Sächsischer Landtag
5. Wahlperiode

DRUCKSACHE 5/13033

# Schutz des Persönlichkeitsrechts im öffentlichen Bereich

# 16. Tätigkeitsbericht

# des

# Sächsischen Datenschutzbeauftragten

Berichtszeitraum: 1. April 2011 bis 31. März 2013

Dem Sächsischen Landtag

vorgelegt zum 31. März 2013

gemäß § 30 des Sächsischen Datenschutzgesetzes

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

Vorbemerkung zum Sprachgebrauch in diesem Bericht:

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

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

Die genaue Fundstelle und Angabe der letzten Änderung sind bei bekannteren Bundesgesetzen (die in den gängigen Gesetzessammlungen leicht zu finden sind) weggelassen worden.

| | |
|---|---|
| AO | Abgabenordnung in der Fassung der Bekanntmachung vom 1. Oktober 2002 (BGBl. I S. 3866; 2003 I S. 61), zuletzt geändert durch Art. 2 Abs. 71 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) |
| AsylbLG | Asylbewerberleistungsgesetz in der Fassung der Bekanntmachung vom 5. August 1997 (BGBl. I S. 2022), zuletzt geändert durch Art. 3 des Gesetzes vom 22. November 2011 (BGBl. I S. 2258) |
| AufenthG | Aufenthaltsgesetz in der Fassung der Bekanntmachung vom 25. Februar 2008 (BGBl. I S. 162), zuletzt geändert durch Art. 3 des Gesetzes vom 6. September 2013 (BGBl. I S. 3556) |
| AuslG | Ausländergesetz, Außerkrafttreten am 30. April 2004, wurde durch AufenthG ersetzt |
| BBergG | Bundesberggesetz vom 13. August 1980 (BGBl. I S. 1310), geändert durch Art. 4 Abs. 71 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 14. August 2009 (BGBl. I S. 2814) |
| BeurkG | Beurkundungsgesetz vom 28. August 1969 (BGBl. I S. 1513), zuletzt geändert durch Art. 1 des Gesetzes vom 15. Juli 2013 (BGBl. I S. 2378) |
| BGB | Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Art. 4 Abs. 5 des Gesetzes vom 1. Oktober 2013 (BGBl. I S. 3719) |

| | |
|---|---|
| BKRG | Bundeskrebsregisterdatengesetz vom 10. August 2009 (BGBl. I S. 2707) |
| BNotO | Bundesnotarordnung in der im Bundesgesetzblatt Teil III, Gliederungsnummer 303-1, veröffentlichten bereinigten Fassung, geändert durch Art. 14 des Gesetzes vom 23. Juli 2013 (BGBl. I S. 2586) |
| DSG NRW | Datenschutzgesetz Nordrhein-Westfalen vom 9. Juni 2000 (GV NRW S. 452) |
| EnWG | Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970, 3621), geändert durch Art. 3 Abs. 4 des Gesetzes vom 4. Oktober 2013 (BGBl. I S. 3746) |
| FamFG | Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit vom 17. Dezember 2008 (BGBl. I S. 2586, 2587), geändert durch Art. 2 des Gesetzes vom 10. Oktober 2013 (BGBl.I S. 3786) |
| GBO | Grundbuchordnung in der Fassung der Bekanntmachung vom 26. Mai 1994 (BGBl. I S. 1114), geändert durch Art. 12 des Gesetzes vom 10. Oktober 2013 (BGBl. I S. 3786) |
| GewO | Gewerbeordnung in der Fassung der Bekanntmachung vom 22. Februar 1999 (BGBl. I S. 202), geändert durch Art. 2 des Gesetzes vom 6. September 2013 (BGBl. I S. 3556) |
| GG | Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Art. 1 des Gesetzes vom 11. Juli 2012 (BGBl. I S. 1478) |
| GVG | Gerichtsverfassungsgesetz in der Fassung der Bekanntmachung vom 9. Mai 1975 (BGBl. I S. 1077), geändert durch Art. 5 Abs. 1 des Gesetzes vom 10. Oktober 2013 (BGBl. I S. 3799) |
| HAG | Heimarbeitsgesetz in der im Bundesgesetzblatt Teil III, Gliederungsnummer 804-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Art. 225 der Verordnung vom 31. Oktober 2006 (BGBl. I S. 2407) |
| 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) |

| | |
|---|---|
| KomBekVO | Verordnung des SMI über die Form kommunaler Bekanntmachungen (Kommunalbekanntmachungsverordnung) vom 19. Dezember 1997 (SächsGVBl. 1998 S. 19) |
| LJHG | Landesjugendhilfegesetz vom 4. März 1992 (SächsGVBl. S. 61) zuletzt geändert durch Art. 2 vom 11. Juni 2010 (SächsGVBl. S. 182, 184) |
| LuftVG | Luftverkehrsgesetz vom 1. August 1922 (RGBl. 1922 I S. 681), zuletzt geändert durch Art. 2 Abs. 175 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) |
| LuftVZO | Luftverkehrs-Zulassungs-Ordnung vom 19. Juni 1964 (BGBl. I S. 370), zuletzt geändert durch Art. 28 des Gesetzes vom 25. Juli 2013 (BGBl. I S. 2749) |
| MiStra | Verwaltungsvorschrift des Sächsischen Staatsministeriums der Justiz über Mitteilungen in Strafsachen vom 19. Mai 2008 (SächsJMBl. S. 86) |
| OWiZuVO | Verordnung der Sächsischen Staatsregierung über Zuständigkeiten nach dem Gesetz über Ordnungswidrigkeiten (Ordnungswidrigkeiten-Zuständigkeitsverordnung vom 16. Juli 2008 (SächsGVBl. S. 481) |
| PAuswG | Personalausweisgesetz vom 18. Juni 2009 (BGBl. I S. 1346), zuletzt geändert durch Art. 4 Abs. 1 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) |
| RBStV | Rundfunkbeitragsstaatsvertrag vom 21. Dezember 2011 (SächsGVBl. S. 640) |
| RGebStV | Rundfunkgebührenstaatsvertrag vom 31. August 1991, gültig bis 31. Dezember 2012 |
| SächsArchivG | Archivgesetz für den Freistaat Sachsen vom 17. Mai 1993 (SächsGVBl. S. 449), zuletzt geändert mit Art. 2 des Gesetzes vom 5. Mai 2004 (SächsGVBl. S. 148) |
| 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), Neufassung vom 14. Dezember 2006 (SächsGVBl. S. 530), zuletzt geändert durch Zweites Gesetz zur Änderung des Gesetzes vom 14. Juli 2011 (SächsGVBl. S. 270) |

| | |
|---|---|
| SächsFöFoG | Sächsisches Gesetz zur Errichtung von Förderfonds (Sächsisches Förderfondsgesetz) vom 15. Dezember 2010 (SächsGVBl. S. 387), geändert durch Art. 5 des Gesetzes vom 13. Dezember 2012 (SächsGVBl. S. 725, 728) |
| SächsGemO | Gemeindeordnung für den Freistaat Sachsen vom 21. April 1993 (SächsGVBl. S. 301), geändert durch Art. 14 des Gesetzes vom 27. Januar 2012 (SächsGVBl. S. 130, 140), geändert durch Art. 2 des Gesetzes vom 18. Oktober 2012 (SächsGVBl. S. 562, 563), zuletzt geändert durch Art. 1 des Gesetz vom 28. März 2013 (SächsGVBl. S. 158) |
| SächsHSFG | Gesetz über die Freiheit der Hochschulen im Freistaat Sachsen (Sächsisches Hochschulfreiheitsgesetz) in der Fassung der Bekanntmachung vom 15. Januar 2013 (SächsGVBl. Bl.-Nr. 1 S. 3 Fsn-Nr.: 711-8/3 - Fassung gültig ab: 1. Januar 2013) (früher SächsHSG) |
| SächsJG | Gesetz über die Justiz im Freistaat Sachsen (Sächsisches Justizgesetz) vom 24. November 2000 (SächsGVBl. S. 482, 2001 S. 704), zuletzt geändert durch Art. 1 des Gesetzes vom 14. Dezember 2012 (SächsGVBl. S. 748) |
| SächsKAG | Sächsisches Kommunalabgabengesetz vom 16. Juni 1993 (SächsGVBl. S. 502), zuletzt geändert durch Art. 6 des Gesetzes vom 18. Oktober 2012 (SächsGVBl. S. 562, 566) |
| SächsKitaG | Sächsisches Gesetz zur Förderung von Kindern in Tageseinrichtungen vom 27. November 2001 (SächsGVBl. S. 705), zuletzt geändert durch Art. 32 des Gesetzes vom 27. Januar 2012 (SächsGVBl. S. 130, 144) |
| SächsMG | Sächsisches Meldegesetz vom 21. April 1993 (SächsGVBl. S. 353), zuletzt geändert durch Art. 2 des Gesetzes vom 6. Dezember 2011 (SächsGVBl. S. 638) |
| SächsPersVG | Sächsisches Personalvertretungsgesetz vom 21. Januar 1993 (SächsGVBl. S. 29), zuletzt geändert durch Art. 10 des Gesetzes vom 27. Januar 2012 (SächsGVBl. S. 130, 139) |
| SächsPolG | Polizeigesetz des Freistaates Sachsen vom 30. Juli 1991 (SächsGVBl. S. 291), Änderung durch Art. 1 des Gesetzes vom 4. Oktober 2011 (SächsGVBl. S. 370), Art. 2 des Gesetzes vom 25. Januar 2012 (SächsGVBl. S. 54), Art. 20 des Gesetzes vom 27. Januar 2012 (SächsGVBl. S. 130, 141), zuletzt geändert durch Art. 20a des Gesetzes vom 27. Januar 2012 (SächsGVBl. S. 130, 141) |

| | |
|---|---|
| SächsStVollzG | Gesetz über den Vollzug der Freiheitsstrafe und des Strafarrests im Freistaat Sachsen (Sächsisches Strafvollzugsgesetz) vom 16. Mai 2013 (SächsGVBl. S.250) |
| SächsVerf | Verfassung des Freistaates Sachsen vom 27. Mai 1992 (SächsGVBl. S. 243), Gesetz zur Änderung der Verfassung des Freistaates Sachsen (Verfassungsänderungsgesetz) vom 11. Juli 2013 (SächsGVBl. S. 502) |
| SächsVermKatG | Gesetz über die Landesvermessung und das Liegenschaftskataster sowie die Bereitstellung von amtlichen Geobasisinformationen im Freistaat Sachsen (Sächsisches Vermessungs- und Geobasisinformationsgesetz - SächsVermGeoG) vom 29. Januar 2008 (SächsGVBl. S. 138), Änderung des Sächsischen Vermessungs- und Geobasisinformationsgesetzes, Art. 2 des Gesetzes vom 19. Mai 2010 (SächsGVBl. S. 134, 140), Gesetz zur Änderung des Sächsischen Vermessungs- und Katastergesetzes vom 19. Juni 2013 (SächsGVBl. S. 482) |
| SächsWG | Sächsisches Wassergesetz vom 23. Februar 1993 (SächsGVBl. S. 201), zuletzt geändert durch Art. 2 des Gesetzes vom 9. Juli 2007 (SächsGVBl. S. 310), Neues Sächsisches Wassergesetz vom 12. Juli 2013 (SächsGVBl. S. 503) |
| SäHO | Vorläufige Haushaltsordnung des Freistaates Sachsen vom 19. Dezember 1990 (SächsGVBl. S. 21), zuletzt geändert durch Art. 1 des Gesetzes vom 13. Dezember 2012 (SächsGVBl. S. 725) |
| SBO | Verordnung des Sächsischen Staatsministeriums für Kultus über den Besuch öffentlicher Schulen im Freistaat Sachsen (Schulbesuchsordnung) vom 12. August 1994 (SächsGVBl. S. 1565) Änderungsvorschriften: Verordnung des SMK zur Änderung der Schulbesuchsordnung vom 4. Februar 2004 (SächsGVBl. S. 66) |
| SchulG | Schulgesetz für den Freistaat Sachsen vom 3. Juli 1991 (SächsGVBl. S. 213), zuletzt geändert durch Art. 2 Abs. 10 des Gesetzes vom 19. Mai 2010 (SächsGVBl. S. 142, 144) |
| SGB I | Das Erste Buch Sozialgesetzbuch - Allgemeiner Teil - (Art. 1 des Gesetzes vom 11. Dezember 1975, BGBl I S. 3015), zuletzt geändert durch Art. 10 des Gesetzes vom 19. Oktober 2013 (BGBl. I S. 3836) |
| SGB II | Das Zweite Buch Sozialgesetzbuch - Grundsicherung für Arbeitsuchende - in der Fassung der Bekanntmachung vom 13. Mai 2011 (BGBl. I S. 850, 2094), zuletzt geändert durch Art. 1 des Gesetzes vom 7. Mai 2013 (BGBl. I S. 1167) |

| | |
|---|---|
| SGB V | Das Fünfte Buch Sozialgesetzbuch - Gesetzliche Krankenversicherung - (Art. 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477, 2482), zuletzt geändert durch Art. 3 des Gesetzes vom 7. August 2013 (BGBl. I S. 3108) |
| SGB VIII | Das Achte Buch Sozialgesetzbuch - Kinder und Jugendhilfe - in der Fassung der Bekanntmachung vom 11. September 2012 (BGBl. I S. 2022), zuletzt geändert durch Art. 1 des Gesetzes vom 29. August 2013 (BGBl. I S. 3464) |
| SGB X | Das Zehnte Buch Sozialgesetzbuch - Sozialverwaltungsverfahren und Sozialdatenschutz - in der Fassung der Bekanntmachung vom 18. Januar 2001 (BGBl. I S. 130), zuletzt geändert durch Art. 6 des Gesetzes vom 25. Juli 2013 (BGBl. I S. 2749) |
| SGB XI | Das Elfte Buch Sozialgesetzbuch - Soziale Pflegeversicherung - (Art. 1 des Gesetzes vom 26. Mai 1994, BGBl. I S. 1014, 1015), zuletzt geändert durch Art. 2a des Gesetzes vom 15. Juli 2013 (BGBl. I S. 2423) |
| SGB XII | Das Zwölfte Buch Sozialgesetzbuch - Sozialhilfe - (Art. 1 des Gesetzes vom 27. Dezember 2003, BGBl. I S. 3022, 3023), zuletzt geändert durch Art. 1 des Gesetzes vom 1. Oktober 2013 (BGBl. I S. 3733) |
| StGB | Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Art. 5 Abs. 18 des Gesetzes vom 10. Oktober 2013 (BGBl. I S. 3799) |
| StPO | Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Art. 5 Abs. 4 des Gesetzes vom 10. Oktober 2013 (BGBl. I S. 3799) |
| StVG | Straßenverkehrsgesetz in der Fassung der Bekanntmachung vom 5. März 2003 (BGBl. I S. 310, 919), zuletzt geändert durch Art. 1 des Gesetzes vom 28. August 2013 (BGBl. I S. 3313) |
| TKG | Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Art. 4 Abs. 108 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) |
| TMG | Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), zuletzt geändert durch Art. 1 des Gesetzes vom 31. Mai 2010 (BGBl. I S. 692) |

| | |
|---|---|
| VersammlG | Versammlungsgesetz in der Fassung der Bekanntmachung vom 15. November 1978 (BGBl. I S. 1789), zuletzt geändert durch Art. 2 des Gesetzes vom 8. Dezember 2008 (BGBl. I S. 2366) |
| VwGO | Verwaltungsgerichtsordnung in der Fassung der Bekanntmachung vom 19. März 1991 (BGBl. I S. 686), geändert durch Art. 5 des Gesetzes vom 10. Oktober 2013 (BGBl. I S. 3786) |
| 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) |
| VwV Informations-Sicherheit | Verwaltungsvorschrift der Sächsischen Staatsregierung zur Gewährleistung der Informationssicherheit in der Landesverwaltung vom 7. September 2011 (SächsABl. S. 1294) |
| VwVPersAktenB | Verwaltungsvorschrift des SMI über die Führung und Verwaltung von Personalakten der Beamten (Verwaltungsvorschrift Personalakten Beamte) vom 11. Dezember 1998 (SächsABl. 1999 S. 10) |
| ZensG 2011 | Zensusgesetz 2011 vom 8. Juli 2009 (BGBl. I S. 1781) |

*Sonstiges*

| | |
|---|---|
| AG | Amtsgericht |
| ARGE | Arbeitsgemeinschaft nach SGB II |
| BfDI | Bundesbeauftragter für den Datenschutz und die Informationsfreiheit |
| BGBl. | Bundesgesetzblatt |
| BGH | Bundesgerichtshof |
| BKA | Bundeskriminalamt |
| BMAS | Bundesministerium für Arbeit und Soziales |
| BMF | Bundesministerium der Finanzen |
| BMG | Bundesministerium für Gesundheit |
| BMI | Bundesministerium des Innern |

| | |
|---|---|
| BMJ | Bundesministerium der Justiz |
| BMWi | Bundesministerium für Wirtschaft und Technologie |
| 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 |
| BVerwG | Bundesverwaltungsgericht |
| BVerwGE | Amtliche Sammlung der Entscheidungen des Bundesverwaltungsgerichts |
| DAAD | Deutscher Akademischer Austausch Dienst |
| DSK | Datenschutzkonferenz (halbjährlich stattfindende Konferenz der Datenschutzbeauftragten des Bundes und der Länder) |
| DuD | Zeitschrift Datenschutz und Datensicherheit |
| DVBl. | Deutsches Verwaltungsblatt |
| EG | Europäische Gemeinschaft |
| ESF | Europäischer Sozialfonds für Deutschland |
| EU | Europäische Union |
| EuGH | Europäischer Gerichtshof |
| EuroPriSe | European Privacy Seal - Europäisches Datenschutz-Gütesiegel |
| EWR | Europäischer Wirtschaftsraum |
| FAZ | Frankfurter Allgemeine Zeitung |
| GEZ | Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten |

| | |
|---|---|
| GmbH | Gesellschaft mit beschränkter Haftung |
| IHK | Industrie- und Handelskammer |
| IVO | Vorgangsbearbeitungssystem der Polizei |
| 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 |
| LT-Drs. | Landtags-Drucksache |
| MdEP | Mitglied des Europäischen Parlaments |
| MDK | Medizinischer Dienst der Krankenversicherung |
| MDR | Mitteldeutscher Rundfunk |
| m. w. N. | mit weiteren Nachweisen |
| NJoZ | Neue Juristische Online-Zeitschrift |
| NJW | Neue Juristische Wochenschrift |
| NVwZ | Neue Zeitschrift für Verwaltungsrecht |
| OLG | Oberlandesgericht |
| OSCI | Online Services Computer Interface |
| OVG | Sächsisches Oberverwaltungsgericht |
| PASS | Polizeiliches Auskunftssystem Sachsen |
| PD | Polizeidirektion |

| | |
|---|---|
| SächsABl. | Sächsisches Amtsblatt |
| GVBl. | Sächsisches Gesetz- und Verordnungsblatt |
| SAB | Sächsische Aufbaubank |
| SAKD | Sächsische Anstalt für kommunale Datenverarbeitung |
| SG | Sozialgericht |
| SIB | Staatsbetrieb Sächsisches Immobilien- und Baumanagement |
| SID | Staatsbetrieb Sächsische Informatik Dienste |
| SK | Sächsische Staatskanzlei |
| SMF | Sächsisches Staatsministerium der Finanzen |
| SMI | Sächsisches Staatsministerium des Innern |
| SMJus | Sächsisches Staatsministerium der Justiz und für Europa |
| 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 |
| StaLa | Statistisches Landesamt des Freistaates Sachsen |
| SVN | Sächsisches Verwaltungsnetz |
| ULD | Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein |
| VwV | Verwaltungsvorschrift |
| WP | Artikel-29-Datenschutzgruppe |

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 Einleitung

Kurz nach Ende des Berichtszeitraums gewann das Thema Datenschutz durch die Snowden-Affäre ungeahnten Aufwind. Durch die Veröffentlichungen wurden die Möglichkeiten und das Ausmaß einer Überwachung deutlich, die selbst kritische Stimmen so nicht vermutet hatten. Das Spektrum der Reaktionen reichte von Unbesorgtheit (das berühmte „Ich habe ja nichts zu verbergen“) über Verzagtheit („man kann ja sowieso nichts mehr machen“), Abwälzen der Verantwortung („Jeder soll selbst für seinen Schutz sorgen“) bis hin zur generellen Kampfansage an Geheimdienste. Das Gute an dem Skandal ist meiner Meinung nach das bessere Bild, das wir alle bekommen von den Möglichkeiten der Auswertung in einer Informationsgesellschaft. Auch wenn hier die Geheimdienste die Protagonisten sind, ist die Profilbildung mit Hilfe der Daten, die wir täglich gewollt und ungewollt erzeugen, nicht nur auf sie beschränkt, sondern findet in allen Lebensbereichen statt. Moderne Stromzähler ermöglichen ein Bild des Einsatzes unserer Hausgeräte (14.12), Besucherstatistiken helfen bei der Analyse der Nutzung von Internetseiten (14.1), ganz zu schweigen von Funkzellenabfragen, die ein wichtiges Thema in der politischen Auseinandersetzung im Berichtszeitraum waren (8.3). Nicht alles ist unzulässig, vieles ist nützlich bei der Erledigung von Aufgaben der öffentlichen Stellen. Aber alles ist zu prüfen, damit wir einen Weg finden, auch unter den Bedingungen und Möglichkeiten moderner Informationsverarbeitung die grundrechtlich verbürgte Selbstbestimmung des Menschen zu sichern. Das hat sowohl im Detail im täglichen Verwaltungsvollzug zu geschehen als auch in den grundsätzlichen Zielbestimmungen der Politik. Beides ist wichtig und nicht zu vernachlässigen. Dies kann nur im Zusammenspiel aller Beteiligten geschehen - Bürger, Politiker, Unternehmer, Journalisten, Verwaltungsmitarbeiter, Aufsichtsbehörden. Einen Eindruck für die Arbeit des Sächsischen Datenschutzbeauftragten vermittelt der aktuelle Tätigkeitsbericht, den ich unter dieses Motto stellen möchte:

“*I cannot do everything, but I can do something. And because I cannot do everything, I will not refuse to do the something that I can do.*“ (Edward Everett Hale)

Bisher bin ich in den von mir verantworteten Tätigkeitsberichten für den öffentlichen Bereich nicht auf die Personalsituation meiner Behörde eingegangen. Mittlerweile zwingt jedoch der Arbeitsanfall der Behörde dazu. Besonders im privatwirtschaftlichen, aber auch im öffentlichen Bereich ist das Pensum so angewachsen, dass Wünschenswertes oft auf der Strecke bleibt, Notwendiges am Belastungsanschlag erledigt wird. Das ist die Kehrseite einer erfreulich gestiegenen Aufmerksamkeit für den Datenschutz innerhalb der Gesellschaft, die natürlich zu deutlich mehr Anfragen nicht nur von Bür-

gern, sondern auch von Unternehmen und Verwaltungen führt. Wenn die Europäische Datenschutzreform zu einer neuen Grundverordnung führt (3.1), ist der Aufgabenzuwachs nicht ohne eine Personalsteigerung leistbar. Dann wird sich zeigen, ob die Absichtserklärungen auch Hand und Fuß haben.

Dem Präsidenten des Sächsischen Landtages und der Verwaltung möchte ich an dieser Stelle für die langjährige Zusammenarbeit danken. Oft wird unterschätzt, wie wichtig und notwendig der reibungslose Ablauf von Verwaltungsvorgängen für die Arbeit einer Dienststelle ist. Die in der Verfassung vorgesehene Verknüpfung mit dem Sächsischen Landtag ist auch in dieser Hinsicht für den Sächsischen Datenschutzbeauftragten ein Gewinn.

## 1.2 Behördliche Datenschutzbeauftragte

Bei meinen Kontrollen muss ich oft feststellen, dass verantwortliche Stellen ihrer Pflicht zur Unterstützung des behördlichen Datenschutzbeauftragten nach § 11 Abs. 2 Satz 4 SächsDSG nicht in ausreichendem Maße nachkommen. Dies erfordert zunächst, für die erforderliche sachliche, personelle und finanzielle Ausstattung zu sorgen, die notwendigen organisatorischen Maßnahmen zu treffen und dem Datenschutzbeauftragten die Teilnahme an Fortbildungsveranstaltungen und am Erfahrungsaustausch mit anderen Datenschutzbeauftragten zu ermöglichen. Dies bedeutet aber auch, dass der Datenschutzbeauftragte angemessen von seinen bisherigen Aufgaben freizustellen ist.

Es ist aber ebenfalls sicherzustellen, dass der Datenschutzbeauftragte seiner Verschwiegenheitspflicht gemäß § 11 Abs. 5 SächsDSG nachkommen kann. Dies bedeutet zum Beispiel, dass zu gewährleisten ist, dass seine Gespräche nicht von Dritten mitgehört werden können. Dies wird regelmäßig nur durch die Bereitstellung eines Einzelbüros (in dem er selbstverständlich auch seine übrigen dienstlichen Aufgaben wahrnehmen kann) zu realisieren sein. Weiterhin ist es unzulässig, Verkehrs- oder gar Inhaltsdaten der Kommunikation des Datenschutzbeauftragten zu kontrollieren. Dies ist bereits bei den jeweiligen Dienstvereinbarungen oder -anweisungen zu berücksichtigen.

Erwähnen möchte ich hier als positives Beispiel eine Polizeidienststelle, die den behördlichen Datenschutzbeauftragten nach Abschluss von Umbaumaßnahmen vorrangig bei der Vergabe eines Einzelzimmers berücksichtigt hat und durch die Zuweisung eines Diensthandys eine Trennung zwischen seinem Hauptamt und seiner Tätigkeit als behördlicher Datenschutzbeauftragter gewährleistet.

# 2 Parlament

In diesem Jahr nicht belegt.

# 3 Europäische Union / Europäische Gemeinschaft

## 3.1 Vorschläge für eine Datenschutz-Grundverordnung und eine Datenschutz-Richtlinie

Am 25. Januar 2012 legte die EU-Kommission zwei Vorschläge für neue, umfassende Rechtsgrundlagen für den Datenschutz in den Mitgliedsstaaten der EU vor.

Mit der Datenschutz-Grundverordnung (GrundVO-E) soll eine unmittelbar in allen Mitgliedsstaaten geltende Rechtsgrundlage für die Verarbeitung personenbezogener Daten und die übrigen Aspekte des Datenschutzes (z. B. Rechte des Betroffenen, interne Datenschutzbeauftragte, Datenschutzaufsichtsbehörden) geschaffen werden. Sie würde auf die Datenverarbeitung der privaten und der meisten öffentlichen Stellen mit Ausnahme der polizeilichen und justiziellen Stellen anwendbar sein; grundsätzlich nicht anwendbar wäre sie auf die der Union nicht übertragenen Rechtsmaterien wie z. B. auf Verarbeitungen zu Zwecken der nationalen Sicherheit (z. B. in den Nachrichtendiensten). So soll u. a. etwa ein „Recht auf Vergessen“ (Art. 17 GrundVO-E) geschaffen, die Übertragbarkeit der Daten von einem zum anderen Anbieter (Art. 18 GrundVO-E) ermöglicht, der Datenschutz durch Technik u. datenschutzfreundliche Voreinstellungen (Art. 23 GrundVO-E) vorgeschrieben, Dokumentationspflichten (Art. 28 GrundVO-E) gestärkt, das sog. Marktortprinzip (Art. 25 GrundVO-E), wonach das Recht desjenigen Ortes gilt, an dem Geschäfte gemacht werden, verankert, die technischen Standards der Datenverarbeitung erhöht und Meldepflichten bei Verletzungen des Datenschutzes (Art. 30 ff. GrundVO-E) eingeführt, die Aufsichtsbehörden (Art. 46 ff. GrundVO-E) gestärkt, das „One-stop-shop“-Prinzip, wonach bei grenzüberschreitenden Sachverhalten grundsätzlich nur eine Datenschutzbehörde zuständig ist (Art. 51 GrundVO-E), eingeführt und die Zusammenarbeit der Datenschutzaufsichtsbehörden durch Amtshilfe und ein besonderes Verfahren der Zusammenarbeit (Art. 55 ff. GrundVO-E) verbessert werden. Damit zielt insbesondere die GrundVO erklärtermaßen auf eine Erleichterung der digitalen Wirtschaft, die Erhaltung der Kontrolle über die eigenen Daten sowie die Erhöhung der rechtlichen und praktischen Sicherheit für Wirtschaft und Staat.

Mit der Datenschutz-Richtlinie (RL-E) soll ein auch für die innerstaatliche Verarbeitung von personenbezogenen Daten im polizeilichen und justiziellen Bereich (ehem. „Dritte Säule“) verbindlicher Rechtsrahmen für den nationalen Gesetzgeber geschaffen werden.

Dieser soll die nationalen Regelungen in diesem Bereich auf das Niveau der „alten“ Richtlinie 95/46/EG von 1995 heben.

Beide Entwürfe, die auf jahrelange Vorarbeiten der Kommission zurückgehen, stellen eine Reaktion auf deren mittlerweile offensichtlichen Defizite der geltenden Richtlinie 95/46/EG von 1995 dar. Sie sollen für die ca. 500 Mio. Einwohner der Union eine „konsequente, zusammenhängende, durchsetzbare Regelung“, die den technischen (Internet etc.) und gesellschaftlichen (Soziale Netzwerke etc.) Entwicklungen seit 1995 Rechnung trägt, bieten. Sie bezwecken übereinstimmend einerseits den Schutz der Grundrechte und Grundfreiheiten bei der Verarbeitung personenbezogener Daten, andererseits die Förderung des freien Verkehrs solcher Daten in der Union (Art. 1 GrundVO-E, Art. 1 RL-E).

Beide Entwürfe werden derzeit im ordentlichen Gesetzgebungsverfahren im Europäischen Parlament und im Rat, d. h. den Regierungen der Mitgliedsstaaten, intensiv diskutiert. Der im Europäischen Parlament für den Verordnungsentwurf zuständige Berichterstatter Jan Phillip Albrecht (GRÜNE), Mitglied des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (LIBE), hat am 17. Dezember 2012 einen ersten „Entwurf einer legislativen Entschließung des Europäischen Parlaments“ vorgelegt. Entsprechendes tat der für den Richtlinienentwurf zuständige Berichterstatter. Die Artikel-29-Gruppe - die europäische Datenschutzkonferenz - hatte bereits am 23. März 2013 zu den Reformvorschlägen im Bereich des Datenschutzes Stellung genommen (WP Dokument Nr. 191). Mittlerweile hat der LIBE-Ausschuss aufgrund der außerordentlich hohen Anzahl von über 4000 Änderungsanträgen seine für Ende Mai 2013 avisierte Abstimmung noch einmal verschoben. Erst im Anschluss daran können die Verhandlungen mit dem Rat aufgenommen werden, der in seiner Arbeitsgruppe „Informationsaustausch und Datenschutz“ (DAPIX) bisher lediglich etwa die Hälfte der 91 Artikel des GrundVO-E abschließend erörtert hat. Die Absicht der derzeitigen (1. Halbjahr 2013) irischen Ratspräsidentschaft, einen Ratsbeschluss noch im Juni 2013 herbeizuführen, lässt sich daher nicht mehr aufrechterhalten. Parlament und Rat werden wohl erst unter der im 2. Halbjahr 2013 folgenden litauischen Präsidentschaft die Voraussetzungen für die abschließenden Gespräche mit der Kommission (sogenannter Trilog) schaffen können. Diese bereits heute absehbare Dauer des Gesetzgebungsverfahrens zeigt einmal mehr, welchen hohen Stellenwert die neuen Rechtsgrundlagen für den Datenschutz haben werden. Wie künftig die Rechte der Betroffenen, die Grundsätze der Datenverarbeitung, insbesondere die Datenübermittlung in unsichere Drittstaaten, die unternehmens- oder behördeninterne Gewährleistung des Datenschutzes, die technischen Standards oder die externe Kontrolle durch Aufsichtsbehörden gestaltet werden, ist ersichtlich für alle Beteiligten nichts Nebensächliches oder Randständiges, sondern eine wesentliche Voraus-

setzung künftigen Handelns. Dabei zeigt sich, dass es bei der Verarbeitung personenbezogener Daten im Kern um das „Öl der Informationsgesellschaft und -wirtschaft“ (Facebook, Google, Sicherheitsbehörden etc.) und mithin um enorm viel Geld und Macht geht.

Wiewohl derzeit zu beiden Entwürfen noch nicht abschließend Stellung genommen werden kann, so zeichnet sich doch für die sächsischen öffentlichen Stellen vom Sächsischen Landtag bis zu den Kommunen und Universitäten Beruhigendes ab. Beide Entwürfe überantworten die Datenverarbeitung im öffentlichen Sektor weitgehend dem nationalen Gesetzgeber:

1. Zunächst fände die GrundVO von vornherein keine Anwendung auf Verarbeitungen „im Rahmen einer Tätigkeit, die nicht in den Geltungsbereich des Unionsrechts fällt, etwa im Bereich der nationalen Sicherheit“, Art. 2 Abs. 2 Buchst. a GrundVO-E. Maßgebend für diese Datenverarbeitungen (z. B. des LfV Sachsen) wäre weiterhin einzig der nationale Rechtsrahmen; zuständig für die Sachsen betreffende Gesetzgebung bliebe ausschließlich der Sächsische Landtag.

2. Sodann fände die GrundVO auch keine Anwendung auf Verarbeitungen „zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder zur Vollstreckung strafrechtlicher Sanktionen durch die zuständigen Behörden“, Art. 2 Abs. 2 Buchst. e GrundVO-E. Maßgebend für diese Datenverarbeitungen (z. B. der Polizei, der Staatsanwaltschaften oder der Justizvollzugsbehörden) wäre die künftige bereichsspezifische „Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr“; zuständig für die Sachsen betreffende Gesetzgebung zur Umsetzung der Richtlinie bliebe auch hier ausschließlich der Sächsische Landtag.

3. Des Weiteren - und hier läge der Schwerpunkt der Gesetzgebung für den öffentlichen Sektor - überantwortete die GrundVO die Rechtsgrundlagen für Datenverarbeitungen „für die Wahrnehmung einer Aufgabe (...), die im öffentlichen Interesse liegt oder in Ausübung hoheitlicher Gewalt erfolgt“ entweder dem „Unionsrecht“ oder dem „Recht des Mitgliedsstaats, dem der für die Verarbeitung Verantwortliche unterliegt“, Art. 6 Abs. 1 Buchst. e i. V. m. Art. 6 Abs. 3 S. 1 GrundVO-E. Bisher wurde die Kompetenz der EU eher als auf wenige Bereiche beschränkt angesehen; nach dem Vertrag von Lissabon gehen EU-Kommission und EuGH allerdings von einer größeren Geltungsbreite des Unionsrechts aus. Bei einem engen Verständnis bildeten auch künftig eigenständige einzelstaatliche, d. h. deutsche, Regelungen die Rechts-

grundlage für Datenverarbeitungen zu öffentlichen Zwecken. Sächsische öffentliche Stellen würden damit auch künftig personenbezogene Daten in der Regel aufgrund einer deutschen staatlichen, kommunalen, universitären, kirchlichen oder anderen öffentlich-rechtlichen Rechtsvorschrift verarbeiten. Bei einem weiteren Verständnis müssten auch diese Rechtsvorschriften sich zumindest im Rahmen des Unionsrechts halten (so auch ausdrücklich der Änderungsvorschlag des Europäischen Parlaments). Die Gesetzgebungszuständigkeit des Sächsischen Landtages bliebe in beiden Fällen weitgehend unberührt.

4. Schließlich überantwortete die GrundVO bestimmte Bereiche „besonderer Datenverarbeitungssituationen“ ausschließlich dem nationalen Gesetzgeber. Dabei handelte es sich um die Bereiche der

   - Verarbeitung personenbezogener Daten allein zu journalistischen, künstlerischen oder literarischen Zwecken (Art. 80 GrundVO-E), d. h. den Mediendatenschutz,

   - Verarbeitung von Gesundheitsdaten (Art. 81 GrundVO-E), d. h. den Gesundheitsdatenschutz,

   - Datenverarbeitung im Beschäftigungskontext (Art. 82 GrundVO-E), d. h. den Arbeitnehmerdatenschutz,

   - Datenverarbeitung im Bereich der sozialen Sicherheit nach Art. 82a GrundVO-E (Albrecht MdEP), d. h. den Sozialdatenschutz,

   - Datenverarbeitung durch die Aufsichtsbehörden nach Art. 84 GrundVO-E, d. h. die Untersuchungsbefugnisse der Datenschutzbeauftragten, sowie der

   - Datenverarbeitung durch Kirchen und religiöse Vereinigungen oder Gemeinschaften nach Art. 85 GrundVO-E, d. h. den kirchlichen Datenschutz.

   Die entsprechende nationale Gesetzgebung müsste sich i. d. R. lediglich im Rahmen der GrundVO halten. Inhaltlichen Änderungsbedarf durch das Inkrafttreten der GrundVO kann ich derzeit in diesen Bereichen nur vereinzelt erkennen. Zuständig für die Sachsen betreffende Gesetzgebung in diesen „besonderen Datenverarbeitungssituationen“ bliebe ausschließlich der Sächsische Landtag.

Insgesamt kann ich feststellen, dass auch Sachsen im öffentlichen Sektor einerseits erhebliche künftige Gestaltungsbefugnisse verbleiben und andererseits wesentliche inhaltliche Änderungen an den bestehenden Rechtsvorschriften nicht zu erwarten sind. Allerdings muss umfassend die Kompatibilität der Rechtsvorschriften mit der GrundVO bzw.

der bereichsspezifischen Richtlinie geprüft werden. Gleichwohl werden sowohl die GrundVO als auch die RL zu einer Anhebung des Datenschutzniveaus in der EU führen - ein gutes Ergebnis, das wohl weniger für Deutschland als für andere Mitgliedsstaaten Änderungen mit sich bringen wird.

Mit der Staatsregierung stehe ich, was deren Positionierung im Bundesrat angeht, in Kontakt. Auf ihre Unterstützung bei der Modernisierung des Datenschutzes in Europa im Interesse der Bürgerinnen und Bürger Sachsens hoffe ich auch künftig.

# 4 Medien

In diesem Jahr nicht belegt.

# 5 Inneres

## 5.1 Personalwesen

### 5.1.1 Vorgesetzter sammelt Fehlverhalten seiner Mitarbeiter in eigener Akte

Der Petent, ein Polizeibeamter, informierte mich darüber, dass sein Fach- und Dienstvorgesetzter persönlich eine Akte über sein angebliches Fehlverhalten führe. Die von mir um Stellungnahme und Löschung gebetene Polizeibehörde bestätigte das Vorhandensein einer derartigen Akte, ging jedoch weiterhin von der Zulässigkeit der damit einhergehenden Datenverarbeitung aus und teilte mit, dass die zu dem Betroffenen angelegte Papierakte auszugsweise Kopien zu Dienstaufsichtsbeschwerden sowie Bußgeldverfahren von unterschiedlichen Sachbearbeitern enthalte. Nach einer von mir vor Ort durchgeführten Kontrolle wurde mir dann entgegengehalten, die Führung der Akte sei gemäß § 37 Abs. 6 SächsDSG zu Dienst- und Fachaufsichtszwecken erforderlich und rechtmäßig.

Ich beanstandete die Unterlagensammlung, da Beschäftigtendaten nur verarbeitet werden dürfen, wenn und soweit dies nach den in § 37 Abs. 1 SächsDSG genannten Voraussetzungen erforderlich ist. Sofern Dienstaufsichtsbeschwerden nach Prüfung zu Maßnahmen der Dienstaufsicht geführt haben, sind die entsprechenden Unterlagen gemäß Nr. A I 2 j) VwV PersAktenB als - ausschließlich durch das Personalreferat zu führende - Personalaktendaten, anderenfalls als Sachaktendaten zu behandeln, die nach Abschluss einer dienstrechtlichen Prüfung gemäß § 20 Abs. 1 Nr. 2 SächsDSG wegen fehlender Erforderlichkeit zu löschen sind. Entsprechendes gilt für die bei der Dienststelle bekannten Bußgeldverfahren gegen den Beamten. Eine willkürliche Zusammenführung von belastenden Fehlverhaltensvorgängen abseits der geregelten personalakten- und disziplinarrechtlichen Verfahrensvorschriften ist hingegen gesetzlich nicht vorgesehen und kann daher auch keine erforderliche Datenverarbeitung gemäß § 37 SächsDSG darstellen. Weitgehend unklar ist bei meiner Kontrolle auch geblieben, welchem dienstlichen Zweck das Dossier eigentlich dienen sollte. Demgegenüber belasteten die zusammengestellten Informationen und das Anlegen der Akte ohne Kenntnis des Betroffenen - auch wenn diese „nur“ als Hintergrundinformationen gedient haben mochten - den Beschäftigten in unangemessener Weise. Wegen des einseitigen Inhalts konnten die Informationen letztendlich auch nicht als (erlaubte) Vorgesetztenaufzeichnungen zur Personalführung und für Beurteilungszwecke gelten. Auch die Bezugnahme auf § 37 Abs. 6 SächsDSG entsprang einer rechtlichen Fehleinschätzung. Die Vorschrift stellt keine Befugnis zur Datenverarbeitung dar, sondern konkretisiert die erlaubte Datenverarbeitung einschränkend in Bezug auf deren Zweckbindung.

Auch aufgrund der Weigerung, die Daten in der unerlaubten Beschäftigtenakte zu löschen, konnte ich von der Möglichkeit, von einer Beanstandung abzusehen, keinen Gebrauch machen. Immerhin wurde mir nach der ausgesprochenen Beanstandung mitgeteilt, dass man nun ebenfalls von einer Rechtswidrigkeit der Datenverarbeitung ausgehe und bestätigte die vorgenommene Löschung sämtlicher Daten der Sonderakte.

### 5.1.2 Bewerbungen per E-Mail

Im Berichtszeitraum stellte ich fest, dass in Stellenausschreibungen sächsischer Staatsministerien die Bewerber regelmäßig darüber informiert wurden, dass sie ihre Bewerbungsunterlagen auch per E-Mail an das jeweilige Staatsministerium übersenden könnten.

Die Behörden befördern auf diese Weise, dass Bewerber die Beschäftigtendaten, die seitens der Behörde erhoben werden - und in vielen Fällen wird es sich um besonders schutzwürdige Daten handeln (§ 4 Abs. 2 SächsDSG) -, ohne ein gesichertes Mindestmaß an Vertraulichkeit, beispielsweise durch Verschlüsselung, über das Internet übermitteln. Diesen unkritischen Umgang mit dem Kommunikationsmedium E-Mail sehe ich aus datenschutzrechtlicher Sicht zunehmend kritisch. Die versandten Dokumente sind einer Vielzahl von Angriffsmöglichkeiten ausgesetzt, die deren Vertraulichkeit und Integrität gefährden könnten. Der ungesicherte E-Mail-Versand kann mit dem Verschicken einer Postkarte verglichen werden. Da die E-Mails eingesehen, verändert oder verfälscht werden können, sollte ein ungesicherter Einsatz von E-Mails in Bewerbungsverfahren generell nicht angeboten werden. Der Empfang von schutzwürdigen personenbezogenen Informationen via E-Mail sollte unter Nutzung von Verschlüsselungssoftware erfolgen.

Ich bat die betreffenden Staatsministerien um Stellungnahme dazu. Die Behörden teilten mir in ihren Antworten mit, dass sie meine Bedenken nicht teilen würden und an der Möglichkeit, die Unterlagen über unverschlüsselte E-Mail-Kommunikation empfangen zu können, festhalten wollen. Ein Geschäftsbereich teilte mir zudem mit, dass die Bewerbung per E-Mail ja nicht verlangt werde. Sofern der Bewerber sich für den Postweg entscheiden würde, entstünden ihm deswegen keine Nachteile. Auf der Grundlage dieses „Wahlrechts“ würde das Recht auf informationelle Selbstbestimmung der Bewerber nicht eingeschränkt. Zudem sei die Möglichkeit zur Übermittlung der Bewerbungsunterlagen per E-Mail erst auf Veranlassung von Bewerbern wegen der Kostenvorteile für diese und im Sinne einer zeitgemäßen bürgernahen Verwaltung eingerichtet worden.

Der Umstand, dass Bewerber Unterlagen an Behörden-E-Mail-Zugänge schicken, kann nicht ausgeschlossen werden. Allerdings kommt die Nennung der E-Mail-Anschrift in der Stellenausschreibung, ohne Hinweis, dass diese lediglich für Rückfragen gedacht ist, einer Aufforderung gleich, die Bewerbungsunterlagen elektronisch einzureichen. Dabei haben sächsische öffentliche Stellen bei Anbietung eines elektronischen Zugangs für den Empfang personenbezogener Daten technisch-organisatorische Maßnahmen zu treffen, die angemessen sind und dem jeweiligen Stand der Technik entsprechen, § 9 SächsDSG. Sofern ein Zugang für die elektronische Übermittlung von Beschäftigtendaten eingerichtet wird, entspricht es einem angemessenen technischen Stand, auch einen verschlüsselten Zugang zum vertraulichen Empfang der Daten anzubieten. Anderenfalls sollte auf die Entgegennahme elektronischer Bewerbungen verzichtet werden bzw. wäre dies explizit in der Stellenausschreibung auszuschließen. Den Beschwichtigungsversuch, dass es ja Entscheidung des Bewerbers selbst sei, ggf. elektronisch und unverschlüsselt zu kommunizieren, kann ich angesichts der gesetzlichen Pflicht, angemessene Datenschutzvorkehrungen zu treffen, nicht nachvollziehen. Dies auch umso weniger, da der Freistaat Sachsen selbst den Behörden mit seinen E-Government-Basiskomponenten seit Jahren Verschlüsselungslösungen anbietet (http://www.egovernment.sachsen.de/55.htm). Die Angebote werden schlicht nicht umgesetzt. Das Secure Mail Gateway ermöglicht den verschlüsselten Austausch von Nachrichten (ohne durchgehende Ende-zu-Ende-Verschlüsselung). Darüber hinaus existiert eine vollverschlüsselte OSCI-Lösung, welche eine Ende-zu-Ende-Verschlüsselung unterstützt. Beide Varianten sind in verschiedenen Ausbaustufen realisierbar und können in die beim Freistaat gängigen Microsoft-Anwendungen integriert werden. Die einfachste Lösung wäre die Einrichtung eines Postfachs beim Secure Mail Gateway und so die Schaffung eines gesicherten Zugangs für Bewerber. Obwohl dies keine Ende-zu-Ende-Verschlüsselung bedeuten würde, wird auch diese Lösung von mir in Beratungen empfohlen, da das Secure Mail Gateway in gesicherter Umgebung platziert ist und der Transport der Kommunikationsinhalte verschlüsselt erfolgt. Damit wird im Vergleich zu einer unverschlüsselt versandten E-Mail ein deutlich höheres Schutzniveau erreicht. Die Handhabung ist sowohl sender- als auch empfängerseitig praktikabel handhabbar und erfordert keine administrative Unterstützung.

E-Government und Bürgernähe muss mit Datenschutz und Datensicherheit einhergehen!

### 5.1.3 Datenschutz bei Telearbeit

Der Beschäftigte eines Landkreises nutzte ein in seiner Wohnung befindliches Arbeitszimmer für dienstliche Telearbeit und fragte, inwieweit eine für Kontrollzwecke zur Abrechnung der Betriebskosten eingesetzte Kommission des Arbeitgebers durch das Be-

treten der Wohnung seine Privatsphäre verletzen und damit gegen Regelungen des Datenschutzes verstoßen würde.

Zunächst war der Anfrage nicht zu entnehmen, ob es sich bei dem Arbeitsverhältnis um eine Neueinstellung in einem Heimarbeits-Vertragsverhältnis nach § 1 Abs. 2 Ziff. a) HAG handelte oder ob sich ein Beschäftigter später zu einer Telearbeit bereiterklärt hatte. Im ersten Fall wären auf den Arbeitsvertrag die Regelungen des Heimarbeitsgesetzes anzuwenden gewesen. Werden anfallende Betriebskosten durch den Landkreis erstattet, so kann dieser den Heimarbeitsplatz gegebenenfalls kontrollieren. Dies muss arbeitsvertraglich vereinbart werden. Damit wäre auch die Einwilligung zum Betreten der Wohnung erteilt. Bei einer bisherigen herkömmlichen Beschäftigung und einer nachträglich vereinbarten Telearbeit sind die Regelungen der Vereinbarung über Heimarbeit nach dem Personalvertretungsgesetz mitbestimmungspflichtig (§ 80 Abs. 3 Nr. 15 SächsPersVG).

Bei einem Betreten der Wohnung durch Vertreter des Arbeitgebers ohne rechtliche Grundlage oder seine freiwillig erteilte Einwilligung, wie der Beschäftigte zunächst befürchtete, wäre die Annahme der Verletzung seines allgemeinen Persönlichkeitsrechts (schon wegen der Unverletzlichkeit der Wohnung nach Art. 13 GG) gerechtfertigt. Der Beschäftigte ergänzte seinen Vortrag noch dahingehend, dass sich seine ursprüngliche Arbeitsaufgabe durch Telearbeit verändert habe. Und er sei auf der Grundlage einer neuen Dienstvereinbarung gebeten worden, eine nachträgliche Vereinbarung zur Telearbeit zu unterzeichnen.

Ich konnte dem Betroffenen mitteilen, dass eine rechtsverbindliche Änderung seines Arbeitsvertrags zur Telearbeit durch seine Unterschrift wirksam wird. Die der Änderung des Arbeitsvertrags zugrunde gelegte Dienstvereinbarung hat zu berücksichtigen, dass die Besichtigung von Heimarbeitsplätzen, soweit sie erforderlich ist, verbindlich geregelt ist und unverhältnismäßige Eingriffe in die Privatsphäre vermieden werden. Ein unter Umständen unerwünschter Eingriff in das allgemeine Persönlichkeitsrecht des Betroffenen durch den Besuch von Vertretern des Arbeitgebers zu Hause bleibt nur aus, wenn das Angebot zur Telearbeit (eine Änderung des bestehenden Arbeitsvertrags ist nur mit seiner Einwilligung möglich) abgelehnt wird.

Allgemein gilt in Bezug auf die Einrichtung von Telearbeitsplätzen:

Datenschutzrechtliche Vorschriften stehen der Einrichtung von Heim- und Telearbeitsplätzen grundsätzlich nicht entgegen. Es sind jedoch Verschwiegenheitspflichten einzuhalten und technische und organisatorische Maßnahmen umzusetzen, die entsprechend

der Schutzwürdigkeit der zu verarbeitenden personenbezogenen Daten erforderlich und angemessen sind.

- Vor der Einführung von Heim- und Telearbeit ist ein Sicherheitskonzept zu erstellen, in dem die geeigneten Maßnahmen detailliert festgelegt werden. Der behördliche Datenschutzbeauftragte, die Personalvertretung und zuständige andere Bedienstete sind zu beteiligen.

- Bestimmte Daten sollten nicht durch Bedienstete auf Heim- und Telearbeitsplätzen verarbeitet werden. Das betrifft insbesondere Patientendaten, die der ärztlichen Schweigepflicht unterfallen, aber auch andere sensible Daten, die einem Amts- oder besonderen Berufsgeheimnis unterliegen. Werden dennoch Arbeitsplätze außerhalb der Dienststelle eingerichtet, ist ggf. im Rahmen der Vorabkontrolle nach § 10 Abs. 4 SächsDSG die Zulässigkeit der Datenverarbeitung zu prüfen.

- Technische Maßnahmen genügen regelmäßig nicht allein und sind durch angepasste personell-organisatorische Regelungen zu ergänzen.

- Neben der normativ wirkenden Dienstvereinbarung zwischen Personalrat und Dienststelle ist zusätzlich eine Einzelvereinbarung zwischen den außer Haus tätigen Bediensteten und der Dienststelle abzuschließen, um die Kontrolle und das notwendige Zutrittsrecht zu den Privaträumen des Heim- bzw. Telearbeitnehmers zu gewährleisten. Heim- und Telearbeitsplätze können nur auf Basis der Freiwilligkeit eingerichtet werden. Ein Anspruch auf Telearbeit besteht nur im Rahmen der Selbstbindung der Verwaltung.

- Der Bedienstete kann die Einwilligung zum Zutritt und zur Kontrolle jederzeit widerrufen, was zur sofortigen Beendigung des Heim- bzw. Telearbeitsverhältnisses zu führen hat.

- Bei Datenschutzverstößen durch den Bediensteten sollte die Vereinbarung seitens des Dienstherrn bzw. Arbeitgebers widerrufen werden können.

### 5.1.4 Vielzahl von Bewerberdaten im Empfängerfeld einer E-Mail - Offener E-Mail-Verteiler

Ein Betroffener wandte sich an mich und teilte mit, dass er eine E-Mail-Nachricht einer Behörde erhalten habe, bei der er sich vor einiger Zeit um eine Stelle beworben hätte. Als ehemaliger Bewerber sei er von der öffentlichen Stelle um Auskünfte, die als Datengrundlage für eine Masterarbeit einer Studentin dienen sollten, gebeten worden. In

der Empfängerzeile der Nachricht waren allerdings 386 weitere Mailadressen ehemaliger Bewerber aufgeführt.

Nach den Angaben des Betroffenen hatte sich die Behörde in ihren Hinweisen darauf festgelegt, dass „persönliche Daten nicht an Dritte weitergegeben werden“. Der ehemalige Bewerber sah in der offenen Übermittlung sowohl einen Verstoß gegen die selbst auferlegte Regel als auch gegen datenschutzgesetzliche Vorschriften und bat mich um Prüfung des Vorgangs.

Datenschutzrechtlich handelt es sich bei E-Mail-Adressen um personenbezogene Daten, § 3 Abs. 1 SächsDSG. Daten der Betroffenen, die in einem Bewerbungsverfahren erhoben worden sind, sind zudem Beschäftigtendaten gemäß § 37 Abs. 1 SächsDSG. Diese spezielle Datenverarbeitungsvorschrift des Sächsischen Datenschutzgesetzes regelt u. a., dass öffentliche Stellen Daten von Bewerbern verarbeiten dürfen, soweit dies zur Eingehung des Dienst- oder Arbeitsverhältnisses erforderlich ist oder ein Gesetz oder eine Dienstvereinbarung dies vorsieht. Bewerberdaten dürfen als Beschäftigtendaten nur unter erschwerten Voraussetzungen an natürliche Personen oder andere nicht-öffentliche Stellen übermittelt werden, § 37 Abs. 3 SächsDSG. Die gesetzlichen Voraussetzungen des Absatzes 3 hierzu waren nicht erfüllt, da weder mit einer Rechtsvorschrift die Offenbarung der E-Mail-Kontaktdaten und damit deren Übermittlung begründet werden konnte, noch die Betroffenen eingewilligt hatten. Datenschutzorganisatorisch ist jede sächsische öffentliche Stelle pflichtig, dafür Sorge zu tragen, dass bestmöglich Maßnahmen zur Gewährleistung des Datenschutzes eingehalten werden, § 9 SächsDSG. Dass daher auch keine offenen E-Mail-Verteiler mit für alle Adressaten sichtbaren E-Mail-Adressen Verwendung finden sollten, müsste man als bekannt voraussetzen.

Abgesehen davon sind überdies Daten, die vor Beginn eines Dienst- oder Arbeitsverhältnisses erhoben worden sind, unverzüglich zu löschen, sobald feststeht, dass ein Dienst- oder Arbeitsverhältnis nicht zustande kommt, § 37 Abs. 5 SächsDSG. Neben der Übermittlung der Daten des Bewerbers an andere natürliche Personen bzw. nicht-öffentliche Stellen mittels eines offenen E-Mail-Verteilers war schon bereits die weitere Speicherung und Nutzung wegen der zuvor nicht erfolgten Löschung der Daten nach Abschluss des Bewerbungsverfahrens unzulässig gewesen.

### 5.1.5 Veröffentlichung von Vertretungsplänen im Internet

Ein Lehrer bat mich um Prüfung, ob die Veröffentlichung des Vertretungsplans der Schule anlässlich eines Streiks mit der Namensnennung der Lehrer im Internet daten-

schutzrechtlich zulässig sei. Meine datenschutzrechtliche Prüfung des Vorgangs ergab, dass dies nicht der Fall war.

Bereichsspezifische gesetzliche Regelungen zur Internetnutzung im Schulbereich fehlen in Sachsen. In Bezug auf die Veröffentlichung von personenbezogenen Daten gilt deswegen das allgemeine Sächsische Datenschutzgesetz. Als öffentliche Stelle ist die Schule lediglich befugt, personenbezogene Daten zu verarbeiten, wenn die Verarbeitung zur gesetzlichen Aufgabenerfüllung erforderlich ist, §§ 12 ff. SächsDSG. Die Verarbeitung von Beschäftigtendaten, die im fünften Abschnitt bereichsspezifisch geregelt ist, ist gemäß § 37 SächsDSG zulässig, wenn sie zu Zwecken der Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes erfolgt. Eine Veröffentlichung dieser Daten ist dabei zulässig, wenn der Betroffene eingewilligt hat oder diese für die Information der Allgemeinheit oder der anderen Beschäftigten erforderlich ist und ihr keine schutzwürdigen Interessen des Betroffenen entgegenstehen, § 37 Abs. 2 SächsDSG.

Die Schule führte in ihrer Stellungnahme aus, dass die Veröffentlichung des Vertretungsplanes erforderlich gewesen sei, um eine ausreichende und rechtzeitige Unterrichtsvertretung und Beaufsichtigung zu gewährleisten.

Angaben wie Vorname, Nachname, dienstliche E-Mail-Adresse, Dienstanschrift etc. sind Amtsträgerdaten. Amtsträgerdaten sind nicht ohne weiteres schutzwürdig (vgl. dazu BVerwG, Beschluss vom 12. März 2008 - 2 B 131/07 zur Veröffentlichung einer E-Mail-Adresse eines Beamten auf der Internetseite einer Behörde). Allerdings wird beamten- und arbeitsrechtlich Fürsorgepflichten Rechnung zu tragen und z. B. dann von einer Veröffentlichung abzusehen sein, wenn der Beschäftigte durch die Veröffentlichung einer Gefährdung ausgesetzt wird.

Personenbezogene Daten können im Internet ohne jede Zweckbindung weltweit abgerufen, verändert oder für andere Zwecke genutzt werden, ohne dass der Einzelne darauf Einfluss nehmen kann. Vor diesem Hintergrund sah ich in der Veröffentlichung personenbezogener Daten im Zusammenhang mit Streikvorhaben und Vertretungsplänen eine Verletzung schutzwürdiger Interessen der Betroffenen, da z. B. Rückschlüsse auf streikwillige oder nicht streikende Lehrkräfte hätten gezogen werden können. Das gilt auch, wenn von der Schule nur Namenskürzel veröffentlicht werden, da eine Personenbeziehbarkeit bleibt.

Als vertretbare Lösung, um das Informationsbedürfnis und die Organisationsanforderungen grundrechtsschonend zu erfüllen, schlug ich der Schule vor, den Zugang zu den Vertretungsplänen mit Passwortzugang zu beschränken. Auf diese Weise wären nur noch Lehrer und Schüler der Schule in der Lage gewesen, auf die Daten zuzugreifen.

Die Schule teilte mir letztendlich dann auch mit, dass die Vertretungspläne künftig in einem passwortgeschützten Bereich veröffentlicht werden würden.

## 5.2 Personalvertretung

In diesem Jahr nicht belegt.

## 5.3 Einwohnermeldewesen

### 5.3.1 Entscheidungsbefugnis des Stadtrates im Bereich des Meldewesens

Ein Stadtratsmitglied machte mich darauf aufmerksam, dass der betreffende Stadtrat eine listenweise Veröffentlichung bzw. Übermittlung von Meldedaten (§ 33 Abs. 3 SächsMG) für Adressbuchzwecke beschlossen habe. Der Rat hatte in seiner Sitzung mit Stimmenmehrheit beschlossen, Vor- und Familiennamen, Doktorgrad und Anschrift aller volljährigen Einwohner an einen Dritten kostenfrei weiterzugeben. Die Weitergabe sollte der Zusammenstellung eines bereits in den Vorjahren erschienenen Adressbuchs der Stadt dienen und im Anhang um ein Einwohnerverzeichnis mit den oben genannten Daten ergänzt werden. Die Stadtverwaltung stützte ihr Vorhaben auf § 33 Abs. 3 SächsMG, wonach Meldebehörden befugt sind, Daten volljähriger Einwohner in Adressbüchern zu veröffentlichen. Die Entscheidungsbefugnis dazu war mit Ratsbeschluss dem Stadtrat übertragen worden, der schließlich den Beschluss zur Veröffentlichung der Meldedaten gefasst hatte.

Gemäß § 2 SächsMG sind Meldebehörden die Gemeinden. Die Aufgaben der Meldebehörden sind Pflichtaufgaben nach Weisung, § 2 Abs. 2 SächsMG. § 53 Abs. 3 SächsGemO bestimmt, dass der Bürgermeister die Weisungsaufgaben in eigener Zuständigkeit erledigt, soweit gesetzlich nichts anderes bestimmt ist. Der Gemeinderat hingegen legt die Grundsätze für die Verwaltung der Gemeinde fest und entscheidet über alle Angelegenheiten der Gemeinde, soweit nicht der Bürgermeister kraft Gesetzes zuständig ist oder ihm der Gemeinderat bestimmte Angelegenheiten überträgt, § 28 Abs. 1 SächsGemO. Eine gesetzliche Aufgabenzuweisung für den Bürgermeister liegt für die Weisungsangelegenheit der Meldebehörde gemäß § 53 Abs. 3 SächsGemO vor und es ist gesetzlich nichts anderes bestimmt. Die rechtliche Betrachtung ergibt also, dass die Gemeindevertretung für eine Entscheidung über die Veröffentlichung von Meldedaten in Adressbüchern und ähnlichen Nachschlagewerken und eine listenweise

Übermittlung der Einwohnermeldedaten an Dritte nicht zuständig ist. Dieses Ergebnis teilte ich dem anfragenden Stadtrat so mit.

### 5.3.2 Aufforderung einer öffentlichen Stelle zur Sammelauskunft zur Erhebung der Zweitwohnungssteuer

Im Berichtszeitraum wurde ich um Stellungnahme gebeten, ob ein Studentenwerk gemäß der Aufforderung eines städtischen Steueramtes zur Sammelauskunft über Wohnheimbewohner verpflichtet ist.

Die erfolgte datenschutzrechtliche Prüfung ergab, dass das durch das Sachgebiet Steuer- und Kassenverwaltung an das Studentenwerk ergangene Auskunftsersuchen, in dem eine namentliche Aufstellung aller Mieter, welche zurzeit in zwei bestimmten Wohnheimen des Studentenwerks in der Stadt ein Zimmer innehatten, nicht erforderlich bzw. unverhältnismäßig war, da das Studentenwerk nicht primär auskunftspflichtig war. Eine Auskunftspflicht des Studentenwerks bestand jedoch gemäß § 14 Nr. 2 SächsMG gegenüber der für falsche und fehlende Wohnungsangaben *erstrangig* zuständigen Meldebehörde der Stadt. Datenschutzrechtlich war seitens der Stadt die Heranziehung des Vermieters als nichtbeteiligtem Dritten zu vermeiden und zunächst die Inanspruchnahme der ohnehin zuständigen Melderegisterbehörde zu veranlassen.

Als Begründung des Auskunftsersuchens wurde von Seiten der Stadt angegeben, dass eine Kontrolle der Briefkastenbeschilderung der Wohnheime ergeben habe, dass von den 233 Bewohnern lediglich 105 Personen mit Haupt- oder Nebenwohnsitz in der Stadt gemeldet waren. Die Stadt hatte das Studentenwerk mit dem Argument der Gleichmäßigkeit der Besteuerung aufgefordert, eine namentliche Aufstellung aller Mieter der beiden Wohnheime zu übersenden.

Das kommunale Steueramt verwies im Hinblick auf sein Auskunftsersuchen auf die Zweitwohnungssteuersatzung der Stadt in Verbindung mit § 3 Abs. 1 Nr. 3a SächsKAG i. V. m. § 93 AO. § 93 AO regelt die Auskunftspflicht von Beteiligten und anderen Personen zur Feststellung eines für die Besteuerung erheblichen Sachverhalts. Voraussetzung für die Pflicht zur Auskunft ist gemäß der Vorschrift, dass die Auskunft erforderlich sein muss. Diese Voraussetzung lag nach meiner Überzeugung aber nicht vor, da die Übermittlung der personenbezogenen Daten aller Mieter der beiden Wohnheime, unabhängig davon, ob für diese eine Zweitwohnungssteuerpflicht besteht, sie sich bereits ordnungsgemäß angemeldet hatten und bereits Zweitwohnungssteuer entrichten, gerade nicht erforderlich gewesen war.

Hinzu kam, dass die Zweitwohnungssteuersatzung der Stadt regelte, dass Grundstückseigentümer, Wohnungseigentümer, Wohnungsgeber und Vermieter, im vorliegenden

Fall das Studentenwerk, lediglich zur Mitteilung über die „Person des Steuerpflichtigen“ und „aller für die Steuererhebung erforderlichen Tatbestände“ verpflichtet waren. Eine Pflicht zur Übermittlung von personenbezogenen Daten bestand nur für die Mieter, die auch steuerpflichtig waren. Über die tatsächlich hierfür notwendigen Angaben verfügte das Studentenwerk jedoch nicht, wohl aber die zuständige Behörde, die die Haupt- und Nebenwohnsitze der Einwohner einer Stadt speichert. Die zur Aufgabenerfüllung des Steueramtes erforderlichen Daten der Mieter konnten also bereits durch die zuständige Registerbehörde, das zuständige Einwohnermeldeamt der Stadt übermittelt werden.

Die Meldebehörden im Freistaat Sachsen registrieren die in ihrem Zuständigkeitsbereich wohnenden Personen (Einwohner), erteilen Melderegisterauskünfte und wirken bei der Durchführung von Aufgaben anderer Behörden mit. Das städtische Steueramt, das per Abruf auf die Meldedaten zuzugreifen berechtigt war, hätte gemäß § 25 Abs. 4 SächsMG als Empfänger regelmäßiger Datenübermittlungen die Meldebehörden unverzüglich zu unterrichten gehabt, dass konkrete Anhaltspunkte für die Unrichtigkeit oder Unvollständigkeit übermittelter Daten vorliegen. Sodann hätte die Meldebehörde den Sachverhalt von Amts wegen in Bezug auf die Anhaltspunkte für die Unvollständigkeit des Melderegisters zu einer Vielzahl namentlich bekannter Einwohner zu ermitteln gehabt, § 25 Abs. 3 SächsMG. Die Meldebehörde konnte wiederum zur Ermittlung das Studentenwerk als Wohnungsgeber heranziehen, § 14 Nr. 2 SächsMG. Letztendlich hätte nach einer Fortschreibung des Melderegisters gemäß § 25 Abs. 2 SächsMG in Verbindung mit der Zweitwohnungssteuersatzung der Stadt eine Datenübermittlung der Meldebehörde an das städtische Steueramt erfolgen können.

