegt. In diesem wird unter anderem Folgendes ausgeführt:

„*Datenschutzgerecht ist eine solche Prüfung im Rahmen eines Gesprächs durchzuführen, dessen Ergebnis zu protokollieren ist. Nachweise über jede einzelne Ausgabe sind durch den Antragsteller dabei nicht zu erbringen. Ihre Anforderung durch die Wohngeldbehörde wäre ein Verstoß gegen § 67 Abs. 1 Zehntes Buch Sozialgesetzbuch (SGB X) i. V. m. §§ 13 ff. WoGG, wonach die Erhebung von Sozialdaten nur zur Feststellung des Einkommens zulässig ist.*“

Es war daher für mich nicht nachvollziehbar, weshalb der Landkreis nunmehr erneut von der datenschutzgerechten Vorgehensweise abwich.

Ich habe den Landkreis angehört und letztlich von meinem Beanstandungsrecht gemäß § 29 SächsDSG Gebrauch gemacht.

Der Landkreis hat im Rahmen der Anhörung den Sachverhalt nicht bestritten. Zum datenschutzrechtlich unzulässigen Vorgehen sei es durch mangelnde gedankliche Präsenz des Erlasses aus dem Jahr 2000 gekommen. Außerdem entspräche das im landeseinheitlichen Wohngeldverfahren hinterlegte Musterschreiben nicht dem Erlass aus dem Jahr 2000, weshalb Zweifel an der Korrektheit des Vorgehens nicht aufgetreten seien. Ferner

wies der Landkreis im Wesentlichen auf Praktikabilitätsgesichtspunkte hin, die aus meiner Sicht keine andere Rechtsauffassung zu begründen vermochten.

Ungeachtet der mangelnden gedanklichen Präsenz des Erlasses des SMI aus dem Jahre 2000 habe ich eine Beanstandung ausgesprochen, da zumindest meine Ausführungen im 8. und 15. Tätigkeitsbericht bekannt waren und auch aufgrund derer eine vertiefte Auseinandersetzung mit dem eigenen Handeln hätte erfolgen können.

In rechtlicher Hinsicht ist die Durchführung der Plausibilitätsprüfung im Rahmen eines persönlichen Gesprächs aus nachstehenden Gründen erforderlich:

Gemäß § 67a Abs. 1 Satz 1 SGB X ist das Erheben von Sozialdaten durch die in § 35 SGB I genannten Stellen zulässig, wenn die Kenntnis der Daten zur Erfüllung einer Aufgabe der erhebenden Stelle nach einem der Sozialgesetzbücher erforderlich ist.

Das Wohngeld dient der wirtschaftlichen Sicherung angemessenen und familiengerechten Wohnens (vgl. § 1 Abs. 1 WoGG). Es richtet sich u. a. nach dem Gesamteinkommen (vgl. § 4 Nr. 3 WoGG), das nach Maßgabe der §§ 13 ff. WoGG zu ermitteln ist.

Die Durchführung der Plausibilitätsprüfung erfolgt aus nachstehenden Gründen:

Häufig seien sich Antragsteller nicht bewusst, über welche Einnahmen sie verfügen. Daher werde das Einkommen oft zu gering angegeben, sodass sich ein Missverhältnis zwischen angegebener Miethöhe und dem angegebenen Einkommen ergebe. Liste der Antragsteller seine Ausgaben auf, ergebe sich oft, dass diese die angegebenen Einnahmen übersteigen. Da nicht davon auszugehen sei, dass der Antragsteller ständig über seine Verhältnisse lebe, sei sein Einkommen wahrscheinlich größer als ursprünglich angegeben.

Ausgehend von Vorstehendem ist die Erhebung von Daten zu den Gesamtausgaben zulässig. Diese kann zulässigerweise auch über die Erhebung von einzelnen Ausgabepositionen und deren Addition erfolgen (vgl. hierzu 8/10.2.5).

Allerdings ist die Forderung nach Vorlage von Nachweisen für jede einzelne Ausgabe unzulässig (vgl. hierzu 15/10.2.16). Denn die Angaben zur Höhe der Ausgaben werden allein als Hilfstatsachen zur Aufdeckung versteckter Einnahmen erhoben. Zu diesem Zweck ist keine detaillierte Kenntnis der einzelnen Ausgaben erforderlich, sodass eine diesbezügliche Datenerhebung ausscheidet.

Die Zulässigkeit der Speicherung der erhobenen Daten richtet sich nach § 67c Abs. 1 Satz 1 SGB X. Hiernach ist das Speichern von Sozialdaten durch die in § 35 SGB I ge-

nannten Stellen zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden gesetzlichen Aufgaben nach einem der Sozialgesetzbücher erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind.

Eine Speicherung der erhobenen Einzelangaben zu den Ausgaben ist unzulässig, da diese Daten zur Aufgabenerfüllung nicht erforderlich sind. Die Einzelangaben zu den Ausgaben dienen allein dem Zweck, durch Addition derselben die Gesamtausgaben zu ermitteln. Die Gesamtausgaben ihrerseits dienen - ausgehend von der Annahme, dass der Betroffene nicht ständig über seine Verhältnisse lebt - dazu, seine tatsächlichen Einnahmen zu ermitteln. Aus diesem Grund ist es unerheblich, welcher Betrag auf welche Ausgabeposition entfällt. Irrelevant sind ferner geringfügige Über- oder Unterschreitungen der angegebenen Ausgaben in einzelnen Monaten. Entscheidend ist die Höhe der (durchschnittlichen) Gesamtausgaben. Denn hieraus ergibt sich der zu deckende Bedarf. Eine Cent-genaue Ermittlung der monatlichen Ausgaben ist hierfür nicht erforderlich.

Für die Speicherung der Nachweise, mit denen die einzelnen Ausgabepositionen belegt werden sollen, gilt das vorstehend Ausgeführte entsprechend. Auch deren Speicherung ist nach Maßgabe des § 67c Abs. 1 Satz 1 SGB X nicht zulässig.

Im Ergebnis ist daher festzuhalten, dass einzig die Datenerhebung bezüglich einzelner Ausgabepositionen zulässig ist. Diese Ermittlung der einzelnen Ausgabepositionen dient dazu, durch Addition die Gesamtausgaben und somit den zu deckenden Bedarf zu ermitteln, da sich hieraus die (wahrscheinlichen) Einnahmen des Antragstellers ergeben. Aus der Zwecksetzung der sogenannten Plausibilitätsprüfung folgt, dass die Forderung der Vorlage von Nachweisen nicht von der behördlichen Datenerhebungsbefugnis gedeckt ist. Darüber hinaus ist sowohl eine Speicherung der erhobenen Einzeldaten als auch - erst recht - eine Speicherung etwaiger Nachweise zu den Einzelangaben unzulässig.

Aus dieser Rechtslage ergeben sich aufgrund des Zwecks der Plausibilitätsprüfung im Wohngeldverfahren verfahrensrechtliche Anforderungen an deren Ausgestaltung.

Diese verfahrensrechtliche Anforderung bezieht sich auf die Art der Datenerhebung. Für die Plausibilitätsprüfung ist die Durchführung der Datenerhebung in einem Gespräch datenschutzrechtlich geboten. Eine Datenerhebung auf schriftlichem Weg scheidet aufgrund der hiermit einhergehenden Dokumentationspflichten und den Anforderungen an eine ordnungsgemäße Aktenführung aus. Die Anforderungen an eine ordnungsgemäße Aktenführung sind Ausfluss des Rechtsstaatsprinzips und dienen der Transparenz, der Nachvollziehbarkeit sowie der Überprüfbarkeit der Rechtmäßigkeit des Verwaltungshandelns.

Reichte ein Antragsteller Angaben zu den Ausgaben schriftlich ein, müsste das Schreiben in die Verwaltungsakte aufgenommen werden. Andernfalls wäre ein hierauf gegründetes Verwaltungshandeln weder transparent noch nachvollziehbar und auch dessen Rechtmäßigkeit ließe sich nicht überprüfen. Auch eine Vorgehensweise dergestalt, dass die Einreichung der Daten in Schriftform gefordert und dieses Schreiben im Nachgang vernichtet wird, kommt nicht in Betracht. Eine solche Vorgehensweise ist zum einen fehleranfällig (Übertragungsfehler/Additionsfehler). Ferner kommt es hierdurch zu einem Verlust der Dokumentationsfunktion der Verwaltungsakte. Überdies ist diese Vorgehensweise für den Antragsteller nicht mehr transparent, da er keine Kenntnis über den Inhalt der Speicherung hat.

10.2.13 Einholung von Mietbescheinigungen bei Dritten

Die in unterschiedlichen Zusammenhängen immer wiederkehrende Frage, wann die Einholung einer Mietbescheinigung bei einem Dritten zulässig ist, beschäftigte mich auch in diesem Berichtszeitraum wieder.

Ein Petent wandte sich an mich und schilderte folgenden Sachverhalt:

Nachdem er seine Nebenkostenabrechnung beim Jobcenter eingereicht hatte, wurde er aufgefordert, eine Mietbescheinigung auszufüllen. Der Petent verweigerte dies, da er der Auffassung war, dass aufgrund des vorliegenden Mietvertrages bereits alle erforderlichen Daten bei der Behörde vorhanden seien. In der Folge wandte sich das Jobcenter ohne weitere Nachricht an die Vermieterin des Petenten und bat diese um Auskunft.

Ich habe diesen Sachverhalt zum Anlass genommen, um bei dem Jobcenter nachzufragen, ob und gegebenenfalls unter welchen Voraussetzungen von diesem Vermieterbescheinigungen eingeholt werden und weshalb der Betroffene hiervon nicht in Kenntnis gesetzt wird.

Auf meine Nachfrage konnte mir das Jobcenter glaubhaft darlegen, dass es im Zusammenhang mit der vom Petenten vorgelegten Nebenkostenabrechnung Unklarheiten gegeben habe, die durch die Mietbescheinigung erklärt werden sollten.

Der Vermieter werde nur angeschrieben, wenn der Leistungsberechtigte seinen Mitwirkungspflichten nicht nachkomme *und* die Angaben für die Leistungsgewährung unbedingt erforderlich seien. Rechtsgrundlage sei in diesen Fällen § 67a Abs. 2 Nr. 2 Buchst. b) Doppelbuchst. aa) SGB X. Danach dürfen personenbezogene Daten ohne Mitwirkung des Betroffen nur erhoben werden, wenn die Aufgaben nach diesem Gesetzbuch - gemeint ist eines der Sozialgesetzbücher - ihrer Art nach eine Erhebung bei

anderen Personen oder Stellen erforderlich machen und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

Das Jobcenter ging davon aus, dass diese Voraussetzungen bereits dann gegeben wären, wenn der Betroffene seinen Mitwirkungspflichten nach §§ 60 ff. SGB I nicht nachkomme.

Dieser Rechtsauffassung konnte ich trotz vielfältiger Einwände, die gegen meine Auffassung geltend gemacht wurden, nicht beitreten. Hierfür waren nachstehende Gründe maßgeblich:

Dass die Behörde den Versuch der Datenerhebung beim Betroffenen unternommen hat, zeigt, dass sie eine Datenerhebung beim Betroffenen für erfolgversprechend hielt. Folglich kann nicht davon ausgegangen werden, dass die behördlichen Aufgaben eine Datenerhebung bei Dritten erforderlich machten.

Dies gilt auch, wenn die Datenerhebung beim Betroffenen letztlich nicht erfolgreich war, weil dieser erklärt hat, am Verfahren nicht (mehr) mitzuwirken. Denn hieraus resultiert keine Erweiterung der Datenerhebungs- und -verarbeitungsbefugnisse. Vielmehr sind derartige Fallgestaltungen über § 66 SGB I zu klären. Hiernach dürfen Leistungen versagt oder entzogen werden, wenn derjenige, der die Leistung erhält oder beantragt hat, den in § 66 Abs. 1 Satz 1 SGB I genannten Mitwirkungspflichten nicht nachkommt und hierdurch die Sachverhaltsaufklärung wesentlich erschwert wird und daher die Leistungsvoraussetzungen nicht nachgewiesen sind.

10.2.14 Keine Übermittlungsbefugnis auf Grundlage des § 67a SGB X

Wird im Rahmen einer zulässigen Datenerhebung bei Dritten die Übermittlung personenbezogener Daten des Betroffenen an diesen Dritten erforderlich, bedarf es hierfür des Vorliegens einer gesetzlichen Übermittlungsbefugnis oder einer Einwilligung des Betroffenen. Soweit in der behördlichen Praxis unter Berufung auf das Urteil des BSG vom 25. Januar 2012 (Az: B14 AS 65/11 R) hiervon zum Teil abweichende Auffassung vertreten wurde, kann dieser nicht gefolgt werden. Sie lässt sich auch dem genannten Urteil nicht entnehmen. Dort heißt es unter Rdnr. 22 (zitiert nach juris) ausdrücklich:

„*Soweit das LSG eine Offenbarungsbefugnis nach § 67a Abs. 2 Satz 2 Nr.2 Buchst. b) SGB X angenommen hat, kann dem nicht gefolgt werden.*“

Unter Rdnr. 23 führt das BSG weiter aus:

„*Unabhängig von der Beantwortung der Frage, ob und inwieweit § 67a Abs. 2 Satz 2 Nr.2 Buchst. b) SGB X eine Befugnis zum Offenbaren von Sozialdaten enthält, …*“

Diesen Ausführungen ist zu entnehmen, dass das BSG diese Frage offen gelassen hat. Wollte man diesem Urteil eine Tendenz entnehmen, so dürfte diese eher in Richtung der gegenteiligen Auffassung gehen. Denn dem Urteil des BSG sind im Folgenden Ausführungen zum Vorliegen einer Einwilligung bzw. einer gesetzlichen Übermittlungsbefugnis zu entnehmen. Für diese Auffassung dürfte zudem die Grundrechtsrelevanz der Thematik sprechen.

10.2.15 Profiling-Bogen des Jobcenters

Eine Petentin, die vom Jobcenter in Arbeit vermittelt werden sollte, wandte sich unter Vorlage eines sogenannten Profiling-Bogens an mich, da sie einzelne Datenerhebungen für unzulässig hielt. Ferner wurde gerügt, dass nach Auffassung der Petentin eine doppelte Datenerhebung vorläge, da mit dem Profiling-Bogen bereits erhobene Daten nochmals abgefragt würden. Ich konnte der Petentin mitteilen, dass die abgefragten Daten für die dauerhafte Vermittlung in Arbeit erforderlich sind und auch keine doppelte Datenerhebung vorlag, sodass der Fragebogen datenschutzgerecht ausgestaltet war.

Die Zulässigkeit der Datenerhebung richtet sich danach, welche Daten zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich sind (vgl. § 67a Abs. 1 Satz 1 SGB X). Bei den Jobcentern ist zwischen der Gewährung des Arbeitslosengeldes II und der Vermittlung in Arbeit zu differenzieren. Im Rahmen der Arbeitsvermittlung ist es Aufgabe der Jobcenter nach § 16 Abs. 1 Satz 2 Nr. 1 SGB II i. V. m. § 37 Abs. 1 SGB III eine sogenannte Potentialanalyse durchzuführen. Diesem Zweck dient der Profiling-Bogen. Inhalt der Potentialanalyse nach § 37 Abs. 1 SGB III ist die Feststellung vermittlungsrelevanter beruflicher und persönlicher Merkmale, beruflicher Fähigkeiten und Eignung sowie nach § 37 Abs. 1 Satz 2 SGB III die Feststellung derjenigen Umstände, die eine Vermittlung erschweren könnte.

Die Vorlage des Schulabschlusszeugnisses und des Ausbildungszeugnisses dient dem Nachweis, dass der angegebene Schul- bzw. Ausbildungsabschluss tatsächlich vorliegt. Da ein Einzelzeugnis, nicht jedoch alle Zeugnisse der gesamten Schul- bzw. Ausbildungszeit gefordert werden, ist dies datenschutzrechtlich unbedenklich. Da die Einzelnoten Auskunft über gewisse, vermittlungsrelevante Persönlichkeitsmerkmale geben können, ist die Anforderung der Zeugnisse zur Aufgabenerfüllung der Jobcenter erforderlich.

Die Vorlage einer etwaigen Anerkennung des ausländischen Abschlusses in Deutschland ist ebenfalls sachgerecht. Diese Information ist vermittlungsrelevant. Je nachdem, ob eine Anerkennung erfolgt ist bzw. erfolgen kann, können sich hieraus unterschiedliche Vermittlungswege ergeben. Während bei einer Anerkennung des ausländischen Abschlusses eine Vermittlung als Fachkraft in Betracht kommt, könnte bei einer Nichtanerkennung nur eine Vermittlung als ungelernte Kraft erfolgen.

Auch der Lebenslauf ist vermittlungsrelevant, da er über die beruflichen Stationen und deren Dauer und damit auch über die Berufserfahrung des zu Vermittelnden Auskunft gibt.

Zudem ist festzuhalten, dass Name, Geburtsdatum und Adresse nicht nochmals nach § 67 Abs. 5 SGB X erhoben, d. h. zielgerichtet beschafft werden. Die Angaben sind bereits eingetragen. Insoweit handelt es sich um eine Datennutzung im Sinne des § 67 Abs. 7 SGB X. Eine solche ist gemäß § 67c Abs. 1 Satz 1 SGB X zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden gesetzlichen Aufgaben erforderlich ist und für Zwecke erfolgt, für die die Daten erhoben worden sind. Die Durchführung des Profiling sowie die anschließende Vermittlung in Arbeit gehört zu den gesetzlich zugewiesenen Aufgaben der Jobcenter. Zudem müssen die Profiling-Bögen eindeutig den jeweiligen Personen zugeordnet werden können. Daher müssen bestimmte, die Person identifizierende Daten auf den Bögen angegeben werden. Die gewählte Vorgehensweise war daher datenschutzrechtlich nicht zu beanstanden.

Hinsichtlich der weiteren abgefragten Daten, beispielsweise zum Gesundheitszustand, zum sozialen Umfeld, etwaigen Vorstrafen und Schulden ist festzuhalten, dass auch diesbezüglich eine Datenerhebungsbefugnis des Jobcenters besteht. Bei derartigen Profiling-Maßnahmen sollen Vermittlungshemmnisse identifiziert und bei der Arbeitsvermittlung beachtet bzw. durch Leistungen der Jobcenter beseitigt werden. In Betracht kommen beispielsweise Leistungen der Schuldnerberatung oder Ähnliches. Denn Ziel derartiger Maßnahmen ist es nach dem Willen des Gesetzgebers, eine dauerhafte Eingliederung in das Arbeitsleben zu erreichen. Dieses Ziel würde verfehlt, wenn aufgrund der Unkenntnis über bestimmte Einschränkungen der zu vermittelnden Person eine Vermittlung in Tätigkeiten erfolgen würde, zu deren dauerhaften Erbringung die betroffene Person nicht in der Lage ist.

Die Angabe von Telefonnummer und E-Mail-Adresse ist freiwillig. Hierauf wurde das betreffende Jobcenter hingewiesen. Es hat aufgrund dieses Hinweises eine Änderung des Formulars vorgenommen.

10.2.16 Einführung von zentralen Anmelde- und Vermittlungsverfahren für Kindertagesstätten in Sachsen

Seit dem 1. August 2013 gibt es gemäß § 24 Abs. 2 Satz 1 SGB VIII einen Rechtsanspruch auf eine frühkindliche Förderung in Kindertagesstätten oder in Kindertagespflege für Kinder, die das erste Lebensjahr vollendet haben. Infolgedessen war ein großer Ansturm auf die ohnehin stark nachgefragten Plätze in den Kindertageseinrichtungen (Kita) zu verzeichnen.

Bislang war die Kita-Anmeldung für Eltern sehr zeitraubend und aufwendig. Oftmals haben die Eltern ihre Kinder in mehreren Einrichtungen angemeldet, um überhaupt eine reelle Chance auf einen der stark nachgefragten Kita-Plätze zu haben. Zur Bewältigung und Vermittlung dieser großen Bedarfsnachfrage haben einige Städte die Einführung eines elektronischen Vermittlungsportales geplant. Das Ziel dieser elektronischen Systeme soll die verlässliche Beratung, Vermittlung und Vergabe von Betreuungsplätzen in den Kindertageseinrichtungen und der Kindertagespflege sein.

Datenschutzrechtlich ist vorab festzulegen und zu prüfen, wer bei einem zentralen elektronischen Anmeldeverfahren auf die personenbezogenen Daten der Kinder und Eltern zugreifen darf und welche Daten in diesem Anmeldeprozess zwischen den beteiligten Stellen ausgetauscht werden dürfen.

Gemäß § 2 Abs. 2 Nr. 3 SGB VIII gehören Angebote zur Förderung von Kindern in Tageseinrichtungen und in der Tagespflege nach Maßgabe der §§ 22 bis 25 SGB VIII zu den Leistungen der Jugendhilfe. Diese Leistungen werden sowohl von freien Trägern als auch von Trägern der öffentlichen Jugendhilfe erbracht. Die durch das Sozialgesetzbuch Achtes Buch begründete Leistungsverpflichtung richtet sich dabei an die Träger der öffentlichen Jugendhilfe. Diese örtlichen Träger der öffentlichen Jugendhilfe sind gemäß § 69 Abs. 1 SDB VIII i. V. m. § 1 Abs. 1 LJHG die Landkreise und kreisfreien Städte. Deshalb habe ich auch die Einrichtung einer zentralen Anmelde- und Platzvergabe in zwei sächsischen Kommunen zur Erfüllung der Aufgabe der örtlichen Bedarfsplanung für erforderlich und damit zulässig gehalten.

Entsprechend den gesetzlichen Vorgaben sind die Träger der öffentlichen Jugendhilfe berechtigt, ausschließlich selbst eine zentrale Platzvergabe sicherzustellen und anzubieten. In datenschutzrechtlicher Hinsicht folgt daraus, dass nach § 62 SGB VIII der öffentliche Träger die Daten erheben darf, die für eine ordnungsgemäße Platzvergabe erforderlich sind. Dies sind die Grunddaten zu den betreffenden Kindern und seinen Eltern. Darüber hinaus können optionale Angaben weiterer Platzvergabekriterien erforderlich sein, die es den Eltern ermöglichen sollen, nähere Auswahlkriterien zur ge-

wünschten Kindereinrichtung, z. B. musische, sprachliche, religiöse oder sportliche Ausrichtung, zu machen.

Solange jedoch noch nicht ersichtlich ist, ob überhaupt ein Betreuungsvertrag zustande kommt, dürfen weiterführende Daten, wie z. B. gewünschte Mittagsverpflegung, ausländische Herkunft (für die Kinder- und Jugendhilfestatistik), Allergien und Erkrankungen der Kinder oder erzieherische Hilfe nach Sozialgesetzbuch Siebentes Buch nicht erhoben werden. Diese Daten dürfen erst bei Abschluss eines Betreuungsvertrages erhoben werden.

Im Weiteren habe ich darauf hingewiesen, dass bei einer Datenübermittlung von Bestandsdaten aus dem elektronischen Anmeldesystem, wie etwa verfügbare Plätze, Auslastung usw., diese Daten für Zwecke einer Bedarfsplanung oder Statistik zu anonymisieren sind.

Da im Bereich der Kinderbetreuung umfangreiche Sozialdaten erhoben und verarbeitet werden, sind die Beteiligung des zuständigen Datenschutzbeauftragten und die Durchführung einer *Vorabkontrolle nach § 10 SächsDSG* unbedingt notwendig. In vielen Fällen hat sich erneut gezeigt, dass die frühzeitige Einbindung des Datenschutzes in derartige Informationsverarbeitungsvorhaben auch erforderlich ist, um datenschutzrechtliche Anforderungen bereits mit Beginn der Entwicklung der Fachanwendungen erkennen und berücksichtigen zu können. Die Datenschutzprüfung der elektronischen Platzvermittlungssysteme umfasste sowohl die Fragestellung, welche Daten für die Anmeldung in der Kita erforderlich sind, als auch die Prüfung der technischen und organisatorischen Datenschutzmaßnahmen für das geplante System.

Die Projekte der geprüften sächsischen Kommunen bestehen beispielsweise aus je zwei Komponenten, einem elektronischen Anmeldeportal für die Vermittlung von Betreuungsplätzen in Kindertageseinrichtungen und einem Verwaltungsportal, die auch durch die freien Träger zur Verwaltung ihrer Kindertageseinrichtungen eingesetzt werden sollen. Alle Stellen haben verschiedene Anbieter der Softwarelösung für die Umsetzung dieser Projekte gewählt. In einem ersten Schritt sollten die Programmkomponenten für die elektronische Platzvergabe datenschutzrechtlich beraten und anschließend für die Nutzung freigegeben werden.

Die Prüfung, inwiefern die Eltern einen berechtigten Anspruch auf einen Betreuungsplatz haben, wird in den geprüften elektronischen Kita-Systemen sehr unterschiedlich gehandhabt. Es gibt Kommunen, welche bereits kurz nach der Geburt eines Kindes einen Berechtigungsschein für einen Betreuungsplatz ausstellen. In einem Kita-System wird die Berechtigung des Anspruchs auf einen Betreuungsplatz erst überprüft, wenn

die Eltern die Anmeldedaten bereits in das elektronische Anmeldeportal übermittelt haben. Um gewährleisten zu können, dass ein berechtigter Anspruch auf einen Kita-Platz besteht, die Schreibweise der Adressdaten korrekt ist und um zu verhindern, dass die Eltern Mehrfachanmeldungen in verschiedenen Einrichtungen vornehmen, werden die Anmeldedaten der Kinder sowie die Daten der Erziehungsberechtigten (z. B. Namen, Geburts- und Adressdaten) mit dem Melderegister der jeweiligen Meldebehörde abgeglichen.

Gemäß § 29 Abs. 6 SächsMG darf die Meldebehörde einer anderen Behörde oder sonstigen öffentlichen Stelle aus dem Melderegister die dort aufgezählten Daten von Einwohnern übermitteln, wenn dies zur Erfüllung der in ihrer Zuständigkeit oder der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich ist. Insoweit kann die Richtigkeit der Angaben des Antragstellers, ob tatsächlich ein Anspruch auf einen Kita-Platz besteht, im Vorfeld überprüft werden. Somit kann ausgeschlossen werden, dass die fehlende Anspruchsberechtigung erst nach der Vermittlung, beim Abschluss des Betreuungsvertrages festgestellt wird.

Neben der Tatsache, dass für einen Melderegisterabgleich die datenschutzrechtlichen Voraussetzungen geprüft werden mussten, habe ich gefordert, dass dieser Datenabgleich für die Betroffenen transparent gemacht wird und zumindest auf dem Elterninformationsblatt der verantwortlichen Stelle ein Hinweis zum Zweck des Meldedatenabgleichs erforderlich ist. Die nach Sächsischer Meldeverordnung vorgesehenen technischen und organisatorischen Maßnahmen sind auch für diesen Datenabgleich umzusetzen.

Bei dem elektronischen Kita-Anmeldesystem einer anderen geprüften Stelle wird für die Eltern die Suche freier Betreuungsplätze bei städtischen Trägern und von der Stadt geförderten Einrichtungen - Einrichtungen in freier Trägerschaft - insofern erleichtert, dass die Eltern nur die tatsächlich für den Anmeldezeitraum verfügbaren Betreuungsplätze in den Einrichtungen angezeigt bekommen. Im Sinne der Datensparsamkeit wird dadurch auch die zusätzliche Datenübermittlung der Anmeldedaten an diejenigen Einrichtungen verhindert, welche keine freien Platzkapazitäten im Antragzeitraum aufweisen.

Durch die Einführung der elektronischen Anmeldeverfahren soll die Vergabe von Betreuungsplätzen in Kindertageseinrichtungen für die Eltern, die Verwaltung und die Betreuungseinrichtung erleichtert und die ohnehin knappen Kapazitäten besser ausgelastet werden. Aber auch die elektronische Vermittlung von Plätzen kann fehlende Platzkapazitäten nicht ausgleichen. Zukünftig wird sich zeigen, ob diese Varianten der elektronischen Platzvermittlung sowohl für die Eltern als auch für die Verwaltung ausreichend praktikabel sind.

10.3 Lebensmittelüberwachung und Veterinärwesen

In diesem Jahr nicht belegt.

10.4 Rehabilitierungsgesetze

In diesem Jahr nicht belegt.