Eine Datenerhebung des Steueramts mit Hilfe von Angaben des Studentenwerks ist hingegen nur dann eine in Betracht kommende geeignete Maßnahme, wenn die Meldebehörde die Melderechtsverhältnisse der Mieter der Studentenwohnheime des Studentenwerks nicht zu klären imstande gewesen wäre. Ich teilte dies so dem Studentenwerk mit, das mich kurz darauf informierte, dass die Stadt den vom Studentenwerk eingelegten Widerspruch abgelehnt habe.

Die Rechtsprechung hat die Ermittlungstätigkeit der Steuerbehörden in Fällen als rechtmäßig angesehen, wenn subsidiäre Meldepflichten Dritter nicht vorgesehen sind und ein Meldegesetz den Verzicht auf Anmeldepflichten normierte. In Sachsen besteht hingegen eine andere Rechtslage, nämlich die Auskunftspflicht des Vermieters in § 14 Nr. 2 SächsMG. Auch ein Verzicht auf die Pflicht zur Anmeldung bei einem Umzug innerhalb einer Gemeinde ist im Sächsischen Meldegesetz nicht vorgesehen gewesen.

Melderechtliche Kontrollmöglichkeiten, das Unterlassen einer Meldung mit Nebenwohnsitz zu überprüfen, waren damit gegeben. Durch die tatbestandliche Anknüpfung

der Zweitwohnungssteuer an das Melderecht ist grundsätzlich sichergestellt, dass die Steuerbehörde Kenntnis von allen Steuerpflichtigen erlangt, die im Stadtgebiet eine Neben- und damit eine Zweitwohnung beziehen; denn gemäß § 10 Abs. 1 SächsMG hat sich derjenige, der eine Wohnung bezieht, innerhalb von zwei Wochen bei der zuständigen Meldebehörde anzumelden. Verstöße sind bußgeldbewehrt. Hinzu kommt die erwähnte Meldepflicht Dritter gemäß § 14 Nr. 2 SächsMG.

Kritikwürdig erschien mir, dass die Stadtverwaltung hingegen hinsichtlich des Melderegisterstands untätig blieb. Wenn tatsächlich, wie gar im Bescheid der Stadtverwaltung dargetan, das Melderegister nicht vollständig wäre und die Meldebehörde ihrer Verpflichtung zur Fortschreibung des Melderegisters bzw. der Ermittlung von Amts wegen nicht nachzukommen in der Lage sein sollte, wäre ein weitergehendes datenschutzrechtliches und kommunalaufsichtliches Handeln angezeigt.

### 5.3.3 Zulässigkeit der „manuellen Nachbereitung“ durch die Meldebehörden auf dem Meldebehördenportal einer Firma - Outsourcing

Im Berichtszeitraum überprüfte ich ein Meldebehördenportal. Die von der Firma betriebene Europäische Meldeauskunft ermöglicht es jedermann, über ein Online-Portal einfache Melderegisterauskünfte bei Meldebehörden in ganz Deutschland zu beauftragen. Die Anfragen werden von dem Unternehmen gebündelt an die Meldebehörden zur Bearbeitung weitergeleitet. Ein Teil dieses Verfahrens ist die sogenannte „manuelle Nachbereitung“ durch die Meldebehörden. Bei der manuell bearbeiteten Melderegisteranfrage wird nach Angabe der Firma der Umstand genutzt, dass bei offensichtlichen Schreibfehlern oder abweichenden Schreibweisen, z. B. von Straßennamen, die Sachbearbeiter der Meldebehörden häufig noch eine Auskunft erteilen, während bei automatisierter Bearbeitung negative Auskünfte übermittelt werden. Für diese manuelle Nachbearbeitung werden der Meldebehörde die beim automatisierten Abgleich nicht identifizierten (negativen) Auskünfte durch das Unternehmen zur Überprüfung erneut bereitgestellt. Dazu loggt sich die Meldebehörde auf dem Firmen-Portal ein, ruft die von der Firma bereitgestellten Auskunftsantragsangaben ab, prüft die Daten und ändert diese manuell im System des Unternehmens.

Nach Prüfung der mir vorgelegten Unterlagen hatte ich Zweifel daran, dass die durch die Meldebehörde in dem Meldebehördenportal vorgenommenen Tätigkeiten zu den im Meldegesetz abschließend aufgezählten Aufgaben der Meldebehörden gehören.

Fraglich ist u. a., auf welcher Rechtsgrundlage die Meldebehörden diese Art der Melderegisterauskunft erteilen, ob die Bereitstellung der Negativauskünfte auf dem Portal der Firma, auf dem sich die Meldebehörde einloggt, dem gesetzlich vorgeschriebenen An-

trag auf Erteilung einer Melderegisterauskunft entspricht, und wie sichergestellt wird, dass entsprechend den gesetzlichen Festlegungen die einfache Melderegisterauskunft nur erteilt wird, wenn die Identität des Betroffenen durch einen automatisierten Abgleich der im Antrag angegebenen mit den im Melderegister gespeicherten Daten des Betroffenen eindeutig festgestellt worden ist.

Im beschriebenen Verfahren meldet sich die Meldebehörde auf dem „Meldeportal“ eines privaten Dritten an, um dort aktiv Daten für Dritte zu pflegen. Dieses Verfahren geht über eine Auskunftserteilung nach § 1 Abs. 1 SächsMG hinaus und ist damit nach meiner Überzeugung nicht von den gesetzlichen Aufgaben der Meldebehörde umfasst. Neben der Frage, wie alle gesetzlichen Vorgaben zur Erteilung der einfachen Melderegisterauskunft nach § 32 Abs. 2 SächsMG auf der Internetplattform einer Privatfirma eingehalten werden, ist zu beachten, dass die Meldebehörde bei dem Verfahren auch nicht zu gewährleisten in der Lage ist, dass dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit getroffen werden, die insbesondere die Vertraulichkeit und die Unversehrtheit der im Melderegister gespeicherten Daten erfordern. Aus den mir zur Verfügung gestellten Unterlagen ging ebenfalls nicht hervor, wie sichergestellt wird, dass eine Meldebehörde nur die in ihrer Zuständigkeit liegenden Meldedaten übermittelt bekommt.

Ich bat das für das Meldewesen zuständige SMI um Stellungnahme zu den Fragen zur „manuellen Nachbereitung“. Das SMI teilte mir in seiner Stellungnahme mit, dass es keine Veranlassung sehen würde, seine zustimmende Auffassung zur Zulässigkeit der manuellen Nachbearbeitung mit Hilfe des Meldeportals der betreffenden Firma durch sächsische Meldebehörden zu ändern. Das Verfahren mit Hilfe des Meldeportals des Unternehmens finde im Sächsischen Meldegesetz seine gesetzliche Grundlage.

Nach Auffassung des SMI hätten die Meldebehörden die Befugnis, im Rahmen ihrer „Organisationshoheit“ ein derartiges Verfahren zur Erteilung von Registerauskünften zu wählen. Das SMI führte weiter aus, dass der Gesetzgeber im Sächsischen Meldegesetz nicht abschließend festlegen würde, auf welche Art und Weise die Melderegisterauskünfte erteilt werden müssen. So würden Melderegisterauskünfte beispielsweise mündlich bei Vorsprache oder schriftlich per Brief oder elektronisch über das Internet oder per Datenträger erteilt werden können. Das neue Bundesmeldegesetz würde noch eine weitere Verfahrensart der Erteilung einfacher Melderegisterauskünfte enthalten, nämlich die der Beauskunftung über das Internet über Portale. Das Sächsische Meldegesetz und das Bundesmeldegesetz würden also nicht bestimmte Verfahrenswege regeln, sondern definierten lediglich gesetzliche Anforderungen an die Ausgestaltung und die Anwendung von Verfahren zur Erteilung von Melderegisterauskünften. § 32 SächsMG - und zukünftig § 44 BMG (das BMG tritt am 1. Mai 2015 in Kraft) - seien

technikoffen im Hinblick auf den Verfahrensweg der Erteilung von Melderegisterauskünften gestaltet, so dass jede Art der Datenübermittlung aus Melderegistern an Private zulässig sei. Damit würden Daten grundsätzlich sowohl schriftlich, mündlich, fernmündlich, elektronisch, per Fax oder E-Mail, durch automatisierten Abruf aus einem Register, durch Eintragung von Melderegisterdaten in Registern eines Dritten oder über Portale übermittelt werden können.

Das SMI teilte aber auch wiederum mit, dass es sich bei dem Meldeportal der Firma nach Auffassung des BMI nicht um ein Portal i. S. d. § 44 Abs. 3 BMG-E handeln würde, sondern um ein Anfrageportal zur qualifizierten Dienstleistung der Meldebehörden. Das Handeln der Meldebehörde durch die manuelle Nachbearbeitung stelle eine Verwaltungstätigkeit gemäß § 44 BMG-E dar. Mit dem „Meldeportal“ des Unternehmens werde den Meldebehörden mithin lediglich ein unterstützendes Werkzeug zur Verfügung gestellt, um in der Sphäre der anfragenden Stelle, für die das Unternehmen im Auftrag handele, Ergebnisse einer manuellen Melderegisterauskunft zu hinterlegen und einen Medienbruch zu verhindern. Ein Untersagen solcher eher als Abfrageportale zu qualifizierenden Dienstleistungen erscheine aus jetziger Sicht auch für die Zeit nach dem Inkrafttreten des Bundesmeldegesetzes nicht notwendig, soweit alle Vorgaben des Bundesmeldegesetzes in Bezug auf die einfache Melderegisterauskunft korrekt abgebildet seien.

Nach Auffassung des SMI sei § 32 Abs. 1 SächsMG und nicht § 32 Abs. 2 SächsMG Rechtsgrundlage für die Erteilung der Auskunft. Das ergebe sich daraus, dass es sich um eine händische Bearbeitung durch einen Mitarbeiter der Meldebehörde handele, der die Daten in eine elektronische Maske eintippe, nachdem er nach Abgleich (Suchlauf) mit dem Melderegister und individueller Prüfung die zu beauskunftenden Angaben eindeutig bestimmt habe. Da die Identifizierung nicht durch automatisierten Abgleich eines Computers, sondern durch einen einzelfallbezogenen Abgleich eines Meldebehördenmitarbeiters erfolge, würde kein Fall des § 32 Abs. 2 SächsMG vorliegen und es sei § 32 Abs. 1 SächsMG anwendbar.

Dieser Rechtsauffassung schließe ich mich nicht an. Die Prüfung der Rechtmäßigkeit der „manuellen Nachbereitung“ ist noch nicht abgeschlossen. Das Problem wird aktuell zwischen den Datenschutzbeauftragten des Bundes und der Länder diskutiert. Das betreffende Meldebehördenportal ist Gegenstand der EuroPriSe-Zertifizierung des ULD Schleswig-Holstein gewesen. Das routinemäßige Verfahren der Rezertifizierung nach zwei Jahren wird derzeit von EuroPriSe durchgeführt. Die von mir genannten Probleme habe ich mit der Bitte um besondere Prüfung und Beachtung an EuroPriSe übersandt.

Grundsätzlich wird man auch die Frage zu stellen haben, inwieweit (Melde-)Behörden auf Portalen in der Sphäre nicht-öffentlicher Stellen Datenverarbeitung durchzuführen berechtigt sein sollen. Bei öffentlichen Stellen, die Daten öffentlicher Register verarbeiten, melde ich in jedem Fall Bedenken an.

### 5.3.4 Zulässigkeit der Erteilung telefonischer Auskünfte aus dem Melderegister

Aus einer Stadtverwaltung erreichte mich die Anfrage bezüglich der Zulässigkeit der Erteilung telefonischer Auskünfte an Behörden aus dem Melderegister über ein Bürgerbüro, ein sogenanntes „Bürgertelefon“. Ich vertrat die Auffassung, dass die telefonische „Erteilung von Auskünften aus dem Melderegister an Behörden“ durch ein Bürgertelefon melde- und datenschutzrechtlich unzulässig ist.

Eine Übertragung von Einzelaufgaben im Sinne von Hilfsdienstleistungen (z. B. die telefonische Information zu Öffnungszeiten, zuständigen Bearbeitern oder für eine Antragstellung mitzubringenden Dokumenten) auf eine zentrale Auskunftsstelle ist meldegesetzlich zwar zulässig, eigentliche Sachentscheidungen bleiben hingegen in der Verantwortung des allein zuständigen Meldeamts und können nicht in organisatorischer Hinsicht auf andere Stellen übertragen werden.

Das Meldegesetz unterscheidet zwischen einer Auskunftserteilung an Private (Einfache Melderegisterauskunft an Private (§ 32 SächsMG) und der Datenübermittlung an Behörden und sonstige öffentliche Stellen (§ 29 SächsMG). Dementsprechend erteilen die Meldebehörden gegenüber Behörden keine Melderegisterauskünfte, sondern übermitteln die Daten von Einwohnern aus dem Melderegister, wenn dies zur Erfüllung der in ihrer Zuständigkeit oder der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich ist. Der Umfang der Übermittlungsbefugnis bei anfragenden Behörden ist nicht auf Adressauskünfte beschränkt, sondern reicht nach § 29 Abs. 1 oder 2 SächsMG so weit, wie die geltend gemachte Erforderlichkeit. Grundsätzlich trägt die Meldebehörde die Verantwortung für die Zulässigkeit der Übermittlung der Meldedaten (§ 29 Abs. 3 Satz 1 SächsMG). Erfolgt hingegen die Übermittlung auf Ersuchen des Empfängers, prüft die Meldebehörde, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt, sofern nicht im Einzelfall Anlass zu weitergehender Prüfung der Zulässigkeit der Übermittlung besteht. Der Empfänger trägt die Verantwortung für die Zulässigkeit der Übermittlung, vgl. § 29 Abs. 3 Satz 2 und 3 SächsMG .

Abgesehen von dem einzuhaltenden Meldegeheimnis und organisationsrechtlichen Bedenken würde eine Wahrnehmung melderechtlicher Aufgaben, d. h. Auskünfte an Private (§ 32 SächsMG) und Übermittlungen an Behörden (§ 29 SächsMG) auch an prak-

tischen Überlegungen scheitern. Würde den Bediensteten des Bürgerbüros nämlich weitergehende melderechtliche Aufgaben übertragen, hätte das Bürgerbüro im Auftrag der Meldebehörde auch zu prüfen, ob behördliche Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegen. Ggf. könnte im Einzelfall auch Anlass zu weitergehender Prüfung der Zulässigkeit der Übermittlung durch das Bürgerbüro bestehen. Dies gilt vor allem vor dem Hintergrund, dass § 29 Abs. 1 und 2 SächsMG die Datenübermittlung als Einzelfallentscheidung regelt.

Soweit regelmäßige Datenübermittlungen gemäß § 29 Abs. 5 SächsMG stattfinden sollen, sind diese nur zulässig, soweit sie durch Bundes- oder Landesrecht unter Festlegung des Anlasses und des Zwecks der Übermittlungen, der Empfänger und der zu übermittelnden Daten bestimmt sind. In diesen Fällen erstreckt sich die Prüfpflicht der Meldebehörden darauf, ob eine Rechtsvorschrift im Sinne des § 29 Abs. 5 SächsMG vorhanden ist und ob deren Voraussetzungen erfüllt sind. Die Meldebehörde muss sicherstellen, dass die regelmäßigen Übermittlungen auf die in der Rechtsvorschrift aufgeführten Daten beschränkt und nur aus den festgelegten Anlässen und gegenüber den zugelassenen Übermittlungsempfängern durchgeführt werden (siehe Kommentierung zu § 29 SächsMG in Darré/Rimmele/Thalheim/Wunsch).

Bei der Übermittlung von Meldedaten an Behörden gemäß § 29 SächsMG handelt es sich aus datenschutzrechtlicher Sicht nicht um eine auf ein Bürgerbüro und Bürgertelefon übertragbare Hilfsdiensttätigkeit, da die Meldebehörde als Voraussetzung für eine Datenübermittlung unterschiedlichste Zulässigkeitsvoraussetzungen zu prüfen und Entscheidungen zu treffen hat.

Der Stadtverwaltung teilte ich zudem mit, dass ein Datenübermittlungsersuchen einer Behörde nur im Ausnahmefall eilbedürftig sein wird. Ein Übermittlungsersuchen einer Behörde kann im Regelfall immer schriftlich an die Meldebehörde übersandt werden. Eine telefonische Übermittlung birgt, auch bei der Möglichkeit eines Rückrufs, immer ein Restrisiko, dass die Meldedaten missbräuchlich abgerufen werden. Die Übermittlung von Meldedaten im Umfang der Übermittlungen nach § 29 Abs. 1 und 2 SächsMG sollte durch die zuständige Meldebehörde deshalb nur in begründeten Ausnahmefällen telefonisch erfolgen.

## 5.4 Personenstandswesen

In diesem Jahr nicht belegt.

## 5.5 Kommunale Selbstverwaltung

### 5.5.1 Gehaltsinformationen im Gemeindeblatt

Bereits unter 15/5.5.6 hatte ich darauf hingewiesen, unter welchen Voraussetzungen personenbezogene Angaben in Beschlussvorlagen und Unterlagen bzw. Niederschriften öffentlicher Stadtratssitzungen veröffentlicht werden dürfen.

Eine Petentin wies mich darauf hin, dass über die Besetzung ihrer Stelle unter Angabe der Gehaltsgruppe im Gemeindeblatt, das auch über das Internet verbreitet wird, informiert wurde und bat mich um datenschutzrechtliche Prüfung.

Die von mir um Stellungnahme gebetene Gemeinde teilte mir mit, dass sie bislang davon ausgegangen war, dass die vollumfängliche Veröffentlichung des in nichtöffentlicher Sitzung gefassten Beschlusses zur Stellenbesetzung nach § 37 Abs. 1 Satz 3 SächsGemO zulässig sei. Sie nahm jedoch bereits vor meinem Schreiben meinen oben erwähnten Tätigkeitsberichtsbeitrag zum Anlass, die Vergütungsgruppe künftig nur in der Begründung aufzuführen und im Beschlusstext unerwähnt zu lassen. Die Begründungen werden von der Gemeinde nicht mit veröffentlicht. Die bereits erfolgte Internetveröffentlichung über die Stellenbesetzung wurde entsprechend angepasst.

### 5.5.2 Namensnennung von Einwendenden gegen kommunale Haushaltssatzung im Gemeindeblatt und im Internet

Ein Einwohner, der Einwendungen gegen eine kommunale Haushaltssatzung geltend machte, wies mich darauf hin, dass sein Name und seine Anschrift in diesem Zusammenhang in einem im Internet verbreiteten Gemeindeblatt veröffentlicht wurden. Dies halte ich aus den nachstehenden Gründen für unzulässig und habe dies der Gemeindeverwaltung auch so mitgeteilt:

Zunächst legt die Vorschrift des § 76 Abs. 1 Satz 4 SächsGemO fest, dass nur (betroffene) Einwohner Einwendungen gegen den Entwurf der Haushaltssatzung vortragen können. Dazu ist es erforderlich, die Einwohnereigenschaft, d. h. Namen und Anschrift zu prüfen und hierfür personenbezogene Daten zu verarbeiten. Danach ist gemäß § 76 Abs. 1 Satz 5 SächsGemO über die fristgemäß erhobenen Einwendungen in öffentlicher Sitzung zu beschließen. Dieser Beschluss ist gemäß § 37 Abs. 1 Satz 3 SächsGemO bekanntzugeben. Im vorliegenden Fall wurde er nach § 2 Nr. 1 KomBekVO im Gemeindeblatt veröffentlicht.

Fraglich ist jedoch, ob dieser Beschluss notwendig so abgefasst zu sein hat, dass er auch die Namen und Anschriften der Einwendenden umfasst, und darüber hinaus, ob diese Personen im Internet veröffentlicht werden sollten.

Bereits die namentliche Nennung ist dann verzichtbar, wenn die Gemeinde die Einwendungen ordnungsgemäß verwaltet und ordnet, denn letztendlich wird regelmäßig der Gegenstand der Einwendung für die Gemeindeöffentlichkeit entscheidend sein und nicht die Identität des Einwendenden. Demgegenüber hat aber die Nennung des Namens, ohne den Inhalt der Einwendung zu kennen, im Beschluss keinerlei Informationsgehalt für die Öffentlichkeit, auch wenn es sich bei Beschlüssen des Gemeinderats um verwaltungsinterne Akten handeln mag. Besser wäre es also, die Inhalte der Einwendungen wiederzugeben und den Schriftsatz des Einwendenden, z. B. mit dem Datum - Zeitpunkt -, zu bezeichnen. Dann könnte der Namensbezug auch wegfallen.

Dem gesetzlichen Öffentlichkeitsgrundsatz wäre nach meiner Überzeugung Genüge geleistet worden, wenn die Verwaltung der Gemeinde in der öffentlichen Beratung über die Einwendungen angemerkt hätte, dass die Zulässigkeit der Einwendung geprüft worden ist, die Einwendenden in der Gemeinde ansässig und daher Einwohner sind, ohne dass konkrete Namen und Anschriften genannt werden. Eine Beschlussfassung in der - wie im Beschwerdefall - durchgeführten Weise unter Nennung des Vor- und Zunamens und der Anschrift war hingegen im Zusammenhang mit dem Gegenstand der Haushaltssatzung so nicht erforderlich.

Persönlichkeitsrechtlich belastender war jedoch die im nächsten Schritt erfolgende namentliche Nennung im Gemeindeblatt, insbesondere zusammen mit der Anschrift. Diese stellt eine Übermittlung an einen unbestimmten Empfängerkreis dar und hätte unter Berücksichtigung der Privatheit der Anschrift, selbst wenn bei einer kleinen Gemeinde eine Zuordnung relativ leicht stattfinden könnte, vermieden werden können.

Fraglich ist darüber hinaus auch gewesen, ob eine Veröffentlichung des Gemeindeblatts im Internet (beispielsweise durch die Bekanntmachungssatzung, die dies vorliegend aber nicht vorsah) überhaupt zulässig gewesen war oder ob nicht vielmehr der in § 2 Nr. 1 KomBekVO vorgeschriebene „Abdruck“ eine Beschränkung darstellt, so dass eine Bekanntmachungssatzung, die eine Internetveröffentlichung vorsieht, gemäß § 4 Abs. 1 Satz 1 SächsGemo unzulässig ist. Ich verweise in diesem Zusammenhang auch auf meine Ausführungen zur Unzulässigkeit der Internetveröffentlichung von Niederschriften von Gemeinderatssitzungen in 14/5.5.2. Die weltweite Übermittlung der Daten über das Internet ist, selbst wenn man davon ausgeht, dass einer Gemeinde nur eine beschränkte Internetöffentlichkeit zuteilwird, wegen der Vervielfältigungsmöglichkeiten, Suchmaschinen und der nicht endlichen Datenverarbeitung im Internet gravierender als eine Veröffentlichung der Druckausgabe des Gemeindeblatts.

Leider habe ich weder die Gemeinde noch die Kommunalaufsicht des zuständigen Landkreises von meiner Auffassung überzeugen können. Der Landrat teilte mir dazu

erstaunlicherweise in bestimmender gradliniger Manier mit, dass Rechtsgrundlage § 24 Abs. 1 der Kommunalverfassung der DDR sei. Die darin vorgesehene Praxis des Abdrucks von vollständigen Beschlusstexten im Gemeindeblatt werde aus Gründen der Verwaltungstransparenz fortgeführt. Ein Verstoß gegen die Sächsische Gemeindeordnung sei nicht erkennbar.

### 5.5.3 Schwärzung des Beifahrers auf Beweisfotos von Verkehrsordnungswidrigkeiten

Aufgrund einer Eingabe bekam ich davon Kenntnis, dass ein Kreisordnungsamt dem Ermittlungsersuchen an die örtliche Polizeidienststelle ein Beweisfoto beigefügt hatte, auf dem der Beifahrer nicht durch Schwärzung anonymisiert worden war.

Zur Ermittlung des Fahrers, gegen den sich das Ordnungswidrigkeitenverfahren gerichtet hatte, war es nicht erforderlich, die Person des Beifahrers zu übermitteln. Eine Datenübermittlung darf nach § 14 Abs. 1 SächsDSG aber nur erfolgen, wenn und soweit sie zur Aufgabenerfüllung erforderlich ist. Hier sind letztlich die Datenschutzinteressen einer - an der Verkehrsordnungswidrigkeit - unbeteiligten Person zu wahren.

Aus der eingeholten Stellungnahme ergab sich, dass die Pflicht zur Schwärzung des Beifahrers vor der Versendung von Lichtbildaufnahmen (vgl. Erlass des SMI vom 15. Mai 1995 i. V. m. der Ergänzung vom 18. Juli 1995, Az. 39-0523/104) dort nicht bekannt zu sein schien. Ich habe das Landratsamt entsprechend belehrt und um Sicherstellung des rechtmäßigen Verfahrens gebeten.

Ferner habe ich das SMI gebeten, die Bußgeldstellen und Polizeibehörden ggf. erneut über die Verfahrensweise zu unterrichten. Darüber hinaus habe ich angeregt, eine entsprechende Regelung in die Neufassung der VwV Verkehrsüberwachung aufzunehmen. Das SMI hat mir eine Prüfung zugesagt.

### 5.5.4 Datenübermittlung der Stadtverwaltung an einen Notar zum Zwecke eines privatrechtlichen Vertragsentwurfs

Zwei Petenten erhielten per Post den Entwurf eines auch sie betreffenden notariellen Vertrages über die Bestellung einer Grunddienstbarkeit, ohne dass sie zuvor Kenntnis von einem derartigen Vorgang hatten. Der Vertragsentwurf enthielt nicht nur ihre Namen, Geburtsdaten, Güterstände, Grundstücksnummern und sonstige Daten, sondern auch die aller übrigen 14 Vertragsbeteiligten.

Meine Ermittlungen ergaben, dass ein Nachbar mit der Bitte um die Bestellung einer Grunddienstbarkeit an die Stadtverwaltung herangetreten war. Diese lud daraufhin die

Eigentümer aller betroffenen Grundstücke zu einer Besprechung ein, an der die Petenten jedoch nicht teilnahmen. Die Anwesenden verständigten sich auf die Bestellung einer Grunddienstbarkeit. Aus Kostengründen sollte diese in Form einer Sammelurkunde beurkundet werden. Darüber sollten alle Beteiligten informiert werden, darunter auch die Petenten. Die Stadtverwaltung sollte mit dem zuständigen Notar Kontakt aufnehmen. Zu diesem Zweck übermittelte sie die Namen und Grundstücksnummern aller Beteiligten, darunter auch die der Petenten, an den Notar. Die weiteren zur Vorbereitung des Vertragsentwurfs erforderlichen Daten erlangte der Notar dann im Wege des automatisierten Abrufverfahrens aus dem maschinell geführten Grundbuch gemäß § 133 GBO, § 21 Abs. 1 BeurkG. Diese Möglichkeit besteht für Rechtsanwälte und Notare, wenn sie dies beantragen und nach Erfüllung der gesetzlichen Vorgaben hierfür zugelassen worden sind. Ein berechtigtes Interesse zur Einsicht in das Grundbuch gemäß § 12 GBO wird bei Notaren i. d. R. unterstellt, da sie für die Beurkundung von Grundstücksgeschäften zuständig sind und aufgrund ihrer Amtsträgerstellung (§ 1 BNotO) besonderes Vertrauen genießen. Dennoch ist der konkrete Abruf nur bei Erforderlichkeit zulässig. Da der Notar im vorliegenden Fall durch die Stadtverwaltung im Namen *aller* Beteiligten mit der Vorbereitung eines Sammelvertrags und dessen Versendung an die einzelnen Vertragspartner beauftragt worden war, durfte er - auch vor dem Hintergrund jahrelanger ordnungsgemäßer Zusammenarbeit - auf deren Angaben vertrauen. Dennoch habe ich auch den Notar darauf hingewiesen, dass der ausdrücklich vorliegenden Einwilligung aller Beteiligten in vergleichbaren Fällen besonderes Gewicht zukommen muss.

Der eigentliche datenschutzrechtliche Verstoß ist jedoch durch die Stadtverwaltung begangen worden. Da eine Einwilligung der Petenten zur Bestellung einer Grunddienstbarkeit tatsächlich nicht vorlag, war die Übermittlung der Daten an den Notar unzulässig. Ich wies die Stadtverwaltung darauf hin, dass das Schweigen eines Betroffenen keine Einwilligungserklärung darstellt und zukünftig keine solche Übermittlung ohne die ausdrückliche und schriftliche Zustimmung des Betroffenen erfolgen darf. Gleichzeitig bat ich um die nachweisliche Belehrung der Bediensteten. Von einer förmlichen Beanstandung nach § 29 Abs. 1 SächsDSG sah ich jedoch ab, da die Stadtverwaltung den datenschutzrechtlichen Verstoß eingesehen hatte und angesichts ihrer Stellungnahme keine Wiederholungsgefahr gegeben war.

### 5.5.5 Videoüberwachung einer Weihnachtspyramide zur Adventszeit

In den letzten Jahren wenden sich zu Beginn der Adventszeit häufig Gemeinden mit der Bitte an mich, die Zulässigkeit der Videoüberwachung von Weihnachtsaufbauten auf öffentlich zugänglichen Plätzen zu prüfen.

Eine Gemeinde plante eine Videoüberwachung einer groß dimensionierten Weihnachtspyramide auf einem Marktplatz, an der zurückliegend bereits mehrfach das Holz und die Elektrik beschädigt und Teile gestohlen worden seien. Die Verwaltung der Gemeinde verwies zudem auf entsprechende polizeiliche Anzeigen, die aber ohne Erfolg geblieben seien. Aus diesem Grund beabsichtigte die Kommune fortan jährlich eine Videoüberwachung vom Vorabend des Ersten Advents bis zum Abbau der Pyramide vorzusehen. Ein Hinweis auf die Videoüberwachung sollte an einem Zaun vor der Pyramide angebracht werden. Zweck der Überwachungsmaßnahme sollte primär die Vermeidung von zukünftigen Beschädigungen sein. Darüber hinaus sollte nach Angaben der Gemeinde eine genaue zeitliche Bestimmung von Tatzeiten im Falle von Sachbeschädigungen möglich sein und festgestellt werden können, um wen und ob es sich um eine Gruppe oder Einzeltäter handeln würde.

Bei Prüfung des Vorhabens gewann ich die Überzeugung, dass durch die eingesetzte Videotechnik das Recht auf informationelle Selbstbestimmung der Weihnachtsmarktbesucher und Passanten unverhältnismäßig eingeschränkt werden würde.

Bei der datenschutzrechtlichen Zulässigkeit einer geplanten Videoüberwachung ist zu beurteilen, ob und inwieweit ein Eingriff in das Recht auf informationelle Selbstbestimmung stattfindet und ob dieser Eingriff tatsächlich zur Aufgabenerfüllung der öffentlichen Stelle erforderlich ist, § 33 Abs. 1 SächsDSG. Die Videoüberwachung ist im Falle eines Eingriffs in das Recht auf informationelle Selbstbestimmung nur dann zulässig, wenn diese ihre Aufgaben ohne Einsatz der optisch-elektronischen Einrichtungen nicht zu erfüllen in der Lage ist. Das Gesetz verlangt zudem, dass durch die Videoüberwachung überwiegende schutzwürdige Interessen Betroffener nicht beeinträchtigt werden.

Die Aufgabe, im Gemeindegebiet für Ordnung und Sicherheit zu sorgen, ist eine Aufgabe der Gemeinde und grundsätzlich ein gesetzlicher Grund, Videoüberwachungsmaßnahmen zulässig durchführen zu können. Sachbeschädigung an einem relativ wertvollen kunsthandwerklichen Gut zu verhindern, ist auch ein geeigneter Zweck. Zur Erreichung des Zwecks hätte es allerdings in keinem Verhältnis gestanden, sämtliche Passanten des Weihnachtsmarktes im Sichtkegelbereich der Videokamera zu erfassen und zu speichern. Zu berücksichtigen war nämlich auch, dass von der Videoüberwachungsmaßnahme überwiegend Personen in großer Anzahl betroffen gewesen wären, die keinerlei Anlass für eine Überwachung geboten hätten, da sie sich normgemäß verhalten. Demgegenüber rechtfertigte auch der von der Gemeinde mitgeteilte bisher eingetretene Schaden in Höhe von 4.000 € aus meiner Sicht nicht die Überwachung sämtlicher Weihnachtsmarktbesucher einer Kleinstadt, die an einer Weihnachtspyramide vorbeiziehen. Eine Videoüberwachung kommt im Hinblick auf Umfang, Tiefe und Ausmaß der personenbezogenen Datenverarbeitung z. B. regelmäßig nur bei Kriminalitäts-

schwerpunkten oder in Bereichen in Betracht, in denen eine deutlich gesteigerte Gefahr für Menschen und Sachen gegenüber dem Rest des Gemeindegebiets oder vergleichbaren anderen Gemeinden festzustellen ist.

Der durch die Videoüberwachung des Marktplatzes verursachte Eingriff in das Recht auf informationelle Selbstbestimmung wäre also unverhältnismäßig und damit rechtswidrig gewesen. Ich teilte dies der Gemeinde mit und machte sie darauf aufmerksam, dass die Installation einer Videoüberwachungsanlage allein keinen Schutz gegen Diebstahl und Vandalismus bietet. Erfahrungen zeigen, dass sich Straftäter allein durch den Anblick von Videoüberwachung kaum von ihrem Vorsatz abbringen lassen. Zudem wären auch noch grundrechtsschonendere Möglichkeiten gegenüber einer derart ausgeweiteten und anlasslosen Überwachung denkbar gewesen, so etwa eine gezielte Bestreifung des Weihnachtsmarktbereichs durch Gemeindebedienstete bzw. Wachpersonal. Die Gemeinde erklärte mir gegenüber letztendlich, auf die Installation und den Betrieb einer Videoüberwachung der Weihnachtspyramide verzichten zu wollen.

### 5.5.6 Unverschlüsselte E-Mail-Kommunikation - datenschutzorganisatorisch unzulässige Übermittlung personenbezogener Daten

Bei einer anlasslosen Kontrolle der Meldebehörde einer Stadtverwaltung fand ich bei einer stichprobenartigen Überprüfung der Akten des Einwohnermeldeamts den Ausdruck einer E-Mail-Nachricht der Zentralen Bußgeldstelle eines Landratsamts, die an die Meldebehörde gerichtet war. In der E-Mail wurde um die Übersendung eines Passfotos gebeten. Aus der - nach der Mitteilung weiter unten aufgeführten - Nachrichtenhistorie ergab sich, dass unter dem Bezug „Übersendung von Personalausweis-/Passfotos im Ordnungswidrigkeitenverfahren“ die Übermittlung verschiedener und zahlreicher personenbezogener Daten stattgefunden hatte.

Das Landratsamt bat ich hierzu um Stellungnahme. Nach Durchsicht der mit der Antwort übersandten Unterlagen und Informationen war nicht von einem datenschutzrechtlichen Verstoß im Zusammenhang mit der durch ministeriellen Erlass festgelegten Verfahrensweise für die Einsichtnahme der Bußgeldbehörde in das Personalausweis- und Passregister zum Bildabgleich bei Verkehrsordnungswidrigkeiten durch die Landkreisverwaltung auszugehen. Datenschutzrechtlich unzulässig war vielmehr die durch das Landratsamt genutzte unsichere Übermittlungsweise. Der elektronische Versand personenbezogener Daten per E-Mail ist nur mit zusätzlichen technischen Maßnahmen, nämlich einer Verschlüsselung zur Sicherung der Vertraulichkeit, datenschutzrechtlich zulässig durchführbar, § 9 Abs. 1 und 2 SächsDSG. Dies gilt selbst für den unverschlüsselten Versand von E-Mails innerhalb des SVN/KDN, da das Verwaltungsnetz trotz erhöhter Sicherheitsstandards im Hinblick auf eine Vertraulichkeit nicht per se als

sicheres Netz zu betrachten ist, solange Daten unverschlüsselt über das Internet übertragen werden. Das zuständige SMJus arbeitet gegenwärtig an verbesserten Konzepten und die Basiskomponente Elektronische Signatur und Verschlüsselung - Teilkomponente Secure Mail Gateway - bietet als zentral bereitgestellte Lösung Sicherheitsmaßnahmen für den elektronischen Versand vertraulicher Unterlagen. Alternativ wäre der Versand auf herkömmlichem Weg per Post oder Kurier zu erledigen.

Das Landratsamt teilte mir in seiner abschließenden Stellungnahme mit, dass Anfragen an die zuständigen Pass- und Personalausweisbehörden zukünftig nicht mehr per unverschlüsselter E-Mail übermittelt würden, sondern auf andere Weise. Zur grundsätzlichen Problematik vgl. auch 15/5.5.1.

### 5.5.7 Audio- und Video-Live-Übertragung von Stadtratssitzungen in einen weiteren Zuschauersaal im Rathaus

Im Berichtszeitraum bat mich eine große Stadtverwaltung um Unterstützung bei der Einrichtung von Liveübertragungen von Stadtratssitzungen. Die Stadt trug vor, dass seitens der Verwaltungsleitung beabsichtigt sei, im historischen Stadtverordnetensaal eine Videoübertragungsanlage zu installieren. Dabei ging die Kommune davon aus, dass es sich wegen der Liveübertragung rechtlich um keine Videoüberwachung handeln würde. Die optisch-elektronische Einrichtung sollte der Übertragung von Audio- und Videosignalen in eine angrenzende Räumlichkeit dienen, um so bei Veranstaltungen mit großem Bürgerinteresse zusätzliche Besucherplätze anbieten zu können.

Ich informierte die Stadt darüber, dass es sich bei der beabsichtigten Videoübertragung entgegen der Auffassung der Verwaltungsleitung um eine Videoüberwachung nach § 33 Abs. 1 SächsDSG handeln würde.

§ 33 SächsDSG bestimmt, dass die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig ist, soweit dies zur Aufgabenerfüllung, insbesondere zur Gewährleistung der öffentlichen Sicherheit und Ordnung, oder zur Wahrnehmung eines Hausrechts erforderlich ist und schutzwürdige Interessen Betroffener nicht überwiegen. Es war also zu prüfen, ob die Videoübertragung aus dem historischen Stadtverordnetensaal zur Aufgabenerfüllung der Stadtverwaltung erforderlich war und schutzwürdige Interessen Betroffener überwogen.

Nach § 37 SächsGemO gilt zunächst der Öffentlichkeitsgrundsatz der Stadtratssitzungen. Damit regelt der sächsische Gesetzgeber, dass die Sitzungen des Rats grundsätzlich öffentlich sind, um die Transparenz kommunaler Verwaltungstätigkeit zu gewährleisten. Öffentlichkeit der Sitzungen bedeutet, dass jedermann im Rahmen des hierfür zur Verfügung stehenden Platzes in der Reihenfolge des Eintreffens freien Zugang

zum Sitzungsraum hat. Die Gemeinderatsmitglieder und sonstigen Personen, die an der Sitzung teilnehmen, z. B. Gemeindebedienstete, die zu einem Tagesordnungspunkt berichten, sowie Bürger, deren Angelegenheiten personenbezogen in der Sitzung behandelt werden, haben es nach § 37 Abs. 1 Satz 1 SächsGemO nur hinzunehmen, dass Zuhörer der Sitzung beiwohnen, sich ggf. Notizen machen und anschließend beispielsweise in der Presse dazu berichtet wird. Aus kommunalrechtlicher Sicht ist zu beachten, dass nach der Rechtsprechung des BVerwG (Urteil vom 3. August 1990 - 7 C 14/90) es im öffentlichen Interesse liegt, dass die Willensbildung im Rat ungezwungen, freimütig und in aller Offenheit erfolgt. Nach der vorgenannten Entscheidung sind zum Beispiel Tonbandaufzeichnungen geeignet, diese Willensbildung dadurch zu beeinträchtigen, dass „insbesondere in kleineren und ländlichen Gemeinden weniger redegewandte Ratsmitglieder durch das Bewusstsein des Tonmitschnitts ihre Spontanität verlieren, ihre Meinung nicht mehr ‚geradeheraus' vertreten oder schweigen, wo sie sonst gesprochen hätten".

Schutzwürdige Interessen Betroffener überwogen im konkreten Fall nach meiner Überzeugung nicht. Es handelte sich auch nicht um eine die Willensbildung des Stadtrats beeinträchtigende Maßnahme, sondern um einen bedarfsbezogenen Betrieb einer Videokamera mit dem Ziel einer reinen Audio- und Video-Live-Übertragung einer Stadtratssitzung in einen Nebenraum. Den Angaben der Kommune zufolge sollte die Technik lediglich dazu eingesetzt werden, um bei Fehlen von Plätzen einer größeren Anzahl interessierter Bürger die Teilnahme an den Stadtratssitzungen zu ermöglichen. Um die schutzwürdigen Interessen der Betroffenen zu wahren, sollte die Ausrichtung der Kamera in der Weise erfolgen, dass nur der jeweilige Redner, die übrigen Ratsmitglieder jedoch - wenn überhaupt, dann nur in einer Übersichtsposition - sowie die sonstigen Zuhörer gar nicht zu sehen sind.

Die geplante Audio- und Video-Live-Übertragung war unter den Voraussetzungen, dass es sich ausschließlich um eine bedarfsbezogene Bildübermittlung in Echtzeit ohne Aufzeichnungs- oder weitere Bearbeitungsmöglichkeit handelt und die schutzwürdigen Interessen der Betroffenen gewahrt bleiben sollten, datenschutzrechtlich zulässig.

Die Kommune als Betreiber der Echtzeit-Bildübermittlung hatte allerdings sicherzustellen und nachzuweisen, dass neben der nicht existierenden Aufzeichnungsmöglichkeit auch eine sonstige weitere Bearbeitung der Bildübermittlung ausgeschlossen war. Wegen der durch die Wirkung einer Kamera möglichen Beeinträchtigung des allgemeinen Persönlichkeitsrechts empfahl ich der Kommune zudem, vor jedem Einsatz der Kamera alle Sitzungsteilnehmer und Besucher vor der Sitzung ausdrücklich über die Art und den Umfang der Übertragung zu informieren. Zusätzlich sollte auf Schildern darauf

hingewiesen werden, dass die Kamera ausschließlich zum Zwecke der Live-Übertragung von Audio- und Videosignalen in den benachbarten Sitzungssaal installiert wurde.

Die Stadtverwaltung teilte mir als Antwort auf meine Empfehlungen mit, dass die zuständigen Fachbereiche der Kommune eine entsprechende Handlungsvorschrift inklusive des erforderlichen Datenschutzkonzepts erstellen würden. Weiter informierte sie mich, dass die Anlage klar und deutlich als Videoübertragungsanlage gekennzeichnet werden solle (Piktogrammhinweis). Zum Schutz der Beschäftigten sollte die Maßnahme in der hausinternen Dienstvereinbarung zum Betrieb von Videoanlagen berücksichtigt werden. Das von mir vorgeschlagene Vorgehen zur Information der Sitzungsteilnehmer und Besucher der Stadtratssitzungen sollte übernommen werden.

Gegenüber anderen Vorgängen, bei denen ich Bildübertragungen regelmäßig als nicht erforderlich und zulässig angesehen hatte - vgl. ausführlich 13/5.5.1 - war hier entscheidend, dass die Bild- und Tonübertragungen in einen weiteren Saal des Rathauses erfolgen sollte, in einen Bereich also, auf den sich auch das Hausrecht erstreckt und in dem die Stadtverwaltung beeinträchtigende Handlungen und Datenschutzverletzungen, wie das Abfilmen und Tonbandaufzeichnungen der Sitzungen, zu unterbinden in der Lage ist.

## 5.6 Baurecht; Wohnungswesen

### 5.6.1 Zulässige Datenerhebung durch die untere Wasserbehörde im Baugenehmigungsverfahren

In einer Eingabe beschwerte sich die Betreiberin einer Firma über eine Datenerhebung durch die untere Wasserbehörde eines Landratsamts. Gegenstand der Beschwerde war die Forderung nach Auskünften über eine Heizöltankanlage für die Lagerung von 6000 Liter Heizöl, die anlässlich einer Begehung wegen des Bauantrags der Firma stattfand. Der Antrag betraf den Anbau eines Heizraums mit einem Feststoffkessel auf dem Firmengelände. Die untere Wasserbehörde war im Rahmen des Baugenehmigungsverfahrens als Träger öffentlicher Belange gehört worden.

Gemäß § 53 Abs. 1 SächsWG hat der Betreiber derartiger Anlagen das Einbauen, Aufstellen, Betreiben oder Stilllegen (länger als ein Jahr) der zuständigen Behörde mindestens einen Monat vor Beginn der Maßnahme anzuzeigen. Bei der unteren Wasserbehörde lag ein entsprechender Antrag nicht vor. Von der Verordnungsermächtigung nach § 53 Abs. 2 SächsWG, das Anzeigeverfahren näher zu regeln, hat die oberste Wasserbehörde bisher keinen Gebrauch gemacht.

Für die Anhörung der Firma durch die untere Wasserbehörde und die damit verbundene Datenerhebung war § 53 Abs. 1 SächsWG eine ausreichende Rechtsgrundlage. Zulässig wäre die Anhörung nach § 53 Abs. 1 SächsWG i. V. m. § 12 Abs. 5 SächsDSG auch dann gewesen, wenn die den Bauantrag für den Anbau eines Heizraums mit einem Feststoffkessel stellende Firma die Heizöltankanlage nicht selbst betrieben hätte, sondern diese durch einen vormaligen Eigentümer betrieben worden wäre. In diesem Fall hätte die untere Wasserbehörde auf den Erhebungszweck für die personenbezogenen Daten hinzuweisen gehabt.

## 5.7 Statistikwesen

### 5.7.1 Ausfall ordnungsgemäßer Aktenführung im Statistischen Landesamt

Wegen eines vollständigen Ausfalls ordnungsgemäßer Aktenführung bei Vorgängen der administrativen Steuerung der Verarbeitung personenbezogener Daten, die den Zensus 2011 betrafen, habe ich das StaLa auf Grundlage von § 29 Abs. 1 Satz 1 Nr. 1 SächsDSG beanstanden müssen:

Nach § 6 Abs. 1 ZensG 2011 führen die statistischen Ämter der Länder eine Gebäude- und Wohnungszählung als schriftliche Befragung durch, deren informationstechnische Verarbeitung und Aufbereitung nach § 12 Abs. 7 ZensG 2011 dem Statistischen Landesamt des Freistaates Sachsen zentral für alle Bundesländer obliegt. Wegen dieser besonderen (bundesweiten) Verantwortung der hiesigen Statistikbehörde und zahlreicher Eingaben, die Unstimmigkeiten bei der Gebäude- und Wohnungszählung betrafen, habe ich mich veranlasst gesehen, das StaLa wegen der administrativen Steuerung der die Verarbeitung personenbezogener Daten betreffenden Gebäude- und Wohnungszählung zu kontrollieren, nachdem mir auf schriftliche Fragen keine hinreichenden Auskünfte erteilt worden waren.

Bei den Kontrollen habe ich festgestellt, dass entgegen Ziffern II.1, III., VI., VII., VIII. und X. der *Gemeinsamen Verwaltungsvorschrift der Sächsischen Staatskanzlei, des Sächsischen Staatsministeriums des Innern, des Sächsischen Staatsministeriums der Finanzen, des Sächsischen Staatsministeriums für Kultus, des Sächsischen Staatsministeriums für Wissenschaft und Kunst, des Sächsischen Staatsministeriums für Wirtschaft und Arbeit, des Sächsischen Staatsministeriums für Soziales und des Sächsischen Staatsministeriums für Umwelt und Landwirtschaft über die Verwaltung von Unterlagen (VwV Registraturordnung - VwVRegO)* vom 21. November 2008 (SächsABl. Jg. 2008, Bl.-Nr. 50, S. 1671) sowie unter Missachtung zahlreicher Bestimmungen der *Verwaltungsvorschrift der Sächsischen Staatsregierung zur Regelung des Dienstbetriebes für die Behörden des Freistaates Sachsen (VwV Dienstordnung)* vom 6. September 2010 (SächsABl. Jg. 2010, Bl.-Nr. 38, S. 1316, ber. S. 1532) sowie der hauseigenen *Dienst-*

*anweisungen zur Behandlung von Posteingängen (DA 08/01/2006 vom 1. Mai 2006), zur Gestaltung des Schriftverkehrs, Zeichnung und Verfügungsaufbau (DA 03/02/2003 vom 15. April 2003)* sowie zur *Zeichnungsregelung (DA 04/05/2003 vom 15. April 2003)* im Referat 23 (Projekt Zensus), dessen übergeordneter Abteilung 2 sowie im Leitungsbereich des StaLa hinsichtlich der administrativen Steuerung der Verarbeitung personenbezogener Daten, die den Zensus 2011 betreffen, keine ordnungsgemäßen Akten i. S. d. genannten Vorschriften geführt wurden. Stattdessen wurden die für die administrative Steuerung der Verarbeitung personenbezogener Daten aktenrelevanten Vorgänge (z. B. Verträge und Korrespondenz mit Dritten, die in das Verarbeitungshandeln involviert sind, Protokolle der für das Verarbeitungshandeln bedeutsamer Sitzungen zahlreicher Gremien sowie interne Vorgänge, wie Entwürfe, Vermerke und Verfügungen)

- ohne vorgangsweise Ordnung, Zusammenstellung (Heftung) und Inhaltsbezeichnung,
- insbesondere ohne bzw. allenfalls unter nachträglicher Vergabe eines Aktenzeichens,
- verteilt bzw. verstreut auf eine Vielzahl von Bediensteten, deren Räumlichkeiten sowie deren diverser elektronischer und physischer Aufbewahrungssysteme sowie
- in zahlreichen Fällen allein elektronisch existent (elektronische Korrespondenz [Mails] und Textdateien bzw. Scans)

nach Belieben des jeweiligen Bearbeiters und seiner Vorgesetzten als quasi höchstpersönliches Arbeitsmittel ohne eine ansatzweise systematische Dokumentation des tatsächlichen Verwaltungshandelns geführt. Die Vollständigkeit und Chronologie der Unterlagen, die Behandlung im Geschäfts- und Verwaltungsgang sowie Entwurfsstände, Verantwortlichkeiten und Mitzeichnungen habe ich wegen der Mängel in der Aktenführung, die einem vollständigen Ausfall gleichkam, bei meinen Kontrollen nicht im Mindesten nachvollziehen können, so dass sich die öffentliche Stelle schon dadurch meiner Kontrolle hat entziehen können, dass sie ihr Verwaltungshandeln nicht dokumentiert hat. Die von mir erbetenen Verwaltungsvorgänge konnten folglich trotz großzügigster Gewährung an Zeit nicht als Akten im Rechtssinne und auch sonst nicht beigebracht werden. Der vollständige Ausfall ordnungsgemäßer Aktenführung zog sich dabei durch alle Ebenen und fand somit seine Ursache nicht in mangelnder Dienstaufsicht des Leitungsbereichs, der vielmehr in vergleichbar nachlässiger Weise verfuhr:

So wurde nach Anweisung der Präsidentin alle Eingangspost mit ihrer Amtsbezeichnung oder ihrem Namen in der Adressierung sowie die Korrespondenz herausgehobener Absender (u. a. Staatskanzlei und Ministerien, auch der Sächsische Datenschutzbeauf-

tragte) in der Weise ungeöffnet direkt dem Leitungsbereich zugestellt, dass die Poststelle lediglich einen Eingangsstempel auf dem Umschlag aufbrachte. Diese „Post der Präsidentin“ wurde erst von deren Vorzimmerkraft geöffnet, jedoch auch dort mit keinem Eingangsstempel oder Aktenzeichen versehen. Die Vorzimmerkraft verfügte auf den Schreiben selbständig die weitere Behandlung im Haus, registrierte sie jedoch nicht. Mit den auf diese Weise vorgeschlagenen Verfügungen gingen die Schreiben dann zur Präsidentin, welche die Verfügungen ändern oder ergänzen konnte. (Farbige) Sichtvermerke und Paraphen der Präsidentin waren auf den Schreiben nur sporadisch zu finden. Die Vergabe von Aktenzeichen erfolgte - wenn überhaupt - erst in den Abteilungen bzw. Referaten. In einem Referat wurden zwar teilweise Aktenzeichen vergeben, hierzu aber keine Akten im Rechtssinne geführt (s. o.). Ausgangsschreiben des Referates erhielt die Präsidentin zu den verfügten Terminen direkt von den Abteilungen bzw. Referaten, vorzugsweise auf elektronischem Wege. Diese wurden dann verändert oder unverändert zur Unterschrift oder mit eingescannter Unterschrift für die Präsidentin in deren Vorzimmer ausgedruckt. Mitgezeichnete Entwürfe gab es in der Regel nicht, sondern allein elektronische Bearbeitungsketten, welche aber den Geschäfts- und Bearbeitungsgang nicht in der gebotenen Weise dokumentiert rechtssicher haben erkennen lassen und mangels Ausdruck der Bearbeitungsstände und damit ordnungsgemäßer Aktenführung im Rechtssinne undokumentiert blieben. Vereinzelt wurden Aktenzeichen der Ausgangsschreiben erst zum Abschluss im Leitungsbereich vergeben, allerdings ohne dass es zu einer Aktenführung beim Entwurfsverfasser kam, dem lediglich ein Ausdruck mit dem Absendevermerk zuging.

Zur Pflicht ordnungsgemäßer Aktenführung auch wegen der Kontrolle durch unabhängige Stellen führt das BVerwG (Beschluss vom 16. März 1988 - 1 B 153/87, NVwZ 1988, S. 621 f.) indes Folgendes aus:

> *„Die den Behörden nach dem Grundgesetz obliegende Vollziehung der Gesetze ist nicht ohne eine Dokumentation der einzelnen Verwaltungsvorgänge denkbar, die das bisherige sachbezogene Geschehen sowie mögliche Erkenntnisquellen für das künftig in Frage kommende behördliche Handeln enthält; dies macht die Führung von Akten erforderlich, ohne dass dies eines ausdrücklichen Ausspruchs im Gesetz bedürfte (BVerfG, NJW 1983, 2135). [...] Die Pflicht zur Aktenführung soll den Geschehensablauf wahrheitsgetreu und vollständig dokumentieren und dient damit in zweifacher Weise der Sicherung gesetzmäßigen Verwaltungshandelns. Die Dokumentation soll den Geschehensablauf so, wie er sich ereignet hat, in jeder Hinsicht nachprüfbar festhalten. Sie soll hierbei nicht lediglich den Interessen der Beteiligten oder der entscheidenden Behörde dienen, sondern auch die Grundlage für die kontinuierliche Wahrnehmung der Rechts- und Fachaufsicht und für die parlamentarische Kontrolle*

*des Verwaltungshandelns bilden. Damit wirkt die Pflicht zur wahrheitsgetreuen und vollständigen Aktenführung zugleich auch präventiv insofern auf das Verwaltungshandeln ein, als sie die Motivation zu allseits rechtmäßigem Verwaltungshandeln stärkt und rechtswidriges Verwaltungshandeln erschwert.*“

Die Aktenführungspflicht öffentlicher Stellen ist schon Ausfluss des Rechtsstaatsprinzips, da nur eine geordnete Aktenführung einen rechtsstaatlichen Verwaltungsvollzug mit der Möglichkeit einer Rechtskontrolle durch Gerichte und Aufsichtsbehörden sowie sonst hierzu berufene Stellen ermöglicht (vgl. Ritgen in Knack/Henneke, VwVfG, 9. Aufl. 2011, § 24 Rdnr. 7 m. w. N.). Zur Rechtskontrolle berufene Stelle ist wegen Art. 57 SächsVerf und § 27 Abs. 1 SächsDSG auch der Sächsische Datenschutzbeauftragte; seine Kontrollbefugnis würde durch einen weitgehenden Ausfall in der Aktenführung mit der Folge ins Leere laufen, mangels tauglicher Prüfungsobjekte nicht seinem verfassungsrechtlichen Auftrag zum Schutz des Grundrechts des Einzelnen auf informationelle Selbstbestimmung auch nur im Ansatz gerecht werden zu können.

Zugleich folgt das Erfordernis des zu dokumentierenden Verwaltungshandelns, also die Verpflichtung zu ordnungsgemäßer Aktenführung, nicht nur aus dem Rechtsstaatsprinzip, sondern hinsichtlich solcher Vorgänge, welche die administrative Steuerung der Verarbeitung personenbezogener Daten und damit in letzter Konsequenz auch das den Einzelnen betreffende Verarbeitungshandeln zum Gegenstand haben, ebenso aus der Pflicht gegenüber dem Betroffenen, durch angemessene organisatorische Maßnahmen die Revisionsfähigkeit und Transparenz - auch der Steuerungsprozesse - des ihn betreffenden Verarbeitungshandelns zu gewährleisten (§ 9 Abs. 1, Abs. 2 Nr. 5 und 6 SächsDSG).

Mithin ist es nach § 28 Abs. 1 Satz 1 SächsDSG Teil der Unterstützungspflicht öffentlicher Stellen gegenüber dem Sächsischen Datenschutzbeauftragten, ungeachtet eines konkreten Kontrollverlangens die jederzeitige organisatorische Gewähr der eigenen Kontrollfähigkeit jedenfalls durch ein Mindestmaß an Aktenführung sicherzustellen. Dem ist das StaLa nicht gerecht geworden.

## 5.8 Archivwesen

### 5.8.1 Auskunft aus dem Universitätsarchiv

Erneut (vgl. auch 9/5.8.4 und 11/5.8.2.) musste ich einer Petentin, die Nachforschungen zur Person ihres (ihr unbekannten) Vaters durchführen wollte, mitteilen, dass derzeit keine Rechtsvorschrift existiert, die eine Nutzung personenbezogenen Archivguts zu diesem Zwecke erlaubt.

Eine Änderung könnte sich hier erst nach Inkrafttreten der Neufassung des Sächsischen Archivgesetzes ergeben (vgl. LT-Drs. 5/9386), wonach eine Verkürzung der Schutzfristen auch zur Wahrnehmung berechtigter Belange einer Person in Betracht kommt.

Als ein solches berechtigtes Anliegen müsste auch die Recherche der eigenen Abstammung angesehen werden.

### 5.8.2 Anspruch auf Einsichtnahme in eine Jugendhilfeakte beim kommunalen Kreisarchiv

Die Petentin hatte wiederholt im Jugendamt des Landkreises Einsicht in die sie betreffende archivierte Jugendhilfeakte genommen, wobei bei einer zweiten Akteneinsicht im Jugendamt wohl Aktenbestandteile fehlten. Sie begehrte deshalb eine erneute Einsichtnahme unmittelbar beim Archiv. Das betreffende Kreisarchiv lehnte dies zunächst mit der Begründung ab, dass ein entsprechendes Verlangen gegenüber dem Jugendamt geltend zu machen sei.

Ich habe gegenüber dem Kreisarchiv folgende Stellungnahme abgegeben:

Bei einem Kreisarchiv handelt es sich um ein kommunales Archiv im Sinne des § 13 SächsArchivG. Gemäß § 13 Abs. 3 Satz 1 SächsArchivG gelten die §§ 5 Abs. 4 bis 8 und die §§ 6 bis 11 für kommunale Archive entsprechend, so dass Betroffene auch gegenüber kommunalen Archiven einen Anspruch haben, Auskunft darüber zu erhalten, ob in dem Archivgut Daten zu ihrer Person enthalten sind sowie darüber hinaus, wenn dies der Fall ist, ein Recht auf Einsicht und Herausgabe von Kopien der Unterlagen haben, vgl. § 6 Abs. 3 Satz 1 und 2 SächsArchivG.

Da dieser Auskunftsanspruch als unmittelbarer Anspruch gegen das (jeweilige) Archiv ausgestaltet ist, ist nicht nachvollziehbar, weshalb eine Einsichtnahme bzw. das Verlangen nach Kopien aus einer archivierten Jugendhilfeakte gegenüber dem Jugendamt geltend gemacht werden sollte.

Das Kreisarchiv hat sich meiner Rechtsauffassung angeschlossen und die Petentin um Terminvereinbarung gebeten.

## 5.9 Polizei

### 5.9.1 Belehrung zur Nutzung polizeilicher Dateien

In meinem letzten Tätigkeitsbericht informierte ich über die besondere Bedeutung der Einhaltung datenschutzrechtlicher Vorschriften im Zusammenhang mit der Nutzung polizeilicher Datenbanken (15/5.9.4). Dabei ging es um die strengen Voraussetzungen

eines Abrufs personenbezogener Daten aus solchen Dateien. Aufgrund des Anstiegs entsprechender Bußgeldverfahren gegen Polizeibeamte seit 2007 und der offensichtlichen Unsicherheit vieler Bediensteter über die Voraussetzungen von Abrufen bat ich das SMI, dieser Frage - auch vor dem Hintergrund der allgemeinen Pflicht zur Amtsverschwiegenheit - besondere Aufmerksamkeit zu schenken.

Das LKA entwarf daraufhin zum Zwecke einer landeseinheitlichen Verfahrensweise ein gesondertes Belehrungsschreiben zur Nutzung der polizeilichen Informationssysteme. Dieses soll an die Verpflichtung auf das Datengeheimnis (§ 6 SächsDSG) angehängt werden. Diese ist generell „bei der Aufnahme ihrer Tätigkeit“ durchzuführen; eine spezielle Unterrichtung über die beim Abruf personenbezogener Daten aus Dateien zu beachtenden Vorschriften ist sinnvollerweise spätestens bei der Erstvergabe von Zugriffsrechten durchzuführen.

Im Rahmen meiner Beteiligung forderte ich zum einen hervorzuheben, dass es in jedem Einzelfall eines dienstlichen Anlasses für die Datenrecherche bedarf. Die technische Möglichkeit des Zugriffs hat nicht bereits die Zulässigkeit des Abrufs zur Folge. Zum anderen forderte ich, die Bediensteten auch über die (Un-)Zulässigkeit der Nutzung der Informationssysteme ohne dienstlichen Anlass zu unterrichten. Bereits der erste Schritt der Datenrecherche, d. h. die Festlegung der Recherchebedingungen und die daraufhin erfolgende Anzeige, ob und in welcher polizeilichen Datenbank Eintragungen zu bestimmten Personen vorhanden sind, stellt einen Abruf personenbezogener Daten i. S. v. § 38 Abs. 1 Nr. 1c SächsDSG oder zumindest einer unbefugte Datenverarbeitung i. S. v. § 38 Abs. 1 Nr. 1a SächsDSG dar. Dies gilt selbst dann, wenn daraufhin aus der Datei keine weitergehenden Informationen abgerufen werden.

Das SMI sagte zu, das Formular entsprechend zu ändern.

In Zukunft wird der Verpflichtung auf das Datengeheimnis bei Bediensteten, die Zugang zu datenbankbasierten Informationssystemen haben oder erhalten sollen, ein Belehrungsformular zur Nutzung polizeilicher Informationssysteme angehängt werden. Die Belehrung wird gemäß § 6 Abs. 2 SächsDSG bei der Erstvergabe von Zugriffsrechten erfolgen und insbesondere auf die Erforderlichkeit eines konkreten dienstlichen Anlasses für jede einzelne Nutzung hinweisen.

### 5.9.2 Erhebung von Kfz-Kennzeichen am Flughafenzaun durch einen Flughafen-Sicherheitsdienst und Übermittlung an das LKA

Im Frühjahr 2012 erhielt ich den Hinweis eines Journalisten, wonach das LKA Sachsen infolge einer Gefahrenanalyse im Zusammenhang mit der militärischen Nutzung des Flughafens den dort eingesetzten privaten Sicherheitsdienst beauftragt hätte, Kfz-

Kennzeichen von Fahrzeugen, die sich in der Nähe des Flughafenzauns aufhalten, zu registrieren und dem LKA zu übermitteln. Hiervon betroffen wären auch Mitglieder von Bürgerinitiativen, die das Flughafengelände - legal - für eigene Zwecke beobachteten und ihre Erkenntnisse im Internet veröffentlichten.

Ich nahm dies zum Anlass einer zunächst schriftlichen Kontrolle nach § 27 SächsDSG, bat um Stellungnahme und fragte insbesondere nach, welche Daten erhoben werden sollten (Kfz-Kennzeichen, Personenbeschreibungen, Fotographien), zu welchem Zweck die Übermittlung erfolgen sollte und mit welchen polizeilichen Dateien ein Abgleich erfolgen würde. Daraufhin teilte das LKA zunächst mit, dass im Zusammenhang mit der Gefährdungslagebewertung, welche aufgrund der Präsenz von us-amerikanischen Truppen und der im Auftrag der NATO stationierten russischen Antonow-Flugzeuge erfolgt sei, im Jahr 2008 eine Besprechung mit dem Flughafenbetreiber stattgefunden habe. Hierbei sei „thematisiert“ worden, dass Kfz-Kennzeichen von offensichtlich zu Ausspähungszwecken genutzten Fahrzeugen an das LKA übermittelt werden können. Auf meine Nachfrage, wie viele Fälle von Datenübermittlungen es seitdem gegeben habe, gab das LKA an, dass im Jahr 2008 ganz vereinzelt Kennzeichen von Kraftfahrzeugen übermittelt worden wären, die als gefährdungsrelevant eingeschätzt wurden. Das LKA habe diese Kennzeichen gemäß § 43 Abs. 1 SächsPolG zur Gefahrenerforschung auf Aktualität, Personenzugehörigkeit und für diese Personen auf mögliche Einträge in den polizeilichen Auskunftssystemen geprüft. Da zu dem Personenkreis keine polizeilich relevanten Erkenntnisse vorgelegen hätten, seien die Daten nicht gespeichert worden. Im Hinblick auf diese Auskunft und die darauf beruhende Einschätzung, dass sich das Handeln der Polizei noch im rechtlich zulässigen Rahmen bewegt hat, habe ich von weiteren Maßnahmen abgesehen.

### 5.9.3 Ermittlungsverfahren aufgrund ungenauer Recherche in polizeilichen Auskunftssystemen

Im Frühjahr 2011 trug mir ein Petent vor, er sei aufgrund einer Namensverwechslung bei der Polizei mit einem Ermittlungsverfahren überzogen worden. Seine Daten seien durch die Polizei einmal im Rahmen eines gegen seine Freundin gerichteten Ordnungswidrigkeitenverfahrens erfasst und nach Abschluss des Verfahrens offenbar nicht gelöscht worden.

Meine Nachfragen bei den beteiligten Polizeibehörden ergaben, dass eine andere Polizeidienststelle um die Ermittlung der aktuellen Adresse des Beschuldigten im Vorgangsbearbeitungssystem IVO ersucht hatte. Die konkrete Beamtin gab, um eine größere Treffermenge zu erzielen, lediglich den Vor- und Nachnamen, nicht aber das Geburtsdatum des Beschuldigten ein und übermittelte die so gefundenen Adressdaten,

nämlich die des mit dem Beschuldigten namensgleichen Petenten, an die ersuchende Polizeidienststelle. Diese übermittelte die Daten wiederum ohne weitere Prüfung an eine dritte Polizeidienststelle zur Durchführung der Beschuldigtenvernehmung, die dann den Petenten traf.

Ich habe die beteiligten Polizeibehörden darauf hingewiesen, dass hier nicht die erforderliche Sorgfalt an den Tag gelegt worden ist. Alle Bediensteten hätten sich von der Richtigkeit der Daten überzeugen müssen oder aber darauf hinweisen müssen, dass dies nicht erfolgt sei. Spätestens vor der Vornahme konkreter Maßnahmen gegen eine Person, hier der Vorladung zur polizeilichen Vernehmung, hätte Sicherheit über die Identität des Vorzuladenden geschaffen werden müssen, etwa durch Abgleich des Geburtsdatums. Ich habe die Polizeidienststellen aufgefordert, die Beamten entsprechend zu belehren.

Die Speicherung der Daten des Petenten in IVO war dagegen datenschutzrechtlich nicht zu beanstanden, da die Speicherung zur Vorgangsverwaltung oder nach Abschluss des Vorgangs zu einer zeitlich befristeten Dokumentation polizeilichen Handelns zulässig ist (§ 43 Abs. 1 Satz 1 SächsPolG). Die Löschung der Daten erfolgt automatisch nach einem festgelegten Zeitraum, der zum Zeitpunkt der Datenrecherche noch nicht abgelaufen war. Auf Antrag kann die Löschung auch früher erfolgen, wenn die Daten von der Polizei nicht mehr benötigt werden. Die im Zusammenhang mit dem gegen seine Freundin gerichteten Ordnungswidrigkeitenverfahren erhobenen Daten des Petenten wurden auf seinen Antrag hin im Mai 2011 gelöscht.

### 5.9.4 Speicherung personenbezogener Daten im Polizeilichen Auskunftssystem Sachsen (PASS) - Beachtung der gesetzlichen Löschungspflicht, wenn der Tatverdacht entfällt

Im Berichtszeitraum wandte sich ein Petent an mich, der aufgrund seiner beruflichen Tätigkeit in öffentlichen Gebäuden eingesetzt wurde, die bestimmten Sicherheitsanforderungen unterliegen. Im März 2011 wurde ihm nunmehr der Zugang zu einer obersten Landesbehörde durch Mitteilung an seinen Arbeitgeber verwehrt und er fürchtete berufliche Konsequenzen. Er vermutete, dass ein fehlerhafter Datensatz existieren könnte, da das LKA zu einem früheren Zeitpunkt gegen ihn wegen eines Verdachts des strafbaren Umgangs mit explosionsgefährlichen Stoffen ermittelt hatte. Eine in diesem Zusammenhang durchgeführte Wohnungsdurchsuchung hatte den Verdacht nicht erhärten können. Das Verfahren gegen den Betroffenen wurde daraufhin im Mai 2008 eingestellt. Die Daten aus dem Ermittlungsverfahren wären nach § 44 Abs. 2 Satz 2 SächsPolG zu löschen gewesen.

Dennoch informierte eine Polizeidirektion, Fachbereich Objektschutz, noch im März 2011 eine oberste Landesbehörde über ihre Sicherheitsbedenken hinsichtlich des weiteren Einsatzes des Petenten. Grund war eine Eintragung im polizeilichen Auskunftssystem „PASS“. Auf meine Anfrage teilte das LKA im Mai 2011 mit, dass die Löschung des Datensatzes - auf ein entsprechendes Auskunftsersuchen des Petenten - zwischenzeitlich veranlasst worden sei und nicht mehr nachvollzogen werden könne, warum die Löschung nicht unmittelbar nach der Verfahrenseinstellung erfolgt sei. Die Speicherung erfolgte demnach nicht nur ohne Rechtsgrundlage, sondern verstieß zudem gegen eine ausdrückliche gesetzliche Löschungspflicht.

Wie sich bei der Einsichtnahme in die Verfahrensakte ergab, hatte die Staatsanwaltschaft auf dem Formblatt zur Erledigung des Verfahrens nicht angegeben, dass die Einstellung erfolgte, weil kein Straftatbestand erfüllt war, sondern es wurde aus „Routine“ angekreuzt, dass die Einstellung aufgrund der Nicht-Nachweisbarkeit der Täterschaft bzw. Schuld erfolgte. Ich bat die Staatsanwaltschaft nunmehr darum das Formblatt sowie die das Verfahren betreffenden Datensätze entsprechend zu korrigieren. Weiterhin bat ich die Generalstaatsanwaltschaft darum, die sächsischen Staatsanwaltschaften darauf aufmerksam zu machen, dass bei der Angabe des Einstellungsgrunds im Rahmen der abschließenden Verfügungen mit der erforderlichen Sorgfalt vorzugehen ist, da dieser Auswirkungen auf Speicherfristen hat und unzutreffende Informationen zu gravierenden Nachteilen für den Betroffenen führen können. Des Weiteren forderte ich die Polizeidirektion auf, gegenüber der obersten Landesbehörde die Sicherheitsbedenken bezüglich des Petenten zurückzunehmen.

Gegen das LKA habe ich eine förmliche Beanstandung gemäß § 29 SächsDSG ausgesprochen, da dieses für die Speicherung der Daten über Mai 2008 hinaus verantwortlich war. Dem lag ein Verstoß gegen § 43 Abs. 2 Satz 2 SächsPolG zugrunde, wonach der Polizeivollzugsdienst personenbezogene Daten, die er im Rahmen strafrechtlicher Ermittlungsverfahren oder von Personen erfahren hat, die verdächtig sind, eine Straftat begangen zu haben, zu löschen hat, wenn der der Speicherung zugrunde liegende Verdacht entfällt.

Zwar hatte die Staatsanwaltschaft auf dem Vordruck zur Mitteilung des Verfahrensausgangs einen falschen Einstellungsmarker gesetzt, der die weitere Speicherung der Daten zuließ. Dies entlastet das LKA aber nicht, da es der gesetzlichen Löschungspflicht bereits aufgrund der eigenen Erkenntnisse nachkommen konnte und musste. Zumindest hätte das LKA nachfragen müssen, wenn sich aus der Mitteilung der Staatsanwaltschaft zum Verfahrensausgang ein Widerspruch zum eigenen Ermittlungsergebnis ergibt. Das LKA teilte mir mit, dass der Vorfall zum Anlass genommen wird, die Mitarbeiter entsprechend zu sensibilisieren.

### 5.9.5 Zuverlässigkeitsüberprüfung von Fremdpersonal vor Betreten eines Behördenareals

Ein Energieversorgungsunternehmen wandte sich an mich und bat um datenschutzrechtliche Überprüfung einer neuen Handhabung, wonach seine Mitarbeiter vor Betreten eines Behördenareals, auf dem u. a. eine Polizeidienststelle ansässig ist, durch das LKA anhand polizeilicher Dateien auf ihre Zuverlässigkeit hin überprüft werden sollen. Hierfür sollte zwei Wochen vor Arbeitsbeginn ein entsprechendes „Antragsformular“ durch den zum Einsatz vorgesehenen Mitarbeiter ausgefüllt werden, in das neben persönlichen Daten auch Angaben zum Arbeitgeber und zum konkreten Einsatzort einzutragen waren. Im Fall der Zutrittsverweigerung sollte der Arbeitgeber, allerdings ohne nähere Begründung, darüber informiert werden.

Ich wendete daraufhin ein, dass eine solche Datenerhebung und nachfolgende Zuverlässigkeitsüberprüfung tatsächlich nur wenig geeignet erscheint, Sabotageakte oder Anschläge etc. durch Fremdpersonal vor Ort zu verhindern. Hierfür erschien mir vielmehr einzig die Begleitung des eingesetzten Fremdpersonals während seines Aufenthalts im Behördenareal geeignet, eine Auffassung, die das LKA grundsätzlich teilte, aber wegen des hohen Personalaufwands für kaum realisierbar hielt.

In meinen Gesprächen mit dem LKA konnte ich jedoch wenigstens eine differenziertere Verfahrensweise erreichen. Künftig will das LKA solche „freiwilligen“ Überprüfungen regelmäßig nur noch auf jene Unternehmen anwenden, die erfahrungsgemäß auch Hilfs- oder Saisonkräfte beschäftigen oder sonstigen konkreten Anlass für eine Überprüfung bieten. Der betroffene Arbeitnehmer soll formularmäßig und voll informiert in seine Überprüfung einwilligen. Die Entscheidung über eine Zutrittsverweigerung soll insbesondere unter Berücksichtigung von Art und Schwere evtl. vorliegender Strafverfahren und ihres Verfahrensausgangs erfolgen. Außerdem sollen der Zutrittsort (z. B. Außenbereich, sensitive Bereiche wie elektrische oder IT-Anlagen) und die Verweildauer im Behördenareal in die Risikoeinschätzung mit einbezogen werden. Im Falle einer Ablehnung sollen die Gründe sorgfältig schriftlich dokumentiert werden. Das Ergebnis der Prüfung sowie die hierfür erhobenen personenbezogenen Daten sollen höchstens zwei Jahre lang aufbewahrt werden. Stehen in diesem Zeitraum weitere Arbeitseinsätze an, soll keine erneute Überprüfung erfolgen.

Mit dieser Verfahrensweise kann ich leben; ich danke dem LKA für die konstruktive Zusammenarbeit.

## 5.10 Verfassungsschutz

In diesem Jahr nicht belegt.

## 5.11 Landessystemkonzept/Landesnetz

### 5.11.1 In der Endlosschleife: VwV SVN

In 15/5.11.1 hatte ich über ein Billing- und Reportingsystem zur Abrechnung und Kontrolle der dienstlichen Telefonate der Behörden im Freistaat berichtet und in diesem Zusammenhang bereits auf das Fehlen einer entsprechenden Rechtsvorschrift hingewiesen. Ende 2011 ist die zum Zeitpunkt des letzten Tätigkeitsberichts noch geltende *Verwaltungsvorschrift der Sächsischen Staatsregierung über die Errichtung, den Betrieb und die Benutzung dienstlicher Telekommunikationsanlagen für die Landesverwaltung des Freistaates Sachsen (Dienstanschlussvorschrift - DAV)* außer Kraft getreten, ohne dass eine Nachfolge-Rechtsvorschrift den Umgang mit Verbindungs- und Rechnungsdaten der Telefonie regelte. Dies war bereits Ende 2009 bekannt, da zu diesem Zeitpunkt die VwV letztmalig verlängert wurde sowie die Umstellung auf das Sächsische Verwaltungsnetz (SVN) im Gange war und die DAV sich noch auf das Vorgänger-Netz, den Info-Highway bezog.

Seit dem ist viel Zeit vergangen und zahlreiche Entwürfe einer neuen VwV erblickten das Licht der Welt. Keiner davon war allerdings so tragfähig, dass sich die Ressorts auf einen hätten einigen können. Seitdem gibt es keine verbindliche landesweite Regelung, wie mit Verbindungsdaten umzugehen ist, wie lange diese gespeichert werden und wie eine stichprobenartige Kontrolle auf Missbrauch aussehen könnte. Gleiches gilt für den Umgang mit E-Mail und Internet in den Behörden des Freistaates.

## 5.12 Ausländerwesen

### 5.12.1 Keine Auskunft an ein Konsulat eines Nicht-EU/EWR-Staates

Ein in Sachsen ansässiges Generalkonsulat eines Nicht-EU/EWR-Staates ersuchte eine untere Ausländerbehörde um Übermittlung der aktuellen Wohnanschrift und derzeitigen Staatsangehörigkeit eines namentlich bezeichneten Betroffenen. Gründe hierfür gab es nicht an. Der Betroffene hat, wie mir die durch die Ausländerbehörde um Rat ersuchte Landesdirektion mitteilte, eine Aufenthaltserlaubnis aus humanitären Gründen nach § 25 Abs. 3 AufenthG, da das Bundesamt für die Anerkennung ausländischer Flüchtlinge bereits 1998 das Vorliegen eines Abschiebungshindernisses nach § 53 Abs. 6 AuslG (jetzt § 60 Abs. 7 AufenthG) festgestellt hatte. Die Ausländerbehörde sah die Auskunftserteilung aufgrund der konkreten Umstände, die aus seiner Sicht u. U. zu diplomatischen Auseinandersetzungen hätten führen können, als problematisch an. Die

Landesdirektion gab dagegen auch noch den § 17 SächsDSG zu Bedenken, der die Übermittlung von personenbezogenen Daten in Staaten, in denen kein angemessenes Datenschutzniveau gewährleistet ist (unsichere Drittstaaten), nur ausnahmsweise erlaubt, etwa wenn der Betroffene eingewilligt hat (§ 17 Abs. 3 Nr. 1 SächsDSG) oder die Übermittlung aus einem Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist (§ 17 Abs. 3 Nr. 6 SächsDSG), was hier im Hinblick auf eine Auskunft *aus dem Melderegister* in Betracht gezogen wurde.

Ich habe der Landesdirektion geraten, die Ausländerbehörde zu bitten, dem Auskunftsersuchen aus folgenden Gründen nicht stattzugeben:

Die §§ 86 ff. AufenthG enthalten keine speziellen Regelungen für die Übermittlung personenbezogener Daten eines ausländischen Staatsangehörigen durch die Ausländerbehörden an eine Nicht-EU/EWR-Stelle, hier das Generalkonsulat. Anzuwenden ist daher § 17 Abs. 1 SächsDSG, wonach die Übermittlung personenbezogener Daten in anderen als den in §§ 14, 15 und 16 SächsDSG genannten Fällen „unter den Voraussetzungen des § 16 Abs. 1 SächsDSG“ zulässig ist, wenn in dem Staat, an den die Daten übermittelt werden sollen, ein angemessenes Datenschutzniveau gewährleistet ist.

Eine Berücksichtigung aller Umstände nach § 17 Abs. 2 SächsDSG (die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und Bestimmungsland, die für den Empfänger geltenden Rechtsvorschriften sowie die für ihn geltenden Standesregeln und Sicherheitsmaßnahmen) des Einzelfalls ergab hier, dass es in dem Herkunftsstaat an einem dem EU/EWR-Niveau entsprechenden Datenschutzniveau fehlt. Damit kam eine Übermittlung nur auf der Grundlage der Einwilligung des Betroffenen (§ 17 Abs. 3 Nr. 1 SächsDSG) in Betracht.

Entgegentreten musste ich auch der Erwägung, dass gemäß § 17 Abs. 3 Nr. 6 SächsDSG eine Übermittlung der gewünschten Angaben, zumindest der zur aktuellen Wohnanschrift, aus dem kommunalen *Melderegister* möglich sein könnte. Denn bei der Anwendung der für eine Übermittlung an öffentliche Stellen außerhalb der EU insofern entsprechend geltenden §§ 32, 32a SächsMG (einfache Melderegisterauskunft, erweiterte Melderegisterauskunft) sind ergänzend wiederum die §§ 16, 17 SächsDSG zu beachten (vgl. Darré in Darré/Rimmele/Thalheim/Wunsch, SächsMG, 2. Aufl., § 29 Rdnr. 1 und vor §§ 32 und 32a, Rdnr. 3). Damit müsste auch eine um die Übermittlung ersuchte Meldebehörde die Wertungen des § 17 SächsDSG und insbesondere des § 32 Abs. 3 SächsMG beachten, wonach auch die einfache Melderegisterauskunft unterbleibt, „wenn für die Meldebehörde Grund für die Annahme besteht, dass dem Betroffenen oder einer anderen Person hieraus eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen erwachsen kann“. Ob dies der

Fall ist, könnte stets nur durch Anhörung des Betroffenen ermittelt werden. Gleiches gilt im Hinblick auf die Auskunft zur gegenwärtigen Staatsangehörigkeit nach § 32a Abs. 1 Satz 3 SächsMG.

Ich habe daraufhin das SMI gebeten, auf eine einheitliche Verfahrensweise bei den Ausländerbehörden hinzuwirken.

Das Ausländerrechtsreferat des SMI hat mir daraufhin in einem Schreiben mitgeteilt, dass Meldebehörden zuständig für Auskünfte nach dem Meldegesetz sind. Außerdem war es der Ansicht, dass das Ersuchen an Ausländerbehörden, eine Anschrift mitzuteilen, ohne dass konkret ein spezifisch ausländerrechtlicher Zweck angegeben wird, schon allein deshalb abzulehnen ist. Zusätzlich teilte es mir mit, dass Ersuchen mit Zweckangabe auf Grundlage der Vorschriften des Aufenthaltsgesetzes geprüft werden. Daraufhin entgegnete ich dem SMI, dass Grundlage für Übermittlungen an Ausländerbehörden Vorschriften wie beispielsweise §§ 90, 90a AufenthG sind, die Übermittlungen unter bestimmten Voraussetzungen vorsehen. Hierbei handelt es sich jedoch nicht um Übermittlungen auf Ersuchen anderer Behörden, sondern um gesetzlich vorgesehene Datenübermittlungen. Deshalb enthält das Aufenthaltsgesetz meines Erachtens keine Erlaubnis zur Übermittlung personenbezogener Daten durch die Ausländerbehörde, selbst wenn die ersuchende Behörde einen Zweck angibt. Außerdem bat ich im Hinblick auf eine einheitliche Verfahrensweise der Ausländer- und Meldebehörden um Auskunft, ob auch aus den Melderegistern derartige Auskünfte erteilt werden.

Anschließend teilte mir das Melderechtsreferat des SMI mit, dass Auskünfte aus den Melderegistern auf Ersuchen anderer Behörden, sonstiger öffentlicher Stellen oder von Privaten unter den Voraussetzungen der §§ 29, 32 und 32a SächsMG grundsätzlich zulässig sind. Es teilte zudem meine Auffassung, dass für das Generalkonsulat die §§ 32 und 32a SächsMG anzuwenden sind, da es sich hierbei nicht um eine Behörde oder ein Organ handelt. Ebenfalls teilte es meine Ansicht, dass § 32 Abs. 3 SächsMG zu beachten ist. Des Weiteren gab es an, dass, auch wenn die dargestellten Ablehnungsgründe unabhängig von der Eintragung einer Auskunftssperre zu beachten sind, diese für die Meldebehörde jedoch im Einzelfall, insbesondere vor dem Hintergrund der unterschiedlichen Zuständigkeiten für die Melderegisterauskünfte und Ausländerangelegenheiten erkennbar sein müssen. Die in diesem Fall dargelegten Gründe empfand es jedoch als nicht ausreichend. Grundsätzlich stimmte es allerdings zu, dass eine Ablehnung des Auskunftsersuchens zulässig war. Zum Schluss versicherte das SMI, dass die Meldebehörden auf die Rechtslage bei Auskunftsersuchen von Auslandsvertretungen zu ausländischen und ehemals ausländischen Staatangehörigen hingewiesen werden, in Zweifelsfällen die zuständige Ausländerbehörde bzw. den Betroffenen selbst zu beteiligen

und immer auch das Vorliegen der Voraussetzungen für die Eintragung einer Auskunftssperre nach § 34 SächsMG zu prüfen ist.

### 5.12.2 Datenschutzorganisatorische Abläufe in der Ausländerbehörde

Im Berichtszeitraum wandte sich ein Betroffener mit dem Hinweis an mich, dass in einer Ausländerbehörde Gespräche der Sachbearbeiter mit Antragstellern in Gegenwart anderer Antragsteller durchgeführt werden würden. Dabei bestünde die Gelegenheit, das andere Gespräch mitzuhören und die Amtshandlungen zu beobachten.

Die Ausländerbehörde bat ich um Stellungnahme. Die Stelle legte Gründe dar, welche die räumlich-organisatorische Gestaltung der Dienstbereiche in dem Gebäude betrafen. Nach meiner Überzeugung rechtfertigten die von der Behörde dargetanen Gründe allerdings keinen Eingriff in die Rechte der Betroffenen in der Form, dass personenbezogene Daten der Antragsteller in Kenntnis von Dritten gelangen. Ich teilte der Behörde daraufhin mit, dass an die räumliche Gestaltung von Ausländerämtern besondere Anforderungen zu stellen sind.

So sei die räumliche Aufteilung und Gestaltung der Arbeitsplätze so vorzunehmen, dass die Gespräche seitens der Betroffenen vertraulich geführt werden können. Das heißt wiederum nicht zwangsläufig, dass den Bediensteten z. B. Einzelzimmer zur Verfügung gestellt werden müssen. Die Räume der Ausländerbehörde sind vielmehr so zu gestalten, dass eine funktionale, bürgernahe Verwaltungstätigkeit mit den Rechten der Betroffenen in Einklang gebracht wird.

Soweit keine alternative vertrauliche Gesprächssituation bereitgestellt werden kann, ist es datenschutzrechtlich unzulässig, dass Gespräche der Sachbearbeiter mit Antragstellern in Gegenwart anderer Antragsteller durchgeführt werden und dabei die Gelegenheit besteht, dass andere Gesprächsinhalte und Amtshandlungen den Dritten gegenüber offenbart werden.

Den Antragstellern ist dementsprechend anzubieten, dass jedes Gespräch auch unter vier Augen in einem separaten Raum geführt werden kann. Möglich wäre auch eine Raumausstattung (z. B. Trennwände oder große Pflanzen), die gewährleistet, dass keine personenbezogenen Daten unbefugten Dritten akustisch oder in sonstiger Form zugänglich gemacht werden. Das heißt z. B. auch, dass Bildschirme uneinsehbar sein müssen.

Auch das von der Ausländerbehörde angeführte Argument der Gewährleistung der Sicherheit der Bediensteten im Ausländeramt darf nicht zu Lasten der Betroffenenrechte gehen. Es sind andere, nicht in die Rechte der Betroffenen eingreifende Maßnahmen (z. B. Notfallschalter) denkbar, die die Sicherheit der Bediensteten gewährleisten kön-

nen. Abgesehen davon ist es durchaus denkbar, dass möglicherweise konflikthaltige Gespräche mit Antragstellern durch zwei Bedienstete geführt werden.

Ich bat die Ausländerbehörde mir mitzuteilen, wie in dieser Angelegenheit weiter verfahren werden soll. Diese teilte zwischenzeitlich mit, dass sie gemeinsam mit dem behördlichen Datenschutzbeauftragten prüfen würde, ob im Einzelfall Veränderungen der räumlichen Gestaltung von Ausländerämtern erforderlich seien und durch welche konkreten Maßnahmen die datenschutzrechtlichen Anforderungen erfüllt werden können. Ich werde die Entwicklungen in der Ausländerbehörde weiter verfolgen.

Die Probleme bei der räumlich/organisatorischen Gestaltung der Ausländerbehörde können auch in anderen Verwaltungsbereichen auftreten. Die ggf. organisatorischen Neuregelungen der Abläufe der Behörde, welche die Rechte der Betroffenen einhalten und erhalten, sind ein dauerhaftes Thema für den Bereich des Datenschutzes.

Umso wichtiger sind die Hinweise Betroffener auf ggf. vorliegende Missstände.

## 5.13 Wahlrecht

In diesem Jahr nicht belegt.

## 5.14 Sonstiges

### 5.14.1 Informationen aus den Eigentümerdaten des amtlichen Vermessungswesens

Ein Petent informierte mich darüber, dass er im Rahmen der Errichtung einer bereits immissionsschutzrechtlich genehmigten Windenergieanlage durch den potentiellen Betreiber angefragt wurde, inwieweit sein Grundstück hierfür genutzt werden könne. Er fragte sich nun zu Recht, woher dieser die Eigentümerdaten hatte.

Der von mir kontaktierte Staatsbetrieb Geobasisinformation und Vermessung Sachsen teilte mir mit, dass in diesen Fällen stets Auskunft erteilt werde, da ein berechtigtes Interesse gemäß § 11 Abs. 2 Satz 4 SächsVermKatG vorliege. Zur Begründung wurde auf die Rechtsauffassung eines privaten Projektentwicklers für Windenergieanlagen verwiesen, die man sich zu Eigen gemacht hatte.

Diese Auffassung wird durch die Oberste Vermessungsbehörde, das SMI, nicht geteilt. Wie das Staatsministerium mir auf Anfrage mitteilte, geht es - wie auch ich - davon aus, dass kein berechtigtes Interesse bei Kauf- oder Mietinteressenten vorliegt. Der Staatsbetrieb Geobasisinformation und Vermessung Sachsen hat die Anfrage zum Anlass genommen, die mit der Datenbereitstellung befassten Mitarbeiter entsprechend über die

rechtlichen Voraussetzungen bei der Bereitstellung von Eigentümerdaten zu unterweisen.

### 5.14.2 Keine Software zur Überwachung sozialer Netzwerke durch die Sächsische Staatskanzlei

Im Berichtszeitraum wurde mir die durch die SK vorgenommene Ausschreibung einer Software zur Überwachung sozialer Netzwerke sowie der Blogosphäre bekannt.

In der Antwort auf eine Kleine Anfrage (LT-Drs. 5/9514) vertrat die Staatsregierung die Ansicht, dass wegen des Ausbaus moderner Informations- und Kommunikationstechniken heutzutage auch die Beobachtung der öffentlichen Debatte im Internet zu ihrer Aufgabenerfüllung erforderlich sei. Aufgrund der Vielzahl der Quellen sei ein wirtschaftliches Monitoring jedoch nur unter Zuhilfenahme IT-gestützter Verfahren möglich. Ziel sei die Erfassung aktueller Meinungsbilder in der Bevölkerung.

Ich wurde leider erst nach der Ausschreibung im Rahmen der Kleinen Anfrage über diesen Sachverhalt informiert. Der Einsatz einer solchen Software ist jedoch nur zulässig, soweit die Erfassung personenbezogener Daten ausgeschlossen werden kann. Gerade dies schien nicht Teil der Ausschreibungsunterlagen gewesen zu sein, obwohl die SK in ihrer Antwort von ausschließlich solchen Angeboten ausging.

Nach einer erneuten Prüfung der derzeitigen Möglichkeiten und voraussichtlichen Kosten distanzierte sich die Sächsische Staatsregierung von dem Vorhaben. Vergleichbare Projekte seien nicht geplant. Tatsächlich dienen den Bevölkerungsumfragen bereits repräsentative und wissenschaftlich fundierte Studien. Daneben können im Internet öffentlich verfügbare Daten mittels Suchprogrammen nach Stichworten durchsucht werden. Auch die Einschaltung von Instituten zur Meinungsforschung ist möglich.

Die Sächsische Staatsregierung hat ihr Vorhaben des Einsatzes einer Software zur Überwachung sozialer Netzwerke und der Blogosphäre aufgegeben. Datenschutzrechtlich zulässig wäre der Einsatz nur gewesen, soweit die Erfassung personenbezogener Daten hätte ausgeschlossen werden können.

### 5.14.3 Prüfung der datenschutzrechtlichen Zulässigkeit der Videoüberwachungsanlagen - vor deren Installation - Videoüberwachung als baulich-technische Sicherungsempfehlung des LKA

Im vorliegenden Berichtszeitraum stellte ich bei der in meiner Zuständigkeit liegenden Prüfung der Rechtmäßigkeit des Betriebs von Videoüberwachungseinrichtungen durch öffentliche Stellen fest, dass die Zentralstelle für polizeiliche Prävention des LKA in

ihren sachverständigen Äußerungen auch die Einrichtung von Videoüberwachung öffentlich zugänglicher Räume empfohlen hatte.

Die Gutachten selbst und besonders die jeweilige Formulierung der Schlussbemerkung in den Ausarbeitungen *„Die vorgeschlagenen mechanischen und elektrischen Mittel zur Gewährleistung einer hohen Sicherheit führen nur bei konsequenter Nutzung aller empfohlenen Sicherungsmaßnahmen zum Erfolg. Die empfohlenen Sicherungsmaßnahmen beinhalten ein schlüssiges Konzept. Eine Reduzierung von Widerstandswerten oder einzelnen Maßnahmen erhöht das Risiko und gefährdet das angestrebte Schutzziel ...“* beförderten nach meiner Überzeugung in der Verwaltungspraxis, dass die öffentlichen Stellen, den Empfehlungen des LKA folgend, ohne weitere datenschutzrechtliche Prüfung Videoanlagen installierten und betrieben. Mit der Gesetzeslage war das nicht in Einklang zu bringen. Die Videoüberwachung stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Der Ausstattung mit optisch elektronischen Einrichtungen hat deshalb, damit diese rechtmäßig durchgeführt werden kann, grundsätzlich eine Abwägung des öffentlichen Interesses mit den Interessen der Betroffenen gemäß § 33 SächsDSG vorauszugehen. Die öffentliche Stelle, die die Videoüberwachung betreibt, ist als Daten verarbeitende Stelle für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich.

Vor diesem Hintergrund bat ich das LKA wegen der vorprägenden Wirkung der LKA-Gutachten jeweils um die Aufnahme eines Hinweises, dass das Gutachten des LKA nicht die durch die verantwortliche Stelle vorzunehmende datenschutzrechtliche Prüfung vor dem Einsatz jeder einzelnen Videokamera ersetzt. Das LKA nahm meinen Hinweis auf und bat die zuständigen Mitarbeiter um Beachtung.

Eine Abstimmung war meinerseits auch mit dem SIB durchzuführen, der als Verwaltungsstelle eine wichtige Schnittstellenfunktion bei der Installation und dem Betrieb von Videoüberwachungsanlagen in und an staatlichen Behördenliegenschaften hat.

Die nachstehend aufgeführten drei Problemkreise sollten so nach meiner Vorstellung über den Staatsbetrieb an die nutzenden Dienststellen kommuniziert werden:

1. *Datenschutzrechtliche Zulässigkeitsprüfung vor der Installation der Videoüberwachungsmaßnahme durch die öffentliche Stelle unter Mitwirkung des SIB (u. a.):*

   Zwingende Voraussetzung für die rechtmäßige Inbetriebnahme einer Videoüberwachungsanlage ist die grundsätzliche Abwägung des öffentlichen Interesses und der Interessen der Betroffenen. Dazu gehört die Durchführung einer datenschutzrechtlichen Zulässigkeitsprüfung nach § 33 SächsDSG. Diese Zulässigkeitsprüfung fand in der behördlichen Praxis nur unzureichend statt. Um zu verhindern, dass die Video-

überwachungstechnik an Neu- und Altbauten ohne vorherige datenschutzrechtliche Prüfung installiert wird, strebte ich ein gleichmäßiges Verwaltungshandeln an. Neben der Frage der generellen Zulässigkeit der Durchführung der Videoüberwachung bei der öffentlichen Stelle ist regelmäßig zwischen den beteiligten Stellen abzustimmen, wie der Eingriff in das Recht auf informationelle Selbstbestimmung möglichst gering gehalten werden kann, ohne den Zweck der Videoüberwachung zu verfehlen.

*2. Auftragsdatenverarbeitung gemäß § 7 SächsDSG*

Die öffentliche Stelle, die die Videoüberwachung einsetzt, ist als Daten verarbeitende Stelle für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Der SIB als die für die Verwaltung der staatlichen Liegenschaften zuständige Stelle des Freistaates Sachsen schließt für die öffentlichen Stellen zentral Verträge mit Anbietern und Bedienern von Videotechnik. Bei der Erfüllung der Verträge werden durch die Auftragnehmer personenbezogene Daten des Nutzers verarbeitet. Für die Verarbeitung dieser Daten ist die hausverwaltende Stelle (der Nutzer) die verantwortliche Stelle im Sinne des Sächsischen Datenschutzgesetzes. Für die u. a. aus datenschutzrechtlicher Sicht komplizierte Rechtssituation zwischen dem SIB (als Auftraggeber), dem Anbieter der Videotechnik (als Auftragnehmer) und der für die Videotechnik zuständige Stelle (als Nutzer) sind bisher regelmäßig keine u. a. die Datenverarbeitung im Auftrag regelnde Nutzungsvereinbarungen geschlossen worden. Neben der Aufnahme datenschutzgerechter Regelungen in die Verträge zwischen SIB und den jeweiligen Auftragnehmern ist auch der Abschluss von Nutzungsvereinbarungen, in denen die Rechte und Pflichten zwischen dem Auftraggeber, dem Auftragnehmer und dem Nutzer verbindlich geregelt werden, erforderlich. Ich verwies in diesem Zusammenhang auf den „Mustervertrag zur Auftragsdatenverarbeitung gemäß § 7 SächsDSG“, der als Grundlage für Verträge dienen könnte und auf meiner Internetseite veröffentlicht ist.

*3. Vorabkontrolle und Verfahrensverzeichnis gemäß § 10 SächsDSG*

Gemäß § 10 SächsDSG ist jede Daten verarbeitende Stelle zur Führung eines Verfahrensverzeichnisses und - sofern die Voraussetzungen vorliegen - zur Durchführung einer Vorabkontrolle gemäß § 10 Abs. 4 SächsDSG verpflichtet. Die gebäudenutzende Stelle benötigt zur rechtmäßigen Durchführung der gesetzlich vorgeschriebenen Verfahren eine Reihe von technischen und organisatorischen Angaben (bis hin zu Systembeschreibungen), die allein vom Auftragnehmer erbracht werden können. Da in den bestehenden Verträgen eine solche Auskunftspflicht des Auftragnehmers bisher zumeist nicht vorgesehen ist, kommt es in der behördlichen Praxis zu Problemen bei der Durchführung der Vorabkontrolle und bei der Führung des Ver-

fahrensverzeichnisses. Ich regte daher eine vertragliche Regelung an, wonach der Auftragnehmer, an der Erstellung der Verfahrensverzeichnisse mitzuwirken und die erforderlichen Angaben dem Auftraggeber und dem Nutzer zuzuleiten hat.

Ein entsprechendes Gespräch mit dem SIB, bei dem ich meine Anliegen verdeutlichen konnte, fand noch im Berichtszeitraum statt.

# 6 Finanzen

## 6.1 Bewusstes Herausstellen der Prangerwirkung von „Ventilwächtern“ durch eine Stadtverwaltung

Im Berichtszeitraum wurde mir die Pressemitteilung einer Stadtverwaltung über den Einsatz von sogenannten Ventilwächtern, d. h. Vorrichtungen, die beim Anfahren automatisch die Luft aus den Reifen von Fahrzeugen ablassen, bekannt. Ventilwächter werden zur Vollstreckung zumeist wegen Geldforderungen am Kraftfahrzeug des Schuldners eingesetzt. In der Pressemitteilung fand sich der nachstehende, die Prangerwirkung dieser Vollstreckungshilfe betonende Absatz:

> *„Denn peinlich ist der Ventilwächter allemal. Die kleinen gelben Dinger sind weithin sichtbar - ebenso gut wie die Hinweisplaketten an Fahrer- und Beifahrertür und das leuchtend rote Pfandsiegel. Dann weiß nicht nur das Amt von den Schulden, sondern die ganze Nachbarschaft.“*

Die Mitteilung ist nicht nur instinktlos und deplatziert, sie ist auch rechtlich bedenklich. Eine Maßnahme, mit der der Schuldner quasi „an den Pranger“ gestellt werden soll, ist kein gesetzlich zulässiges Mittel der Verwaltungsvollstreckung. Der Schuldner hat die Übermittlung von Angaben über seine Person an die Öffentlichkeit nur zu dulden, wenn sie unvermeidliche Begleiterscheinung einer ansonsten rechtmäßigen Vollstreckungsmaßnahme sind. Die Passage in der Pressemitteilung erweckt hingegen den Eindruck, die Prangerwirkung sei Ziel des Einsatzes von Ventilwächtern, eventuell auch um die Schuldner mittels einer Offenbarungswirkung doch noch zur Zahlung zu zwingen. Ich habe die Stadtverwaltung daher gebeten, zukünftig von Hinweisen auf eine zu erzielende Prangerwirkung bei Vollstreckungsmaßnahmen Abstand zu nehmen.

## 6.2 Verwendungsnachweise bei ESF-Förderung durch die SAB

Verstößt die Forderung der SAB Original-Kontoauszüge als Verwendungsnachweis für ausgereichte ESF-Fördermittel vorzulegen gegen Regelungen des Datenschutzes? Reicht es nicht, entsprechende Kopien einzureichen, fragte mich ein betroffener Bürger.

Ich konnte Folgendes mitteilen:

Die SAB ist als Anstalt des öffentlichen Rechts in Sachsen beauftragt, Fördermittel auszureichen. Sie unterliegt dabei den staatlichen Vorgaben. Für die Vergabe von ESF-Fördermitteln ist für die SAB die Richtlinie Mikrodarlehen des SMWA nach § 1 Abs. 1 Nr. 8 und § 2 Abs. 2 SächsFöFoG verbindlich. Diese verweist auf weitere anzuwendende Rechtsvorschriften, unter anderem auf die Regelungen der Sächsischen Haus-

haltsordnung und die dazugehörige Verwaltungsvorschrift. Für die Vergabe von Mikrodarlehen ist unter anderem für Projektförderungen festgelegt, dass Nachweise über Einzelzahlungen (Einnahme- und Ausgabebelege) „im Original“ vorzulegen sind (Ziffer 6.5 Allgemeine Nebenbestimmungen für Zuwendungen zur Projektförderung (ANBest-P) zur Verwaltungsvorschrift zu § 44 SäHO). Die Antragsformulare zur Gewährung von Mikrodarlehen sowie die genannte Richtlinie Mikrodarlehen sind auf der Internetseite der SAB vorhanden. Ein Bewerber um ein Mikrodarlehen bei der SAB kann sich in dem Bewilligungsverfahren vor der Antragstellung über die mit der Bewilligung verbundenen Bedingungen vertraut machen. Mit der zu unterzeichnenden Antragstellung zur Gewährung des Mikrodarlehens erteilt der Antragsteller separat eine datenschutzrechtliche Einwilligungserklärung für die vorgesehene zweckgebundene Datenverarbeitung auf der Grundlage der zugrundeliegenden Regelungen.

Die Verarbeitung der personenbezogenen Daten durch die SAB war hinsichtlich der abverlangten Originalbelege nicht zu beanstanden. Betroffenen ist zu empfehlen, soweit auf Originalbelegen auch andere Kontobewegungen verzeichnet sind, diese zu schwärzen oder auf eine Antragstellung und die Förderung gänzlich zu verzichten. Einige Banken bieten ihren Kunden übrigens auch die Möglichkeit, für Einzelbuchungen gesonderte Bankbelege - ohne andere Zahlvorgänge - zu erhalten.

## 6.3 Erhebung von Angehörigendaten durch das Landesamt für Steuern und Finanzen (LSF)

Im Berichtszeitraum erreichte mich eine anonyme Anfrage zu einer Verfügung des LSF. Die Bediensteten aller sächsischen Finanzämter sollten Steuernummer(n), Kfz-Kennzeichen, Grunderwerbssteuerkonten und Bewertungsaktenzeichen derjenigen Steuerfälle angeben, zu denen sie in einem Angehörigenverhältnis nach § 15 AO stehen. Die Abfrage sollte dem Ausschluss der Befangenheit der am Verwaltungsverfahren beteiligten Amtsträger dienen, denn nach § 82 AO dürfen bestimmte Personen in einem Verwaltungsverfahren für eine Finanzbehörde nicht tätig werden, wenn sie beispielsweise Angehörige eines Beteiligten sind.

Gegenüber der LSF wies ich darauf hin, dass § 82 AO lediglich für die laufenden Verfahren ein Verbot vorsieht. Eine Abgabe von personenbezogenen Daten für die Zukunft auf Vorrat und in Bereichen, in denen der betroffene Bedienstete gar nicht tätig ist, halte ich für problematisch.

Das Landesamt teilte mir mit, dass es meine Rechtsauffassung zu § 82 AO teile und es nicht beabsichtigt gewesen sei, die Angehörigenverhältnisse aller Bediensteten unabhängig vom Zuständigkeitsbereich abzufragen. Anfragen aus den Finanzämtern hätten

jedoch bestätigt, dass die Verfügung insoweit teilweise falsch verstanden worden sei. Das LSF habe sich deshalb dazu entschieden, die Verfügung zu überarbeiten und klarzustellen, dass nur die einschlägigen Steuernummern verlangt würden, auf die der jeweilige Bedienstete bearbeitenden Zugriff hat.

Mit der überarbeiteten Verfügung wird ein rechtsstaatliches Verwaltungsverfahren sichergestellt. Der Fall zeigt, dass eine datenschutzrechtliche Prüfung im konkreten Fall zur Klarstellung beitragen kann. Für die gute Zusammenarbeit danke ich dem LSF.

## 6.4 Erklärung über die Zustimmung zur unverschlüsselten elektronischen Übermittlung von steuerlichen Daten

Ein Steuerberater wandte sich an mich, weil er Bedenken im Hinblick auf die Forderung eines Finanzamts zur Abgabe einer Erklärung über die Zustimmung zur unverschlüsselten elektronischen Übermittlung von steuerlichen Daten per E-Mail hatte. Ich teilte daraufhin dem SMF mit, dass ich eine solche Einwilligungserklärung grundsätzlich für bedenklich halte, da der Betroffene nicht überblicken kann, welche Daten im jeweiligen Fall übermittelt werden und welche Konsequenzen dies nach sich zieht. Deshalb sollte eine solche Einwilligung meines Erachtens stets auf einen konkreten Fall bezogen werden.

Der genannte Vordruck für die Zustimmung zur unverschlüsselten Übermittlung war ein durch das LSF zur Verfügung gestelltes Muster, das die Finanzämter verwenden sollten. Die Zustimmungserklärung war jedoch nicht zwingend. Ich habe den Fall deshalb zum Anlass genommen, das SMF auf die Freiwilligkeit der Zustimmung hinzuweisen und eine verschlüsselte elektronische Kommunikation zu fordern. Der Vordruck wies zwar auf die Risiken der Übertragung per E-Mail hin, erwähnte aber bisher nicht die Möglichkeit, die Zustimmung auf bestimmte Steuerarten, Veranlagungszeiträume oder konkrete Sachverhalte zu beschränken. Ich empfahl, den Vordruck entsprechend zu ergänzen.

Das SMF erklärte daraufhin, dass eine verschlüsselte elektronische Kommunikation zwischen Finanzämtern und Steuerpflichtigen zurzeit nicht möglich sei. Es teilte mir weiterhin mit, dass man den Rechtsgedanken des § 30 Abs. 4 Nr. 3 AO, der die erforderliche Zustimmung zur Offenbarung der Daten regelt, auf den Versand von Steuerdaten per E-Mail entsprechend anwende. Die Zustimmung könne auf bestimmte Steuerarten, Veranlagungszeiträume oder konkrete Sachverhalte beschränkt werden.

Das SMF und das LSF überarbeiteten daraufhin das Formblatt. Der Steuerpflichtige hat nun die Möglichkeit, die Zustimmung zur Übermittlung aller Daten zu geben, oder diese

auf speziell angegebene Möglichkeiten zu beschränken. Eine Verfügung des LSF weist zudem die Finanzämter noch einmal ausdrücklich auf die Freiwilligkeit der Zustimmungserklärung hin.

Für die Zukunft habe ich gegenüber dem SMF angeregt, eine Möglichkeit zur verschlüsselten Datenübermittlung einzuführen, um die Gefahr einer ungewollten Offenbarung steuerlicher Daten für den Steuerpflichtigen zu reduzieren.

# 7 Kultus

## 7.1 Einsichtnahmerecht in die Schülerakte

Im Berichtszeitraum baten mich die Eltern eines Schülers, sie bei der Einsichtnahme in die Schülerakte ihres Kindes zu unterstützen. Vorgänge dieser Art gehen relativ häufig in meiner Behörde ein. Vorwiegend verfügen weder die Betroffenen über die Erfahrung noch sind die Schulen geübt, Einsichtnahmen ohne externen Rat ordnungsgemäß zu handhaben.

Gemäß der Verwaltungsvorschrift des SMK zur Verwendung von Vordrucken für die schulische Verwaltung (Schulformular-VwV) haben die Schulen über jeden einzelnen Schüler eine Kartei mit persönlichen Daten und Noteneintragungen von Halbjahresinformationen, Halbjahreszeugnissen und Zeugnissen vom Schuleintritt bis zum Ende der Schulzeit zu führen. Gemäß der Schulformular-VwV kann die Schülerkartei auch allgemeine Eintragungen vom Schulleiter und vom Klassenlehrer enthalten. Für das Einsichtnahmerecht selbst enthalten die schulrechtlichen Vorschriften keine Bestimmungen; so ist § 18 SächsDSG anzuwenden. Diese Vorschrift regelt u. a., dass dem Betroffenen - im vorliegenden Fall den gesetzlichen Vertretern des minderjährigen Schülers - von der Daten verarbeitenden Stelle - der Schule - auf Antrag kostenfrei und ohne unzumutbare Verzögerung Auskunft zu erteilen ist über die zu seiner Person gespeicherten Daten, den Zweck und die Rechtsgrundlage der Verarbeitung, die Herkunft der Daten und die Empfänger von Übermittlungen sowie die übermittelten Daten, soweit dies gespeichert oder sonst bekannt ist.

Sind die personenbezogenen Daten in Akten gespeichert, die zur Person des Betroffenen geführt werden, ist zudem auf Verlangen Einsicht in die Akten zu gewähren, § 18 Abs. 3 SächsDSG. Dabei ist zu beachten, dass in dem Antrag die Art der personenbezogenen Daten näher bezeichnet werden müssen, über die Auskunft erteilt werden soll. Die Schule bestimmt als die Daten verarbeitende Stelle das Verfahren, insbesondere die Form der Auskunftserteilung und Einsichtnahme nach pflichtgemäßem Ermessen; dabei dürfen berechtigte Interessen Dritter nicht beeinträchtigt werden, § 18 Abs. 4 SächsDSG.

Voraussetzung für die Einsichtnahme in die bei der Schule über den Schüler vorhandenen Unterlagen ist damit ein von den Eltern gestellter Antrag. Davon ausgehend, dass sich die Bitte auf Einsichtnahme in die „Schulakte des Kindes“ auf die Schülerkartei gemäß Nr. II.2 Schulformular-VwV bezog, bat ich die Eltern den entsprechenden Antrag auf Einsichtnahme in die Schülerkartei des Kindes schriftlich an die Schule zu stellen. Auskunft und Akteneinsichtnahme nach dem Sächsischen Datenschutzgesetz

erfordern keine Begründung der Antragsteller. Die Schule sollte nach dem Antrag Einblick in die entsprechenden Unterlagen gewährt haben.

## 7.2 Zulässigkeit der Forderung der Schule den Grund der Erkrankung eines Kindes mitteilen zu müssen

Ratsuchend wendete sich die Mutter eines Schülers an mich und teilte mir mit, dass sie bei dem letzten Elternabend der Schule ihres Kindes darüber informiert worden sei, dass bei Krankheit zukünftig zwingend eine Bescheinigung vorzulegen wäre, aus der der Grund der Erkrankung ersichtlich sein müsste.

Datenschutzrechtlich ist die Forderung der Schule nach Mitteilung der Art der Erkrankung (im Sinne einer Diagnose) rechtswidrig. Nach § 4 SächsDSG ist die Schule als öffentliche Stelle befugt, personenbezogene Daten zu verarbeiten, wenn eine Rechtsvorschrift dies erlaubt. Gemäß § 2 SBO ist der Schule unter Angabe des Grundes und der voraussichtlichen Dauer der Verhinderung unverzüglich mitzuteilen, wenn ein Schüler durch Krankheit oder aus anderen nicht vorhersehbaren zwingenden Gründen verhindert ist, die Schule zu besuchen. Bei einer Krankheitsdauer von mehr als fünf Tagen sowie bei Teilzeitunterricht von mehr als zwei Unterrichtstagen, kann der Klassenlehrer oder der Tutor vom Entschuldigungspflichtigen die Vorlage eines ärztlichen Zeugnisses verlangen.

„Angabe des Grundes“ im Sinne der SBO bedeutet lediglich, dass allgemeine Angaben, z. B. „krankheitsbedingt“ oder aus „gesundheitlichen Gründen“ zu machen sind. Darüber hinausgehende Daten zum gesundheitlichen Zustand eines Schülers ist die Schule nicht zu erheben befugt.

Gesundheitsdaten dürfen nach dem Sächsischen Datenschutzgesetz als besonders schützenswerte Daten 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. Für die Erfüllung der Aufgaben der Schule ist lediglich der Grund des Fernbleibens vom Unterricht, hier: z. B. „aus gesundheitlichen Gründen“ zur Gewährleistung der Schulpflicht gemäß § 26 SchulG erforderlich. Im Ausnahmefall, bei auffällig häufigen oder langen Erkrankungen, ist der Schulleiter gemäß § 2 Abs. 3 SBO berechtigt, vom Entschuldigungspflichtigen die Vorlage eines amts- oder vertrauensärztlichen Zeugnisses zu verlangen. Die Anforderung ist durch den Schulleiter besonders zu be-

gründen. Auffällig lang sind Erkrankungen von mehr als zehn Tagen, bei Teilzeitunterricht von mehr als vier Unterrichtstagen. Selbst in diesen Fällen darf - mangels anderslautender Rechtsvorschrift - das amts- oder vertrauensärztliche Zeugnis lediglich allgemeine Angaben, z. B. „aus gesundheitlichen Gründen“ enthalten. Ich teilte dies der Mutter des Schülers mit.

## 7.3 Zulässigkeit der Erhebung des Grundes für eine Sportbefreiung durch die Schule

Die Mutter eines Schülers bat mich um Mitteilung, ob das Vorgehen einer Schule bzw. eines Sportlehrers im Zusammenhang mit Sportbefreiungen rechtlich zulässig sei. So seien in einer Klasse die Eltern aufgefordert worden, vom Kinderarzt auf Sportbefreiungsattesten vermerken zu lassen, wegen welches ärztlichen Grundes die Kinder vom Sport befreit werden sollten. Zudem sollten sich die Eltern im Falle von Sportbefreiungen mit dem Sportlehrer in Verbindung setzen. Erfolge von Seiten der Eltern keine Ansprache des Sportlehrers, würde dieser die Schüler zur Art der Erkrankung befragen und solle dem jeweiligen Schüler dann mitteilen, inwieweit dieser am Sportunterricht teilnehmen solle.

Angaben zur Art einer Erkrankung sind Angaben zur Gesundheit einer Person, die nach dem Sächsischen Datenschutzgesetz als besonders schutzwürdig eingestuft sind und nur unter beschränkten Voraussetzungen verarbeitet werden dürfen, § 4 Abs. 2 SächsDSG. Eine Rechtsvorschrift, die die Erhebung der Gesundheitsdaten des Schülers (im Sinne einer Diagnose) bei Sportbefreiungen ausdrücklich vorsieht oder zwingend voraussetzt, liegt nicht vor.

Die Voraussetzungen des § 4 Abs. 2 SächsDSG sind nicht erfüllt.

§ 3 Abs. 2 SBO bzw. die Verwaltungsvorschrift des SMK und des SMS zur Befreiung vom Sportunterricht vom 1. März 1996 sind keine Vorschriften, die eine Erhebung von Gesundheitsdaten durch die Schule zu begründen geeignet sind. Auch wenn die Schule Entscheidungen über Befreiungen vom Sportunterricht trifft, ist die Stelle weder befugt, bei Vorliegen eines ärztlichen Attests, Gesundheitsdaten und ärztliche Diagnosen zu ermitteln noch ärztliche Einschätzungen zu hinterfragen oder zu interpretieren. Auch eine Befragung von Schülern zur Art der Erkrankung durch den Sportlehrer ist ohne Einwilligung der Eltern minderjähriger Schüler datenschutzrechtlich nicht zulässig. Auf Anfrage hin wurde mir von der Schule bestätigt, dass derartige Angaben nicht gefordert würden und man keine Gesundheitsdaten ohne Einwilligung der Eltern erheben werde. Die Schule wies ich auf die geltende Rechtslage hin und bat darum, die Lehrkräfte an der Schule diesbezüglich noch einmal gesondert zu informieren. Vgl. auch 7.2.

# 8 Justiz

## 8.1 Übersendung von Anklageschriften gegen Ausländer an Ausländerbehörden

Im Berichtszeitraum wurde mir mitgeteilt, dass Staatsanwaltschaften in anderen Ländern Kopien von Anklageschriften oder Strafbefehlen gegen Ausländer nach Nr. 42 MiStra an die örtlich zuständige Ausländerbehörde übersendeten.

Dies halte ich von § 87 Abs. 4 Satz 1 AufenthG nicht gedeckt. Nach dieser Vorschrift dürfen die Staatsanwaltschaften die zuständige Ausländerbehörde lediglich über die *Einleitung* sowie die *Erledigung* des Straf- oder Bußgeldverfahrens unterrichten. Die Vorschrift erlaubt den Staatsanwaltschaften somit nicht die routinemäßige und zeitlich zwischen der Einleitung und der Erledigung liegende Übersendung einer Kopie der Anklageschrift oder des Strafbefehls, die i. d. R. viele zusätzliche Informationen zum Beschuldigten und zu Dritten enthalten. Benötigt die Ausländerbehörde im Einzelfall weitere Informationen, um über eine Ausweisung des betroffenen Ausländers zu entscheiden, kann sie jedoch weitere erforderliche Daten nach den §§ 86 und 87 AufenthG bei der Staatsanwaltschaft erheben.

Ich habe die Generalstaatsanwaltschaft gebeten, dafür Sorge zu tragen, dass in Sachsen nicht routinemäßig Kopien der Anklageschrift oder des Strafbefehls übersandt werden. Die Behörde teilte mir mit, dass das in Sachsen (neben Bayern, Baden-Württemberg, dem Saarland und Thüringen) im Rahmen der Geschäftsstellenautomatisierung eingesetzte Textverarbeitungssystem TV-STA die Mitteilungen nach Nr. 42 MiStra automatisiert erzeuge, sobald über eine Checkbox eine konkrete Mitteilung nach der MiStra aktiviert werde. Das eingesetzte Geschäftsstellenautomatisierungssystem „web.sta 3.1“ lasse jedoch systemseitig die (fehlerhafte) Beifügung der Anklageschrift oder des Strafbefehls als Anlage technisch durchaus zu, da „web.sta 3.1“ keine Plausibilitätsprüfung vornehme. Die Generalstaatsanwaltschaft teile meine Bedenken und verspreche, die Leiter der sächsischen Staatsanwaltschaften entsprechend zu informieren.

Die Übermittlung einer Kopie einer Anklage- oder Strafbefehlsschrift an die Ausländerbehörde ist zum Zeitpunkt und im Rahmen einer Mitteilung nach Nr. 42 MiStra unzulässig.

## 8.2 Datenerhebung in der JVA beim „Antrag auf Eintragung in die Besucherkartei“

Mehrere Gefangene einer JVA und deren Angehörige wandten sich an mich und beschwerten sich darüber, dass auf einem Antragsformular zur Eintragung in die Besu-

cherkartei die Angabe personenbezogener Daten, wie die Telefonnummer, das Geburtsdatum, die Adresse und die „genaue Bezeichnung der Beziehung“ zum Gefangenen verlangt wurden.

Die Vollzugsbehörde darf nach § 179 Abs. 1 StVollzG personenbezogene Daten erheben, soweit deren Kenntnis für den ihr nach dem Strafvollzugsgesetz aufgegebenen Vollzug der Freiheitsstrafe erforderlich ist und diese Daten zur Aufgabenwahrnehmung der JVA notwendig sind. Zu diesen Aufgaben gehören die Gestaltung des Vollzugs und insbesondere die Kontakte des Gefangenen zur Außenwelt. Zur unzweifelhaften Identifizierung eines Besuchers dürfen meines Erachtens deren Name, Anschrift und Geburtsdatum erhoben werden. Besucher, die keine Angehörigen des Gefangenen sind, kann der Anstaltsleiter ablehnen, wenn zu befürchten ist, dass sie einen schädlichen Einfluss auf den Gefangenen haben oder seine Eingliederung behindern, während Besuche von Verteidigern sowie Rechtsanwälten oder Notaren zu gestatten sind. Aus diesen Gesichtspunkten ist die Frage nach der „Art der Beziehung“ berechtigt. Bei allen übrigen Besuchern ist allerdings die Erhebung der „genauen Beziehung“, wie zum Beispiel die Angaben „Ex-Freundin“ oder „Schulkamerad“ unzulässig. Auch die Erhebung der Telefonnummer ist zur unzweifelhaften Identifizierung eines Besuchers nicht erforderlich.

Meine Ansicht teilte ich der JVA mit und empfahl die Formulierung „Bezeichnung der Beziehung (z. B. Angehöriger, Bekannter, Freund)“ zu verwenden sowie die Angabe der Telefonnummer als freiwillig zu kennzeichnen. Diese Vorschläge wurden von der JVA angenommen und das Formblatt entsprechend geändert. Das SMJus bat daraufhin alle sächsischen Justizvollzugsanstalten um Anpassung ihrer Formulare. Hierfür möchte ich mich beim SMJus bedanken.

## 8.3 Funkzellenabfragen zum Februar 2011 in Dresden („Handygate“)

Der wohl gravierendste Datenschutzverstoß im Berichtszeitraum bestand in den zum Teil unverhältnismäßigen Funkzellenabfragen durch das LKA, die PD Dresden und die Staatsanwaltschaft Dresden zum 13., 18. und 19. Februar 2011 in Dresden anlässlich des 66. Jahrestages der Bombardierung der Stadt im Zweiten Weltkrieg. Die meisten davon standen in einem Zusammenhang mit Versammlungen und Gegendemonstrationen am 19. Februar 2011. Insgesamt wurden durch das LKA und die PD Dresden, wobei zwischen den Maßnahmen beider Behörden zu trennen ist, über eine Million Verkehrsdatensätze bei Telekommunikationsdienstleistern erhoben. Daraus wurden allein zum 19. Februar 2011 für den Innenstadtbereich von Dresden mehr als 257.000 Rufnummern und in der Folge über 40.000 Betroffene namentlich ermittelt. Damit wurde der rechtsstaatliche Grundsatz der Verhältnismäßigkeit massiv verletzt; ferner blieben

strafprozessuale Sonderrechte von Abgeordneten sowie Rechtsanwälten und Journalisten unberücksichtigt. Das Ausmaß des staatlichen Eingriffs in die Grundrechte so vieler mitbetroffener Dritter erregte bundesweit Aufsehen. Zahlreiche parlamentarische Anfragen und Debatten im Sächsischen Landtag und im Deutschen Bundestag befassten sich mit den Vorgängen. Drei (leider bisher erfolglose) parlamentarische Initiativen zur Neufassung der derzeitigen Rechtsgrundlage, des § 100g Abs. 2 StPO, eine davon seitens der Sächsischen Staatsregierung[1], wurden ergriffen. Die sächsische Polizei erstellte u. a. eine Handreichung für ihre Beamten, um die Voraussetzungen und Grenzen von Funkzellenabfragen künftig sicherer beurteilen zu können. Das SMJus bat den Generalstaatsanwalt, mich künftig auf Funkzellenabfragen, „in denen eine Vielzahl unbeteiligter Personen … betroffen sein könnte“, hinzuweisen. Darüber hinaus erfolgte im Berichtszeitraum eine zwischen SMJus, Generalstaatsanwalt und mir vereinbarte quartalsweise Benachrichtigung über durchgeführte Funkzellenabfragen. Ich habe zudem den Eindruck gewonnen, dass meine Beanstandungen dazu beigetragen haben, dass Polizei und Staatsanwaltschaften die Verhältnismäßigkeit von Funkzellenabfragen, insbesondere wenn eine große Anzahl von mitbetroffenen Dritten zu erwarten ist, zukünftig genauer prüfen werden.

Neben diesen - zum Teil durchaus positiven - Folgen war die wohl gravierendste Folge der Funkzellenabfragen rund um das Geschehen am 19. Februar 2011 zugleich die politischste: Ein Verlust an Vertrauen in die Sicherheitsbehörden. Mir drückten viele, und zwar wohlmeinende und keineswegs extremen politischen Lagern zugehörige, Bürger ihr Unverständnis über deren Vorgehensweise aus. Auch zeigte sich mir der vom BVerfG in ständiger Rechtsprechung so wohlbeschriebene „Einschüchterungseffekt“ staatlicher Datenerhebungsmaßnahmen auf die Ausübung der Versammlungsfreiheit.

Doch der Reihe nach: Nachdem mich erstmals der BfDI am 16. Juni 2011 auf die Verwertung von Funkzellendaten in einem Verfahren wegen eines Verstoßes gegen § 21 VersammlG[2] hingewiesen hatte, bat ich die PD Dresden, das LKA und die Staatsanwaltschaft Dresden nach § 27 SächsDSG unverzüglich um Auskunft über die näheren Umstände. Meine ersten Kontrollbesuche und Gespräche mit den verantwortlichen Beamten erhärteten meinen Verdacht, dass die Akteure hier zum Teil weit über das Ziel hinausgeschossen waren. In den folgenden Monaten kontrollierte ich mehrfach und eingehend die zu den zugrundeliegenden Ermittlungsverfahren geführten Akten der Polizei und der Staatsanwaltschaft Dresden und führte weitere Gespräche. Mein Schrift-

[1] BR-Drs 532/11.
[2] „Wer in der Absicht, nicht verbotene Versammlungen oder Aufzüge zu verhindern oder zu sprengen oder sonst ihre Durchführung zu vereiteln, Gewalttätigkeiten vornimmt oder androht oder grobe Störungen verursacht, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.“

wechsel erstreckte sich bald auch auf die Generalstaatsanwaltschaft, das SMJus und das SMI.

Mit Schreiben vom 8. September 2011 habe ich nach alledem das LKA und die PD Dresden als auch die für die dort bearbeiteten Ermittlungsverfahren verantwortliche Staatsanwaltschaft Dresden nach § 29 SächsDSG förmlich beanstandet. Ich habe dies im Wesentlichen damit begründet, dass nach dem Willen des Gesetzgebers und unter Berücksichtigung der Umstände des Einzelfalls hätte klar sein müssen, dass von der Anregung bzw. Beantragung von einigen der Funkzellenabfragen zum 18. und 19. Februar 2011 wegen ihrer unangemessen langen Dauer und der zu erwartenden außerordentlich hohen Anzahl von mitbetroffenen Dritten aus Gründen der Verhältnismäßigkeit hätte abgesehen werden müssen. Dabei konnte ich insbesondere auf den Gesetzgeber verweisen. Der Deutsche Bundestag hatte 2007 mit § 100g Abs. 2 Satz 2 StPO die Rechtsgrundlage, auf der nichtindividualisierte Funkzellenabfragen durchgeführt werden, geschaffen. Dabei hat er in der Gesetzesbegründung gerade auf die Beachtung des Prinzips der Verhältnismäßigkeit großen Wert gelegt:

> *„Im Rahmen der Verhältnismäßigkeitsprüfung ist aber insbesondere zu berücksichtigen, inwieweit dritte Personen von der Maßnahme mit betroffen werden. Die Maßnahme kann daher im Einzelfall aus Verhältnismäßigkeitsgründen zeitlich und örtlich weiter zu begrenzen sein oder muss unterbleiben, wenn eine solche Begrenzung nicht möglich ist und das Ausmaß der Betroffenheit Dritter als unangemessen erscheint.“ (BT-Drs. 16/5846, S. 55).*

Dem Sächsischen Landtag habe ich nach § 30 Abs. 2 SächsDSG einen ausführlichen 53-seitigen Bericht vorgelegt (LT-Drs. 5/6787)[3]. Darin stellte ich die technischen und rechtlichen Grundlagen von Funkzellenabfragen und anderen elektronischen Überwachungsmaßnahmen, die Mitte Februar 2011 in Dresden zum Einsatz kamen, die Ermittlungsmaßnahmen der beteiligten Polizeibehörden sowie die erforderlichen Maßnahmen zur Gewährleistung der Rechte der Betroffenen und die m. E. erforderlichen sachlichen Konsequenzen ausführlich dar. U. a. forderte ich die Benachrichtigung der namentlich bekannten Betroffenen, eine unverzügliche Reduzierung des gespeicherten Datenbestands in den Arbeitsdateien auf das zur Strafverfolgung erforderliche Ausmaß, die Löschung der zur Strafverfolgung nicht erforderlichen Daten, die Sperrung der Rohdaten, die Erstellung eines allgemeinen Reduzierungskonzepts für künftige Fälle, die Schaffung untergesetzlicher Handlungsanweisungen sowie die Präzisierung der gesetzlichen Grundlagen von nichtindividualisierten Funkzellenabfragen.

[3] http://edas.landtag.sachsen.de/ oder http://www.saechsdsb.de/images/stories/sdb_inhalt/behoerde/oea/bericht-funkzellenabfragen.pdf.

Nach den Beanstandungen drang ich gegenüber den beteiligten Behörden auf möglichst grundrechtsfreundliche Verfahrensweisen. Leider zog sich die Erteilung von Auskünften an Betroffene nach § 491 StPO in der Folge ebenso hin wie die Erfüllung der Amtspflicht zur Benachrichtigung von „an der Telekommunikation Beteiligten“ nach § 101 StPO. Die Staatsanwaltschaft Dresden erteilt Auskünfte nur auf schriftliche Ersuchen; initiativ - wie § 101 Abs. 4 StPO vorsieht - benachrichtigt sie auch nicht in den Fällen, in denen neben Verbindungs- auch die dazu gehörigen Bestandsdaten erhoben worden sind, der Betroffene also namentlich bekannt ist. Damit bin ich sehr unzufrieden; hier wird m. E. eine durch den Gesetzgeber vorgesehene grundrechtssichernde Maßnahme unterlaufen. Noch nach über einem Jahr, im Februar 2012, hatte das LKA kein Bestandsdatum gelöscht. Ich habe daraufhin erneut darauf gedrungen, dass endlich ein tragfähiges Konzept zur Reduzierung des Datenbestands auf das zur Strafverfolgung erforderliche Maß entwickelt und umgesetzt wird.

Den Vorgang werde ich weiter im Auge behalten.

## 8.4 Datenerhebung bei Gefangenen für die GEZ

In 15/8.3 wies ich auf die Problematik der Datenerhebung bei Gefangenen in JVAs für die GEZ hin. Die Gefangenen müssen zur Genehmigung der Nutzung eines Fernsehgeräts ein vorgedrucktes Formular ausfüllen, in dem Angaben gemacht werden müssen, die ich für datenschutzrechtlich bedenklich ansehe. Dazu gehören die Angabe des Umstands der Inhaftierung sowie personenbezogene Daten über Dritte. Die von mir angeschriebene JVA versicherte daraufhin, dass diese Daten in Zukunft nicht mehr übermittelt werden sollten und den Gefangenen das allgemein übliche Anmeldungsformular der GEZ zur Verfügung gestellt werden solle, falls sie den Umstand der Inhaftierung nicht preisgeben wollen.