11 Landwirtschaft, Ernährung und Forsten

11.1 Online-Beantragung des Fischereischeins

Im Berichtszeitraum erreichte mich die Anfrage, wie ein Online-Antragsverfahren für Verlängerungen von Fischereischeinen ausgestaltet werden könnte. Wer in Sachsen die Fischerei ausüben möchte, muss über einen gültigen Fischereischein verfügen. Personen mit Hauptwohnsitz im Freistaat bedürfen eines Fischereischeins der Fischereibehörde, der bei dieser zu beantragen ist. Der Fischereischein ist gleichzeitig ein Lichtbildausweis. Ein aktuelles Lichtbild ist für das Dokument einzureichen (vgl. Abschnitt 4 SächsFischG). Das weitere Verfahren ist in der Durchführungsverordnung zum Fischereigesetz (Sächsische Fischereiverordnung) geregelt. Gemäß § 31 SächsFischVO enthält der Fischereischein unter anderem neben den Namen des Inhabers, dem Geburtsdatum, der Gültigkeitsdauer und dem Ort und Zeitpunkt der Ausstellung, das Passbild und eine Unterschrift. Ich wies darauf hin, dass bei der Online-Beantragung relativ hohe informationssicherheitstechnische Anforderungen erfüllt werden müssten und keine Prüfung der Echtheit der Lichtbilddaten und der Unterschrift der beantragenden Personen stattfindet. Insofern wäre nicht sichergestellt worden, dass die Person auf dem Ausweisdokument tatsächlich die Person ist, die sie vorgibt zu sein. Letztendlich verzichtete der Geschäftsbereich auf das Online-Verfahren. Die Umsetzung von E-Government-Lösungen scheitert nicht selten an Detailfragen.

12 Umwelt und Landesentwicklung

12.1 Wildkameras

Im Berichtszeitraum wurde ich zur Problematik des Einsatzes von Wildkameras und Wildvideokameras angefragt. Auch eine Landtagsdrucksache bezog sich hierauf (vgl. LT-Drs. 5/14422 zum Thema „Der Einsatz von so genannten Wildkameras und sonstigen Formen der elektronischen Überwachung im Freistaat Sachsen“. Ich nehme die Nachfrage zum Anlass, um in meinem Tätigkeitsbericht für den öffentlichen Bereich klarstellend zu der interessierenden Problematik zu informieren.

Der Einsatz von Wildvideokameras durch sächsische öffentliche Stellen unterliegt meiner datenschutzrechtlichen Kontrolle gemäß § 27 SächsDSG. Der Einsatz von Videokameras durch private Stellen im öffentlich zugänglichen Waldbereich in Sachsen, zum Beispiel durch Jäger, unterfällt hingegen dem Bundesdatenschutzgesetz und der Aufsichtsbehörde nach dem Bundesdatenschutzgesetz, die organisatorisch aber auch bei meiner Behörde angesiedelt ist (§ 6b BDSG). Vgl. dazu auch den entsprechenden Abschnitt 8.1.2 zur Videoüberwachung des 7. Tätigkeitsberichts zum Schutz des Persönlichkeitsrechts im nicht-öffentlichen Bereich.

Die Freiheit des öffentlichen Raums und sich persönlichkeitsrechtlich unbeobachtet darin bewegen zu können, auch in Waldbereichen, ist nach meiner Überzeugung ein Gut von sehr hohem gesellschaftlichen Wert, den es für die Allgemeinheit zu wahren gilt. Zwar gab es bisher noch keine Beschwerden zu Wildkameras bei meiner Behörde. Allerdings wäre - sollte der Einsatz der Kameras stark zunehmen - durchaus auch über eine gesetzliche Regelung, zum Beispiel im Waldgesetz nachzudenken, um bereichsspezifisch die Rechtslage eindeutig klarzustellen und eine Beobachtung öffentlicher Räume zu reglementieren.

Die Zulässigkeit des Einsatzes von - zumeist sensorgesteuerten - Wildvideokameras in öffentlich zugänglichen Bereichen unterliegt § 33 SächsDSG. Die Staatsregierung verweist in ihrer Antwort auf die vorbezeichnete Kleine Anfrage auf europarechtliche Notwendigkeiten, streng geschützte Wildarten, wie Wölfe und Wildkatzen, einem „Monitoring“ zu unterziehen. Gleichzeitig führt die Staatsregierung in ihren Überlegungen zur Zulässigkeit der Videoüberwachung nach dem Bundesdatenschutzgesetz aus, dass der Einsatz von Wildkameras in öffentlich zugänglichen Räumen nur insoweit denkbar sei, als dass die Kameraeinstellungen so gewählt werden, dass die erfassten Personen nicht identifizierbar sind. Diese Grundsätze müssen nach meiner Auffassung aber auch für die öffentlichen Bereiche gelten, die durch öffentliche Stellen videografiert werden, zumal die zulässigen Zwecke in § 33 SächsDSG mit Regelbeispielen genannt werden. Ein

„Monitoring“ des Wildbestandes zählt nicht dazu und wäre nach meiner Überzeugung auch nicht ein geeigneter gleichwertiger Zweck im Sinne von § 33 SächsDSG.

Im Ergebnis ist zu überlegen, ob der vorgegebene Zweck des Wildartenschutzes nicht auch durch einfache Kamerafallen erreicht werden kann. Für die Verwendung von Fotokameras würden die verfügbaren allgemeinen Datenerhebungsgrundlagen genügen. Die Zulässigkeit einer Videobeobachtung unterliegt hingegen weit höheren gesetzlichen Hürden. Durch datenschutzorganisatorische Maßnahmen, geeignete Kamerawinkel und -positionen können Datenschutzrisiken gering gehalten werden. Die technische Entwicklung und die Verwaltungspraxis der Wald- und Forstbehörden werde ich weiter verfolgen und den Einsatz von Wildkameras werde ich gelegentlich kontrollieren.

13 Wissenschaft und Kunst

13.1 Forschungsprojekt zum sogenannten Warnschussarrest

In Deutschland gibt es seit 2013 den „Warnschussarrest“, geregelt ist er in § 16a JGG: Jugendliche Straftäter, die zu einer Bewährungsstrafe verurteilt wurden, können zur Abschreckung für bis zu vier Wochen inhaftiert werden.

Mit dem Warnschussarrest werden verschiedene Ziele verfolgt: Er soll dem Jugendlichen seine Verantwortlichkeit für das begangene Unrecht und die Folgen weiterer Straftaten verdeutlichen, er soll es ermöglichen, einen Jugendlichen für eine begrenzte Zeit aus einem Lebensumfeld mit schädlichen Einflüssen herauszunehmen, durch die Behandlung im Arrestvollzug soll der Jugendliche auf die Bewährungszeit vorbereitet werden und schließlich soll auf den Jugendlichen im Arrestvollzug nachdrücklich erzieherisch eingewirkt werden, sofern dies - evtl. auch zum Zwecke der Erhöhung der Erfolgschancen einer Bewährung - geboten ist.

Da die Einführung dieses Warnschussarrests nicht unumstritten war, wurde ein niedersächsisches Forschungsinstitut in Kooperation mit einer hessischen Universität vom BMJV beauftragt, diese Sanktionsmöglichkeit bundesweit zu evaluieren. Das Projekt nahm im Januar 2014 seine Arbeit auf.

Ein zentrales Anliegen des Forschungsprojekts lag nach dem mir vorgelegten Datenschutzkonzept in der Klärung der Frage, wie die neue Norm von den Gerichten genutzt wird; hierzu sollte primär eine Aktenanalyse durchgeführt werden. Die Auswertung der Verfahrensakten sollte vor Ort durch Rechtsreferendare erfolgen. Geplant war darüber hinaus auch die schriftliche Fragebogenaktion mit unterschiedlichen Gruppen von Praktikern (Jugendrichter, Jugendstaatsanwälte, Bewährungshelfer, Vollzugsleiter, Jugendgerichtshelfer). Ein dritter Schwerpunkt lag in der Befragung ehemaliger Warnschussarrestanten.

Zu dem betreffenden Forschungsprojekt habe ich gegenüber dem SMJus Stellung genommen:

Bei früheren Justizforschungsvorhaben habe ich mich im Hinblick auf eine Aktenauswertung durch Außenstehende damit einverstanden erklärt, dass dann, wenn die Anonymisierung einen Aufwand erfordern würde, der, wie auch hier, wegen der ohnehin schon bestehenden übermäßigen Arbeitsbelastung gerade der Justiz, von der aktenführenden Stelle nicht geleistet werden kann, diese nicht durch die abgebende Stelle, sondern durch einen Mitarbeiter des Forschungsinstituts erfolgen darf unter der Voraus-

setzung, dass dieser Mitarbeiter nicht an der weiteren Durchführung des Forschungsvorhabens beteiligt ist und vor der Aufnahme seiner Tätigkeit die erforderliche Datengeheimnisverpflichtungserklärung abgibt.

Daran habe ich auch für diesen Fall festgehalten.

Bei der schriftlichen Fragebogenerhebung sind sämtliche Probanden ausdrücklich in einem Informationsanschreiben darauf hinzuweisen, dass die Teilnahme an der Befragung freiwillig ist. Eine Rechtsgrundlage für eine Pflicht zur Teilnahme an einer solchen Befragung sehe ich nicht. Die Auskünfte der Experten haben ohne jeden Bezug zu bestimmten Personen zu erfolgen.

Die Freiwilligkeit der Teilnahme und die schriftliche Aufklärung darüber gelten insbesondere auch für die schriftliche Befragung von Warnschussarrestanten sowie für die geplante persönliche Befragung von Inhaftierten. Die schriftliche Teilnahmeerklärung des Inhaftierten ist dabei nicht in die Gefangenenakte aufzunehmen, sondern separat in der Haftanstalt aufzubewahren.

Die im Rahmen des Forschungsprojekts zudem geplante Rückfalluntersuchung durch Einholung von Auskünften aus dem Bundeszentralregister habe ich auf § 42a BZRG gestützt.

Zur Auswertung der Einzeldatensätze der Strafverfolgungsstatistik bzw. deren Zulässigkeit wurde gegenüber meinem niedersächsischen Kollegen - als für das beauftragte niedersächsische Forschungsinstitut zuständige Aufsichtsbehörde - ausgeführt, dass die Einzeldatensätze im Hinblick auf Personen anonymisiert seien und damit keine Verbindung zu Daten der Aktenanalyse erfolge. Eine De-Anonymisierung sei von vornherein ausgeschlossen. Eine De-Anonymisierung sollte lediglich auf Ebene der Landgerichtsbezirke erfolgen (eine Identifizierbarkeit auf Personen-Ebene sei weiterhin ausgeschlossen), um - gemäß dem Forschungsauftrag - räumliche Unterschiede in der Sanktionspraxis zu untersuchen. Dies habe ich abschließend dem SMJus so mitgeteilt.

13.2 Datenerhebung für ein Forschungsprojekt per E-Mail - offener E-Mail-Verteiler

Eine sächsische Universität führte für ein Forschungsprojekt eine sogenannte Breitenerhebung durch. Problematisch in diesem Zusammenhang war, dass in der Kopfzeile sämtliche E-Mail-Adressen aller potentiellen Teilnehmer - insgesamt handelte es sich um *513* - offen sichtbar waren.

Dieser Versand einer E-Mail mit offenem Verteiler ist datenschutzrechtlich unzulässig.

Die E-Mail-Adresse ist ein personenbezogenes Datum im Sinne von § 3 Abs. 1 SächsDSG. Durch den E-Mail-Versand mittels eines offenen Verteilers wurden die E-Mail-Adressen der Betroffenen den anderen im Verteiler genannten Personen bekannt gegeben. Hierbei handelt es sich um eine Übermittlung i. S. d. § 3 Abs. 2 Satz 2 Nr. 5 Buchst. a SächsDSG. Die hierin liegende Datenverarbeitung (vgl. § 3 Abs. 2 Satz 1 SächsDSG) ist gemäß § 4 Abs. 1 SächsDSG nur zulässig, wenn hierfür entweder eine gesetzliche Befugnis besteht oder der Betroffene eingewilligt hat.

Bei der Übermittlung der E-Mail-Adressen an die weiteren Betroffenen handelt es sich um eine Datenübermittlung an nicht-öffentliche Stellen, sodass sich deren Zulässigkeit nach § 16 SächsDSG bestimmt. Nach dessen Absatz 1 ist die Übermittlung personenbezogener Daten an natürliche Personen zulässig, wenn sie zur Erfüllung der Aufgaben der übermittelnden Stelle erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 13 Abs. 1 bis 4 SächsDSG zulassen würden. Es ist nicht ersichtlich, dass die Aufgabenerfüllung nur möglich ist, wenn sämtliche E-Mail-Adressen den anderen Beteiligten übermittelt werden. Ein E-Mail-Versand mit Verwendung des BCC-Feldes wäre möglich gewesen. Auch ein berechtigtes Interesse der Empfänger an der Kenntnis der zu übermittelnden Daten dürfte nicht bestehen, sodass es an einer Übermittlungsbefugnis fehlt. Auch eine Einwilligung der Betroffenen in die Datenübermittlung lag nicht vor.

In ihrer Stellungnahme zum Vorgang teilte die betroffene Universität mit, dass sie datenschutzrechtlichen Belangen höchste Priorität einräume.

Bei Projekten, die den Umgang mit personenbezogenen Daten erfordern, erfolge eine Beratung und Begleitung durch den Datenschutzbeauftragten. Bei der E-Mail handele es sich um einen bedauerlichen Einzelfall.

Der Datenschutzbeauftragte der Universität hatte nach Kenntnis des Sachverhalts sofort entsprechende Maßnahmen eingeleitet und den Vorfall zum Anlass für eine nochmalige Belehrung bezüglich der Einhaltung datenschutzrechtlicher Bestimmungen genommen, sodass ich von einem weiteren Tätigwerden absehen konnte.

13.3 Online-Bewerbungen für einen Studienplatz an einer sächsischen Hochschule

Ein Petent wandte sich mit einer Eingabe gegen das Online-Bewerbungssystem einer sächsischen Hochschule an mich. Er war der Auffassung, dass zu viele Daten erhoben würden. Seiner Ansicht nach wäre es nicht erforderlich, Daten zum bisherigen Studienverlauf zu erheben. Es sei ausreichend, wenn der Bewerber versichern würde, den Prü-

fungsanspruch in dem betreffenden Fach nicht verloren zu haben. Überdies würden die Daten ungeprüft erhoben.

Nach der Rechtsgrundlage der Datenerhebung befragt, teilte mir die Hochschule mit, dass bezüglich des Umfangs der Datenerhebung die Verordnung des SMWK zur Verarbeitung personenbezogener Daten der Studienbewerber, Studenten und Prüfungskandidaten für statistische und Verwaltungszwecke der Hochschulen (Sächsische Studentendatenverordnung - SächsStudDatVO) zugrunde gelegt werde.

Als Rechtsverordnung bedurfte die Sächsische Studentendatenverordnung nach Art. 75 Abs. 1 Satz 1 SächsVerf einer gesetzlichen Ermächtigungsgrundlage. Gemäß Art. 75 Abs. 1 Satz 3 SächsVerf ist die Rechtsgrundlage in der Verordnung anzugeben.

Ausweislich der Sächsischen Studentendatenverordnung war danach § 106 Abs. 1 Satz 3 des Gesetzes über die Hochschulen im Freistaat Sachsen (Sächsisches Hochschulgesetz - SächsHG) vom 11. Juni 1999 (SächsGVBl. S. 294) Rechtsgrundlage. § 106 Abs. 1 Satz 3 SächsHG bestimmte, dass das SMWK ermächtigt wird, durch Rechtsverordnung zu bestimmen, welche personenbezogenen Daten von Studienbewerbern, Studenten, Prüfungskandidaten, Absolventen und externen Nutzern von Hochschuleinrichtungen, die insbesondere für die Immatrikulation, die Rückmeldung, die Teilnahme an Lehrveranstaltungen, die Prüfungen, die Nutzung von Hochschuleinrichtungen, die Hochschulplanung und die Kontaktpflege mit ehemaligen Hochschulmitgliedern erforderlich sind, verarbeitet werden.

Mit Inkrafttreten der Neufassung des Gesetzes über die Hochschulen im Freistaat Sachsen (Sächsisches Hochschulgesetz - SächsHSG) am 1. Januar 2009 ist das Sächsische Hochschulgesetz in der Fassung vom 11. Juni 1999 und somit auch der § 106 Abs. 1 Satz 3 SächsHG a. F. außer Kraft getreten (vgl. § 115 SächsHSG vom 10. Dezember 2008, SächsGVBl. S. 900). Seither ist die Frage des zulässigen Datenverarbeitungshandelns in § 14 SächsHSG bzw. jetzt § 14 SächsHSFG geregelt.

Die vorgenannte Norm gestattet die Verarbeitung personenbezogener Daten durch die sächsischen Hochschulen nur, soweit dies für die in den § 14 Abs. 1 Nr. 1 bis 10 SächsHSFG beschriebenen Zwecke erforderlich ist. Nach § 14 Abs. 1 Nr. 1 SächsHSFG dürfen die Hochschulen die für die Zulassung und Immatrikulation erforderlichen personenbezogenen Daten verarbeiten. Gemäß § 14 Abs. 3 Satz 1 SächsHSFG bestimmt das SMWK durch Rechtsverordnung, welche Daten verarbeitet werden *dürfen*.

Der Inhalt einer solchen Verordnung kann indes nicht weiter gehen als die grundlegende gesetzliche Norm, sodass eine vom SMWK zu erlassende Rechtsverordnung keine über

§ 14 Abs. 1 SächsHSFG hinausgehende Datenverarbeitungsbefugnis zu begründen vermag.

Daher ist eine Erhebung von Daten, die zur Aufgabenerfüllung, respektive zur Zweckerfüllung nach § 14 Abs. 1 Nr. 1 bis 10 SächsHSFG nicht erforderlich ist, unzulässig. Sie kann nicht auf die Regelungen der Studentendatenverordnung gestützt werden. Denn es ist davon auszugehen, dass die Studentendatenverordnung das rechtliche Schicksal ihrer außer Kraft getretenen Ermächtigungsgrundlage geteilt hat.

Jedenfalls bestehen aber Bedenken dagegen, dass die Studentendatenverordnung mit der derzeitigen Rechtslage übereinstimmt. Denn während nach § 106 Abs. 1 Satz 3 SächsHG dem SMWK die einschränkungslose Bestimmung von Daten, deren Verarbeitung erfolgen sollte, übertrug, bestimmt § 14 Abs. 3 Satz 1 SächsHSFG, dass die Bestimmungen der zu verarbeitenden Daten in den Grenzen des § 14 Abs. 1 SächsHSFG erfolgen muss. Die Sächsische Studentendatenverordnung ist daher zumindest insoweit rechtswidrig, als diese die Verarbeitung des Geburtsnamens und des Geburtsortes vorsieht. Denn hierzu wurde mir von Seiten der Hochschule mitgeteilt, dass diese Daten zur Bearbeitung eines Immatrikulationsantrags nicht erforderlich seien.

Auf meinen diesbezüglichen Hinweis wurde mir mitgeteilt, dass die Universität auf die Erhebung der als freiwillig gekennzeichneten Daten, derer sie zur Bearbeitung des Antrags auf einen Studienplatz ohnehin nicht bedarf, verzichten wird. Darüber hinaus werden meine Hinweise in das Gespräch mit den Vertretern des SMWK zur Erarbeitung einer Hochschulpersonendatenverordnung eingebracht.

Es bleibt zu hoffen, dass es dem SMWK gelingt, diese Verordnung zeitnah zu erarbeiten und zu verabschieden, um diese unsichere Rechtslage sowohl im Interesse der Betroffenen als auch im Interesse der Hochschulen zu beseitigen.

13.4 Generisches Datenschutzkonzept für medizinische Anwendungen

Die Technologie- und Methodenplattform für vernetzte medizinische Forschung e. V. (TMF) hat den generischen Lösungsansatz für Datenschutzkonzepte aktualisiert und umfassend weiterentwickelt. Dieser „Leitfaden zum Datenschutz in medizinischen Forschungsprojekten - Generische Lösungen der TMF 2.0“ enthält Empfehlungen und Musterlösungen für eine datenschutzgerechte Verwendung von Patientendaten in der medizinischen Forschung und im Forschungsverbund.

Der neue Leitfaden zeigt anhand eines modularen und skalierbaren Ansatzes (Klinisches Modul, Studienmodul, Forschungsmodul und Biobankenmodul) verschiedene Wege zum datenschutzgerechten Aufbau von Forschungsverbünden auf. Konkrete Lösungen zur datenschutzgerechten Ausgestaltung von Patienteninformation und -aufklärung, zur Anwendung von Anonymisierungs- oder Pseudonymisierungsverfahren, zu Erörterungen der Rechtsgrundlagen und Datentreuhänderschaft sowie zu den technischen und organisatorischen Maßnahmen für die informationstechnische Infrastruktur der Forschungsverbünde können abgeleitet werden.

Der aktualisierte Leitfaden wurde mit den zuständigen Arbeitskreisen Wissenschaft sowie Technik der DSK intensiv diskutiert und abgestimmt. Dem folgend hat die DSK im März 2014 medizinischen Forschungseinrichtungen und Forschungsverbänden empfohlen, diesen Leitfaden mit den darin enthaltenen generischen Konzepten als Basis für die konkrete Ausgestaltung ihrer Datenschutzkonzepte zu nutzen.

Der Leitfaden bietet damit einen Rahmen, an dem sich Forschungseinrichtungen bei der Einarbeitung in die Datenschutzthematik und bei der konkreten Erstellung von Datenschutzkonzepten orientieren können. Diese Vorgehensweise des Datenschutzhandelns im medizinischen Bereich kann, unter Berücksichtigung der jeweils gültigen gesetzlichen Grundlagen, auch auf andere Lebensbereiche übertragen werden.

Dieses Konzept wurde als Band 11: „Leitfaden zum Datenschutz in medizinischen Forschungsprojekten - Generische Lösungen der TMF 2.0“ in der Schriftenreihe der TMF (http://www.tmf-ev.de/schriftenreihe) veröffentlicht.

14 Technischer und organisatorischer Datenschutz

14.1 Neuer Dienststellenschlüssel für die Verschlüsselung

Der Sächsische Datenschutzbeauftragte bietet seit vielen Jahren die Möglichkeit verschlüsselte Nachrichten mit Ende-zu-Ende-Sicherheit an die Dienststelle zu senden und selbstverständlich auch auf diesem Weg zu antworten. Es freut mich, dass diese Kommunikationsform in den letzten Jahren ein wenig aus dem Schattendasein hervortritt und breiter genutzt wird. Jedenfalls lässt sich dies für unsere Dienststelle konstatieren; der Anteil an verschlüsselten E-Mails ist deutlich angestiegen.

Den technisch und algorithmisch in die Jahre gekommenen Schlüssel des Sächsischen Datenschutzbeauftragten habe ich kürzlich erneuert, er lässt sich auf den üblichen Keyservern oder auf meiner Website (https://www.datenschutz.sachsen.de unter Allgemein/ Die Behörde/Kontakt oder Impressum) finden.

Die durchgängige Ende-zu-Ende-Verschlüsselung der elektronischen Kommunikation muss endlich zur Normalität im 21. Jahrhundert werden. Ich empfehle daher allen Bürgern des Freistaates, eine solche Verschlüsselung auch privat einzurichten. Dank der Snowden-Informationen ist die Aufmerksamkeit hinsichtlich einer vertraulichen elektronischen Kommunikation spürbar angestiegen, was auch an dem Angebot entsprechender Programme und Dienstleistungen ablesbar wird. Der Installationsaufwand hält sich mittlerweile in Grenzen und das Internet bietet zahlreiche brauchbare Anleitungen, auch für Nicht-Techniker...

14.2 Entwicklung eines Standard-Datenschutzmodells (SDM)

Die 85. DSK hat im März 2013 eine Arbeitsgruppe mit der Entwicklung eines Standard-Datenschutzmodells (SDM) beauftragt. Diese Arbeitsgruppe ist mit Vertretern verschiedener Bundesländer, darunter auch Sachsen besetzt. Auf der 88. DSK im Oktober 2014 wurde ein erster vollständiger Entwurf des Modells zur Abstimmung vorgelegt. Der Modellentwurf fand in der DSK breite Zustimmung. Die Arbeitsgruppe wurde damit beauftragt, auf der Grundlage des Modells einen Katalog mit Referenz-Datenschutzmaßnahmen zu entwickeln.

Ein solcher Katalog 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 werden 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 weiterhin methodisch am etablierten IT-Grundschutz des BSI.

Das Standard-Datenschutzmodell basiert auf sieben Gewährleistungszielen, welche unmittelbar oder mittelbar in allen Landesdatenschutzgesetzen und dem Bundesdatenschutzgesetz gesetzlich verankert sind. Dies sind zunächst *Datensparsamkeit, Verfügbarkeit, Integrität, Vertraulichkeit und Transparenz*, die im Sächsischen Datenschutzgesetz noch spezifisch um Authentizität und Revisionsfähigkeit erweitert werden. Hinzu kommt die Nichtverkettbarkeit, als Umsetzung des Grundsatzes der Zweckbindung und die Intervenierbarkeit, als Ausdruck der unmittelbaren Betroffenenrechte.

Anders als die Methoden der Informationssicherheit, die ausschließlich der Gewährleistung der Sicherheit der Organisation dienen, zielt das SDM auch auf die wirkungsvolle Umsetzung der Rechte der Betroffenen ab. Ein wesentlicher Aspekt ist, dass die dreistufigen Schutzbedarfsfeststellungen, wie man sie vom Grundschutz kennt, explizit aus der Sicht der Betroffenen formuliert und dass die zu betrachtenden Risiken anhand der Gewährleistungsziele analysiert werden. Neben den Risiken der konkreten personenbezogenen Datenverarbeitung werden auch die Risiken der IT-Systeme und -Prozesse betrachtet.

Aus sächsischer Sicht kann das SDM auch bei der Umsetzung der gesetzlichen Vorgaben des 2014 in Kraft getretenen Sächsischen E-Government-Gesetzes eine wichtige Rolle spielen. In § 5 SächsEGovG wird gefordert, dass staatliche und kommunale Behörden Datenschutz- und Informationssicherheitskonzepte erstellen müssen. Für die Informationssicherheit bietet der Grundschutz das methodische Gerüst, für den Datenschutz kann das SDM diese Funktion erfüllen. Für staatliche Behörden gilt dies insbesondere, da § 9 Abs. 2 SächsEGovG die Schutzziele des § 9 Abs. 2 SächsDSG vorgibt, also einen Schutzzielkatalog, der über die vom BSI-Grundschutz definierten Schutzziele hinausgeht. Auch hier kann das SDM die methodische Lücke zwischen existierenden Standards und gesetzlichen Forderungen mit dem erweiterten Maßnahmenkatalog ausfüllen.

Bis zum Herbst 2015 soll dieser Maßnahmenkatalog getrennt für Daten, Systeme und Prozesse mit ca. 100 Referenzmaßnahmen für alle sieben Gewährleistungsziele befüllt sein und der DSK zur Abstimmung vorgelegt werden.

14.3 Cookies und Tracking öffentlicher Stellen (Update)

Immer wieder gibt es Nachfragen von Behörden und interessierten Bürgern, inwieweit Behörden Besucherstatistiken über die Nutzung ihrer Webseiten führen dürfen. Die maßgebliche Vorschrift ist § 15 Abs. 3 TMG. Es gibt im Wesentlichen drei Anforderungen:

- Nutzungsprofile dürfen unter Pseudonym angelegt werden und dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden, d. h. dass es verboten ist IP-Adressen in voller Länge zu verarbeiten, bspw. für Geo-Lokation,
- ein Widerspruchsrecht gegen die Erstellung des Nutzungsprofils ist einzurichten und
- auf diese Widerspruchsmöglichkeit ist deutlich hinzuweisen.

Ein Setzen von Cookies mit einer pseudonymen Ziffer und einer Lebensdauer über die laufende Session hinaus muss damit deutlich im Impressum dargestellt werden und eine einfache Möglichkeit dies zu unterbinden, muss angeboten werden.

Weiterhin ist das Sächsische Datenschutzgesetz zu beachten: Wenn sich die Behörde für derartige Statistiken eines Dienstleisters bedient, ist dieser über einen Vertrag zur Datenverarbeitung im Auftrag nach § 7 SächsDSG zu binden, da in aller Regel eine Übermittlung der Nutzungsdaten an den Dienstleister technisch erforderlich ist.

Damit ist die Nutzung von Tracking-Diensten, welche keinen Vertrag nach Sächsischem Datenschutzgesetz anbieten, wie z. B. Google Analytics, für öffentliche Stellen in Sachsen nicht möglich.

Öffentlichen Stellen ist ein Besuchertracking somit nur möglich, wenn Produkte eingesetzt werden, welche die Vorgaben des Telemediengesetzes und des Sächsischen Datenschutzgesetzes in Bezug auf die Auftragsdatenverarbeitung erfüllen. Dies wird von einigen deutschen Anbietern erfüllt, auch existiert eine diesbezüglich einsetzbare open-source-Lösung (ohne Auftragsdatenverarbeitung als selbstbetriebene Software).

Es sei angemerkt, dass es noch differierende Auffassungen zwischen Bundesregierung und den Datenschutzbehörden zur Umsetzung der Richtlinie 2009/136/EG („Cookie-Richtlinie“) in nationales Recht gibt. Die Richtlinie verlangt einen „consent“, also eine aktive Zustimmung, und die Bundesregierung hält dies mit dem Telemediengesetz für ausreichend klar geregelt. Inwieweit diese Auffassung haltbar ist, wird sich zeigen.