Das SMJus nahm sich ebenfalls des Falles an und schloss sich meiner Auffassung an. Es teilte mir mit, dass es sich, da es sich nicht um Justiz-Formulare, sondern um GEZ-Formulare handele, auch selbst an die GEZ gewandt und um Anpassung der entsprechenden Formulare gebeten habe. Der JVA wurde das Schreiben ebenfalls zur Kenntnisnahme übersandt und gleichzeitig erneut darum gebeten, bis zur Klärung des Sachverhalts die Daten nicht mehr an die GEZ zu übermitteln bzw. die Gefangenen auf die Freiwilligkeit der Angaben hinzuweisen.

Mit der zum 1. Januar 2013 wirksam gewordenen Umstellung der Rundfunkfinanzierung vom bisherigen Gebühren- auf das neue Beitragsmodell hat sich die Rechtslage insofern grundlegend geändert; im Rundfunkbeitragsstaatsvertrag ist nunmehr ausdrücklich festgestellt worden, dass „Hafträume in Justizvollzugsanstalten“ nicht als

„Wohnung“ gelten, so dass Gefangene keine Rundfunkbeiträge schulden (vgl. § 3 Abs. 2 Nr. 4 RBStV).

## 8.5 Entwurf des Gesetzes über den Vollzug der Freiheitsstrafe und des Strafarrests im Freistaat Sachsen sowie zur Änderung weiterer Gesetze

Im Berichtszeitraum wurde mir der Entwurf eines Sächsischen Strafvollzugsgesetzes (SächsStVollzG-E) zur Stellungnahme übersandt. Seit dem 1. September 2006 liegt die Gesetzgebungskompetenz für den Justizvollzug nach Art. 70 Abs. 1 GG bei den Ländern. Datenschutzrechtliche Aspekte des Strafvollzugs hatte ich bereits in den Jahren 2006/2007 im Rahmen der Einführung des Sächsischen Jugendstrafvollzugsgesetzes intensiv und konstruktiv erörtert (vgl. 13/8.1). Der Entwurf des Strafvollzugsgesetzes wurde insbesondere vom Gedanken der Resozialisierung und Eingliederung Strafgefangener getragen. In datenschutzrechtlicher Hinsicht übernahm er wesentliche Inhalte des Strafvollzugsgesetzes des Bundes und berücksichtigte die Erfahrungen mit dem Jugendstrafvollzugsgesetz.

Zwei meiner Anregungen im Beratungsverfahren zum Sächsischen Strafvollzugsgesetz möchte ich herausgreifen:

Die zunächst vorgesehene Pflicht von Anstaltsärzten, die im Rahmen der allgemeinen Gesundheitsfürsorge eines Strafgefangenen festgestellten Befunde zu offenbaren, sofern dies in irgendeiner Weise zur Aufgabenerfüllung der Anstalt oder Aufsichtsbehörde unerlässlich sein könnte, wurde auf mein Anraten in eine entsprechende Befugnis abgeändert. Diese muss im Hinblick auf das Arzt-Patienten-Verhältnis und die Aufgabenerfüllung der Anstalt oder der Gefahrenabwehr pflichtgemäß ausgeübt werden.

Meine Bedenken hinsichtlich der Benachrichtigungspflicht der nahen Angehörigen im Falle einer schweren Erkrankung des Gefangenen durch die Anstalt ohne dessen Einwilligung fanden bis zur Einbringung in den Landtag leider keine Berücksichtigung. Datenschutzrechtlich ist dies bedenklich, da es sich hierbei um besonders schutzwürdige Daten i. S. v. § 4 Abs. 2 SächsDSG handelt. Der Wunsch des Gefangenen auf Verzicht einer solchen Benachrichtigung sollte respektiert werden. Daher sollte eine Benachrichtigung nur erfolgen, wenn der Gefangene eingewilligt hat. Daneben sind der Anstalt eventuell die Adressen der zu informierenden Personen nicht bekannt. Dieses Problem könnte umgangen werden, wenn der Gefangene bei seiner Aufnahme bestimmt, wer im Falle einer schweren Erkrankung benachrichtigt werden soll. Dies könnte ebenfalls die Grundlage einer wirksamen Einwilligung des Strafgefangenen zur entsprechenden Benachrichtigung darstellen.

Erfreulich ist allerdings eine Klarstellung im neuen Strafvollzugsgesetz, die bisherige Meinungsverschiedenheiten zwischen mir und den Strafvollzugsbehörden über die Überwachung von Gefangenentelefonaten obsolet werden lässt. Während die Behörden nach alter Rechtslage eine Befugnis zur generellen Überwachung dieser Gespräche angenommen hatten, bestimmt das Gesetz nun unmissverständlich, dass eine Überwachung von Telefongesprächen nur dann zulässig ist, soweit dies im Einzelfall wegen einer Gefährdung der Erreichung des Vollzugsziels oder aus Gründen der Sicherheit oder Ordnung in der Anstalt erforderlich ist.

Der Sächsische Landtag hat das neue Strafvollzugsgesetz beschlossen. Es ist am 1. Juni 2013 in Kraft getreten.

## 8.6 Unzuständigkeit des SDB bei Zustellungen im Rahmen laufender gerichtlicher Verfahren

In diesem wie in den vorangegangenen Berichtszeiträumen erreichten mich immer wieder Beschwerden gegen die Art und Weise, wie Gerichte Schriftstücke an Beteiligte zustellen lassen.

So wurden in einem Fall Schriftstücke für eine Partei an einen Rechtsanwalt zugestellt, obwohl das Gericht Kenntnis davon hatte, dass dieser nur teilweise und nicht zur Entgegennahme von Schriftstücken bevollmächtigt worden war und später auch aus der Kanzlei ausgeschieden war.

In einem anderen Fall wurde ein Schreiben aus einem laufenden Scheidungsverfahren nicht nur an den Petenten selbst, sondern auch an ihn unter der Anschrift des Arbeitgebers versandt. Da das Schreiben allgemein an den Arbeitgeber adressiert war, wurde es durch dritte Personen geöffnet und gelesen.

Meine Zuständigkeit ist in allen diesen Fällen aus verfassungsrechtlichen Gründen nicht gegeben. Nach § 27 Abs. 4 SächsDSG unterliegen Gerichte meiner Kontrolle nur, soweit sie in *Justizverwaltungsangelegenheiten* tätig sind. Die Zustellung von Schriftstücken durch ein Gericht während eines gerichtlichen Verfahrens stellt aber eine Tätigkeit im Rahmen der Rechtspflege dar. Denn alle der Rechtsfindung auch nur mittelbar dienenden Sach- und Verfahrensentscheidungen und die zu deren Vorbereitung und Durchführung dienenden Handlungen gehören zum Kernbereich der richterlichen Tätigkeit (BGH, Urteil vom 22. Februar 2006 - RiZ R 3/05, NJW 2006, 1674 Rdnr. 21; vgl. auch Gola/Schomerus, BDSG, 10. Aufl., § 24 Rdnr. 11). Daran ändert auch die Tatsache nichts, dass die Zustellungen durch Urkundsbeamte der Geschäftsstelle erfolgen.

In diesen Fällen werden jene als Organ der Rechtspflege und nicht als Teil der Justizverwaltung tätig.

Zuständig für die Überprüfung der Rechtmäßigkeit von Zustellungen während eines gerichtlichen Verfahrens ist statt meiner nach § 22 Abs. 3 Satz 2 GVG i. V. m. § 15 Abs. 1 Nr.1 SächsJG der jeweilige Gerichtspräsident oder -direktor.

Der Sächsische Datenschutzbeauftragte ist gemäß § 27 Abs. 4 SächsDSG für die Gerichte nur im Rahmen ihrer Tätigkeit in Justizverwaltungsangelegenheiten zuständig. Daher besteht für die Prüfung der Zustellung von Schriftstücken durch ein Gericht im Rahmen eines gerichtlichen Verfahrens nur die Möglichkeit einer Dienstaufsichtsbeschwerde.

## 8.7 Einsatz von „Staatstrojanern“

Die FAZ berichtete am 9. Oktober 2011 („O`zapft is“) über erhebliche datenschutzrechtliche Mängel eines durch das BKA zur Strafverfolgung eingesetzten Schadprogramms („Bayerntrojaner“), mit dessen Hilfe die von einem Computer eines Verdächtigen geführte Kommunikation mitgelesen und -gehört werden kann („Quellen-Telekommunikationsüberwachung“ - Quellen-TKÜ). Im Vergleich zur Überwachung beispielsweise eines Festnetz-Telefongesprächs durch herkömmliche TKÜ während des Übertragungsvorgangs greift die Quellen-TKÜ zusätzlich in die Integrität eines PCs, Notebooks oder sonstigen IT-Systems des Betroffenen ein. Nach dem FAZ-Bericht habe das vom BKA gekaufte Trojaner-Programm über erhebliche Nachladefunktionen („Hintertüren“), die die vom BVerfG in seinem Urteil vom 27. Februar 2008 („Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme“) gezogenen Grenzen des rechtlich Zulässigen systematisch zu überschreiten erlaubten, verfügt. So wäre etwa die Aktivierung eingebauter Mikrofone oder Kameras oder ein Keylogging möglich gewesen. Die daraufhin geführte öffentliche Diskussion über die Missachtung des Urteils und die technischen Möglichkeiten der Überwachung informationstechnischer Systeme (Computer, Handys etc.) durch staatliche Stellen wurde auch in Sachsen geführt.

Im Rahmen dieser Diskussion habe ich sächsische Stellen um Auskunft gebeten, wann sie welche Trojaner bisher eingesetzt haben. Mir wurde mitgeteilt, dass die sächsische Polizei nur in wenigen Fällen solche Programme einzusetzen versucht habe. Davon sei ein Fall noch vor dem o. g. Urteil gelegen.

Ich stimme nicht nur mit meinem bayerischen Amtskollegen Dr. Thomas Petri darin überein, dass es im Hinblick auf Quellen-TKÜ und „Online-Durchsuchung“ noch erheblichen Handlungs-, insbesondere Gesetzgebungsbedarf gibt, etwa hinsichtlich

- des gegenüber der herkömmlichen TKÜ (bei der mittels des Providers der Inhalt einer Kommunikation auf dem Übertragungsweg erhoben wird) wesentlich tieferen Eingriffs, der eine eigenständige Rechtsgrundlage erfordert, deren Voraussetzungen enger als die der herkömmlichen TKÜ gefasst sein müssen,
- der praktisch sehr schwierigen Abgrenzung von „Quellen-TKÜ“ und „Online-Durchsuchung“,
- der praktisch ebenfalls sehr schwierigen Unterbindung von „Nachladefunktionen“,
- der Art und Weise der Durchführung von Begleitmaßnahmen wie dem Auslesen von Softwarelisten zur Vorbereitung der Installation der Software,
- der Möglichkeit einer effektiven Kontrolle dieser Schadprogramme sowie
- der Pflicht zur Benachrichtigung der Betroffenen.

Ich empfehle der Sächsischen Staatsregierung dringend, hierzu im Bundesrat initiativ zu werden, um rasch zu rechtssicheren gesetzlichen Grundlagen, etwa für den Bereich der Strafverfolgung, zu gelangen. Auf die Entschließung der Konferenz der Datenschutzbeauftragten von Bund und Ländern vom 16./17. März 2011 („Ohne gesetzliche Grundlage keine Telekommunikationsüberwachung auf Endgeräten“) sowie einen entsprechenden Antrag der Fraktionen CDU und SPD des Berliner Abgeordnetenhauses (17/0729) vom 19. Dezember 2012 weise ich hin.

Ich stelle fest: Derzeit gibt es keine Rechtsgrundlage für den Einsatz von Staatstrojanern durch sächsische Stellen.

# 9 Wirtschaft und Arbeit

## 9.1 Straßenverkehrswesen/Verkehrswesen

### 9.1.1 Übermittlung von Kfz-Halterdaten an die GEZ

Ich bekam bereits mehrfach Hinweise, dass die GEZ im Vorfeld der Kontrollbesuche von Autohäusern entsprechende Kfz-Zulassungslisten der zuständigen Kfz-Zulassungsbehörden erhalten haben sollte, um eine Gebührenpflicht zu prüfen. Diese Vermutungen konnten bisher nicht belegt werden, da entsprechende Listen nicht nachgewiesen werden konnten und die Kfz-Zulassungsstellen Herausgaben in diesem Zusammenhang bestritten. Datenschutzrechtlich zu beachten ist, dass die Übermittlung von Fahrzeug- und Halterdaten grundsätzlich nur unter den Voraussetzungen des § 35 StVG zulässig ist, die in den Fällen der Rundfunkgebührenpflicht aber nicht erfüllt sind.

Nunmehr teilte mir ein Petent mit, dass er gegen einen Gebührenbescheid einen verwaltungsgerichtlichen Rechtsschutz gesucht habe. Der Kläger machte dabei geltend, dass er gemäß § 5 Abs. 4 RGebStV als Unternehmer von den Gebühren befreit sei und verwies auf eine Entscheidung des Verwaltungsgerichtshofs Mannheim dieses Inhalts vom 30. Oktober 2008 (Az. 2 S 984/08). Teil der Gerichtsakten war eine derartige Kfz-Zulassungsliste. Die zur Stellungnahme aufgeforderte Kfz-Zulassungsstelle, die durch die Kreisgebietsreform zum 1. August 2008 nunmehr der zuständige Landkreis war, bestritt zunächst die Datenübermittlung. Nachdem ich die Behörde mit der Kopie der entsprechenden Kfz-Zulassungsliste konfrontierte, wurde jedoch eingeräumt, dass durch die damals zuständige Kfz-Zulassungsstelle „solche Listen in Absprache mit den damaligen Leitern an die GEZ übermittelt wurden. Die GEZ hat diese Auskünfte dann offensichtlich an den Gebührenbeauftragten des MDR weitergeleitet."

Da der unerlaubte Datenabfluss an die GEZ durch den Landkreis als neuer zuständiger Kfz-Zulassungsstelle nicht fortgeführt wurde, entschied ich, von einer Beanstandung abzusehen.

Eine Übermittlung ist auch weiterhin nur gemäß § 35 StVG zulässig. Auch nach Inkrafttreten des neuen Rundfunkbeitragsstaatsvertrags zum 1. Januar 2013 hat sich an den Übermittlungsvoraussetzungen nichts geändert.

### 9.1.2 Verarbeitung von GPS-Daten von Taxifahrzeugen durch eine Kommune

In der Tagespresse wurde von einem Programm „Verkehrs-Analyse-Management- und Optimierungssystem" VAMOS zur Verbesserung des fließenden Verkehrs unter anderem unter Einbeziehung von GPS-Daten von Taxis, Bussen und Bahnen zur Informationsgewinnung berichtet. Ein selbständiger Taxi-Unternehmer und Mitglied der Taxi-

genossenschaft wandte sich deshalb an mich, weil er weder durch die Taxigenossenschaft darüber unterrichtet worden sei, noch seine Einwilligung für eine Datenweitergabe an die Stadt erteilt habe.

Ich prüfte das Verfahren anhand der mir zur Verfügung gestellten Unterlagen und der Stellungnahme der Stadt. Dabei stellte ich Folgendes fest:

Im Rahmen eines vom Bund geförderten Leitprojektes koordiniert VAMOS verschiedene Verkehrssteuerungs-, Verkehrsleit- und -informationssysteme. Grundlage des Programms zur Verbesserung der Verkehrsabläufe ist die Kenntnis der aktuellen Verkehrslage im Straßennetz, wobei mitfahrende Fahrzeuge einen wichtigen Beitrag leisten. Zu diesem Zweck besteht unter anderem eine Kooperation mit der Taxigenossenschaft, wobei lediglich eine vorher bestimmte Anzahl deren Fahrzeuge einbezogen werden. Über den Leitrechner der Taxigenossenschaft werden dem System VAMOS der Stadt die Daten einzelner Fahrten der einbezogenen Fahrzeuge bereitgestellt. Jede so erfasste Fahrt erhält eine gesonderte ID-Nummer. Auf diese Weise ist eine Zuordnung der Einzelfahrten zu einem konkreten Taxi und dem Fahrzeugführer nicht möglich. Eine Weitergabe personenbezogener Daten erfolgt nicht. Unter diesen Bedingungen hatte ich keine datenschutzrechtlichen Bedenken mehr.

### 9.1.3 Datenverarbeitung bei Erlaubniserteilung für Piloten

Ein Pilotenbewerber vermutete einen unzulässigen Eingriff in sein Recht auf informationelle Selbstbestimmung, als die zuständige Luftfahrtbehörde neben anderen Nachweisen auch die Vorlage einer Auskunft aus dem Verkehrszentralregister verlangte, obwohl sie selbst als auskunftsberechtigte Stelle eine Auskunft über ihn beim Kraftfahrtbundesamt (KBA) hätte anfordern können. In der Auskunftserteilung an den Bewerber selbst würden bereits getilgte, aber in der sogenannten Überliegefrist von einem Jahr befindliche Registereintragungen enthalten sein. Bei einer Auskunftserteilung an eine Behörde würden jedoch diese in der Überliegefrist befindlichen (für den Bewerber nachteiligen) Eintragungen nicht mitgeteilt werden.

Die Landesdirektion Sachsen als zuständige Luftfahrtbehörde wies in ihrer Antwort auf meine Anfrage auf § 4 LuftVG i. V. m. § 24 LuftVZO hin. Demnach erfolgt die Hinzuziehung der Auskünfte aus dem Verkehrszentralregister im Erlaubnisverfahren für Luftfahrer (so heißen Piloten im Amtsdeutsch) aufgrund § 4 LuftVG zur Überprüfung der fliegerischen Zuverlässigkeit. Neben anderen Unterlagen hat der Bewerber nach § 24 Abs. 3 Nr. 3 LuftVZO dem Ausbildungsbetrieb oder der registrierten Ausbildungseinrichtung vor Beginn der Ausbildung eine Erklärung darüber abzugeben, dass die Beantragung einer Auskunft aus dem Verkehrszentralregister nach § 30 Abs. 8 StVG

erfolgt ist. Die in § 24 Abs. 3 Satz 1 LuftVZO aufgeführten Unterlagen, dazu gehört die Auskunft nach § 30 Abs. 8 StVG, sind der Luftfahrtbehörde spätestens bis zum ersten Alleinflug vorzulegen (§ 24 Abs. 4 Satz 2 LuftVZO). Die Vorlage der Auskunft durch den Lizenzbewerber dient der Überprüfung, ob der Bewerber erheblich oder wiederholt gegen verkehrsrechtliche Vorschriften verstoßen hat und deshalb nicht die erforderliche (fliegerische) Zuverlässigkeit besitzt (§ 24 Abs. 1 Nr. 3 i. V. m. Abs. 2 Nr. 2 LuftVZO). Die Auskunft aus dem Verkehrszentralregister ist Bestandteil der Luftfahrerakte.

Das geschilderte Verfahren ist datenschutzrechtlich nicht zu beanstanden gewesen.

## 9.2 Gewerberecht

### 9.2.1 Übermittlung von Gewerbedaten an Private

Ein Gewerbetreibender machte darauf aufmerksam, dass seine Daten wie Name, betriebliche Anschrift, angezeigte Tätigkeit, Telefon- und Faxnummern sowie E-Mail- und Internetadresse vom Gewerbeamt an eine private Firma übermittelt wurden. Ziel der das Gewerberegister führenden Stadt sei die Veröffentlichung ortsansässiger Gewerbetreibender auf der Internetseite der Stadt.

Auf Nachfrage bestätigte die Stadt die Angaben. Die genannten Angaben zu Telefon- und Faxnummern sowie E-Mail- und Internetadressen seien im Bereich Wirtschaftsförderung aus öffentlichen Verzeichnissen und aus Werbeveröffentlichungen der Gewerbetreibenden selbst erfasst und an die private Firma zur Verbesserung der Internetpräsentation der Stadt übermittelt worden. Auf der Internetseite der Stadt seien die aufbereiteten Daten der Gewerbetreibenden unter „Firmen-Datenbank“ einzusehen.

Die Übermittlung der genannten Daten ist spezialgesetzlich durch § 14 Abs. 5 GewO auf die Veröffentlichung des Namens des Gewerbetreibenden, seine betriebliche Anschrift und die angezeigte Tätigkeit beschränkt. Die Erhebung und Übermittlung der übrigen an die Firma übermittelten Daten durch die Stadt setzt (bei unterstellter erforderlicher Kenntnis der Daten zur eigenen Aufgabenerfüllung) die allgemeine Zugänglichkeit dieser Daten zwingend voraus.

Ich habe der Stadt mitgeteilt, dass die Gewerbetreibenden über den Erhebungszweck und die Freiwilligkeit der Auskunftserteilung gemäß § 12 Abs. 2 SächsDSG hinzuweisen sind, soweit Einzelangaben den nach § 14 Abs. 5 GewO zulässigen Rahmen verlassen und die zu veröffentlichenden Daten nicht aus öffentlichen Verzeichnissen stammen. Einzuholende Einwilligungen bedürfen der Schriftform und haben sich ausdrücklich auf den Zweck der Datenerhebung und die damit verbundene Übermittlung an die private Firma zu beziehen. Mit dem privaten Auftragnehmer ist bei vorliegender

Einwilligungserklärung der Betroffenen der Zweck der Datenverarbeitung, die Veröffentlichung der Daten auf der Internetseite der Stadt, sowie der Ausschluss der Datennutzung für andere Zwecke (§ 14 Abs. 12 GewO) schriftlich zu vereinbaren.

Ist eine erforderliche Einwilligung bisher nicht erteilt worden oder wird sie durch einen Betroffenen nicht erteilt, sind seine über Name, betriebliche Anschrift und angezeigte Tätigkeit hinausgehenden Angaben auf der Internetseite der Stadt zu löschen und der Auftragnehmer ist um Löschung dieser Daten zu ersuchen.

## 9.3 Industrie- und Handelskammern; Handwerkskammern

### 9.3.1 Nachweis besonders bestellter Bevollmächtigter bei der IHK

Ein Mitglied einer IHK vermutete eine willkürliche Entscheidung und Benachteiligung durch die Kammer. Mit seiner an mich gerichteten Anfrage wendete er sich gegen die Prüfung der Eigenschaft des besonders bestellten Bevollmächtigten zur Teilnahme an der Vollversammlung durch einen Fragebogen der IHK.

Die Vollversammlung ist das Beschlussgremium der IHK. Die Mitglieder der Vollversammlung werden durch die Kammerzugehörigen gewählt. Nach § 5 Abs. 2 IHK-G sind auch *besonders bestellte Bevollmächtigte von Kammerzugehörigen* wählbar. Das Nähere über die Ausübung und Durchführung der Wahl ist nach § 5 Abs. 3 IHK-G in der Wahlordnung zu regeln. Tatsächlich war eine für den Betroffenen transparente Datenerhebung anhand vorher zu erkennenden und zu erfüllenden Kriterien nicht gegeben. Die Wahlordnung der IHK enthält weder eine Begriffsbestimmung des besonders bestellten Bevollmächtigten, noch werden zu erfüllende Prüfkriterien genannt. Der Hinweis auf eine Ermächtigung für eine zweckgebundene Datenerhebung fehlte ebenfalls.

Das Anliegen der IHK, durch gezielte Fragen nur tatsächlich besonders bestellte Bevollmächtigte als Kandidaten für die Vollversammlung zuzulassen, erscheint dennoch berechtigt. In einer Beratung mit der IHK wurde vereinbart, die rechtlichen Voraussetzungen für die Prüfung der Eigenschaft des besonders bestellten Bevollmächtigten durch entsprechende Änderungen in der Wahlordnung zu verbessern. Ein weiterhin einsetzbarer Fragebogen wird in Umfang und Tiefe der Fragen auf das erforderliche Maß zu beschränken und sollte in der Wahlordnung abgebildet sein. Ich beabsichtige, die Änderungen der Wahlordnung zu verfolgen.

## 9.4 Offene Vermögensfragen

In diesem Jahr nicht belegt.

# 10 Gesundheit und Soziales

## 10.1 Gesundheitswesen

### 10.1.1 Elektronische Gesundheitskarte - Bilddatenerhebung bei den Versicherten

Im Berichtszeitraum befasste ich mich wiederholt mit der Frage, ob Versicherte verpflichtet sind, ein Lichtbild an die gesetzlichen Krankenkassen zu übermitteln bzw. welche Folgen eine Verweigerung hat. Aus der Praxis wurde mir berichtet, dass die Krankenkassen die Versicherten auffordern würden, das benötigte Lichtbild einzureichen. Dieser Aufforderung seien Versicherte jedoch in einer erheblichen Anzahl nicht nachgekommen. In diesem Zusammenhang wurde auch die Frage aufgeworfen, ob gesetzliche Krankenkassen berechtigt sind, Lichtbilder (Passfotos) bei den Pass- und Personalausweisbehörden anzufordern.

§ 24 Abs. 2 PAuswG bestimmt, dass Personalausweisbehörden anderen Behörden auf deren Ersuchen Daten aus dem Personalausweisregister übermitteln dürfen, wenn:

1. die ersuchende Behörde aufgrund von Gesetzen oder Rechtsverordnungen berechtigt ist, solche Daten zu erhalten,
2. die ersuchende Behörde ohne Kenntnis der Daten nicht in der Lage wäre, eine ihr obliegende Aufgabe zu erfüllen, und
3. die ersuchende Behörde die Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erheben kann oder wenn nach der Art der Aufgabe, zu deren Erfüllung die Daten erforderlich sind, von einer solchen Datenerhebung abgesehen werden muss.

Die Befugnis der gesetzlichen Krankenkassen zur Erhebung eines Lichtbilds ist im Fünften Buch des Sozialgesetzbuchs geregelt, § 284 Abs. 1 Satz 1 Nr. 2 SGB V i.V. m. § 291 Abs. 2 Satz 1 bzw. § 291a Abs. 2 Satz 1 SGB V. Die Sozialdaten, dazu gehört auch das Lichtbild, sind dabei grundsätzlich beim Versicherten selbst anzufordern, vgl. § 67a Abs. 2 Satz 1 SGB X. Unter bestimmten Voraussetzungen - vgl. § 67a Abs. 2 Satz 2 SGB X - kann das Lichtbild auch bei anderen Leistungsträgern bzw. bei anderen Stellen angefordert werden. Vorliegend käme § 67a Abs. 2 Satz 2 Nr. 2 a) SGB V in Betracht, wonach das Lichtbild bei anderen Personen oder Stellen (Pass- oder Personalausweisbehörden) erhoben werden darf, wenn eine Rechtsvorschrift die Erhebung bei ihnen zulässt oder die Übermittlung an die erhebende Stelle ausdrücklich vorschreibt.

Eine Rechtsvorschrift, die eine Datenerhebung der Krankenkassen bei den Pass- bzw. Personalausweisbehörden zulässt oder die Übermittlung von den Pass- bzw. Personal-

ausweisbehörden an die Krankenkassen ausdrücklich vorschreibt, liegt jedoch weder im Sozialgesetzbuch noch im Pass- oder im Personalausweisgesetz vor.

§ 24 Abs. 2 PAuswG enthält zwar eine Ermächtigungsgrundlage für die Datenübermittlung aus dem Pass- bzw. Personalausweisregister an andere Behörden. Allerdings muss nach § 24 Abs. 2 Satz 1 Nr. 1 PAuswG die ersuchende Behörde ihrerseits aufgrund konkreter Rechtsvorschriften berechtigt sein, solche Daten zu erhalten.

Die gesetzlichen Krankenkassen sind zwar aufgrund der genannten Vorschriften des Sozialgesetzbuchs Fünftes Buch befugt, ein Lichtbild des Versicherten für die Krankenversichertenkarte bzw. die elektronische Gesundheitskarte zu erhalten, diese Berechtigung bezieht sich jedoch nicht darauf, dieses von den Pass- oder Personalausweisbehörden zu empfangen.

Bei der Beibringung der Fotos handelt es sich um eine versicherungsvertragliche Nebenpflicht der Versicherten, vgl. 13/10.1.1, 15/10.1.3. Diese sind selbst gehalten, ihren Mitwirkungspflichten nachzukommen, um ihre Gesundheitsversorgung zu sichern. Das setzt voraus, dass die Krankenversicherungen die Versicherten auffordern, entsprechende Lichtbilder beizubringen oder diese von den Versicherten selbst anzufertigen. Ausnahmen, was die Beschaffung der Fotos betrifft, gelten nur für die Versicherten, denen es objektiv nicht möglich ist, selbst ein Foto zu besorgen, z. B. Schwerstbehinderte.

## 10.2 Sozialwesen

### 10.2.1 Mitwirkungspflichten des Antragstellers im Sozialleistungsverfahren - Entbindung der Ärzte von der Schweigepflicht

Mich erreichen Anfragen von Petenten, denen Sozialleistungen versagt werden, da sie nach Auskunft des jeweils zuständigen Amtes ihre Mitwirkungspflichten nicht erfüllen, konkret: Ihre behandelnden Ärzte nicht von der Schweigepflicht entbinden.

Ob für den Antragsteller im Sozialleistungsverfahren gemäß § 60 SGB I die Mitwirkungspflicht besteht, seine behandelnden Ärzte von der Schweigepflicht zu entbinden, ist meiner Auffassung nach mit Urteil des BSG vom 17. Februar 2004, Az.: B 1 KR 4/02 R (gefunden in: juris), höchstrichterlich entschieden. Ermächtigungsgrundlage ist insoweit § 66 Abs. 1 SGB I. Danach kann der Leistungsträger eine beantragte Sozialleistung ohne weitere Ermittlungen ganz oder teilweise bis zur Nachholung von Mitwirkungshandlungen versagen, wenn der Antragsteller seinen Mitwirkungspflichten nach den §§ 60 bis 62, 65 SGB I nicht nachkommt und er hierdurch oder absichtlich in anderer Weise die Aufklärung des Sachverhalts erheblich erschwert. Die Versagung ist

ausgeschlossen, wenn die Leistungsvoraussetzungen unabhängig von der fehlenden Mitwirkung nachgewiesen sind. Das BSG bestätigt insoweit ein Urteil des LSG Freiburg vom 30. November 2001 (siehe Rdnr. 3 a. a. O). In diesem Urteil stützt das LSG die Klageabweisung auf die Erwägung, die Versicherte sei verpflichtet gewesen, der Krankenkasse bzw. einem von ihr hinzuzuziehenden Gutachter die Angaben zugänglich zu machen, die zur Prüfung des geltend gemachten Anspruchs erforderlich seien, somit auch der Erteilung von Auskünften durch ihren behandelnden Arzt zuzustimmen und diesen entsprechend von der Schweigepflicht zu entbinden.

Schweigepflichtentbindungserklärungen sind von Hilfeempfängern gegenüber ihren Ärzten oder Ämtern und Einrichtungen allerdings grundsätzlich nur abzugeben, soweit es im Einzelfall für die Erfüllung der gesetzlichen Aufgabe des SGB-Leistungsträgers erforderlich ist (§ 67a Abs. 1 Satz 1 und 2 SGB X). Aus dem Erforderlichkeitsgrundsatz folgt dabei, dass die Entbindung nicht pauschal, sondern lediglich im notwendigen Umfang verlangt werden darf, also in der Erklärung *soweit wie möglich* angegeben werden muss, zu welchem Krankheitsbild, Behandlungszeitraum oder Befund Auskünfte eingeholt werden müssen. Der Betroffene muss abschätzen können, welche Daten warum an wen übermittelt werden sollen und welchen Willen er somit in Verfügung über sein Recht auf informationelle Selbstbestimmung erklärt.

Allerdings darf eine Einschränkung des Umfangs einer Schweigepflichtentbindung durch eine laienhafte Umschreibung des Krankheitsbildes nicht zu einer Beschränkung der Diagnosefreiheit der befassten Ärzte führen bzw. die medizinische oder sozialrechtlich relevante Aussagefähigkeit der erforderlichen Auskünfte schmälern. Je allgemeiner ein Krankheitsbild ist, desto schwieriger ist es dabei, die Erklärung so abzufassen, dass sie alle notwendigen Auskünfte abdeckt, gleichzeitig aber nicht uferlos wirkt.

Vor diesem Hintergrund sehe ich die Pflicht der SGB-Behörde zur Wahrung des Sozialdatenschutzes jedenfalls dann als ausreichend erfüllt an, wenn sie bei Abfassung der Erklärung geprüft hat, ob sich der Umfang der Schweigepflichtentbindungserklärung verantwortungsvoll beschränken lässt und das Ergebnis der behördlichen Einschätzung die Grenzen des vertretbaren Beurteilungsspielraums nicht verletzt. Insoweit ist die Praxis der Behörden im Umgang mit Schweigepflichtentbindungserklärungen weiterhin kritisch zu begleiten.

### 10.2.2 Zuständigkeit für Ordnungswidrigkeitenverfahren wegen Datenschutzverstößen nach SGB X

Anknüpfend an meinen Beitrag in 15/10.2.3, weise ich darauf hin, dass § 13 OWiZuVO wie folgt lautet:

*§ 13*
*Zuständigkeit des Sächsischen Datenschutzbeauftragten*

*Der Sächsische Datenschutzbeauftragte ist zuständig für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 43 Bundesdatenschutzgesetz (BDSG) in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. August 2006 (BGBl. I S. 1970) sowie nach § 85 des Zehnten Buches Sozialgesetzbuch - Sozialverwaltungsverfahren und Sozialdatenschutz - (SGB X) in der Fassung der Bekanntmachung vom 18. Januar 2001 (BGBl. I S. 130), das zuletzt durch Artikel 3 des Gesetzes vom 22. Dezember 2011 (BGBl. I S. 2983, 3014) geändert worden ist.*

Die Vorschrift erfasst somit nunmehr auch die Zuständigkeit des Sächsischen Datenschutzbeauftragten für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 85 SGB X.

### 10.2.3 Einschränkung der Übermittlungsbefugnis nach § 76 SGB X vs. Anspruch auf Löschung und Sperrung gemäß § 84 SGB X

Ein Petent, der sich gerichtlich bereits erfolgreich gegen die Verwendung eines Reha-Entlassungsberichts gewandt hatte, befragte mich, welche Maßnahmen der Rentenversicherungsträger aufgrund des obsiegenden Beschlusses zu treffen habe.

Das SG hatte entschieden, dass die Sozialdaten zu sperren seien, da der Betroffene der Verwertung des Reha-Entlassungsberichts widersprochen hätte.

Der Rentenversicherungsträger hatte den Entlassungsbericht in einem verschlossenen Briefumschlag aufbewahrt, wobei über der Klebestelle der Stempel der Rentenversicherung angebracht worden war. Dies genügte dem Betroffenen nicht.

Aus datenschutzrechtlicher Sicht musste zunächst ermittelt werden, welche Rechtsgrundlage dem Beschluss des SG zu Grunde lag, da sich hiernach die ausgelösten Rechtsfolgen und auch die zu treffenden Maßnahmen richteten. Problematisch war, dass die Formulierung, die Sozialdaten seien zu sperren, da der Betroffene deren Nutzung widersprochen habe, der datenschutzrechtlichen Systematik widerspricht.

Gemäß § 84 Abs. 1 Satz 1 SGB X sind Sozialdaten zu berichtigen, wenn sie unrichtig sind. Zwar hatte sich der Betroffene zunächst gegenüber dem Rentenversicherungsträger gegen die Richtigkeit der Daten gewandt. Über die objektive bzw. nachweisbare Richtigkeit oder Unrichtigkeit der in dem Reha-Entlassungsbericht enthaltenen Daten wurde mir jedoch nichts bekannt. Der Beschluss des SG enthielt insoweit keine Feststellungen.

Unabhängig davon dürfte gemäß § 84 Abs. 1 Satz 2 SGB X keine Sperrung erfolgen wenn die Richtigkeit oder Unrichtigkeit der Daten nicht erwiesen werden kann. Die ungeklärte Sachlage müsste aktenkundig gemacht werden. Zudem bestimmt § 84 Abs. 1 Satz 3 SGB X, dass bestrittene Daten nur mit einem Hinweis hierauf genutzt und übermittelt werden dürfen.

Ungeachtet dessen sind Sozialdaten zu löschen, wenn deren Speicherung unzulässig ist oder wenn deren Kenntnis zur Erfüllung der dem Sozialleistungsträger obliegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Betroffeneninteressen beeinträchtigt werden, vgl. § 84 Abs. 2 SGB X.

Eine Sperrung gemäß § 84 Abs. 3 SGB X ersetzt unter den gesetzlichen Voraussetzungen die Löschung im Sinne des § 84 Abs. 2 SGB X. Voraussetzung für eine Sperrung gemäß § 84 Abs. 3 SGB X ist daher das Vorliegen der Löschungsvoraussetzungen nach § 84 Abs. 2 SGB X sowie eines die Löschung ausschließenden Grundes im Sinne des § 84 Abs. 3 SGB X. Auch hierzu hatte das SG keine Feststellungen getroffen.

Es führt in der Begründung des Beschlusses aus, dass der Anspruch auf Abtrennung der Sozialdaten auf § 76 Abs. 2 Nr. 1 SGB X beruhe. Gemäß § 76 Abs. 2 SGB X dürfen Sozialdaten, die im Zusammenhang mit einer Begutachtung wegen des Erbringens von Sozialleistungen oder wegen der Ausstellung einer Bescheinigung übermittelt worden sind, weiter übermittelt werden, es sei denn gegen die weitere Übermittlung wurde widersprochen.

Die Einwendungen des Betroffenen gegen die Richtigkeit des Reha-Entlassungsberichts und den hierauf gestützten Widerspruch gegen die weitere Nutzung hat das SG (wohl) als Widerspruch gegen die Übermittlung der Sozialdaten gemäß § 76 Abs. 2 Nr. 1 SGB X gewertet. Danach dürfen die im Reha-Entlassungsbericht genannten Sozialdaten nicht an Dritte weitergeleitet, d. h. übermittelt werden.

Zur Durchsetzung dieses Übermittlungsverbots hielt ich es für geboten, dass der Reha-Entlassungsbericht der Akte entnommen und in einem anderen Aktenband geführt wird.

In die „Hauptakte“ ist ein sogenanntes Fehlblatt mit dem Inhalt, dass die betroffenen Blätter der Akte entnommen und in einem „Sonderband“ geführt werden, einzufügen. Im Ergebnis würden dann die Daten einem Gutachter in keiner Weise zugänglich gemacht werden.

### 10.2.4 Mitteilung nach § 83a SGB X

Während des Berichtszeitraums hatte sich eine SGB-Stelle an mich gewandt. Dort war es im September 2011 zu einer Störung bei der Postausgangsbearbeitung gekommen, bei der die rechtmäßigen Empfänger eines Schreibens im gleichen Umschlag ein weiteres, nicht für sie bestimmtes Schreiben erhalten haben. Die betreffenden Schreiben haben jeweils Informationen über die Bewilligung von Leistungen der betreffenden Stelle enthalten. Insgesamt wurden so 85 fehlerhafte Briefe festgestellt.

§ 83a SGB X, der die Meldepflicht bei Datenpannen regelt, ist § 42a BDSG nachgebildet und enthält eine Informationspflicht bei unrechtmäßiger Kenntniserlangung von Sozialdaten nach § 67 Abs. 12 SGB X (besondere Arten personenbezogener Daten).

Eine wesentliche Voraussetzung für eine bestehende Unterrichtungspflicht ist, dass durch die - hier außer Frage stehende - unrechtmäßige Übermittlung personenbezogener Daten schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen.

Nach meiner Einschätzung war davon hier nicht auszugehen. Angesichts des Inhalts der Schreiben (Bewilligung von Sozialleistungen) und der Tatsache, dass jeweils nur Daten eines einzelnen Betroffenen an einen - sich zudem in einer ähnlichen Lebenssituation befindlichen - Dritten übermittelt und diese Dritten jeweils bekannt und in dieser Angelegenheit auch sofort mit dem Ziel der Rücksendung bzw. der Vernichtungsbestätigung angesprochen worden waren, ließen keine schwerwiegenden Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen vermuten, weil offenbar das fälschlich beigelegte Schreiben nicht einen in der Nähe des Empfängers wohnenden Adressaten betroffen hat, so dass der gegebene Personenbezug sich nicht konkret ausgewirkt haben dürfte.

Da eine Einschätzung wie vorliegend jeweils nur auf den konkreten Einzelfall bezogen getroffen werden kann, habe ich der betroffenen SGB-Stelle allerdings empfohlen, sich auch zukünftig in Zweifelsfällen in gleicher Weise an mich zu wenden.

### 10.2.5 Auskunftsverweigerung durch den MDK

Im Berichtszeitraum erreichte mich die Anfrage, ob der sich aus § 83 Abs. 1 SGB X ergebende Auskunftsanspruch des Betroffenen eingeschränkt werden könne, wenn Anhaltspunkte dafür bestünden, dass die Gutachter des MDK bei Erteilung der Auskünfte unter Druck gesetzt würden.

Hierzu habe ich wie folgt Stellung genommen:

Einschränkungen des in § 83 Abs. 1 SGB X geregelten Auskunftsrechts sind auf Grundlage des § 83 Abs. 4 SGB X möglich.

Eine Ablehnung der Auskunft auf Grundlage des § 83 Abs. 4 Nr. 1 SGB X, demzufolge die Auskunftserteilung unterbleiben darf, wenn die rechtmäßige Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgabe gefährdet würde und auch eine Interessenabwägung zu keinem anderen Ergebnis führt, erachte ich - regelmäßig - nicht als statthaft.

Allerdings kann eine Verweigerung der Auskunftserteilung unter Umständen auf § 83 Abs. 4 Nr. 3 SGB X gestützt werden. Danach kann die Erteilung einer Auskunft auch abgelehnt werden, soweit die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten geheim gehalten werden müssen. Eine derartige Geheimhaltungspflicht begründet auch § 25 Abs. 3 SGB X, der gemäß § 276 Abs. 3 SGB V für die Einsicht in Akten des MDK entsprechend gilt. Der Schutz der Gutachter bzw. deren Familien vor verbalen und/oder körperlichen Übergriffen stellt ein berechtigtes Interesse, d. h. ein öffentliches oder privates Interesse rechtlicher, wirtschaftlicher oder ideeller Art dar, das nach der Sachlage als schutzwürdig anzuerkennen ist.

Von dieser grundsätzlichen Möglichkeit ist jedoch restriktiv Gebrauch zu machen. In diesem Zusammenhang ist insbesondere zu berücksichtigen, dass der in § 83 SGB X niedergelegte Auskunftsanspruch Ausfluss des verfassungsrechtlich gewährleisteten Rechts auf informationelle Selbstbestimmung ist. Ferner wohnt dem Auskunftsanspruch noch eine verfahrensrechtliche Komponente inne.

Voraussetzung für eine Ablehnung der Auskunft ist daher das Vorliegen ausreichender tatsächlicher Anhaltspunkte dafür, dass es bei Offenbarung des Akteninhalts zu Angriffen auf den Gutachter kommt. Die der Entscheidung zugrunde liegenden Tatsachen sowie die Vornahme der Interessenabwägung sollten im Hinblick auf die Grundrechtsrelevanz aktenkundig gemacht werden.

### 10.2.6 Übersendung von Befundunterlagen bzw. eines Gutachtens des MDK an einen gerichtlich bestellten Sachverständigen in Betreuungssachen

Ein Arzt war in einer Betreuungsangelegenheit per Gerichtsbeschluss mit der Erstellung eines psychiatrischen Fachgutachtens beauftragt worden. Mit Verweis auf den gerichtlichen Beschluss wurde der MDK um Übersendung bei ihm vorhandener Unterlagen seitens des Arztes gebeten. Der MDK bat mich um eine datenschutzrechtliche Stellungnahme hierzu.

Ergebnis: Ich sehe keine Rechtsvorschrift, die es dem MDK erlaubt, entsprechende Gutachten bzw. dazugehörige Befundunterlagen einem gerichtlich bestellten Sachverständigen auf dessen Aufforderung hin für seine Gutachtenserstellung zu übermitteln.

Dies ergibt sich aus Folgendem:

Nach § 280 FamFG hat - wie im streitgegenständlichen Fall - in Verfahren in Betreuungssachen seitens des Gerichts vor der Bestellung eines Betreuers oder der Anordnung eines Einwilligungsvorbehalts eine förmliche Beweisaufnahme durch Einholung eines Gutachtens über die Notwendigkeit der Maßnahme stattzufinden. Der Sachverständige soll Arzt für Psychiatrie oder Arzt mit Erfahrung auf dem Gebiet der Psychiatrie sein. Der Sachverständige hat den Betroffenen vor der Erstattung des Gutachtens persönlich zu untersuchen oder zu befragen (so auch ausdrücklich der mir vorgelegte Gerichtsbeschluss). Das Gutachten hat sich auf die in § 280 Abs. 3 FamFG genannten Bereiche zu erstrecken.

§ 282 FamFG regelt das Verfahren, soweit ein Gutachten des MDK nach § 18 SGB XI vorliegt. In diesem Fall gilt:

Das Gericht kann im Verfahren zur Bestellung eines Betreuers von der Einholung eines Gutachtens nach § 280 Abs. 1 FamFG absehen, soweit durch die Verwendung eines bestehenden ärztlichen Gutachtens des Medizinischen Dienstes der Krankenversicherung nach § 18 des Elften Buches Sozialgesetzbuch festgestellt werden kann, inwieweit bei dem Betroffenen infolge einer psychischen Krankheit oder einer geistigen oder seelischen Behinderung die Voraussetzungen für die Bestellung eines Betreuers vorliegen.

Das Gericht darf dieses Gutachten einschließlich dazu vorhandener Befunde zur Vermeidung weiterer Gutachten bei der Pflegekasse anfordern. Das Gericht hat in seiner Anforderung anzugeben, für welchen Zweck das Gutachten und die Befunde verwandt werden sollen. Das Gericht hat übermittelte Daten unverzüglich zu löschen, wenn es feststellt, dass diese für den Verwendungszweck nicht geeignet sind.

Kommt das Gericht zu der Überzeugung, dass das eingeholte Gutachten und die Befunde im Verfahren zur Bestellung eines Betreuers geeignet sind, eine weitere Begutachtung ganz oder teilweise zu ersetzen, hat es vor einer weiteren Verwendung die Einwilligung des Betroffenen oder des Pflegers für das Verfahren einzuholen. Wird die Einwilligung nicht erteilt, hat das Gericht die übermittelten Daten unverzüglich zu löschen.

Das Gericht kann unter den Voraussetzungen des § 282 Absätze 1 bis 3 FamFG von der Einholung eines Gutachtens nach § 280 FamFG insgesamt absehen, wenn die sonstigen Voraussetzungen für die Bestellung eines Betreuers zur Überzeugung des Gerichts feststehen.

Daraus ergibt sich, dass nach dem eindeutigen Gesetzeswortlaut das Gericht - aber auch nur dieses, nicht der von ihm bestellte Sachverständige - auf ein Gutachten des MDK zurückgreifen kann. In diesem Fall ergibt sich die Datenübermittlungsbefugnis der Pflegekasse aus § 94 SGB XI, dessen Absatz 2 lautet:

*„Die nach Absatz 1 erhobenen und gespeicherten personenbezogenen Daten dürfen für andere Zwecke nur verarbeitet oder genutzt werden, soweit dies durch Rechtsvorschriften des Sozialgesetzbuches angeordnet oder erlaubt ist. Auf Ersuchen des Betreuungsgerichts hat die Pflegekasse diesem zu dem in § 282 Abs. 1 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit genannten Zweck das nach § 18 zur Feststellung der Pflegebedürftigkeit erstellte Gutachten einschließlich der Befunde des Medizinischen Dienstes der Krankenversicherung zu übermitteln.“*

Eine Datenübermittlungsbefugnis des MDK, welche sich aus dem Sozialgesetzbuch ergeben müsste, ist nicht ersichtlich.

### 10.2.7 Unzulässige Übermittlung von Sozialdaten durch eine kommunale Kindertagesstätte

Als auf dem Gelände einer in Privatrechtsform betriebenen kommunalen Kindertagesstätte ein Kraftfahrzeug beschädigt wurde, nahm die Polizei Ermittlungen zum Unfallverursacher auf. Hierzu wurden sämtliche Eltern mit einem roten Fahrzeug zum Polizeirevier gebeten. Die Namen und Anschriften der Eltern waren durch die Leiterin der Kindertagesstätte durch Übergabe der (Kinder-)Anwesenheitsliste vom Unfalltag bekannt gegeben worden.

Obgleich die Kindertagesstätte in Privatrechtsform betrieben wurde, handelte es sich um eine § 35 SGB I unterfallende öffentliche Stelle, so dass das Datenverarbeitungshandeln

der Kindertagesstätte nach den Regelungen des Sozialdatenschutzes im Sozialgesetzbuch Zehntes Buch zu beurteilen war.

In der Übergabe der Anwesenheitsliste der Kinder an die Polizei war eine Übermittlung, d. h. ein Bekanntgeben gespeicherter, nicht gespeicherter oder durch Datenverarbeitung gewonnener Sozialdaten (vgl. § 67 Abs. 6 Nr. 3 SGB X) an einen Dritten zu sehen, die gemäß § 67d Abs. 1 SGB X nur statthaft gewesen wäre, wenn sich hierfür aus den §§ 68 bis 77 SGB X oder einer anderen Rechtsvorschrift aus einem der Sozialgesetzbücher eine Übermittlungsbefugnis ergeben hätte.

Vorliegend waren die Voraussetzungen der in Betracht kommenden Übermittlungsbefugnisse nicht gegeben.

§ 68 Abs. 1 Satz 1 SGB X gestattet im Einzelfall auf Ersuchen die dort näher bezeichneten Daten zu übermitteln, soweit kein Grund zu der Annahme besteht, dass schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Für eine rechtmäßige Datenübermittlung auf Grundlage des § 68 Abs. 1 Satz 1 SGB X ist immer eine konkrete Abwägung zwischen dem öffentlichen Informationsinteresse und dem Interesse des Einzelnen am Schutz seiner Sozialdaten erforderlich. Die Beantwortung von Ausforschungsersuchen, d. h. Ersuchen auf Datenübermittlungen, in Fällen, in denen nur die Zugehörigkeit zu einer bestimmten Personengruppe bekannt ist, darf daher auf dieser Rechtsgrundlage nicht erfolgen.

Die Datenübermittlung konnte auch nicht auf Grundlage des § 73 Abs. 1 oder 2 SGB X erfolgen, da es an der gemäß § 73 Abs. 3 SGB X erforderlichen richterlichen Anordnung fehlte.

Das kommunale Unternehmen hat mir gegenüber unter anderem vorgebracht, dass es das vorliegende Übermittlungsersuchen fälschlich nach den (hier nicht maßgeblichen) Regelungen des Sächsischen Datenschutzgesetzes beurteilt habe.

Ich habe den Fall zum Anlass genommen, auf die Vorrangigkeit der Regelungen des Sozialgesetzbuchs, also des Sozialdatenschutzes in deren Anwendungsbereich und die hier abweichend zum Sächsischen Datenschutzgesetz geregelte Übermittlungsverantwortung hinzuweisen.

Da sich das städtische Unternehmen für den Verstoß entschuldigt und Maßnahmen zur Vermeidung weiterer Verstöße getroffen hat, habe ich von einer Beanstandung abgesehen.

### 10.2.8 Aufforderung des Jugendamts zur Erhebung der Anwesenheitszeiten der in Kindertagesstätten in freier Trägerschaft betreuten Kinder

Gleich mehrfach wandten sich Eltern mit der Bitte an mich, die Datenerhebung einer sächsischen kreisfreien Stadt bei freien Trägern der Jugendhilfe im Zusammenhang mit dem Besuch von Kindertagesstätten zu prüfen.

Die Stadt hatte sich schriftlich an die freien Träger gewandt und forderte diese auf, für einen Zeitraum von einem Monat sämtliche Kinder mit Name, Vorname, Betreuungsbeginn und Abholzeit in einer Liste zu erfassen und diese sodann dem Jugendamt vorzulegen.

Auf meine - unter Hinweis auf die besondere Eilbedürftigkeit - gestellte Nachfrage bei der Stadt erhielt ich erst auf nachdrückliche Wiederholung und Hinweis auf die mir obliegende Kontrollbefugnis eine Antwort.

In dieser wurde mitgeteilt, dass die Finanzierung der Kindertagesstätten in dieser Stadt auf der Grundlage von Platzpauschalen in Abhängigkeit von der zwischen den Eltern und den Trägern der Kindertagesstätten vereinbarten Betreuungszeiten erfolgen würde. Die Stadt sei gemäß § 17 Abs. 2 SächsKitaG verpflichtet, den durch Elternbeiträge und den Elternanteil nicht gedeckten Anteil der in § 14 SächsKitaG geregelten Betriebskosten zu übernehmen, wozu zwischen der Gemeinde und dem Träger der Einrichtung eine Vereinbarung zu treffen sei. Aufgrund dieser Vereinbarung sei die Stadt berechtigt, die zweckentsprechende Mittelverwendung zu prüfen. Hierzu wiederum sei ein Vergleich zwischen der im (Betreuungs-)Vertrag vereinbarten Betreuungszeit und den tatsächlichen Präsenzzeiten der Kinder erforderlich. Außerdem habe man in Abstimmung mit dem städtischen Datenschutzbeauftragten die Abfrage der Anwesenheitsdaten zwischenzeitlich präzisiert.

Auf meine erneute Nachfrage, weshalb zur Prüfung der zweckentsprechenden Mittelverwendung ein Vergleich zwischen der vereinbarten Betreuungszeit und der tatsächlichen Anwesenheitszeit erforderlich sei, wenn die Finanzierung auf Grundlage der vereinbarten Betreuungszeit - so die Ausführungen der Stadt - erfolge, erhielt ich ein nahezu wörtlich mit dem ersten Antwortbrief übereinstimmendes Schreiben.

Diese Tatsache habe ich zum Anlass genommen, mir den Inhalt des (jetzt) geforderten Datensatzes darstellen zu lassen. Überdies habe ich stichprobenartig geprüft, inwieweit eine Präzisierung der Abfrage der Anwesenheitsdaten stattgefunden hat.

Die Prüfung ergab, dass zwischenzeitlich auf die Übermittlung der Namen der Kinder verzichtet wurde. Von einer Präzisierung der Abfrage gegenüber den freien Trägern

konnte indes keine Rede sein. Mittlerweile waren die Schreiben so ausgestaltet, dass die Daten zwar namentlich gefordert wurden und zugleich auf die Möglichkeit (!) einer anonymisierten Übermittlung hingewiesen wurde. Besonders überrascht hat mich jedoch der folgende, in den Schreiben der Stadt zu findende Passus an die freien Träger:

> *„Wir möchten nochmals darauf verweisen, dass die Erhebung der Daten rechtmäßig ist und sowohl vom Datenschutzbeauftragten der Stadt [...] als auch dem Sächsischen Datenschutzbeauftragten genehmigt wurde."*

Ich habe daher die Stadt gemäß § 29 Abs. 1 Satz 1 SächsDSG angehört und schließlich eine Beanstandung ausgesprochen, da zum einen das Datenverarbeitungshandeln rechtswidrig war und zum anderen trotz meiner hiergegen erhobenen Einwände gegenüber den freien Trägern der Jugendhilfe behauptet wurde, ich hätte die Datenerhebung genehmigt. Hierin war ein weiterer Verstoß gegen die Vorschriften über das Verhältnis zwischen dem Sächsischen Datenschutzbeauftragten und den seiner Kontrolle unterstehenden Stellen (§§ 27 f. SächsDSG) zu sehen.

Da die Stadt auch im Anhörungsverfahren nicht darlegen konnte, weshalb die Anwesenheitszeiten für die Kontrolle der zweckentsprechenden Mittelverwendung erforderlich hätten sein sollen, war die Datenerhebung gemäß § 62 Abs. 1 SGB X unzulässig. Dabei wäre die Kontrolle der zweckentsprechenden Mittelverwendung tatsächlich als Aufgabe der Kinder- und Jugendhilfe anzuerkennen gewesen. Wenn die Finanzierung aufgrund der vereinbarten Betreuungszeit erfolgt, werden Mittel bereits dann zweckentsprechend verwandt, wenn sie zur Vorhaltung der vertraglich geschuldeten Betreuungsleistungen verwandt werden. Auf die tatsächliche Inanspruchnahme der Leistungen kommt es somit nicht an, so dass die zu deren Prüfung erfolgende Datenerhebung rechtswidrig war.

In der Folge war auch eine sich an die Erhebung anschließende Datennutzung rechtswidrig, da diese nicht durch einer Rechtsvorschrift in einem der Sozialgesetzbücher erlaubt oder angeordnet war, vgl. § 67b Abs. 1 Satz 1, 2. Fall SGB X, und zudem auch keine die Datennutzung rechtfertigenden Einwilligungen der Betroffenen ersichtlich waren. Überdies war auch die Datenspeicherung rechtswidrig, da es auch hier wieder an der Erforderlichkeit zur Aufgabenerfüllung fehlte.

Auch auf die Beanstandung des weiteren Verstoßes konnte ich nicht verzichten, da die Behauptung eines Missverständnisses der umfangreichen, mit mir geführten Korrespondenz mich nicht überzeugt hat. Zu dem Zeitpunkt, als die Behauptung, ich hätte die Datenerhebung genehmigt, aufgestellt wurde, beschränkte sich die mit mir geführte „intensive Kommunikation" auf meine Anfrage, Wiederholungen derselben, einen

Antwortbrief der Stadt sowie ein weiteres Schreiben von mir. In letzterem hatte ich zur Prüfung des Sachverhalts weitere Informationen angefordert.

Auf meine Veranlassung wurden nach Angaben der Stadt die erhobenen Daten datenschutzgerecht vernichtet und darüber hinaus auch gegenüber den Freien Trägern klargestellt, dass es keine Genehmigung der Datenerhebung durch mich gegeben hat. Es bleibt zu hoffen, dass die Stadt - wie von ihr behauptet - durch das Beanstandungsverfahren tatsächlich mehr für die Belange des Datenschutzes sensibilisiert wurde und diese - wie mir ebenfalls versichert wurde - zukünftig stärker berücksichtigen wird.

### 10.2.9 Gemeindliche Bedarfskriterien für die Vergabe von Plätzen in Kindertagesstätten

Wiederholt beschäftigten mich Datenerhebungen im Zusammenhang mit der Vergabe von Plätzen in Kindertagesstätten.

Zu der Frage der (beabsichtigten) Aufstellung gemeindlicher Bedarfskriterien habe ich wie folgt Stellung genommen:

Kinder haben ab Vollendung des dritten Lebensjahres bis zum Schuleintritt gemäß § 24 Abs. 1 Satz 1 SGB VIII einen Anspruch auf einen Platz in einer Kindertagesstätte. Diese aus dem Sozialgesetzbuch Achtes Buch folgende Leistungspflicht trifft den örtlichen Träger der öffentlichen Jugendhilfe, vgl. § 3 Abs. 2 Satz 2 SGB VIII. Die Träger der öffentlichen Jugendhilfe werden gemäß § 69 Abs. 1 SGB VIII durch das Landesrecht bestimmt. Gemäß § 1 Abs. 1 LJHG sind die Landkreise und kreisfreien Städte örtlicher Träger der öffentlichen Jugendhilfe. Nach § 8 Satz 1 LJHG können kreisangehörige Gemeinden unter der Voraussetzung des § 8 Satz 2 LJHG im Einvernehmen mit dem örtlichen Träger der öffentlichen Jugendhilfe dessen Aufgaben wahrnehmen. Hierdurch werden die kreisangehörigen Gemeinden jedoch nicht zum örtlichen Träger der öffentlichen Jugendhilfe. Dies ergibt sich daraus, dass sich die Norm ausdrücklich auf die Aufgabenwahrnehmung beschränkt, ohne die Trägerschaft zu übertragen. Anspruchsverpflichtet gemäß § 24 Abs. 1 Satz 1 SGB VIII bleibt daher in jedem Fall der betreffende Landkreis oder die betreffende kreisfreie Stadt.

Da die Bedarfskriterien den sich aus dem Sozialgesetzbuch Achtes Buch ergebenden Anspruch konkretisieren, kommt eine Datenerhebung zur Feststellung des Vorliegens der Bedarfskriterien nur durch den örtlichen Träger der öffentlichen Jugendhilfe in Betracht. Denn die Erhebung von Sozialdaten ist nur statthaft, wenn die Daten zur Erfüllung der jeweiligen Aufgabe erforderlich sind, vgl. § 62 Abs. 1 SGB VIII. Die hier in Rede stehende Aufgabe, d. h. die Feststellung des Anspruchsumfangs, obliegt jedoch dem Leistungsverpflichteten, mithin dem örtlichen Träger der öffentlichen Jugendhilfe.

Eine Rechtsgrundlage für die Aufstellung (weiterer) gemeindlicher Bedarfskriterien existiert nicht, da diese nicht zur Erfüllung einer der Gemeinde nach dem Sozialgesetzbuch Achtes Buch obliegenden Aufgabe dienen. Denn soweit der leistungsverpflichtete örtliche Träger der öffentlichen Jugendhilfe einen bestimmten Anspruchsumfang festgestellt hat, scheidet dessen Einschränkung durch die (kreisangehörige) Gemeinde aus. Eine zur Feststellung gemeindlicher Bedarfskriterien erfolgende Datenerhebung gemäß § 62 Abs. 1 SGB VIII wäre daher unzulässig.

### 10.2.10 Anforderung einer Vermieterbescheinigung durch kommunale Jobcenter

Es erreichten mich eine Vielzahl von Anfragen zu der Frage, wann die Einholung einer Mietbescheinigung beim Vermieter im Zusammenhang mit der Gewährung von Leistungen nach dem Sozialgesetzbuch Zweites Buch statthaft sei. Ich habe diese Frage regelmäßig wie folgt beantwortet:

1. Aus der Mietbescheinigung selbst darf nicht ersichtlich sein, welchem Zweck diese dient. Diese darf also insbesondere keine Hinweise wie „zur Vorlage beim Kommunalen Jobcenter“ o. Ä. enthalten. Denn durch eine derartige Ausgestaltung der Mietbescheinigung werden zugleich auch Sozialdaten des Betroffenen (Antragstellung bzw. Bezug von Leistungen nach dem Sozialgesetzbuch Zweites Buch) einem Dritten gegenüber (hier: Vermieter) offenbart. Für eine derartige Datenübermittlung (zum Begriff: § 67 Abs. 6 Satz 2 Nr. 3 SGB X) besteht jedoch kein Erfordernis.

2. Eine Bescheinigung des Vermieters darf nur angefordert werden, wenn die Erhebung der erforderlichen Daten beim Betroffenen ausscheidet, sei es, weil dieser über die erforderlichen Daten nicht verfügt oder weil Zweifel an deren Richtigkeit bestehen.

Verschiedene SGB II-Behörden teilten diese Auffassung nicht. Zum Teil beriefen sie sich nur lapidar darauf, dass die mit der Mietbescheinigung angeforderten Daten für die Leistungsgewährung erforderlich seien, zum Teil erfolgte zu der Thematik ein umfassender Meinungsaustausch. Eine SGB II-Behörde schaltete die zuständige Aufsichtsbehörde, das SMS, ein.

Im Ergebnis konnte ich mich mit dieser SGB II-Behörde dann auf folgende Vorgehensweise verständigen:

1. Grundsätzlich wird ausschließlich das Zusatzblatt 1.1 zum Leistungsantrag verwendet, das ausschließlich vom Antragsteller auszufüllen ist.

2. Die Mietbescheinigung wird so gestaltet, dass das Logo des Jobcenters aus dem Antrag entfernt wird, sodass der Aussteller der Mietbescheinigung nicht mehr erkennbar ist.

3. Mietbescheinigungen werden künftig nur noch angefordert:

   - zur Klärung bei nicht plausiblen Angaben im Rahmen eines Ordnungswidrigkeitenverdachts bzw. eines Verdachts auf Leistungsmissbrauch sowie
   - zur Sachverhaltsaufklärung, wenn die Leistungsberechtigten keine weiteren Nachweismöglichkeiten haben bzw. keine anderen Angaben zur Verfügung stehen.

Es ist davon auszugehen, dass andere SGB II-Behörden sich dieser Auffassung anschließen werden.

### 10.2.11 Eine unzulässige zweckändernde Nutzung von Sozialdaten, ein fahrlässiger Umgang mit dem städtischen Datenschutzbeauftragten und eine grobe Missachtung meines Auftrags aus Art. 57 SächsVerf i. V. m. § 27 f. SächsDSG

Eine Beanstandung gemäß § 29 Abs. 1 Satz 1 Nr. 2 SächsDSG i. V. m. § 81 Abs. 2 Satz 2 und 3 SGB X habe ich im folgenden Fall aussprechen müssen:

Wegen des seinerzeit offenbar nur sehr zögerlichen Interesses der Anspruchsberechtigten an einer Inanspruchnahme von Sozialleistungen aus dem mit Bundesgesetz vom 24. März 2011 eingeführten sogenannten „*Bildungs- und Teilhabepaket der Bundesregierung*“ sah sich der Geschäftsbereich Soziales einer sächsischen Großstadt aus diesem Grunde und - damit jedenfalls nicht ganz in Übereinstimmung zu bringen - auch wegen „*immenser telefonischer und persönlicher Anfragen*“ dazu veranlasst, am 16. Mai 2011 alle rund 5.000 Haushalte des Gemeindegebiets anzuschreiben, die zum Stichtag 1. Januar 2011 wenigstens einen Monat im Wohngeldbezug standen und in denen mögliche Anspruchsberechtigte für die neuen Sozialleistungen lebten. Zu diesem Schritt sah sich die öffentliche Stelle auch deshalb ermuntert bzw. ermächtigt, weil die Bundesministerin für Arbeit und Soziales und der Deutsche Städtetag am 21. April 2011 - wie den jeweiligen Pressemitteilungen zu entnehmen ist - an einem „Runden Tisch“ ein persönliches Anschreiben etwaiger Anspruchsberechtiger vereinbart hätten.

Ähnlich gehaltene Schreiben des Geschäftsbereichs Soziales der betreffenden Stadt erhielten über dessen Hauspost wenige Tage zuvor auch rund weitere 630 Empfänger wegen ihres Bezugs von Leistungen nach dem 3. oder 4. Kapitel SGB XII sowie rund 50 Empfänger von Leistungen nach § 2 AsylbLG.