14.4 Einsatz von privaten mobilen Endgeräten und ‚Apps' in öffentlichen Stellen

Immer mehr kommunale und staatliche Behörden setzen auf Apps bei der Bewältigung ihrer Aufgaben. Die omnipräsenten Smartphones sollen Bürgern den Zugriff auf Dienstleistungen der Behörden ermöglichen oder im internen Einsatz die Arbeit der Bediensteten unterwegs erleichtern.

Einige der von Behörden eingesetzten oder angebotenen Apps habe ich unter die Lupe genommen. Hierbei ist besonders auf die Sicherung der mobilen Endgeräte sowie die Sicherung der Authentifizierung und Datenübertragung zu achten. Die spezifischen Risiken der jeweiligen Nutzung sind gesondert zu betrachten (z. B. Verlustrisiko mit Missbrauchsgefahr im Außeneinsatz).

Die VwV Dienstordnung der Sächsischen Staatsregierung regelt für Behörden des Freistaates Sachsen in Nr. 32 e), dass für die Erledigung dienstlicher Aufgaben nur dienstlich bereitgestellte Geräte und Datenträger sowie freigegebene Programme benutzt werden dürfen. Daran muss gelegentlich mit aller Deutlichkeit erinnert werden, wenn in Projekten Ansätze in Richtung „Bring your own device (BYOD)", also mit dem Ziel des Einsatzes privater Endgeräte, verfolgt werden. Zur Nutzung von privaten Smartphones der Bediensteten kann ich ausdrücklich keine Empfehlung abgeben. Die Bereitstellung geeigneter Endgeräte ist Aufgabe der Behörden, ebenso wie die wirksame Durchsetzung angemessener und geeigneter Sicherheitsmaßnahmen.

Treten Behörden als Anbieter von Apps auf, sind zahlreiche rechtliche Bestimmungen zu beachten. In aller Regel sind mehrere Beteiligte bei einem solchen Verfahren anzutreffen, sei es der Entwickler oder Betreiber der Software (falls Auftragsdatenverarbeitung im Spiel ist) oder der Betreiber des App-Stores. Zu empfehlen ist die Beachtung der „Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter", welche von den Datenschutzbehörden gemeinsam erarbeitet wurde (https:// www. datenschutz.sachsen.de unter Öffentlicher Bereich/Informationen/Arbeitshilfen, vgl. auch 7. Tätigkeitsbericht für den nicht-öffentlichen Bereich unter Punkt 14.6.1). Diese richtet sich zwar primär an privatwirtschaftliche Anbieter, welche dem Bundesdatenschutzgesetz unterliegen, lässt sich mit Anpassungen aber auch für den öffentlichen Bereich anwenden.

14.5 Einsatz von Windows XP

Das Betriebssystem Windows XP von Microsoft wird seit April 2014 seitens des Herstellers nicht mehr unterstützt. Dies bedeutet, dass seitdem keine Behebung von sicherheitskritischen Fehlern mehr erfolgt und diese Systeme massiv gefährdet sind. Die Ankündigung des Support-Endes seitens Microsoft erfolgte frühzeitig und war somit seit einigen Jahren vorher bekannt.

Dennoch haben mich auch nach Supportende noch Fragen von Verwaltungen erreicht, was denn zu tun sei. Für eine vollständige Migration sei kein Geld vorhanden oder einzelne Fachverfahren würden nur unter Windows XP laufen.

Das BSI empfiehlt dringend eine Migration bestehender Windows XP-Umgebungen auf moderne Betriebssysteme, dieser Empfehlung habe ich mich für den Aufsichtsbereich des Sächsischen Datenschutzbeauftragten angeschlossen. Eine Absicherung von Windows XP-Systemen mit herkömmlichen Schutzmechanismen der Informationssicherheit wie Firewalls und Anti-Viren-Software ist nicht möglich, da spezifische Angriffsvektoren von diesen Systemen nicht abgedeckt werden können. Vielmehr sorgt der Einsatz von Windows XP für eine verstärkte Bedrohungslage für alle Systeme im Informationsverbund.

Eine Migration ist also, wie man heutzutage gern sagt, alternativlos.

Wer sich nicht von Windows XP trennen kann und dennoch für das gesetzlich vorgeschriebene angemessene Sicherheitsniveau sorgen will bzw. muss, treibt die Kosten und die Komplexität des Sicherheitsprozesses gewaltig nach oben. Das BSI empfiehlt für diesen Fall u. a.:

- Verlagerung von allen Programmen, Diensten, Zugängen und Benutzerkonten, die nicht unbedingt auf diesem System laufen müssen, auf andere Systeme mit modernen Betriebssystemen, um die Angriffsfläche zu verkleinern,
- Installation von Schutzmechanismen, wie Application Whitelisting, welche typischerweise auch noch für veraltete Betriebssysteme unterstützt werden, oder die Nutzung der Richtlinien für Softwareeinschränkungen,
- Isolierung des Systems so weit wie möglich, idealerweise durch vollständige Trennung vom Rest des Netzes,
- Ist eine Trennung nicht möglich, so sollte das System in ein spezielles Netzsegment platziert, durch möglichst restriktive Firewalls geschützt und mittels Intrusion-Detection-Systemen gesondert überwacht werden.

Einen derartigen Aufwand zu betreiben, stellt eine Verwaltung vor Herausforderungen, die im Rahmen eines geregelten IT-Betriebs nur schwer und mit unverhältnismäßig hohem Aufwand zu bewältigen sind. Vor allem dann nicht, wenn der Einsatz von Windows XP mit dem Kostenargument einhergeht. Um es klar zu sagen: Ein Einsatz von Windows XP in einem Verwaltungsnetz, in dem personenbezogene Daten verarbeitet werden, ist nicht tolerabel.

14.6 Nutzung von Clouddienstleistern durch öffentliche Stellen

Im Berichtszeitraum gab es vermehrt Anfragen von Behörden, ob es zulässig sei, Daten in eine wie auch immer gestaltete Cloud einzuspeisen. Meist ging es um einzelne Fachverfahren, wie die Verwaltung von Bibliotheken oder die Bereitstellung eines Zentralkalenders über verteilte Umgebungen. Die Ablage von allgemeinen Behördendaten in der Cloud war bislang eher kein Thema, meist ging es um ein konkretes Produkt, welches von einem Cloud-Dienstleister angeboten wurde.

Das Thema Cloud findet seit vielen Jahren Beachtung durch die Datenschützer. Neben den allgemein gültigen, technischen Anforderungen an derartige Angebote, zu denen die „Orientierungshilfe Cloud Computing der Arbeitskreise Technik und Medien der DSK sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises (Version 2.0; Stand 9. Oktober 2014)“ (www.datenschutz.sachsen.de unter Öffentlicher Bereich/Informationen/Arbeitshilfen) umfassend Auskunft gibt, sind für sächsische Behörden die spezifischen Regelungen des Sächsischen Datenschutzgesetzes zu beachten, insbesondere für das Cloud-Computing.

§ 17 Abs. 1 SächsDSG regelt die Übermittlung in Drittländer außerhalb der Europäischen Union, welche nur unter der Voraussetzung der Erforderlichkeit möglich ist. Diese Erforderlichkeit bezieht sich auf die Erforderlichkeit der Datenübermittlung und nicht etwa auf faktische Zwänge, wie preiswertester Anbieter o. Ä. Daran wird es regelmäßig fehlen. Diese Übermittlung in Drittländer umfasst auch mögliche Supportfälle. Es ist also im Einzelfall zu prüfen, ob ein Anbieter, trotz Niederlassung in Deutschland oder der EU, nicht doch an einer Stelle des Prozesses Daten außerhalb der Europäischen Union verarbeitet. Vielfach erfährt man dies nur durch ein gründliches Studium der Verträge in Verbindung mit hartnäckigen Nachfragen.

Daran ändert sich auch nichts, wenn die Cloud durch einen Auftragnehmer betrieben wird. Auch in diesem Fall müssen gemäß § 7 Abs. 4 SächsDSG die Voraussetzungen des § 17 Abs. 1 SächsDSG vorliegen.

Es kommt daher realistischer Weise nur die Nutzung einer europäischen Cloud in Form einer Auftragsdatenverarbeitung in Betracht, bei der jegliche außereuropäischen Zugriffsrechte ausgeschlossen sind. Jeder Anbieter, der für sächsische Behörden tätig werden möchte, ist nach § 7 SächsDSG mit einem Auftragsdatenverarbeitungsvertrag zu binden, inklusive der Verpflichtung auf das Datengeheimnis nach Sächsischem Datenschutzgesetz. Schon an diesem formalen Punkt scheitert die Nutzung zahlreicher Dienste, welche die Auftragsdatenverarbeitung zwar anbieten, allerdings nur bezogen auf das Bundesdatenschutzgesetz, welches für Bundesbehörden und private Nutzer der Dienste Anwendung findet. Diese rechtlichen Restriktionen haben auch den SID bewogen, an einer eigenen Lösung zu arbeiten. Ich bin gern bereit an dieser beratend mitzuwirken.

14.7 Nutzung von Skype für Videokonferenzen im Jugendamt

Ein Landkreis hat sich an mich mit der Frage gewandt, ob es möglich sei, das Produkt Skype der Firma Microsoft für Videokonferenzen im Jugendamt für interne Zwecke als auch für die Kommunikation mit externen Trägern einzusetzen. Auf die Kommunikation von Sozialdaten sollte dabei zum Glück verzichtet werden, es ginge nur um übliche Verwaltungsthemen.

Ich halte das Produkt für einen Einsatz in öffentlichen Stellen im Freistaat Sachsen insgesamt für ungeeignet. Es gibt viele Fragen rund um die Abhörsicherheit von Skype, welche hauptsächlich von Spekulationen befeuert sind, da die Firma „security by obscurity“ betreibt und keine Stellungnahme zu aufgeworfenen Sicherheitsfragen abgegeben hat. Fest steht, dass die Firma ein proprietäres Netzwerkprotokoll benutzt und für Endkunden damit eine „black box“ darstellt.

Für sächsische öffentliche Stellen kommt Skype als Dienstleister für die Verarbeitung personenbezogener Daten schon aufgrund von § 7 Abs. 2 SächsDSG nicht in Frage, da eine Kontrolle über Art und Umfang der Datenverarbeitung aufgrund der vorgenannten Gründe faktisch nicht durchsetzbar wäre. Auch im konkret geschilderten Einsatzszenario, bei dem auf die Kommunikation von Sozialdaten verzichtet werden sollte, handelt es sich um eine Verarbeitung personenbezogener Daten, da die Videokommunikation der Beschäftigten untereinander bereits die personenbezogene Verarbeitung von Beschäftigtendaten darstellt.

Die Kommunikation einer Behörde stellt ein essentiell schutzwürdiges Objekt dar, dessen Kanäle stets unter angemessener technischer und vertraglicher Kontrolle bleiben sollten. Kosten- oder Praktikabilitätsgründe haben sich dem unterzuordnen.

14.8 Online-Petitionssysteme öffentlicher Stellen

Immer mehr Kommunen und zum Teil auch staatliche Stellen wollen den Bürgern eine Mitbestimmung durch die Abgabe von Petitionen oder generell Meinungen zu öffentlichen Themen ermöglichen. Der Zugang über eine Online-Plattform soll dabei helfen Berührungsängste abzubauen und auch die jüngere Generation für gesellschaftliche und politische Themen zu gewinnen.

Folgende Punkte sind dabei zu beachten oder sollten bei der Planung berücksichtigt werden:

Umgang mit Nutzerdaten:

Im Telemediengesetz findet sich keine Rechtsgrundlage für eine Speicherung von Nutzungsdaten außerhalb der Abrechnungszwecke. Dies gilt auch für IP-Adressen. Eine Speicherung der IP-Adresse bei der Nutzung der kommunalen oder staatlichen Angebote im Netz ist daher nicht zulässig. Im Impressum oder den Nutzungsbedingungen ist darauf hinzuweisen. Auch die Möglichkeit, dass Beleidigungen oder andere Straftaten, durch die Möglichkeit der Abgabe eigener Beiträge im Petitionssystem dadurch nicht aufgeklärt werden können, stellt kein Argument für eine Speicherung dar. Vielmehr ist der Anbieter in der Pflicht, derartige Verstöße zu kontrollieren (siehe Moderation).

Pseudonyme Nutzung ermöglichen:

In § 13 Abs. 6 TMG ist klar geregelt: „Der Diensteanbieter hat die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.“ Dies gilt selbstverständlich auch für kommunale oder staatliche Angebote. Mitunter wurde die Auffassung vertreten, dass es für die Meinungsäußerung in politischen oder gesellschaftlichen Themen doch wichtig sei, dass der Bürger mit Klarnamen erkenntlich sei. Aber die Gesetzeslage ist eindeutig, der Nutzer hat ein Recht auf pseudonyme Nutzung und auf dieses Recht ist er explizit hinzuweisen.

Löschen ermöglichen:

Dem Nutzer steht nach § 13 Abs. 4 TMG ein vollumfängliches Recht auf eine Beendigung des Nutzungsverhältnisses inklusive unmittelbarer Löschung oder Sperrung zu. Mitunter ist dies in den Petitionssystemen nicht vorgesehen, mit dem Argument, dass dann die Nachvollziehbarkeit von Diskussionen leide. Dem mag zuzustimmen sein, der rechtliche Anspruch steht aber eindeutig über diesem.

Zugriff von Suchmaschinen:

In Zeiten des allgegenwärtigen Zugriffs der Suchmaschinen auf Inhalte im Netz stellt sich die Frage, ob dies in jedem Fall gewünscht ist. Sollen die Äußerungen der Bürger zu lokalen oder regionalen Themen systematisch global erschlossen werden oder besser nicht? Über den „Robots Exclusion Standard“ kann der Inhaber der Website den Zugriff der Suchroboter steuern und so verhindern, dass Äußerungen der Bürger für die Suchmaschinen indexiert werden.

Moderation und Umgang mit Störungen:

Bei der Möglichkeit, dass Externe eigene Beiträge auf einer Website veröffentlichen können, kann es auch zu Störungen in Form von unangemessener Nutzung kommen. Im Vorfeld sollten daher Regeln nach außen (neudeutsch: „Netiquette“) definiert und kommuniziert werden und Abläufe für den internen Umgang mit Störungen festgelegt werden.

15 Vortrags- und Schulungstätigkeit

Wie jedes Jahr führten meine Mitarbeiter umfangreiche Schulungen unter anderem für behördliche Datenschutzbeauftragte insbesondere bei der Akademie für öffentliche Verwaltung des Freistaates Sachsen, dem Sächsischen Kommunalen Studieninstitut, der Sächsischen Verwaltungs- und Wirtschaftsakademie sowie dem Sächsischen Bildungsinstitut durch (siehe auch 7.1).

Zu einer guten Tradition ist der gemeinsam mit der KISA und der KDN GmbH veranstaltete Informationstag „Datenschutz und IT-Sicherheit in sächsischen Kommunen“ sowie die mit dem OLG Dresden alljährlich durchgeführte ganztägige Schulungsveranstaltung für Rechtsreferendare geworden.

16 Ordnungswidrigkeitenverfahren

16.1 Übersicht

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).*

Die Auflistung zeigt, dass dem Sächsischen Datenschutzbeauftragten in weiteren zusätzlichen Bereichen, neben den bisherigen (§ 38 SächsDSG und § 85 SGB X), die Funktion der Verwaltungsbehörde zur Verfolgung und Ahndung von Ordnungswidrigkeiten übertragen worden ist. Das bedeutet ein höheres Maß an Aufgaben und Verantwortung.

Den größten Teil der bearbeiteten Ordnungswidrigkeitenverfahren nehmen bisher noch die Verfahren zur Ahndung von Verstößen nach § 38 Abs. 1 Nr. 1 SächsDSG ein, in denen unbefugt nicht offenkundige personenbezogene Daten

- verarbeitet,
- zum Abruf bereitgehalten oder
- für sich selbst oder einen anderen abgerufen oder auf andere Weise verschafft worden sind.

Aber auch die Zahl der Verfahren, in denen unbefugt Sozialdaten, die nicht allgemein zugänglich sind, erhoben oder verarbeitet wurden (§ 85 Abs. 2 Nr. 1 SGB X), nimmt zu.

Im Berichtszeitraum sind durch meine Behörde 62 Ordnungswidrigkeitenverfahren im öffentlichen Bereich abgeschlossen worden. Die Summe der rechtskräftigen Buß- und Verwarngelder belief sich auf 11.160 Euro.

Im Vergleich zum vorangegangenen Berichtszeitraum sind mehr Verfahren zur Vorlage an die Gerichte gelangt, was sich auf die gesamte Verfahrensdauer auswirkt, und weshalb trotz steigendem Bearbeitungsaufwand und -volumen im Bereich der Ordnungswidrigkeiten insgesamt weniger Verfahren zum Abschluss kommen konnten. Meine Einflussnahmemöglichkeiten im Hauptverfahren als sachkundiger Beteiligter habe ich

weiter verstärkt und ausgebaut. 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 zur 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, Pkt. 11.2), effizienter und vorteilhafter.

In den Fällen, in denen ein Bußgeldbescheid wegen des Verstoßes gegen § 38 Abs. 1 Nr. 1 SächsDSG erlassen worden ist, handelt es sich zum überwiegenden Teil um von den Betroffenen nicht dienstlich veranlasste Abrufe personenbezogener Daten in ihnen ausschließlich für dienstliche Zwecke zur Verfügung stehenden, nicht allgemein zugänglichen, elektronischen Informationssystemen bzw. um die unerlaubte Verarbeitung personenbezogener Daten in diesem Zusammenhang. Dies geht in der Regel mit einer Verletzung des Datengeheimnisses gemäß § 6 SächsDSG einher.

Nach wie vor handelt es sich beim Hauptanteil dieser Ordnungswidrigkeitenverfahren um Verfahren gegen Bedienstete der sächsischen Polizei. Nachdem die Belehrung sächsischer Polizeibeamter über den Datenschutz im Zusammenhang mit der Nutzung polizeilicher Datenbanken auf meine Anregung hin durch die einzelnen Polizeidienststellen intensiviert wurde (vgl. 16/16.1), besteht oftmals immer noch die von mir bereits geschilderte Unsicherheit hinsichtlich der zulässigen Nutzung polizeilicher Datenbanken. Dies betrifft nunmehr häufig den Umstand, dass eben allein aus der technischen Möglichkeit des Zugriffs auf personenbezogene Daten oder einem Zugriffsstatus bestimmter Daten oder Dokumente gerade keine Aussage über die Befugnis des einzelnen Beamten zur Verarbeitung dieser Daten abgeleitet werden kann. 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 der einzelne Beamte nur berechtigt, die zur Erfüllung seiner konkreten dienstlichen Aufgabe erforderlichen Daten zu verarbeiten. So ist es lebensfremd und abwegig anzunehmen, dass Abfragen in polizeilichen Datenbanken etwa darüber, ob Bekannte, Freunde oder Kollegen in polizeilichen Verfahren erfasst sind, durch Polizeibeamte ohne dienstlichen Anlass zulässig sein könnten, nur weil derartige Recherchen technisch möglich sind.

Ich rechne jedoch damit, dass die von mir durchgeführten Ordnungswidrigkeitenverfahren auch diesbezüglich eine Präventionswirkung entfalten. Unabhängig davon halte ich die Verfolgung von unbefugten Zugriffen auf polizeiliche Daten für unabdingbar,

um die Polizeibediensteten auch zukünftig zu ihrer besonderen Pflichtenwahrung und Vorbildwirkung zu ermahnen. Auch durch bloße Unkorrektheit im Umgang mit den polizeilichen 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.

17 Materialien

17.1 Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

17.1.1 Entschließung zwischen der 85. und 86. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5. September 2013: Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass noch immer nicht alles getan wurde, um das Ausmaß der nachrichtendienstlichen Ermittlungen mithilfe von Programmen wie PRISM, TEMPORA und XKEYSCORE für die Bundesrepublik Deutschland aufzuklären.

Schon die bisherigen Erkenntnisse lassen den Schluss zu, dass die Aktivitäten u. a. des US-amerikanischen und des britischen Geheimdienstes auf eine globale und tendenziell unbegrenzte Überwachung der Internetkommunikation hinauslaufen, zumal große Internet- und Telekommunikationsunternehmen in die Geheimdienstaktionen eingebunden sind.

Da zahlreiche Anbieter von Kommunikationsdienstleistungen, deren Server in den USA stehen, personenbezogene Daten der Menschen in der Bundesrepublik Deutschland verarbeiten, betreffen die Berichte, dass US-amerikanische Geheimdienste auf dem Territorium der USA personenbezogene Daten umfassend und anlasslos überwachen, auch ihre Daten. Unklar ist daneben noch immer, ob bundesdeutsche Stellen anderen Staaten rechtswidrig personenbezogene Daten für deren Zwecke zur Verfügung gestellt und ob bundesdeutsche Stellen rechtswidrig erlangte Daten für eigene Zwecke genutzt haben.

Die staatliche Pflicht zum Schutz der Grundrechte erfordert es, sich nicht mit der gegenwärtigen Situation abzufinden. Die Regierungen und Parlamente des Bundes und der Länder sind dazu aufgerufen, das ihnen im Rahmen ihrer Zuständigkeiten Mögliche zu tun, um die Einhaltung des deutschen und des europäischen Rechts zu gewährleisten. Das Bundesverfassungsgericht hat festgestellt, dass es „zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland gehört, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss“, „dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf“. Es müssen daher alle Maßnahmen getroffen werden, die den Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen und ihr Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme für die Zukunft sicherstellen.

Für die Wahrung der Grundrechte der Menschen in der Bundesrepublik Deutschland kommt es nun darauf an, die notwendigen Konsequenzen zu ziehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deshalb:

- Nationales, europäisches und internationales Recht so weiterzuentwickeln und umzusetzen, dass es einen umfassenden Schutz der Privatsphäre, der informationellen Selbstbestimmung, des Fernmeldegeheimnisses und des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme garantiert.

- Sofern verfassungswidrige nachrichtendienstliche Kooperationen erfolgen, müssen diese abgestellt und unterbunden werden.

- Die Kontrolle der Nachrichtendienste muss durch eine Erweiterung der Befugnisse sowie eine gesetzlich festgelegte verbesserte Ausstattung der parlamentarischen Kontrollgremien intensiviert werden. Bestehende Kontrolllücken müssen unverzüglich geschlossen werden. In diesem Zusammenhang ist zu prüfen, ob die Datenschutzbeauftragten verstärkt in die Kontrolle der Nachrichtendienste eingebunden werden können.

- Es sind Initiativen zu ergreifen, die die informationelle Selbstbestimmung und das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme sicherstellen.

- Dazu gehört,
    - zu prüfen, ob das Routing von Telekommunikationsverbindungen in Zukunft möglichst nur über Netze innerhalb der EU erfolgen kann.
    - sichere und anonyme Nutzungsmöglichkeiten von Telekommunikationsangeboten aller Art auszubauen und zu fördern. Dabei ist sicherzustellen, dass den Betroffenen keine Nachteile entstehen, wenn sie die ihnen zustehenden Rechte der Verschlüsselung und Nutzung von Anonymisierungsdiensten ausüben.
    - die Voraussetzungen für eine objektive Prüfung von Hard- und Software durch unabhängige Zertifizierungsstellen zu schaffen.

- Völkerrechtliche Abkommen wie das Datenschutz-Rahmenabkommen und das Freihandelsabkommen zwischen der EU und den USA dürfen nur abgeschlossen werden, wenn die europäischen Datenschutzgrundrechte ausreichend geschützt werden. Das bedeutet auch, dass jeder Mensch das Recht hat, bei vermutetem Datenmissbrauch den Rechtsweg zu beschreiten. Das Fluggastdatenabkommen und das Überwachungsprogramm des Zahlungsverkehres müssen auf den Prüfstand gestellt werden.

- Auch innerhalb der Europäischen Union ist sicherzustellen, dass die nachrichtendienstliche Überwachung durch einzelne Mitgliedstaaten nur unter Beachtung grundrechtlicher Mindeststandards erfolgt, die dem Schutzniveau des Art. 8 der Charta der Grundrechte der Europäischen Union entsprechen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert alle Verantwortlichen auf, die umfassende Aufklärung mit Nachdruck voranzutreiben und die notwendigen Konsequenzen zügig zu treffen. Es geht um nichts weniger als das Grundvertrauen der Bürgerinnen und Bürger in den Rechtsstaat.

17.1.2 Entschließung der 86. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 1./2. Oktober 2013 in Bremen: Forderungen für die neue Legislaturperiode: Die Datenschutzgrundrechte stärken!

Die rasante technologische Entwicklung und ausufernde Datensammlungen bei Unternehmen, Nachrichtendiensten und anderen Behörden stellen eine gewaltige Herausforderung für den Datenschutz dar. Die Verletzlichkeit der Vertraulichkeit der Kommunikation und der Privatsphäre rückt - wie repräsentative Studien belegen - mehr und mehr in das Bewusstsein der Menschen. Zu Beginn der 18. Legislaturperiode des Deutschen Bundestages fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wirksame Maßnahmen zum Schutz der informationellen Selbstbestimmung.

Auch um den Vorgaben des Bundesverfassungsgerichts zum Schutz der Grundrechte in der Informationsgesellschaft Rechnung zu tragen, ist das Datenschutzrecht nicht nur auf nationaler, sondern auch auf europäischer und internationaler Ebene weiter zu entwickeln. Von besonderer Bedeutung ist dabei ein europäischer Datenschutz auf hohem Niveau. Flankierend müssen völkerrechtliche Rechtsinstrumente initiiert und weiterentwickelt werden.

Gesetzliche Schutzvorkehrungen und Maßnahmen zu deren Durchsetzung sind insbesondere in den folgenden Bereichen bedeutsam:

- Im besonders eingriffsintensiven Bereich der öffentlichen Sicherheit müssen wirksame Schranken für Grundrechtseingriffe dem Grundsatz der Verhältnismäßigkeit, dem informationellen Trennungsprinzip und dem Schutz des Kernbereichs privater Lebensgestaltung Rechnung tragen. Wichtig ist eine umfassende Kontrolle der Sicherheitsbehörden. Die Bundesregierung muss sich auch auf europäischer und internationaler Ebene für den wirksamen Schutz der Grundrechte einsetzen. Dies gilt insbesondere für

die Verhinderung von umfassender und anlassloser Überwachung durch Nachrichtendienste.[1]

- Angesichts der mit dem zunehmenden Wettbewerb im Sozial- und Gesundheitswesen verbundenen Risiken für die informationelle Selbstbestimmung müssen die Schutzrechte für die Privat- und Intimsphäre von Patientinnen, Patienten und Versicherten gestärkt werden.[2]

- Die Vertraulichkeit und Integrität elektronischer Kommunikation sind zu fördern. Der öffentliche Bereich muss hier mit gutem Beispiel vorangehen und die Ende-zu-Ende-Verschlüsselung z. B. mit Hilfe von OSCI-Transport flächendeckend einsetzen.[3]

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bietet bei der Verwirklichung dieser Anliegen ihre Mitwirkung an.

17.1.3 Entschließung der 86. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 1./2. Oktober 2013 in Bremen: Handlungsbedarf zum Datenschutz im Bereich der Öffentlichen Sicherheit in der 18. Legislaturperiode des Deutschen Bundestages

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht für die kommende Legislaturperiode dringenden datenschutzrechtlichen Handlungsbedarf im Bereich der öffentlichen Sicherheit. Die technische Entwicklung der Datenverarbeitung droht praktisch alle Bereiche unseres Lebens offenzulegen. Ungeheuer große Datenmengen können inzwischen in Echtzeit verknüpft und ausgewertet werden. Bei der weitgehend heimlich durchgeführten anlass- und verdachtslosen Datenauswertung rücken zunehmend auch Menschen in den Fokus von Nachrichtendiensten und Ermittlungsbehörden, die selbst keinerlei Anlass für eine Überwachung gegeben haben. Hieran können weitere Maßnahmen anknüpfen, die für die Betroffenen erhebliche Folgen haben. Dies gefährdet die Grundrechte auf informationelle Selbstbestimmung, auf Fernmeldegeheimnis und auf Gewährleistung des Schutzes der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die internationalen Überwachungsaktivitäten von Nachrichtendiensten machen dies deutlich. Die Bundesrepublik Deutschland ist verpflichtet, sich dagegen zu wenden und auf europäischer und internationaler Ebene dafür einzusetzen, dass es keine umfassende

[1] Siehe dazu die Entschließungen „Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen“ und „Handlungsbedarf zum Datenschutz im Bereich der öffentlichen Sicherheit in der 18. Legislaturperiode des Deutschen Bundestags“.
[2] Siehe dazu die heutige Entschließung „Stärkung des Datenschutzes im Sozial- und Gesundheitswesen“.
[3] Siehe dazu die heutige Entschließung "Sichere elektronische Kommunikation gewährleisten - Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln“.