Die Schreiben wurden dabei trotz erheblicher rechtlicher Bedenken des erst kurz vor dem Versand beteiligten städtischen Datenschutzbeauftragten versandt, obgleich dieser mit E-Mail vom 4. Mai 2011 unter Darlegung seiner Einwände einen Verzicht empfohlen hatte. Anhaltspunkte für eine vor dem Ausgang der Schreiben und dem Beginn meiner Kontrolle erfolgte rechtliche Auseinandersetzung mit seinem Vorbringen bzw. sonst mit den Vorschriften des Sozialdatenschutzes - und sei es nur in der behaupteten „summarischen“ Weise - habe sich in den Akten allerdings nicht finden lassen. Als Antwort auf seine Bedenken bekam der städtische Datenschutzbeauftragte am gleichen Tag lediglich die kurze elektronische Mitteilung des Büros des Beigeordneten für Soziales, wonach seine E-Mail an das Sozialamt „*zur Beachtung*“ weitergeleitet worden wäre. Derweil veranlasste das Büro des Beigeordneten für Soziales die Versendung der Schreiben. Der städtische Datenschutzbeauftragte wurde in der Angelegenheit nicht weiter konsultiert, selbst zu dem Zeitpunkt als ich die datenschutzrechtliche Gestattung des für die Versendung notwendigen Verarbeitungshandelns hinterfragt habe.

Der Zweck, für den die für die Versendung der Schreiben notwendigen Daten - Leistungsempfänger-Daten - ursprünglich erhoben worden waren, war, Anträge auf Gewährung von Sozialleistungen zu bearbeiten, über sie zu entscheiden und gegebenenfalls die Leistungen zu gewähren. Im Bereich der Sozialleistungsgewährung - in Abgrenzung zur ausnahmsweise im Sozialrecht vorgesehenen Tätigkeit von Sozialleistungsträgern im Bereich der Gefahrenabwehr: Jugendhilfe - wird der Zweck durch die Stellung und die Aufrechterhaltung des Antrags auf Leistungsgewährung bestimmt, also inhaltlich begrenzt; hinzukommen kann ein im Erhebungszeitpunkt nach dem zu diesem Zeitpunkt geltenden Recht absehbarer damit in gesetzlich bestimmtem Sachzusammenhang stehender weiterer Verfahrens-Zweck und auch ein nach dem zu dem betreffenden Zeitpunkt geltenden Recht in Betracht zu ziehender und gezogener Ersatz-Verfahrenszweck (z. B. EU-Rente statt Rehabilitationsverfahren, s. näher Rombach in Hauck/Haines Rdnr. 28 bis 30 zu § 67c SGB X), als mittelbar durch den Antrag zum Verfahrenszweck gemachter Zweck.

Mit der für die Versendung der Schreiben vorgenommenen Nutzung von Daten von Leistungsempfängern nach den Vorschriften des Wohngeldgesetzes, nach dem 3. oder 4. Kapitel SGB XII sowie nach § 2 AsylbLG ist jedoch ein anderer, jenseits der bisherigen Verfahrenszwecke liegender Zweck verfolgt worden, und zwar derjenige, *potentielle* Anspruchsinhaber auf andere mögliche Leistungen nach dem Sozialgesetzbuch aufmerksam zu machen, die von diesen bisher nicht beantragt und auch nicht in dem gerade erläuterten Sinne mittelbar zum Verfahrenszweck gemacht worden waren. Somit beinhaltete die von der Stadt vorgenommene Nutzung der ursprünglich für andere durch die betreffenden Leistungs-Anträge bestimmten Zwecke erhobenen Daten eine

*Zweckänderung*. Diese ist nach § 67c Abs. 2 Nr. 1 SGB X nur zulässig, soweit die Daten zur Erfüllung einer Aufgabe nach anderen Rechtsvorschriften des Sozialgesetzbuchs als jenen, für die sie ursprünglich erhoben wurden, *erforderlich* sind.

Eine die Zweckänderung gestattende Aufgabe der Sozialverwaltung, potentielle Anspruchsberechtigte von Leistungen nach dem sogenannten Bildungs- und Teilhabepaket mittels eines an diese persönlich gerichteten Schreibens auf die Möglichkeit ihrer Leistungsberechtigung und einen etwaigen Leistungsumfang aufmerksam zu machen, besteht aber nicht:

1. *Nach § 14 SGB I* ist der Leistungsträger verpflichtet, ausgehend von einem bestehenden Sozialrechtsverhältnis einzelne Personen individuell und bezogen auf ihre konkrete Situation über die Wahrnehmung ihrer Rechte nach dem Sozialgesetzbuch zu beraten. Die als subjektives Recht gegenüber dem Leistungsträger und eben nicht als dessen allgemeine Beratungsbefugnis und -pflicht gefasste Vorschrift setzt dabei ein konkretes Beratungsverlangen voraus, welches hier jedoch nicht vorliegt. Gegen oder auch nur ohne den Willen des Betroffenen sollen ihm grundsätzlich keine Ratschläge erteilt werden, es sei denn, es bestünde für den Leistungsträger deswegen eine Rechtspflicht zur Beratung bzw. Aufklärung, weil dem Betroffenen ohne diese erhebliche sozialrechtliche Nachteile drohen und davon auszugehen wäre, dass bei einem Hinweis auf Gestaltungsmöglichkeiten jeder Betroffene diese auch nutzen würde (vgl. Sauer in Wiegand/Menard/Jahn/Figge/Wältermann, Sozialgesetzbuch für die Praxis, Kommentar, Stand 211/2010, § 14 Rdnr. 9 m. w. N.). Dies erfasst allerdings nur wenige Fallkonstellationen, in denen der Leistungsträger wegen des Unterlassens der Beratung bzw. einer damit einhergehenden Verletzung seiner Aufklärungspflicht Gefahr liefe, für den Beratungsmangel rechtlich einstehen zu müssen. Im Fall der Nichtinanspruchnahme von Leistungen des sogenannten Bildungs- und Teilhabepakets erleiden die Betroffenen hinsichtlich der ihnen bisher gewährten Leistungen jedoch keinen Nachteil, da es sich um eigenständige Leistungen handelt, deren Inanspruchnahme nicht zuletzt aufgrund des elterlichen Erziehungsrechts völlig freiwillig und deren Attraktivität abhängig von der individuellen Lebensgestaltung ist. Für die Zulässigkeit einer Nutzung von Sozialdaten für Zwecke einer abstrakten Spontan- bzw. Initiativberatung zu den Vorzügen des Bildungs- und Teilhabepakts sehe ich jedenfalls mit Blick auf § 14 SGB I schon aus diesem Grund keinen Raum. Zudem handelt es sich bei dem von der Stadt verfassten Schreiben auch nicht um eine Beratung i. S. d. Vorschrift, denn über die Adressatenauswahl hinaus ist nicht erkennbar, inwiefern es gerade der besonderen individuellen Situation des jeweils Angeschriebenen Rechnung trägt. Anders gesagt: Der Grad der Individualisierung der Schreiben erschöpft sich in den durch die Datenverarbeitung

ermittelten Angaben im Adressfeld und der persönlichen Anrede; ansonsten hat jeder Empfänger eine völlig identische - also nicht weiter individualisierte - Mitteilung erhalten. Statt einer Beratungsleistung i. S. d. § 14 SGB I handelt es sich bei den Schreiben also um ein bloßes, sich an alle auch nur irgendwie potentiell Berechtigte richtendes, allgemeines Beratungsangebot bzw. eine für die Sozialleistung werbende Informationsschrift mit Antragsformular, deren Empfängerkreis lediglich - möglicherweise des Aufwands wegen - begrenzt werden sollte.

2. *Nach § 13 SGB I* sind die Leistungsträger zwar verpflichtet und damit auch berechtigt, im Rahmen ihrer Zuständigkeit die Bevölkerung über die Rechte und Pflichten nach dem Sozialgesetzbuch aufzuklären. Eine solche, sich an die Bevölkerung in ihrer Gesamtheit richtende Aufklärung ist jedoch grundsätzlich nicht persönlich angelegt und kommt deswegen nicht in der Weise gezielt in Betracht, dass der Kreis der Adressaten datenverarbeitungstechnisch durch Suchläufe ermittelt werden darf (vgl. Sauer in Wiegand/Menard/Jahn/Figge/Wältermann, § 13 Rdnr. 15). Vom Anwendungsbereich der Vorschrift erfasst sind somit allein allgemeine - sich an jedermann richtende - Informationsmittel, wie beispielsweise die Publikation von Broschüren oder das Schalten von Informationsanzeigen in Printmedien. Die Stadt wäre also lediglich befugt gewesen, den Inhalt des Schreibens im Amtsblatt zu veröffentlichen oder allen Leistungsbeziehern - ohne eine (datenverarbeitungstechnische) Eingrenzung auf den Kreis der potentiell Anspruchsberechtigten - beim Versand von Bescheiden eine Informationsbroschüre beizulegen. Dass es solche, keine Datenverarbeitung erfordernden und damit im Sinne der Verhältnismäßigkeit milderen, Alternativen auch aus Sicht der Sozialverwaltung jedenfalls „grundsätzlich“ gegeben hätte, hat die Behörde mir gegenüber eingeräumt.

3. *§ 4 Abs. 2 Satz 2 SGB II* enthält, wie sich aus der Gesetzesbegründung (BT-Drs. 17/3404, 26. Oktober 2010, S. 91, zu Nr. 5, zu Absatz 2) ergibt, lediglich die Aufgabe, darauf hinzuwirken, dass organisatorische Strukturen geschaffen werden, die die Gewährung der Leistungen aus dem Bildungs- und Teilhabepaket auch tatsächlich ermöglichen - jedoch über das Hinwirkungsgebot hinaus keine unmittelbare Aufgabenzuweisung im Sinne einer individuellen und von einem Beratungsersuchen unabhängigen Beratungspflicht oder auch nur -befugnis: Satz 4 des § 4 Abs. 2 SGB II verpflichtet die SGB II-Behörde allein zu dem, was im neunten (und letzten) Satz der genannten Gesetzesbegründung zum neuen § 4 Abs. 2 SGB II genannt ist, nämlich dazu, in Unterstützung der Eltern dazu beizutragen, dass diese mittels verbindlicher Absprachen über die Inanspruchnahme von Angeboten darauf hinwirken, dass die Kinder und Jugendlichen die Angebote auch tatsächlich in Anspruch nehmen. Auch dies begründet keine Pflicht oder auch nur Befugnis zur Nutzung von Sozialdaten

außerhalb durch entsprechende Anträge durch Elternseite gestalteter Sozialleistungsverhältnisse (und damit Zwecke). Die SGB II-Behörde wird durch § 4 Abs. 2 SGB II nicht zur Jugendhilfebehörde. Abgesehen davon: Die Vorschrift gilt nur für die SGB II-Behörde, also gerade nicht für die das Wohngeldrecht, das Kindergeldrecht, die Sozialhilfe und das Asylbewerberleistungsgesetz ausführenden Behörden, also diejenigen Sozialleistungsbehörden der Stadt, für die der Sächsische Datenschutzbeauftragte die zuständige Datenschutzkontrollbehörde ist (vgl. § 50 Abs. 4 Satz 3 SGB II).

Da sich auch aus sonstigem Recht keine Aufgabenzuweisung ergibt, die das Erfordernis einer Zweckänderung nach § 67c Abs. 2 Nr. 1 SGB X begründen könnte, fehlte es also an der für die Daten-Nutzung nötigen rechtlichen Grundlage. Ein (sozial-)politisches Erfordernis bzw. Bedürfnis, auf das sich die Stadt und andere Stellen mittelbar zu berufen schienen, ist vom Anwendungsbereich des § 67c Abs. 2 Nr. 1 SGB X nicht erfasst. Pressemitteilungen, Rundschreiben, Ministergespräche oder Runde Tische dürfen nicht die Suche nach Rechtsgrundlagen für Grundrechtseingriffe ersetzen.

Im Kontext der Beanstandung habe ich mir auch einen Hinweis auf den fahrlässigen Umgang mit dem städtischen Datenschutzbeauftragten und seinen Bedenken und der darin liegenden völligen Verkennung seiner Funktion nach § 11 Abs. 4 SächsDSG erlaubt.

Des Weiteren habe ich im Rahmen meiner Kontrolle folgende „Auffälligkeiten“ im Umgang mit meiner Aufsichtstätigkeit als grobe Missachtung meines Auftrags aus Art. 57 SächsVerf i. V. m. § 27 f. SächsDSG feststellen müssen:

Ausweislich eines in dem betreffenden Verwaltungsvorgang befindlichen - und wegen seiner Hinzunahme zur Vorgangsakte damit amtlichen - Vermerks hat sich der Geschäftsbereich Soziales der betreffenden Stadt wegen meiner Kontrolle nicht nur dazu veranlasst gesehen, sich - was nicht weiter zu kritisieren wäre - im Nachhinein bei anderen Stellen um rechtliche Argumentationshilfen zu bemühen, welche die Rechtmäßigkeit des eigenen Verwaltungshandelns stützen können. Jedoch die ebenso aktenkundige (untaugliche) Absicht, den Bundesdatenschutzbeauftragten einschalten zu wollen, um meiner Behörde *„Einhalt zu gebieten“* und ein offenbar am 25. August 2011 stattgefundenes Gespräch des Sozialbürgermeisters der Stadt mit Vertretern des SMS und des Sächsischen Städte- und Gemeindetags, zu dessen Ergebnis in der Akte hinsichtlich meiner behördlichen Tätigkeit vermerkt ist *„Anfrage blocken“* und *„Angelegenheit als ‚erledigt betrachten‘“*, wirft ein sehr bedenkliches Licht auf das Verständnis der Beteiligten von meiner verfassungsmäßigen Rolle. Grotesk mutet dabei an, dass von der beanstandeten Stadt hierzu erklärt wird, dass der die Beratung „kaum noch treffend

wiedergebende“ Vermerk nicht für die „Öffentlichkeit“, zu der offenbar auch meine Behörde gezählt wird, bestimmt gewesen und im Übrigen ja auch nicht von den Besprechungsteilnehmern „bestätigt“ worden sei, wobei offen gelassen wird, welche andere - und offenbar gewichtigere - Form der Autorisierung es für ein Verwaltungshandeln geben kann, als einen Vermerk hierüber aktenkundig werden zu lassen.

Das SMS habe ich gemäß § 29 Abs. 1 Satz 2 SächsDSG als zuständige Aufsichtsbehörde über die Beanstandung unterrichtet.

## 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 Weinbau - Pächterdaten

Der Pächter eines Weinbergs hatte einzelne Parzellen an Unterpächter verpachtet. Das zuständige SMUL beabsichtigte, da die Rebanlagen nicht genehmigt waren, Sanktionen zu erlassen. Der von der Behörde deswegen angesprochene Hauptpächter verwies auf die abgeschlossenen Unterpachtverträge, die er in Kopie übersandte. Auf diesen waren die Anschriften der Unterpächter auf deren Wunsch hin geschwärzt. Als die Behörde diese dennoch anschrieb, wandte sich der Hauptpächter wegen eines vermuteten Datenschutzverstoßes an mich.

Eine rechtswidrige Datenverarbeitung vermochte ich jedoch nicht festzustellen. Die Erhebung der Adressen der Unterpächter war gemäß § 12 Abs. 4 Nr. 8 SächsDSG rechtmäßig erfolgt, da eine gesonderte Ermittlung der Adressen der Unterpächter einen unverhältnismäßigen Aufwand erfordert hätte. Die Erhebung der Adressen erfolgte dabei aus den übersandten und der Behörde zur Verfügung gestellten Vertragsdokumenten, da die Pächterdaten wegen der unzureichend erfolgten Schwärzung auf den Schriftstücken immer noch relativ leicht zu erkennen waren. Das beanspruchte Interesse der Unterpächter am Unterbleiben der Übermittlung ihrer Namen und Anschriften war dabei nach meiner Einschätzung nicht schutzwürdig, da die Rebanlagen nicht genehmigt waren.

# 12 Umwelt und Landesentwicklung

## 12.1 Datenschutz bei Behördenanfragen und Widerspruchsverfahren

Eine als Verein organisierte Interessengemeinschaft für regionalen Umweltschutz, vertreten durch ihren Vorsitzenden und dessen Stellvertreter, beschwerte sich über den Umgang des Sächsischen Oberbergamts mit ihren personenbezogenen Daten. Unter Verwendung des Briefbogens des Vereins hatten sich die Betroffenen an das Sächsische Oberbergamt mit Fragen und Hinweisen zu vermuteten unzulässigen Emissionen durch eine ansässige Firma gewandt. Das Sächsische Oberbergamt sandte daraufhin eine Kopie des Beschwerdeschreibens an die Firma mit der Bitte um Stellungnahme.

Die Beantwortung von Anfragen und Beschwerden gehört zu den Aufgaben einer Behörde. Die Nutzung personenbezogener Daten ist zulässig, soweit dies zur Erfüllung der Aufgaben erforderlich ist (§ 13 Abs. 1 SächsDSG). Die Nutzungsbefugnis ist von weiteren Datenverarbeitungsphasen zu trennen und aus ihr folgt keine Übermittlungsbefugnis. Vor einer Übermittlung personenbezogener Daten ist gesondert zu prüfen, ob diese zur Erfüllung der Aufgaben der Stelle erforderlich ist. Eine Verfahrensweise im Umgang mit Anfragen oder Beschwerden, die - ohne eine Prüfung auf Erforderlichkeit - grundsätzlich die Datenübermittlung an andere (öffentliche oder nicht-öffentliche) Stellen vorsieht, ist jedenfalls datenschutzrechtlich unzulässig.

Eine Weiterleitung und Übermittlung des Beschwerdeschreibens des Vereins an die Firma verletzte nach meiner Überzeugung die Datenschutzrechte der Unterzeichner des Schreibens. Auch die Überlegung, die Vertreter des Vereins seien allgemein bekannt und auf der Internetpräsentation des Vereins veröffentlicht, geht nicht weit genug. Durch die Beschwerdeschreiben werden die ansonsten evtl. allgemein zugänglichen Informationen der Vereinsvertreter in neue Bezüge und Zusammenhänge gestellt.

Auch ist es unerheblich, ob das übermittelte Schreiben von einem Mitglied des Vereins als natürliche Person und Grundrechtsträger stammt oder durch ein Mitglied des Vorstands selbst. Zwar können juristische Personen das Datenschutzrecht für sich nicht in Anspruch nehmen. Einzelne Mitglieder - so auch die rechtlichen Vertreter - der juristischen Person sind jedoch als natürliche Person geschützt, wenn sich die Angaben über die Personengemeinschaft auch auf sie beziehen, das heißt auf sie „durchschlagen“ (Gola/Schomerus, BDSG, 10. Aufl., § 3 Rdnr. 11a). Enthält also z. B. eine Datei Angaben über juristische und natürliche Personen, so empfiehlt es sich, diese so zu behandeln, als unterlägen diese insgesamt den datenschutzrechtlichen Bestimmungen (Weichert in Däubler/Klebe/Wedde/Weichert, BDSG, 2. Aufl., § 3 Rdnr. 13). Im Übri-

gen ist auch im Datenschutzrecht (§ 18 SächsDSG) wie im allgemeinen Verwaltungsrecht ein redlicher Hinweisgeber durch die öffentliche Stelle vor der Preisgabe seiner Daten zu schützen. Soweit eine Übermittlung von Bestandteilen des Schreibens nach Auffassung des Sächsischen Oberbergamts für die Abgabe einer substantiellen Stellungnahme durch die Firma unerlässlich gewesen war, hätte eine Unkenntlichmachung der Angaben zum Einsender und Hinweisgeber erfolgen können.

Ich habe das Sächsische Oberbergamt auf die nach meiner Überzeugung nicht erforderliche und damit unzulässige Datenübermittlung und einen Verstoß gegen § 13 Abs. 1 SächsDSG hingewiesen. Die Behörde sicherte mir zu, meine datenschutzrechtlichen Hinweise künftig zu beachten und erarbeitete auf deren Grundlage eine spezielle Dienstanweisung zum Datenschutz bei Bürgeranfragen an Behörden.

In einem etwas anders zu beurteilenden Fall wandten sich Bürger mit Widersprüchen gegen einen Zulassungsbescheid an das Sächsische Oberbergamt. Gegenstand war der vorzeitige Beginn gemäß § 57 Abs. 1 BBergG für ein Vorhaben eines Unternehmens. Anschließend beschwerten sich die Betroffenen bei mir darüber, dass das Sächsische Oberbergamt die jeweiligen Widersprüche an den durch den Bescheid begünstigten Unternehmer nach § 13 Abs. 2 VwVfG (als Beteiligten) in Form einer vollständigen Textkopie übermittelt hatte.

Rechtsgrundlage für die Datenübermittlung waren die Regelungen des Vorverfahrens gemäß §§ 68, 71 VwGO, §§ 28, 29 VwVfG. Nach § 28 Abs. 1 VwVfG ist vor Erlass eines in seine Rechte eingreifenden Verwaltungsakts den Beteiligten Gelegenheit zu geben, sich zu den für die Entscheidung erheblichen Tatsachen zu äußern. Dabei ist es in der Regel - auch vor dem Hintergrund einer möglichen Akteneinsichtnahme nach § 29 VwVfG - geboten, neben den vorgetragenen Argumenten auch den Namen und die Anschrift des Beteiligten in einem Drittwiderspruch an den Betroffenen zu übermitteln. Insoweit sind Datenübermittlungen also zulässig. Allerdings haben auch die Bürger als Beteiligte nach § 30 VwVfG Anspruch auf ausschließlich befugte Offenbarung ihrer zum persönlichen Lebensbereich gehörenden Geheimnisse sowie der Betriebs- und Geschäftsgeheimnisse durch die Behörde. § 30 VwVfG realisiert insofern den vom BVerfG aufgestellten Anspruch des Bürgers auf informationelle Selbstbestimmung im öffentlichen Recht (Stelkens/Bonk/Sachs, VwVfG, § 30 Rdnr. 2) und soll der Festigung des Vertrauens zwischen Bürger und Verwaltung dienen. Daraus ergibt sich das Erfordernis der Prüfung auf geheim zu haltende Inhalte in Schreiben der Beteiligten in dem Verfahren und gegebenenfalls einer Interessenabwägung durch die Behörde vor einer möglichen Offenbarung.

Das Sächsische Oberbergamt bestätigte mir in seiner Stellungnahme, die genannten Rechtsvorschriften und Geheimhaltungsbestimmungen beachtet zu haben.

# 13 Wissenschaft und Kunst

## 13.1 Prüfungsunfähigkeitsnachweise

Gleich mehrfach erreichten mich Eingaben Studierender zu Formularen ihrer Prüfungsbehörden, die Betroffene von ihrem Arzt ausfüllen lassen sollten, wenn sie aus gesundheitlichen Gründen nicht an einer Prüfung teilnehmen, sie abbrechen oder nach Beendigung von ihr zurücktreten wollen. Die Betroffenen wollten von mir wissen, inwieweit dies zulässig ist.

Das Verlangen einer Prüfungsbehörde zum Nachweis der Prüfungsunfähigkeit ein ärztliches Attest vorzulegen, stellt einen Eingriff in das Recht des Studierenden dar, grundsätzlich selbst über die Verwendung seiner Daten zu entscheiden. Ein solcher Eingriff bedarf einer gesetzlichen Grundlage, die sich in der Regel aber aus den jeweils einschlägigen Prüfungsordnungen ergibt, die als Satzungen auf Grundlage der Bestimmungen des Sächsischen Hochschulgesetzes erlassen wurden.

Die Prüfungsunfähigkeit ist allerdings ein Rechtsbegriff, dessen Voraussetzungen vom Prüfungsausschuss, nicht vom Arzt festzustellen sind (vgl. BVerwG, DVBl. 1996, S. 1379 f.). Demgemäß ist der Prüfungsausschuss befugt, solche Daten zum Leistungsvermögen des Prüflings zu erheben, die ihn als Prüfungsbehörde befähigen, in eigener Verantwortung eine Entscheidung darüber zu treffen, ob gesundheitliche Gründe es rechtfertigen, nicht an der Prüfung teilzunehmen, sie abzubrechen oder nach Beendigung von ihr zurückzutreten. Im Attest müssen somit die aus ärztlicher Sicht bestehenden krankheitsbedingten und zugleich prüfungsrelevanten körperlichen, geistigen und/oder seelischen Beeinträchtigungen und deren Auswirkungen auf das Leistungsvermögen des Prüflings konkret und nachvollziehbar beschrieben werden. Es ist jedoch nicht erforderlich, neben den Befunden bzw. Krankheitssymptomen und den sich aus diesen ergebenden Beeinträchtigungen auch die ärztliche Diagnose als solche zu erheben, also Arzt oder Prüfling eine verpflichtende Preisgabe der Krankheitsangabe abzuverlangen. Da Formulare einzelner Prüfungsbehörden gleichwohl entsprechende Angaben vorsahen, bin ich mehrfach tätig geworden, auch dann, wenn das entsprechende Formularfeld ausdrücklich mit dem Hinweis „*optional*“ gekennzeichnet war, weil dies trotzdem zu Angaben verleitet, die eine Prüfungsbehörde nicht beanspruchen kann.

## 13.2 Übermittlung von Kontaktdaten Promovierender an den DAAD

Eine Hochschule, die teilweise vom DAAD geförderte Promotionsstudiengänge anbot, wurde von diesem um Mitteilung der Kontaktdaten der Promovierenden gebeten. Die Promovierenden sollten - auf freiwilliger Basis - um eine Teilnahme an einem sogenannten Promovierendenpanel, d. h. an einer Evaluierung der geförderten Promo-

tionsstudiengänge, ersucht werden. Eine Verpflichtung der Hochschule zur Teilnahme war nicht ersichtlich.

Ich bin daher zu folgendem Ergebnis gelangt:

Eine Verpflichtung der Hochschule zur Übermittlung der Promovierendendaten besteht nicht. Insbesondere kann nicht angenommen werden, dass die Datenübermittlung zur Erfüllung der Aufgaben der Hochschule erforderlich ist. Eine Datenübermittlung könnte daher allenfalls mit Einwilligung der Studierenden erfolgen.

Unberührt hiervon bleibt die Möglichkeit der Studierenden, an der Evaluierung teilzunehmen. Soweit die Hochschule dies zu unterstützen beabsichtigt, kann sie dies zur Information der Promovierenden hierüber tun. So könnten beispielsweise entsprechende Fragebögen des DAAD durch die Hochschule weitergeleitet werden.

Ob dem DAAD eine Befugnis zur Erhebung der Daten zusteht, blieb ungeprüft, da dessen Datenschutzkontrolle nicht in meinen Zuständigkeitsbereich fällt.

## 13.3 Übermittlung von Studentendaten an die Polizei

Der Datenschutzbeauftragte einer sächsischen Hochschule fragte an, ob er Daten im Rahmen polizeilicher Ermittlungen übermitteln dürfe. Ich habe in diesem Zusammenhang erneut (wie auch in 15/13.5 - hier noch zum Sächsischen Hochschulgesetz) darauf hingewiesen, dass die Bestimmung des § 14 SächsHSFG in ihrem Anwendungsbereich äußerst unklar ist, woraus nach wie vor eine erhebliche Rechtsunsicherheit resultiert. Eine gesetzgeberische Klarstellung wäre daher zu begrüßen.

Unabhängig davon habe ich der Hochschule mitgeteilt, dass sich aus meiner Sicht jedenfalls folgende Auffassung vertreten ließe:

Datenübermittlungen sind grundsätzlich sowohl zum Zwecke der Erfüllung von Aufgaben der übermittelnden Stelle als auch zur Aufgabenerfüllung des Empfängers zulässig. Insoweit könnte davon ausgegangen werden, dass § 14 SächsHSFG nur insoweit eine abschließende Regelung trifft, als die eigenen Übermittlungszwecke der Hochschule betroffen sind.

Für den Fall, dass die Übermittlung zum Zwecke der Aufgabenerfüllung des Empfängers diente, könnte dann auf die insoweit maßgeblichen Vorschriften, im vorliegenden Fall das Sächsische Datenschutzgesetz, zurückgegriffen werden. Für den zur Prüfung stehenden Fall ließe sich dann eine Übermittlungsbefugnis gemäß § 14 Abs. 1 i. V. m. § 13 Abs. 2 Nr. 4 SächsDSG bejahen.

## 13.4 Aktenführung im Amt für Ausbildungsförderung

Im Zuge einer anderweitig veranlassten Kontrolle eines Amts für Ausbildungsförderung wurde ich darauf aufmerksam, dass die Behörde aus Gründen der Papierersparnis nicht benötigte Schriftstücke mit personenbezogenen Daten, die eine freie Rückseite hatten, als Druckerpapier nutzte, anstatt diese datenschutzgerecht zu vernichten. Dies hatte zur Folge, dass sich in mindestens 226 Förderakten Dokumente befanden, deren Rückseiten vorgangsfremde personenbezogene Daten Dritter enthielten. Ich habe jedoch (noch) von einer Beanstandung abgesehen, weil die Behörde umgehend Maßnahmen ergriff, den Missstand zu beseitigen und Anweisungen erließ, die künftigen Verstößen vorbeugen sollen. Die Behörde verpflichtete sich mir gegenüber, in allen 226 vom Verstoß betroffenen Förderakten sowie in allen weiteren Akten, bei denen eine datenschutzwidrige Veraktung vorgangsfremder personenbezogener Daten festgestellt wird, eine Trennung der Daten nach folgendem Verfahren vorzunehmen (§ 13 Abs. 5 Satz 1 SächsDSG):

1. Von dem Datenschutzverstoß betroffene Seiten werden den Förderakten entnommen und durch eine als Duplikat gekennzeichnete und vom Sachbearbeiter hinsichtlich der Authentizität der Vorderseite beglaubigte Kopie ersetzt, deren Rückseite frei bleibt, also keine vorgangsfremden personenbezogenen Daten Dritter mehr enthält.

2. Die entnommenen Originale werden in eine neu anzulegende Sammlung von Austauschseiten überführt, zu der ein Inhaltsverzeichnis geführt wird, das es erlaubt, die entnommenen Seiten jeweils anhand des Aktenzeichens der Ursprungsakte, dem Namen des Geförderten sowie des vom Datenschutzverstoß betroffenen Dritten jederzeit aufzufinden. Die Nutzung der gesonderten Sammlung von Austauschseiten ist auf berechtigte Zwecke der Revision des Verarbeitungshandelns beschränkt. Wird eine Förderakte vernichtet, sind zeitgleich auch die aus ihr entnommenen Originale, die sich in der Sammlung von Austauschseiten befinden, zu vernichten.

3. Jeder Förderakte, der Originale entnommen wurden, wird ein vom Sachbearbeiter signiertes Vorblatt mit einer Erläuterung zu den Gründen der Veränderung der Akte vorgeheftet, auf dem alle wegen des Datenschutzverstoßes ausgetauschten Seiten einzeln mit ihrer Seitenzahl, der Angabe des Zeitpunkts ihres Austauschs sowie dem genauen Ort ihres Verbleibs, also Aktenzeichen und Seitenzahl der Sammlung der Austauschseiten, vermerkt sind.

4. Akteneinsicht in Förderakten oder deren Übersendung (auch in Kopie) werden nur noch gewährt bzw. vorgenommen, wenn zuvor geprüft wurde, ob die Akte vom Datenschutzverstoß betroffen ist; ist dies der Fall ist die Akte zunächst unter Trennung der Daten entsprechend der Ziffern 1 bis 3 zu verändern.

5. Ergibt sich aus einer vom Datenschutzverstoß betroffenen Akte, dass - etwa im Wege der Akteneinsicht - personenbezogene Daten unbefugt Dritten übermittelt wurden, die weder Behörde noch Organ der Rechtspflege sind, ist der vom Datenschutzverstoß Betroffene von der Verletzung seines Rechts auf informationelle Selbstbestimmung zu benachrichtigen.

## 13.5 Nutzung von Meldedaten für Forschungszwecke u. a.

Bei den mir im Berichtszeitraum zur Prüfung vorgelegten Forschungsvorhaben (insbesondere aus dem Universitätsbereich) traten meist gleichgelagerte Fragestellungen auf:

1. So ist oftmals der Zugang zu den Melderegistern für die Zusammenstellung der Probandengruppe ein Problempunkt. Denn das Sächsische Meldegesetz enthält keine ausdrücklich normierte Datenverarbeitungsregelung zu Forschungszwecken.

   Schon in früheren Forschungsvorhaben habe ich die Auffassung vertreten, dass § 29 Abs. 1 SächsMG auch dann erfüllt ist, wenn die Aufgabe(n) der Stelle, an die die Meldedaten übermittelt werden sollen, im Wesentlichen (und nicht nur als Nebenaufgabe) Forschung betrifft, die Datenübermittlung aus den Melderegistern dann also als zur Aufgabenerfüllung der Forschungsstelle erforderlich angesehen werden kann (Forschung=Aufgabe).

   Dies erkenne ich zum Beispiel für die Universitätsklinika an, zu deren Aufgabe ja gerade auch wesentlich die Durchführung von Forschungsvorhaben zählt, wenn die Übermittlung der Meldedaten - unter Zugrundelegung der von der Forschungseinrichtung jeweils konkret angeführten Gründe - für die (bevölkerungsbezogene) Ermittlung der Probandengruppe und mithin für die Durchführung der Studie erforderlich ist.

   Aufgrund Art. 5 Abs. 3 GG besteht dabei ein weiter Beurteilungsspielraum der Forschungseinrichtung, welche Daten die Einrichtung zur Durchführung der Studie benötigt und in welcher Form gerade auch eine Probandenstichprobe (z. B. zur Herstellung einer bevölkerungsbezogenen Vergleichsgruppe) erreicht werden soll.

2. Weiterhin wollen die Forschungseinrichtungen oftmals eine Rückmeldung ihrer Probanden auch im Falle der Nichtteilnahme.

   Bei einer auf Freiwilligkeit basierenden Befragung muss ich mich nicht dazu äußern, wenn ich nicht teilnehmen will. Die Einholung einer Erklärung zu den Gründen der Nichtteilnahme, an deren Kenntnis für Forschungseinrichtungen oftmals ein Interesse besteht, ist datenschutzrechtlich unbedenklich, wenn die Rückmeldung zu den Grün-

den einer Nichtteilnahme anonym, also ohne Namensnennung und ohne Angaben von Adressdaten, erfolgt.

3. Schließlich muss ich die Forschung betreibenden Stellen immer wieder darauf hinweisen, dass ich keine Genehmigung oder Zustimmung bezüglich ihres Forschungsvorhabens aussprechen kann. Das Sächsische Datenschutzgesetz sieht eine solche nicht vor und macht eine solche insbesondere auch nicht zur Voraussetzung für die Durchführung des Forschungsvorhabens. Ich kann daher lediglich eine Stellungnahme bzw. Einschätzung abgeben, ob ich das betreffende Forschungsvorhaben datenschutzrechtlich für bedenklich oder unbedenklich halte. Insoweit kann allenfalls in das Informationsschreiben an potentielle Teilnehmer - um diese letztlich zu einer Teilnahme zu animieren - aufgenommen werden, dass das Vorhaben dem Sächsischen Datenschutzbeauftragten zur Stellungnahme vorgelegt worden ist und dieser das betreffende Forschungsvorhaben datenschutzrechtlich für unbedenklich hält.

# 14 Technischer und organisatorischer Datenschutz

## 14.1 Besucherstatistiken bei öffentlichen Stellen

Ein immer wiederkehrendes Thema ist die sogenannte Reichweitenanalyse von Webseiten, auch bekannt als Besuchertracking oder -statistik. Dabei werden unter Zuhilfenahme eines Dienstes die Aktivitäten der Besucher einer Webseite gemessen und visuell aufbereitet. Zusätzlich können mit den beim Aufruf einer Webseite durch den aufrufenden Rechner übertragenen Angaben (IP-Adresse, http-Header) Analysen über die Herkunft (sogenannte Geolokation über die IP-Adresse) und die technische Ausstattung des Besuchers analysiert werden. Die Betreiber einer Webseite versprechen sich davon Hinweise auf die Akzeptanz des Angebots. Dass eine solche Beobachtung der Nutzer auf Vorbehalte stößt, ist verständlich. In der analogen Welt wäre es auch befremdlich, wenn ein Mitarbeiter im Kaufhaus oder einer Bibliothek einem auf Schritt und Tritt folgte und dabei ständig Notizen machte. Problematischer wird es, wenn eine Besucherstatistik durch einen Drittanbieter erstellt wird, der vielleicht kostenlos ist, bei dem es aber unklar bleibt, ob er die erlangten Daten nicht auch für weitere/eigene Zwecke nutzt. Aus diesen Gründen sind die Anforderungen an Besucherstatistiken in § 15 Abs. 3 TMG geregelt und wurden durch einen Beschluss des Düsseldorfer Kreises im Jahr 2009 ergänzend beschrieben. Der Düsseldorfer Kreis hat den Beschluss zwar mit Blick auf die nicht-öffentlichen Stellen gefasst, für öffentliche Stellen gilt jedoch das Gleiche. Vereinfacht gesagt, muss eine Besucherstatistik transparent sein, auf die Verarbeitung und Speicherung vollständiger IP-Adressen verzichten und die Möglichkeit zum Widerspruch gegen ein solches Tracking bieten.

Auch in diesem Berichtszeitraum habe ich zahlreiche Kommunen auf datenschutzrechtliche Mängel bei der Umsetzung einer Besucherstatistik auf deren Webseiten aufmerksam machen müssen. Da den Hinweisen stets unverzüglich nachgekommen wurde, musste ich keine Beanstandungen aussprechen. Die Mängel reichten von komplett verstecktem Tracking über fehlende Widerspruchsmöglichkeiten oder fehlende Auftragsdatenverarbeitungsverträge mit den extern eingesetzten Dienstleistern. Oftmals kamen die Hinweise von Besuchern der kommunalen Webseiten. Es ist also durchaus so, dass die Bürger im Freistaat sehr genau darauf achten, wie ernst die öffentlichen Einrichtungen die informationelle Selbstbestimmung der Bürger nehmen.

Am Rande zum Thema: Für Google Analytics, den weltweit wohl am weitesten verbreiteten Trackingdienst, gilt, dass aus meiner Sicht die mit dem SMI und den beiden kommunalen Spitzenverbänden erzielte Übereinkunft, auf Webseiten öffentlicher Stellen den Einsatz von Google Analytics ausdrücklich nicht zu empfehlen, nach wie vor gültig ist. Zwar hat sich die Firma Google in den vergangenen Jahren bemüht, den

Dienst datenschutzfreundlicher zu gestalten, beispielsweise durch spezielle Einstellungen für Webseitenbetreiber oder eine eigene Widerspruchslösung. Dennoch gibt es weiterhin Kritik an der Wirksamkeit der Widerspruchslösung und deren fehlender Unterstützung für mobile Endgeräte. Aus Sicht eines Internetnutzers geht von Seiten, welche Google Analytics einsetzen, aufgrund der neuen Datenschutzerklärung von Google über die Zusammenführung der Daten der verschiedenen Dienste auch eine erhöhte Gefahr für das informationelle Selbstbestimmungsrecht aus. Letztlich entscheidend für einen Verzicht auf den Einsatz von Google Analytics ist jedoch, dass es datenschutzfreundlichere Lösungen gibt, die entweder in Eigenregie betrieben werden können oder speziell auf die rechtliche Lage in Deutschland zugeschnitten sind. Geeignete Produkte lassen sich im Internet auch mit Tracking-freien Suchmaschinen finden.

## 14.2 Dialog-Plattform des Freistaates Sachsen

Ende des Jahres 2011 hat sich die SK mit der Bitte an mich gewandt, eine geplante Dialog-Plattform für eine Online-Kommunikation mit den Bürgern des Freistaates zu bewerten. Gerade vor dem Hintergrund unserer unterschiedlichen Auffassungen zur Zulässigkeit der Nutzung kommerzieller sozialer Netzwerke durch Behörden begrüße ich es ausdrücklich, wenn öffentliche Stellen die Kommunikation mit den Bürgern in eigener Verantwortung betreiben. Nur so kann nach meiner Auffassung die Verantwortung hinsichtlich der Datenverarbeitungsprozesse gewahrt und die gebotene Transparenz gegenüber dem Bürger sichergestellt werden.

Mit einer Dialog-Plattform einhergehen aber auch höhere Anforderungen an den Datenschutz. Im Gegensatz zu einer normalen Webseite, auf der keine oder nur wenige personenbezogene Daten vorgehalten werden, hat die Dialog-Plattform ein Anmeldesystem, speichert also personenbezogene Daten der Nutzer wie Name, E-Mail-Adresse und Zugangskennwort. Zusätzlich verarbeitet die Plattform Meinungsäußerungen der Nutzer zu politischen Themen; es werden also sensible Daten verarbeitet, welche für potenzielle Angreifer durchaus von Interesse sein könnten.

Neben anderen technischen Maßnahmen zur Verbesserung der Sicherheit, wie einen permanenten Monitoring-Prozess im Hinblick auf die Rechtmäßigkeit der Äußerungen auf der Dialog-Plattform, habe ich vor der Inbetriebnahme einen Penetrationstest gefordert. Mit einem solchen Test werden eine Webseite und die beteiligten Systeme systematisch und umfassend auf mögliche Schwachstellen und Angriffsvektoren überprüft. Im Anschluss an den Test können diese behoben werden. Die SK war mit diesem Vorgehen einverstanden und hat einen solchen Test durch die Informatikfakultät einer sächsischen Hochschule durchführen lassen. Die dabei festgestellten nicht gravierenden

Schwachstellen wurden bis zur Inbetriebnahme der Dialog-Plattform im März 2012 ausgeräumt.

## 14.3 Hackerangriff auf E-Mail-Konto einer Bürgermeisterin

In der Vorweihnachtszeit des Jahres 2011 hatte der Ehemann einer Beigeordneten einer sächsischen Kommune einen denkwürdigen Auftritt im Büro der Bürgermeisterin: Er verkündete recht lautstark im Beisein eines Pressevertreters, der sich zu jener Zeit im Büro der Bürgermeisterin aufhielt, dass ein bestimmtes Schreiben Konsequenzen nach sich ziehen würde. Dieses Schreiben hätte er in seinem Briefkasten als anonyme Post gefunden. Er hinterließ das Schreiben und verließ das Büro. Die verwunderte Bürgermeisterin sah sich das Schreiben genauer an, es handelte sich um einen Entwurf eines Anwaltsbüros in einer Personalsache, die fragliche Beigeordnete betreffend, für ein Schreiben an das fachaufsichtlich zuständige Landratsamt. Der Entwurf des Anwaltsbüros selbst hatte den unmittelbaren Verfügungsbereich der Bürgermeisterin jedoch nie verlassen und befand sich lediglich in ihrem persönlichen E-Mail-Postfach. Für das Auftauchen des Schreibens im Briefkasten der ersten Beigeordneten und ihres Mannes kam daher aus Sicht der Bürgermeisterin nur ein externer Hackerangriff auf ihr E-Mail-Postfach in Frage. Sie hat sich unmittelbar an meine Behörde gewandt. Ich habe ihr zur Strafanzeige gegen Unbekannt geraten und empfohlen, die für die Netzwerkinfrastruktur des kommunalen Netzes zuständigen Stellen über den Verdacht zu informieren. Wenige Tage später meldete sich die Bürgermeisterin erneut. Die Auswertung der Zugriffsdaten auf ihr E-Mail-Postfach hätten ergeben, dass Zugriffe von einem bestimmbaren Rechner aus dem kommunalen Netz heraus erfolgt sind. Ich habe daraufhin veranlasst, dass der Netzbetreiber des kommunalen Netzes die in Frage kommenden Zugriffsdaten sperrt und damit eine standardisierte Löschung verhindert wird. Kurz darauf hat ein Mitarbeiter des kommunalen Netzes den Zugriff auf das E-Mail-Postfach der Bürgermeisterin zur Selbstanzeige gebracht.

Ich habe den Vorfall zum Anlass einer Kontrolle der Informationstechnik der Stadt und zur Erörterung mit den Verantwortlichen für die kommunale Netzinfrastruktur genommen. Es stellte sich heraus, dass derjenige, welcher den Zugriff auf das E-Mail-Postfach der Bürgermeisterin zur Selbstanzeige gebracht hatte, vorher bei der Stadt als Administrator tätig war und in dieser Funktion u. a. auch das Postfach eingerichtet hatte. Trotz der späteren Trennung von der Stadt waren seine Zugangsdaten und sein Passwort weiter nutzbar. Eine regelmäßige Änderungsroutine war ebenfalls nicht vorgesehen. Außerdem war der E-Mail-Server der Stadt, auf dem sich das Postfach der Bürgermeisterin befand, für einen Fernzugriff administriert. Das heißt, E-Mails konnten mit Wissen der Adresse des E-Mail-Servers und passender Kennung nicht nur innerhalb der Verwaltung der Stadt, sondern im gesamten kommunalen Datennetz abgerufen werden. Diese Funk-

tion wurde in der Stadt gar nicht benötigt und war auch nicht dokumentiert. Bei Betrachtung all dieser Umstände kann wohl kaum noch von einem Hackerangriff gesprochen werden, sondern eher von einer Verkettung von Umständen, bei denen neben der Energie eines Mitarbeiters, der seine Vertrauensposition ausnutzte, auch von einer erheblichen Mitverantwortung der Stadt ausgegangen werden muss. Der Vorfall zeigt vor allem eines: Informationstechnik ist längst mehr als ein bloßes Hilfsmittel der Verwaltung, durch ihre Nutzung entstehen erhebliche Gefahren für die Vertraulichkeit und Integrität der Daten einer Kommune. Nur durch ein aktives und vorausschauendes Informationssicherheitsmanagement lassen sich die bestehenden Risiken und Gefahren minimieren. Ich habe die Stadt im Anschluss an den Vorfall mehrfach beraten und zahlreiche Verbesserungsvorschläge für die Informationstechnik unterbreitet - und dringend die Bestellung eines Beauftragten für Informationssicherheit empfohlen.

## 14.4 Herbstakademie des Sächsischen Bildungsinstituts zu sozialen Netzen

Vom 22. bis 24. Oktober 2012 fand die Herbstakademie 2012 des Sächsischen Bildungsinstituts unter dem Titel „Medienbildung in der Schule - Soziale Netzwerke“ in Meißen statt. Meine Behörde war sowohl mit einem Workshop zu Datenschutzfragen als auch bei der abschließenden Podiumsdiskussion vertreten.

Die Herbstakademie markierte den Start einer andauernden Diskussion mit den Verantwortlichen im SMK und Lehrern vor Ort in den Schulen über den richtigen Umgang mit sozialen Netzwerken aus Sicht der Schule und des einzelnen Lehrers. Festzustellen war zunächst ein hohes Maß an Verunsicherung seitens der Lehrer. Die sozialen Netze sind Teil der Lebenswirklichkeit der Schüler und haben einen hohen Stellenwert in deren Lebensgestaltung. Das betrifft sicherlich nicht alle, aber wohl viele. Wie soll sich ein Lehrer verhalten, wenn Schüler mit ihm im Netzwerk Kontakt aufnehmen? Sind die sozialen Netzwerke gar als Teil der Unterrichtsgestaltung oder zur organisatorischen Abwicklung des Schulalltags geeignet?

Mit den Lehrern gemeinsam wurden zunächst die datenschutzrechtlichen Grundlagen für das Verhältnis zwischen Schule, Lehrer und Schüler erarbeitet und im Anschluss die Kritikpunkte an den großen sozialen Netzwerken erörtert. Aufgrund der Geschäftsmodelle und der zahlreichen ungeklärten rechtlichen Probleme halte ich die kommerziell ausgerichteten sozialen Netzwerke für jede Form der schulischen Arbeit nicht geeignet.

Unter dem Stichwort Medienkompetenz ist es aber selbstverständlich auch wichtig und richtig, dass die Lehrer Wissen über soziale Netzwerke haben und auch vermitteln

können. Meine Behörde hat dabei angeregt, eigene Projekte mit Bezug zum Internet zu starten, welche im Gegensatz zu kommerziell vermarkteten sozialen Netzwerken aber im Schutzraum der Schule stattfinden sollen. Dies könnten beispielsweise Wikis zu speziellen Themen sein oder eigene Webprojekte der Schüler. Bei der Diskussion mit den Lehrern wurde dabei auch immer wieder auf die Frage der personellen Ressourcen und der geeigneten technischen Ausstattung in den Schulen aufgeworfen. So verständlich dann der Griff nach kostenlosen Werkzeugen der sozialen Netzwerke auch erscheinen mag - fehlende eigene Ressourcen legitimieren deren Nutzung nicht.

## 14.5 Musterleitlinie für Informationssicherheit für sächsische Kommunen der SAKD

Im Jahr 2012 hat die SAKD eine Musterleitlinie für Informationssicherheit für sächsische Kommunen[4] veröffentlicht. Damit wurde ein erster Schritt für eine landesweite Integration der staatlichen und kommunalen Behörden in eine gemeinsame Informationssicherheitsstrategie erreicht. Wir erinnern uns: Seit dem Jahr 2008 gibt es auf staatlicher Seite eine ressortübergreifende Arbeitsgruppe Informationssicherheit bei der auch meine Behörde von Anfang an mitwirkt. Im Jahr 2011 wurde die Sicherheitsleitlinie des Landes als VwV Informationssicherheit[5] vom Kabinett verabschiedet. Die SAKD hat sich eng daran orientiert.

Bedauerlicherweise wurde darauf verzichtet, die auf Landesseite vorgeschriebenen Standards des BSI auch für die Kommunen verbindlich festzuschreiben. Es kann jeder einzelnen Kommune nur empfohlen werden, sich daran zu orientieren, da die BSI-Vorgaben in ihrem Umfang und ihrer Systematik eine praxisgerechte Einführung ermöglichen und andererseits ein Informationssicherheitsmanagement ohne zugrunde liegende Standards kaum zu nachvollziehbaren Ergebnissen führt. Insgesamt sind die gemeinsamen Bemühungen auf staatlicher und kommunaler Ebene ausdrücklich zu begrüßen. Durch den Ausbau des SVN in ein gemeinsam von staatlichen und kommunalen Behörden genutztes Netz ist in Fragen der Sicherheit eine gemeinsame Strategie zwingend erforderlich. Es bleibt auch festzuhalten, dass einige Kommunen bereits Vorreiter auf dem Gebiet der Informationssicherheit sind, einige sogar durch unabhängige Auditoren überprüft und zertifiziert wurden. Allerdings stelle ich bei Kontrollen in den Kommunen immer wieder technische wie organisatorische Mängel fest. Es gibt also Nachholbedarf. Dies gilt im Übrigen auch für die staatliche Seite, wo nach dem Bekenntnis zur Informationssicherheit in einigen Behörden nun auch tatsächlich die dafür notwendigen personellen, technischen und finanziellen Ressourcen bereitgestellt werden müssen. Mittelfristiges Ziel auf landes- wie auch kommunaler Seite muss es sein, für alle relevanten

[4] http://www.sakd.de/fileadmin/standardisierung/Musterleitlinie.doc.
[5] http://revosax.sachsen.de/Details.do?sid=9151014765 114.

Verfahren den jeweils zutreffenden Schutzbedarf festzulegen - nicht zuletzt, damit Bedrohungsszenarien und ihre möglichen Auswirkungen auf einer soliden Grundlage kompetent beurteilt werden können.

## 14.6 Sicherheitslücken bei der Online-Erhebung

Durch einen anonymen Hinweis wurde ich im Jahr 2011 auf einen Blog-Eintrag hingewiesen, bei dem ein Hacker Sicherheitslücken bei einer Online-Erhebung einer Behörde des Freistaates Sachsen festgestellt und dokumentiert hatte.

Eine öffentlich im Internet zugängliche Seite der Behörde enthielt eine Liste mit Session-IDs, mit denen man ein abgelegtes Cookie derart manipulieren konnte, dass damit ein mit höheren Rechten ausgestatteter Benutzer simuliert werden konnte. Dieser hatte dann Zugriff auf eine Datenbank, welche personenbezogene Daten (Name, Anschrift, E-Mail, Telefonnummer) enthielt. Die Datenbank war Teil eines Fachverfahrens, die Datensätze gehörten Ansprechpartnern von Einrichtungen und Unternehmen, für die die Behörde zuständig war. Ein derart möglicher Zugriff durch unberechtigte Dritte stellt eine schwerwiegende Sicherheitslücke dar.

Ich habe die betroffene Behörde umgehend zur Stellungnahme aufgefordert.

Der Hacker hatte die Behörde parallel zur Veröffentlichung der Sicherheitslücke auf seinem Blog per E-Mail informiert. Die Behörde hat unter Hinzuziehung des SID schnell reagiert und innerhalb weniger Stunden den von der Sicherheitslücke betroffenen Webserver deaktiviert. Somit war ein aktives Ausnutzen der Sicherheitslücke nicht mehr möglich. Die Behörde hat sich weiterhin umgehend bemüht, den Blogeintrag über den Anbieter der Blogging-Plattform zu löschen. Insoweit bin ich mit dem Vorgehen der Behörde einverstanden gewesen.

Der Vorfall wirft dennoch ein bezeichnendes Licht auf den Stand der Informationssicherheit im Freistaat Sachsen. Ohne den Hinweis des Hackers wäre ein Ausnutzen der Sicherheitslücke vermutlich noch heute möglich bzw. war es davor, ohne dass die Behörde dies auch nur bemerkt hätte. Der Vorfall zeigt auch, dass die Behörden im Freistaat Sachsen nicht vor Angriffen gefeit sind. Mit den verantwortlichen Stellen und im Rahmen der Arbeitsgruppe Informationssicherheit habe ich den Vorfall thematisiert und gefordert, bei Webangeboten, bei denen personenbezogene Daten verarbeitet werden, die Applikationssicherheit im Vorfeld durch unabhängige Dritte mit einem Penetrationstest zu überprüfen.

## 14.7 TK-Anlagen in Kommunen mit Flatrate-Tarif

Zahlreiche Kommunen haben in den vergangenen Jahren ihre Telefontarife auf einen als Flatrate bekannten Pauschaltarif umgestellt. Dabei fallen dann keine verbindungsspezifischen Kosten für Telefonate in das deutsche Festnetz mehr an, ebenso je nach Option - auch nicht mehr bei Verbindungen in das entsprechende Mobilfunknetz. Damit einhergehend sind auch die Regelungen zum Umgang mit privaten Telefonaten in den Dienstvereinbarungen über die Nutzung der kommunalen Telekommunikationsanlagen überarbeitet worden. Aus gutem Willen gegenüber den Beschäftigten heraus hatten einige kontrollierte Kommunen die Mitnutzung der Telekommunikationsanlage für private Zwecke in geringem Umfang erlaubt, gleichzeitig aber eine Regelung zum Zugriff auf Einzelverbindungsdaten zur Klärung von Sachverhalten geschaffen. Auf eine Abrechnung der Privatgespräche wurde verzichtet, auch weil es aufgrund der Tarifstruktur schwierig sein dürfte, einen realen Kostenschlüssel zu ermitteln. Diese Kombination aus privater Telefonie und dienstlicher Kontrolle ist jedoch nicht rechtskonform.

Durch die Gestattung der privaten Kommunikation wird die Kommune selbst zum Telekommunikationsanbieter und darf aufgrund des Fernmeldegeheimnisses damit Verbindungsdaten nur zu Abrechnungszwecken speichern. Gerade dies erfolgt aber nicht. Wird keine technische Trennung zwischen Dienst- und Privatgesprächen vorgenommen, ist somit die Speicherung der Verbindungsdaten generell nicht zulässig. Dabei spielt es keine Rolle, ob die Datenspeicherung von der Kommune selbst oder einem beauftragten Telekommunikationsanbieter vorgenommen wird.

Zur Lösung des Problems ergeben sich drei Ausgestaltungsmöglichkeiten:

*1. Verbot der privaten Telefonie mit der Möglichkeit der Nutzung von Calling-Cards*

Bei dieser Variante würde die private Nutzung der Telefonanlage untersagt mit der Ausnahme von sogenannten Calling-Cards. Diese funktionieren wie Pre-Paid-Karten und können von jedem beliebigen Festnetzanschluss genutzt werden. Der Freistaat Sachsen stellt im Rahmen des SVN/KDN-Vertrags ein eigenes Angebot für die Bediensteten unter www.sachsencall.de bereit. Dies kann auch von den Kommunen genutzt werden, denkbar ist aber jeder Anbieter solcher Dienste. Wenn Calling-Cards zugelassen werden, muss jedoch sichergestellt werden, dass keine Verbindungen zu 0800er-Nummern gespeichert werden, da die Calling-Card-Anbieter diese Nummern zur Abwicklung nutzen.

*2. Trennung der Handhabung von Festnetz- und Mobilfunkgesprächen*

Wenn Telefonate in das deutsche Festnetz keine Kosten verursachen, wäre es denkbar, eine Trennung der Speicherpraxis für Festnetz- und Mobilfunkgespräche einzuführen, beispielsweise durch die Einführung einer bestimmten Vorwahl für Privatgespräche. Festnetztelefonate dürften dann auch privat geführt werden, eine Speicherung von Verbindungsdaten fände nicht statt. Mobilfunkgespräche dürften dann ausschließlich dienstlich erfolgen, mit der Folge, dass Speicherung und Überprüfungen der Verbindungsdaten möglich wären.

*3. Totalverzicht auf Verbindungsdatenspeicherung*

Zulässig wäre es, wenn auf eine Speicherung von Verbindungsdaten vollumfänglich verzichtet würde. Eine Kontrolle der Nutzung der Telekommunikationsanlage wäre dann zulässig, wenn diese lediglich auf der Abrechnung der Kosten für den einzelnen Anschluss erfolgen würde. Eine Prüfung auf Basis der Verbindungsdaten wäre nicht statthaft, daher dürfen diese auch nicht gespeichert werden.

Auch ein generelles Verbot für Privattelefonate wäre rechtlich zulässig. In Zeiten der überwiegenden Ausstattung der Bevölkerung mit Mobiltelefonen wäre dies auch vertretbar. Letztendlich müssen die Kommunen und die bei der Erstellung einer Dienstvereinbarung beteiligten Personalvertretungen aber einen geeigneten Kompromiss entwickeln. Wichtig ist, dass Verstöße gegen das Fernmeldegeheimnis wirksam unterbunden werden. Dabei geht es auch um den Schutz der eigenen Mitarbeiter. Ein Verstoß gegen das Fernmeldegeheimnis nach § 88 TKG ist strafbar gemäß § 206 StGB und kann mit einer Freiheitsstrafe von bis zu fünf Jahren geahndet werden.

## 14.8 Überprüfung des Statistischen Landesamtes beim Zensus

Das StaLa war im Rahmen des Zensus 2011 für die technische Durchführung der Gebäude- und Wohnungszählung zuständig. Dabei wurden Angaben zu allen im Freistaat Sachsen befindlichen Gebäuden und Wohnungen beim Eigentümer oder der zuständigen Wohnungsverwaltung erfasst. Die Erhebung wurde durch ein Online-Verfahren unterstützt. Durch Bürgeranfragen und einen Artikel in der lokalen Presse wurde ich auf Unregelmäßigkeiten bei der Datenerfassung aufmerksam. Aufgrund eines Serverfehlers war die Online-Erhebung für die Gebäude- und Wohnungszählung für ca. zwei Stunden nicht erreichbar.

Ich habe den Vorfall untersucht und bekam von dem für die technische Umsetzung zuständigen SID umgehend einen entsprechenden Fehlerbericht vorgelegt. Demnach

gab es Kommunikationsprobleme in der Proxy-Kaskade zwischen dem beauftragten Dienstleister T-Systems und dem SID beim Transport innerhalb des SVN.

Mehrere Bürger, die eine Fehlermeldung nach dem Ausfüllen des Online-Fragebogens erhalten hatten, hatten sich an mich gewandt und waren sich nun unsicher, ob sie der gesetzlichen Meldepflicht nachgekommen seien oder nicht.

Ich habe die Log-Daten des Eingangs-Servers zum fraglichen Zeitpunkt überprüft und konnte feststellen, dass alle Datensätze, die vom Nutzer durch Absenden im Browser abgesetzt und anschließend mit einer Fehlermeldung quittiert wurden, dennoch unbeschadet beim StaLa eingegangen waren.

## 14.9 Verwendung von Video-Plattformen durch öffentliche Stellen

Mit einigem Unmut stelle ich seit geraumer Zeit eine unkritische Nutzung der Video-Plattform YouTube (welche sich seit längerem im Besitz der Firma Google befindet) durch öffentliche Stellen fest. Diese laden in Eigenproduktion erstellte Image-Filme oder dergleichen auf die Plattform und binden diese dann wiederum in ihre eigenen Webauftritte ein. Es entsteht dabei ein sogenanntes „Mash-Up“, ein Mix aus unterschiedlichen Webquellen. Technisch wird dabei beim Aufruf einer Seite mit einem eingebundenen YouTube-Video eine Verbindung zu den Servern von Google hergestellt und ein Cookie von YouTube mit einer Gültigkeitsdauer von einem halben Jahr auf dem Rechner platziert. Mit diesem ist der Rechner für YouTube und damit die Firma Google wiedererkennbar, wenn Google-Dienste in Anspruch genommen werden. Durch die Verbindung beim Aufruf erfährt YouTube die IP-Adresse des Rechners, außerdem wird der sogenannte http-Header übertragen. Dieser enthält u. a. Angaben zum verwendeten Betriebssystem und Browser, zur eingestellten Sprache, zur Bildschirmauflösung und den installierten PlugIns des Browsers - insgesamt also eine Menge an Informationen, welche zur Profilbildung genutzt werden können. Verschärfend kommt hinzu, dass die Firma Google seit dem 1. März 2012 trotz zahlreicher Proteste alle Dienste von Google unter eine Datenschutzerklärung zusammengefasst und verkündet hat, die gewonnenen Daten der verschiedenen Plattformen (Suche, Mail, Drive, Play, YouTube und viele weitere) künftig zusammenzuführen, um dem Nutzer die „Nutzung unserer Produkte noch unkomplizierter und intuitiver“ zu gestalten. Dass dabei Nutzungsprofile entstehen, die tief in die auch intimste Gedankenwelt eines Menschen hineingreifen, blieb zumindest seitens Google unerwähnt. Doch an dieser Stelle soll es, um zum Thema zurückzukehren, nicht um die Datenverarbeitung durch Google gehen. Es geht vielmehr um öffentliche Stellen, die YouTube-Videos auf ihren Webseiten einbinden. Den wenigsten Besuchern der Startseite der Staatsregierung www.sachsen.de dürfte klar sein, dass die Firma Google über ihren Besuch automatisch über die beschriebenen

Mechanismen informiert wird. Auf kommunaler Seite sind mir derartige Video-Einbindungen bislang nicht bekannt. Unverständlich an dieser Angelegenheit ist vor allem, dass keinerlei technische Erforderlichkeit für eine solche Praxis besteht. Dem Freistaat sollte es ohne größeren Aufwand möglich sein, die erstellten Videos mit einem eigenen Streaming-Dienst an den Zuschauer zu bringen. Löblicherweise tut dies die Polizei auf ihren Seiten unter www.polizei.sachsen.de mit einer eigenen Videothek und zeigt damit, dass das notwendige Know-how in Sachsen durchaus vorhanden ist. Ich habe mich in der Angelegenheit an die für den Internetauftritt des Freistaates zuständige Staatskanzlei gewandt.

## 14.10 Wirbel um eine Datensicherung

In einer sächsischen Kommune kam es nach einem hart geführten und polarisierenden Wahlkampf zu einem knappen Wechsel im Amt des Bürgermeisters. Aufgrund einer Wahlanfechtung konnte der gewählte Kandidat das Amt nicht antreten, so dass die Beigeordnete die Geschäfte der Stadt zu führen hatte. Die abgewählte Bürgermeisterin hat jede Kooperation mit der Beigeordneten verweigert und eine Übergabe der laufenden Geschäfte abgelehnt. Zudem hat sie sich - noch im Amt - ihren dienstlichen Laptop und das dienstliche Handy im sogenannten Insich-Geschäft an sich als Privatperson verkauft. In der täglichen Arbeit hat die Beigeordnete bemerkt, dass elektronische Unterlagen zum Teil schwer oder nicht auffindbar waren. Sie hat daraufhin den kompletten Datenbestand der Stadtverwaltung in einer außerordentlichen Datensicherung zusammengefasst und diesen verschlüsselt auf einer Festplatte speichern lassen. Die Festplatte wurde in einem Tresor der Stadtverwaltung in einem anderen Brandabschnitt als das Produktivsystem verbracht, dass Passwort für die Entschlüsselung war nur der beauftragten und vertraglich gebundenen IT-Firma zugänglich. Ziel der Sicherung war es, den Datenbestand zum Zeitpunkt des Amtsendes dauerhaft zu erhalten. Die eigentlichen Sicherungssysteme der Stadt haben die Daten lediglich in einem 14-Tage-Zeitfenster gesichert. Die Beigeordnete hat im Nachgang den Stadtrat in öffentlicher Sitzung über ihr Vorgehen informiert. Die Beigeordnete sah sich im Anschluss einer zum Teil anonym vorgetragenen Kritik ausgesetzt. In sozialen Netzen und in Foren wurde wild spekuliert und allerlei Theorien im Zusammenhang mit der Bürgermeisterwahl wurden laut. Generell wurde die Rechtmäßigkeit der Datensicherung in Frage gestellt und der Vorwurf der Manipulation durch die Beigeordnete stand im Raum. Die Beigeordnete hat sich daraufhin an meine Behörde gewandt und gebeten, ihr Vorgehen zu bewerten. In Anbetracht der von ihr geschilderten Umstände habe ich die Datensicherung nicht nur als rechtmäßig, sondern geradezu als zwingend notwendig erachtet. Die dabei eingehaltenen Standards entsprechen den Vorgaben des § 9 SächsDSG. Ein Vier-Augen-Prinzip wurde technisch erzwungen, indem der physische

Besitz der Festplatte in der Stadtverwaltung verbleibt und eine Verschlüsselung der Festplatte nur im Zusammenspiel mit dem IT-Servicepartner der Stadtverwaltung aufgehoben werden kann.

Die Stadtverwaltung hatte sich in diesem Zusammenhang auch nach einem angemessenen Sicherungszyklus für die Daten der Bürokommunikation der Stadt erkundigt. Ein Patentrezept dafür gibt es leider nicht. Die Datensicherung folgt den Schutzzielen der Informationssicherheit und muss sich daher daran bemessen. Es kommt also darauf an, welche konkreten Praxisanforderungen mit Hilfe einer Datensicherung und -wiederherstellung erreicht werden sollen. Dabei ist zwischen den verschiedenen Datenarten (Software-, System-, Anwendungs- und Protokolldaten) zu unterscheiden. Weiterhin ist von Relevanz, ob die Daten auch in Papierform vorliegen oder ausschließlich in elektronischer Form (z. B. in Fachverfahren). Aus datenschutzrechtlicher Sicht bedeutsam sind bei Protokolldaten evtl. festgelegte Löschfristen (z. B. Löschung von Internetnutzungsprotokollen in einer Dienstvereinbarung). Diese Fristen dürfen dann nicht durch eine Datensicherung umgangen bzw. ausgeweitet werden. Ausgehend von solchen Überlegungen empfiehlt sich die Anwendung des Maßnahmenkatalogs „M 6.34 Erhebung der Einflussfaktoren der Datensicherung“[6] aus den IT-Grundschutz-Katalogen des BSI. Aus der behördlichen Kontrollpraxis kann ich berichten, dass in Behörden die Bürokommunikationsdaten in vielen Fällen als Sieben-Tages-, Monats- und Jahressicherung vorgehalten wird und die Sicherung in aller Regel täglich wochentags während der Nachtstunden erfolgt.

Bezüglich des Insich-Geschäfts der ehemaligen Bürgermeisterin habe ich eine Prüfung seitens der Kommunalaufsicht empfohlen, um sicherzustellen, dass keine dienstlichen Daten mit dem Wechsel des Besitzes abhandengekommen sind.

## 14.11 Zugriff auf E-Mails bei erlaubter privater Nutzung

Als echter Dauerbrenner kann der Zugriff auf E-Mails durch den Arbeitgeber gewertet werden und auch in diesem Berichtszeitraum gibt es wieder interessante Praxisfälle.

Einer Petentin war von ihrem Arbeitgeber gekündigt worden. Sie hat sich dagegen gewehrt - ein Rechtsstreit war anhängig - und gegenüber meiner Behörde den Verdacht geäußert, dass der Arbeitgeber in ihrer Abwesenheit ihre E-Mails bearbeitet hatte. Der Fall war dahingehend heikel, dass der Arbeitgeber keine Regelung zur E-Mail-Nutzung erlassen hatte, der private Gebrauch der dienstlichen E-Mail wohl aber bewusst geduldet wurde und der betrieblichen Praxis entsprach. Die Petentin war vor der Kündigung längere Zeit krank und hatte in dieser Zeit Zugriff auf ihren E-Mail-Account über das

[6] https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/m/m06/m06034.html

Internet. Zeitgleich mit der Kündigung war der Account nicht mehr erreichbar. Die Petentin vermutete, dass der Arbeitgeber die E-Mails dabei auch ausgewertet haben könnte.

Bei einer Kontrolle vor Ort hat der Arbeitgeber eingeräumt, dass private E-Mail-Nutzung zugelassen wird. Weiterhin war festgelegt worden, dass bei Urlaub oder Krankheit eine Weiterleitung an den jeweiligen Vertreter zu erfolgen hat. Eine technische Trennung zwischen dienstlicher und privater E-Mail existierte nicht.

Im Rahmen der Kontrolle wurden die Zugriffe auf das Postfach der Petentin überprüft. Das E-Mail-System war so konfiguriert, das auch lesende Zugriffe auf Ordnerebene dokumentiert wurden. Dabei konnte neben regulären Zugriffen durch die Petentin selbst nur der sperrende Zugriff seitens des Administrators zum Zeitpunkt der Kündigung nachgewiesen werden. Ein Zugriff auf Nachrichteninhalte seitens des Administrators oder anderer ggf. berechtigter Personen war nicht nachweisbar. Die Sperrung erfolgte laut Aussage des Vertreters der kontrollierten Stelle aufgrund des anhängigen Rechtsstreits, da unklar war, ob eine Rückkehr ins Arbeitsverhältnis möglich ist. Der Petentin wurde nach der Kündigung schriftlich die Möglichkeit eingeräumt, ihren Account beim Arbeitgeber auf private E-Mails zu sichten und diese ggf. auszudrucken und/oder zu löschen.

Im Ergebnis der Kontrolle war also ein Zugriff des Arbeitgebers auf Nachrichteninhalte nicht nachweisbar, so dass dieser mit einem blauen Auge davon kam. Wäre ein Nachweis erkennbar gewesen, wäre daraus eventuell ein Fall für den Staatsanwalt geworden. Das Zulassen der privaten E-Mail-Nutzung und die festgelegten Vertretungsregeln stellen einen schweren datenschutzrechtlichen Mangel dar. Da keine physische und logische Trennung zwischen dienstlichen und privaten E-Mails erfolgt, ist mithin der gesamte Mailbestand als privat zu betrachten und entzieht sich damit weitgehend den Einflussmöglichkeiten des Arbeitgebers, welcher für die privaten E-Mails den neutralen Status eines Diensteanbieters, also wie der Mailprovider im Privatbereich, einnimmt. Weiterhin ist das Fernmeldegeheimnis zu wahren, welches sowohl den Empfänger als auch den Sender einer Nachricht schützt (§ 88 TKG). Eine Verletzung des Fernmeldegeheimnisses ist strafbewehrt (§ 206 StGB).

Der Arbeitgeber hat unmittelbar nach der Kontrolle die Regelungen für die E-Mail-Nutzung geändert und eine strikte Trennung zwischen dienstlich und privat durchgesetzt. Eine pauschale Weiterleitung von E-Mails wurde nicht mehr angewiesen, stattdessen sollten automatische Antworten mit Benennung eines Vertreters erfolgen. Ich habe daher auf eine Beanstandung verzichtet. Auf die von meiner Dienststelle entworfene und auf meiner Internetseite veröffentlichte Musterdienstvereinbarung zur E-Mail-

Nutzung sei an dieser Stelle erneut verwiesen. Mit dem Zulassen privater E-Mails auf dienstlichen Accounts begibt sich der Arbeitgeber, auch wenn es in guter Absicht erfolgt, in vorprogrammierte Schwierigkeiten ohne Not. Wer den Mitarbeitern diese Möglichkeit geben möchte, sollte es im Rahmen einer gestatteten privaten Internetnutzung tun, so dass die Mitarbeiter private Post über einen Webmail-Dienst im Browser abrufen können.

## 14.12 Vermeidung des gläsernen Kunden durch datenschutzgerechten Betrieb der neuen intelligenten Zähler (Smart Meter) für den Energieverbrauch in Häusern und Wohnungen

*Rechtliche Entwicklung*

Das Energiewirtschaftsgesetz wurde am 14. April 2011 novelliert. Es verpflichtet Messstellenbetreiber bei Neubau und größeren Renovierungen bereits seit dem Jahr 2010, soweit dies technisch und wirtschaftlich zumutbar ist, digitale Zähler (Smart Meter) einzubauen, welche den tatsächlichen Energieverbrauch und die Nutzungsdauer messen.

In § 21e Abs. 4 EnWG wurde auch geregelt, dass zur Datenerhebung, -verarbeitung, -speicherung, -prüfung, -übermittlung ausschließlich solche technischen Geräte eingesetzt werden dürfen, die den Anforderungen von Schutzprofilen entsprechen. Folglich dürfen nur noch Messsysteme verwendet werden, bei denen die Einhaltung der Anforderungen des Schutzprofils in einem Zertifizierungsverfahren festgestellt wurde.

Insbesondere wurden mit § 21g EnWG für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten aus dem Messsystem wichtige Datenschutzforderungen formuliert, insbesondere:

- der Grundsatz der Zweckbindung und Verhältnismäßigkeit,
- das Koppelungsverbot zwischen günstigen Tarifen und Offenlegung des Nutzerverhaltens,
- das Einwilligungserfordernis des Anschlussnutzers in die Datenverarbeitung sowie
- Kontroll- und Einwirkungsmöglichkeiten für das Fernmessen und Fernwirken.

Zur Konkretisierung dieser Datenschutzforderungen müssen lt. § 21g EnWG noch spezielle gesetzliche Regelungen zur Datenverarbeitung mit Smart Metern erlassen werden.

Die Gesetzesnovellierung hat zum Ziel, die Netzlast in Energienetzen zu optimieren, den Tageslastgang zu glätten und eine stabile Energieversorgung zu gewährleisten. Der

Endverbraucher soll einerseits dazu angehalten werden, Energie dann zu verbrauchen, wenn sie vermehrt im Netz zur Verfügung steht, und andererseits sollen Anreize für einen sparsamen Umgang mit Energie gesetzt werden.

Dafür ist es erforderlich, eine automatisierte Messwerterfassung über Smart Meter-Technologie einzuführen. Der Gesetzgeber verpflichtet im Gegenzug den Energielieferanten, dem Letztverbraucher (bezeichnet z. B. den Wohnungsinhaber als Energieverbraucher) lastabhängige Tarife und Zeitzonentarife anzubieten.

Tatsächlich ermöglichen diese digitalen intelligenten Zähler (Smart Meter) die genaue Erfassung des Energieverbrauchs des Letztverbrauchers (z. B. Energieverbrauch einer Wohnung). Die charakteristischen Lastprofilkurven der einzelnen Haushaltsgeräte (z. B. Kühlschrank, Waschmaschine, Geschirrspüler) können durch sekundengenaue Messungen abgebildet werden. Auch wenn die Messungen im Intervall von 15 Minuten erfolgen, kann anhand typischer Lastkurven erkannt werden, wann welche Geräte im Haushalt genutzt wurden. Über Smart Meter können detaillierte personenbezogene bzw. haushaltsbezogene Nutzungsprofile erstellt und dadurch die Lebensgewohnheiten der Bewohner offenbart werden. Alle Daten, die mit einem Smart Meter erhoben werden, sind somit auch personenbeziehbar.

Diese detaillierte Abbildung der Verbrauchsprofile kann einerseits durch die Möglichkeit der Verknüpfung mit anderen Daten zu tiefgreifenden Verletzungen der Persönlichkeitsrechte der Betroffenen führen. Zum anderen können Persönlichkeitsrechte auch durch die Offenbarung der Energieverbrauchsdaten über Fernmesssysteme beeinträchtigt werden, wenn der Letztverbraucher keine Transparenz oder Kontrolle über die Fernmessung hat.

Bereits mit der Entschließung „Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauchs“ der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben sich die Datenschutzbeauftragten grundsätzlich positioniert, dass es durch den Einsatz von Smart Metern, langfristige Aufzeichnungen oder die Verknüpfung von Verbrauchsprofilen nicht zu einer Beeinträchtigung des Rechts auf informationelle Selbstbestimmung oder der verfassungsrechtlich garantierten Unverletzlichkeit der Wohnung kommen darf.

*Schutzprofil und Technische Richtlinie des BSI*

Um einen einheitlichen technischen Sicherheitsstandard für den Einsatz von Smart Metern zu gewährleisten und um die Sicherheitseigenschaften der beim Letztverbraucher eingebauten Messgeräte bewerten zu können, wurde das BSI in Abstimmung mit dem Bundes- und den Landesdatenschutzbeauftragten mit der Erarbeitung eines Schutz-

profils (Protection Profile) und einer Technischen Richtlinie, die Funktionalitäts- und Interoperabilitätsanforderungen spezifiziert, für das zentrale Kommunikations-Gateway des Smart Meter[7] beauftragt. Im Schutzprofil sind alle erforderlichen Mindestsicherheitsanforderungen definiert. Es soll nicht nur für Stromzähler, sondern für alle Elektrizitäts- und Gaszähler angewendet werden können. Zukünftig müssen alle Smart Meter auf Basis dieses Schutzprofils geprüft werden. Das Zertifikat dient als verbindlicher Nachweis über die Erfüllung der Schutzziele. Jedoch bleiben Fragen der datenschutzrechtmäßigen Erhebung und Verarbeitung von Messdaten mit Smart Metern weitestgehend unbeantwortet.

*Orientierungshilfe Smart Meter*

Ergänzend zu den Vorgaben zur Informationssicherheit der Technischen Richtlinie enthält die Orientierungshilfe Smart Meter grundlegende Vorgaben zur datenschutzgerechten Konzeption der technischen Systeme für das Smart Metering. Es wird erläutert, wie die zentralen Forderungen des Datenschutzes nach *Zweckbindung, Datensparsamkeit und Erforderlichkeit* berücksichtigt werden können, um somit die IT-Sicherheit und den Datenschutz auf Seiten des Letztverbrauchers zu unterstützen.

Die Orientierungshilfe wurde durch eine Ad-hoc-Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder erarbeitet und am 27. Juni 2012 veröffentlicht. Sie enthält Beschreibungen und datenschutzrechtliche Bewertungen verschiedener Anwendungsfälle (Use Cases) für die einzelnen Datenverarbeitungsprozesse beim Smart Metering unter Berücksichtigung des jeweiligen *Schutzbedarfs* der Daten. Es werden alle Anwendungsfälle, angefangen von der Strommessung mittels Zählern über die Verarbeitung im Smart Meter, bis hin zur Nutzung der Daten durch die an der Energielieferung, Energieverteilung und Abrechnung beteiligten Stellen betrachtet.

„Die Datenschutzbeauftragten des Bundes und der Länder halten es für erforderlich, dass insbesondere folgende Punkte beachtet werden:

- Eine Verarbeitung der Smart Meter-Daten darf nur erfolgen, soweit es für die im Energiewirtschaftsgesetz aufgezählten Zwecke erforderlich ist.
- Die Ableseintervalle müssen so groß sein, dass aus dem Verbrauch keine Rückschlüsse auf das Verhalten der Nutzer gezogen werden können.

[7] Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems (Protection Profile for the Gateway of a Smart Metering System)
https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil_Gateway/schutzprofil.html;jsessionid=4C5E32C4CC183DCD8F18513ABF992BC9.2_cid286.

- Smart Meter-Daten sollen möglichst ohne Personenbezug übermittelt werden, die Verwendung von anonymisierten, pseudonymisierten oder aggregierten Daten ist zu prüfen.
- Es muss möglich sein, hoch aufgelöste Daten lokal beim Letztverbraucher abzurufen, ohne dass dieser auf eine externe Verarbeitung der Daten angewiesen ist.
- Die Daten sollen an möglichst wenige Stellen übermittelt werden.
- Es sind angemessene Löschfristen für die Daten festzulegen, um eine Vorratsdatenspeicherung zu vermeiden.
- Die Kommunikations- und Verarbeitungsschritte von Smart Metering müssen zu jeder Zeit für den Letztverbraucher sichtbar und nachweisbar sein.
- Zusätzlich bedarf es durchsetzbarer Ansprüche der Betroffenen auf Löschung, Berichtigung und Widerspruch.
- Die rechtliche und tatsächliche Herrschaft des Letztverbrauchers über das Smart Meter und die von diesem erhobenen und verarbeiteten Daten muss stets gewährleistet sein. Der Letztverbraucher muss Zugriffe auf das Smart Meter erkennen und dies im Zweifel unterbinden können. Auch darf es keine Pflicht geben, einen bestimmten Tarif zu wählen oder an der Zählerstandsgangmessung teilzunehmen.
- Smart Meter dürfen von außen nicht frei zugänglich sein. Es müssen eindeutige Profile für den berechtigten Zugang zu den Daten definiert werden. Anhaltspunkte hierfür bieten die Vorgaben im Schutzprofil und in der Technischen Richtlinie des BSI.
- Schon bei der Konzeption und Gestaltung der technischen Systeme muss die Gewährleistung des Datenschutzes berücksichtigt werden (Privacy by Design). Der Letztverbraucher muss mit Hilfe der Technik alle notwendigen Informationen, Optionen und Kontrollmöglichkeiten erhalten, die ihm die Kontrolle seines Energieverbrauchs und die Gestaltung seiner Privatsphäre ermöglichen. Insbesondere müssen rechtlich verbindliche Vorgaben für die Konzeption der Geräte, Verfahren und Infrastrukturen sowie für deren Einsatz geschaffen werden."[8]

*Fazit*

Die Energienutzung darf nicht mit datenschutzrechtlichen Beeinträchtigungen verbunden sein. Bei der Nutzung von Smart Metern muss sichergestellt werden, dass der Grundsatz der *Datenvermeidung, Zweckbindung*, die Prinzipien *Vertraulichkeit, Integrität, Verfügbarkeit und Transparenz* der Datenverarbeitung sowie die *Datensouveränität der Betroffenen* gewahrt bleiben.

*Verbrauchswerte sollen ausschließlich der Kontrolle des Betroffenen unterliegen.*

[8] Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. Juni 2012 (siehe Pkt. 17.1.12) zur Orientierungshilfe zum datenschutzgerechten Smart Metering.

Die Orientierungshilfe ist auf meiner Web-Seite unter der Rubrik Informationen, Arbeitshilfen veröffentlicht.

## 14.13 Orientierungshilfe Mandantenfähigkeit - Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur*

### 14.13.1 Einleitung**

Zur Zentralisierung und Konsolidierung verteilter Datenverarbeitung sowie aus Kostengründen greifen Daten verarbeitende Stellen zunehmend auf kooperative Betriebsmodelle zurück, die die gemeinsame Nutzung von Systemen und Programmen zur automatisierten Verarbeitung personenbezogener Daten vorsehen.

Die gemeinsame Nutzung einer solchen Infrastruktur unterliegt erhöhten Anforderungen an die Trennung der personenbezogenen Daten, um die aus der gemeinsamen Nutzung entstehenden Risiken für die informationelle Gewaltenteilung, die Zweckbindung und Vertraulichkeit hinreichend zu reduzieren.

In diesem Dokument werden eine *Begriffsdefinition*, die aus Datenschutzsicht *notwendigen Schritte zur Prüfung* einer ausreichenden Trennung von automatisierten Verfahren bei der Nutzung einer gemeinsamen IT-Infrastruktur (Mandantenfähigkeit) und notwendige *Ergänzungen bestehender Datenschutz- und Informationssicherheitsmanagementsysteme* (DSMS/ISMS) dargestellt.

### 14.13.2 Begriffsdefinition

Der Begriff „Mandant“ oder „Mandantenfähigkeit“ wird häufig verwendet, wenn es Unternehmen, Behörden oder Organisationen ermöglicht werden soll, Daten in einer Datenbank logisch zu trennen und zu verwalten. Mit Hilfe der Mandantenfähigkeit können z. B. Daten verschiedener Abteilungen einer Organisation / eines Unternehmens oder verschiedener Kunden eines IT-Services / Rechenzentrums getrennt vorgehalten werden.

Die Datenschutzgesetze der Länder und des Bundes fordern jedoch, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben worden sind, getrennt voneinander verarbeitet werden. Die getrennte Verarbeitung betrifft sowohl die Speicherung

* Die Orientierungshilfe vom 11. Oktober 2012 wurde erstellt von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und vom Arbeitskreis Technische und organisatorische Datenschutzfragen

** Die Nummerierung der Orientierungshilfe und entsprechende Verweise wurden dem Layout meines TBs angepasst. Das Original finden Sie auf meiner Internetseite: www.datenschutz.sachsen.de.

als auch die Verarbeitungsfunktionen wie etwa Datenbanktransaktionen oder Datensatzbuchungen.

Aus wirtschaftlichen oder praktikablen Gründen kann es aber sinnvoll sein, dass Ressourcen wie Hard- und Software, also IT-Infrastrukturen für verschiedene, voneinander zu trennende Datenbestände gemeinsam genutzt werden. In begründeten Fällen kann daher auch eine gemeinsame Speicherung mit mandantenbezogener Kennzeichnung der Daten zulässig sein. Voraussetzung hierfür ist, dass die Daten mandantenbezogen geführt und Verarbeitungsfunktionen, Zugriffsberechtigungen und Konfigurationseinstellungen je Mandant eigenständig festgelegt werden können. Die Datenverarbeitung muss dabei zwingend durch technische Maßnahmen getrennt voneinander erfolgen. Insbesondere gilt das auch dann, wenn für die jeweiligen Daten unterschiedliche Stellen verantwortlich sind oder es sich bei den personenbezogenen Daten um besondere Arten personenbezogener Daten handelt.

Der abgeschlossene Datenhaltungs- und Verarbeitungskontext einer im datenschutzrechtlichen Sinne verantwortlichen Stelle wird in diesem Papier nachfolgend als „*Mandant*“ bezeichnet, die getrennte Speicherung und Verarbeitung als „*Mandantentrennung*“. Ein Verfahren ist „*mandantenfähig*“, wenn es eine Mandantentrennung umsetzt.

Weitere Definitionen:

- *Gemeinsame IT-Infrastrukturen* umfassen alle informationstechnischen Ressourcen, die nicht physisch voneinander getrennt sind. Hierzu gehören beispielsweise Anwendungssysteme für mehrere Mandanten sowie gemeinsame Datenbank-Managementsysteme und Datenbanken, Speicher- und Managed Storage-Systeme sowie Backup-Systeme in konventionellen und virtualisierten Umgebungen.
- *Gemeinsame Verfahren* im Sinne dieser Orientierungshilfe sind automatisierte Verfahren, die mehreren Daten verarbeitenden Stellen die Verarbeitung personenbezogener Daten in oder aus einem Datenbestand ermöglichen. Gemeinsame Verfahren sind auch Verfahren, die die Übermittlung von Daten einer Stelle durch Abruf einer oder mehrerer anderer Stellen ermöglichen.
- Ein *Datenzugriff* ist die Ausführung einer (möglicherweise komplexen) Funktion eines Anwendungssystems, mit dem personenbezogene Daten genutzt oder anderweitig verarbeitet werden, und kann insbesondere die Ausführung einer Folge von Transaktionen bewirken.
- *Transaktionen* sind unteilbare, konsistente und gegeneinander isolierte logische Einheiten von Programmschritten eines Anwendungssystems.

### 14.13.3 Anwendungsbereich

Die folgenden Betrachtungen gelten für Verfahren zur Verarbeitung personenbezogener Daten, bei denen im Sinne der Datenschutzgesetze mehrere Daten verarbeitende Stellen eine Datenverarbeitung auf einer gemeinsamen IT-Infrastruktur ausführen, die Datenverarbeitung aus Rechtsgründen aber voneinander zu trennen ist.

### 14.13.4 Prüfung auf ausreichende Trennung der Verfahren

Zur Prüfung, ob eine ausreichende Trennung bei der gemeinsamen Nutzung einer IT-Infrastruktur gewährleistet wird und die Datenschutz- und Datensicherheitsanforderungen angemessen und wirksam umgesetzt werden, sollten die folgenden Prüfschritte durchlaufen werden.

**Prüfschritt 1: Rechtliche Grundlagen**

Die Prüfung, ob durch technische und organisatorische Maßnahmen eine ausreichende Trennung der Verfahren erreicht werden kann und durch welche, setzt eine vorlaufende rechtliche Betrachtung voraus. Dazu sind heranzuziehen:

- die für das jeweilige Fachverfahren anzuwendenden spezialgesetzlichen Bestimmungen,
- die datenschutzrechtlichen Grundsätze und
- die allgemeinen datenschutzrechtlichen Bestimmungen.

Im öffentlichen Bereich ist hierbei regelmäßig der vom Bundesverfassungsgericht im Volkszählungsurteil entwickelte datenschutzrechtliche Grundsatz der informationellen Gewaltenteilung (Abschottungsgebot), welcher staatliche Behörden dazu verpflichtet, personenbezogene Daten auch gegenüber anderen staatlichen Behörden abzuschotten.

Rechtsgründe für die Trennung von Verfahren sind

- gesetzliche Vorgaben,
- insbesondere unterschiedliche Zweckbestimmungen der Datenverarbeitung,
- die Tatsache, dass für verschiedene Teilsysteme unterschiedliche verantwortliche Stellen existieren. Dies gilt auch für so genannte gemeinsame Verfahren.

Die in den nachfolgenden Abschnitten dargestellten Anforderungen und Hinweise sind nicht anwendbar auf die ausschließliche Verarbeitung von Daten, die auf landes- oder spezialgesetzlicher Grundlage unter gemeinsamer rechtlicher Verantwortung stehen, oder auf den automatisierten Abruf über die Grenzen einer gemeinsamen IT-Infrastruktur hinweg.

Die Datenverarbeitung und die technischen und organisatorischen Sicherheits- und Datenschutzmaßnahmen müssen sich an diesen rechtlichen Vorgaben orientieren.

Zu betrachten und zu bewerten sind u. a.:

- Welche Daten verarbeitenden Stellen sollen die Infrastruktur gemeinsam nutzen?
- Welche Rechtsgrundlage und welche Zweckbestimmung oder Zweckbindung liegt der jeweiligen Verarbeitung zugrunde?
- Wo liegt die gesetzgeberische Regelungskompetenz (EU/Bund/Land) für die jeweilige Verarbeitung?
- Gibt es eine Ermächtigungsbefugnis, durch welche ggf. auch eine gemeinsame Verarbeitung (gemeinsame und verbundene automatisierte Dateien) zugelassen werden dürfte - und wurde von dieser Gebrauch gemacht? Oder ist diese ausgeschlossen?

Die konkrete Ausprägung der gemäß Trennungsgebot notwendigen Umsetzung einer getrennten Datenverarbeitung muss sich am Schutzbedarf der Daten orientieren.

*Beispiel: So können z. B. bei einem sehr hohen Schutzbedarf die aus der gemeinsamen Nutzung einer IT-Infrastruktur entstehenden Restrisiken nicht tragbar sein oder Rechtsnormen, die mit einer gemeinsamen Nutzung von IT-Infrastrukturen verbundenen Offenbarungen verbieten. In diesen Fällen ist dann eine physikalische Trennung bzw. ein Betrieb durch zwei unterschiedliche Stellen zwingend geboten, und die Nutzung eines von einer einzelnen Stelle betriebenen mandantenfähigen Verfahrens ist nicht zugelassen.*

**Prüfschritt 2: Ausgestaltung von Übermittlungen zwischen Mandanten**

Bei einer getrennten Verarbeitung auf gemeinsamer IT-Infrastruktur ist die Verarbeitung von Daten eines Mandanten in einem anderen Mandanten als Datenübermittlung auszugestalten. Die rechtlichen Grundlagen und Anforderungen an die Zulässigkeit der Übermittlung und die Form ihrer Durchführung sind vorab zu prüfen. So können abhängig vom anwendbaren Recht besondere Anforderungen an den automatisierten Abruf von Daten oder die Übernahme von Daten aus einem gemeinsam verantworteten Datenbestand bestehen.

Um die Übermittlungen auf das Zulässige zu beschränken, darf die Auswahl von Daten zur Übermittlung in jedem Fall nur an Identitätsdaten (Name, Vorname, etc.) und solche Attribute oder Eigenschaften der Betroffenen anknüpfen, für deren Übermittlung eine Rechtsgrundlage besteht. Zulässige Suchkriterien sind in der Regel vorher vertraglich

festzuhalten. Die Einschränkung auf diese Suchkriterien ist technisch durchzusetzen. Übermittelte Daten müssen dem empfangenden Mandanten zugeordnet werden, um die neu entstandene rechtliche Verantwortung zu kennzeichnen Der Fakt der Übermittlung ist zu protokollieren. Zur Isolierung der Übermittlung von Transaktionen innerhalb eines Mandanten darf auf übermittelte Daten erst nach Abschluss der Übermittlung und ihrer Protokollierung zugegriffen werden.

**Prüfschritt 3: Abgeschlossenheit der Transaktionen innerhalb eines Mandanten**

Zur Prüfung auf eine ausreichende Trennung der einzelnen Mandanten auf einer gemeinsamen Infrastruktur ist die „Abgeschlossenheit“ der Datenverarbeitung innerhalb eines Mandanten zu betrachten. Die Prüfung auf Abgeschlossenheit muss transaktionsbasiert erfolgen und nachweisen, dass die Datentrennung erhalten bleibt.

*Ein Mandant gilt als „abgeschlossen“, wenn jede Transaktion in einem Mandanten einen gültigen Datenbestand eines Mandanten in einen neuen gültigen Datenbestand überführt und hierbei von Daten anderer Mandanten nicht abhängt und auf diese Daten aufgrund technischer Maßnahmen weder lesend noch schreibend zugreift.*

Diese transaktionsorientierte Prüfung auf Abgeschlossenheit muss ganzheitlich für die für das Verfahren genutzten Komponenten zur Datenverarbeitung, Datenhaltung und Datenübertragung durchgeführt werden.

*Die Datenhaltung muss jedoch stets so organisiert werden, dass für jede Instanz eines personenbezogenen Datums die Zuordnung zu genau einem Mandanten erfolgt.* Eine ausreichende Trennung der Daten auf Ebene der Datenhaltung kann durch unterschiedliche Techniken erfolgen, z. B. durch eine abgeschlossene Einheit mit eigenen Datensätzen und einem vollständigen Satz von Tabellen. *Sämtliche Zugriffe auf personenbezogene Daten müssen die vergebenen Zugriffsberechtigungen (siehe Prüfschritt 4) sowie diese Zuordnung berücksichtigen und durchsetzen.*

Die Abgeschlossenheit muss insbesondere auch für die Risiken und Maßnahmen aus den Bereichen Datenschutz und Datensicherheit gelten. Die Abgeschlossenheit eines Mandanten bedingt zwangsweise auch eine sicherheitstechnische Isolation eines Mandanten. Bei ausreichender Trennung der Datenverarbeitung dürfen Datenschutzprobleme oder -vorfälle eines Mandanten nicht zu einer Gefährdung anderer Mandanten führen.

Wäre beispielsweise in einem System die Möglichkeit gegeben, mandantenübergreifende Zugriffe auf eigene Daten oder Daten eines anderen Mandanten zu initiieren, ohne dass die o. g. Voraussetzungen für eine zulässige Übermittlung vorliegen, oder

wird diese Möglichkeit nur durch organisatorische Maßnahmen ausgeschlossen, so läge keine Abgeschlossenheit vor und die Mandantenfähigkeit wäre nicht gegeben.

**Prüfschritt 4: Unabhängigkeit der Konfiguration**

*Eine ausreichende Mandantentrennung setzt voraus, dass die Zugriffsberechtigungen die Verarbeitungsfunktionen und die Konfigurationseinstellungen je Mandant eigenständig festgelegt werden.*

Die eigenständige Vergabe von Zugangsberechtigungen bedingt das Anlegen von mandantenspezifischen Benutzerkennungen, mit denen nur auf Daten ihres Mandanten zugegriffen werden kann.

Sind für die technischen Sicherheits- und Datenschutzmaßnahmen auf Basis einer Risikoanalyse oder aufgrund gesetzlicher Vorgaben mandantenspezifische Anforderungen ersichtlich, so müssen diese Anforderungen auf Mandantenebene umgesetzt und gemäß der Vorgaben der einzelnen Mandanten konfigurierbar sein.

Als Anforderungen sind hierfür mandantenspezifisch zumindest vorzusehen

- ein getrenntes, mandantenspezifisches System zur Berechtigungsvergabe,
- Konfigurationsmöglichkeiten für die Nutzungsprotokollierung sowie
- eine administrative Protokollierung.

Die Berechtigungsvergabe muss über ein auf Ebene des einzelnen Mandanten abgeschlossenes Berechtigungssystem erfolgen. Hierzu ist sicherzustellen, dass eine mandantenübergreifende Berechtigungsvergabe auf Anwendungsebene weder aus den einzelnen Mandanten heraus noch durch die mandantenübergreifenden Funktionen zur Verwaltung der einzelnen Mandanten möglich ist. So müssen beispielsweise für jeden Mandanten eigene Rollen definierbar sein.

Die Zuordnung zu jeweils einem Mandanten ist in der folgenden Abbildung verdeutlicht:

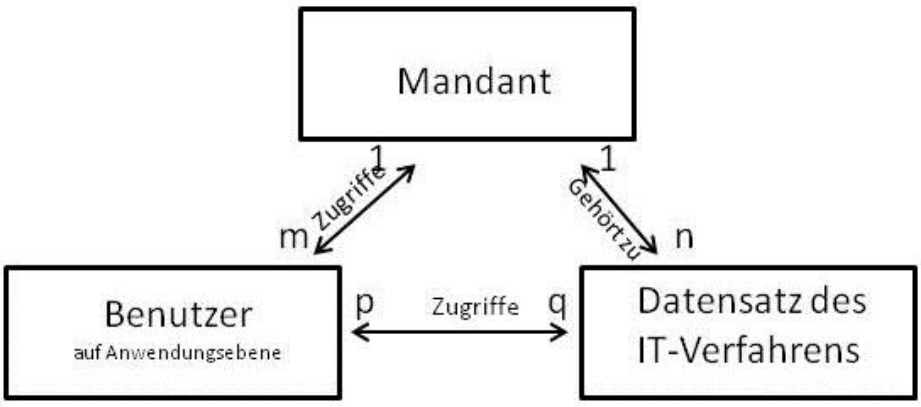


*Abbildung 1: Schematische Darstellung Berechtigungsvergabe*

Die mandantenspezifische Nutzungsprotokollierung darf sich nur auf Schritte zur Datenverarbeitung beziehen, die den jeweiligen Mandanten betreffen. Die Anforderungen der „Orientierungshilfe Protokollierung“[1] der Datenschutzbeauftragten des Bundes und der Länder sind hierfür mandantenspezifisch umzusetzen.

Die administrative Protokollierung muss sich auf die funktionalen Änderungen der Datenverarbeitung für den jeweiligen Mandanten beziehen. Genau wie die Speicherung dieser nutzerspezifischen Protokollierung müssen auch die administrativen Protokolleinträge für jeden Mandanten getrennt gespeichert werden.

Es muss gewährleistet werden, dass die jeweiligen Daten verarbeitenden Stellen zusätzlich zur mandantenspezifischen administrativen Protokollierung Zugang zu den Einträgen der Protokollierung erhalten, die im Rahmen der mandantenübergreifenden Verwaltung des Verfahrens durchgeführt wird. Zusätzlich zur mandantenspezifischen administrativen Protokollierung sind auch die Protokolleinträge zugänglich zu machen, die im Rahmen der mandantenübergreifenden Verwaltung des Verfahrens durchgeführt wurden.

**Prüfschritt 5: Beschränkung der mandantenübergreifenden Verwaltung der Datenverarbeitung**

*Mandantenübergreifende Funktionen zur Verwaltung der Mandanten und der gemeinsam genutzten Infrastruktur dürfen grundsätzlich keine Verarbeitung personenbezogener Daten eines Mandanten ermöglichen.*

Ausgenommen hiervon sind Funktionsträgerdaten der einzelnen Mandanten, die dazu dienen, das mandantenspezifische Berechtigungssystem erstmalig einzurichten. Auch das Anlegen und Löschen von Mandanten innerhalb des Systems gehört zu den Funk-

[1] http://www.lfd.m-v.de/dschutz/informat/protokol/oh-proto.pdf.

tionen einer mandantenübergreifenden Verwaltung. Die Organisation der Datenspeicherung muss gewährleisten, dass für diese Verwaltungsfunktionen auch die geltenden Bestimmungen für eine Auftragsdatenverarbeitung eingehalten werden können.

*Beispiel: So muss bspw. bei Beendigung des Auftragsdatenverhältnisses für einen Mandanten den Anforderungen nach Herausgabe und Löschung der verbliebenen Daten entsprochen werden können, ohne dass dies Auswirkungen auf die Verarbeitung anderer Mandanten hat.*

Die mandantenübergreifende Verwaltung muss revisionssicher protokolliert werden. Diese Protokolle müssen auch bei einer Prüfung einzelner Mandanten genutzt werden können.

Mandantenübergreifende Datenzugriffe sind nur in begründeten Ausnahmefällen zulässig und nur im für die jeweilige Aufgabenstellung erforderlichen Umfang, insbesondere für die mandantenübergreifende Verwaltung und zur Beseitigung von Notfallsituationen, wenn andere Maßnahmen mit geringeren Zugriffsrechten nicht ausreichend sind. Die Vergabe der hierfür vorgehaltenen Rollen ist sehr restriktiv zu handhaben und diese Rollen dürfen nicht Nutzern auf Anwendungsebene zugeordnet werden.

Mandantenübergreifende Funktionen und Einrichtungen müssen einem Management unterliegen. Dazu gehören

- die Definition eines differenzierten Administrationskonzepts,
- eine revisionssichere Protokollierung der administrativen Tätigkeiten und Festlegung eines Protokollierungskonzepts,
- die Definition eines mandantenspezifischen und mandantenübergreifenden Berichtswesens,
- die Definition von Revisionen über das Gesamtsystem und
- die Definition von Prozessen für das mandantenspezifische und mandantenübergreifende Change-Management.

### 14.13.5 Konzeption und Umsetzung des Datenschutzmanagements

#### Risikoanalyse

Die Datenschutzgesetze des Bundes und der Länder fordern, vor der Entscheidung über die Einführung oder die wesentliche Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden sollen, eine Risikoanalyse durchzuführen. Diese Risikoanalyse dient als Nachweis, dass die Gefahren für die Rechte der Betroffenen durch angemessene technische und organisatorische Sicherheits- und

Datenschutzmaßnahmen beherrscht werden können. Hierbei müssen auch die speziellen Risiken für die Vertraulichkeit, Integrität, Verfügbarkeit, Transparenz, Nicht-Verkettbarkeit und Intervenierbarkeit bei der getrennten Datenverarbeitung auf einer gemeinsamen IT-Infrastruktur betrachtet werden.

Die Risikoanalyse muss diese Risiken insbesondere mit dem Fokus auf den für die Betroffenen entstehenden Gefährdungen einer unzureichenden Datentrennung betrachten.

Wenn die IT-Grundschutz-Standards und die IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) angewendet werden, ist eine Risikoanalyse gemäß dem BSI-Standard 100-3 erforderlich, wenn ein hoher oder sehr hoher Schutzbedarf gegeben ist oder die genannten speziellen Risiken nicht von Bausteinen aus den IT-Grundschutz-Katalogen abgedeckt sind. Ergeben sich zusätzliche, noch nicht berücksichtigte Risiken, so sind diese nach dem genannten Standard zu bewerten und falls erforderlich mit weiteren Maßnahmen auf ein tragbares Maß zu vermindern.

**Nachweis ausreichender Sicherheits- und Datenschutzmaßnahmen und Dokumentationspflicht**

Der Nachweis einer wirksamen Umsetzung der auf Basis der Risikoanalyse erforderlichen Sicherheits- und Datenschutzmaßnahmen muss insbesondere die Maßnahmen umfassen, die eine Trennung der Daten auf Ebene der Datenhaltung, Datenverarbeitung und des Datentransports sicherstellen.

Als Nachweis einer ausreichenden Trennung einzelner Mandanten ist darzustellen, ob bzw. wie die Daten eines Mandanten zwischen der gemeinsamen Infrastruktur und der mandantenspezifischen Infrastruktur übertragen werden können. Im Rahmen dieses Nachweises ist zum einen darzustellen, mit welchen technischen und organisatorischen Mitteln die im Verfahren verarbeiteten personenbezogenen Daten getrennt werden. Dabei muss berücksichtigt werden, welche Daten verarbeitende Stellen die gemeinsame Infrastruktur nutzen. Zum anderen ist darzustellen, wie die für den Nachweis einer ordnungsgemäßen Datenverarbeitung notwendigen Daten, z. B. die Nutzungsprotokollierung, die administrative Protokollierung und die vergebenen Berechtigungen für einzelne Mandanten getrennt gespeichert werden und in eine andere Infrastruktur überführt werden können.

Eine getrennte Datenverarbeitung ist durch technische Maßnahmen sicherzustellen. Die jeweils damit verbundenen spezifischen Vor- und Nachteile sowie deren Risiken müssen dabei betrachtet werden. Die technische Umsetzung einer getrennten Datenverarbeitung mithilfe relationaler Datenbanken kann durch unterschiedliche Maßnahmen erfolgen:

- Alle Mandanten nutzen dieselben Tabellen in einer einzigen, gemeinsamen Datenbank eines Datenbanksystems. Jeder Datensatz wird um ein Attribut für den jeweils zutreffenden Mandanten ergänzt. Lediglich die Applikation realisiert die Trennung, indem sie dieses Attribut auswertet.
- Jeder Mandant arbeitet auf seinen eigenen Tabellen innerhalb derselben (d. h. einer einzigen) Datenbank. Die Tabellennamen enthalten jeweils ein mandantenspezifisches Präfix.
- Jeder Mandant erhält seine eigene Datenbank mit eigenen Tabellen.
- Arbeiten Mandanten auf eigenen Tabellen oder eigenen Datenbanken, lässt sich die Mandantentrennung in Abhängigkeit von den Konfigurationsmöglichkeiten des verwendeten Datenbankmanagementsystems durch eine Abbildung auf verschiedene physische Speicherstrukturen (wie Datendateien, dedizierte Speicherorte (Tablespaces), Raw Devices) innerhalb der gemeinsamen IT-Infrastruktur verstärken.
- Jeder Mandant wird durch einen eigenen Prozess des Datenbankmanagementsystems (DBMS) bedient. Jeder dieser DBMS-Prozesse legt die mandantenspezifischen Daten in separaten Datenbanken in derselben oder in unterschiedlichen physischen Strukturen ab.
- Jeder Mandant bekommt seine eigene virtuelle Maschine mit eigener virtueller Festplatte für das Datenbanksystem.

Der Nachweis sollte die Durchführung und Ergebnisse der Prüfschritte 1 bis 5 umfassen.

**Restrisikobetrachtung**

Risiken, die nicht oder nur zum Teil durch die Datensicherheits- und Datenschutzmaßnahmen ausreichend reduziert wurden, müssen explizit ausgewiesen werden. Risiken, die aufgrund einer unzureichenden Trennung der Mandanten bestehen, sind gesondert aufzuführen.

*Die Übernahme der Restrisiken muss schriftlich durch den Leiter der dem Mandanten zugeordneten Daten verarbeitenden Stelle erfolgen.* Die Übernahme der Restrisiken muss durch alle Daten verarbeitenden Stellen erfolgen, die auf der gemeinsamen Infrastruktur eine getrennte Datenverarbeitung durchführen. Die Übernahme der Restrisiken ist wechselseitig allen an der getrennten Datenverarbeitung beteiligten Stellen zur Kenntnis zu geben.

**Datenschutz- und Sicherheitsmanagement**

*Wird eine gemeinsame Infrastruktur zur getrennten Verarbeitung personenbezogener Daten genutzt, so ist ein mandantenübergreifendes Datenschutz- und Sicherheitsmanagement einzurichten.*

Jede Daten verarbeitende Stelle hat für die mandantenbasierte Verarbeitung personenbezogener Daten einen Ansprechpartner in Fragen des Datenschutzes und der Datensicherheit zu benennen. Üblicherweise sind hierfür die betrieblichen oder behördlichen Datenschutz- und IT-Sicherheitsbeauftragten zu benennen.

Die gemeinsam genutzte Infrastruktur muss regelmäßig durch das gemeinsame, mandantenübergreifende Datenschutz- und Sicherheitsmanagement auf angemessene technische und organisatorische Datenschutz- und Sicherheitsmaßnahmen sowie eine wirksame Umsetzung insbesondere der Datentrennung geprüft werden. Die Prüfergebnisse, insbesondere solche, aus denen sich mandantenübergreifende Auswirkungen ergeben können, sind allen Mandanten zur Verfügung zu stellen.

Im Rahmen des gemeinsamen, mandantenübergreifenden Datenschutz- und Sicherheitsmanagements ist ein gesondertes Vorgehen für mandantenübergreifende Datenschutz- und Sicherheitsvorfälle einzurichten, welches eine Beteiligung aller Mandanten in der Bearbeitung der Datenschutz- und Sicherheitsvorfälle vorsieht.

Das gemeinsame, mandantenübergreifende Datenschutz- und Sicherheitsmanagement muss in die betrieblichen Prozesse der gemeinsam genutzten Infrastruktur eingebunden sein. Insbesondere darf die Planung und Umsetzung von Änderungen an der gemeinsamen Infrastruktur nur unter Beteiligung des Datenschutz- und Sicherheitsmanagements aller an der getrennten Datenverarbeitung beteiligten Stellen erfolgen.

### 14.13.6 Fazit

Die ordnungsmäßige, getrennte Verarbeitung personenbezogener Daten in einer gemeinsamen IT-Infrastruktur muss, aufsetzend auf einer Betrachtung der rechtlichen Rahmenbedingungen, durch zusätzliche technische und organisatorische Sicherheitsmaßnahmen sichergestellt werden.

Zum Nachweis einer ordnungsgemäßen Verfahrenstrennung ist es zunächst erforderlich,

- die *rechtlichen Grundlagen*, auch zur Zulässigkeit der Datenübermittlungen zwischen Mandanten, wo diese vorgesehen sind, zu prüfen,
- die *Revisionsfähigkeit der Übermittlungen* zwischen den Mandanten,

- die *Abgeschlossenheit der Transaktionen innerhalb der Mandanten* und
- die *Unabhängigkeit der Konfiguration* nachzuweisen sowie
- die *Beschränkungen der mandantenübergreifenden Verwaltung der Datenverarbeitung* strikt umzusetzen.

Auf Basis dieser Vorüberlegungen ist dann das *Datenschutz- und Sicherheitsmanagement* auf diese besondere Form der Datenverarbeitung anzupassen.

## 14.14 Orientierungshilfe „Soziale Netzwerke“[*]

### 14.14.1 Einführung[**]

#### 1. Thematische Ausrichtung

Die vorliegende Orientierungshilfe reflektiert das gemeinsame Verständnis der Datenschutzbeauftragten und Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich über die Wahrung des Datenschutzes bei der Verwendung sozialer Medien, insbesondere sozialer Netzwerke, zur Erfüllung eigener Aufgaben oder Geschäftszwecke. Ziel ist es, neben der Konkretisierung der gesetzlichen Mindeststandards auch Best-Practice-Ansätze aufzuzeigen, soweit der gesetzliche Normierungsrahmen Lücken hinsichtlich eines ausreichenden Schutzes des Rechts auf informationelle Selbstbestimmung und des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aufweist. Die Darstellung zielt auf die datenschutzrechtliche Bewertung der verschiedenen „Schichten“ sozialer Netzwerke. Diese Schichten setzen sich aus den Inhaltsdaten, Bestandsdaten und Nutzungsdaten zusammen. Die Bewertung basiert auf den bestehenden gesetzlichen Grundlagen, den einschlägigen Beschlüssen und Entschließungen der nationalen und internationalen Gremien, insbesondere der Artikel-29-Datenschutzgruppe.

Auf eine Trennung zwischen der Darstellung „technischer“ und „rechtlicher“ Anforderungen wird in der Orientierungshilfe bewusst verzichtet. Vielmehr wurden als Leitlinie die Schutzziele der Datensicherheit und des Datenschutzes, Vertraulichkeit, Integrität, Verfügbarkeit, Intervenierbarkeit, Transparenz und Nichtverkettbarkeit (Zweckbindung) herangezogen. In diesen Schutzzielen lassen sich sämtliche Anforderungen am besten vereinen.

[*] Die Orientierungshilfe vom 14. März 2013 wurde erstellt von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.
Redaktion: Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit.
[**] Die Nummerierung der Orientierungshilfe und entsprechende Verweise wurden dem Layout meines TBs angepasst. Das Original finden Sie auf meiner Internetseite: www.datenschutz.sachsen.de.

## 2. Zielgruppen

Die Orientierungshilfe richtet sich an Betreiber sozialer Netzwerke. Sie richtet sich auch an Behörden und Unternehmen, die mit sozialen Netzwerken ihre Aufgaben erfüllen (wollen) oder ihre Geschäftszwecke verfolgen. Außerhalb des Fokus liegen die privaten Nutzer sozialer Netzwerke. Die Orientierungshilfe ist insofern keine Anleitung für den datenschutzgerechten Gebrauch solcher Netzwerke. Hinweise und Anleitungen für Nutzer[1] derartiger Dienste werden von verschiedenen Datenschutzbehörden und anderen Einrichtungen zur Verfügung gestellt.

## 3. Schutzziele

Diese Orientierungshilfe verwendet neben den „klassischen“ Schutzzielen Vertraulichkeit (Kapitel 14.14.7), Verfügbarkeit (Kapitel 14.14.8) und Integrität (Kapitel 14.14.6) als Maßstab auch die modernen Datenschutzziele Nichtverkettbarkeit (Kapitel 14.14.4), Transparenz (Kapitel 14.14.5) und Intervenierbarkeit (Kapitel 14.14.9)[2].

Diese ergänzenden Ziele sind teilweise bereits in Datenschutzgesetzen oder anderen Normen explizit verankert (so z. B. in § 10 Abs. 2 Nr. 6 DSG NRW), lassen sich aber auch aus den anderen Regelungen ableiten, die die Aufrechterhaltung des technisch-organisatorischen Datenschutzes zum Inhalt haben.

## 4. Begriffsdefinitionen

Die in dieser Orientierungshilfe verwendeten Begriffe von zentraler Bedeutung werden im Folgenden erläutert.

*Soziales Netzwerk:* Gesamtheit aus technischer und organisatorischer Infrastruktur mit Soft- und Hardware, Betreiber(n) und Nutzern dieser Infrastruktur sowie der darin vorhandenen Daten.

*Betreiber oder Anbieter:* Eine Organisation, in der Regel juristische Person, die die wesentlichen organisatorischen und technischen Bestandteile eines sozialen Netzwerks bereitstellt und den Dienst damit ermöglicht und darüber den Umfang und die Bedingungen der Nutzung festlegt.

*Mitglied:* In Bezug auf ein bestimmtes soziales Netzwerk bei diesem registrierte Person[3].

[1] Mit der geschlechtsneutralen Form werden Frauen wie Männer gleichermaßen umfasst.
[2] Siehe z. B. Rost/Pfitzmann „Datenschutz-Schutzziele - revisited“, in DuD 6/2009.
[3] Dies kann eine natürliche Person, d. h. ein privater Nutzer oder eine juristische Person als professioneller Nutzer sein.

*Nutzer:* Person, die Dienste eines sozialen Netzwerks nutzt, sei es als registriertes Mitglied oder als nicht-registrierter Externer.

*Dritter:* Jede andere natürliche oder juristische Person, die nicht Betreiber oder Nutzer in Bezug auf ein bestimmtes soziales Netzwerk ist.

## 5. Allgemeine datenschutzrechtliche Anforderungen

Die Datenschutzbeauftragten des Bundes und der Länder und die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben sich mittlerweile mehrfach in Form von Beschlüssen und Entschließungen zum Datenschutz in sozialen Netzwerken geäußert. Sie haben bei den Betreibern die Beachtung verschiedener Anforderungen angemahnt.

- Information
  Es müssen leicht zugängliche und verständliche Informationen darüber existieren, welche Daten für welche Zwecke erhoben und verarbeitet werden. Nur eine größtmögliche Transparenz bei Abschluss des Vertrags über eine Mitgliedschaft bzw. informierte Einwilligungen gewährleisten die Wahrung des Rechts auf informationelle Selbstbestimmung (siehe Pkt. 1 unter 14.14.5).

- Standard-Einstellungen
  Sämtliche Voreinstellungen für die Verwendung personenbezogener Daten des Netzwerkes müssen auf dem Einwilligungsprinzip beruhen, jedenfalls soweit nicht der Zweck der Mitgliedschaft eine Angabe von Daten zwingend voraussetzt. Eine Datenverarbeitung zunächst zu beginnen und nur eine Widerspruchsmöglichkeit in den Voreinstellungen zu ermöglichen, entspricht nicht den gesetzlichen Vorgaben (siehe Pkt. 2 unter 14.14.5). Voreinstellungen sind so zu wählen, dass Risiken für die Privatsphäre der Nutzer minimiert werden und dem Prinzip der Erforderlichkeit Rechnung getragen wird.

- Betroffenenrechte
  Es muss eine einfache Möglichkeit für Betroffene geben, ihre Ansprüche auf Auskunft, Berichtigung und Löschung von Daten geltend zu machen. Grundvoraussetzung hierfür ist die Angabe von entsprechenden Kontaktdaten an leicht auffindbarer Stelle, damit die Betroffenen wissen, wohin sie sich wenden können (siehe Pkt. 3 unter 14.14.9).

- Biometrische Daten
  Die Verwertung von Fotos für Zwecke der Gesichtserkennung und das Speichern und Verwenden von biometrischen Gesichtserkennungsmerkmalen sind ohne ausdrück-

liche und bestätigte Einwilligung der abgebildeten Person unzulässig (siehe Pkt. 2 unter 14.14.2 und Pkt. 2 unter 14.14.10).

- Pseudonyme Nutzung und Löschverpflichtungen
  Das Telemediengesetz (TMG) schreibt die Eröffnung pseudonymer Nutzungsmöglichkeiten in sozialen Netzwerken vor, soweit dies technisch möglich und zumutbar ist. Nutzer müssen die Möglichkeit haben, in dem sozialen Netzwerk unter Pseudonym oder mehreren Pseudonymen zu handeln. Dies dient der Wahrung des informationellen Grundrechts bei der Nutzung des Internet. Das TMG enthält im Hinblick auf Nutzungsdaten - soweit keine Einwilligung vorliegt - ein Verbot der personenbeziehbaren Profilbildung und die Verpflichtung, nach Beendigung der Mitgliedschaft sämtliche Daten zu löschen (siehe 14.14.4).

- Social Plug-ins
  Das direkte Einbinden von Social Plug-ins in Websites deutscher Anbieter ist unzulässig, wenn dadurch eine Datenübertragung an den jeweiligen Anbieter des Social Plug-ins ausgelöst wird, ohne dass die Internetnutzer hinreichend informiert werden und ohne ihnen die Möglichkeit zu geben, die Datenübertragung zu unterbinden (siehe Pkt. 1 unter 14.14.5).

- Datensicherheit
  Die großen Mengen an teils sehr sensiblen Daten, die in sozialen Netzwerken anfallen, sind durch geeignete technisch-organisatorische Maßnahmen zu schützen. Anbieter müssen nachweisen können, dass sie solche Maßnahmen getroffen haben (siehe Pkt. 5 unter 14.14.2).

- Minderjährigenschutz
  Daten von Minderjährigen sind besonders zu schützen. Insofern kommt datenschutzfreundlichen Standardeinstellungen eine wichtige Bedeutung zu. Informationen über die Verarbeitung von Daten müssen auf den Empfängerhorizont von Minderjährigen Rücksicht nehmen und für diese leicht verständlich und beherrschbar sein.

- Kontaktpersonen
  Betreiber, die außerhalb des Europäischen Wirtschaftsraumes ansässig sind, müssen gemäß § 1 Abs. 5 Satz 3 BDSG einen Inlandsvertreter bestellen, der Ansprechperson für die Datenschutzaufsicht ist.

### 14.14.2 Technische Grundlagen - Datensicherheit

Aus einem informationstechnischen Blickwinkel bestehen soziale Netzwerke typischerweise aus folgenden Komponenten:

- Client (Internet-Browser oder Smartphone-App),
- Übertragungsnetz (Internet),
- Server-Infrastruktur,
- Datenhaltungs-Infrastruktur (sog. Content Delivery Networks).

Diese Komponenten haben jeweils ihre eigenen Datensicherheitsanforderungen, die unterschiedliche Sicherheitsmaßnahmen erforderlich machen. Die Maßnahmen dienen der Datensicherheit und damit grundsätzlich dem Datenschutz (etwa die Verschlüsselung). Mitunter existieren auch widerstreitende Interessen, z. B. wenn durch Beobachtung des Nutzerverhaltens Angriffe auf das Netzwerk verhindert werden sollen und dabei zusätzliche, das Recht auf informationelle Selbstbestimmung gefährdende Datenverarbeitung stattfindet.

In diesem Kapitel werden verschiedene Aspekte der Technik sozialer Netzwerke beleuchtet und im Hinblick auf ihre Datensicherheitsanforderungen diskutiert. Die getroffene Auswahl ist nicht abschließend, sondern stellt eine Fokussierung auf diejenigen Bereiche dar, die in der Datenschutzdiskussion von besonderer und aktueller Bedeutung sind.

## 1. Datenhaltung

Betreiber (zentralisierter) sozialer Netzwerke verwalten typischerweise große Datenmengen[4]. Die zum performanten Betrieb solcher Datenmengen genutzten Techniken und Architekturen sind vergleichsweise neu und entwickeln sich noch immer rasch weiter. Die wichtigsten Anforderungen an diese Systeme sind:

- Die Systeme sollten über ausreichende Sicherheitsoptionen wie Zugriffschutz und Authentisierung verfügen, da die entsprechenden Anforderungen nicht von Beginn an in die Entwicklung der Systeme eingegangen sind.
- Die Daten sollten auf logische und räumlich einheitliche Speicherorte verteilt werden, um die Löschung und Beauskunftung von Nutzerdaten nicht zu erschweren.
- Das Löschen von Daten sollte nicht über das Entfernen der Indexeinträge, die zum Auffinden der eigentlichen Daten genutzt werden, erfolgen. Vielmehr sind die Daten tatsächlich zu löschen.

[4] Die von großen Anbietern wie Facebook oder Google betriebenen Datenbanken gehören zu den größten der Welt. Facebook hatte Mitte 2010 ein Datenvolumen von 15 Petabytes (PB, dies sind 15.000.000 Gigabytes) bei einem Anstieg von 60 TB pro Tag; siehe Thusoo et al: „Data warehousing and analytics infrastructure at facebook“, in Proceedings of the 2010 international conference on Management of data, http://borthakur.com/ftp/sigmodwarehouse2010.pdf. Aktuell werden mehr als 100 PB angegeben, http://www.facebook.com/notes/facebook-engineering/under-the-hood-hadoop-distributed-filesystem-reliability-with-namenode-and-avata/10150888759153920.

## 2. Biometrische Techniken

Biometrie stellt zunächst keine typische Technik sozialer Netzwerke dar, da biometrische Merkmale wie Fingerabdrücke oder Gesichtsgeometrien nicht erhoben werden.

Allerdings hat die biometrische Erkennung von Gesichtern auf den Fotos der Nutzer mittlerweile Einzug in verschiedene Netzwerke gehalten. Dies ist offenbar auch auf Fotos geringerer Qualität mit einigem Erfolg möglich, zumindest wenn sich die Erkennung nur auf die relativ überschaubare Menge der Freunde eines Nutzers beschränkt. In der Regel handelt es sich dabei um lernende Systeme, die eine anfängliche und fortlaufende „Mitarbeit“ derjenigen Nutzer erfordern, die Personen auf Fotos manuell markieren.

Der Umstand, dass hierbei - aus Sicht des Betreibers eines sozialen Netzwerkes - ohne aufwändige zusätzliche Erhebungen eine massentaugliche biometrische Datenbasis geschaffen wird, birgt datenschutzrechtliche Risiken. Details hierzu werden in Abschnitt 14.14.10 Pkt. 2 erörtert.

## 3. Tracking

Obwohl kein exklusives Thema sozialer Netzwerke, ist das Tracking von Nutzern ein wichtiges Element in der Gesamtfunktionalität vieler Netzwerke. Als Instrument zur Steuerung und Analyse von Werbeeinblendungen trägt das Tracking entscheidend dazu bei, die Einnahmen der unentgeltlich angebotenen Netzwerke zu sichern. Dabei haben soziale Netzwerke gegenüber anderen Angeboten im Internet einen entscheidenden Vorteil: Sie kennen ihre Nutzer[5]. Es ist ihnen daher immer möglich, die Aktivitäten nutzerspezifisch zu verfolgen. Der Nutzer kann sich dem nicht durch Browsereinstellungen o. Ä. entziehen, ohne seinen Anmeldestatus zu verlieren.

In technischer Hinsicht stehen sozialen Netzwerken die typischen Methoden für das Tracking zur Verfügung: Cookies, Flash-Cookies bzw. LSO (Local Shared Objects) oder HTML5 Client-Side Storage. Meist wird eine Kombination dieser Techniken eingesetzt (mehr zum Nutzertracking und zur Reichweitenanalyse in 14.14.10 Pkt. 4).

## 4. Werbung

Insbesondere für diejenigen sozialen Netzwerke, die ihre Mitgliedschaft kostenlos anbieten, bilden Werbeeinnahmen die bei weitem größte Einnahmequelle. Entsprechend wird auf die Möglichkeiten Wert gelegt, die Werbung möglichst zielgenau und damit erfolgversprechend und gewinnbringend platzieren zu können.

[5] Jedenfalls soweit es sich um ihre Mitglieder handelt und die Anmeldung nicht unter Pseudonym erfolgt ist. Nichtmitglieder können Soziale Netzwerke zwar auch aufrufen, sind in ihren Möglichkeiten in der Regel aber sehr beschränkt.

Den sozialen Netzwerken ist es oft möglich, sowohl die Angaben soziographischer Natur ihrer Nutzer (Alter, Geschlecht, Wohnort etc.) als auch deren aktuelle Aktivitäten bei der Werbeeinblendung zu berücksichtigen. Besonders interessant ist dies, wenn sich die Beobachtung der Nutzer über die Grenzen des eigenen Netzwerks hinaus auf das gesamte Web erstreckt. Dies ist mit Hilfe sog. Social Plug-ins möglich, die Webseitenanbieter in ihre Seiten integrieren.

Statt bzw. ergänzend zu der Finanzierung durch Werbung bestehen andere Möglichkeiten der Kostendeckung, etwa Nutzungsentgelte.

## 5. Technische und organisatorische Maßnahmen zur Datensicherheit

Soziale Netzwerke sind verpflichtet, Maßnahmen zur Gewährleistung der Datensicherheit zu ergreifen. Sie verwalten die persönlichen Daten, Beziehungen, Fotos, Meinungen, Interessen und Gewohnheiten von Millionen, nicht selten minderjährigen Menschen.

### 5.1 Verhinderung systematischer Massendownloads von Profildaten aus dem sozialen Netzwerk

Anbieter sozialer Netzwerke müssen sicherstellen, dass die Nutzer ihrer Angebote die Profildaten und Kommunikationsinhalte anderer Nutzer nicht ohne ausdrückliche Einwilligung der Betroffenen automatisiert von Dritten ausgelesen werden können.

Folgende Maßnahmen gegen den automatisierten und systematischen Abruf (z. B. durch crawler) von Profildaten und Kommunikationsinhalten sollten getroffen werden:

- Der Zugriff von Suchmaschinen oder anderen Indexierern auf die Profile der Nutzer sollte von diesen im Rahmen der Datenschutzeinstellungen festgelegt werden können und in den Standardeinstellungen deaktiviert sein.
- Betreiber von sozialen Netzwerken sollten Maßnahmen ergreifen, die eine Massenkopie von Daten aus dem Netzwerk verhindern. Zu solchen Maßnahmen zählen z. B. die Beobachtung von auffälligen Aktivitäten im Netzwerk (Unterscheidung zwischen manuellen und maschinellen Zugriffen) oder die externe Auditierung der eigenen Infrastruktur.

### 5.2 Angriffe auf den sozialen Graphen

Vereinfacht lassen sich soziale Netzwerke als Graphen betrachten, die Knoten (Nutzerprofile) und Kanten (Freundschaftsbeziehungen) verbinden. Ziel vieler Betreiber von Netzwerken ist es, diesen Graphen möglichst groß und engmaschig zu machen. Insbe-

sondere soll er nicht in voneinander unabhängige Bereiche zerfallen. Diese aus Netzwerksicht wünschenswerte Eigenschaft macht soziale Netzwerke (und auch andere zusammenhängende Netzwerke) anfällig für sich von Knoten zu Knoten fortpflanzende Missbräuche.

Eine einmal gefundene Schwachstelle (z. B. zum Auslesen oder Verändern von Daten) kann ausgehend von einem Nutzer (z. B. dem Account eines Angreifers) rasch in dem gesamten Netzwerk ausgenutzt werden und damit die Infrastruktur in ihrer Gesamtheit gefährden. Einige aktuellere Beispiele hierfür sind Koobface[6], Ramnit[7] oder LilyJade[8]; das Problem reicht bis in die Anfangszeiten sozialer Netzwerke zurück (z. B. 2005 der Spacehero-Wurm auf MySpace[9]).

Betreiber sozialer Netzwerke müssen sämtliche nach dem Stand der Technik als erforderlich anzusehenden Maßnahmen ergreifen, damit solche Angriffe unterbunden werden oder zumindest so rechtzeitig erkannt werden, dass Gegenmaßnahmen getroffen werden können. Hierzu sollten u. a. folgende Vorkehrungen getroffen werden:

- Einführung von CAPTCHAs[10], um Programme (sog. Social Bots) zu behindern,
- Plausibilitätsprüfungen von Nutzeraccounts, um insbesondere automatisiert betriebene Accounts zu erkennen,
- Beobachtung der Aktivitäten im Netzwerk auf Auffälligkeiten (z. B. besonders hohe Zugriffszahlen) und entsprechende Gegenmaßnahmen (z. B. zeitliche oder zahlenmäßige Begrenzung abfragbarer oder herunterladbarer Profile),
- Meldungen anderer Nutzer.

Diese Vorkehrungen[11] können systematische Massendownloads von Profildaten erschweren, sind jedoch nicht lückenlos[12] und erfordern ein permanentes Nachsteuern. Datensicherheit ist als Prozess zu begreifen, der zyklisch immer wieder durchlaufen werden muss. Die Betreiber sozialer Netzwerke müssen die Nutzer über bestehende Restrisiken informieren.

[6] http://en.wikipedia.org/wiki/Koobface
[7] http://www.spiegel.de/netzwelt/web/zehntausende-opfer-mehrzweck-wurm-kapert-facebook-konten-a-807521.html
[8] http://www.securelist.com/en/blog/706/Worm_2_0_or_LilyJade_in_action
[9] http://namb.la/popular/
[10] Completely Automated Public Turing test to tell Computers and Humans Apart, siehe http://de.wikipedia.org/wiki/CAPTCHA.
[11] Z. B. Facebook Immune System, http://allfacebook.de/wp-content/uploads/2011/10/FacebookImmuneSystem.pdf, oder Everything you ever wanted to know about Facebook Security, http://www.scribd.com/doc/70451272/Facebook-Security-Infographic.
[12] Z. B. The Socialbot Network: When Bots Socialize for Fame and Money, http://lersse-dl.ece.ubc.ca/record/264/files/ACSAC_2011.pdf?version=1.

### 14.14.3 Verantwortlichkeit

Nach Art. 2 d) der RL 95/46/EG (EG-Datenschutzrichtlinie[13]) ist für die Verarbeitung Verantwortlicher die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Hiervon zu unterscheiden ist der Auftragsdatenverarbeiter im Sinne von Art. 2 e) der RL 95/46/EG als die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet. Bei der Beurteilung wird auf die konkrete Funktion bei der Durchführung der Datenverarbeitung abgestellt. Die jeweilige Stelle kann für gewisse Datenverarbeitungen als verantwortliche Stelle, für andere Verarbeitungen auch als Auftragsdatenverarbeiter tätig werden. Je nach eingenommener Rolle können sich somit unterschiedliche Funktionen für Anbieter und Betreiber, aber auch die Nutzer eines sozialen Netzwerks ergeben.