Überwachung gibt. Hierzu hat die Konferenz bereits die Entschließung „Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen“ verabschiedet. Die Konferenz erwartet von der Bundesregierung außerdem, dass sie sich für die Aufhebung der EU-Richtlinie zur anlasslosen Vorratsdatenspeicherung von Telekommunikationsdaten einsetzt.

Die Übertragung weiterer, mit Grundrechtseingriffen verbundener, Kompetenzen an EU-Agenturen ist nach deutschem Verfassungsrecht nur vertretbar, wenn ein vergleichbarer Grundrechtsschutz gewährleistet ist. Die Konferenz fordert deshalb die Bundesregierung dazu auf, sich für entsprechende Nachbesserungen des von der Europäischen Kommission vorgelegten Entwurfs einer Europol-Verordnung einzusetzen.

Auch auf nationaler Ebene besteht gesetzgeberischer Handlungsbedarf. Unter Beachtung der Rechtsprechung des Bundesverfassungsgerichts insbesondere zur Antiterrordatei müssen für Maßnahmen, die intensiv in Grundrechte eingreifen, hinreichend bestimmte Schranken festgelegt werden. Sie müssen dem Grundsatz der Verhältnismäßigkeit, dem informationellen Trennungsprinzip und dem Kernbereichsschutz privater Lebensgestaltung stärker als bisher Rechnung tragen. Gesetzgeberischen Handlungsbedarf sieht die Konferenz insbesondere für gemeinsame Dateien und Zentren von Polizeien und Nachrichtendiensten, die nicht individualisierte Funkzellenabfrage, die strategische Fernmeldeüberwachung und für den Einsatz umfassender Analysesysteme.

Der Gesetzgeber muss zudem für wirksame rechtsstaatliche Sicherungen sorgen. Das Gebot des effektiven Rechtsschutzes setzt größtmögliche Transparenz der Datenverarbeitung und grundsätzlich Benachrichtigungen der Betroffenen voraus. Unverzichtbar ist die umfassende Kontrolle auch durch unabhängige Datenschutzbeauftragte. Die Sicherheitsbehörden müssen ihnen dazu alle notwendigen Informationen frühzeitig zur Verfügung stellen.

17.1.4 Entschließung der 86. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 1./2. Oktober 2013 in Bremen: Sichere elektronische Kommunikation gewährleisten - Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln

Die elektronische Datenübermittlung zwischen den Bürgern beziehungsweise der Wirtschaft und der öffentlichen Verwaltung im Zusammenhang mit E-Government-Verfahren erfordert insbesondere auch mit Blick auf die umfassenden und anlasslosen Überwachungsmaßnahmen ausländischer Geheimdienste technische und organisatorische Maßnahmen, um den Anforderungen an Datenschutz und Datensicherheit gerecht zu werden. Zur Sicherung der Vertraulichkeit, Integrität, Authentizität, Zweckbindung und

Transparenz bei der Datenübertragung sind kryptographische Verfahren erforderlich. Diese Verfahren können sowohl die Verbindungen zwischen den Endpunkten der Übertragung (Ende-zu-Ende-Verschlüsselung) als auch die Verbindungen zwischen den an der Übertragung beteiligten Netzknoten (Verbindungsverschlüsselung) sichern.

Für die Ende-zu-Ende-Verschlüsselung steht mit dem Online Services Computer Interface (OSCI-Transport) bereits seit einigen Jahren ein bewährter Standard zur Verfügung, den die Datenschutzkonferenz bereits im Jahr 2005 mit der Entschließung „Sicherheit bei E-Government durch Nutzung des Standards OSCI“ Bund, Ländern und Kommunen empfohlen hat. Das so genannte Verbindungsnetz, über das nach dem Netzgesetz ab 2015 jegliche Datenübermittlung zwischen den Ländern und dem Bund erfolgen muss, stellt hingegen nur eine Verbindungsverschlüsselung zwischen den Übergabepunkten zur Verfügung.

Die Datenschutzbeauftragten von Bund und Ländern weisen darauf hin, dass beide Ansätze sich ergänzen und dass deshalb auch nach Inbetriebnahme des Verbindungsnetzes der OSCI-Standard erforderlich ist.

Beide Ansätze haben ihre spezifischen Vor- und Nachteile, aus denen sich unterschiedliche Einsatzgebiete ergeben. Das Verbindungsnetz ist als geschlossenes Netz konzipiert. Durch die Infrastruktur des Verbindungsnetzes kann eine bestimmte Verfügbarkeit garantiert und die Vertraulichkeit der Nachrichten zwischen den Netzknoten gesichert werden.

An der OSCI-Infrastruktur kann hingegen prinzipiell jede deutsche Behörde teilnehmen. Mit OSCI kann die Vertraulichkeit der übertragenen Inhalte zwischen zwei Kommunikations-Endpunkten gesichert werden, so dass an keiner Zwischenstation im Netz Nachrichten im Klartext unbefugt gelesen oder geändert werden können. Anders als bei der Verbindungsverschlüsselung kann mit OSCI die Integrität und Authentizität der übermittelten Nachricht gegenüber Dritten nachgewiesen werden. Darüber hinaus können OSCI-gesicherte Nachrichten nicht unbemerkt verloren gehen und der Zugang von Sendungen kann mittels Quittungen bestätigt werden. Schließlich ist das Anbringen elektronischer Signaturen nach dem Signaturgesetz möglich.

Deshalb halten die Datenschutzbeauftragten des Bundes und der Länder den Einsatz von Standards zur Ende-zu-Ende-Verschlüsselung wie OSCI-Transport für geboten und fordern den IT-Planungsrat auf, diese kontinuierlich weiterzuentwickeln und verbindlich festzulegen. Sie fordern daneben Bund, Länder und Kommunen auf, die vorhandenen Standards bereits jetzt einzusetzen.

17.1.5 Entschließung der 86. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 1./2. Oktober 2013 in Bremen: Stärkung des Datenschutzes im Sozial- und Gesundheitswesen

Sozial- und Gesundheitsdaten gehören zu den intimsten Informationen über einen Menschen und sind deshalb auf einen besonders hohen Schutz angewiesen. Gerade sie sind jedoch auch insbesondere für Leistungserbringer und Sozialversicherungsträger von hohem wirtschaftlichem Wert. Durch die zunehmende Digitalisierung auch im Sozial- und Gesundheitswesen eröffnen sich vielfältige Erkenntnismöglichkeiten durch die Auswertung der anfallenden persönlichen Daten.

Vor dem Hintergrund des sich verschärfenden Wettbewerbs der Beteiligten im Sozial- und Gesundheitswesen geraten die Rechte der Patientinnen und Patienten und Versicherten immer stärker unter Druck. Dies zeigt sich zum Beispiel darin, dass eine Reihe von Krankenkassen und andere Sozialleistungsträger im Rahmen der Informationsbeschaffung die Empfänger von gesetzlichen Leistungen (zum Beispiel Krankengeld) über ihren Gesundheitszustand über das erforderliche Maß hinaus befragen und dabei gesetzlich vorgesehene Verfahren wie zum Beispiel die Einschaltung des Medizinischen Dienstes der Krankenversicherung umgehen.

Auch durch die Einbindung des Internets bei der Informationsverarbeitung im Gesundheitswesen, zum Beispiel durch Nutzung von Cloud-Diensten, sozialen Netzwerken und Big-Data-Strukturen, sowie durch die weit verbreitete Arbeitsteilung im Medizinbereich und insbesondere die Einschaltung von informationstechnischen Dienstleistern (Outsourcing) wird die Gefahr von „gläsernen Patientinnen und Patienten oder Versicherten“ weiter verstärkt.

Der Wettbewerb im Sozial- und Gesundheitswesen darf nicht zu Lasten der Rechte von Patientinnen und Patienten und Versicherten ausgetragen werden. Bei der künftigen Ausgestaltung des Gesundheitsbereichs müssen die Schutzrechte für die Privat- und Intimsphäre nachhaltig gestärkt und für Transparenz gesorgt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an die Regierungen und Parlamente des Bundes und der Länder:

- Bei der Nutzung neuer technischer Möglichkeiten muss das Recht auf informationelle Selbstbestimmung als unverzichtbares Grundrecht von vornherein berücksichtigt werden (privacy by design). Die Entwicklung datenschutzfreundlicher Technologien, zum Beispiel von Anonymisierungs-, Pseudonymisierungs- und Verschlüsselungsverfahren, sollte gefördert und deren Einsatz nach dem aktuellen Stand der Technik gesetzlich abgesichert werden.

- Die Telematikinfrastruktur ist umgehend und funktionsfähig so zu realisieren, dass die medizinische Kommunikation zwischen den Beteiligten im Gesundheitsbereich vertraulich und zuverlässig realisiert wird und die Patientinnen und Patienten praktisch in die Lage versetzt werden, ihr Recht auf informationelle Selbstbestimmung wahrzunehmen.

- Für die zunehmende Einschaltung technischer Dienstleister durch Leistungserbringer, insbesondere niedergelassene Ärztinnen und Ärzte, müssen angemessene datenschutzgerechte gesetzliche Regelungen verabschiedet werden.

17.1.6 Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2014 in Hamburg: Beschäftigtendatenschutz jetzt!

Trotz zahlreicher Aufforderungen durch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie des Deutschen Bundestages ist die Verabschiedung einer angemessenen Regelung des Beschäftigtendatenschutzes in der vergangenen Legislaturperiode erneut gescheitert. Der Koalitionsvertrag für die 18. Legislaturperiode sieht vor, das nationale Datenschutzniveau im Beschäftigtendatenschutz bei den Verhandlungen zur Europäischen Datenschutzgrundverordnung zu erhalten und darüber hinausgehende Standards zu ermöglichen. Falls mit einem Abschluss der Verhandlungen über die Europäische Datenschutzgrundverordnung nicht in angemessener Zeit gerechnet werden kann, soll eine nationale Regelung geschaffen werden.

Dies reicht nicht aus. Wann die Datenschutzgrundverordnung verabschiedet wird, ist derzeit völlig unklar. Ohnehin ist mit einem Inkrafttreten dieser europäischen Regelungen schon aufgrund der notwendigen Umsetzungsfrist erst in einigen Jahren zu rechnen. Aufgrund der voranschreitenden technischen Entwicklung, die eine immer weiter gehende Mitarbeiterüberwachung ermöglicht, besteht unmittelbarer Handlungsbedarf. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung deshalb auf, ein nationales Beschäftigtendatenschutzgesetzes umgehend auf den Weg zu bringen. Die Formulierung „in angemessener Zeit“ lässt befürchten, dass der Beschäftigtendatenschutz in dieser Legislaturperiode schon wieder auf die lange Bank geschoben wird.

Ein Beschäftigtendatenschutzgesetz muss ein hohes Datenschutzniveau gewährleisten und einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem Recht auf informationelle Selbstbestimmung des Arbeitnehmers schaffen.

Dies wird erkennbar in den vielfältigen Fragestellungen, für die es bislang keine klaren rechtlichen Vorgaben gibt. Zu nennen sind hier beispielsweise die immer umfassendere Videoüberwachung, Dokumentenmanagementsysteme, die die Leistung der Beschäftigten transparent werden lassen, die zunehmende Verquickung von Arbeit und Privatem verbunden mit der dienstlichen Nutzung von privaten Arbeitsmitteln wie Handy und Laptop, die Nutzung von dienstlich zur Verfügung gestellten Kfz mit oder ohne die Erlaubnis privater Nutzung oder die private Nutzung der vom Arbeitgeber zur Verfügung gestellten E-Mail- und Internetzugänge, der zunehmende Einsatz biometrischer Verfahren sowie die Erhebung und Verarbeitung von Bewerberdaten beispielweise aus sozialen Netzwerken.

Hierfür müssen künftig gesetzliche Standards geschaffen werden, um sowohl die Rechtssicherheit für die Arbeitgeber zu erhöhen als auch einen wirksamen Grundrechtsschutz für die Beschäftigten zu schaffen.

17.1.7 Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2014 in Hamburg: Struktur der künftigen Datenschutzaufsicht in Europa

Ein zentrales Verhandlungsthema bei den Beratungen im Rat der EU betrifft die Frage, welche Aufgaben die Datenschutzbehörden künftig haben und wie sie in Fällen, die mehrere Mitgliedstaaten oder die gesamte EU betreffen, besser zusammenarbeiten können. Die Europäische Kommission hatte hierzu das Prinzip einer einheitlichen Anlaufstelle („One-Stop-Shop“) vorgeschlagen, wonach die Datenschutzbehörde am Sitz der Hauptniederlassung EU-weit zuständig ist für die Aufsicht über alle Niederlassungen eines Unternehmens innerhalb der EU. Daneben schlug sie die Einführung eines Kohärenzverfahrens vor, das es den Datenschutzbehörden ermöglichen soll, in grenzüberschreitenden Fällen zu einheitlichen Entscheidungen im Rahmen des europäischen Datenschutzausschusses zu gelangen.

Vor dem Hintergrund der aktuell im Rat erörterten unterschiedlichen Modelle plädieren die Datenschutzbeauftragten des Bundes und der Länder für einen effektiven und bürgernahen Kooperations- und Entscheidungsmechanismus, der folgende Kernelemente beinhalten sollte:

1. Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen den Grundsatz, dass jede Aufsichtsbehörde im Hoheitsgebiet ihres Mitgliedstaats die ihr mit der Verordnung übertragenen Aufgaben und Befugnisse über alle Datenverarbeitungen ausübt, durch welche Personen dieses Mitgliedstaates betroffen sind, unabhängig davon,

ob die verantwortliche Stelle über eine Niederlassung innerhalb dieses Mitgliedstaates verfügt oder nicht.

2. Die Datenschutzbeauftragten des Bundes und der Länder befürworten die Einführung eines One-Stop-Shop-Mechanismus für Fälle, in denen der Datenverarbeiter über mehrere Niederlassungen in unterschiedlichen EU-Mitgliedstaaten verfügt. In diesem Fall fungiert die Aufsichtsbehörde am Ort der Hauptniederlassung als federführende Behörde, die mit den Aufsichtsbehörden der Mitgliedstaaten, in denen der Verantwortliche über weitere Niederlassungen verfügt oder in denen Personen betroffen sind, eng kooperiert. Es bleibt damit den betroffenen Personen unbenommen, sich an die Aufsichtsbehörden ihres Heimatlandes zu wenden.

3. Die federführende Behörde und die mit zuständigen nationalen Aufsichtsbehörden kooperieren mit dem Ziel einer einheitlichen Entscheidungsfindung. Im Falle der Einigkeit erlässt die federführende Behörde die erforderlichen Maßnahmen gegenüber der Hauptniederlassung des Verantwortlichen. Der Verantwortliche ist verpflichtet, die Maßnahmen in allen Niederlassungen innerhalb der EU umzusetzen.

4. Sofern eine nationale Behörde dem Maßnahmenentwurf der federführenden Behörde widerspricht, ist der Europäische Datenschutzausschuss mit dem Fall zu befassen, der hierzu verbindliche Leitlinien erlassen oder sonstige verbindliche Maßnahmen treffen kann.

5. Die Datenschutzbeauftragten des Bundes und der Länder befürworten die in dem Verordnungsentwurf enthaltenen Elemente zur Stärkung der Verantwortlichkeit der Unternehmen zur Einhaltung des Datenschutzrechts. Hierzu zählen die EU-weite Einführung betrieblicher Datenschutzbeauftragter, Datenschutz-Folgeabschätzungen, Privacy-by-Design und Privacy-by-Default, Zertifizierungen, Datenschutzsiegel und Verhaltensregeln. Fragen zur Rechtskonformität einer Datenverarbeitung können im Rahmen der vorherigen Zurate Ziehung mit den Aufsichtsbehörden geklärt werden.

6. Für die Einführung formeller, fristgebundener Verfahren zur Erlangung EU-weit gültiger Compliance-Entscheidungen besteht aus Sicht der Datenschutzbeauftragten des Bundes und der Länder daneben kein Bedarf. Insbesondere darf die Klärung von Compliance-Fragen nicht zu einer Verlagerung der Verantwortlichkeit auf die Aufsichtsbehörden und zur Einschränkung aufsichtsbehördlicher Maßnahmen im Falle von Datenschutzverstößen führen.

7. Ein originärer Schwerpunkt der Aufsichtstätigkeit in Bezug auf Zertifizierungsprozesse sollte darin liegen, im Rahmen der Norminterpretation Prüfstandards mitzugestalten, auf deren Grundlage die Vergabe von Zertifikaten geprüft wird.

17.1.8 Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2014 in Hamburg: Biometrische Gesichtserkennung durch Internetdienste - Nur mit Wahrung des Selbstbestimmungsrechts Betroffener!

Die Nutzung biometrischer Daten wird zunehmend zu einem Phänomen des Alltags. Dies gilt in besonderer Weise für die biometrische Gesichtserkennung, die in sozialen Medien auf dem Vormarsch ist. Für den Zweck der Auswertung von Personenfotos werden die Gesichter der Nutzer biometrisch erfasst, so dass ein späterer Abgleich mit anderen Fotos die Identifizierung einzelner Personen ermöglicht. Dazu werden sogenannte Templates erstellt. Dies sind mathematische Modelle der wesentlichen Merkmale des Gesichts wie etwa dem Abstand von Augen, Mundwinkel und Nasenspitze. Es darf nicht verkannt werden, dass die Vermessung der Gesichtsphysiognomie in hohem Maße die schutzwürdigen Interessen Betroffener berührt, denn stets ist die dauerhafte Speicherung eines Referenz-Templates des eigenen Gesichts erforderlich.

Dass die Templates dann in den Datenbanken global agierender Internetunternehmen gespeichert werden, stellt nicht erst seit den Enthüllungen über das Überwachungsprogramm Prism, das den US-Geheimdiensten den Zugriff auf die Datenbanken der US-Anbieter erlaubt, ein erhebliches Risiko für das Persönlichkeitsrecht des Einzelnen dar.

Die biometrische Gesichtserkennung ist eine Technik, die sich zur Ausübung von sozialer Kontrolle eignet und der damit ein hohes Missbrauchspotential immanent ist. Mit ihrer Hilfe ist es möglich, aus der Flut digitaler Fotografien im Internet gezielt Aufnahmen von Zielpersonen herauszufiltern. Darüber hinaus könnten durch den Abgleich von Videoaufnahmen mit vorhandenen Templates in Echtzeit Teilnehmerinnen und Teilnehmer etwa von Massenveranstaltungen sowie von Demonstrationen oder einfach nur Passanten individualisiert und identifiziert werden. Der Schutz der Anonymität des Einzelnen in der Öffentlichkeit lässt sich damit zerstören, ohne dass die Betroffenen ihre biometrische Überwachung kontrollieren oder sich dieser entziehen können.

An die Erzeugung biometrischer Templates der Gesichter von Personen durch Internet-Dienste sind daher hohe rechtliche Anforderungen zu stellen, die das informationelle Selbstbestimmungsrecht von Betroffenen in höchst möglicher Weise berücksichtigen:

- Die Erhebung, Verarbeitung und/oder Nutzung biometrischer Daten zur Gesichtserkennung zum Zweck der Erstellung eines dauerhaften biometrischen Templates kann

nur bei Vorliegen einer wirksamen Einwilligung des Betroffenen i. S. d. § 4a BDSG rechtmäßig erfolgen.

- Die Einwilligung in die Erstellung biometrischer Templates zur Gesichtserkennung muss aktiv und ausdrücklich durch den Betroffenen erteilt werden. Die Betroffenen müssen vor der Erteilung der Einwilligung über die Funktionsweise der Erstellung und Nutzung der sie möglicherweise betreffenden Templates und die damit verfolgten Zwecke und Risiken in klarer und verständlicher Weise umfassend informiert werden. Eine Zweckänderung ist unzulässig. Sie bedarf einer Einwilligung, die dem Standard an die Einwilligungen bei der Verarbeitung besonderer personenbezogener Daten, § 4a Abs. 3 BDSG, entspricht.

- Die Einwilligung kann nicht durch den Verweis auf entsprechende Klauseln in allgemeinen Nutzungsbedingungen oder Datenschutzerklärungen ersetzt werden.

- Für eine logische Sekunde kann es nach § 28 Abs. 1 Satz 1 Nr. 2 bzw. Nr. 3 BDSG auch ohne Einwilligung zulässig sein, ein Template zu erstellen, mit dem ein Abgleich mit bereits vorhandenen, zulässigerweise gespeicherten Templates im Rahmen des von der Einwilligung abgedeckten Zwecks möglich ist. Betroffene sind über den Umstand, dass Bilder zum Abgleich mit bestehenden Templates verwendet werden, zu informieren.

- Derartige biometrische Templates zum automatischen Abgleich, bei denen eine Einwilligung fehlt, sind unverzüglich nach dem Abgleich zu löschen.

- Die Speicherung von biometrischen Templates von Dritten, die - anders als die Nutzer von sozialen Medien - regelmäßig nicht einwilligen können, ist ausgeschlossen.

17.1.9 Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2014 in Hamburg: Öffentlichkeitsfahndung mit Hilfe sozialer Netzwerke - Strenge Regeln erforderlich!

Mit zunehmender Beliebtheit sozialer Netzwerke bei Bürgerinnen und Bürgern steigt das Interesse von Strafverfolgungsbehörden, diese sozialen Netzwerke auch zur Öffentlichkeitsfahndung zu nutzen. So gibt es in Deutschland bereits Polizeidienststellen, die mittels Facebook nach Straftätern suchen. Auch die 84. Konferenz der Justizministerinnen und Justizminister hat sich im November 2013 mit dem Thema befasst.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es erneut für notwendig darauf hinzuweisen, dass eine Nutzung sozialer Netzwerke privater Betreiber (wie z. B. Facebook) zur Öffentlichkeitsfahndung aus datenschutzrechtlicher Sicht sehr problematisch ist. Durch die weltweit recherchierbare Veröffentlichung von Fahndungsdaten wird in weitaus schwerwiegenderer Weise in die Grundrechte Betroffener (Tatverdächtiger oder auch Zeugen) eingegriffen, als dies bei der Nutzung klassischer Medien der Fall ist. Auch sind im Internet veröffentlichte Daten einer Fahndungsausschreibung nur sehr schwer bzw. gar nicht mehr zu löschen. Geben Nutzerinnen und Nutzer der Sozialen Netzwerke in Diskussionsforen und Nutzerkommentaren öffentlich Spekulationen, Behauptungen und Diskriminierungen ab, beeinträchtigt dies die Persönlichkeitsrechte der Betroffenen erheblich. Solche Funktionen sind in von den Ermittlungsbehörden betriebenen Angeboten weder geeignet noch erforderlich, um die behördlichen Aufgaben zu erfüllen. Die Konferenz weist darauf hin, dass Öffentlichkeitsfahndung nur auf Diensten von Anbietern erfolgen darf, die die datenschutzrechtlichen Vorgaben des Telemediengesetzes zur Nutzungsdatenverarbeitung, insbesondere der Regeln zur Reichweitenmessung gemäß §§ 13 Abs. 4 Nr. 6, 15 Abs. 3 TMG, und das Recht auf anonyme und pseudonyme Nutzung gemäß § 13 Abs. 6 TMG beachten.

Sofern es Strafverfolgungsbehörden gleichwohl gestattet werden soll, zu Zwecken der Öffentlichkeitsfahndung auf soziale Netzwerke mit deaktivierter Kommentierungsfunktion zurückzugreifen, so darf dies - ungeachtet der generellen Kritik an der Nutzung sozialer Netzwerke durch öffentliche Stellen - nur geschehen, wenn folgende Maßgaben beachtet werden:

- Die Vorschriften der Strafprozessordnung (§ 131 Abs. 3, § 131 a Abs. 3, § 131 b StPO) zur Öffentlichkeitsfahndung kommen aufgrund der technikoffenen Formulierung als Rechtsgrundlage für die Öffentlichkeitsfahndung im Internet grundsätzlich in Betracht. Sie sind aber im Hinblick auf den Verhältnismäßigkeitsgrundsatz nur eingeschränkt anzuwenden. Eine entsprechende Klarstellung durch den Gesetzgeber wäre wünschenswert. Zumindest aber sind die besonderen Voraussetzungen der Fahndung im Internet, insbesondere in sozialen Netzwerken in Umsetzungsvorschriften zu konkretisieren. Änderungsbedarf besteht beispielsweise für die Anlage B der RiStBV.

- In materiell-rechtlicher Hinsicht haben die Strafverfolgungsbehörden den Verhältnismäßigkeitsgrundsatz strikt zu beachten. Die zu schaffenden Regelungen müssen den besonderen Gefahren der Öffentlichkeitsfahndung in sozialen Netzwerken gerecht werden. Insbesondere muss sichergestellt werden, dass eine solche Fahndung nur bei im Einzelfall schwerwiegenden Straftaten überhaupt in Betracht gezogen werden kann.

- In verfahrensrechtlicher Hinsicht müssen die Umsetzungsregelungen die Staatsanwaltschaft verpflichten, bereits im Antrag auf richterliche Anordnung der Maßnahme die Art, den Umfang und die Dauer der Öffentlichkeitsfahndung konkret anzugeben. Dies umfasst insbesondere die ausdrückliche Angabe, ob und warum die Anordnung auch die Öffentlichkeitsfahndung in sozialen Netzwerken umfassen soll.

- Es ist sicherzustellen, dass
  - die zur Öffentlichkeitsfahndung verwendeten personenbezogenen Daten von den Strafverfolgungsbehörden ausschließlich auf im eigenen Verantwortungsbereich stehenden Servern gespeichert und verarbeitet werden, nicht hingegen auf Servern der privaten Anbieter,
  - die Weitergabe und der automatisierte Abruf der personenbezogenen Daten aus dem Internet durch Web-Crawler und ähnliche Dienste so weit als technisch möglich verhindert werden,
  - die Kommunikation zwischen den Strafverfolgungsbehörden und den Nutzern nur außerhalb der sozialen Netzwerke erfolgt.

17.1.10 Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2014 in Hamburg: Gewährleistung der Menschenrechte bei der elektronischen Kommunikation

Die Enthüllungen des Whistleblowers Edward Snowden haben ein Ausmaß an geheimdienstlicher Überwachung aufgezeigt, das viele zuvor nicht für möglich gehalten hatten. Die tendenziell unbegrenzte und kaum kontrollierte Überwachung der elektronischen Kommunikation aller verletzt das auch im digitalen Zeitalter weltweit anerkannte Recht auf Privatheit in täglich wiederkehrender millionenfacher Weise. Dies beeinträchtigt zugleich die Wahrnehmung anderer Menschenrechte wie der Meinungs- und Versammlungsfreiheit. Es ist eine gesamtgesellschaftliche Aufgabe, berechtigtes Vertrauen in die prinzipielle Unverletzlichkeit der Kommunikation wieder herzustellen.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher schon im September 2013 gefordert, auf diese neue Qualität der Überwachung rechtlich und politisch zu reagieren. Darüber hinaus sind aber auch technische und organisatorische Schutzmaßnahmen erforderlich. Der Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen sowie der Vertraulichkeit und Integrität informationstechnischer Systeme muss wieder hergestellt und dauerhaft gesichert werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher die Prüfung und Umsetzung folgender Maßnahmen:

1. Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten,
2. Bereitstellung einer einfach bedienbaren Verschlüsselungs-Infrastruktur,
3. Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verfahren zur Verbindungsverschlüsselung,
4. Sichere und vertrauenswürdige Bereitstellung von Internetangeboten,
5. Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten,
6. Ausbau der Angebote und Förderung anonymer Kommunikation,
7. Angebot für eine Kommunikation über kontrollierte Routen,
8. Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung,
9. Beschränkung des Cloud Computing mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheit,
10. Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung,
11. Sensibilisierung von Nutzerinnen und Nutzern moderner Technik,
12. Ausreichende Finanzierung von Maßnahmen der Informationssicherheit.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzkonferenz hat einen Anforderungskatalog formuliert, der die hier genannten Maßnahmen konkretisiert (siehe Anlage zu dieser Entschließung).

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Anbieter elektronischer Kommunikationsdienste auf, entsprechende Technologien und Dienste zur Verfügung zu stellen. Die Verwaltungen in Bund und Ländern, insbesondere die zuständigen Regulierungsbehörden, sind aufgefordert, auf die Durchsetzung der o. g. Maßnahmen zu dringen. Der Gesetzgeber ist aufgerufen, die zu ihrer Durchsetzung ggf. nötigen Änderungen und Präzisierungen an dem bestehenden Rechtsrahmen vorzunehmen.

Anlage zur Entschließung „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation

1. Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten als wesentliches Element für den Schutz von Daten

Der verschlüsselte Transport und die verschlüsselte Speicherung von Daten müssen zu einem in Produkte und Verfahren integrierten Standard werden, der durch jedermann einfach zu nutzen ist. Sichere kryptographischen Algorithmen, die seit vielen Jahren zur Verfügung stehen, stellen auch für Geheimdienste eine erhebliche Hürde dar und erschweren die unberechtigte Kenntnisnahme der so geschützten Daten wesentlich.

Für die Sicherung der Übertragungswege sollen Verfahren zum Einsatz kommen, die eine nachträgliche Entschlüsselung des abgeschöpften Datenverkehrs erschweren (perfect forward secrecy).

2. *Bereitstellung einer von jeder Person einfach bedienbaren Verschlüsselungs-Infrastruktur*

Für eine breite Anwendung von Verschlüsselung durch die Bürgerinnen und Bürger wird eine Infrastruktur benötigt, die es jeder Person weitgehend ohne Barrieren (in Form von Wissen, nötiger spezieller Software oder finanziellen Mitteln) ermöglicht, den von ihr verwendeten Kommunikationsadressen Schlüssel authentisch zuzuordnen und die anderer zu nutzen. Die Entstehung dieser Infrastruktur bedarf der Förderung durch den Staat unter Einbeziehung bestehender Instrumente bspw. durch Entwicklung kryptografischer Zusatzfunktionen des neuen Personalausweises.

Es mangelt also nicht vorrangig an theoretischen Konzepten, sondern an einer ausreichenden Durchdringung in der Praxis. Der öffentliche wie der private Sektor müssen daher ihre Anstrengungen erhöhen, Verschlüsselungstechniken selbst einzusetzen und in ihre Produkte und Dienstleistungen einzubinden.

3. *Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verbindungsverschlüsselung*

Der Einsatz von Mechanismen für eine Ende-zu-Ende-Verschlüsselung muss gefördert werden. Die Enthüllungen von Edward Snowden haben gezeigt, dass der Zugriff auf Daten besonders einfach ist, wenn sie an Netzknoten unverschlüsselt vorliegen oder innerhalb interner Netze unverschlüsselt übertragen werden. Nur eine Ende-zu-Ende-Verschlüsselung ist in der Lage, die Inhaltsdaten auch an diesen Stellen zu schützen. Die zusätzliche Verschlüsselung der Verbindungen zwischen den an der Übertragung beteiligten Netzknoten (Verbindungsverschlüsselung) hingegen schützt die Metadaten der Kommunikation in allen Zwischenknoten der verschlüsselten Wegstrecke. Durch die Kombination beider Verfahren kann ein Optimum an Schutz zwischen den Endpunkten erreicht werden.

Für beide Ansätze stehen etablierte Verfahren zur Verfügung, sowohl in Bezug auf kryptografische Verfahren und Datenformate, als auch in Bezug auf das Identitäts- und Schlüsselmanagement, von dessen Stringenz die Sicherheit wesentlich abhängt.

4. Sichere und vertrauenswürdige Bereitstellung von Internetangeboten

Sämtliche Internetangebote öffentlicher Stellen sollten standardmäßig über TLS (Transport Layer Security) / SSL (Secure Socket Layer) unter Beachtung der Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik angeboten werden. Die Behörden sollten sich hierbei mit Zertifikaten ausweisen, die von vertrauenswürdigen Ausstellern herausgegeben wurden, die sich in europäischer, und vorzugsweise in öffentlicher Hand befinden. Nichtöffentliche Stellen stehen gleichermaßen in der Verpflichtung, die Nutzung von ihnen angebotener Telemedien einschließlich der von einem Nutzer abgerufenen URIs (Uniform Resource Identifier) gegen Kenntnisnahme Dritter im Rahmen der Verhältnismäßigkeit durch Verschlüsselung zu schützen.

5. Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten

Die von der Wissenschaft bereits untersuchten Methoden metadatenarmer E-Mail-Kommunikation müssen weiterentwickelt und sowohl für E-Mail als auch für andere nachrichtenbasierte Kommunikationsformate alltagstauglich gemacht werden. Denn auch eine wirksame Ende-zu-Ende-Verschlüsselung verhindert nicht, dass beim E-Mail-Versand Metadaten anfallen, die aussagekräftige Rückschlüsse auf die Kommunikationspartner und deren Standorte zulassen. Die an die Öffentlichkeit gelangten Dokumente von Geheimdiensten haben gezeigt, dass allein durch Analyse der E-Mail-Metadaten riesige Datenbanken gefüllt wurden, mit denen nachvollzogen werden kann, wer mit wem von welchem Ort aus kommuniziert hat.

6. Ausbau der Angebote und Förderung anonymer Kommunikation

Verfahren zur anonymen Nutzung von Internet und Telekommunikationsangeboten müssen gefördert und entsprechende Angebote ausgebaut werden. Nutzerinnen und Nutzer müssen Anonymisierungsdienste nutzen können, ohne dass ihnen daraus Nachteile entstehen. Die Einbindung derartiger Konzepte trägt substantiell zur Umsetzung der gesetzlich normierten Forderung nach Datensparsamkeit bei und verringert die Gefahr missbräuchlicher Nutzung von Daten.

7. Angebot für eine Kommunikation über kontrollierte Routen

Deutsche und internationale Provider sollen Angebote zur Verfügung stellen, über selbst bestimmte Wege untereinander zu kommunizieren. Möglichst kurze, geografisch lokale Routen können ggf. die Wahrscheinlichkeit illegitimen Eingriffs in den Datenstrom reduzieren. Kontrollmöglichkeiten über die Datenströme werden verbessert, wenn

die Kommunikation vollständig über eigene Leitungen abgewickelt oder verschlüsselt wird.

Solche Konzepte dürfen jedoch nicht verwechselt werden mit der Kontrolle des Internet oder Versuchen, Teile davon abzuschotten - dies wäre in jeder Hinsicht kontraproduktiv. Sie müssen daher sowohl anbieterneutral als auch supranational angegangen werden und setzen optimal direkt bei den zugrunde liegenden technischen Standards an.

8. Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung

Die Kommunikation mittels mobiler Geräte und der Zugang zum Internet mit Hilfe mobiler Kommunikationstechnik müssen den gleichen Datenschutz- und Sicherheitsanforderungen wie denen bei drahtgebundener Kommunikation genügen.

Dazu gehört sowohl eine wirksame Verschlüsselung als auch die Geheimhaltung von Daten, die zur Lokalisierung der Nutzerinnen und Nutzer genutzt werden können.

Der Schutz des Fernmeldegeheimnisses durch die Mobilfunkanbieter wird dadurch gefördert, dass

- alle Übertragungswege - sowohl vom Gerät zur Basisstation, als auch innerhalb des Netzwerks des TK-Anbieters - verschlüsselt werden,
- für die Verschlüsselung vom Mobilgerät zur Basisstation im GSM-Netz mindestens die Chiffre A5/3 zur Anwendung kommt, bis eine nachhaltig sichere Nachfolgechiffre zur Verfügung steht,
- eine Authentifizierung der Basisstationen gegenüber den Mobilgeräten erfolgt (diese Funktionalität bedarf der Unterstützung durch die vom TK-Anbieter bereitgestellte SIM-Karte) und
- die Kenntnis von Lokalisierungsdaten auf die Betreiber der Netze, in welche das jeweilige Gerät sich einbucht, und den Betreiber seines Heimatnetzes beschränkt wird.

Die Bundesnetzagentur sollte im Rahmen ihrer Aufgaben und Befugnisse aktiv auf die TK-Anbieter zur Durchsetzung dieser Maßnahmen einwirken.

Ferner bedarf es einer internationalen Anstrengung zur Anpassung oder Neudefinition von Standards für Mobilfunknetzwerke aller Generationen mit dem Ziel, die durchgreifende Gewährleistung von Vertraulichkeit der Inhaltsdaten sowie der Vertraulichkeit und Datensparsamkeit der Verkehrs- und Standortdaten zu ermöglichen.

Wie für TK-Anbieter, so gilt auch für Anbieter von Telemedien für die mobile Nutzung, insbesondere in Form mobiler Anwendungen (Apps), dass sie die Erhebung von personenbezogenen Daten auf das für die jeweils erbrachte Dienstleistung erforderliche Minimum beschränken müssen und die Übertragung dieser Daten durch Verschlüsselung schützen sollten. Apps sollten künftig so durch Nutzerinnen und Nutzer konfigurierbar sein, dass diese selbst bestimmen können, wem welche Daten zu welchem Zweck übermittelt werden.

9. Beschränkung des Cloud Computings mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheitstechnik

Sollen personenbezogene Daten in einer Cloud-Anwendung verarbeitet werden, so dürfen nur Anbieter zum Zuge kommen, deren Vertrauenswürdigkeit sowohl in Bezug auf die Gewährleistung der Informationssicherheit, als auch in Bezug auf den Rechtsrahmen, innerhalb dessen sie operieren, gegeben ist.

Dazu gehören unter anderem ein (zertifiziertes) Informationssicherheitsmanagement, die sichere Verschlüsselung der zu verarbeitenden Daten sowohl bei ihrer Übertragung in und aus der Cloud als auch bei ihrer Speicherung und eine durch den Auftraggeber kontrollierte Vergabe von Unteraufträgen. Das Datenschutzniveau dieser Dienste sollte durch unabhängige und fachkundige Auditoren geprüft und zertifiziert werden.

10. Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung

Hard- und Software sollten so entwickelt und hergestellt werden, dass Anwenderinnen und Anwender und unabhängige Dritte sich jederzeit von der Wirksamkeit der getroffenen Sicherheitsvorkehrungen überzeugen können. Open-Source-Produkte ermöglichen derartige Prüfungen besonders gut. Daher ist der Einsatz von Open-Source-Produkten zu fördern.

Darüber hinaus ist es erforderlich, die bereits bestehenden Zertifizierungsverfahren für informationstechnische Produkte und die Informationssicherheit von Verarbeitungsvorgängen breiter zur Anwendung zu bringen und um weitere Zertifizierungsverfahren zu ergänzen, um die Vertrauenswürdigkeit von informationstechnischen Produkten zu stärken. Voraussetzung dafür sind unabhängige und fachkundige Auditoren sowie transparente Kriterienkataloge und Zertifizierungsprozesse.

11. Sensibilisierung von Nutzerinnen und Nutzern moderner Technik

Viele technische Vorkehrungen zum Schutz elektronisch übermittelter und gespeicherter Daten entfalten nur dann ihre volle Wirksamkeit, wenn die Nutzerinnen und Nutzer deren Vorteile kennen, mit diesen Vorkehrungen umgehen können und sie selbst einsetzen. Daher ist eine breit angelegte Bildungsoffensive erforderlich, mit der die notwendigen Kenntnisse und Fähigkeiten vermittelt werden.

12. Ausreichende Finanzierung für Maßnahmen der Informationssicherheit

Die Ausgaben der öffentlichen Hand für Informationssicherheit müssen erhöht werden und in einem angemessenen Verhältnis zum gesamten IT-Budget stehen. Die Koalitionspartner auf Bundesebene haben die Bundesbehörden bereits verpflichtet, zehn Prozent des IT-Budgets für die Sicherheit zu verwenden. Dies muss in angemessener Weise auch für Landesbehörden und andere öffentliche Stellen gelten. Die Ressourcen werden sowohl für die Planung und Absicherung neuer Vorhaben insbesondere des E-Governments als auch für die Revision und sicherheitstechnische Ergänzung der Verfahren und der Infrastruktur im Bestand benötigt.

17.1.11 Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2014 in Hamburg: Datenschutz im Kraftfahrzeug - Automobilindustrie ist gefordert

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist auf die datenschutzrechtlichen Risiken hin, die mit der zunehmenden Datenverarbeitung in Kraftfahrzeugen und ihrer Vernetzung untereinander, mit ihrer Umgebung und mit dem Internet entstehen. Die Datenverarbeitung in modernen Fahrzeugen schafft Begehrlichkeiten, die dort anfallenden Daten für die verschiedensten Zwecke nutzen zu wollen - etwa bei Arbeitgebern und Versicherungen. Dabei besteht die Gefährdungslage bereits im Zeitpunkt des Erfassens von Daten in den im Auto integrierten Steuergeräten und nicht erst mit deren Auslesen oder Übermitteln. Bereits diese personenbezogenen Daten geben Auskunft über Fahrverhalten und Aufenthaltsorte und können zur Informationsgewinnung über den Fahrer bzw. den Halter bis hin zur Bildung von Persönlichkeitsprofilen herangezogen werden.

Um eine selbstbestimmte Fahrzeugnutzung frei von Furcht vor Überwachung zu gewährleisten, sind Automobilhersteller, Händler, Verkäufer, Werkstätten ebenso wie Anbieter von Kommunikations- und Telediensten rund um das Kraftfahrzeug im Rahmen ihres Wirkungskreises in der Pflicht, informationelle Selbstbestimmung im und um das Kraftfahrzeug zu gewährleisten.

Dazu gehört:

- Bereits in der Konzeptionsphase sind bei der Entwicklung neuer Fahrzeugmodelle und neuer auf Fahrzeuge zugeschnittene Angebote für Kommunikations- und Teledienste die Datenschutzgrundsätze von privacy by design bzw. privacy by default zu verwirklichen.

- Datenverarbeitungsvorgängen im und um das Fahrzeug muss das Prinzip der Datenvermeidung und Datensparsamkeit zu Grunde liegen. Daten sind in möglichst geringem Umfang zu erheben und umgehend zu löschen, nachdem sie nicht mehr benötigt werden.

- Die Datenverarbeitungen müssen entweder vertraglich vereinbart sein oder sich auf eine ausdrückliche Einwilligung stützen.

- Für Fahrer, Halter und Nutzer von Fahrzeugen muss vollständige Transparenz gewährleistet sein. Dazu gehört, dass sie umfassend und verständlich darüber zu informieren sind, welche Daten beim Betrieb des Fahrzeugs erfasst und verarbeitet sowie welche Daten über welche Schnittstellen an wen und zu welchen Zwecken übermittelt werden. Änderungen sind rechtzeitig anzuzeigen.

  Die Betroffenen müssen in die Lage versetzt werden, weitere Nutzer ebenfalls zu informieren.

- Auch bei einer vertraglich vereinbarten oder von einer Einwilligung getragenen Datenübermittlung an den Hersteller oder sonstige Diensteanbieter sind Fahrer, Halter und Nutzer technisch und rechtlich in die Lage zu versetzen, Datenübermittlungen zu erkennen, zu kontrollieren und ggf. zu unterbinden. Zudem muss Wahlfreiheit für datenschutzfreundliche Systemeinstellungen und die umfangreiche Möglichkeit zum Löschen eingeräumt werden.

- Schließlich muss durch geeignete technische und organisatorische Maßnahmen Datensicherheit und -integrität gewährleistet sein. Dies gilt insbesondere für die Datenkommunikation aus Fahrzeugen heraus.

Auf dieser Grundlage wirkt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder darauf hin, dass Automobilhersteller, Zulieferer und ihre Verbände bundesweit einheitliche Datenschutzstandards auf hohem Niveau setzen, die dazu beitragen, dass Innovation auch mit gesellschaftlicher Akzeptanz einhergeht.

17.1.12 Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2014 in Hamburg: Effektive Kontrolle von Nachrichtendiensten herstellen!

Die Enthüllungen über die Spähaktivitäten ausländischer Nachrichtendienste haben verdeutlicht, wie viele Kommunikationsdaten in der digitalisierten Welt anfallen, welche Begehrlichkeiten diese Daten offensichtlich auch bei Nachrichtendiensten demokratischer Länder wecken und mit welchen weitreichenden Methoden die Nachrichtendienste Informationen erfassen, sammeln und analysieren. Auch die deutschen Nachrichtendienste haben weitreichende Befugnisse zur Erhebung, Sammlung und Auswertung personenbezogener Daten sowie zum Austausch dieser untereinander bzw. mit Polizeibehörden. Die Befugnisse der Nachrichtendienste schließen auch die Überwachung der Telekommunikation ein. Damit einher geht im Bereich der strategischen Auslandsüberwachung des BND ein Kontrolldefizit. Auch eine Beteiligung des Bundesnachrichtendienstes durch Datenaustausch mit ausländischen Diensten steht im Raum. In den vergangenen Jahren wurden die gesetzlichen Befugnisse der Nachrichtendienste stetig erweitert. So wurden die Antiterrordatei und die Rechtsextremismusdatei als gemeinsame Dateien von Polizei und Nachrichtendiensten eingeführt sowie gemeinsame Zentren von Nachrichtendiensten und Polizeibehörden errichtet. Die Berichte der NSU-Untersuchungsausschüsse des Deutschen Bundestages und einiger Landesparlamente haben darüber hinaus erhebliche Kontrolldefizite auch bei den Verfassungsschutzämtern offengelegt. Nach der Einschätzung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist daher eine Reform der rechtsstaatlichen Kontrolle der deutschen Nachrichtendienste dringend geboten.

Für die Betroffenen ist die aufgrund der Befugnisse der Nachrichtendienste und Sicherheitsbehörden vorgenommene Datenverarbeitung in weitem Maße intransparent, daher ist auch der Individualrechtsschutz faktisch eingeschränkt. Umso wichtiger ist die Kontrolle durch unabhängige Stellen. In der Entscheidung zum Antiterrordateigesetz vom 24. April 2013 hat das Bundesverfassungsgericht insoweit hervorgehoben, dass der Verhältnismäßigkeitsgrundsatz bei Datenverarbeitungen, die für die Betroffenen nur eingeschränkt transparent sind, gesteigerte Anforderungen an eine wirksame Ausgestaltung der Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis stellt. Eine wichtige Rolle kommt dabei den Datenschutzbeauftragten des Bundes und der Länder zu, die neben den parlamentarischen Kontrollinstanzen die Kontrolle über die Nachrichtendienste ausüben. Bestimmte Bereiche nachrichtendienstlicher Tätigkeiten sind der Eigeninitiativkontrolle durch die Datenschutzbeauftragten des Bundes und der Länder von vornherein entzogen. Es ist sinnvoll, das bei den Datenschutzbeauftragten des Bundes und der Länder bereits vorhandene Fachwissen auch in diesem Bereich zu

nutzen und die Datenschutzbehörden mit den entsprechenden Prüfbefugnissen und den hierfür erforderlichen personellen Ausstattung und Sachmitteln auszustatten.

Das Bundesverfassungsgericht hat mit der Entscheidung vom 24. April 2013 zum Zusammenwirken zwischen den Datenschutzbeauftragten und den parlamentarischen Kontrollinstanzen festgestellt: „Wenn der Gesetzgeber eine informationelle Kooperation der Sicherheitsbehörden vorsieht, muss er auch die kontrollierende Kooperation zugunsten des Datenschutzes ermöglichen.“ In diesem Sinne darf die Verteilung der Kontrolle auf mehrere Stellen nicht die Effektivität der Kontrolle einschränken. Für den Bereich der Telekommunikationsüberwachung nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses ist die Kontrolle durch die G10-Kommission aus eigener Initiative derzeit gesetzlich nicht vorgesehen. Ebenso fehlt ein Kontrollmandat der Datenschutzbeauftragten für Beschränkungen des Fernmeldegeheimnisses. Vor dem Hintergrund der Ausführungen des Bundesverfassungsgerichtes erscheint eine Einbindung der Datenschutzbeauftragten neben den parlamentarischen Kontrollinstanzen aber erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher den Gesetzgeber auf, die Datenschutzbehörden mit entsprechenden Prüfbefugnissen auszustatten, damit das bei ihnen vorhandene Fachwissen auch in diesem Bereich genutzt werden kann.

17.1.13 Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2014 in Hamburg: Marktmacht und informationelle Selbstbestimmung

Die Konzentration wirtschaftlicher Macht und der Missbrauch marktbeherrschender Stellungen ist bisher Gegenstand des Wettbewerbs- und insbesondere des Kartellrechts. So untersucht gegenwärtig die Europäische Kommission mögliche Verstöße von Google gegen das Europäische Wettbewerbsrecht wegen mangelhafter Neutralität der Suchergebnisse.

Darüber hinaus ist jedoch zu lange übersehen worden, dass die zunehmenden Unternehmenskäufe vor allem im Bereich der Internetwirtschaft zu einer massiven Anhäufung von personenbezogenen Daten bis hin zur Monopolbildung in bestimmten Bereichen führen können. Datenmacht wird zur Marktmacht. Im April 2007 kaufte Google für 3,1 Mrd. US-Dollar das Werbeunternehmen Double- Click. Die Übernahme wurde sowohl von den Kartellbehörden in den USA und in Europa gebilligt, ohne dass die Auswirkungen dieser Übernahme auf den Datenschutz der Nutzer in diesen Entscheidungen berücksichtigt worden wäre. Facebook hat im vergangenen Jahr für die Über-

nahme von WhatsApp 18 Mrd. US-Dollar gezahlt. Auch dieser Zusammenschluss ist inzwischen sowohl in den USA als auch in der EU genehmigt worden, ohne dass es wirksame Garantien gegen eine weitere Verschlechterung des Datenschutzes gibt.

Sowohl der Europäische Datenschutzbeauftragte als auch die deutsche Monopolkommission haben inzwischen auf die möglichen Auswirkungen der Zusammenschlüsse gerade von solchen Internet-Unternehmen auf die informationelle Selbstbestimmung hingewiesen, deren Geschäftsmodelle wesentlich auf der Anhäufung von personenbezogenen Daten beruhen. Die massive Ausweitung von scheinbar kostenlosen Diensten und die wachsende Bedeutung von „Big Data“ erfordert nach Ansicht des Europäischen Datenschutzbeauftragten einen intensiveren Dialog zwischen den Datenschutz- und den Kartellbehörden, um die Wahlfreiheit wie auch die informationelle Selbstbestimmung der Nutzer angesichts abnehmender Konkurrenz aufrechtzuerhalten oder wiederherzustellen und um die Aufsichtsbefugnisse koordiniert einzusetzen. Die Monopolkommission hat in ihrem XX. Hauptgutachten (2012/2013 - Kapitel I) für eine verstärkte Kooperation von Datenschutz- und Wettbewerbsbehörden plädiert und sich für eine schnelle Verabschiedung der europäischen Datenschutzgrundverordnung eingesetzt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder setzt sich ebenfalls für eine Datenschutzgrundverordnung auf hohem Niveau ein. Sie ist davon überzeugt, dass insbesondere das Recht auf Datenportabilität sowohl die Souveränität des einzelnen Nutzers stärken als auch die auf der Sammlung personenbezogener Daten beruhende Machtposition einzelner Marktteilnehmer begrenzen kann.

Die Konferenz der Datenschutzbeauftragten weist daraufhin, dass eine stärkere Zusammenarbeit mit den Kartellbehörden sinnvoll ist. Ziel muss es dabei zugleich sein, den Datenschutz im Wettbewerb besser zu fördern.

17.1.14 Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2014 in Hamburg: Unabhängige und effektive Datenschutzaufsicht für Grundrechtsschutz unabdingbar

Die Bundesregierung hat am 27. August 2014 einen Gesetzentwurf zur Stärkung der Unabhängigkeit der Datenschutzaufsicht im Bund beschlossen (siehe BR Drs. 395/14). Er sieht vor, dass die bisher beim Bundesministerium des Inneren eingerichtete Bundesbeauftragte für den Datenschutz und die Informationsfreiheit in eine eigenständige oberste Bundesbehörde umgewandelt wird.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass nunmehr auch der Bundesgesetzgeber die vom Europäischen Gerichtshof in mehreren Urteilen konkretisierten Voraussetzungen für eine völlig unabhängige Datenschutzaufsicht herstellen will. Es ist erfreulich, dass die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit künftig keiner Aufsicht durch eine andere Behörde mehr unterliegen wird und aufgrund ihres Status‘ als eigenständiger oberster Bundesbehörde ohne jeden Einfluss anderer Behörden selbst über ihren eigenen Haushalt und ihr eigenes Personal verfügen kann.

Die Konferenz weist jedoch auf wesentliche Punkte hin, denen auch der Gesetzesentwurf keine beziehungsweise nur unzureichend Rechnung trägt:

- Eine effektive Datenschutzaufsicht setzt die rechtliche Stärkung der Durchsetzungsbefugnisse der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zwingend voraus. Ihr müssen in ihrem Zuständigkeitsbereich gegenüber den Post- und Telekommunikationsanbietern die gleichen Anordnungs- und Untersagungsbefugnisse eingeräumt werden, wie sie den Aufsichtsbehörden der Länder gegenüber der Privatwirtschaft schon seit Jahren zustehen. Der Bundesbeauftragten ist in diesem Bereich auch die Stellung einer Obersten Bundes- und Bußgeldbehörde einzuräumen. Nur dann stehen auch ihr wirksame Eingriffsbefugnisse, wie sie die Europäische Datenschutzrichtlinie fordert, zur Verfügung.

- Eine unabhängige, funktionsfähige und effektive Datenschutzkontrolle setzt zudem voraus, dass die BfDI als künftige oberste Bundesbehörde mit ausreichenden personellen und sächlichen Mitteln ausgestattet ist, um ihren gesetzlichen Kontroll- und Beratungsaufgaben nachkommen zu können. Entsprechendes gilt für alle Datenschutzbehörden in den Ländern. Ebenso wie in vielen Ländern ist dies für die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit im vorliegenden Entwurf des Bundesdatenschutzgesetzes nicht der Fall.

- Die Genehmigung, als Zeugin auszusagen, wird durch den Gesetzesentwurf in problematischer Weise eingeschränkt. Zwar wird der generelle Genehmigungsvorbehalt des BMI aufgehoben, das Gesetz sieht aber weite Ausnahmen hiervon vor, diese sind zu streichen. Zumindest muss das Letztentscheidungsrecht bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit verbleiben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, der Bundesbeauftragten sowohl effektive Sanktionsmöglichkeiten an die Hand zu geben als auch die nötigen Personalmittel für eine den Aufgaben entsprechende Personalausstattung zur Verfügung zu stellen. Die Konferenz erinnert

auch die Länder daran, dass auch sie ihren Datenschutzaufsichtsbehörden ausreichend Personalmittel zur Verfügung stellen müssen, um die bereits bestehenden Kontrolldefizite zu Lasten der Bürgerinnen und Bürger und deren Grundrechtsschutz abzubauen.

17.1.15 Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 8./9. Oktober 2014 in Hamburg: Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen

Der Europäische Gerichtshof (EuGH) hat mit seinem Urteil vom 13. Mai 2014 - C-131/12 „Google Spain“ einen fundamentalen Beitrag zum Schutz der Persönlichkeitsrechte im Internet geleistet. Die Namenssuche in Suchmaschinen kann erhebliche Auswirkungen auf die Persönlichkeitsrechte haben. Mit Suchmaschinen lassen sich weltweit in Sekundenschnelle detaillierte Profile von Personen erstellen. Oft sind Einträge über eine unbegrenzte Zeit hinweg abrufbar. Sie können dann zu sozialen und wirtschaftlichen Nachteilen für die Betroffenen führen, die ggf. ein Leben lang mit früheren oder vermeintlichen Verfehlungen konfrontiert bleiben. Das Urteil stellt nun klar, dass die Betreiber von Suchmaschinen ein Recht Betroffener auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen umzusetzen haben. Künftig bleiben die Betroffenen daher nicht nur darauf angewiesen, ihre Ansprüche unmittelbar gegenüber den Informationsanbietern zu verfolgen, die häufig nur schwer oder auch gar nicht zu realisieren sind.

Betroffene können sich nun auch direkt an die Suchmaschinenbetreiber wenden und verlangen, dass bei der Suche einzelne Links zu ihrem Namen künftig nicht mehr angezeigt werden.

Das Urteil ordnet dabei allerdings nicht an, bestimmte Inhalte, wie Presseartikel oder Artikel aus der Wikipedia, zu löschen oder ihre Auffindbarkeit im Internet unmöglich zu machen. Vielmehr soll - nach einer erfolgreichen Beschwerde des Betroffenen - der entsprechende Link lediglich bei Eingabe eines bestimmten Personennamens nicht mehr angezeigt werden. Der betroffene Inhalt bleibt mit allen anderen Suchbegriffen weiterhin frei zugänglich (für Inhalte, die regelmäßig durch Eingabe des Namens einer Person in eine Suchmaschine gefunden werden, weil es sich um eine Person des öffentlichen Lebens handelt, hat der EuGH ausdrücklich eine Ausnahme vorgesehen).

Zu Recht wird in der Debatte auf die erhebliche Macht der Anbieter von Suchmaschinen hingewiesen, über die Veröffentlichung von Suchergebnissen zu entscheiden. Diese Macht besteht jedoch nicht erst seit der Entscheidung des EuGH. Tatsächlich haben Inhalteanbieter keinen Rechtsanspruch am Nachweis ihrer Inhalte durch Suchmaschinen. Anbieter von Suchmaschinen sind keine neutralen Sachwalter der Informationsgesell-

schaft, sondern kommerziell handelnde Wirtschaftsunternehmen. Welche Suchergebnisse den Nutzern angezeigt wurden, bestimmt sich damit jedenfalls auch nach den kommerziellen Interessen von Suchmaschinen und ihren Vertragspartnern. Darüber hinaus unterlagen Suchmaschinen auch bereits vor der Entscheidung des EuGH bei der Gestaltung der Suchergebnisse äußeren Beschränkungen (z. B. durch das Urheberrecht). Mit dem Urteil wird klargestellt, dass Suchmaschinen neben diesen Erwägungen jetzt auch die Grundrechte der Betroffenen zu berücksichtigen haben.