#### 1. Verantwortungsverteilung bei sozialen Netzwerken

#### 1.1 Betreiber von sozialen Netzwerken

Betreiber von sozialen Netzwerken, die Online-Kommunikationsplattformen zur Nutzung bereitstellen, sind regelmäßig als verantwortliche Stelle nach Art. 2 d) der RL 95/46/EG bzw. § 3 Abs. 7 BDSG anzusehen.[14] Sie bestimmen über die Zwecke und Mittel der Datenverarbeitung. Die Fähigkeit, die Verarbeitungszwecke zu bestimmen, ist bereits feststellbar, wenn mit den im Rahmen der Nutzung der Dienste erhobenen Daten zum Beispiel Werbe- oder Marketingzwecke verfolgt werden. Hierbei werden Nutzungsdaten (z. B. IP-Adresse, Browsertyp, Cookies) und Inhaltsdaten (eingestellte Fotos, eingestellte Beiträge) verarbeitet. Eine entsprechende Zwecksetzung ergibt sich nicht selten aus den Allgemeinen Geschäftsbedingungen des Betreibers des sozialen Netzwerks. Die Entscheidung über die Mittel der Datenverarbeitung, d. h. die zum Einsatz kommende Soft- und Hardware, wie auch die Entscheidung über die Verarbeitung selbst, z. B. über die Speicherdauer, liegt im Regelfall ebenfalls bei den Betreibern von sozialen Netzwerken. Die Bezeichnung als „verantwortliche Stelle“ oder als „Auftragsdatenverarbeiter“ (auch in schriftlichen Vereinbarungen oder Verträgen) ist nicht maßgebend für die Bewertung. Es kommt auf die tatsächliche Aufgabenverteilung an, also welcher Stelle die jeweilige Funktion bzw. Rolle bei der Datenverarbeitung zukommt.

[13] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 S. 31).
[14] Art. 29-Datenschutzgruppe, WP 163 vom 12.07.2009, S. 6.

### 1.2 Professionelle Nutzer

Denkbar ist, dass mehrere verantwortliche Stellen gemeinsam über die Zwecke und Mittel der Datenverarbeitung entscheiden. Dies führt dazu, dass alle Stellen die Adressaten für die Einhaltung der Datenschutzvorschriften und insbesondere für die Erfüllung der Betroffenenrechte (Auskunft, Löschung, Sperrung, Berichtigung etc.) sind. Die Artikel-29-Datenschutzgruppe hat festgestellt, dass bezüglich der Akteure in einem sozialen Netzwerk sowohl die Konstellation denkbar ist, dass zwei oder mehrere Verantwortliche gemeinsam die vollständige Kontrolle über die Zwecke und Mittel ausüben, als auch der Fall, dass zwei oder mehrere Verantwortliche nur bezüglich eines Teils der Datenverarbeitung gemeinsam eine solche Kontrollfunktion besitzen.[15] Die Verfolgung gleicher Ziele und der Einsatz gleicher Mittel können auf verschiedene gemeinsam für die Datenverarbeitung Verantwortliche verteilt sein. Bei komplexen Verarbeitungsformen macht dies eine klare Zuweisung von Verantwortlichkeiten notwendig.[16] Unklarheiten dürfen sich nicht zu Lasten der Nutzer des sozialen Netzwerks auswirken. Diese müssen ihre Rechte auf Benachrichtigung, Löschung, Sperrung, Berichtigung und Widerspruch richtig adressieren können.

Webseitenbetreiber sind für die Datenverarbeitung Verantwortliche, wenn sie mittels Einbindung von Inhalten und von Diensten sozialer Netzwerkebetreiber (z. B. Social Plug-ins) zur Ausgestaltung ihres eigenen Dienstes die Datenverarbeitung der Anbieter des sozialen Netzwerks technisch ermöglichen.[17]

Die Verantwortlichkeit der Verwender der Dienste sozialer Netzwerke wird vor allem dann begründet, wenn diese zur Ausgestaltung ihres eigenen Angebotes die Dienste der Netzwerkanbieter nutzen und dabei eigene Geschäftszwecke verfolgen, z. B. durch die Inanspruchnahme von vom Betreiber zur Verfügung gestellten Statistiken. Derartige Nutzungsstatistiken werden auf der Grundlage von personenbezogenen Nutzerdaten der Nutzer erstellt.

### 2. Nutzer als verantwortliche Stelle

Nutzer von sozialen Netzwerken sind im Regelfall als Betroffene im Sinne von Art. 2 a) der RL 95/46/EG, § 3 Abs. 1 BDSG und nicht als für die Datenverarbeitung Verantwortliche. Allerdings ist nicht ausgeschlossen, dass sie selbst über die Zwecke und Mittel der Datenverarbeitung entscheiden bzw. mitentscheiden. Im Zusammenhang mit dem Freunde-Finder-Verfahren sozialer Netzwerke wurde etwa angenommen, dass die

[15] Art.-29-Datenschutzgruppe, WP 169 vom 16.02.2010, S. 26.
[16] Vgl. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Wer ist datenschutzrechtlich verantwortlich für Facebook-Fanpages und Social-Plugins? www.datenschutzzentrum.de/facebook/facebook-verantwortlichkeit.html.
[17] Ernst, Social Plugins: Der „Like-Button“ als datenschutzrechtliches Problem, NJOZ 2010, 1917, 1918.

Nutzer und der Betreiber des sozialen Netzwerks bewusst und gewollt zusammenwirken, indem die Nutzer die erforderlichen Adressdaten bereitstellen und der Netzwerkbetreiber die Erstellung von Einladungs-E-Mails und deren Versand übernimmt.[18]

Nutzer sind datenschutzrechtlich für die Verarbeitung personenbezogener Daten anderer Personen verantwortlich, wenn sie diese in ihren Nutzerprofilen oder auf den Plattformen in sozialen Netzwerken veröffentlichen. Nur wenn der Nutzer in Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten tätig wird, kommen die Datenschutzvorschriften nicht zur Anwendung (vgl. Art. 3 Abs. 2 der EG-Datenschutzrichtlinie, § 1 Abs. 2 Nr. 3 BDSG).[19] Die Annahme einer ausschließlich persönlichen oder familiären Datenverarbeitung ist bei der Verwendung fremder personenbezogener Daten jedoch zumeist nicht gegeben; dies gilt insbesondere, wenn die personenbezogenen Informationen für jedermann sichtbar sind. Selbst wenn die Sichtbarkeit auf bestimmte Kreise bzw. Listen beschränkt ist, wird der persönliche und familiäre Bereich verlassen, wenn sich Netzwerkbetreiber eigene Nutzungs- und Verarbeitungsrechte an den eingestellten Informationen einräumen. Ausgeschlossen ist eine familiäre und persönliche Nutzung sozialer Netzwerke außerdem, wenn der Nutzer das Profil ganz oder teilweise zu beruflichen oder geschäftlichen Zwecken verwendet.

Von einer rein familiären und persönlichen Nutzung eines sozialen Netzwerkes kann ausgegangen werden, wenn die Zugriffsmöglichkeiten auf Informationen anderer Betroffener in dem Profil des jeweiligen Nutzers auf die von ihm selbst ausgewählte Kontakte beschränkt ist und eine Nutzung dieser Daten durch den Netzwerkbetreiber ausgeschlossen wird, d. h. die verwendeten Informationen ausschließlich zur privaten Kommunikation und Interaktion verwendet werden.

### 14.14.4 Rechtliche Grundlagen - Zulässigkeit

Die europäische und deutsche Rechtsordnung verpflichten Betreiber sozialer Netzwerke, beim Erheben, Verarbeiten und Nutzen personenbezogener Daten die datenschutzrechtlichen Vorgaben einzuhalten, Art. 7 RL 95/46/EG und § 4 Abs. 1 BDSG.

#### 1. Anwendbares Recht

Für die Bestimmung, welche Rechtsordnung Anwendung findet, ist der Sitz des Dienstanbieters maßgeblich. Das für soziale Netzwerke einschlägige Telemedienrecht verweist zur Bestimmung des anzuwendenden Rechts auf die allgemeinen Regeln des

[18] LG Berlin, Urteil vom 06.03.2012, 16 O 551/10 (nicht rechtskräftig).
[19] Vgl. Art. 3 Abs. 2 der EG-Datenschutzrichtlinie, § 1 Abs. 2 Nr. 3 BDSG, sowie Art. 29-Datenschutzgruppe, WP 163 vom 12.07.2009, S. 6.

BDSG, § 3 Abs. 3 Nr. 4 TMG. Anwendbar sind somit die Regelung des § 1 Abs. 5 BDSG bzw. zu dessen europarechtskonformen Auslegung Art. 4 RL 95/46/EG.

Danach ist die Anwendung deutschen Datenschutzrechts ausgeschlossen, wenn der Betreiber des Netzwerkes seinen Sitz in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum hat. In diesen Fällen kommt das jeweilige nationalstaatliche Recht des Sitzlandes zur Anwendung.

Deutsches Datenschutzrecht findet bei Betreibern sozialer Netzwerke Anwendung, die ihren Sitz *nicht* in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum innehaben und im Inland Daten erheben, verarbeiten oder nutzen. Dies ist der Fall, wenn der Betreiber zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind. Die Artikel-29-Datenschutzgruppe legt den Begriff „Mittel“ weit aus. Unter diesen Begriff fallen demnach auch Anlagen von Auftragsdatenverarbeitern[20], die im Auftrag der Betreiber Daten im Inland erheben oder verarbeiten. Ein Bezug zum Inland wird auch dann hergestellt, wenn Cookies oder Javascript auf den Endgeräten der Nutzer zur Durchführung der Datenverarbeitung durch den Betreiber gespeichert oder ausgeführt werden.[21]

Dieser stark technisch orientierte Ansatz wird durch einen normativen Ansatz ergänzt. Zweck der Regelung des Art. 4 RL 95/46/EG ist es, das datenschutzrechtliche Schutzniveau nicht dadurch zu gefährden, dass außereuropäische Anbieter in den Markt drängen, ohne sich den auf diesem Markt geltenden Regeln unterwerfen zu müssen. Zugleich sollen zu heterogene Regelungsanforderungen an die Betreiber vermieden werden.

Die stark auf die objektiven Merkmale abstellende Bestimmung der Erhebung, Verarbeitung und Nutzung von Daten im Inland, wird durch die Zweckbestimmung des Betreibers ergänzt. Unter das Datenschutzrecht des jeweiligen Ziellandes fallen Betreiber nur, wenn auch der Wille zur Datenverarbeitung von personenbezogenen Daten im jeweiligen Land zum Ausdruck kommt. Die durch das Internet hervorgerufene Vernetzung erlaubt aus technischer Sicht, jeden Dienst von jedem Ort der Welt aus abzurufen. Daher soll nationales Datenschutzrecht für Angebote gelten, die sich explizit oder implizit an die Betroffenen in dem jeweiligen Land richten. Indizien für eine derartige

[20] A. A. VG Schleswig, Beschl. v. 14.02.2013; https://www.datenschutzzentrum.de/presse/20130215-verwaltungsgericht-facebook.htm.
[21] Art.-29-Datenschutzgruppe, Stellungnahme 8/2010 zum anwendbaren Recht v. 16.12.2010, WP 179 0836-02/10/DE, S. 25 f.

Ausrichtung des Angebotes könnten die Spracheinstellungen, Domainendungen oder die direkte inhaltliche Ansprache sein.

Deutsches Datenschutzrecht findet daher auf Betreiber mit Sitz im außereuropäischen Ausland Anwendung, die im Inland Daten erheben, verarbeiten und nutzen und deren Angebot sich an in Deutschland lebende Personen richtet.

Wenn der nichteuropäische Betreiber eine Niederlassung in einem Mitgliedstaat der Europäischen Union betreibt, findet das jeweilige Landesrecht des europäischen Sitzstaates Anwendung. Voraussetzung ist jedoch, dass es sich bei der Niederlassung um eine datenschutzrechtlich relevante Niederlassung handelt. Die Niederlassung muss für das jeweils in Frage stehende Verfahren die datenschutzrechtliche Verantwortung, d. h. die tatsächliche Entscheidungsbefugnis über Art und Umfang der Datenverarbeitung innehaben.

Öffentliche Stellen des Bundes und der Länder als Betreiber sozialer Netzwerke unterliegen den nationalen datenschutzrechtlichen Anforderungen aus dem BDSG bzw. den jeweiligen Landesdatenschutzgesetzen bzw. dem Bundesdatenschutzgesetz und dem Telemedienrecht. Die Anwendung des datenschutzrechtlichen Teils des Telemediengesetzes gilt gemäß § 11 Abs. 1 TMG nicht für soziale Netzwerke, soweit die Bereitstellung solcher Dienste im Dienst- und Arbeitsverhältnis zu ausschließlich beruflichen oder dienstlichen Zwecken oder innerhalb von oder zwischen nicht-öffentlichen Stellen oder öffentlichen Stellen ausschließlich zur Steuerung von internen Arbeits- oder Geschäftsprozessen erfolgt.

## 2. Gesetzliche Grundlagen im Bundesdatenschutz- und Telemediengesetz

Das deutsche Datenschutzrecht legt für Betreiber sozialer Netzwerke Anforderungen fest. Maßgelblich ist der Zweck der Erhebung und der Verarbeitung und die technische Natur des Datums. Somit kann ein „technisches Datum“ unterschiedlichen rechtlichen Regelungsregimen unterfallen. Der Name eines Betroffenen kann insoweit ein Bestands-, Nutzungs-, Abrechnungs- und Inhaltsdatum sein; dessen Verarbeitung kann im TMG oder im BDSG bzw. LDSG geregelt sein.

### 2.1 Inhaltsdaten

Zu den Inhaltsdaten zählen Informationen der Betroffenen, die Gegenstand der Leistungserbringung durch den Betreiber des sozialen Netzwerkes sind und den „Inhalt“ des Dienstes ausmachen. Dazu gehören die Profilinformationen eines persönlichen Profils und die Inhalte der Kommunikation. Derartige Informationen unterfallen entweder bereichsspezifischen Gesetzen oder den allgemeinen Regeln des BDSG oder LDSG.

### 2.2 Bestandsdaten

Bestandsdaten unterliegen den Regeln des § 14 Abs. 1 TMG. Bestandsdaten sind Angaben, die für die Begründung, Durchführung und Beendigung eines Nutzungsverhältnisses notwendig sind. Welche konkreten Daten das sind, wird durch den jeweiligen Nutzungsvertrag bestimmt. Dazu zählen identifizierende Nutzerangaben (Name, Anschrift, E-Mail), Zugangsdaten (Nutzername, ID, Kennwort) oder weitere vertragsrelevante Informationen (Tarife, Nutzungszeiten etc.).

### 2.3 Nutzungsdaten

In den Anwendungsbereich des TMG fallen auch sämtliche Daten, die erforderlich sind, um die Inanspruchnahme des sozialen Netzwerkes zu ermöglichen und abzurechnen. Die Erhebung, Verarbeitung und Nutzung derartiger Nutzungsdaten ist in § 15 TMG umfassend geregelt. Zu den Nutzungsdaten zählen Merkmale zur Identifikation des Nutzers (IP-Adresse, Cookies, Nutzerkennung), Angaben über Beginn und Ende der Nutzung und Angaben über die in Anspruch genommenen Dienste. Soweit die Nutzungsdaten für die Abrechnung kostenpflichtiger Angebote des sozialen Netzwerkbetreibers verwendet werden, handelt es sich um Abrechnungsdaten, deren Verwendung durch § 15 Abs. 4 TMG geregelt wird.

## 3. Rechtsnatur der Mitgliedschaft in einem sozialen Netzwerk

Soziale Netzwerke sind ein relativ neues Phänomen der Entwicklung des Internets, deren rechtliche Einordnung, die entscheidend für die datenschutzrechtliche Bewertung ist, nicht einfach ist. Eine einheitliche, allgemein anerkannte Auffassung zu ihrer Rechtsnatur hat sich daher bislang noch nicht herausgebildet.

### 3.1 Vertragliche Ausgestaltung

Der Vorteil einer vertraglichen Ausgestaltung ist es für Betreiber sozialer Netzwerke, dass in Deutschland der Abschluss von Nutzungsverträgen grundsätzlich formfrei möglich ist. Es gilt der Grundsatz der Privatautonomie: Jeder kann mit jedem einen Vertrag über einen individuell gewünschten Inhalt abschließen. Dabei darf nicht außer Acht gelassen werden, dass über verbraucherschützende Vorschriften wie die §§ 305 ff. BGB zivilrechtlich eine Inhaltskontrolle möglich ist.

Datenschutzrechtlich gilt, dass Datenerhebungen und -verwendungen, die für den Vertragszweck erforderlich sind, grundsätzlich auf gesetzlicher Grundlage nach § 28 Abs. 1 S. 1 Nr. 1 BDSG bzw. § 14 Abs. 1 TMG zulässig sind. Ähnlich wie bei der Mitgliedschaft in einem Verein sind jedoch Regelungen, die mit dem Hauptzweck der

Mitgliedschaft nichts zu tun haben, aber von hoher datenschutzrechtlicher Relevanz sind, kritisch zu hinterfragen: Ebenso wenig wie ein Sportverein über eine Satzungsregelung, nach der die Mitgliederdaten an Sportartikelhersteller verkauft werden dürfen, diese Datenübermittlung legitimieren kann, kann sich ein Betreiber eines sozialen Netzwerks über seine Nutzungsrichtlinien ausbedingen, die Mitgliederdaten zu einem Zweck zu verwenden, der mit der vereinbarten Nutzung des sozialen Netzwerks unmittelbar nichts zu tun hat. Dies gilt z B. für die oben erwähnte Werbung, es sei denn, der Vertrag ist so deutlich ausgestaltet, dass der Nutzer sich darüber im Klaren ist, dass er auch einen Vertrag über die werbliche Nutzung seiner Daten schließt.

Wenn der Betreiber des sozialen Netzwerks die Nutzungsbedingungen ändert, braucht er jedenfalls bei wesentlichen Änderungen die Zustimmung des Nutzers; ansonsten gelten für diesen die alten Bedingungen fort. Ein kollektives Einverständnis der Nutzer in Form eines fehlenden Widerspruchs durch ein betreiberseitig definiertes Quorum genügt nicht. Anders als beim Verein, bei dem von Gesetzes wegen Satzungsänderungen nur unter der Beteiligung der Mitglieder möglich sind (vgl. § 33 BGB), werden die Nutzungsbedingungen bei sozialen Netzwerken einseitig durch den jeweiligen Betreiber gesetzt. Hieran ändern auch betreiberseitig initiierte Abstimmungen über geplante Änderungen nichts. Es handelt sich letztlich um eine Änderung des Nutzungsvertrags, mit der das einzelne Mitglied einverstanden sein muss.

Allerdings ist es im vertraglichen Bereich denkbar, dass das Mitglied seine Zustimmung durch konkludentes Handeln äußert. Dies kann sogar in einem Unterlassen bestehen, wie sich im Umkehrschluss aus § 308 Nr. 5 BGB ergibt. Voraussetzung ist, dass dies entsprechend vorher vertraglich vereinbart wird und dem Mitglied eine angemessene Frist zur Abgabe einer ausdrücklichen Erklärung eingeräumt wird sowie bei Fristbeginn ein Hinweis auf die vorgesehene Bedeutung seines Verhaltens erfolgt.

Liegt ein wirksamer Vertrag vor, muss der Betreiber eines sozialen Netzwerks im Rahmen seiner Informationspflichten nach § 13 Abs. 1 TMG und § 4 Abs. 3 S. 1 BDSG den Nutzer über die konkreten Datenflüsse unterrichten (sofern sich diese nicht bereits direkt aus der vertraglichen Regelung ergeben). Im Fall von pseudonymer Nutzerdatenanalyse ist der Nutzer ebenfalls darüber zu Unterrichten und auf sein Widerspruchsrecht hinzuweisen, § 15 Abs. 3 TMG.

### 3.2 Einholen einer datenschutzrechtlichen Einwilligung

Das Rechtsinstitut der Einwilligung kommt in denjenigen Konstellationen zum Tragen, in denen die beabsichtigte Datenerhebung und -verwendung nicht mehr von dem (vertraglich vereinbarten) Zweck des Nutzungsverhältnisses gedeckt ist. Dies ist insbeson-

dere dann der Fall, wenn der Zweck in keinem Zusammenhang mit der Nutzung des sozialen Netzwerkes steht. Auch der Umgang mit personenbezogenen Daten zum Zweck der individualisierten Werbung bedarf der Einwilligung. Denn für die unmittelbare Inanspruchnahme des Dienstes ist die Datenverarbeitung zum Zweck der Werbung nicht erforderlich.

In diesen Fällen muss der Nutzer informiert einwilligen, d. h. er muss über Zweck und Umfang der Datenverarbeitung aufgeklärt werden und sein Einverständnis aktiv - beispielsweise durch das Setzen eines Häkchens - bekunden. Wichtig ist - parallel zu den Ausführungen zur vertraglichen Ausgestaltung - dass beim Nutzer ein entsprechender Rechtsbindungswillen vorhanden ist und auch nachgewiesen werden kann. Im Einzelnen sieht das Gesetz in § 13 Abs. 2 und 3 TMG vor, dass der Dienstanbieter bei einer elektronischen Einwilligung sicherstellen muss, dass

- der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat,
- die Einwilligung protokolliert wird,
- der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann,
- der Nutzer die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann und
- er auf dieses Widerrufsrecht hingewiesen wird.

Die Einwilligung ist das Mittel der Wahl für Datenerhebungen und -verwendungen, die über den im Rahmen der Mitgliedschaft vereinbarten Vertragszweck hinausgehen.

Aufgrund der Gestaltungsmacht des Netzwerkbetreibers ist dieser in der Lage, den Umfang der geschuldeten vertraglichen Leistung zu bestimmen. Eine einseitige nachträgliche Erweiterung der Pflichten des Nutzers durch das Abverlangen einer Einwilligung unter der Bedingung, nur bei der Erteilung der Einwilligung das Nutzungsverhältnis fortzusetzen, stellt die Freiwilligkeit der Erteilung der Einwilligung in Frage. Soziale Netzwerke sind auf die Pflege der Kommunikationsbeziehungen, die Teil der menschlichen Identität sind, ausgerichtet. Wird die Fortnutzung des Dienstes von der Erteilung der Einwilligung abhängig gemacht, hat der Nutzer nur die Wahl seine Kommunikationsbeziehung abzubrechen oder den Eingriff in seine Persönlichkeitsrechte zu legitimieren. Auch die Nutzung von personenbezogenen Daten Betroffener, die nicht Nutzer des jeweiligen Netzwerkes sind bzw. nicht mit den Betreibern direkt in Kontakt stehen, ist in der Regel nur auf der Grundlage einer entsprechenden Einwilligung der Betroffenen möglich. Nicht auszuschließen sind Fälle, in denen Betreiber ein berechtigtes Interesse darlegen können, personenbezogene Daten zu verarbeiten und auch Personen, die nicht Nutzer des Netzwerkes sind, diesen Eingriff dulden müssen, z. B. Maßnahmen der Datensicherheit gegen Angriffe von außen. Eine derartige Befugnis ist jedoch im

jeweiligen Einzelfall plausibel zu begründen und muss die Ausnahme bleiben. Den schutzwürdigen Interessen dieser Betroffenen, die womöglich eine bewusste Entscheidung getroffen haben, einen bestimmten Dienst nicht zu nutzen, sollte Rechnung getragen werden.

## 4. Zweckbindung und Nichtverkettbarkeit

Einige Datenschutzgesetze haben inzwischen die Nichtverkettbarkeit als Schutzziel bzw. als allgemeine Maßnahme zur Datensicherheit aufgenommen. Ziel der Nichtverkettbarkeit ist, dass personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können. So fordern §§ 12 Abs. 2 TMG, 28 Abs. 1 S. 2 BDSG, Art. 6 Abs. 1 lit b) RL 95/46/EG, dass bei der Datenverarbeitung gewährleistet sein muss, dass personenbezogene Daten nur dann zu einem anderen Zweck verarbeitet und genutzt werden dürfen, soweit dafür eine gesetzliche Rechtfertigung existiert oder die Betroffenen in die Zweckänderung eingewilligt haben.

Im Rahmen von sozialen Netzwerken geht es somit zum einen um die Frage, welche Inhalts-, Nutzungs- und Bestandsdaten in das Profil eines Nutzers einfließen, aber auch, inwieweit unterschiedliche Profile innerhalb des Netzwerkes, aber auch mit Profilen oder weiteren Inhalts-, Nutzungs- und Bestandsdaten des Nutzers außerhalb des Netzwerkes durch den Anbieter oder Dritte, verbunden werden können. Im Sinne der informationellen Selbstbestimmung muss das Netzwerk dem Nutzer die Möglichkeit bieten, zu entscheiden, wer was wann über ihn weiß und dies auch jederzeit feststellen zu können. Die folgenden Grundsätze sollten zur Förderung der Kontrolle beachtet werden[22]:

- Den Nutzern sollten Möglichkeiten zur Verfügung stehen, mit denen sie Verkettungen bzw. Zweckänderungen ihrer Daten und deren Ausmaß erkennen können.
- Die Nutzer sollten in der Lage sein, die Verkettung ihrer Daten über ein geeignetes Identitätsmanagement zu kontrollieren. Dazu gehört auch die Möglichkeit, in dem sozialen Netzwerk unter verschiedenen Pseudonymen (z. B. zur Trennung beruflicher und privater Nutzung) zu agieren (vgl. dazu unten Pkt. 5).
- Verkettungen müssen rückgängig gemacht werden können, indem z. B. Verknüpfungen von Profilen mit einer App oder einem Profil in einem anderen Netzwerk gelöscht werden können.
- Die Vertrauenswürdigkeit in die Verarbeitung sollte durch geeignete Nachweise gefördert werden (IT-Grundschutz, Audits, Zertifizierung).

[22] Vgl. Studie „Verkettung digitaler Identitäten“ ULD / TU Dresden, https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf.

## 5. Anonyme und pseudonyme Nutzung

Das TMG fordert in § 13 Abs. 6 von Betreibern sozialer Netzwerke, die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzende ist über diese Möglichkeit zu informieren. Den Nutzenden muss jedenfalls ermöglicht werden, in dem Sozialen Netzwerk unter Pseudonym zu agieren. Eine Offenlegung der tatsächlichen Identität des Nutzers gegenüber dem Betreiber des Sozialen Netzwerks kann dagegen zur Erschwerung von Missbrauch insbesondere dann hingenommen werden, wenn die Nutzer das Netzwerk nicht nur passiv (Herunterladen von Informationen), sondern auch aktiv (Einstellen von Informationen) nutzen können. Betreiber sozialer Netzwerke für Privatnutzung sollten die Nutzung von Pseudonymen aktiv fördern.

Bei Netzwerken, die im beruflichen Kontext genutzt werden, ist es in der dortigen Zielgruppe zwar eher unüblich, anonym bzw. unter Pseudonym aufzutreten. Trotzdem gilt die Verpflichtung aus § 13 Abs. 6 TMG zur Eröffnung einer optionalen Möglichkeit, in dem Netzwerk unter Pseudonym zu handeln, auch für solche Netzwerke. Bei entsprechenden Vorgaben zur Gestaltung der Pseudonyme muss die Qualität des Netzwerkes nicht leiden, so dass eine Unzumutbarkeit für den Anbieter nicht anzunehmen ist.

## 6. Zweckbindung

Zentrale Intention der Nichtverkettbarkeit ist die Sicherung der Zweckbindung. Das bedeutet, dass personenbezogene Daten nur für den Zweck verarbeitet werden dürfen, den die gesetzliche Vorgabe erlaubt bzw. der im Rahmen der Einwilligung durch den Betreiber des sozialen Netzwerkes vorgegeben worden ist. Nach § 13 Abs. 1 TMG hat der Dienstanbieter den Nutzer vor der Erhebung über den Zweck zu informieren. Soll der Zweck geändert werden, so ist dies nur möglich, wenn entweder hierfür eine gesetzliche Grundlage besteht oder die Einwilligung beim Betroffenen eingeholt wird (vgl. auch § 12 Abs. 2 TMG). Der Zweck muss im Rahmen der Einwilligung so umrissen werden, dass es dem Betroffenen möglich ist einzuschätzen, welche Verkettungsmöglichkeiten sich hieraus ergeben. Pauschale Zweckbestimmungen wie „zur Erbringung des Dienstes“ sind nicht ausreichend.

## 7. Trennungsprinzip

Um die Nichtverkettbarkeit auch technisch zu unterstützen, gilt im Datenschutzrecht das Trennungsprinzip. Nach § 13 Abs. 4 Nr. 4 TMG hat der Dienstanbieter durch technische und organisatorische Vorkehrungen sicherzustellen hat, dass die personenbezogenen Daten über die Nutzung verschiedener Telemedien durch denselben Nutzer getrennt verwendet werden können. Außerdem muss sichergestellt sein, dass Nutzungsprofile

i. S. d. § 15 Abs. 3 TMG nicht mit Angaben zur Identifikation des Trägers des Pseudonyms zusammengeführt werden können (§ 13 Abs. 4 Nr. 5 TMG). Für soziale Netzwerke bedeutet das, dass Nutzungsprofile, die zum Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung des sozialen Netzwerks erstellt werden, getrennt von den Nutzerprofilen verarbeitet werden müssen, die aus den Inhaltsdaten eines Nutzers bestehen. Für Nutzungsprofile sind Pseudonyme zu verwenden. Fallen noch bei weiteren Telemedien (z. B. Chat-Dienste, Spiele etc.) personenbezogene Daten an, so sind auch diese Daten und Profilinformationen von den übrigen Daten so weit wie möglich zu trennen.

### 14.14.5 Transparenz und Kontrolle

#### 1. Transparenz

Nach §13 Abs. 1 TMG hat der Dienstanbieter die Nutzer vor der Datenverarbeitung über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der RL 95/46/EG in allgemein verständlicher Form zu unterrichten. Nach § 4 Absatz 3 BDSG sind den Betroffenen von der verantwortlichen Stelle deren Identität, der Zweck der Datenverarbeitung und die Kategorien von Empfängern mitzuteilen. Letzteres gilt jedoch nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss.

Diese Anforderungen gelten sowohl für die Erhebung von Nutzungs- und Bestandsdaten nach dem TMG als auch für Inhaltsdaten nach dem BDSG. Die Einwilligung nach § 13 TMG bzw. § 4a BDSG ist nur wirksam, solange sie in Kenntnis des vorgesehenen Zwecks der Erhebung, Verarbeitung oder Nutzung erteilt wurde.

Neben der Information über Art, Umfang und Zwecke der Erhebung und Verwendung sind Nutzer über ihre Rechte zu informieren, z. B. über das Recht, der Einwilligung zur Verarbeitung zu widersprechen (§ 13 Abs. 3 TMG) und über die Möglichkeit, das Angebot anonym oder pseudonym zu nutzen (§ 13 Abs. 6 TMG). Zusätzlich muss der Betreiber des sozialen Netzwerks kommerzielle Inhalte sowie die dahinterstehende natürliche oder juristische Person klar als solche kennzeichnen (§ 6 TMG).

Informationen und Nutzungsbedingungen, die Rechte und Pflichten der Nutzer und des Betreibers des sozialen Netzwerks regeln, müssen in einer verständlichen und übersichtlichen, deutschsprachigen, barrierefreien Erklärung, die im gesamten Angebot leicht zugänglich ist, bereitgestellt werden (Datenschutzerklärung und Nutzungsbestimmungen). Die Informationen müssen umfassend sein, also z. B. auch Informationen zu personenbezogenen Daten enthalten, die mit Hilfe von Cookies erhoben werden. Die

Verwendung der Daten ist strukturiert und klar anzugeben, insbesondere die Weitergabe und der Zugriff durch berechtigte Dritte ist eindeutig festzulegen. Die Informationen sind stets zu aktualisieren, insbesondere bei neuen und geänderten Funktionen, und allen Nutzern vor der Einführung zur bestätigenden Kenntnis zu geben.

Nutzer sollten über mögliche Konsequenzen ihres Handelns auch während der Nutzung des Dienstes (z. B. bei der Veränderung von Datenschutz-Einstellungen einer Bildersammlung) informiert werden, z. B. durch eingebaute, kontext-sensitive Funktionen, die angemessene Informationen auf der Basis der jeweiligen Handlungen der Nutzer liefern.

Die Information der Nutzer sollte sich auch auf den Umgang mit Daten von Personen, die nicht Nutzer des Netzwerkes sind, beziehen: Betreiber sozialer Netzwerke sollten auch über Ge- und Verbote im Hinblick darauf informieren, wie die Nutzer diese Daten behandeln dürfen, die in ihren Profilen enthalten sind (z. B. wann die Einwilligung eines Betroffenen vor der Veröffentlichung eingeholt werden muss oder über mögliche Konsequenzen von Regelverstößen). Insbesondere spielen Fotos in Nutzerprofilen, auf denen Personen abgebildet sind, die bei dem Netzwerk nicht angemeldet sind oder von der Veröffentlichung keine Kenntnis haben (in vielen Fällen sogar versehen mit Hinweisen auf den Namen und/oder das Nutzerprofil), in diesem Kontext eine Rolle. Die derzeit weit verbreiteten Praktiken stehen in vielen Fällen nicht in Einklang mit den bestehenden Regelungen des Schutzes des Rechts am eigenen Bild gemäß dem Kunsturhebergesetz.

Die verantwortliche Stelle ist mit einfach zugänglicher Kontaktmöglichkeit anzugeben; bei ausländischen Anbietern sollte auch eine Kontaktmöglichkeit in dem Land, auf dessen Markt das Angebot ausgerichtet ist, angegeben sein. Ferner ist zu empfehlen, die Nutzer über den Regulierungsrahmen zu informieren, dem der Betreiber des sozialen Netzwerks unterliegt. Für den Fall der Insolvenz oder des Verkaufs sind Nutzer darüber zu informieren, wie mit ihren personenbezogenen Daten umgegangen wird.

Gibt es verschiedene Nutzergruppen, sind sowohl die Datenschutzbestimmungen als auch die Nutzungsbedingungen nach Nutzergruppen zu untergliedern, sodass - falls Regelungen nur bestimmte Nutzergruppen betreffen sollten - jeder Nutzer eindeutig erkennen kann, welche Bestimmungen für ihn gelten. Dies kann der Fall sein, wenn das soziale Netzwerk neben den Nutzern mit persönlichem Profil z. B. auch professionelle Nutzer oder Drittanbieter und Entwickler im Netzwerk zulässt.

Insbesondere über den Zugriff und die Verarbeitung durch Dritte (z. B. Anbieter von Anwendungen innerhalb des Netzwerks, Kooperations- und Werbepartner oder auch Sicherheitsbehörden) sind die Nutzer zu informieren. Dies gilt auch, wenn z. B. für die

Anzeige von Werbeeinblendungen in dem Browser-Fenster eines Nutzers die IP-Adresse dieses Nutzers an einen anderen Dienstanbieter weitergegeben wird, der den Inhalt der Werbung liefert.

Bietet das soziale Netzwerk Schnittstellen für Drittanbieter an, sind der Umfang und die Weiterverwendung der Daten genau zu definieren und zu benennen.

Informationen sollten auch über verbleibende Sicherheitsrisiken gegeben werden und über andere mögliche Konsequenzen der Veröffentlichung personenbezogener Daten in einem Profil, wie auch über mögliche Zugriffe durch Dritte (einschließlich Strafverfolgungsbehörden und Geheimdiensten).

**2. Kontrolle durch den Nutzer**

Das Recht auf informationelle Selbstbestimmung setzt Kontrollbefugnisse für den Nutzer voraus. Der Anspruch, selbst zu bestimmen, wer wann was über die eigene Person weiß, soll dem Nutzer sowohl gegenüber dem Betreiber des sozialen Netzwerks als auch gegenüber anderen Nutzern und Drittanbietern eingeräumt werden. Dies schließt nicht nur die selbstgenerierten Daten (z. B. Informationen über die eigene Person), sondern auch fremdgenerierte Daten (z. B. Markierungen auf Fotos durch Dritte) mit ein. Die Kennzeichnung von Fotos (d. h. das Hinzufügen von Links auf existierende Nutzerprofile oder des Namens der abgebildeten Person/en) sollte an die vorherige Einwilligung der Betroffenen gebunden sein.

Die Konfigurations- und Einstellungsmöglichkeiten sollten also zulassen, dass Informationen gruppen- oder personenbezogen sichtbar sind. Eine Weitergabe an Dritte (Nutzer des Netzwerks, Entwickler, Werbepartner) ohne explizite Einwilligung des Betroffenen ist unzulässig. Verständliche und übersichtliche Hilfestellungen zu den Einstellungsmöglichkeiten inklusive klarer Angaben über die möglichen Auswirkungen, ggf. ergänzt durch FAQs, sowie die höchstmögliche Schutzeinstellung zum Zeitpunkt der Registrierung (datenschutzfreundliche Standardeinstellungen, die der Nutzer auf eigenen Wunsch verändern kann) erlauben dem Nutzer, selbstbestimmt mit seinen Informationen umzugehen. Informationen, die auf Grund schwacher Schutzeinstellungen (möglicherweise sogar ohne das Wissen der Nutzer) offen für Dritte innerhalb und außerhalb des Netzwerks abrufbar sind und ggf. durch Suchmaschinen erfasst werden, unterliegen nicht mehr der Kontrolle der Nutzer und widersprechen dem Grundsatz der informationellen Selbstbestimmung. Die Kontrolle des Nutzers über die eigenen Daten muss auch gewährleistet werden, wenn er diese bewusst an Dritte weitergibt. Eine Weitergabe der Daten durch diese Dritten ohne Einwilligung des Betroffenen ist grundsätzlich nicht zulässig.

Werden Daten durch den Nutzer gelöscht, sollten Anbieter sicherstellen, dass die Löschung auch für etwaige Kopien, die Dritten zur Verfügung gestellt wurden umgesetzt wird, es sei denn, der Nutzer hat in die weitere Nutzung eingewilligt.

Um kontrollieren zu können, welche Daten der Betreiber über die betroffene Person gespeichert hat, muss die Umsetzung des Auskunftsanspruchs nach § 34 Abs. 1 BDSG durch den Betreiber des sozialen Netzwerks gesichert sein. Dies kann über ein Online-Abrufverfahren erfolgen, muss aber alle vom Betreiber gespeicherten Daten (Inhalts-, Bestands- und Nutzungsdaten) beinhalten. Es bedarf in diesem Fall eines bestmöglichen Schutzes vor Missbrauch.

Bei international ausgerichteten Netzwerken ist darauf zu achten, dass die Nutzerkontrolle nicht durch Sprachbarrieren gefährdet ist.

### 3. Interne Kontrolle

Die Einhaltung der Datenschutzbestimmungen muss in internen Datenschutzrichtlinien und Konzepten festgelegt sowie ggf. durch einen internen Datenschutzbeauftragten kontrolliert werden.[23] Hierbei muss sichergestellt sein, dass dieser in seiner Funktion weisungsfrei, der Unternehmensleitung direkt unterstellt, ausreichend geschult und qualifiziert ist. Dieser muss hinreichend unterstützt und rechtzeitig über datenschutzrelevante Änderungen informiert werden. Neue oder geänderte Funktionen sind in der Regel durch eine Vorabkontrolle auf Datenschutzverstöße zu kontrollieren (insbesondere bei Risiken für die Rechte und Freiheiten der Betroffenen wie z. B. bei der Verarbeitung besonderer Datenkategorien wie politische Meinung, religiöse oder philosophische Überzeugungen, Gesundheit oder Sexualleben).[24]

Datenschutzkonzepte (inklusive Rechte- und Rollenkonzepte) und technische Dokumentationen sind vor dem Produktivbetrieb zu erstellen und legen - neben der Dokumentation der Systeme und ihrer Funktionen - insbesondere den Umgang und die Verwendung (Zweckbindung) der zu verarbeitenden Daten, den Schutzbedarf der Daten sowie die technischen und organisatorischen Maßnahmen fest, die vom Betreiber des sozialen Netzwerks zu ergreifen sind. Die Datenschutzkonzepte sind zu aktualisieren, sobald Änderungen oder Neuerungen entwickelt werden.

Technische und organisatorische Maßnahmen sind insbesondere zu ergreifen, um zu gewährleisten, dass die Vertraulichkeit und Integrität der Daten gesichert ist. Die Verknüpfung verschiedener Daten bzw. die Zweckentfremdung der Daten ist zu verhindern. Hierfür ist eine revisionssichere Protokollierung zu installieren, die die Zugriffe auf die

[23] Vgl. § 4f BDSG.
[24] Vgl. § 4d Abs. 5 BDSG.

Anwendung und auf das System protokolliert („wer hat wann mit welchen Mitteln was veranlasst bzw. worauf zugegriffen?“ und „wer hatte von wann bis wann welche Zugriffsrechte?“). Zusätzlich kontrolliert ein Monitoring die Verfügbarkeit der Systeme und informiert rechtzeitig über Unregelmäßigkeiten. Die Informationen der Systeme sind über festgelegte Mitarbeiter bei Bedarf auszuwerten und ggf. in geeignete Maßnahmen zu überführen.

### 4. Externe Kontrolle

Die externe Kontrolle der Einhaltung der datenschutzrechtlichen Bestimmungen obliegt den Aufsichtsbehörden für den Datenschutz, die entsprechend der gesetzlichen Vorgaben deutsches Datenschutzrecht (vgl. Pkt. 1 unter 14.14.4) oder das Datenschutzrecht des jeweiligen Sitzstaates anzuwenden haben. Die Zuständigkeit der deutschen Aufsichtsbehörden ergibt sich aus § 38 Abs. 1 S. 1 BDSG.

Die sachliche Zuständigkeit der Aufsichtsbehörde ergibt sich aus dem jeweiligen Landesdatenschutzgesetz bzw. dem Bundesdatenschutzgesetz. Die örtliche Zuständigkeit knüpft an den (deutschen) Sitz der verantwortlichen Stelle an.

Um die ergriffenen technisch-organisatorischen Maßnahmen zu verbessern, können verantwortliche Stellen ihre Verfahren und Anwendungen auch durch einen unabhängigen Auditor prüfen und bewerten lassen.

## 14.14.6 Integrität und Authentizität

Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.[25] Dieses Recht schließt die Gewährleistung der Unversehrtheit und der korrekten Funktionsweise von Systemen mit ein. Die Integrität der Daten ist gegeben, wenn die Daten vollständig und unverändert sind.[26]

Nutzer müssen sich also darauf verlassen können, dass die Informationen - ihre eigenen, aber auch die der anderen Nutzer - vollständig und richtig, d. h. nicht durch Dritte verändert, sind, es sei denn, dies ist eindeutig erkennbar. Nach der Anlage zu § 9 Satz 1 BDSG ist durch technische und organisatorische Maßnahmen sicherzustellen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung nicht verändert werden können. Zusätzlich muss durch die verantwortliche Stelle sichergestellt sein, dass die Systeme und Anwendungen korrekt funktionieren. Werden Sicherheitslücken oder bereits eingetretene Schadensfälle ent-

[25] 1 BvR 370/07, 1 BvR 595/07, http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html.
[26] https://www.bsi.bund.de/cln_174/DE/Themen/weitereThemen/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html

deckt, sind sofort Gegenmaßnahmen zu ergreifen und betroffene Nutzer umgehend darüber und über die ergriffenen Maßnahmen zu informieren. Der Umfang an personenbezogenen Daten in sozialen Netzwerken und deren teilweise hoher Schutzbedarf erfordern hohe Standards bei der IT-Sicherheit, um die Daten vor Missbrauch wie z. B. Identitätsdiebstahl zu schützen.

Eng verbunden mit dem Begriff der Integrität ist die Authentizität der Nutzer sowie der technischen Systeme. Personen oder Organisationen, die in die eigene Kontaktliste aufgenommen werden, haben oft einen weiter reichenden Zugriff auf die persönlichen Informationen. Ein Nutzer muss also erkennen können, wer hinter dem Profil steht. Private Nutzer haben das Recht, Telemedien anonym oder pseudonym zu nutzen, jedoch muss das Vortäuschen einer falschen Identität (Identitätsdiebstahl) ausgeschlossen werden. Hierfür muss die verantwortliche Stelle Maßnahmen ergreifen, um so gut wie möglich sicherzustellen, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Dies beinhaltet einerseits Sicherheitsmaßnahmen, um den Zugriff auf die Konten der Nutzer zu schützen (z. B. Zugriff nur über gesicherte Verbindungen, Passwortmindestanforderungen), aber auch Überwachungssysteme, um z. B. Missbrauch durch virtuelle Profile (sog. Social bots[27]) schnell zu erkennen und zu verhindern.

Lässt ein soziales Netzwerk zu, dass Organisationen, öffentliche Stellen oder Unternehmen Seiten im Netzwerk betreiben, sollte dies nur vertretungsberechtigten Personen erlaubt sein. Gibt ein Nutzer vor, im Namen von Organisationen, öffentlichen Stellen oder Unternehmen zu handeln, kann so das Vertrauen der Nutzer erschlichen werden, die der Organisation, der öffentlichen Stelle oder dem Unternehmen ggf. weiter reichenden Zugriff auf Informationen geben.

### 14.14.7 Vertraulichkeit

Soziale Netzwerke werden zu unterschiedlichen Zwecken von öffentlichen Stellen, insbesondere von Sicherheitsbehörden, genutzt. Informationen aus sozialen Netzwerken können für öffentliche Stellen etwa erforderlich sein, um Straftaten aufzuklären oder um Gefahren für die öffentliche Sicherheit zu erkennen und abzuwehren. Inwieweit ein Zugriff auf die Daten in sozialen Netzwerken zulässig ist, müssen die öffentlichen Stellen nach den für sie geltenden Rechtsvorschriften in eigener Verantwortung bewerten.

Betreiber sozialer Netzwerke sind nach deutschem Recht z. B. verpflichtet, beschlagnahmte Unterlagen nach § 98 StPO an Strafverfolgungsbehörden herauszugeben oder,

[27] http://www.heise.de/security/meldung/Studie-Viele-Facebook-Nutzer-sind-sorglos-1370431.html.

soweit sie Telekommunikationsdienste anbieten, nach § 100g StPO Auskunft über Verkehrsdaten zu erteilen.

Behörden erlangen Informationen nicht nur über Auskunftsersuchen an die Betreiber, sondern häufig durch eigene Recherchen in sozialen Netzwerken.

Es bestehen erhebliche datenschutzrechtliche Bedenken gegen eine Anwendung der Ermittlungsgeneralklauseln als Rechtsgrundlage für verdeckte Recherchen in nicht öffentlich zugänglichen Bereichen sozialer Netzwerke.

### 14.14.8 Verfügbarkeit

Die verantwortliche Stelle hat sicherzustellen, dass personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können. Dies bedeutet für Betreiber sozialer Netzwerke zunächst, dass die Daten gegen zufällige oder absichtliche Zerstörung und Verlust durch das Ergreifen von technischen und organisatorischen Maßnahmen geschützt werden müssen.[28] Weiter muss sichergestellt sein, dass Nutzer nicht nur jederzeit auf ihre personenbezogenen Daten zugreifen können, sondern auch die Verfügungsgewalt hierüber haben. Eine dritte Ebene betrifft die öffentliche Verfügbarkeit der Daten.

Zur Sicherstellung der technischen Verfügbarkeit muss die Infrastruktur durch den Betreiber so abgesichert sein, dass z. B. externe Einflüsse wie Feuer oder Wasser bestmöglich abgewehrt werden können, eine dauerhafte Stromversorgung gewährleistet ist und die Daten durch Backup-Konzepte vor Verlust geschützt sind.

Die Verfügbarkeit der Daten für Nutzer beinhaltet zunächst den Zugriff auf ihre personenbezogenen Daten in dem sozialen Netzwerk. Dies steht in direktem Zusammenhang mit der o. g. technischen Verfügbarkeit sowie mit den Zugriffsrechten auf die eigenen Daten. Inhaltsdaten müssen unter der direkten Kontrolle der Nutzer stehen, d. h. die Daten sind zur Bearbeitung und Löschung durch den Nutzer selbst verfügbar zu halten. Kündigt ein Nutzer sein Konto in dem sozialen Netzwerk, sollte die Möglichkeit bestehen, die dort gespeicherten (Inhalts-) Daten vor der Löschung zu exportieren (diese Möglichkeit kann auch ohne das Löschbegehren zu jedem Zeitpunkt zur Verfügung gestellt werden). Dies schließt neben Texten auch die Fotos und weitere Medien ein. Die exportierten Daten sollten in gängigen, wiederverwendbaren Formaten zur Verfügung gestellt werden.[29]

[28] Vgl. BDSG, Anlage zu § 9 Satz 1: Es sind „(…) sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind, (…) zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)."

[29] Geeignet wären etwa PDF oder XML.

Die öffentliche Verfügbarkeit von Profilen, d. h. die Sichtbarkeit von personenbezogenen Daten wie Profilname, Foto oder Geschlecht, erleichtert zwar das Auffinden der Person in dem sozialen Netzwerk, darf aber nicht außerhalb der Verfügungsgewalt der betroffenen Person stehen. Öffentlich zugängliche Daten - sowohl innerhalb des Netzwerks für registrierte Nutzer als auch außerhalb des Netzwerks, z. B. durch die Indexierung durch Suchmaschinen - erhöhen das Risiko eines Identitätsdiebstahls, so dass Nutzer zur Ausübung ihres Rechts auf informationelle Selbstbestimmung die Möglichkeit haben müssen, die Verfügbarkeit ihrer Daten gegenüber Dritten einzuschränken. Dabei ist angezeigt, dass die jeweils datenschutzfreundlichste Variante bereits seitens des Anbieters voreingestellt ist.

### 14.14.9 Intervenierbarkeit (Betroffenenrechte)

#### 1. Änderungen des Funktionsumfangs sozialer Netzwerke

Soziale Netzwerke sind komplexe Gebilde, welche einer stetigen Änderung unterworfen sind. Durch die Einführung neuer Funktionen können - möglicherweise unbeabsichtigt - Änderungen erfolgen, die sich enorm auf die Rechtevergabe auswirken.

Die Einhaltung der Prinzipien „Privacy by Design“ und davon abgeleitet „Privacy by Default“ wird daher von Daten- wie auch Verbraucherschützern beständig gefordert. „Privacy by Design“ setzt eine auf Datenschutzbelange Rücksicht nehmende Entwicklung von Produkten voraus. „Privacy by Default“ bedeutet in der Anwendung auf soziale Netzwerke, dass neue Nutzer beim Beitritt und bestehende Nutzer bei der Einführung neuer Funktionen eine selbstbestimmte Entscheidung treffen können, für wen welche Daten sichtbar oder gesperrt sind. Dies sollte zunächst nur der Nutzer selbst sein, welcher dann schrittweise sein Profil für weitere Personen oder Gruppen öffnen kann. Die dabei geltenden Regeln und Abläufe müssen transparent sein und sollten auf evtl. unbeabsichtigte Änderungen verständlich hinweisen. Die Nutzergruppen, welche Zugriff auf die Daten des Netzwerkes haben können, müssen klar benannt werden (z. B. Freunde, Freunde von Freunden, Nicht-Mitglieder, Suchmaschinen), um dem Nutzer einfache Entscheidungen zu ermöglichen. Werden die Nutzungsregeln für ein soziales Netzwerk geändert, muss dies transparent erfolgen und muss mit einer angemessenen Übergangsfrist bekanntgegeben werden. Weiterhin ist Nutzern die Möglichkeit einzuräumen, Änderungen abzulehnen (siehe hierzu auch Pkt. 3.1 unter 14.14.4).

Neue Funktionen dürfen niemals ohne aktive Änderungen der Einstelllungen durch den Nutzer zu einer Ausweitung des Umfangs der veröffentlichten Daten oder deren Sichtbarkeit innerhalb und außerhalb des Netzwerks führen.

## 2. Löschen

### 2.1 Löschen von Inhalten der Nutzer

Betreiber sozialer Netzwerke sind grundsätzlich verpflichtet, Löschungsbegehren der Nutzer in Bezug auf deren eigene personenbezogene Daten unverzüglich umzusetzen.

Das Löschen als technischer Prozess ist bei digitalen Verfahren ein mehrstufiger Prozess, der in der Regel für den Nutzer intransparent bleibt. Verteilte Dateisysteme führen teilweise zu Problemen, erteilte Löschbefehle physisch auszuführen, da die Daten an mehreren Orten physisch vorgehalten werden und einzelne Objekte mehrfach vorhanden sein können. Zudem können sich logische und rechtliche Grenzen bei solchen Daten ergeben, die zum Bestandteil der Profile anderer Nutzer geworden sind (z. B. durch Zitieren, Verweisen, „Liken“).

Zwar kann es im Interesse der Nutzer sein, die Daten für eine Wiederherstellung versehentlich gelöschter Daten noch kurzfristig vorzuhalten (vergleichbar mit einem Papierkorb); die sich daran anschließende Löschung muss jedoch sicher und endgültig erfolgen. Insbesondere muss ein Netzwerkbetreiber zuverlässige und überprüfbare Aussagen darüber treffen, wann zur Löschung vorgesehene Daten endgültig vernichtet sind.

Netzwerkbetreiber sollten außerdem die Möglichkeit vorsehen, personenbezogene Daten, die zum Gegenstand der Profile anderer Nutzer geworden sind, zu entfernen. Betreiber können jedoch die Löschung begrenzen, wenn dadurch die Wahrnehmung berechtigter und gesetzlich anerkannter Interessen, z. B. die Wahrnehmung der Meinungsfreiheit, der jeweiligen Profilinhaber beeinträchtigt werden. Die Grenzen der Löschung sind gegenüber den Nutzern transparent zu machen.

### 2.2 Verfallsdaten von Inhalten der Nutzer

Bereits längere Zeit wird über das „Gedächtnis des Internets“ und die Wiederauffindbarkeit von Informationen, die zum Teil schon lange zurückliegen, diskutiert. Die derzeitige Generation der Nutzer sozialer Netzwerke wird im Alter ein mehr oder weniger vollständiges digitales Abbild ihrer selbst im Netz vorfinden.[30] Vor dem Hintergrund der stetig voranschreitenden technischen und analytischen Möglichkeiten ruft dies nachvollziehbare Ängste hervor.

Die Frage nach Verfallsdaten, automatischen Löschroutinen und Sperrungen stellt sich insbesondere im Kontext der sozialen Netzwerke. Es gibt erste technische Ansätze zur

[30] Vgl. BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V., Studie Soziale Netzwerke - zweite, erweiterte Studie, http://www.bitkom.org/files/documents/BITKOM_Publikation_Soziale_Netzwerke_zweite_Befragung.pdf.

automatisierten Löschung von Daten[31], die sich jedoch bisher auch noch nicht genug praxistauglich erwiesen haben.[32]

In erster Linie sind die Betreiber gefordert, entsprechende Funktionen einzuführen und nutzerfreundlich zu gestalten. Hierbei sind verschiedene Modelle denkbar, angefangen von Standardfragen bei der Veröffentlichung von Beiträgen nach deren vorgesehener Gültigkeitsdauer bis hin zu einfach zu bedienenden Löschroutinen. Denkbar ist auch, die öffentliche Zugänglichkeit von Profildaten zeitlich zu begrenzen.

Weiterhin ist angesichts neuerer technischer Entwicklungen, z. B. auf Basis von HTML5[33] oder IPv6[34], zu prüfen, inwieweit damit mehr Selbstkontrolle über Nutzerdaten bzw. eine Aufweichung der bestehenden Kunden-Contentprovider-Strukturen möglich ist.

## 2.3 Abmeldung von einem sozialen Netzwerk

Die Abmeldung aus einem sozialen Netzwerk muss einfach und endgültig möglich sein. Die von einzelnen Netzwerken geübte Praxis, Profile in einen „Ruhezustand“ zu versetzen, um dem Nutzer eine spätere Rückkehr zu ermöglichen, ist unzureichend. Der Nutzer muss eine vollständige Kontrolle über seine Daten erlangen und selbst bestimmen können, wie mit seinen Daten verfahren wird. Dabei kann grob zwischen endgültiger Abmeldung (und damit einhergehender Löschung), Ruhezustand (und Nichtsichtbarkeit für Dritte) und einer Mitnahme der Daten (mit anschließender Löschung beim Betreiber) unterschieden werden. In diesen Fällen sind folgende Anforderungen zu erfüllen:

- Der Nutzer sollte eine explizite Löschbestätigung anfordern können, indem der Betreiber eine Löschung in Textform zusichert.
- Die Effektivität der Löschroutinen oder anlassbezogenen Löschungen sollten durch den Betreiber mittels entsprechender allgemein zugänglicher Dokumentation nachgewiesen werden.
- Die Betreiber haben transparent über die Aufbewahrungsfristen für inaktive Accounts zu informieren.

[31] Vgl. Saarland University - Information Security and Cryptography Group - Prof. Dr. Michael Backes, X-pire! - Wie man dem Internet das „Vergessen“ beibringt, http://www.infsec.cs.uni-saarland.de/ projects/forgetful-internet/.
[32] Vgl. Universität Regensburg, Lehrstuhl Wirtschaftsinformatik 4 - Management der Informationssicherheit, Fakultät für Wirtschaftswissenschaften, Prof. Dr. Hannes Federrath, Digitaler Radiergummi und seine Folgen, http://www-sec.uni-regensburg.de/research/streusand/.
[33] Vgl. Konrad Lischka, Hier liest Facebook nicht mit, SPIEGEL ONLINE, http://www.spiegel.de/netzwelt/web/0,1518,825950,00.html.
[34] Vgl. Lutz Donnerhacke, Kommentar: IPv6 und der Datenschutz, heise online, http://www.heise.de/netze/artikel/Kommentar-IPv6-und-der-Datenschutz-1375692.html.

### 3. Auskunft an Betroffene

Betreiber sozialer Netzwerke sind zur (vollständigen) Auskunft nach § 34 BDSG bzw. § 13 Abs. 7 TMG verpflichtet.

Für Auskunftsersuchen hat der Betreiber eine einfach zu erreichende Kontaktmöglichkeit innerhalb des Netzwerks einzurichten. Um Missbrauch zu verhindern, müssen Auskunftsersuchen angemessen sicher autorisiert werden, z. B. durch eine Bestätigungsmail an die für das Nutzerprofil registrierte E-Mail-Adresse. Der Nutzer muss die Form der Auskunft (in Textform/elektronisch) wählen können.

Eine Auskunft muss Inhalts-, Bestands- und Nutzungsdaten vollständig umfassen. Inhalts- und Bestandsdaten sind dabei die im Netzwerk hinterlegten persönlichen Daten, Kommunikationen, Bilder und Videos. Nutzungsdaten umfassen das Logging des Nutzers, also welche Seiten des sozialen Netzwerks oder externer Quellen, die über Social Plug-ins mit dem Netzwerk verbunden sind, er besucht hat, wann und wie er sich ein- oder ausgeloggt hat oder welche Anfragen ihn innerhalb des Netzwerks erreicht haben. Ebenfalls vom Auskunftsrecht umfasst sind Nutzungsdaten, durch die der Nutzer auch nach dem Ausloggen für das Netzwerk identifizierbar bleibt, z. B. über ein Cookie oder das Browserprofil. Weiterhin sollten einfache Möglichkeiten des Downloads von eigenen Profilen etabliert werden. Der Entwurf der neuen EU-Datenschutzgrundverordnung sieht ein solches Prinzip der Datenportabilität als Recht der informationellen Selbstbestimmung der Nutzer vor.

Auch Nicht-Nutzern ist ein Recht auf Auskunft zu den über sie gespeicherten personenbezogenen Daten einzuräumen. Dafür müssen Betreiber sozialer Netzwerke transparent darstellen, in welcher Weise Daten von Nicht-Nutzern erhoben und verarbeitet werden, z. B. durch den Abgleich von Adressbüchern von Mitgliedern, welche auch Daten von Nicht-Mitgliedern enthalten können.

## 14.14.10 Einzelthemen

### 1. Zugriff auf Adressen

Häufig werden von den Betreibern Funktionen angeboten, die es dem Nutzer ermöglichen, ein auf dem Gerät (PC, Smartphone) gespeichertes oder bei einem E-Mail-Provider geführtes Adressbuch dem sozialen Netzwerk vollständig zur Verfügung zu stellen (sog. Friend-Finding).

Hierbei ist neben der expliziten Einwilligung des Nutzers eine Möglichkeit zur Vorabprüfung der Adressen und zur Sperrung von Einzeladressen durch den Nutzer vor der

Übertragung notwendig. Eine automatische Übertragung aller Adressen eines Nutzers an ein soziales Netzwerk ist nicht zulässig. Der Nutzer hat die Verantwortung für die Daten der betroffenen Dritten. Er muss erkennen können, welche Adressen übertragen wurden und muss diese bei Bedarf löschen können.

Besondere Risiken bestehen beim Hochladen beruflich erlangter Kontaktdaten in ein Profil eines Sozialen Netzwerks, z. B. wenn Ärzte oder Psychotherapeuten Kontaktdaten ihrer Patienten bzw. Klienten dafür freigeben und diese dann auf einmal z. B. Freundschaftsanfragen an ihre dortigen Profile übermittelt bekommen. Auf diese Risiken sollten Betreiber Sozialer Netzwerke hinweisen.

Eine Nutzung der Adressdaten durch den Betreiber eines Sozialen Netzwerks für eigene Zwecke im Rahmen der Werbung für den Beitritt zum eigenen Netzwerk (Friend-Finding) ist nur mit Einwilligung der Betroffenen zulässig.

## 2. Biometrie

Der Einsatz biometrischer Verfahren im Rahmen sozialer Netzwerke erfordert besondere Rahmenbedingungen. Von praktischer Bedeutung ist dabei vor allem das Verfahren der Gesichtserkennung, welches die automatische Markierung von Personen auf in das soziale Netzwerk hochgeladenen Bildern erlaubt.

Die Erstellung, Speicherung und weitere Verwendung biometrischer Daten erfordert die vorherige, explizite Einwilligung der Betroffenen. Diese Einwilligung kann nur auf der Basis einer umfassenden Information der Betroffenen über die Art und Weise der Verwendung der entsprechenden persönlichen Daten in diesem Zusammenhang erfolgen (informierte Einwilligung).

Betreiber eines sozialen Netzwerks dürfen lediglich die Daten registrierter Nutzer, deren entsprechende Einwilligung vorliegt, verarbeiten. „No matches“, also personenbeziehbare biometrische Daten, die keinem Nutzer des sozialen Netzwerkes zuzuordnen sind, müssen unverzüglich und irreversibel gelöscht werden. Neue, nachträgliche Erkennungs- bzw. Zuordnungsvorgänge („Matchingläufe“), etwa über den Bestand nicht identifizierter Personen, sind nicht zulässig. Ein biometrischer Abgleich eines neuen Mitglieds (oder nach der Einwilligung eines Mitglieds) mit dem bisherigen, kompletten Datenbestand des sozialen Netzwerkes darf nicht erfolgen.

Nur unter den soeben genannten Bedingungen ist die Einholung einer Einwilligung zur Erstellung temporärer biometrischer Daten entbehrlich. Nach Erstellung des temporären Templates muss durch den Betreiber geprüft werden, ob eine Einwilligung in die dauerhafte Speicherung des Templates vorliegt. Ist dies nicht der Fall, muss nach den

beschriebenen Bedingungen eine Löschung vorgenommen werden. Die Erfüllung dieser Anforderung ist durch eine entsprechende Dokumentation nachzuweisen.

Die Möglichkeit zur jederzeitigen Rücknahme der Einwilligung ist sicherzustellen; die sich daraus ergebenen Konsequenzen müssen technisch umgesetzt werden. Das Referenztemplate muss gelöscht und dessen Verknüpfung bzw. Zuordnung über den gesamten Datenbestand des sozialen Netzwerkes aufgelöst werden.

Für die Übermittlung biometrischer Daten durch den Betreiber des sozialen Netzwerkes an Dritte oder die Nutzung für andere Dienste ist eine entsprechende weitergehende Einwilligung beim Betroffenen erforderlich (informierte Einwilligung).

Es ist technisch und organisatorisch sicherzustellen, dass die biometrischen Daten ausschließlich für die Zwecke genutzt werden, für die sie auch erhoben wurden und denen die Betroffenen im Rahmen ihrer Einwilligung zugestimmt haben.

Bei der Aufnahme und der Übertragung der Bilder (Upload) sind verschlüsselte Kommunikationswege zu nutzen. Dies gilt insbesondere dann, wenn die biometrischen Algorithmen im Endgerät der Nutzer ablaufen und die Ergebnisse dieser Verfahren mit zentralen Datenbanken abgeglichen werden.[35]

### 3. Werbung

Im Hinblick auf Bestandsdaten (zum Begriff siehe Pkt. 2.2 unter 14.14.4) sieht das einschlägige TMG keine andere gesetzliche Grundlage für eine Verwendung zum Zweck der Werbung als die Einwilligung der Nutzenden vor. Gleiches gilt für die Nutzungsdaten (zum Begriff siehe Pkt. 2.3 unter 14.14.4), jedenfalls wenn diese nicht lediglich unter einem Pseudonym zusammengeführt werden (siehe unten Pkt. 4 Reichweitenanalyse). Im Hinblick auf die nach dem BDSG zu beurteilenden Inhaltsdaten ist insbesondere für Werbung auf der Basis von Profildaten nach § 3 Abs. 9 BDSG - dies sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben - eine informierte Einwilligung der Betroffenen erforderlich.

### 4. Reichweitenanalyse

Betreiber sozialer Netzwerke, vor allem diejenigen, die eine Finanzierung des Angebotes über Werbeeinnahmen durchführen, betreiben Reichweitenanalysen, mittels derer

[35] Vgl. auch Working Paper 192 der Art. 29-Gruppe, Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten, vom 22. März 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_de.pdf.

die Art und Weise der Nutzung des Dienstes sowie die Interessen und Vorlieben der Nutzer festgestellt, analysiert und ausgewertet werden können.

Durch eine derartige Reichweitenanalyse werden umfangreiche und sehr detaillierte Aussagen über die Nutzerinnen und Nutzer durch die Betreiber erhoben, die umfangreiche und sehr detaillierte Aussagen über die Nutzer erlauben, die über die willentlich und bewusst angegebenen Informationen hinausgehen. Die Nutzer sollten grundsätzlich selbst in die Lage versetzt werden, die Datenverarbeitung in ihren Geräten zu steuern. Letzteres ist z. B. durch den Einsatz von Browser-Plug-ins realisierbar. Dadurch kann z. B. das Speichern von Cookies oder Ausführen von JavaScript-Programmen unterbunden werden.

Der Umfang und die Art der Daten der Reichweitenanalyse kann von der Verarbeitung rein technischer Angaben, wie z. B. des genutzten Betriebssystems bis hin zu einer detaillierten Erfassung der Mouse-Aktivitäten eines einzelnen Nutzers reichen. Auch der Fokus der Analyse kann unterschiedlich sein. Einige Anbieter können durch den Einsatz von Social Plug-ins nicht nur die Nutzung des eigenen Dienstes analysieren. Auch die Nutzung anderer Angebote des Internets durch die in dem jeweiligen Netzwerk angemeldeten Nutzer wird analysiert.