Das Urteil konkretisiert die Kriterien, unter welchen sich ausländische Unternehmen an europäisches bzw. nationales Datenschutzrecht halten müssen. Dieses für den Grundrechtsschutz maßgebliche Urteil muss nunmehr von den Suchmaschinenbetreibern umfassend umgesetzt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auf folgende Punkte hin:

- Die effektive Wahrung der Persönlichkeitsrechte des Betroffenen setzt voraus, dass Anbieter von Suchmaschinen die Suchergebnisse bei einem begründeten Widerspruch weltweit unterbinden. Angesichts der territorialen Unbeschränktheit des Internet muss der Schutz des Einzelnen vor einer unberechtigten Verbreitung personenbezogener Daten universell gelten.

- Der verantwortliche Betreiber der Suchmaschine hat regelmäßig die Rechte der Betroffenen gegen die Interessen der Öffentlichkeit an einem freien und umfassenden Informationszugang im Einzelfall abzuwägen. Dabei ist insbesondere auf die Schwere der Persönlichkeitsrechtsbeeinträchtigung, die Stellung des Betroffenen im öffentlichen Leben sowie auf den zeitlichen Ablauf zwischen der Veröffentlichung und dem Antrag des Betroffenen beim Suchmaschinenbetreiber abzustellen.

- Die Entscheidung über die Verbreitung von Suchergebnissen, die Umsetzung von Widersprüchen und die Abwägungsentscheidung mit dem öffentlichen Interesse treffen zunächst die Suchmaschinenbetreiber. Die Kontrolle dieser Entscheidungen obliegt den jeweiligen Aufsichtsbehörden für den Datenschutz oder den staatlichen Gerichten. Alternative Streitbeilegungs- oder Streitschlichtungsverfahren dürfen das verfassungsmäßige Recht der Betroffenen auf eine unabhängige Kontrolle durch die dafür vorgesehenen staatlichen Institutionen nicht beschneiden.

- Eine Befugnis der Anbieter von Suchmaschinen, Inhaltsanbieter routinemäßig über die Sperrung von Suchergebnissen zu informieren, besteht nicht. Dies gilt auch dann, wenn die Benachrichtigung nicht ausdrücklich den Namen des Betroffenen enthält.

17.1.16 Entschließung zwischen der 88. und 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. November 2014: Keine PKW-Maut auf Kosten des Datenschutzes!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) fordert die Bundesregierung auf, bei der geplanten Einführung einer allgemeinen Maut auf Bundesautobahnen und einzelnen Bundesfernstraßen auf eine automatisierte Erhebung, Verarbeitung und Nutzung von Fahrzeugkennzeichen aller Verkehrsteilnehmer über elektronische Kontrollpunkte zu verzichten. Für Abrechnungs- und Kontrollzwecke besteht hierfür kein Erfordernis, denn es stehen - beispielsweise durch Einführung einer physischen Vignette nach dem Vorbild anderer Staaten - mildere und gleichermaßen effektive Mittel zur Kontrolle der Entrichtung der Maut zur Verfügung, ohne täglich an hunderten Kontrollpunkten hunderttausende Kfz-Kennzeichen zu erfassen und zu speichern. Für die Kontrolle in Deutschland zugelassener Pkw ist die (optisch-)elektronische Überwachung schon deswegen nicht erforderlich, weil die Abrechnung über die Zulassungs- und Kfz-Steuerdaten erfolgen soll. Allein die Möglichkeit, sich die Infrastrukturabgabe für gänzlich ungenutzte Pkw erstatten zu lassen, rechtfertigt nicht die vorgesehene elektronische Erfassung und sogar dauerhafte - bis zu 13 Monaten währende - Speicherung von Bewegungsdaten in Deutschland zugelassener Pkw.

Die DSK lehnt die im Entwurf eines Infrastrukturabgabengesetzes geplante Einrichtung eines Zentralen Infrastrukturregisters beim Kraftfahrtbundesamt und einer Datei sämtlicher mautpflichtiger Autobahnnutzungen von Personenkraftwagen beim Bundesamt für Güterverkehr ab. Ebenso weist sie auf die Gefahren der Einbeziehung privater Betreiber in die Erhebung der Infrastrukturabgabe einerseits und eines privaten Dritten in die Überwachung der Infrastrukturabgabe andererseits im Hinblick auf die umfangreichen geplanten Befugnisse der Betreiber bzw. des Dritten zur Datenerhebung und -verarbeitung hin. Die DSK mahnt die Bundesregierung eindringlich zur Einhaltung der verfassungsrechtlich gebotenen Prinzipien der Datenvermeidung und Datensparsamkeit.

17.1.17 Entschließung zwischen der 88. und 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14. November 2014: Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern

Zur Verbesserung der Versorgung von Krebspatienten bauen die Bundesländer derzeit auf bundesgesetzlicher Grundlage ein flächendeckendes Netz von klinischen Krebsregistern auf. Diese Register erhalten hierzu vielfältige Daten über alle krebskranken Personen von allen niedergelassenen Ärzten und Krankenhäusern, die sie behandeln.

Andererseits sollen die Register den behandelnden Ärzten die empfangenen Patientendaten zum Abruf zur Verfügung stellen. Die hierbei übermittelten Daten sind hoch sensibel und können mannigfaltig missbraucht werden. Dem müssen die Maßnahmen zu ihrem Schutz entsprechen.

Mit dieser Entschließung legt die Konferenz einen Katalog von Anforderungen vor und ruft die Bundesländer auf, für deren Erfüllung bei der Ausgestaltung der Kommunikation zwischen medizinischen Leistungserbringern und den klinischen Krebsregistern Sorge zu tragen.

Anlage zur Entschließung „Anforderungen an den Schutz der Datenübermittlungen zwischen medizinischen Leistungserbringern und klinischen Krebsregistern“

Katalog von Anforderungen:

Im Zuge der Umsetzung des Krebsregister- und -früherkennungsgesetzes in den Ländern werden neue Übermittlungswege zwischen verschiedenen medizinischen Leistungserbringern und den klinischen Krebsregistern (KKR) erforderlich. Auf diesen Wegen werden Daten unterschiedlichen Schutzbedarfs transportiert. Der überwiegende Teil von ihnen kann jedoch als hoch sensibel eingeschätzt werden.

Mit dem folgenden Anforderungskatalog sollen Maßnahmen skizziert werden, die einzusetzen sind, um Vertraulichkeit, Authentizität und Integrität der Daten, aber auch die Integrität der eingesetzten Systeme zu gewährleisten. Insgesamt muss ein Schutzniveau erreicht werden, dass dem der Gesundheits-Telematikinfrastruktur gemäß §§ 291a, 291b SGB V entspricht.

Folgende Szenarien können nach den Risiken, die ihnen innewohnen, differenziert werden:

Szenario 1: Die **Meldung** von Daten, die von den klinischen Krebsregistern gemäß § 65 c Abs. 1 Satz 1 Nr. 1 SGB V zu erfassen sind.

Szenario 2: Die **patientenbezogene Rückmeldung** von Auswertungsergebnissen im Sinne von Nr. 3.01 des GKV-Förderkatalog in Hinblick auf die Aufgabe der KKR gemäß § 65c Abs. 1 Satz 1 Nr. 2 SGB V.

Szenario 3: Die **aggregierten Rückmeldungen** an die Leistungserbringer, soweit die übertragenen Daten einen Bezug zu einzelnen behandelnden Personen aufweisen.

Szenario 4: Die **Bereitstellung** von patientenbezogenen Dokumentationsdaten für Zwecke der einrichtungsübergreifenden Behandlung, insbesondere für Tumorkonferenzen im Hinblick auf die Aufgabe der KKR gemäß § 65c Abs. 1 Satz 1 Nr. 4 SGB V.

Im Weiteren wird bei jeder Anforderung auf die Szenarien, auf die sie anwendbar sind, mit ihrer Nummer hingewiesen. Wo erforderlich wird eine zusätzliche Unterscheidung zwischen nachrichtenbasierten Übermittlungsverfahren und webbasierten Dialogverfahren getroffen, worauf durch Zusatz der Buchstaben N bzw. W hingewiesen wird.

Nachrichtenbasierte versus dialogbasierte Übermittlung

1. Vorzugswürdige Form der Übermittlung ist die Lieferung verschlüsselter strukturierter Dateien, wie sie derzeit bei der Meldung der Klinikregister an eine Reihe von epidemiologischen Registern praktiziert wird. Die verschlüsselten Dateien können dabei auch per Web-Upload bzw. -Download übertragen werden.

   Leistungserbringer benötigen für diese Übermittlungsvariante ein Krankenhaus-Informationssystem (KIS) bzw. Praxisverwaltungssystem (PVS), das einen Datenexport in dem vom KKR vorgegebenen Format ermöglicht, oder eine Software zur dezentralen Datenerfassung, die von dem KKR bereitgestellt werden könnte. Die Verschlüsselung bzw. Entschlüsselung und die Signatur der Daten bzw. die Signaturprüfung kann durch separate Software realisiert werden, die kostenfrei erhältlich ist. Investitionen für eine Anpassung von Netzen und Systemen der Leistungserbringer werden in dieser Variante voraussichtlich nur in geringem Maße erforderlich.

   Die Anforderungen an die Transportsicherheit und die Sicherheit der Systeme und Netze, die ausschließlich mit verschlüsselten Daten in Berührung kommen, liegen auf normalem, nicht erhöhtem Niveau. (Szenarien 1N-4N)

2. Eine Übermittlung von Daten zwischen meldenden Leistungserbringern und klinischen Krebsregistern in einem webbasierten Dialogverfahren steht erheblich größeren Schwierigkeiten gegenüber. Für Szenario 1 liegen praktische Erfahrungen aus der epidemiologischen Krebsregistrierung vor, die sich allerdings nur auf eine Erhebung pseudonymisierter Daten beziehen. Von einer Umsetzung für das mit besonders hohen Risiken verbundene Szenario 4 wird dagegen dringend abgeraten.

   Leistungserbringer können bei dieser Variante zwar KIS bzw. PVS verwenden, die nicht für Zwecke der Kommunikation mit den KKR angepasst wurden. Jedes für

den Zugriff auf die Webanwendung des KKR verwendete System des Leistungserbringers muss jedoch besonders gesichert und in einem Netzabschnitt betrieben werden, der gleichzeitig den Sicherheitsansprüchen für die Verarbeitung von klaren Patientendaten und für eine Anbindung an dedizierte medizinische Netze genügt, vgl. hierzu den Beschluss des Düsseldorfer Kreises vom 04./05. Mai 2011 zu Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze. Soweit nicht bereits ein hierfür geeigneter Netzaufbau vorliegt, sind nennenswerte Aufwendungen bei den Leistungserbringern zu tätigen.

Ferner sind hohe (Szenarien 1-2) bis sehr hohe (Szenario 4) Anforderungen an die Sicherheit der auf Seiten des KKR beteiligten Systeme zu ergreifen, die bei der Ausgestaltung des Dialogsystems und bei dessen Anbindung an das Backend zu berücksichtigen sind. Eine nachträgliche Anpassung eines bestehenden Systems, dessen Design nicht von vornherein auf die besonderen Sicherheitsanforderungen dieses Einsatzumfeldes ausgerichtet wurde, erscheint wenig erfolgversprechend. (Szenarien 1W, 2W, 4W)

3. Die Anwendung weiterer Übermittlungsverfahren, deren Anwendung bisher noch nicht in Betracht gezogen wurde, ist möglich. Sie bedürfen jedoch einer eigenen Risikoanalyse.

   Als Beispiel sei eine direkte Übermittlung von Meldedaten aus dem KIS bzw. PVS eines Leistungserbringers an das Register über eine von diesem Register angebotene Webschnittstelle und einen gesicherten Kanal genannt. Auch hier wäre Verschlüsselung und Signatur der Inhaltsdaten geboten. Würde dieses Verfahren auch für den Abruf verwendet, entsprächen die Risiken weitgehend denen des webbasierten Dialogverfahrens. Darüber hinaus wäre der Gewährleistung der Integrität des abrufenden Systems besondere Aufmerksamkeit zu widmen.

Vertrauensdienste, kryptografische Algorithmen und Verfahren

4. Die verwendeten kryptografischen Algorithmen und Verfahren müssen eine langfristige Sicherheit gewähren und dem Katalog BSI -TR 03116-1 entnommen sein. (Szenarien 1-4)

5. Für die Identifizierung der Teilnehmer des Verfahren, die zu verwendenden Authentisierungsmittel, deren Ausgabe, Anwendung und Rückruf, sowie die Schlüsselspeicherung sind mindestens die Anforderungen des Schutzniveaus hoch+ gemäß Abschnitten 3 und 4 der BSI-TR 03107-1 zu erfüllen. (Szenarien 1-4)

6. (optional) Für Übermittlung, Authentisierung und Verschlüsselung sollen Verfahren der Telematikinfrastruktur nach § 291b SGB V verwendet werden, sobald diese verfügbar sind. (Szenarien 1-4)

7. Die Wurzel der zur Zertifizierung von Teilnehmer- und KKR-Schlüsseln verwendeten PKI ist allen Beteiligten integritätsgeschützt zur Verfügung zu stellen. Die Revokation von öffentlichen Schlüsseln bei Kompromittierung der zugeordneten privaten Schlüssel muss unverzüglich in einem im Vorhinein festgelegten Zeitrahmen erfolgen. (Szenarien 1-4)

Maßnahmen zum Vertraulichkeitsschutz während des Transports der Daten

8. Bei jeder Übermittlung ist eine Ende-zu-Ende-Verschlüsslung einzusetzen. (Szenarien 1-4)

9. Bei Übermittlungen an KKR sind Schlüssel einzusetzen, deren Authentizität die sendende Stelle zweifelsfrei feststellen kann. (Szenario 1)

10. Bei Übermittlungen an Leistungserbringer sind zertifizierte personen- oder leistungserbringerspezifische Schlüssel einzusetzen. (Szenarien 2-4)

11. Übermittlungen zu und von den klinischen Krebsregistern sollen über besonders geschützte medizinische Netze abgewickelt werden, bei webbasierten Verfahren ist dies zwingend erforderlich. (Szenarien 1-4)

12. Die erfolgreiche Authentisierung des KKR muss für die meldenden bzw. abrufenden Personen klar erkennbar sein. (Szenarien 1W-4W)

13. Es dürfen ausschließlich behandelnde Ärztinnen und Ärzte sowie Personen, die bei ihnen oder in einem behandelnden Krankenhaus als berufsmäßige Gehilfen tätig sind, personenbezogene Abrufe tätigen. (Szenarien 2+4)

14. Im Zuge eines Datenabrufs müssen sich die abrufenden Personen in analoger Anwendung der Regelungen des § 291a Abs. 3 Satz 1 Nr. 4 SGB V zum Zugriff auf Daten mit einer Zwei-Faktor-Lösung authentifizieren. Der elektronische Heilberufeausweis ist hierfür geeignet. (Szenarien 2W+4W)

15. Die Registrierung der Leistungserbringer muss durch die KKR selbst oder durch Stellen vorgenommen werden, die von den Ländern in analoger Anwendung von § 291a Abs. 5c SGB V bestimmt wurden. (Szenarien 2-4)

16. Das System, das zur Bereitstellung der Daten für die Rückmeldung von Auswertungsergebnissen an die Leistungserbringer verwendet wird, muss sicherstellen, dass Rückmeldungen mit Daten eines Patienten oder einer Patientin nur für solche Leistungserbringer bereitgestellt werden, die bezüglich dieses Patienten bzw. dieser Patientin eine Meldung abgegeben haben, und nur dann, wenn kein Widerspruch der Betroffenen vorliegt. (Szenario 2)

17. Aggregierte Auswertungsergebnisse, die sich auf einzelne behandelnde Personen beziehen, dürfen nur an diese selbst bzw. an die Stellen übermittelt werden, bei denen sie tätig sind. (Szenario 3)

18. Abrufe von Daten müssen auf der Grundlage eines Berechtigungskonzeptes autorisiert werden, mit dem sichergestellt wird, dass nur an der Behandlung der jeweiligen betroffenen Person beteiligte Leistungserbringer Zugang zu den Daten über diese Person erhalten. Das Bestehen des Abrufrechts ist auf die Dauer der Behandlung zu beschränken. Soweit landesrechtlich vorgesehen muss das Berechtigungskonzept vorsehen, dass Willenserklärungen der Betroffenen, die auf die Einschränkung der Offenbarung ihrer Daten gerichtet sind, effektiv berücksichtigt werden können. (Szenario 4)

Maßnahmen zum Vertraulichkeitsschutz gespeicherter Daten und zur Gewährleistung der Integrität der beteiligten IT-Systeme

19. Ambulante Leistungserbringer müssen die „Empfehlungen zu Datenschutz und Datensicherheit in der Arztpraxis“ der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung beachten. Hierauf ist bei der Registrierung hinzuweisen. (Szenarien 1-4)

20. Die Verschlüsselung der zu meldenden und die Entschlüsselung der von einem klinischen Krebsregister abgerufenen Daten darf nur auf Geräten erfolgen, die zur allgemeinen Verarbeitung von Patientendaten der Leistungserbringer vorgesehen sind. (Szenarien 1-4)

21. Hierzu gehört, dass von den zu Meldung oder Abruf genutzten Geräte dann kein allgemeiner Zugang zu Diensten des Internets möglich sein darf, wenn unverschlüsselte Patientendaten auf ihnen zur Anzeige gebracht oder gespeichert werden. (Szenarien 1-4)

22. Bei den KKR sind für die Server, welche zur Abwicklung der Übermittlungen eingesetzt werden, Informationssicherheitsmaßnahmen zu treffen, die bei ausschließlicher Verarbeitung verschlüsselter Daten dem normalen, sonst dem besonders ho-

hen Schutzbedarf der zu übermittelnden Daten gerecht werden. Dies schließt die Maßnahmen nach den Grundschutzbausteinen des Bundesamtes für Sicherheit in der Informationstechnik, insbesondere nach Baustein B 5.21 der Grundschutzkataloge, und die in der ISi-Reihe empfohlenen Maßnahmen ein. (Szenarien 1-4)

23. Bei Dialogverfahren sind die dort aufgeführten Maßnahmen jedoch nicht notwendig ausreichend. Es wird eine besonders eingehende Risikoanalyse erforderlich, die sich auf alle beteiligten Systeme erstrecken und alle bekannten Angriffsvektoren, die gegenwärtig hohe Angriffsintensität auf Webanwendungen sowie darüber hinaus aufgrund einschlägiger Erfahrung der Vergangenheit die Kompromittierung einzelner Sicherheitsvorkehrungen berücksichtigen muss (defense in depth). (Szenarien 1W-4W)

24. Die Sicherung hat alle OSI-Netzebenen einschließlich der Anwendungsebene zu berücksichtigen. Nur im Vorhinein autorisierten Systemen ist der Aufbau einer Verbindung zu ermöglichen. Diese Beschränkung muss kryptografisch durchgesetzt werden; eine Beschränkung auf Basis von IP-Adressen reicht nicht aus. Die Absicherung mittels TLS allein bietet aufgrund der Häufigkeit und Schwere der in der vergangenen Zeit aufgetretenen Schwachstellen keine ausreichenden Garantien für die Sicherheit des Zugriffs. (Szenarien 1W-4W)

25. Die Integrität der Komponenten für die Bereitstellung eines Webdienstes (Webserver, Anwendungsserver, Datenbank) bedürfen besonderen Integritätsschutzes. Eine direkte Anbindung an das Datenhaltungssystem des Registers in der inneren Sicherheitszone ist nicht zulässig. Die Datenhaltung des Backends der Webanwendung ist nur verschlüsselt zulässig. (Szenarien 1W-4W)

26. Kryptografische Schlüssel, deren Kenntnis für den Zugriff auf den Datenbestand erforderlich ist, sind in dedizierten Systemen hardwareseitig zu kapseln und ihre Nutzung durch ein Intrusion Prevention System zu überwachen. Ungewöhnliche Nutzungsmuster müssen zu einer Unterbrechung der Nutzungsmöglichkeiten und einer Untersuchung des Sicherheitsstatus des Verfahrens führen. Kryptografische Schlüssel, die in der inneren Sicherheitszone des Registers verwendet werden, dürfen innerhalb der Webanwendung nicht genutzt werden. (Szenario 4W)

Maßnahmen zur Gewährleistung der Authentizität der Daten

27. Da die übermittelten Daten einer folgenden Behandlung zugrunde gelegt werden können, ist es erforderlich, die Integrität der Daten während ihrer Übermittlung zu

schützen und sicherzustellen, dass die Daten stets ihrem Ursprung zuzuordnen sind. (Szenarien 1+4)

28. Nachrichten der Leistungserbringer mit Krebsregisterdaten sind entweder mit einer personenbezogenen mindestens fortgeschrittenen elektronischen Signatur oder leistungserbringerbezogen mit einem mindestens fortgeschrittenen elektronischen Siegel i. S. v. Artikel 3 Nr. 26 der EU-Verordnung 910/14 zu authentisieren. (Szenarien 1+4)

Maßnahmen zur Transparenz und Datenschutzkontrolle

29. Abrufe sind leistungserbringer- und personenbezogen zu protokollieren. Die Protokolle sind mindestens ein Jahr zu speichern. Sie müssen gegen Veränderung geschützt werden. (Szenarien 2-4)

30. Für die Protokolle ist ein Verfahren zur anlassbezogenen Auswertung vorzuhalten. (Szenarien 2-4)

31. Der Inhalt der Protokolldaten ist bezogen auf Abrufe von Daten einer Patientin oder eines Patienten auf deren Antrag zu beauskunften. (Szenario 4)

Um einen datenschutzgerechten Betrieb der Verfahren der klinischen Krebsregister für die Kommunikation mit den Leistungserbringern zu gewährleisten, wird den verantwortlichen Stellen der Länder empfohlen, die vorgenannten Anforderungen bereits bei der Ausschreibung von Leistungen zur Bereitstellung der von den KKR benötigten Informationstechnik zu berücksichtigen.

17.1.18 Entschließung zwischen der 88. und 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. Dezember 2014: Schluss mit den datenschutzrechtlichen Missständen beim Umgang mit Krankengeldbeziehern!

Bei dem derzeit praktizierten „Krankengeldfallmanagement“ lädt eine Vielzahl von Krankenkassen ihre Versicherten in der vierten Woche einer Arbeitsunfähigkeit zu einem persönlichen Gespräch ein. Die Krankenkassen stellen Fragen zur Arbeitsplatz-, Krankheits-, familiären und sozialen Situation des Versicherten. Außerdem sollen die Ärzte der Versicherten häufig medizinische Fragen beantworten sowie Arzt-, Krankenhaus- oder Rehaentlassberichte an die Krankenkasse schicken. Vielfach werden Versicherte, die im Krankengeldbezug stehen, - zum Teil mehrfach wöchentlich - von Krankenkassenmitarbeitern oder in deren Auftrag von Dritten angerufen, um sich nach dem Fortschritt der Genesung zu erkundigen.

Zudem werden nach den Prüferfahrungen der Datenschutzbeauftragten des Bundes und einiger Länder Versicherte beim „Krankengeldfallmanagement“ von ihrer Krankenkasse oftmals unter Druck gesetzt. Auch der Patientenbeauftragte der Bundesregierung sowie die Unabhängige Patientenberatung Deutschland (UPD) haben an dieser Praxis starke Kritik geübt.

Die Krankenkassen sind zur Beurteilung sensibler medizinischer Daten aufgrund der bisherigen gesetzgeberischen Grundentscheidung auf ein Tätigwerden des Medizinischen Dienstes der Krankenversicherung (MDK) angewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist die Bundesregierung darauf hin, dass es nicht nachvollziehbar ist, dass mit dem Entwurf eines Gesetzes zur Stärkung der Versorgung in der gesetzlichen Krankenversicherung (GKV-Versorgungsstärkungsgesetz - GKV-VSG) das bisherige datenschutzrechtlich problematische Vorgehen von vielen Krankenkassen beim sog. Krankengeldfallmanagement nunmehr legitimiert werden soll. Zukünftig sollen danach die Versicherten bei einem (absehbaren) Krankengeldbezug „Anspruch auf eine umfassende Prüfung, individuelle Beratung und Hilfestellung, welche Leistungen und unterstützende Angebote zur Wiederherstellung der Arbeitsfähigkeit erforderlich sind“ gegenüber ihrer gesetzlichen Krankenkasse haben. Die Krankenkasse soll dabei die erforderlichen personenbezogenen Daten mit Einwilligung des Versicherten erheben, verarbeiten und nutzen dürfen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, von dieser Regelung Abstand zu nehmen. Vielmehr sind die derzeit bestehenden gesetzlichen Regelungen konsequent umzusetzen.

17.1.19 Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19. März 2015 in Wiesbaden: Datenschutz nach „Charlie Hebdo“: Rechtsstaat und Grundrechte beweisen sich gerade in Zeiten terroristischer Bedrohung!

Terrorismus und internationale Kriminalität erfordern effektive Abwehrmaßnahmen auch in freiheitlichen Verfassungsstaaten. Für etwaige Defizite kann der Datenschutz nicht verantwortlich gemacht werden. Eine Zielrichtung terroristischer Angriffe ist es, Furcht und Hass in der Gesellschaft zu verbreiten und demokratische Freiheitsrechte zu beseitigen. Die Verteidigung und Bewahrung der verfassungsmäßigen Freiheitsrechte sind zentrale Grundbedingungen zur Abwehr der vom Terrorismus ausgehenden Gefahren.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt ihren nach den Terror-Anschlägen vom 11. September 2001 formulierten Appell, dass alle neu erwogenen Maßnahmen sich daran messen lassen müssen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus wirklich zielführend und erforderlich sind und ob sie den Verfassungsgrundsatz der Verhältnismäßigkeit einhalten. Weder die Vorratsdatenspeicherung noch die pauschale Übermittlung von Flugpassagierdaten erfüllen diese Voraussetzungen. Einseitiges Streben nach einer umfassenden Sicherheit darf nicht den bisherigen gesellschaftlichen Konsens über die wertsetzende Bedeutung bürgerlicher Freiheits- und Persönlichkeitsrechte überlagern. Es darf in unserem Land zu keiner Verschiebung zugunsten staatlicher Überwachung und zu Lasten freier und unbeobachteter Aktion, Bewegung und Kommunikation der Bürgerinnen und Bürger kommen. Der Datenschutz ist nicht ein Hindernis für Abwehrmaßnahmen, sondern selbst ein identitätsstiftendes Merkmal des Verfassungsstaates oder - mit den Worten des Bundesverfassungsgerichts - „elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens“. Ließe man jeden Eingriff in die informationelle Selbstbestimmung zu, hätten die Terroristen eines ihrer Ziele erreicht.

17.1.20 Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19 März 2015 in Wiesbaden: Datenschutzgrundverordnung darf keine Mogelpackung werden!

Der Rat der Europäischen Innen- und Justizminister hat sich am 12. und 13. März 2015 erneut mit der Reform des Europäischen Datenschutzrechts befasst und dabei über drei weitere Kapitel der geplanten Datenschutz-Grundverordnung (DSGVO) grundsätzlich geeinigt. Hierzu gehören u. a. die zentralen Vorschriften über die Datenschutzgrundsätze und die Zulässigkeit der Verarbeitung personenbezogener Daten.

Die Datenschutzbeauftragten des Bundes und der Länder warnen eindringlich vor einer Aushöhlung des Datenschutzes in Europa durch eine Abkehr von den tragenden grundrechtlich vorgegebenen Datenschutzgrundsätzen. Die vom Rat nunmehr vorgeschlagene Fassung des Kapitels II der DSGVO hebelt zentrale Datenschutzgrundsätze aus:

- Der Rat verabschiedet sich mit seiner Einigung vom Grundsatz der Datensparsamkeit. Damit wird ein tragender Grundsatz des Rechts auf informationelle Selbstbestimmung aufgegeben, der die Datenverarbeitung auf das unbedingt notwendige Maß reduziert und einen Anreiz für datenschutzfreundliche Technologien darstellt.

- Nach den Vorstellungen des Rates sollen einerseits personenbezogene Daten ohne jede weitere Rechtsgrundlage zu anderen Zwecken als dem ursprünglichen Erhebungs-

zweck verarbeitet werden dürfen, wenn der neue Zweck mit dem ursprünglichen Zweck noch vereinbar ist. Zweckänderungen sollen andererseits schon dann erlaubt sein, wenn der Datenverarbeiter hieran ein überwiegendes berechtigtes Interesse hat. Durch das Zusammenspiel dieser beiden Möglichkeiten und die ausdrücklich gewünschte Privilegierung der Datenverarbeitung zu Direktmarketingzwecken werden Zweckänderungen in einem derart weiten Umfang zulässig, dass das für den Datenschutz elementare Prinzip der Zweckbindung preisgegeben wird. Dies würde die Entscheidungsfreiheit und die Transparenz für den Einzelnen in problematischer Weise einschränken.

- Ferner wird in den Vorschlägen des Rates das Instrument der Einwilligung entwertet. In der Vergangenheit hat sich gezeigt, dass das bloße Unterlassen des Erhebens von Widersprüchen gegenüber der Datenverarbeitung (opt-out) eben nicht mit einer expliziten Willensbekundung (opt-in) gleichzusetzen ist. Der Vorschlag des Rates, „ausdrücklich“ zu streichen und durch den minder klaren Begriff „eindeutig“ zu ersetzen, ermöglicht es gerade den global agierenden Diensteanbietern, durch Verwendung pauschaler Datenschutzbestimmungen weitreichende Datenverarbeitungsbefugnisse ohne eine ausdrückliche Einwilligung des Nutzers für sich zu reklamieren. Mit diesem Vorschlag wird das informationelle Selbstbestimmungsrecht der Nutzer wesentlich geschwächt.

- Schließlich will der Rat die Verarbeitung personenbezogener Daten zu Forschungszwecken derart weitgehend privilegieren, dass ein angemessener Ausgleich mit dem Recht auf informationelle Selbstbestimmung der Betroffenen kaum noch möglich ist.

Mit diesen Vorschlägen fällt der Rat nicht nur hinter die Entwürfe der Europäischen Kommission und des Europäischen Parlaments zurück. Er ebnet dadurch den Weg zu einer Verschlechterung des derzeitigen Datenschutzniveaus, obwohl die Verbesserung des Datenschutzes eines der erklärten politischen Ziele der Reform ist.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an Bund und Länder, den Rat, das Europäische Parlament und die Europäische Kommission, sich in den im zweiten Halbjahr 2015 anstehenden Trilogverhandlungen für eine Verbesserung des Datenschutzniveaus einzusetzen und eine Aushöhlung zentraler Datenschutzgrundsätze zu verhindern.

17.1.21 Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19. März 2015 in Wiesbaden: Verschlüsselung ohne Einschränkungen ermöglichen

Zur Stärkung des Brief-, Post- und Fernmeldegeheimnisses und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie im Interesse der ungestörten Kommunikation in Wirtschaft und Verwaltung sind neben entsprechenden gesetzlichen Regelungen und deren Umsetzung wirksame technische Vorkehrungen erforderlich, um elektronisch übermittelte und gespeicherte Daten vor Zugriffen Unberechtigter zu schützen. Schutzbedürftig sind neben der Kommunikation von Privatpersonen auch die geschäftliche Kommunikation von Wirtschaftsunternehmen, die Kommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte, Anwälte, Psychologen, Steuerberater), und die Kommunikation mit und innerhalb der öffentlichen Verwaltung.

Mit modernen kryptographischen Verfahren zur Verschlüsselung von Daten stehen datenschutzfreundliche Technologien zur Verfügung, die prinzipiell von jedermann genutzt werden können. Einer umfassenden und leicht nutzbaren Verschlüsselung stehen jedoch noch technische und organisatorische Hürden entgegen. Dies führt dazu, dass diese Schutzmaßnahmen bisher viel zu selten genutzt werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher,

- eine einfach bedienbare Verschlüsselungs-Infrastruktur und insbesondere eine sichere Ende-zu-Ende-Verschlüsselung ohne Eingriffsmöglichkeiten Dritter bereitzustellen,
- die Entwicklung sicherer, transparenter und einfach bedienbarer kryptographischer Verfahren ohne Hintertüren auf allen, insbesondere auch mobilen Plattformen zu fördern,
- die Wirtschaft bei der Wahrung der Vertraulichkeit und Integrität ihrer geschäftlichen Kommunikation zu unterstützen und
- kryptographische Technologien in E-Government-Verfahren standardmäßig zu implementieren.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert einen aktiven Einsatz der Politik bei der Gestaltung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die Bundesregierung hat in ihren eigenen Zielstellungen aus der Digitalen Agenda 2014-2017 deutlich gemacht, wie wichtig eine zuverlässige und sichere Verschlüsselung

ist.[1] Die Pläne der De-Mail-Anbieter für eine Ende-zu-Ende-Verschlüsselung ab April 2015 sind zwar ein erster Schritt in die richtige Richtung. Dennoch wird im Zusammenhang mit der Bekämpfung des internationalen Terrorismus in letzter Zeit erneut über eine Schwächung von Verschlüsselungstechnologien diskutiert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt Forderungen ab, den Einsatz kryptographischer Verfahren durch staatliche Regulierungen zu unterbinden oder zumindest einzuschränken. Solche Regulierungen könnten leicht umgangen werden, wären kaum kontrollierbar, würden Grundrechte einschränken, den Schutz von Berufs- und Geschäftsgeheimnissen gefährden und Schwachstellen schaffen, die auch von Kriminellen ausgenutzt werden können. Im Ergebnis wäre dann der erhoffte Nutzen bei der Bekämpfung des internationalen Terrorismus äußerst fraglich.

17.1.22 Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19. März 2015 in Wiesbaden: IT-Sicherheitsgesetz nicht ohne Datenschutz!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht Informationssicherheit als eine Grundvoraussetzung an, um die Grundrechte auf informationelle Selbstbestimmung sowie auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme und das Telekommunikationsgeheimnis zu wahren.

Der von der Bundesregierung eingebrachte Gesetzentwurf für ein IT-Sicherheitsgesetz (BT-Drs. 18/4096 v. 25.02.2015) soll dazu beitragen, die Sicherheit informationstechnischer Systeme bei kritischen Infrastrukturen zu verbessern. Der Ausbau des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) zu einer nationalen Zentrale für Informationssicherheit, die Festlegung von Sicherheitsstandards, die Pflicht zur Sicherheitsvorsorge in Unternehmen sowie die Melde- und Benachrichtigungspflichten bei sicherheitsrelevanten Vorfällen sollen dabei wichtige Bausteine einer nationalen Strategie für mehr Informationssicherheit sein.

Datenschutz und Informationssicherheit haben weitreichende Schnittmengen, nehmen in einzelnen Bereichen jedoch unterschiedliche Gewichtungen vor. Bei einer Gesamtabwägung darf es nicht zu einer Unterordnung oder gar Missachtung der grundrechtlich verankerten Bestimmungen des Datenschutzrechts kommen. Auch um das Vertrauen der Bevölkerung in die Gesetzgebung zur IT-Sicherheit zu stärken, muss ein beiden Seiten gerecht werdender Abwägungs- und Abstimmungsprozess deutlich zum Ausdruck

[1] Zitat: „Wir unterstützen mehr und bessere Verschlüsselung. Wir wollen Verschlüsselungsstandort Nr. 1 in der Welt werden. Dazu soll die Verschlüsselung von privater Kommunikation in der Breite zum Standard werden."

kommen. Dies gilt sowohl bei der Festlegung von Sicherheitsstandards, als auch bei der Beurteilung von Einzelfällen.

Wenn Maßnahmen zur Erhöhung der Informationssicherheit ergriffen werden, geht damit in vielen Fällen auch eine Verarbeitung personenbezogener Daten einher. Die damit verbundenen Eingriffe in das Recht auf informationelle Selbstbestimmung sowie in das Telekommunikationsgeheimnis müssen gesetzlich auf das unabdingbar Erforderliche beschränkt werden. Es muss im Gesetz klar geregelt sein, welche personenbezogenen Daten im Rahmen der IT-Sicherheitsmaßnahmen von wem für welche Zwecke erhoben, verarbeitet und gespeichert werden dürfen. Diesen Anforderungen genügt der vorliegende Entwurf nicht. So fehlen Regelungen, die verpflichteten Unternehmen Klarheit über die Notwendigkeit und Zulässigkeit bestimmter Angriffspräventions- und -erkennungssysteme geben. Regeln zur Zweckbindung erhobener Daten sind nur für das BSI vorgesehen. Vorgaben zur Datensparsamkeit etwa durch Anonymisierung, Pseudonymisierung, frühzeitiges Löschen und Abschotten sind bei den vorgesehenen Maßnahmen zur Verbesserung der Informationssicherheit bisher nicht geplant.

Die Informationssicherheit darf nicht allein den Behörden im Direktionsbereich des Bundesministeriums des Innern überlassen bleiben, die bei einer Abwägung zwischen Informationssicherheit einerseits und klassischer Gefahrenabwehr und Strafverfolgung andererseits Interessenkonflikten ausgesetzt sein könnten. Die Beteiligung unabhängiger Datenschutzbehörden ist daher gefordert.

Neben der Zuständigkeit des BSI für die Informationssicherheit muss im Gesetzentwurf auch die Zuständigkeit der Datenschutzaufsichtsbehörden für Fragen der Geeignetheit und Angemessenheit der vom Datenschutzrecht geforderten technisch-organisatorischen Maßnahmen mit in den Blick genommen werden. Insofern sind die Datenschutzaufsichtsbehörden auch an der Festlegung von Informationssicherheitsstandards beteiligt und müssen daher in die Meldewege eingebunden und bei der Beratung der Beteiligten im Sinne des o. g. Abwägungsprozesses zwischen Informationssicherheits- und Datenschutzmaßnahmen beteiligt werden. Zudem kann mit der Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle an das BSI eine datenschutzrechtliche Meldeplicht von Datenpannen verbunden sein, woraus auch eine rechtliche Einbindung der Datenschutzaufsichtsbehörden in die Meldewege resultiert. Dies setzt unabhängige und leistungsfähige Datenschutzaufsichtsbehörden und deren entsprechende Ausstattung voraus.

Die Bestrebungen nach mehr IT-Sicherheit dürfen sich nicht allein auf die Verabschiedung eines IT-Sicherheitsgesetzes beschränken. Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme enthält einen objektiven Auftrag an den Staat, für vertrauenswürdige und sichere IT-Infrastrukturen zu sorgen.

Dabei kommt der Weiterentwicklung und Implementierung von Verfahren eine zentrale Funktion zu, die gleichzeitig eine starke Verschlüsselung und eine effektive Erkennung von Sicherheitsvorfällen ermöglichen.

17.1.23 Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19. März 2015 in Wiesbaden: Mindestlohngesetz und Datenschutz

Die Umsetzung des Mindestlohngesetzes wirft eine Reihe von datenschutzrechtlichen Problemen auf, die einer Klärung bedürfen.

Unter anderem haftet ein Unternehmen dafür, wenn ein Subunternehmer - und ggf. auch dessen Subunternehmer - den Beschäftigten nicht den Mindestlohn zahlt; außerdem kann ein hohes Bußgeld verhängt werden, wenn der Auftraggeber weiß oder fahrlässig nicht weiß, dass Auftragnehmer den Mindestlohn nicht zahlen. Da das Mindestlohngesetz nicht bestimmt, wie die Überprüfung durch den Auftraggeber konkret zu erfolgen hat, sichern sich - wie Industrie- und Handelskammern berichten - zahlreiche Unternehmen vertraglich durch umfangreiche Vorlagepflichten und Einsichtsrechte in Bezug auf personenbezogene Beschäftigtendaten beim Subunternehmer (z. B. Lohnlisten, Verdienstbescheinigungen usw.) ab. Dies ist in Anbetracht der schutzwürdigen Interessen der Beschäftigten weder datenschutzrechtlich gerechtfertigt noch im Hinblick auf die soziale Zielrichtung des Mindestlohngesetzes erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, bei der in Aussicht genommenen Überprüfung des Mindestlohngesetzes stärker auf die Belange des Datenschutzes zu achten. Auch im Interesse einer unbürokratischen Lösung sollte der Gesetzgeber klarstellen, dass eine schriftliche Erklärung des Auftragnehmers ausreicht, um die Voraussetzungen des Mindestlohngesetzes einzuhalten. Dies kann eventuell durch Vertragsstrafenregelungen, Übernahme des Haftungsrisikos durch Bankbürgschaften sowie vertragliche Zustimmungsvorbehalte für den Fall der Beauftragung weiterer Subunternehmer durch den Auftragnehmer abgesichert werden. Aus Datenschutzsicht sind allenfalls stichprobenartige Kontrollen von geschwärzten Verdienstbescheinigungen hinnehmbar. Bei einer Novellierung des Gesetzes, sollte der Gesetzgeber darüber hinaus klarstellen, dass Zugriffe des Auftraggebers auf personenbezogene Beschäftigtendaten des Auftragnehmers unzulässig sind.

17.1.24 Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19. März 2015 in Wiesbaden: Nachbesserungen beim eHealth-Gesetz und klare Regelungen zum Einsatz externer Dienstleister bei Berufsgeheimnisträgern erforderlich

Mit dem Entwurf eines Gesetzes für sichere und digitale Kommunikation und Anwendungen im Gesundheitswesen („eHealth-Gesetz“) würde die Bundesregierung die Gelegenheit verpassen, die zunehmende IT-Nutzung im Gesundheitswesen datenschutzgerecht auszugestalten und insbesondere die Anforderungen an die Vertraulichkeit und Transparenz der Datenverarbeitung zu regeln.

Aus diesem Grund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber insbesondere zu folgenden Ergänzungen des Gesetzentwurfs auf:

1. Der Gesetzentwurf hat zum Ziel, die elektronische Gesundheitskarte einschließlich der Telematikinfrastruktur als zentrale Kommunikationsplattform im Gesundheitsbereich zu etablieren. So soll der Einsatz freiwilliger Anwendungen, in denen Patientendaten verarbeitet werden, forciert werden. Es muss allerdings bei dem Grundsatz bleiben, dass die Betroffenen über die Speicherung von Diagnosen und anderen medizinischen Daten auf der Gesundheitskarte selbst entscheiden können. Zur Wahrung der Transparenz ist das den Betroffenen eingeräumte Zugriffsrecht auf ihre Daten von besonderer Bedeutung. Ihnen wird damit auch die Wahrnehmung ihrer Rechte, insbesondere auf Auskunft und Löschung, ermöglicht. Entgegen der Gesetzeslage und entsprechender Ankündigungen ist eine Erprobung des Patientenzugriffs bislang unterblieben. Es ist daher sicherzustellen, dass die Versicherten ihre gesetzlich zugestandenen Rechte auch wahrnehmen können. Für den Fall, dass die notwendigen Funktionalitäten nicht zeitgerecht zur Verfügung stehen, sollte der Gesetzgeber angemessene Sanktionen festlegen.

2. Nach dem Gesetzentwurf richtet die Gesellschaft für Telematik zukünftig ein öffentlich über das Internet verfügbares Interoperabilitätsverzeichnis „für technische und semantische Standards, Profile und Leitfäden für informationstechnische Systeme im Gesundheitswesen“ ein. Sie wird dabei von Experten insbesondere aus dem IT-Bereich beraten. Zur Sicherung des hohen Schutzniveaus von Gesundheitsdaten sind auch Datenschutzexperten hinzuzuziehen.

3. Der Bundesgesetzgeber muss klare Rahmenbedingungen für die Einschaltung externer Dienstleister durch Berufsgeheimnisträger schaffen und den Vertraulichkeitsschutz bei den Dienstleistern sicherstellen. Die Einschaltung von externen Dienst-

leistern ist für Berufsgeheimnisträger oft ohne Alternative, wenn sie - wie auch vom Gesetzgeber beispielsweise mit dem eHealth-Gesetz gewünscht - moderne Informationstechnik nutzen wollen. Jedoch ist damit regelmäßig die Gefahr eines Verstoßes gegen die Schweigepflicht verbunden.

Vor diesem Hintergrund muss der Gesetzgeber Rechtssicherheit schaffen, unter welchen Voraussetzungen Berufsgeheimnisträger externe Dienstleister einschalten dürfen. Die notwendige rechtliche Regelung muss (z. B. in § 203 StGB) gewährleisten, dass die Kenntnisnahme von Berufsgeheimnissen auf das unbedingt Erforderliche beschränkt wird, die Dienstleister einer Schweigepflicht unterworfen und die Patientendaten auch bei ihnen durch ein Beschlagnahmeverbot abgesichert werden. Zudem muss durch Weisungsrechte der Berufsgeheimnisträger deren Verantwortlichkeit für die Berufsgeheimnisse gewahrt bleiben. Über technische und organisatorische Maßnahmen und über das Herstellen von Transparenz ist das für sensible Daten erforderliche Schutzniveau herzustellen.

17.1.25 Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19. März 2015 in Wiesbaden: Big Data zur Gefahrenabwehr und Strafverfolgung: Risiken und Nebenwirkungen beachten

Zunehmend sind Systeme zur Datenanalyse auch für Polizeibehörden am Markt verfügbar. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist daher frühzeitig - bevor diese Systeme in der Fläche beschafft werden - darauf hin, dass der Einsatz solcher Systeme durch die Polizei geeignet ist, elementare Grundsätze des Datenschutzes und des Rechts auf informationelle Selbstbestimmung in Frage zu stellen. Solche Verfahren können enorme Mengen von heterogenen - strukturierten wie unstrukturierten - Daten mit hoher Geschwindigkeit auswerten. Sogenannte selbst lernende Algorithmen sind in der Lage, die Kriterien für die Auswertung selbst zu entwickeln und an neue Erkenntnisse anzupassen. Damit sollen Zusammenhänge zwischen Straftaten erkannt werden und Vorhersagen über künftige Straftaten oder Gefahren bereits im Vorfeld getroffen werden („Predictive Policing“).

Dies kann zu einer weiteren Verschiebung der polizeilichen Eingriffsschwelle in das Vorfeld von Gefahren und Straftaten führen. Die Gefahr fehlerhafter Prognosen ist der Vorfeldanalyse stets immanent - mit erheblichen Auswirkungen auf die dabei in Verdacht geratenen Personen.

Besonders kritisch ist es, wenn Analysesysteme vermeintlich harmlose, allgemein zugängliche Daten aus dem Internet auswerten, etwa aus Foren oder sozialen Netzwerken.

Diese können zudem mit polizeilichen Speicherungen verknüpft und einer konkreten Person zugeordnet werden. Es besteht das Risiko, dass die Systeme die Daten aus einem ganz anderen Zusammenhang verwenden, denen kein gefährdendes oder strafbares Verhalten zu Grunde liegt. Dann können Bürgerinnen und Bürger nicht mehr sicher sein, welche ihrer Handlungen von der Polizei registriert und nach welchen Kriterien bewertet werden - zumal diese stets nur auf statistischen Erfahrungswerten beruhen, die im Einzelfall nicht zutreffen müssen. Sind die Kriterien und die Funktionsweise der Auswertealgorithmen nicht bekannt, ist es den Betroffenen unmöglich, das Ergebnis mit eigenen Angaben zu widerlegen.

Auch wenn die derzeit in der Praxis bei einzelnen Länderpolizeien eingesetzten Verfahren, mit denen relevante polizeiliche Daten ausschließlich ortsbezogen und nicht personenbezogen ausgewertet werden, nicht die beschriebenen Risiken hervorrufen, kann die Bewertung bei nur geringfügigen Änderungen eine ganz andere sein. Die ständig weiterentwickelten technischen Auswertemöglichkeiten bergen schon heute das Potential dafür, dass Bürgerinnen und Bürger die Kontrolle über ihre Daten - in einem Umfang und auf eine Art und Weise - verlieren könnten, die in der Vergangenheit nicht vorstellbar gewesen ist.

Die derzeitigen gesetzlichen Vorschriften in Bund und Ländern enthalten - mit Ausnahme der Regelungen zur Rasterfahndung - keine ausdrücklichen Vorgaben für den Einsatz weit gefasster Analysesysteme. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist angesichts der beschriebenen Gefahren darauf hin, dass der Einsatz solcher Systeme durch die Polizei nur in engen Grenzen als verfassungsrechtlich zulässig zu betrachten ist.

17.1.26 Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19. März 2015 in Wiesbaden: Safe Harbor bietet keinen ausreichenden Schutz für den Datentransfer in die USA

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Safe Harbor-Entscheidung der Europäischen Kommission aus dem Jahr 2000 keinen ausreichenden Schutz für das Grundrecht auf Datenschutz bei der Übermittlung personenbezogener Daten in die USA entfaltet.

Im Jahr 2010 haben die deutschen Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich bereits ausgeführt, dass die Erklärung über eine Selbst-Zertifizierung, wie sie die Safe Harbor-Grundsätze vorsehen, für Datenübermittlungen in die USA nicht ausreicht. Sie wiesen darauf hin, dass sich übermittelnde Unternehmen von den Datenempfängern nachweisen lassen müssen, dass die Safe Harbor-Grundsätze auch eingehalten

werden. Mit den Enthüllungen von Edward Snowden wurde offengelegt, dass US-Sicherheitsbehörden systematisch und massenhaft auf in die USA übermittelte personenbezogene Daten zugreifen, und damit die Safe Harbor-Grundsätze mit großer Wahrscheinlichkeit gravierend verletzt werden.

Die Konferenz weist darauf hin, dass bei Übermittlungen in einen Staat, in dem europäisches Datenschutzrecht nicht direkt anwendbar ist, zumindest folgende Garantien für den Datenschutz gegeben sein müssen: Die Zweckbindung der Daten ist grundsätzlich sicherzustellen. Staatliche Zugriffsmöglichkeiten müssen auf ein angemessenes und grundrechtskonformes Maß begrenzt bleiben. Den Betroffenen ist ein effektiver Anspruch auf Auskunft und auf Berichtigung bzw. Löschung falscher bzw. unzulässig gespeicherter Daten zu gewähren. Bei Verstößen bedarf es eines effektiven Rechtsschutzes. Formelle und sprachliche Barrieren dürfen nicht dazu führen, dass die Betroffenen ihre Rechte nicht wahrnehmen können.

17.2 Sonstiges

17.2.1 Musterdienstvereinbarung für öffentliche Stellen über den Betrieb von Videoüberwachungsanlagen

[Der nachstehende Text bietet Beispiele und Anregungen, ist nicht abschließend und beispielhaft und auf den individuellen Fall anzupassen.]

Präambel
Die Videoüberwachung dient der Gewährleistung der schutzwürdigen Belange *[An dieser Stelle wären die gesetzlich in § 33 SächsDSG genannten oder gleichwertigen Gründe zu nennen.]* der Dienststelle.

Eine Beobachtung der Beschäftigten zur Verhaltens- und Leistungskontrolle durch die Videoüberwachungsanlage wird ausgeschlossen. Dem Schutz des informationellen Selbstbestimmungsrechts der betroffenen Beschäftigten ist bestmöglich Rechnung zu tragen. Informationen, die die Dienststelle entgegen den Bestimmungen dieser Dienstvereinbarung erhebt, dürfen nicht gegen betroffene Beschäftigte verwendet werden. Personelle und dienstrechtliche Maßnahmen auf Grundlage unzulässig erhobener Daten sind unwirksam.

Die Vereinbarung ist nur zulässig, soweit die gesetzlichen Voraussetzungen erfüllt sind.

Es gelten die Begriffsbestimmungen des Sächsischen Datenschutzgesetzes.

§ 1 Geltungsbereich

Die Dienstvereinbarung gilt für die Einführung und den Einsatz von optisch elektronischen Einrichtungen (Videoüberwachungsanlagen) im Zuständigkeitsbereich der Dienststelle.

§ 2 Zulässigkeit der Videoüberwachung

(1) Die Videoüberwachung im Bereich der Dienststelle ist unter Einhaltung der gesetzlichen Bestimmungen zulässig, wenn sie zum Zweck

1. des Schutzes der Dienststelle, insbesondere der Gebäudeanlage, der Außenanlagen und der Einrichtungen,
2. der Wahrung des Hausrechts innerhalb der Dienststelle,
3. der Sicherheit und des Schutzes der Besucher und der Beschäftigten der Dienststelle und
4. zur Verfolgung von Straftaten im Dienststellenbereich

erforderlich ist.

[Beispielhaft; die einschlägigen Zwecke sind einzutragen.]

(2) Die Videoüberwachung an Arbeitsplätzen ist

1. zur Überwachung des Kassenbereichs bei der Geldausgabe
2. in erforderlichen Ausnahmefällen und zeitlich begrenzt zum Schutz der Mitarbeiter

zulässig.

[Beispielhaft; die einschlägigen Zwecke sind einzutragen.]

(3) Der Zweck der Videoüberwachungsanlage ist in jedem Einzelfall vorher festzulegen und in der entsprechenden Verfahrensbeschreibung, bezogen auf jede einzelne Überwachungsmaßnahme, zu dokumentieren.

Eine verdeckte Überwachung der Arbeitsplätze und Tonaufzeichnungen finden nicht statt.

(4) Eine Videoaufzeichnung findet nicht statt. [oder] Eine Videoaufzeichnung erfolgt zum Zweck der

1. ….
2. ….

Aufgezeichnete Videodaten werden spätestens nach *[Hier wäre eine datenschutzgerechte (verhältnismäßige) Frist einzutragen.]* gelöscht.

§ 3 Verfahren

(1) Der behördliche Datenschutzbeauftragte ist gemäß § 10 Abs. 4 SächsDSG rechtzeitig über die geplante Videoüberwachung oder maßgebliche Änderungen des automatisierten Verfahrens zu unterrichten.

(2) Erweiterungen der Funktionen oder wesentliche Änderungen beim Verfahren der Videoüberwachung bedürfen der Zustimmung der Personalvertretung. Eine Stellungnahme des behördlichen Datenschutzbeauftragten ist zuvor einzuholen.
[Ggfs. im Falle von Videoaufzeichnungen]
(3) Im Falle einer Auswertung der Videoaufzeichnungen durch die hierzu berechtigten Beschäftigten ist jeweils zuvor der behördliche Datenschutzbeauftragte zu informieren.
Eine Auswertung der Daten durch die hierzu berechtigten Beschäftigten erfolgt nur zu den festgelegten Zwecken. Eine Weitergabe der Videoaufzeichnungen erfolgt nicht, es sei denn, es ist zu Zwecken der Strafverfolgung oder auf Anordnung eines Gerichts erforderlich. Auswertungen sind zu dokumentieren.

§ 4 Technische und organisatorische Maßnahmen
(1) Die technischen Anlagen zur Videoüberwachung sind gegen unbefugte Eingriffe zu sichern.
(2) Der Kreis der zutrittsberechtigten Beschäftigten ist klein zu halten. Zutrittsberechtigung erhalten nur die Beschäftigten, die diese Aufgaben bedingt benötigen.
(3) … *[Ggfs. sind weitere datenschutzorganisatorische Maßnahmen zu nennen.]*

§ 5 Umsetzung der Videoüberwachungsmaßnahme
(1) Videoüberwachungsanlagen sind in den betroffenen Bereichen deutlich kenntlich zu machen und so anzubringen, dass sie vor dem Betreten des Überwachungsbereichs wahrgenommen werden können. Auf dem Schild ist die verantwortliche Stelle zu nennen. Soweit die Überwachung nur temporär erfolgt, ist darauf unter Mitteilung der Zeiten hinzuweisen.
(2) Schwenkbare, zoomfähige und 360°-Kameras sind nur einzusetzen, soweit dies für den zuvor festgelegten Zweck erforderlich ist. Die Sichtkegel- und Zoombereiche sind in der Verfahrensbeschreibung mit Bildskizze festzulegen.

§ 6 Evaluation
Unter Beteiligung des behördlichen Datenschutzbeauftragten ist in jährlichen Abständen zum Jahresabschluss zu prüfen, ob ein Grund für die Videoüberwachung fortbesteht. Entfallen Gefährdungen oder stellt sich die Maßnahme als nicht mehr erforderlich heraus, ist sie teilweise oder vollständig zu beenden.

§ 7 Inkrafttreten
Die Dienstvereinbarung tritt unmittelbar nach Unterzeichnung beider Parteien in Kraft.

Ort, Datum	Ort, Datum
Unterschrift für die Dienststellenleitung	Unterschrift für die Personalvertretung

17.2.2 Kernteam Verschlüsselung - Handlungsempfehlungen und Umsetzungsplanung

Handlungsempfehlungen

1. Sicherer Webzugang, Schwerpunkt HTTPS

1.1 Einführung geregelter Prozesse zur Domainnamensverwaltung

1.1.A Zentrale Erfassung von Domains, Diensten und Zuständigkeiten

1.1.B Definierte Prozesse zur Neubeauftragung, Aktualisierung und Abschaltung

1.2 Strategische Verschlüsselungsempfehlungen

1.2.A HTTPS-Verschlüsselung für alle Webseiten anbieten

1.2.B Mit HSTS die Nutzung von HTTPS erzwingen

1.2.C Mit Forward Secrecy die rückwirkende Entschlüsselung verhindern

1.3 Umsetzung konkreter technischer Verschlüsselungsempfehlungen

1.3.A Beseitigung von HTTPS-Zertifikatsfehlern (ungültig, abgelaufen, selbstsigniert) durch Einsatz von Zertifikaten der Sachsen Global CA

1.3.B Zentrale Algorithmenunterstützung von TLS1.2, Abschaltung unsicherer Algorithmen wie RC4 und SSLv2

1.3.C Härtung der HTTPS-Konfiguration zur Vermeidung von Angriffen wie Insecure Renegotiation, TLS-Compression, BEAST, CRIME und Heartbleed

2. Sicherer Datenaustausch im SVN

2.1 Verschlüsselung als wesentliches Leistungsmerkmal im SVN 2.0 entwickeln

2.1.A Grundverschlüsselung der Leitungen zwischen allen Behördenstandorten mindestens als Option in SVN 2.0-Ausschreibung aufnehmen

2.1.B Aufnahme und Bewertung der Anforderungen an weitergehende Verschlüsselungslösungen (z. B. Ende-zu-Ende-Verschlüsselung)

2.2 Grundlagen für moderne Verschlüsselungsverfahren im SVN schaffen

2.2.A Prüfung Aktualisierungsbedarf Hard- und Software im SVN bzgl. der Unterstützung moderner Verschlüsselungsverfahren

2.2.B Ablösung unsicherer Verschlüsselungsalgorithmen im SVN (z. B. SHA-1 als Grundlage elektronischer Zertifikate der Landes-PKI)

2.3 E-Mail-Verschlüsselung im und zum SVN flächendeckend einsetzen

2.3.A Flächendeckende Unterstützung von STARTTLS von und zu externen E-Mail-Partnern

2.3.B Flächendeckende E-Mail-Verschlüsselung im SVN zwischen den Ressorts (Exchange-Konzept, Server-zu-Server Kommunikation)
2.3.C Flächendeckende E-Mail-Verschlüsselung im SVN innerhalb der Behörden (Exchange-Konzept, hier: Outlook-Client-zu-Server Kommunikation)

Umsetzungsplan

Kurzfristige Maßnahmen (2. Quartal 2014)

Alle dringlichen Maßnahmen, die sofort umgesetzt werden sollen, sind im Folgenden fett gedruckt hervorgehoben. Die anderen Maßnahmen sind noch näher zu untersetzen.

1.1 Einführung geregelter Prozesse zur Domainnamensverwaltung
Das Kernteam legt einen entsprechenden Vorschlag vor.

1.2 Strategische Verschlüsselungsempfehlungen
Die SVN-Leitstelle legt ein Angebot zu Kosten und Rahmenbedingungen zur zentralen Umstellung aller Webseiten der Landesverwaltung auf HTTPS vor.

1.3 Umsetzung konkreter technischer Verschlüsselungsempfehlungen
Das Kernteam legt eine Handlungsanleitung zur Umstellung auf Zertifikate der Sachsen Global CA und zur Beseitigung der vorhandenen Zertifikatsfehler für Systeme mit Apache und Microsoft IIS vor.

Alle Ressorts stellen die von ihnen betriebenen HTTPS-Seiten mit fehlerhaften Zertifikaten auf Zertifikate der Sachsen Global CA um, soweit möglich. Alle Zertifikatsfehler werden beseitigt.

Das Kernteam erarbeitet auf Basis einer Erfassung der auf die Webseiten der Landesverwaltung zugreifenden Systeme eine Empfehlung der abzuschaltenden veralteten Verschlüsselungsalgorithmen wie RC4 oder SSLv2. Nach Beschluss durch die AG IS erarbeitet das Kernteam eine entsprechende Handlungsanleitung zur Abschaltung veralteter Algorithmen für Systeme mit Apache und Microsoft IIS.

Analog zu den veralteten Algorithmen erarbeitet das Kernteam eine Empfehlung und - nach Beschluss durch die AG IS - eine Handlungsanleitung zur Härtung der HTTPS-Konfiguration.

2.1 Verschlüsselung als wesentliches Leistungsmerkmal im SVN 2.0 entwickeln
Die Grundverschlüsselung aller Leitungen wird vom SMJus mindestens als Option in SVN 2.0-Ausschreibungsunterlagen aufgenommen.

2.2 Grundlagen für moderne Verschlüsselungsverfahren im SVN schaffen
Das Kernteam erarbeitet auf Basis der auf die Landes-PKI zugreifenden Systeme eine Empfehlung der zu aktualisierenden Hard- und Software sowie zur Abschaltung unsicherer Verschlüsselungsalgorithmen.

2.3 E-Mail-Verschlüsselung im und zum SVN flächendeckend einsetzen
Das Kernteam erstellt eine Handlungsanleitung für Outlook-Client-zu-Server-Verschlüsselung.

Die Ressorts stellen flächendeckend auf verschlüsselte Exchange-Kommunikation um.

STARTTLS wird durchgängig umgesetzt, den Kommunen wird im Benehmen mit SAKD und KDN GmbH die Umsetzung empfohlen.

Kurzfristige Maßnahmen (3. Quartal 2014)

1.1 Einführung geregelter Prozesse zur Domainnamensverwaltung
Prüfung des Vorschlags des Kernteams und Beschluss der AG IS.

1.2 Strategische Verschlüsselungsempfehlungen
Prüfung des Angebots der SVN-Leitstelle zur flächendeckenden Umstellung auf HTTPS und Beschluss der AG IS zum weiteren Vorgehen.
Das Kernteam erarbeitet eine Empfehlung zur Umsetzung von HSTS und Forward Secrecy.

1.3 Umsetzung konkreter technischer Verschlüsselungsempfehlungen
Das Kernteam erarbeitet eine Empfehlung zur Umsetzung von TLS1.2.
Die veralteten Verschlüsselungsalgorithmen wie RC4 oder SSLv2 werden auf den zentralen Proxys (nach außen) abgeschaltet. Die HTTPS-Konfiguration wird gehärtet.

2.2 Grundlagen für moderne Verschlüsselungsverfahren im SVN schaffen
Die Empfehlung des Kernteams der zu aktualisierenden Hard- und Software sowie zur Abschaltung unsicherer Verschlüsselungsalgorithmen wird geprüft. Die AG IS fasst einen entsprechenden Beschluss.

Mittelfristige Maßnahmen (4. Quartal 2014)

1.1 Einführung geregelter Prozesse zur Domainnamensverwaltung
Geregelte Prozesse zur Domainnamensverwaltung werden eingeführt.

1.2 Strategische Verschlüsselungsempfehlungen

Prüfung der Empfehlung des Kernteams zur Umsetzung von HSTS und Forward Secrecy und Beschluss der AG IS zum weiteren Vorgehen.
Das Angebot zur flächendeckenden Umstellung auf HTTPS wird zentral (nach außen) umgesetzt.

1.3 Umsetzung konkreter technischer Verschlüsselungsempfehlungen
Prüfung der Empfehlung des Kernteams für die Unterstützung von TLS 1.2 und Beschluss der AG IS zum weiteren Vorgehen.
Die veralteten Verschlüsselungsalgorithmen wie RC4 oder SSLv2 werden auf den gehosteten Webseiten und auf allen HTTPS-Seiten der Ressorts abgeschaltet. Die HTTPS-Konfiguration wird gehärtet.

2.1 Verschlüsselung als wesentliches Leistungsmerkmal im SVN 2.0 entwickeln
Aufnahme und Bewertung der Anforderungen an weitergehende Verschlüsselungslösungen im SVN 2.0 durch das Kernteam mit den Ressorts.
Die vom Kernteam vorgelegten Anforderungen an weitergehende Verschlüsselungslösungen werden geprüft und von der AG IS beschlossen. Anschließend nimmt das SMJus diese Anforderungen mindestens als Option in die SVN2.0-Ausschreibungsunterlagen auf.

2.2 Grundlagen für moderne Verschlüsselungsverfahren im SVN schaffen
Die Ressorts aktualisieren veraltete, auf die Landes-PKI zugreifende Hard- und Software. Das SMJus schaltet die unsicheren Verschlüsselungsalgorithmen seitens der Landes-PKI ab.

2.3 E-Mail-Verschlüsselung im und zum SVN flächendeckend einsetzen
Alle Ressorts stellen flächendeckend auf verschlüsselte Kommunikation zwischen den Outlook-Clients und Exchange-Servern um.

Mittel- und langfristige Maßnahmen

1.2 Strategische Verschlüsselungsempfehlungen
Die flächendeckende Umstellung der gehosteten Webseiten sowie aller Internetseiten der Ressorts auf HTTPS wird im beschlossenen Umfang umgesetzt.
Das Kernteam erarbeitet eine Handlungsanleitung zur Umsetzung von HSTS und Forward Secrecy unter Apache und Microsoft IIS. Die Handlungsanleitung wird zunächst auf den zentralen Proxys und den gehosteten Webseiten, später auf allen HTTPS-Seiten der Ressorts umgesetzt.
TLS1.2 wird zunächst auf den zentralen Proxys und den gehosteten Webseiten, später auf allen HTTPS-Seiten der Ressorts umgesetzt.

17.2.3 Sichere HTTPS-Konfiguration für Apache-Webserver

1. Generelle Hinweise und Einschränkungen

Dieses Dokument erläutert die sichere Konfiguration der Transportverschlüsselung HTTPS (HTTP mit TLS) mit einem Apache-Webserver. Die TLS-Verschlüsselung garantiert die Echtheit und Vertraulichkeit der übertragenen Daten.

Die Verschlüsselung ist nur ein Aspekt im Betrieb einer sicheren Webapplikation. Sie bietet keinen Schutz vor gewöhnlichen Web-Sicherheitslücken wie Cross-Site-Scripting (XSS), SQL-Injections oder Cross-Site-Request-Forgery (CSRF). Der Schutz vor solchen Lücken ist nicht Gegenstand dieser Dokumentation.

Zur allgemeinen Sicherheit ist es generell sehr wichtig, Webanwendungen wie beispielsweise Content-Management-Systeme (Wordpress, Joomla etc.) regelmäßig zu aktualisieren. Bei Eigenentwicklungen ist der Einsatz aktueller Sicherheitstechnologien wie Prepared Statements und Content-Security-Policy anzuraten.

2. Zertifikat

Um eine HTTPS-Verbindung zu konfigurieren benötigt man ein Zertifikat. Dieses Zertifikat kann man von einer beliebigen Zertifizierungsstelle erhalten, die Sicherheit ist unabhängig von der gewählten Zertifizierungsstelle.

Es gibt die Möglichkeit sogenannte EV-Zertifikate (Extended Validation) zu erhalten. Bei diesen wird im Browser neben dem Schlosssymbol der eingetragene Name des Zertifikatsinhabers in grün angezeigt. EV-Zertifikate sind deutlich teurer und haben keinen Einfluss auf die Sicherheit der Verschlüsselung.

Eine Zertifizierungsstelle, die einfache Zertifikate kostenlos ausstellt, ist StartSSL:

```
https://startssl.com/
```

Bei der Erstellung der Zertifikate ist zu beachten:

- Für Zertifikate kommen heute fast immer RSA-Schlüssel zum Einsatz. RSA-Schlüssel mit einer Länge von 1024 Bit gelten als unsicher und werden heute nicht mehr verwendet. RSA-Schlüssel mit 2048 Bit sind üblich, längere Schlüssel mit 4096 Bit sind ebenfalls möglich. Letztere sind geringfügig langsamer, schützen jedoch vor möglichen Durchbrüchen bei Angriffen auf RSA. Aktuelle Versionen von OpenSSL erstellen standardmäßig 2048-Bit-Schlüssel.

- RSA-Schlüssel sollten mit einem Exponenten von e=65537 erstellt werden. Bei allen aktuellen Tools wie beispielsweise OpenSSL ist dies die Standardeinstellung, sehr alte Tools erstellen unter Umständen Schlüssel mit einem Exponenten von e=3, was als riskant gilt.

- Zertifikate sollten mit SHA256 unterschrieben werden. Bis vor kurzem waren Zertifikatsunterschriften mit SHA1 üblich, obwohl schon seit 2005 bekannt ist, dass SHA1 Sicherheitsprobleme hat. Auf den verwendeten Algorithmus hat man selbst keinen Einfluss. Vor kurzem hat Google angekündigt, ab 2015 vor Zertifikaten mit dem alten SHA1-Algorithmus zu warnen. Daher ist davon auszugehen, dass Zertifizierungsstellen heute keine derartigen Zertifikate mehr ausstellen. Besitzt man noch ein mit SHA1 unterschriebenes Zertifikat sollte man sich zeitnah um einen Austausch bemühen.

- Einige Zertifizierungsstellen bieten die Möglichkeit, den privaten Schlüssel für das Zertifikat zu erstellen. Von dieser Möglichkeit ist abzuraten, da in diesem Fall die Zertifizierungsstelle im Besitz des privaten Schlüssels ist. Vielmehr sollte man ein sogenanntes Certificate Request (CSR) erstellen.

- Neue Zertifikate sollten immer auch mit einem neuen Schlüssel genutzt werden. Die Wiederverwendung eines Schlüssels aus dem alten Zertifikat, die von manchen Zertifizierungsstellen angeboten wird, ist nicht empfehlenswert.

Certificate Requests (CSRs) lassen sich mit dem Kommandozeilentool von OpenSSL erstellen:

```
openssl req -newkey rsa:2048 -new -sha256 -nodes -keyout
https.key -out https.csr
```

Für ein Zertifikat mit einem längeren (4096 Bit-)Schlüssel lautet der Befehl entsprechend:

```
openssl req -newkey rsa:4096 -new -sha256 -nodes -keyout
https.key -out https.csr
```

3. Softwareversionen

Üblicherweise werden Webserver auf Linux-Systemen mit der Software Apache httpd und OpenSSL betrieben.

Viele der verbesserten TLS-Funktionen sind nur in jüngeren Versionen dieser Programme verfügbar. So wurde beispielsweise die Unterstützung eines sicheren Forward Secrecy-Schlüsselaustauschs erst mit Apache Version 2.4.8 eingeführt. OpenSSL unterstützt viele wichtige Features erst mit der Version 1.0.1j.

Falls möglich sollte man den Einsatz alter Apache-Versionen (2.2, 2.0) oder alter OpenSSL-Versionen (0.9.8, 1.0.0) vermeiden.

4. Protokollversionen

Für einige Verwirrung sorgen die Versionen der verschiedenen SSL/TLS-Protokolle.

In den 90er Jahren hat die Firma Netscape das Protokoll SSL entwickelt. Die erste Version trug die Versionsnummer 2 (SSLv2), eine offizielle Version 1 gibt es nicht. SSLv2 erwies sich bereits nach kurzer Zeit als sehr unsicher, daher wurde die Version 3 (SSLv3) entwickelt. Seit der kürzlich entdeckten POODLE-Attacke gilt auch SSLv3 als vollständig unsicher. Beide alten SSL-Protokolle sollten auf keinen Fall mehr verwendet werden. Kompatibilitätsprobleme mit der Abschaltung der Protokolle SSLv2 und SSLv3 gibt es nur sehr wenige. Lediglich Nutzer mit dem sehr alten Internet Explorer 6.0 können Seiten dann nicht mehr nutzen.

Das Nachfolgeprotokoll von SSL nennt sich TLS. Von ihm sind bislang drei Versionen erschienen: 1.0, 1.1 und 1.2. Bis vor kurzem war TLS 1.0 die einzig gebräuchliche TLS-Version. Daher ist es bis auf weiteres nicht möglich, aus Kompatibilitätsgründen auf TLS 1.0 zu verzichten. Auch in TLS 1.0 und TLS 1.1 gibt es Sicherheitsprobleme (BEAST, Lucky Thirteen), diese sind allerdings nicht extrem kritisch und die gängigen Browser haben Gegenmaßnahmen gegen diese Schwächen implementiert.

In der Apache-Konfiguration kann man die Protokolle mit dem Befehl SSLProtcol einstellen. Die empfehlenswerte Konfiguration lautet:

```
SSLProtocol -SSLv2 -SSLv3 +TLSv1 +TLSv1.1 +TLSv1.2
```

5. Ciphersuiten

TLS unterstützt eine ganze Reihe unterschiedlicher Kombinationen von Verschlüsselungsalgorithmen. Generell verzichten sollte man auf alle sogenannten Export-Algorithmen (RC2, RC4 mit 40/64 Bit, Single-DES mit 56 Bit). Diese sehr schwachen Algorithmen wurden in den 90er Jahren als Reaktion auf damals geltende US-Exportbeschränkungen eingeführt. Sie lassen sich mit aktuellen Computern trivial brechen. Ebenfalls als problematisch gilt heute der Algorithmus RC4, er sollte nicht mehr verwendet werden (Beschlussempfehlung).

Als sicher und unbedenklich gilt der standardisierte AES-Algorithmus. Der Algorithmus Triple-DES ist zwar relativ alt, gilt aber ebenfalls als unbedenklich. Er kann beibehalten werden, um die Kompatibilität mit Windows XP weiterhin zu ermöglichen.

Problematisch ist der sogenannte CBC-Modus von AES. Die Probleme mit dem CBC-Modus haben unter anderem zur BEAST-Attacke und zur Lucky Thirteen-Attacke geführt. Empfehlenswert ist die Verwendung von AES im GCM-Modus. Dies wird allerdings erst von der jüngsten TLS-Version 1.2 unterstützt. Aus Kompatibilitätsgründen kann man heute auf AES im CBC-Modus leider nicht verzichten.

Im Entwurfsstadium befindet sich ein neuer Algorithmus namens ChaCha20. Dieser Algorithmus gilt ebenfalls als sehr sicher. Die Unterstützung ist allerdings in aktuellen OpenSSL-Versionen noch nicht vorhanden.

Empfehlenswert ist der Einsatz von Forward Secrecy-Verfahren. Diese gewährleisten, dass selbst in einer Situation, in der es einem Angreifer gelingt, den privaten Schlüssel zu stehlen, die Kommunikation aus der Vergangenheit weiterhin sicher ist. Forward Secrecy kann in TLS entweder mit dem klassischen Diffie Hellman-Verfahren (DHE) oder mit dem Diffie Hellman-Verfahren in elliptischen Kurven (ECDHE) genutzt werden.

Die unterstützten Ciphersuiten kann man im Apache-Webserver mit der Direktive SSLCipherSuites einstellen. Eine empfehlenswerte Konfiguration lautet:

```
SSLCipherSuite HIGH:!MEDIUM:!LOW:!aNULL@STRENGTH
```

6. Kompression

TLS bietet die Möglichkeit Daten zu komprimieren. Wie sich herausgestellt hat ist diese Datenkomprimierung ein Sicherheitsrisiko (CRIME-Attacke). Sie sollte daher nicht verwendet werden. Zu beachten ist, dass die Datenkomprimierung von HTTP ebenfalls ein Sicherheitsrisiko darstellen kann (BREACH-Attacke). Derartige Angriffe können je-

doch im Rahmen von HTTPS nicht verhindert werden, das ist vielmehr Aufgabe der verwendeten Web-Applikation.

Die Kompression kann man in Apache mit folgender Konfiguration ausschalten:

```
SSLCompression off
```

7. Unsichere Neuaushandlung von Verbindungen

Im Jahr 2009 wurde ein Sicherheitsproblem in der sogenannten Renegotiation (Neuaushandlung von Verbindungen) von TLS entdeckt. Im RFC 5746 wurde ein sicheres Verfahren für die Renegotiation eingeführt. Die alte, unsichere Renegotiation wird nur von sehr alten OpenSSL-Versionen unterstützt. Ist diese vorhanden, so ist dies ein Hinweis darauf, dass das darunterliegende System schon sehr lange Zeit keine Sicherheitsaktualisierungen mehr erhalten hat. Vermutlich gibt es dann weitere, gravierendere Sicherheitsprobleme.

Bei der Verwendung aktueller Software sind keine besonderen Maßnahmen notwendig, es wird automatisch die sichere Renegotiation verwendet.

8. Protokoll-Downgrades und SCSV

Ein Problem von aktuellen Webbrowsern ist, dass ein Angreifer die Möglichkeit hat, die Verwendung eines älteren, weniger sicheren Protokolls zu erzwingen. Dies ist insbesondere im Zusammenhang mit SSLv3 ein großes Problem (POODLE-Angriff), weshalb wie bereits erläutert die Unterstützung von SSLv3 auf jeden Fall abgeschaltet werden muss.

Generell verhindert werden Protokolldowngrade-Angriffe durch ein Verfahren namens SCSV, es muss allerdings von Client und Server unterstützt werden. OpenSSL unterstützt SCSV seit der Version 1.0.1j. Da SCSV als Pseudo-Ciphersuite aktiviert wird ist hierfür die Konfiguration der Ciphersuiten relevant. Wird die oben empfohlene Konfiguration verwendet, so wird SCSV auf aktuellen Systemen automatisch aktiviert.

9. OCSP Stapling

Das OCSP-Protokoll ermöglicht die Gültigkeitsprüfung von Zertifikaten bei der verwendeten Zertifizierungsstelle. Das traditionelle OCSP-Protokoll ist sehr unzuverlässig, da es nicht funktioniert, wenn die Server einer Zertifizierungsstelle nicht erreichbar sind.

Empfehlenswert ist die Aktivierung des Features OCSP Stapling. Damit wird die Gültigkeitsinformation für ein Zertifikat automatisch beim Verbindungsaufbau mitgeschickt. OCSP Stapling wird in Apache 2.4 unterstützt und kann mit folgender Option aktiviert werden:

```
SSLUseStapling on
SSLStaplingCache shmcb:/var/tmp/ocsp/cache(10240000)
```

Das Verzeichnis für den OCSP-Stapling-Cache (hier im Beispiel /var/tmp/ocsp-stapling-cache/) muss auf ein leeres Verzeichnis verweisen, auf das der Apache-Prozess Schreibzugriff hat.

10. HTTPS-Only-Webseiten

Viele große Webseiten (Google, Facebook, Twitter) sind inzwischen nur noch über verschlüsselte Verbindungen erreichbar. Es spricht meistens nichts dagegen, Webangebote ausschließlich über HTTPS verfügbar zu machen. Die Auswirkungen auf die Performance sind in aller Regel minimal. Die ausschließliche Verwendung von HTTPS verbessert das Ranking einer Webseite in der Suchmaschine von Google.

Bei reinen HTTPS-Webseiten schaltet man von der HTTP-Webseite eine Umleitung, die entsprechende Konfiguration sieht so aus:

```
<VirtualHost *:80>
 ServerName www.beispiel.de
 RedirectPermanent / https://www.beispiel.de/
</VirtualHost>
```

11. HTTP Strict Transport Security (HSTS)

Auch reine HTTPS-Seiten sind für eine Angriffsform namens SSL-Stripping anfällig. Hierbei versucht ein Angreifer, die Weiterleitung von HTTP auf HTTPS zu verhindern.

Um derartige Stripping-Angriffe zu vereiteln gibt es das Feature HTTP Strict Transport Security (HSTS). Hierbei teilt eine Webseite dem Webbrowser mit, dass diese Seite für einen definierten Zeitraum ausschließlich über HTTPS erreichbar ist. Ein empfehlenswerter Zeitraum ist etwa ein Jahr.

Der Strict-Transport-Security-Header kann entweder direkt in der Apache-Konfiguration oder in der Webapplikation selbst gesendet werden. In einem virtuellen Host von Apache kann man Strict-Transport-Security mit folgender Konfiguration eintragen:

```
Header always set Strict-Transport-Security "max-age=31536000"
```

Der Zeitraum wird in Sekunden angegeben, das Beispiel hier gilt für ein Jahr. Falls der Befehl includeSubdomains angegeben wird gilt die HSTS-Einstellung automatisch für alle Subdomains.

Es ist auch möglich, seine Webseite direkt in einigen Browsern (zurzeit Chrome und Firefox) als HTTPS-Only-Seite vormerken zu lassen, in dem Fall führt ein Browser überhaupt keine Verbindungsversuche mittels HTTP mehr durch:

```
https://hstspreload.appspot.com/
```

12. HTTP Public Key Pinning (HPKP)

Ein sehr neues Feature ist das sogenannte Pinning von TLS-Schlüsseln. Dabei kann eine Webseite einen Browser anweisen, sich den aktuell verwendeten Schlüssel und einen Ersatzschlüssel (für einen zukünftigen Zertifikatstausch) für einen definierten Zeitraum zu merken.

HTTP Public Key Pinning (HPKP) ist entstanden als Reaktion auf zahlreiche Fälle, in denen Zertifizierungsstellen gehackt wurden und gefälschte Zertifikate ausgestellt wurden (Comodo, Diginotar, Türktrust, India CCA). Es schützt vor Angreifern, die in der Lage sind, auf eine kompromittierte Zertifizierungsstelle zuzugreifen.

HPKP ist ein sehr mächtiges Feature, es kommt allerdings mit einem nicht zu unterschätzenden Risiko: Wenn man sämtliche privaten Schlüssel verliert sperrt man unter Umständen Nutzer aus, ohne dass man etwas dagegen unternehmen kann. Die Verwendung von HPKP sollte sehr gut geplant sein, die Verantwortlichkeit für die Aufbewahrung der privaten Schlüssel ist dabei essentiell.

Die Funktionsweise von HPKP ist mit HSTS vergleichbar und geschieht über einen HTTP-Header, der beispielsweise in der Konfiguration des virtuellen Hosts gesetzt werden kann:

```
Header always set Public-Key-Pins 'max-age=5184000; pin-sha256="TcPnP28kGjkPyRoA0X47W3GZGlBTBRQvjBopIdqQ79s=";pin-sha256="Ogse+MdesZR9UWApeVWIMKiF8CpobFoIp/MEg+1DYZo=";'
```

Der Zeitraum wird wie bei HSTS in Sekunden angegeben, das Beispiel setzt die Pins für 60 Tage. Als Pins werden die Zertifikate UU-encodiert, mit SHA256 gehasht und an-

schließend Base64-codiert. Ein Skript, mit dem die passenden Pins zu Zertifikaten erstellt werden können, findet sich hier:

```
https://github.com/hannob/hpkp
```

13. Konfiguration in Kürze

Alle empfehlenswerten Konfigurationsoptionen für den gesamten Apache-Server:

```
SSLProtocol -SSLv2 -SSLv3 +TLSv1 +TLSv1.1 +TLSv1.2
SSLCipherSuite HIGH:!MEDIUM:!LOW:!aNULL@STRENGTH
SSLCompression off
SSLUseStapling on
SSLStaplingCache shmcb:/var/tmp/ocsp/cache(10240000)
```

Eine Beispielkonfiguration für einen virtuellen Host, HTTP-Teil:

```
<VirtualHost *:80>
ServerName www.beispiel.de
RedirectPermanent / https://www.beispiel.de/
</VirtualHost>
```

HTTPS-Teil:

```
<VirtualHost *:443>
ServerName www.beispiel.de
DocumentRoot /home/example/websites/beispiel.de/htdocs
SSLCertificateFile /etc/apache2/certs/beispiel.crt
SSLCertificateKeyFile /etc/apache2/certs/beispiel.key
SSLCertificateChainFile        /etc/apache2/certs/beispiel-
intermediate.pem
SSLEngine On
Header   always   set   Strict-Transport-Security   "max-
age=31536000"
Header always set Public-Key-Pins 'max-age=5184000; pin-
sha256="TcPnP28kGjkPyRoA0X47W3GZGlBTBRQvjBopIdqQ79s=";pin-
sha256="Ogse+MdesZR9UWApeVWIMKiF8CpobFoIp/MEg+1DYZo=";'
</VirtualHost>
```

14. Weitere Sicherheitslücken

In OpenSSL wurden zuletzt zahlreiche Sicherheitsprobleme in der Implementierung festgestellt. Neben dem Heartbleed-Bug ist insbesondere die CCS-Injection-Lücke als kritisch anzusehen. Heartbleed und CCS-Injection können durch den Einsatz aktueller Softwareversionen verhindert werden.

Verschiedene andere im Jahr 2014 entdeckte Lücken (BERserk, Goto Fail, Tripple Handshake) sind zwar ebenfalls kritisch, betreffen aber Clientanwendungen und Webbrowser. Auf Serverseite kann man hier nichts unternehmen. Generell ist natürlich die Verwendung aktueller Browserversionen dringend anzuraten.

15. Tests der Konfiguration

Der SSL-Test der Firma Qualys gilt als de-facto-Standard für sichere TLS-Konfigurationen.

Der Test ist online hier zu finden:

`https://ssllabs.com/ssltest/`

Der Qualys-Test liefert detaillierte Informationen zur verwendeten Konfiguration und gibt ein Rating für die Sicherheit der HTTPS-Verbindung aus. Bei Nutzung aller hier im Dokument beschriebenen Ratschläge erhält man zum aktuellen Zeitpunkt (Oktober 2014) ein A+ als Gesamtwertung. Die Kriterien des Tests werden ständig angepasst, somit ist dies keine Gewährleistung für eine gute Wertung in der Zukunft.

Zwei Kommandozeilen-Tools, die einen ähnlichen Test manuell durchführen sind sslyze und testssl.sh:

`https://testssl.sh/`
`https://github.com/nabla-c0d3/sslyze/releases`

Stichwortverzeichnis