Unabhängig von der technischen Art und Weise der eingesetzten Reichweitenanalyse ist diese nur zulässig, wenn sie auf einer entsprechenden rechtlichen Grundlage beruht. Als gesetzliche Rechtsgrundlage kommt § 15 Abs. 3 TMG zur Anwendung. Danach ist die Analyse der Nutzung des angebotenen Dienstes oder darüber hinaus zur

- Werbung,
- Marktforschung oder
- bedarfsgerechten Gestaltung des eigenen Dienstes

zulässig. Die Wahrung dieser Voraussetzung ist durch den Betreiber des Netzwerkes nachzuweisen. Dies gilt insbesondere in den Fällen, in denen die Analyse des Nutzungsverhaltens über das eigene Angebot hinausreicht. Eine anbieterübergreifende Reichweitenanalyse kann nicht auf § 15 Abs. 3 TMG gestützt werden und bedarf regelmäßig der Einwilligung der Nutzenden.

Die Reichweitenanalyse muss den Nutzern kenntlich gemacht werden. Ihnen ist außerdem gemäß § 15 Abs. 3 TMG die Möglichkeit einzuräumen, der Erhebung, Verarbeitung und Nutzung der Informationen über die Nutzung des Dienstes oder anderer Angebote des Internets widersprechen zu können. Auf das Widerspruchsrecht sind die Nutzer hinzuweisen.

Die Erstellung der Nutzungsprofile ist nur bei Verwendung von Pseudonymen zulässig. Die IP-Adresse ist kein Pseudonym i. S. d. § 15 Abs. 3 TMG.[36] Betreiber haben daher sicherzustellen, dass die Pseudonyme nicht aus leicht reidentifzierbaren Daten bestehen.

Gemäß Art. 5 Abs. 3 der E-Privacy-Richtlinie muss der Nutzer bei Cookies, die nicht zur Erbringung eines Dienstes erforderlich sind, vor deren Speicherung seine Einwilligung erteilt haben. Diese Regel ist bei Cookies, die zur Reichweitenanalyse genutzt werden, anwendbar.

Betreiber sozialer Netzwerke sind, anders als andere Anbieter von anmeldefreien Internetdiensten, zumeist sehr einfach in der Lage, die unter Pseudonym erstellten Nutzungsprofile einzelnen Nutzern zuzuordnen. Eine derartige Verknüpfung zwischen den von den Nutzern erstellten Profilen und den durch den Betreiber erstellten Nutzungsprofilen ist nur zulässig, wenn die Betroffenen vorher eingewilligt haben. Die Einwilligung muss den Anforderungen des § 4a BDSG bzw. § 13 Abs. 2 TMG entsprechen.

Eine Zusammenführung dieser Angaben ohne die Einwilligung der Nutzer ist unzulässig und stellt einen Bußgeldtatbestand dar.

Für Themennetzwerke, die für besondere Nutzergruppen eingerichtet wurden, können Beschränkungen hinsichtlich der grundsätzlichen Zulässigkeit der Nutzungsanalyse bestehen. So unterliegen aufgrund des hohen Schutzbedarfes besonderer personenbezogener Daten (§ 3 Abs. 9 BDSG) soziale Netzwerke zu den Themen Gesundheit, sexuelle Orientierung, politische oder religiöse Anschauungen etc., gesonderten und besonderen Rechtfertigungsanforderungen hinsichtlich der Durchführung der Reichweitenanalyse. Die Erforschung und Auswertung des Nutzerverhaltens ist nur auf der Grundlage einer Einwilligung zulässig. Gleiches gilt für soziale Netzwerke ohne unmittelbaren thematischen Bezug zu besonderen personenbezogenen Daten bei denen derartige Daten zum Zweck der Reichweitenanalyse genutzt werden. Auch hier ist eine gesonderte Einwilligung erforderlich.

## 5. Nutzung auf mobilen Endgeräten

Die Verwendung eines sozialen Netzwerks auf einem mobilen Gerät unterscheidet sich in einigen Punkten wesentlich von der Verwendung mit einem Webbrowser, wenn spezielle Apps oder eine Integration von (mehreren) sozialen Netzwerken in das Betriebssystem des mobilen Gerätes zum Einsatz kommen. Die grundsätzlichen Funktionalitäten wie Kontakte knüpfen und pflegen, Nachrichten austauschen und Bilder und Fotos teilen, sind auf mobilen Geräten wie Smartphones oder Tablets ebenfalls vorhanden.

[36] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 26./27. November 2009 in Stralsund, http://www.informationsfreiheit-mv.de/dschutz/beschlue/Analyse.pdf.

Darüber hinaus sind Lokalisierungsdaten über den eigenen Aufenthaltsort sowie ggf. die Standorte anderer Teilnehmer des sozialen Netzwerks verfügbar.

## 5.1 Umgang mit Lokalisierungsdaten

Mobile Endgeräte verfügen üblicherweise über Ortungsdienste, welche mit GPS sowie durch Informationen aus WLAN-Hotspots und Mobilfunkmasten realisiert werden. Sollen diese standortbezogenen Daten an ein soziales Netzwerk übertragen werden, wird eine Einwilligung des Nutzers benötigt, soweit dies nicht für die Erbringung der jeweiligen Dienstleistung erforderlich ist. Die Voreinstellung dieser Datenübertragung sollte derart sein, dass keine Daten übertragen werden. Sollen die Standortdaten allen Personen eines sozialen Netzwerks zugänglich gemacht werden, dann ist eine eindrückliche Warnung an den Nutzer erforderlich. Alle Einstellungen zur Lokalisierung sollten über einen leicht auffindbaren Menüpunkt klar erkennbar und jederzeit änderbar sein. Eine Deaktivierung Nutzung und Löschung der Standortdaten muss jederzeit leicht möglich sein; eine Deaktivierung aller Ortungsdienste des Gerätes ist hierfür nicht ausreichend.

Die fortlaufende Speicherung von Aufenthaltsinformationen im Sinne einer Historie ist nur gestattet, solange und soweit dies für die Erbringung einer Dienstleistung erforderlich ist. Nutzer sind über evtl. existierende Datenbestände historischer Aufenthaltsinformationen im Rahmen der Information nach § 13 Abs. 1 TMG zu unterrichten. Sie sollten darüber hinaus jederzeit die Möglichkeit haben, Aufenthaltshistorien zu löschen.

## 5.2 Übertragung

Personenbezogene Daten dürfen nur an den Betreiber des sozialen Netzwerks übertragen werden. Eine Übermittlung dieser Daten an andere Empfänger (wie den Hersteller der App-Software) ist im Allgemeinen nicht erforderlich und damit auch nicht zulässig. Sollten doch Diagnose- oder Trackingdaten zusätzlich erfasst werden, so muss hierzu die explizite Einwilligung des Nutzers eingeholt oder sämtliche personenbezogenen Daten vor der Übertragung i. S. d. § 3 Abs. 6 BDSG anonymisiert werden.

Eine Übertragung der Daten muss über eine ausreichend verschlüsselte Verbindung (SSL/TLS) erfolgen und gegen unberechtigte Zugriffe (Man-In-The-Middle-Angriffe) geschützt sein.

## Literatur

[1] Recommendation CM/Rec(2012)4 of the Committee of Ministers to Member States on the protection of human rights with regard to social networking services, https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec%282012%294&Language=lanEngl

ish&Ver=original&Site=CM&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864#RelatedDocuments

[2] Selbstbedienungsladen Smartphone: Apps greifen ungeniert persönliche Daten ab, http://www.heise.de/ct/artikel/Selbstbedienungsladen-Smartphone-1464717.html

[3] Data Protection Commissioner of Ireland: Facebook Ireland Ltd Report of Audit, http://dataprotection.ie/documents/Facebook%20Report/Facebookauditreport1.pdf

[4] Data Protection Commissioner of Ireland: Facebook Technical Analysis Report, http://dataprotection.ie/documents/Facebook%20Report/report.pdf/appendices.pdf

[5] Data Protection Commissioner of Ireland: Facebook Ireland Ltd Report of Re-Audit, http://dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf

[6] Tao Stein et al.: Facebook Immune System, http://allfacebook.de/wp-content/uploads/2011/10/FacebookImmuneSystem.pdf

[7] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 08. Dezember 2011): Datenschutz in sozialen Netzwerke, http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/08122011DSInSozialenNetzwerken.pdf?__blob=publicationFile

[8] Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 17./18. April 2008 in Wiesbaden: Datenschutzkonforme Gestaltung sozialer Netzwerke, http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/170408DatenschutzkonformeGestaltungSozNetzwerke.pdf?__blob=publicationFile

[9] Artikel-29-Datenschutzgruppe: Stellungnahme 5/2009 zur Nutzung sozialer Online-Netzwerke (WP 163), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_de.pdf

[10] International Working Group on Data Protection in Telecommunications: Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten - „Rom Memorandum“ - 43. Sitzung, 3.-4. März 2008, http://www.datenschutz-berlin.de/attachments/470/675.36.13.pdf

[11] Berliner Beauftragter für Datenschutz und Informationsfreiheit: ICH SUCHE DICH. Wer bist du? Soziale Netzwerke & Datenschutz, Juli 2012, http://www.datenschutz-berlin.de/attachments/894/2012-Broschuere-Soziale-Netzwerke.pdf

[12] Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit: selbst & bewusst. Tipps für den persönlichen Datenschutz bei Facebook, Januar 2013, http://www.datenschutz-hamburg.de/uploads/media/selbst_bewusst-Datenschutz_bei_Facebook_01.pdf

[13] Datenschutzbeauftragter des Kantons Zürich: Checkliste Privacy Facebook, November 2012, https://dsb.zh.ch/internet/datenschutzbeauftragter/de/ueber_uns/veroeffentlichungen/leitfaeden_und_checklisten/_jcr_content/contentPar/publication_1/publicationitems/titel_wird_aus_dam_e/download.spooler.download.1355402195455.pdf/Checkliste+Privacy+Facebook.pdf

**Abkürzungen**

| | |
|---|---|
| AGB | Allgemeine Geschäftsbedingungen |
| API | Application Programming Interface |
| BDSG | Bundesdatenschutzgesetz |
| BGB | Bürgerliches Gesetzbuch |
| CAPTCHA | Completely Automated Public Turing test to tell Computers and Humans Apart |
| FAQ | Frequently Asked Questions |
| GG | Grundgesetz |
| GPS | Global Positioning System |
| HDFS | Hadoop Distributed File System |
| HTML | Hyptertext Markup Language |
| IP | Internet Protocol |
| KUG | Kunsturhebergesetz |
| LDSG | Landesdatenschutzgesetz |
| LSO | Local Shared Object |
| RL | Richtlinie |
| SSL | Secure Sockets Layer |
| stopp | Strafprozessordnung |
| TLS | Transport Layer Security |
| TMG | Telemediengesetz |
| WLAN | Wireless Local Area Network |

# 15 Vortrags- und Schulungstätigkeit für behördliche Datenschutzbeauftragte

## 15.1 Datenschutz- und IT-Sicherheit in sächsischen Kommunen

Gemeinsam führten die KISA, die KDN GmbH und meine Behörde den Informationstag „Datenschutz und IT-Sicherheit in sächsischen Kommunen“ in der Veranstaltungshalle des Kleinbahnhofs Wilsdruff durch.

Bei der erfolgreichen Veranstaltung, an der behördliche Datenschutzbeauftragte und IT-Sicherheitsbeauftragte von ungefähr achtzig Gemeinden teilnahmen, wurden zwölf Fachvorträge zu aktuellen und wichtigen Themen der Informationssicherheit und des Datenschutzes präsentiert, darunter Referate zu den Aufgaben und Erfahrungen eines IT-Sicherheitsbeauftragten, der Musterleitlinie Informationssicherheit, Erfahrungen zur Herangehensweise bei Informationssicherheitsprojekten und zu aktuellen Bedrohungen und Gefahren in sozialen Netzwerken und dem Internet. Weitere Themen waren u. a. die Zulässigkeit und Grenzen der Videoüberwachung durch Kommunen im öffentlichen Raum, die Bestellung externer Datenschutzbeauftragter und die Anfertigung von Verfahrensverzeichnissen. Relevant, aber in der behördlichen Praxis häufig nur unzureichend beachtet, werden Fragen der Archivierung und des Datenschutzes. Informationen eines referierenden Vertreters des Sächsischen Hauptstaatsarchivs dazu waren hilfreich.

Zwischen den Vorträgen hatten die Teilnehmer Gelegenheit, interessierende Themen zu Datenschutz und IT-Sicherheit untereinander und mit den Referenten zu diskutieren und Erfahrungen auszutauschen.

Die Veranstaltungsreihe soll im Jahr 2013 durch meine Behörde gemeinsam mit der KISA und der KDN GmbH zu aktuellen Themen fortgesetzt werden.

# 16 Ordnungswidrigkeitenverfahren

## 16.1 Übersicht

*Der Sächsische Datenschutzbeauftragte ist zuständig für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 38 SächsDSG (§ 38 Abs. 3 Satz 1 SächsDSG). Seit März 2012 ist er außerdem auch für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach § 85 SGB X zuständig (§ 85 SGB X i. V. m. § 13 OwiZuVO).*

Im Berichtszeitraum sind durch meine Behörde 95 Ordnungswidrigkeitenverfahren abgeschlossen worden.

Es handelte sich zum größten Teil um Verfahren zur Ahndung von Verstößen nach § 38 Abs. 1 Nr. 1 SächsDSG, 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.

Zum überwiegenden Teil betrifft dies von den Betroffenen nicht dienstlich veranlasste Abrufe personenbezogener Daten in ihnen ausschließlich für dienstliche Zwecke zur Verfügung stehenden, nicht allgemein zugänglichen, elektronischen Informationssystemen bzw. die unerlaubte Verarbeitung personenbezogener Daten in diesem Zusammenhang. Die Handlung des unbefugten Abrufs bzw. der unbefugten Verarbeitung personenbezogener Daten durch eine für eine öffentliche Stelle tätige Person stellt in der Regel auch gleichzeitig eine Ordnungswidrigkeit nach § 38 Abs. 1 Nr. 3 SächsDSG dar, da diese personenbezogenen Daten auch dem Datengeheimnis gemäß § 6 SächsDSG unterliegen.

In 77 dieser Verfahren sind zur Ahndung der Verstöße Bußgeldbescheide gegen die Betroffenen erlassen worden bzw. wurde ein Verwarngeld verhängt. Davon sind 16 Verfahren nach eingelegtem Einspruch gegen den Bußgeldbescheid dem zuständigen Amtsgericht vorgelegt worden. Zwei Verfahren wurden durch das jeweilige Amtsgericht eingestellt, in 14 Fällen steht eine Entscheidung noch aus.

17 Verfahren sind durch meine Behörde von Amts wegen eingestellt worden. Ein Verfahren wurde wegen Verstoßes gegen das Bundesdatenschutzgesetz an die zuständige Behörde abgeben.

Die Summe der rechtskräftigen Buß- und Verwarngelder belief sich auf insgesamt 17.485 €. Der starke Anstieg dieser Summe im Vergleich zum vergangenen Berichts-

zeitraum ist auf den Anstieg der Meldungen der einzelnen ordnungswidrigen Handlungen und deren konsequente Verfolgung zurückzuführen.

Bemerkenswert ist, dass es sich dabei häufig um Verfahren gegen Bedienstete der sächsischen Polizei handelte. Bereits in den vergangenen Jahren regte ich eine intensivere Belehrung sächsischer Polizeibeamter über den Datenschutz im Zusammenhang mit der Nutzung polizeilicher Datenbanken an, was durch das SMI dankenswerter Weise auch umgesetzt wurde und durch die einzelnen Polizeidienststellen durchgeführt wird (vgl. 15/5.9.4 und 5.9.1). Die Situation zeigt jedoch, dass offenbar unter den Beamten immer noch die von mir bereits geschilderte Unsicherheit hinsichtlich der zulässigen Nutzung polizeilicher Datenbanken besteht. Ich gehe jedoch fest davon aus, dass durch die inzwischen verstärkte Belehrung und die konsequente Verfolgung derartiger Verstöße zukünftig mit dem Einsetzen eines Lernprozesses und somit einer Verbesserung zu rechnen ist.

Neben der Verletzung des Rechts auf informationelle Selbstbestimmung der betroffenen Personen sind Verstöße gegen datenschutzrechtliche Bestimmungen nach wie vor in hohem Maße geeignet, das Vertrauen der Allgemeinheit in die Rechtmäßigkeit des Umganges mit personenbezogenen Daten durch den Polizeivollzugsdienst zu beeinträchtigen.

Hinsichtlich der bei Gericht anhängigen Verfahren bestehen für mich als Verwaltungsbehörde, trotz des Übergehens der Verfahrensherrschaft von der Verwaltungsbehörde auf die Staatsanwaltschaft, gewisse Einflussnahmemöglichkeiten (vgl. 15/11.3), die ich im Berichtszeitraum noch stärker nutzte. Dies betrifft insbesondere Besprechungen mit den Staatsanwaltschaften über inhaltliche datenschutzrechtliche Fragen und die regelmäßige Teilnahme an den Hauptverhandlungen, um meine besondere Sachkunde zur Verfügung zu stellen und eine gleichmäßige Behandlung meiner Belange zu erwirken. Nach wie vor ungünstig wirkt sich in diesem Zusammenhang der Umstand aus, dass die Zuständigkeit zur Entscheidung über den Einspruch gegen einen Bußgeldbescheid im Jahr 2008 vom bis dahin zuständigen Amtsgericht Dresden (Amtsgericht am Sitz der Verwaltungsbehörde) auf die Amtsgerichte am jeweiligen Begehungsort übergegangen sind. Die einzelnen Amtsgerichte sind mit datenschutzrechtlichen Ordnungswidrigkeitenverfahren nur selten befasst, die Bearbeitung derartiger Einsprüche ist dementsprechend aufwändig und es fehlt - verständlicherweise - oftmals an entsprechenden Erfahrungswerten. Umso wichtiger ist es für mich, die mir per Gesetz eingeräumten Einflussnahmemöglichkeiten nicht ungenutzt zu lassen.

# 17 Materialien

## 17.1 Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

### 17.1.1 Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München: Antiterrorgesetze zehn Jahre nach 9/11 - Überwachung ohne Überblick

In der Folge der Anschläge vom 11. September 2001 wurden der Polizei, den Strafverfolgungsbehörden und den Nachrichtendiensten zahlreiche neue Befugnisse eingeräumt, die sich durch eine große Streubreite auszeichnen und in die Grundrechte zahlreicher Bürgerinnen und Bürger eingreifen. Zunehmend werden Menschen erfasst, die nicht im Verdacht stehen, eine Straftat begangen zu haben oder von denen keine konkrete Gefahr ausgeht. Unbescholtene geraten so verstärkt in das Visier der Behörden und müssen zum Teil weitergehende Maßnahmen erdulden. Wer sich im Umfeld von Verdächtigen bewegt, kann bereits erfasst sein, ohne von einem Terrorhintergrund oder Verdacht zu wissen oder in entsprechende Aktivitäten einbezogen zu sein.

Zunehmend werden Daten, z. B. über Flugpassagiere und Finanztransaktionen, in das Ausland übermittelt, ohne dass hinreichend geklärt ist, was mit diesen Daten anschließend geschieht (vgl. dazu Entschließung der 67. Konferenz vom 25./26. März 2004 „Übermittlung von Flugpassagierdaten an die US-Behörden“; Entschließung der 78. Konferenz vom 8./9. Oktober 2009 „Kein Ausverkauf von europäischen Finanzdaten an die USA!“).

Das Bundesverfassungsgericht hat in seinem Urteil zur Vorratsdatenspeicherung von Telekommunikationsdaten vom 2. März 2010 (1 BvR 256/08) klargestellt: Es gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Die Verfassung fordert vielmehr ein austariertes System, bei dem jeder Eingriff in die Freiheitsrechte einer strikten Prüfung seiner Verhältnismäßigkeit standhält.

Von einem austarierten System der Eingriffsbefugnisse kann schon deshalb keine Rede sein, weil die Wechselwirkungen zwischen den verschiedenen Eingriffsinstrumentarien nie systematisch untersucht worden sind. Bundesregierung und Gesetzgeber haben bislang keine empirisch fundierten Aussagen vorgelegt, zu welchem Überwachungs-Gesamtergebnis die verschiedenen Befugnisse in ihrem Zusammenwirken führen. Die bislang nur in einem Eckpunktepapier angekündigte Regierungskommission zur Überprüfung der Sicherheitsgesetze ersetzt die erforderliche unabhängige wissenschaftliche Evaluation nicht.

Viele zunächst unter Zeitdruck erlassene Antiterrorgesetze waren befristet worden, um sie durch eine unabhängige Evaluation auf den Prüfstand stellen zu können. Eine derartige umfassende, unabhängige Evaluation hat jedoch nicht stattgefunden. Dies hat die Bundesregierung nicht davon abgehalten, gleichwohl einen Entwurf für die Verlängerung und Erweiterung eines der Antiterrorpakete in den Gesetzgebungsprozess einzubringen (BT-Drs. 17/6925).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher erneut, die Auswirkungen der bestehenden Sicherheitsgesetze - gerade in ihrem Zusammenwirken - durch eine unabhängige wissenschaftliche Evaluierung (so bereits die Entschließung der 79. Konferenz vom 17./18. März 2010 „Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich“) zu untersuchen. Die Wirksamkeit der Regelungen, ihre Erforderlichkeit für den gesetzgeberischen Zweck und ihre Angemessenheit, insbesondere im Hinblick auf die Bedrohungslage sowie die Auswirkungen für die Betroffenen müssen vor einer weiteren Befristung endlich kritisch überprüft werden.

### 17.1.2 Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München: Datenschutz als Bildungsaufgabe

Ein großer Teil der wirtschaftlichen, gesellschaftlichen und persönlichen Aktivitäten findet mittlerweile im Internet statt. Millionen von Bürgerinnen und Bürgern nutzen seine Möglichkeiten und gehen dabei auch besondere Risiken ein, ohne dass ihnen dies immer bewusst wäre. Dies gilt insbesondere für Kinder und Jugendliche, aber auch erwachsene Internetnutzerinnen und -nutzer werden von der digitalen Welt zunehmend überfordert.

Vielen sind die Grundlagen, Funktionsbedingungen und wirtschaftlichen Spielregeln des Internet nicht oder nur zum Teil bekannt. Die meisten Internetnutzerinnen und -nutzer haben außerdem den Überblick darüber verloren, wer wann und zu welchem Zweck welche Daten von ihnen speichert, sie mit anderen Datensätzen verknüpft und ggf. auch an Dritte weitergibt. Wer aber nicht weiß, was mit seinen Daten geschieht oder geschehen kann, kann auch das informationelle Selbstbestimmungsrecht nicht effektiv ausüben.

Um dieser Entwicklung entgegenzuwirken, muss der Datenschutz auch als Bildungsaufgabe verstanden und praktiziert werden. Es genügt nicht, allein auf rechtliche Regelungen sowie auf datenschutzfreundliche technische Voreinstellungen und Anwendungen zu setzen. Die digitale Aufklärung ist unverzichtbar als Teil einer Datenschutz-

kultur des 21. Jahrhunderts. Sie beinhaltet zum einen die Vermittlung von Wissen und zum anderen die Entwicklung eines wachen, wertebezogenen Datenschutzbewusstseins.

So wie Bildung eine gesamtgesellschaftliche Aufgabe ist, so ist auch die Bildung im Hinblick auf die Datenschutzfragen unserer Zeit eine Aufgabe, die nicht nur dem Staat, sondern ebenso der Wirtschaft und der Zivilgesellschaft wie auch den Eltern im Verhältnis zu ihren Kindern obliegt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt deshalb und unterstützt vielfältige Überlegungen und Aktivitäten, die sich stärker als bisher um eine größere Datenschutzkompetenz der Internetnutzenden bemühen.

Die Datenschutzkonferenz hält die bisherigen Bemühungen allerdings noch nicht für ausreichend. Will man die Internetnutzerinnen und -nutzer dazu befähigen, Vorteile und Gefahren von Internetangeboten abzuwägen und selbstverantwortlich zu entscheiden, in welchem Umfange sie am digitalen Leben teilhaben wollen, sind weitergehende und nachhaltige Anstrengungen notwendig. Vor allem ist sicherzustellen, dass

1. dabei viel intensiver als bisher die Möglichkeiten des Selbstdatenschutzes, der verantwortungsvolle Umgang mit den Daten anderer und die individuellen und gesellschaftlichen Auswirkungen einer leichtfertigen Nutzung des Internets thematisiert werden,
2. sich die schulischen und außerschulischen Programme und Projekte zur Förderung von Medienkompetenz nicht auf Fragen des Jugendmedienschutzes und des Urheberrechts beschränken, sondern den Datenschutz als wesentlichen Bestandteil mit einbeziehen,
3. Medien- und Datenschutzkompetenz entweder in einem eigenständigen Schulfach oder in einem Fächerspektrum mit Leitfächern verpflichtend zu verankern ist,
4. die Vermittlung von Datenschutz als integraler Bestandteil von Medienkompetenz ausdrücklich in den Bildungsstandards und Lehrplänen verankert wird und dass die entsprechenden Anforderungen bewertungs- bzw. prüfungsrelevant ausgestaltet werden und
5. Medien- und Datenschutzkompetenz und insbesondere die digitale Aufklärung zum verbindlichen Gegenstand der Lehrerausbildung gemacht werden.

Digitale Aufklärung und Erziehung zum Datenschutz bestimmen letztlich auch über den Stellenwert, den Privatsphäre und Persönlichkeitsrecht und damit Menschenwürde und Demokratie künftig in der internetgeprägten Gesellschaft insgesamt haben werden.

### 17.1.3 Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München: Datenschutzkonforme Gestaltung und Nutzung vom Cloud-Computing

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert Cloud-Anbieter auf, ihre Dienstleistungen datenschutzkonform zu gestalten. Cloud-Anwender hingegen dürfen Cloud-Services nur dann in Anspruch nehmen, wenn sie in der Lage sind, ihre Pflichten als verantwortliche Stelle in vollem Umfang wahrzunehmen und die Umsetzung der Datenschutz- und Informationssicherheitsanforderungen geprüft haben.

Dies betrifft neben den Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit der Daten insbesondere die in diesem Umfeld schwierig umzusetzenden Anforderungen an Kontrollierbarkeit, Transparenz und Beeinflussbarkeit der Datenverarbeitung. Cloud-Computing darf nicht dazu führen, dass Daten verarbeitende Stellen, allen voran ihre Leitung, nicht mehr in der Lage sind, die Verantwortung für die eigene Datenverarbeitung zu tragen.

Zu verlangen sind also mindestens

- offene, transparente und detaillierte Informationen der Cloud-Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption, damit die Cloud-Anwender einerseits entscheiden können, ob Cloud-Computing überhaupt in Frage kommt und andererseits Aussagen haben, um zwischen den Cloud-Anbietern wählen zu können,
- transparente, detaillierte und eindeutige vertragliche Regelungen der Cloudgestützten Datenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und zur Interoperabilität,
- die Umsetzung der abgestimmten Sicherheits- und Datenschutzmaßnahmen auf Seiten von Cloud-Anbieter und Cloud-Anwender und
- aktuelle und aussagekräftige Nachweise (bspw. Zertifikate anerkannter und unabhängiger Prüfungsorganisationen) über die Infrastruktur, die bei der Auftragserfüllung in Anspruch genommen wird, die insbesondere die Informationssicherheit, die Portabilität und die Interoperabilität betreffen.

Die Datenschutzbeauftragten des Bundes und der Länder bieten ihre Unterstützung bei der Entwicklung und bei der Nutzung von Cloud-Computing-Diensten an. Details zur datenschutzgerechten Ausgestaltung dieser Dienste sind einer Orientierungshilfe[1] der

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

Arbeitskreise „Technik“ und „Medien“ zu entnehmen, die die Datenschutzkonferenz zustimmend zur Kenntnis genommen hat.

### 17.1.4 Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München: Vorbeugender Grundrechtsschutz ist Aufgabe der Datenschutzbeauftragten!

Der Sächsische Datenschutzbeauftragte hat mit einem Bericht zu den nicht individualisierten Funkzellenabfragen und anderen Maßnahmen der Telekommunikationsüberwachung im Februar 2011 durch die Polizei und die Staatsanwaltschaft Dresden Stellung genommen (Landtags-Drucksache 5/6787). In nicht nachvollziehbarer Weise ist die Kompetenz des Sächsischen Datenschutzbeauftragten zur Kontrolle von Verfahrensweisen von Polizei und Staatsanwaltschaften im Vorfeld einer bzw. nach einer richterlichen Anordnung in Frage gestellt worden.

Die Konferenz ist der Auffassung, dass derartige Äußerungen von der gebotenen inhaltlichen Aufarbeitung der Dresdener Funkzellenabfragen ablenken. Die gesetzliche Befugnis des Sächsischen Datenschutzbeauftragten zur Kontrolle aller polizeilichen und staatsanwaltschaftlichen Maßnahmen der Datenverarbeitung steht außer Frage. Es ist auch im Bereich der Strafverfolgung eine verfassungsrechtlich begründete Kernaufgabe der unabhängigen Datenschutzbeauftragten, einen vorgezogenen Rechtsschutz dort zu gewährleisten, wo Einzelne aufgrund der verdeckten Datenverarbeitung des Staates nicht oder nicht ausreichend früh anderweitigen Rechtsschutz erlangen können. Der Sächsische Datenschutzbeauftragte hat die polizeiliche Anregung bzw. staatsanwaltschaftliche Beantragung der konkreten Funkzellenabfragen als unverhältnismäßig und die besonderen Rechte von Abgeordneten, Verteidigerinnen und Verteidigern nicht wahrend beanstandet. Es kann dahinstehen, ob die funktional als Ausübung vollziehender Gewalt (vgl. BVerfGE 107, 395, 406) zu qualifizierende richterliche Anordnung solcher Maßnahmen von Landesdatenschutzbeauftragten kontrolliert werden kann, da die jeweiligen richterlichen Anordnungen in den konkreten Fällen nicht beanstandet wurden.

### 17.1.5 Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München: Einführung von IPv6 steht bevor: Datenschutz ins Netz einbauen!

Viele Betreiber und Anwender stellen in diesen Monaten ihre Netzwerktechnik auf das Internet-Protokoll Version 6 (IPv6) um. Grundsätzlich darf es mit einer Migration von IPv4 zu IPv6 nicht zu einer Verschlechterung der technischen Rahmenbedingungen zur

Ausgestaltung von Privacy kommen. Neuen Herausforderungen muss mit wirksamen Konzepten begegnet werden.

IPv6 stellt eine nahezu unbegrenzte Anzahl von statischen IP-Adressen zur Verfügung, die eine dynamische Vergabe von IP-Adressen, wie sie zur Zeit bei Endkunden gängig ist, aus technischer Sicht nicht mehr erforderlich macht. Aber durch die Vergabe statischer Adressen erhöht sich das Risiko, dass Internetnutzende identifiziert und ihre Aktivitäten auf einfache Weise webseitenübergreifend zu individuellen Profilen zusammen geführt werden können. Sowohl der von den Internet-Providern bereitgestellte Adressanteil (Präfix) als auch gerätespezifische Anteile in den IPv6-Adressen machen eine dauerhafte Identifizierung möglich. Die Zuordnung einer IP-Adresse zu einer bestimmten Person bedarf nicht zwingend einer Beteiligung des Zugangsanbieters. Mit Hilfe von Zusatzinformationen, die dem Betreiber eines Internet-Angebots vorliegen oder ihm offenstehen, beispielsweise Identifikationskonten von Online-Shops oder Sozialen Netzen, ist eine eindeutige Zuordnung von Nutzern möglich. Die vereinfachten Möglichkeiten zur Profilbildung und Zusammenführung von Profilen erhöhen zudem das Risiko und verstärken die Auswirkungen krimineller Handlungen. Mit Blick darauf, dass sich ein Identifikationsrisiko aus beiden Teilen der neuen Adressen ergeben kann, sind Maßnahmen in unterschiedlichen Bereichen erforderlich.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, bei der Umstellung auf IPv6 Datenschutz und IT-Sicherheit zu gewährleisten. Anbieter von Internetzugängen und Diensten sowie Hersteller von Hard- und Software-Lösungen sollten ihre Produkte datenschutzgerecht gestalten (privacy by design) und dementsprechende Voreinstellungen wählen (privacy by default). Internetnutzenden sollten bei der Beschaffung von Hard- und Software sowie beim Abschluss von Verträgen auf diese Aspekte besonders achten.

- Access Provider sollten Kundinnen und Kunden statische und dynamische Adressen ohne Aufpreis zuweisen. Auf Kundenwunsch sollten statische Adressen gewechselt werden können.
- Kundinnen und Kunden sollten mit nutzerfreundlichen Bedienelementen bei der Auswahl der Adressen für jeden von ihnen genutzten Dienst unterstützt werden.
- Hard- und Softwarehersteller sollten die „Privacy Extensions“ unterstützen und standardmäßig einschalten (privacy by default), um die Wiedererkennung von Nutzenden anhand von Hardwareadressen zu erschweren.
- Die Hard- und Softwarehersteller sollten Lösungen für dezentrale Kommunikationsdienste (peer to peer) in Kundensystemen entwickeln, die den Verzicht auf zentrale Plattformen und Portale ermöglichen. Sie sollten interessierten Dritten die Entwicklung solcher Dienste gestatten.

- Content Provider dürfen zur Reichweitenmessung nur die ersten 4 Bytes der IPv6-Adresse heranziehen und müssen den Rest der Adresse löschen, denn eine Analyse von Nutzungsdaten ist nach Ansicht der Datenschutzaufsichtsbehörden nur auf der Grundlage anonymisierter IP-Adressen zulässig. Die ersten 4 Bytes sind für eine Geolokalisierung ausreichend.
- Zugangsanbieter und Betreiber von Internetangeboten sollten nicht protokollierende Proxy-Server einsetzen und die Voraussetzungen schaffen, dass ein Internetzugang oder die Nutzung von im Internet bereitgestellten Inhalten in anonymer Form möglich ist (Anonymisierungsdienste).
- Hersteller und Anbieter von Betriebssystemen und vorkonfigurierten Geräten (wie PCs, Smartphones und Routern) sollten ihre Anstrengungen bei der Pflege und Weiterentwicklung ihrer Produkte intensivieren und regelmäßig Fehler bereinigte Versionen ihrer IPv6-fähigen Software anbieten.
- Angesichts häufig mangelnder Reife von IPv6-fähigen Produkten ist Anwendern vom Einsatz von IPv6 innerhalb von lokalen Netzen noch abzuraten, wenn dort sensible personenbezogene Daten verarbeitet werden sollen und funktionsfähige Filtereinrichtungen weder zentral noch auf den einzelnen Rechnern im LAN vorhanden und aktiviert sind.
- Eigentümerinnen und Eigentümer von IP-Adressen dürfen nur auf Wunsch in das weltweite, stark zentralisierte „Internet-Telefonbuch“ whois aufgenommen werden. Die Bundesregierung wird aufgefordert, sich für eine datenschutzfreundliche Gestaltung des whois-Dienstes einzusetzen, dahingehend, dass die Internet-Verwaltung ICANN den whois-Dienst künftig als verteilte Datenbank gestaltet, so dass die Daten der Eigentümerinnen und Eigentümer jeweils durch lokale Dienstleister oder Selbstverwaltungsgremien gespeichert, gepflegt und von ihnen nach Maßgabe des lokalen Rechts an Dritte übermittelt werden.

Die Datenschutzbeauftragten des Bundes und der Länder werden die Einführung von IPv6 wachsam beobachten und bieten allen Akteuren ihre Unterstützung an.

### 17.1.6 Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München: Anonymes elektronisches Bezahlen muss möglich bleiben!

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Bundesgesetzgeber auf, bei der Bekämpfung von Geldwäsche auf umfassende und generelle Identifizierungspflichten beim Erwerb von elektronischem Geld zu verzichten. Ein aktueller Gesetzentwurf der Bundesregierung zum Geldwäschegesetz (BT-Drs. 17/6804) sieht vor, über bereits bestehende - allerdings nicht umgesetzte - gesetzliche Verpflichtungen

hinaus umfangreiche Daten über sämtliche Erwerber elektronischen Geldes zu registrieren. Der anonyme Erwerb von E-Geld würde damit generell abgeschafft.

Dies ist besonders kritisch, da umfangreiche Kundinnen- und Kundendaten unabhängig vom Wert des E-Geldes erhoben werden müssen. Beispielsweise ist eine Tankstelle bereits beim Verkauf einer E-Geld Karte im Wert von fünf Euro verpflichtet, den Namen, das Geburtsdatum und die Anschrift der Kundinnen und Kunden zu erheben und für mindestens fünf Jahre aufzubewahren.

Eine generelle Identifizierungspflicht würde außerdem dazu führen, dass anonymes Einkaufen und Bezahlen im Internet selbst bei Bagatellbeträgen praktisch ausgeschlossen werden. Anonyme Bezahlsysteme im Internet bieten ihren Nutzern jedoch Möglichkeiten, die Risiken eines Missbrauchs ihrer Finanzdaten beispielsweise durch Hackerangriffe zu minimieren. Sie sind zugleich ein wichtiger Baustein, um die Möglichkeit zum anonymen Medienkonsum zu erhalten, da Online-Medien zunehmend gegen Bezahlung angeboten werden. Auf jeden Fall muss verhindert werden, dass personenbeziehbare Nutzungsdaten über jeden einzelnen Artikel in Online-Zeitungen oder einzelne Sendungen im Internet-TV schon immer dann entstehen, wenn eine Nutzung gebührenpflichtig ist.

Nach den vorgesehenen Regelungen würden noch mehr personenbezogene Daten unbescholtener Bürgerinnen und Bürger erfasst und ganz überwiegend anlasslos gespeichert. Dies steht im Widerspruch zur Rechtsprechung des Bundesverfassungsgerichts. In seinem Urteil zur Vorratsdatenspeicherung von Telekommunikationsdaten vom 2. März 2010 (1 BvR 256/08) hatte das Gericht gemahnt, dass Gesetze, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielen, mit der Verfassung unvereinbar sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt die vorgesehene verdachtsunabhängige, undifferenzierte und schrankenlose Datenerfassung ab, die auch europarechtlich nicht geboten ist. Die dritte Geldwäscherichtlinie (2005/60/EG) erlaubt den Mitgliedstaaten, von Identifizierungspflichten abzusehen, wenn der Wert des erworbenen elektronischen Guthabens 150 Euro nicht übersteigt. Der Bundesgesetzgeber sollte durch Einführung eines entsprechenden Schwellenwerts diesem risikoorientierten Ansatz folgen.

### 17.1.7 Entschließung der 82. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28./29. September 2011 in München: Datenschutz bei sozialen Netzwerken jetzt verwirklichen!

Anlässlich der aktuellen Diskussionen um den Datenschutz bei sozialen Netzwerken, wie beispielsweise Facebook, stellt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder klar, dass sich die Anbieter solcher Plattformen, die auf den europäischen Markt zielen, auch dann an europäische Datenschutzstandards halten müssen, wenn sie ihren Sitz außerhalb Europas haben.

Die Konferenz stellt insbesondere fest, dass die direkte Einbindung von Social-Plugins beispielsweise von Facebook, Google+, Twitter und anderen Plattformbetreibern in die Webseiten deutscher Anbieter ohne hinreichende Information der Internet-Nutzenden und ohne Einräumung eines Wahlrechtes nicht mit deutschen und europäischen Datenschutzstandards in Einklang steht. Die aktuelle von Social-Plugin-Anbietern vorgesehene Funktionsweise ist unzulässig, wenn bereits durch den Besuch einer Webseite und auch ohne Klick auf beispielsweise den „Gefällt-mir“-Knopf eine Übermittlung von Nutzendendaten in die USA ausgelöst wird, auch wenn die Nutzenden gar nicht bei der entsprechenden Plattform registriert sind.

Die Social-Plugins sind nur ein Beispiel dafür, wie unzureichend einige große Betreiber sozialer Plattformen den Datenschutz handhaben. So verwendet Facebook mittlerweile Gesichtserkennungs-Technik, um Bilder im Internet bestimmten Personen zuzuordnen; Betroffene können sich dem nur mit erheblichem Aufwand entziehen. Sowohl Facebook als auch Google+ verlangen, dass die Nutzenden sich identifizieren, obwohl nach deutschem Recht aus guten Gründen die Möglichkeit zumindest einer pseudonymen Nutzung solcher Dienste eröffnet werden muss.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher alle öffentlichen Stellen auf, von der Nutzung von Social-Plugins abzusehen, die den geltenden Standards nicht genügen. Es kann nicht sein, dass die Bürgerinnen und Bürger, die sich auf den Seiten öffentlicher Stellen informieren wollen, mit ihren Daten dafür bezahlen. Unbeschadet der rechtlichen Verantwortung sollten die öffentlichen Stellen auf solchen Plattformen keine Profilseiten oder Fanpages einrichten.

Die Obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich haben bereits 2008 und zuletzt 2010 in Beschlüssen Anforderungen an die datenschutzkonforme Gestaltung sozialer Netzwerke formuliert. Die Konferenz der Datenschutzbeauftragten fordert die Anbieter sozialer Netzwerke auf, diese Beschlüsse umzusetzen, soweit dies noch nicht geschehen ist. In diesem Zusammenhang unterstützen die

Datenschutzbeauftragten Bestrebungen zur Entwicklung von technischen Lösungen zur datenschutzkonformen Gestaltung von Webangeboten.

Bedauerlicherweise hat die Bundesregierung ihrer schon im letzten Jahr gemachten Ankündigung, gesetzgeberische Maßnahmen gegen die Profilbildung im Internet vorzuschlagen, keine Taten folgen lassen. Der bloße Verweis darauf, dass die Diensteanbieter Selbstverpflichtungen eingehen sollten, wird dem akuten Schutzbedarf der immer zahlreicher werdenden Nutzerinnen und Nutzer nicht gerecht. Die Konferenz der Datenschutzbeauftragten unterstützt den Gesetzentwurf des Bundesrates zur Änderung des Telemediengesetzes (BT-Drs. 17/6765) als einen Schritt in die richtige Richtung.

### 17.1.8 Entschließung der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 21./22. März 2012 in Potsdam: Ein hohes Datenschutzniveau für ganz Europa!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht der Europäischen Kommission, den Datenschutz in der Europäischen Union zu modernisieren und zu harmonisieren.

Der Entwurf einer **Datenschutz-Grundverordnung** enthält Regelungen, die zu einer Weiterentwicklung des europäischen Datenschutzrechts führen können. Dazu gehören vor allem

- das Prinzip Datenschutz durch Technik,
- der Gedanke datenschutzfreundlicher Voreinstellungen,
- der Grundsatz der Datenübertragbarkeit,
- das Recht auf Vergessen,
- die verbesserte Transparenz durch Informationspflichten der verantwortlichen Stellen
  und
- die verschärften Sanktionen bei Datenschutzverstößen.

Hervorzuheben ist zudem die Geltung des europäischen Rechts für Anbieter aus Drittstaaten, deren Dienste sich auch an europäische Bürgerinnen und Bürger richten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für wesentlich, dass bei der Harmonisierung des Datenschutzrechts ein möglichst hohes Niveau für alle Mitgliedsstaaten vorgeschrieben wird. Die Konferenz hatte bereits im Konsultationsverfahren die Auffassung vertreten, dass diesem Ziel angesichts der gewachsenen Traditionen und Rechtsstandards in den Mitgliedsstaaten und der eingeschränkten begrenzten Rechtssetzungskompetenz der EU in Bezug auf innerstaatliche Datenverarbeitungsvor-

gänge im öffentlichen Bereich am wirksamsten durch eine Richtlinie Rechnung getragen werden kann. Wenn jetzt stattdessen der Entwurf einer unmittelbar geltenden Verordnung vorgelegt wird, muss diese im Sinne eines europäischen Mindestdatenschutzniveaus den Mitgliedsstaaten zumindest in Bezug auf die Datenverarbeitung der öffentlichen Verwaltung die Möglichkeit eröffnen, durch einzelstaatliches Recht weitergehende Regelungen zu treffen, die entsprechend der jeweiligen Rechtstradition die Grundrechte der Bürgerinnen und Bürger absichern und Raum für eine innovative Rechtsfortbildung schaffen. Nur so können beispielsweise in Deutschland die in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Datenschutzgrundsätze bewahrt und weiterentwickelt werden.

Die Konferenz erkennt an, dass die Institution der betrieblichen Datenschutzbeauftragten erstmals verbindlich in Europa eingeführt werden soll. Die Erfahrungen in Deutschland mit den betrieblichen Datenschutzbeauftragten als unabhängige Kontroll- und Beratungsstellen in Unternehmen sind ausgesprochen positiv. Die Konferenz bedauert deshalb, dass die Kommission grundsätzlich nur Unternehmen mit mindestens 250 Beschäftigten zur Bestellung von Datenschutzbeauftragten verpflichten will. Dieses Vorhaben bedroht eine gewachsene und erfolgreiche Kultur des betrieblichen Datenschutzes in Deutschland.

Über die bereits in dem Verordnungsentwurf vorgeschlagenen Modernisierungen hinaus hält die Konferenz weitere Schritte für erforderlich, die sie etwa in ihrem Eckpunktepapier für ein modernes Datenschutzrecht vom 18. März 2010 vorgeschlagen hat:

- eine strikte Reglementierung der Profilbildung, insbesondere deren Verbot bei Minderjährigen,
- ein effektiver Schutz von Minderjährigen, insbesondere in Bezug auf das Einwilligungserfordernis eine Anhebung der Altersgrenze,
- die Förderung des Selbstdatenschutzes,
- pauschalierte Schadensersatzansprüche bei Datenschutzverstößen,
- einfache, flexible und praxistaugliche Regelungen zum technisch-organisatorischen Datenschutz, welche vor allem die Grundsätze der Vertraulichkeit, der Integrität, der Verfügbarkeit, der Nichtverkettbarkeit, der Transparenz und der Intervenierbarkeit anerkennen und ausgestalten,
- das Recht, digital angebotene Dienste anonym oder unter Pseudonym nutzen zu können und
- die grundsätzliche Pflicht zur Löschung der angefallenen Nutzerdaten nach dem Ende des Nutzungsvorganges.

Die Regelungen zur Risikoanalyse, Vorabkontrolle und zur Zertifizierung bedürfen der weiteren Präzisierung in der Verordnung selbst.

Für besonders problematisch hält die Konferenz die vorgesehenen zahlreichen Ermächtigungen der Europäischen Kommission für delegierte Rechtsakte, die dringend auf das unbedingt erforderliche Maß zu reduzieren sind. Alle für den Grundrechtsschutz wesentlichen Regelungen müssen in der Verordnung selbst bzw. durch Gesetze der Mitgliedsstaaten getroffen werden.

Die Konferenz weist darüber hinaus darauf hin, dass das im Entwurf der Datenschutz-Grundverordnung vorgesehene Kohärenzverfahren, welches die Aufsichtsbehörden in ein komplexes Konsultationsverfahren einbindet, die Unabhängigkeit der Datenschutzaufsicht beeinträchtigen und zu einer Bürokratisierung des Datenschutzes führen würde. Es muss deshalb vereinfacht und praktikabler gestaltet werden.

Die durch Artikel 8 der EU-Grundrechte-Charta und Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union gewährleistete Unabhängigkeit der Datenschutzaufsichtsbehörden gilt auch gegenüber der Europäischen Kommission. Die vorgesehenen Befugnisse der Kommission in Bezug auf konkrete Maßnahmen der Aufsichtsbehörden bei der Umsetzung der Verordnung wären damit nicht vereinbar.

Wiederholt hat die Konferenz auf die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch im **Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen** in Europa hingewiesen. Sie bedauert, dass der für diesen Bereich vorgelegte Richtlinienentwurf in vielen Einzelfragen hinter dem Entwurf für eine Datenschutz-Grundverordnung und hinter dem deutschen Datenschutzniveau zurückbleibt, etwa im Hinblick auf die Prinzipien der Datenverarbeitung (wie den Grundsatz der Erforderlichkeit) und auf die Rechte der Betroffenen (insbesondere zum Schutz des Kernbereiches der privaten Lebensgestaltung). Auch in diesem Bereich sollte die Richtlinie unter angemessener Berücksichtigung der mitgliedsstaatlichen Verfassungstraditionen ein EU-weit möglichst hohes Mindestniveau festschreiben.

Die Konferenz erklärt, dass sie den Gang des Gesetzgebungsverfahrens konstruktiv und kritisch begleiten wird.

### 17.1.9 Entschließung der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 21./22. März 2012 in Potsdam: Europäische Ermittlungsanordnung darf Grundrechtsgarantien nicht aushebeln

Zurzeit wird auf europäischer Ebene der Entwurf einer Richtlinie über die Europäische Ermittlungsanordnung in Strafsachen beraten. Diese hat massive Auswirkungen auf den

Grundrechtsschutz der Bürgerinnen und Bürger in den EU-Mitgliedstaaten. Sie kann dazu führen, dass der verfahrensrechtliche Schutzstandard bei strafprozessualen Maßnahmen europaweit auf niedrigstes Niveau abgesenkt wird. So kann sie etwa zur Folge haben, dass ein Mitgliedstaat für einen anderen Daten oder Beweismittel erhebt und diesem übermittelt, obwohl die Erhebung nach eigenem Recht nicht zulässig wäre.

Der Richtlinienentwurf verfolgt vorrangig das Ziel einer weitgehenden gegenseitigen Anerkennung von Eingriffsentscheidungen der Strafverfolgungsbehörden, ohne dass einheitliche Verfahrensgarantien geschaffen werden. Dies wirft Probleme auf, wenn der Anordnungsstaat niedrigere Schutzstandards aufweist als der Vollstreckungsstaat. Die Möglichkeiten der Mitgliedstaaten, eine entsprechende Anordnung eines anderen Mitgliedstaates zurückzuweisen, sind nicht immer ausreichend. Eingriffsschwellen, Zweckbindungs- und Verfahrensregelungen müssen gewährleisten, dass die Persönlichkeitsrechte der Betroffenen gewahrt werden.

Eine effektive grenzüberschreitende Strafverfolgung im vereinten Europa darf nicht zu Lasten des Grundrechtsschutzes der Betroffenen gehen. Die Anforderungen der EU-Grundrechte-Charta sind konsequent einzuhalten. Die Europäische Ermittlungsanordnung muss in ein schlüssiges Gesamtkonzept zur Datenerhebung und -verwendung im Bereich der inneren Sicherheit und der Strafverfolgung eingebettet werden, das die Grundrechte der Bürgerinnen und Bürger gewährleistet.

### 17.1.10 Entschließung der 83. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 21./22. März 2012 in Potsdam: Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum - nicht ohne Datenschutz

Mit erheblichen öffentlichen Mitteln werden derzeit zahlreiche Forschungsprojekte finanziert, die darauf abzielen, mit Hilfe modernster Technik - insbesondere der Videoüberwachung und dem Instrument der Mustererkennung - menschliche Verhaltensweisen zu analysieren. Dadurch sollen in öffentlich zugänglichen Bereichen mit hohem Sicherheitsbedarf „potentielle Gefährder“ frühzeitig entdeckt werden. Zu derartigen Forschungsvorhaben zählen beispielsweise das Projekt „INDECT“ (Intelligentes Informationssystem zur Überwachung, Suche und Detektion für die Sicherheit der Bürger in urbaner Umgebung), das von der Europäischen Union gefördert wird, oder in Deutschland Projekte wie ADIS (Automatisierte Detektion interventionsbedürftiger Situationen durch Klassifizierung visueller Muster), CamInSens (Verteilte, vernetzte Kamerasysteme zur in situ-Erkennung personeninduzierter Gefahrensituationen) oder die Gesichtserkennung in Fußballstadien.

Bei der Mustererkennung soll auf Basis von Video- oder anderen Aufzeichnungen, die mit Daten aus anderen Informationsquellen kombiniert werden, das Verhalten aller erfassten Personen computerunterstützt ausgewertet werden. Menschen, deren Verhalten als ungewöhnlich eingestuft wird, können so in Verdacht geraten, zukünftig eine Straftat zu begehen. Gerade bei der Mustererkennung von menschlichem Verhalten besteht daher die große Gefahr, dass die präventive Analyse einen Anpassungsdruck erzeugt, der die Persönlichkeitsrechte der betroffenen Bürgerinnen und Bürger verletzen würde.

Insoweit ist generell die Frage aufzuwerfen, inwieweit die grundrechtliche Zulässigkeit des Einsatzes der zu erforschenden Überwachungstechnik hinreichend untersucht wird. Bei Projekten, bei denen öffentliche Stellen des Bundes und der Länder beteiligt sind, sollten jeweils die zuständigen Datenschutzbehörden frühzeitig über das Projektvorhaben informiert und ihnen Gelegenheit zur Stellungnahme eingeräumt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an alle öffentlichen Stellen von Bund und Ländern, aber auch an die der Europäischen Union, die solche Projekte in Auftrag geben oder Fördermittel hierfür zur Verfügung stellen, bereits bei der Ausschreibung oder Prüfung der Förderfähigkeit derartiger Vorhaben rechtliche und technisch-organisatorische Fragen des Datenschutzes in ihre Entscheidung mit einzubeziehen. Nur so kann verhindert werden, dass Vorhaben öffentlich gefördert werden, die gegen Datenschutzvorschriften verstoßen.

### 17.1.11 Entschließung zwischen der 83. und 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 23. Mai 2012: Patientenrechte müssen umfassend gestärkt werden

*Datenschutzkonferenz fordert die Bundesregierung zur Überarbeitung des vorgelegten Gesetzentwurfs auf!*

Mit dem im Januar 2012 der Öffentlichkeit vorgestellten und nun dem Bundeskabinett zugeleiteten Entwurf eines Gesetzes zur Verbesserung der Rechte von Patientinnen und Patienten (Patientenrechtegesetz) sollen insbesondere die bislang von den Gerichten entwickelten Grundsätze des Arzthaftungs- und Behandlungsrechts zusammengeführt und transparent für alle an einer Behandlung Beteiligten geregelt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder teilt das Anliegen der Bundesregierung, die Rechte von Patientinnen und Patienten zu stärken.

Die Datenschutzkonferenz hält allerdings die vorgelegten Regelungen in dem Entwurf eines Patientenrechtegesetzes für nicht ausreichend. Sie fordert die Bundesregierung

nachdrücklich auf, den Gesetzentwurf zu überarbeiten und dabei die folgenden Aspekte zu berücksichtigen:

- Die vertraglichen Offenbarungsobliegenheiten der Patientinnen und Patienten gegenüber den Behandelnden dürfen nicht ausgeweitet werden. Die Patientinnen und Patienten dürfen nicht zur Offenlegung von Angaben über ihre körperliche Verfassung verpflichtet werden, die keinen Behandlungsbezug haben.
- Die Patientinnen und Patienten müssen in jedem Fall und nicht erst auf Nachfrage über erlittene Behandlungsfehler informiert werden.
- Der Gesetzentwurf sollte im Zusammenhang mit der Behandlungsdokumentation um verlässliche Vorgaben zur Absicherung des Auskunftsrechts der Patientinnen und Patienten sowie zur Archivierung und Löschung ergänzt werden.
- Der Zugang der Patientinnen und Patienten zu der sie betreffenden Behandlungsdokumentation darf nur in besonderen Ausnahmefällen eingeschränkt werden. Die in dem Entwurf vorgesehenen Beschränkungen sind zu weitgehend und unpräzise. Zudem sollte klargestellt werden, dass auch berechtigte eigene Interessen der Angehörigen einen Auskunftsanspruch begründen können.
- Der Gesetzentwurf ist um Regelungen zur Einbeziehung Dritter im Rahmen eines Behandlungsvertrages (Auftragsdatenverarbeitung) zu ergänzen.
- Regelungsbedürftig ist ferner der Umgang mit der Behandlungsdokumentation beispielsweise im Falle eines vorübergehenden Ausfalls, des Todes oder der Insolvenz des Behandelnden. Im Bereich der Heilberufe fehlt es - anders als z. B. bei den Rechtsanwälten - an einem bundesweit einheitlichen Rechtsrahmen.

### 17.1.12 Entschließung zwischen der 83. und 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. Juni 2012: Orientierungshilfe zum datenschutzgerechten Smart Metering

Intelligente Energienetze und -zähler sind ein zentraler Baustein zur Sicherstellung einer nachhaltigen Energieversorgung im Sinne einer ressourcenschonenden, umweltfreundlichen und effizienten Produktion, Verteilung und Nutzung von Energie. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine Orientierungshilfe beschlossen, die Empfehlungen zur datenschutzgerechten Konzeption von technischen Systemen für das Smart Metering enthält. Kernstück der Orientierungshilfe ist die Beschreibung und datenschutzrechtliche Bewertung sog. Use Cases, d. h. Anwendungsfälle, für die einzelnen Datenverarbeitungsprozesse beim Smart Metering unter Berücksichtigung des jeweiligen Schutzbedarfs der Daten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für erforderlich, dass insbesondere folgende Punkte beachtet werden:

- Eine Verarbeitung der Smart Meter Daten darf nur erfolgen, soweit es für die im Energiewirtschaftsgesetz aufgezählten Zwecke erforderlich ist.
- Die Ableseintervalle müssen so groß sein, dass aus dem Verbrauch keine Rückschlüsse auf das Verhalten der Nutzer gezogen werden können.
- Smart Meter Daten sollen möglichst nur anonymisiert, pseudonymisiert oder aggregiert übermittelt werden.
- Es muss möglich sein, hoch aufgelöste Daten lokal beim Letztverbraucher abzurufen, ohne dass dieser auf eine externe Verarbeitung der Daten angewiesen ist.
- Die Daten sollen an möglichst wenige Stellen übermittelt werden.
- Es sind angemessene Löschfristen für die Daten festzulegen, um eine Vorratsdatenspeicherung zu vermeiden.
- Die Kommunikations- und Verarbeitungsschritte von Smart Metering müssen zu jeder Zeit für den Letztverbraucher sichtbar und nachweisbar sein. Er muss Zugriffe auf den Smart Meter erkennen und dies im Zweifel unterbinden können.
- Zusätzlich bedarf es durchsetzbarer Ansprüche der Betroffenen auf Löschung, Berichtigung und Widerspruch.
- Der Letztverbraucher muss die Möglichkeit haben, einen Tarif zu wählen, bei dem möglichst wenig über seinen Lebensstil offenbart wird, ohne dass dies für seine Energieversorgung nachteilig ist.
- Smart Meter dürfen von außen nicht frei zugänglich sein. Es müssen eindeutige Profile für den berechtigten Zugang zu den Daten definiert werden. Anhaltspunkte hierfür bieten die Vorgaben im Schutzprofil und in der Technischen Richtlinie des BSI.
- Schon bei der Konzeption und Gestaltung der technischen Systeme muss die Gewährleistung des Datenschutzes berücksichtigt werden (Privacy by Design). Der Letztverbraucher muss mit Hilfe der Technik alle notwendigen Informationen, Optionen und Kontrollmöglichkeiten erhalten, die ihm die Kontrolle seines Energieverbrauchs und die Gestaltung seiner Privatsphäre ermöglichen, wobei der Stand der Technik nicht unterschritten werden darf. Insbesondere müssen rechtlich verbindliche Vorgaben für die Konzeption der Geräte, Verfahren und Infrastrukturen sowie für deren Einsatz geschaffen werden.

### 17.1.13 Entschließung zwischen der 83. und 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22. August 2012: Melderecht datenschutzkonform gestalten!

Das vom Deutschen Bundestag am 28. Juni 2012 beschlossene neue Melderecht weist erhebliche datenschutzrechtliche Defizite auf. Schon die im Regierungsentwurf enthaltenen Datenschutzbestimmungen blieben zum Teil hinter dem bereits geltenden

Recht zurück. Darüber hinaus wurde der Regierungsentwurf durch das Ergebnis der Ausschussberatungen des Bundestages noch einmal deutlich verschlechtert.

Bei den Meldedaten handelt es sich um Pflichtangaben, die die Bürgerinnen und Bürger gegenüber dem Staat machen müssen. Dies verpflichtet zu besonderer Sorgfalt bei der Verwendung, insbesondere wenn die Daten an Dritte weitergegeben werden sollen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher den Bundesrat auf, dem Gesetzentwurf nicht zuzustimmen, damit im Vermittlungsverfahren die erforderlichen datenschutzgerechten Verbesserungen erfolgen können. Dabei geht es nicht nur darum, die im Deutschen Bundestag vorgenommenen Verschlechterungen des Gesetzentwurfs der Bundesregierung rückgängig zu machen, vielmehr muss das Melderecht insgesamt datenschutzkonform ausgestaltet werden. Hierfür müssen auch die Punkte aufgegriffen werden, die von den Datenschutzbeauftragten im Gesetzgebungsverfahren gefordert worden sind, aber unberücksichtigt blieben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält insbesondere in den folgenden Punkten Korrekturen und Ergänzungen für erforderlich:

- Einfache Melderegisterauskünfte für Zwecke der Werbung und des Adresshandels bedürfen ausnahmslos der Einwilligung des Meldepflichtigen. Dies gilt auch für die Aktualisierung solcher Daten, über die die anfragenden Stellen bereits verfügen und die Weitergabe der Daten an Adressbuchverlage.
  Melderegisterauskünfte in besonderen Fällen, wie Auskünfte an Parteien zu Wahlwerbungszwecken und an Presse oder Rundfunk über Alters- und Ehejubiläen sollten im Interesse der Betroffenen ebenfalls nur mit Einwilligung der Meldepflichtigen zulässig sein.
- Der Meldepflichtige muss sonstigen einfachen Melderegisterauskünften widersprechen können. Die Übermittlung hat bei Vorliegen eines Widerspruchs zu unterbleiben, sofern der Anfragende kein rechtliches Interesse geltend machen kann.
- Die Zweckbindung der bei Melderegisterauskünften übermittelten Daten ist zu verstärken. Die im Gesetzentwurf nur für Zwecke der Werbung und des Adresshandels vorgesehene Zweckbindung muss auch auf die Verwendung für sonstige gewerbliche Zwecke erstreckt werden.
- Angesichts der Sensibilität der Daten, die im Rahmen einer erweiterten Melderegisterauskunft mitgeteilt werden, und der relativ niedrigen Voraussetzungen, die an die Glaubhaftmachung des berechtigten Interesses gestellt werden, sollte anstelle des berechtigten Interesses ein rechtliches Interesse an der Kenntnis der

einzelnen Daten vom potentiellen Datenempfänger glaubhaft gemacht werden müssen.

- Die Erteilung einfacher Melderegisterauskünfte im Wege des Abrufs über das Internet oder des sonstigen automatisierten Datenabrufs sollte wie bisher nur zulässig sein, wenn die betroffene Person ihr nicht widerspricht.
- Die Hotelmeldepflicht sollte entfallen, weil es sich dabei um eine sachlich nicht zu rechtfertigende Vorratsdatenspeicherung handelt. Hotelgäste dürfen nicht schlechthin als Gefahrenquellen oder (potentielle) Straftäter angesehen und damit in ihrem Persönlichkeitsrecht verletzt werden.
- Die erst vor wenigen Jahren abgeschaffte Mitwirkungspflicht des Wohnungsgebers bei der Anmeldung des Mieters darf nicht wieder eingeführt werden. Die Verpflichtung des Meldepflichtigen, den Vermieter zu beteiligen, basiert auf einer Misstrauensvermutung gegenüber der Person des Meldepflichtigen. Der Gesetzgeber hat die damalige Abschaffung der Vermietermeldepflicht unter anderem damit begründet, dass die Erfahrungen der meldebehördlichen Praxis zeigen, dass die Zahl der Scheinmeldungen zu vernachlässigen ist. Es liegen keine Anhaltspunkte dafür vor, dass sich dies zwischenzeitlich geändert hat. Ferner steht der Aufwand hierfür - wie auch bei der Hotelmeldepflicht - außer Verhältnis zum Nutzen.

### 17.1.14 Entschließung der 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 7./8. November 2012 in Frankfurt (Oder): Europäische Datenschutzreform konstruktiv und zügig voranbringen!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht der Europäischen Kommission, den Datenschutz in Europa auf hohem Niveau zu harmonisieren. Sie hat dies bereits in ihrer Entschließung vom 21./22. März 2012 verdeutlicht. In zwei umfassenden Stellungnahmen vom 11. Juni 2012 haben die Datenschutzbeauftragten des Bundes und der Länder eine Vielzahl einzelner Aspekte der Datenschutzreform bewertet und Empfehlungen für den weiteren Rechtssetzungsprozess gegeben.

Angesichts der aktuellen Diskussionen in Deutschland und im Rat der Europäischen Union sowie entsprechender Äußerungen aus der Bundesregierung im Rahmen des Reformprozesses betont die Konferenz folgende Punkte:

- Im Hinblick auf geforderte Ausnahmen für die Wirtschaft ist es für die Datenschutzbeauftragten des Bundes und der Länder unabdingbar, in der **Datenschutz-Grundverordnung** an der bisherigen Systematik des Datenschutzrechts festzuhalten. Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn dies

durch eine gesetzliche Grundlage oder die Einwilligung des Betroffenen legitimiert ist. Die hier für die Wirtschaft geforderten Ausnahmen lehnt die Konferenz ab. Wollte man in Zukunft nur noch eine besonders risikobehaftete Datenverarbeitung im Einzelfall regeln und die so genannte alltägliche Datenverarbeitung weitgehend ungeregelt lassen, würde dies zu einer massiven Einschränkung des Datenschutzes führen und die Rechte der Betroffenen deutlich beschneiden.

Jede Verarbeitung scheinbar „belangloser“ Daten kann für den Einzelnen schwerwiegende Folgen haben, wie das Bundesverfassungsgericht bereits 1983 ausdrücklich klargestellt hat. Diese Aussage gilt heute mehr denn je. Deshalb lehnt es die Konferenz ab, angeblich „belanglose“ Daten von einer Regelung auszunehmen.

Soweit die Datenschutz-Grundverordnung eine Datenverarbeitung erlaubt, enthält der Reformvorschlag der Kommission bereits jetzt Ansätze für am Risiko der Datenverarbeitung ausgerichtete Differenzierungen. Diese sollten dort, wo ein risikobezogener Ansatz angemessen ist, weiter ausgebaut werden.

- Die Konferenz spricht sich nachdrücklich dafür aus, das bewährte Konzept eines grundsätzlich einheitlichen Datenschutzrechts sowohl für den öffentlichen als auch für den nicht-öffentlichen Bereich beizubehalten und insbesondere für die Datenverarbeitung im öffentlichen Bereich die Möglichkeit eines höheren Schutzniveaus durch einzelstaatliches Recht zu belassen.
- Sie hält es für sinnvoll, für den Beschäftigtendatenschutz in der Datenschutz-Grundverordnung selbst qualifizierte Mindestanforderungen festzulegen und klarzustellen, dass die Mitgliedstaaten über diese zugunsten des Datenschutzes hinausgehen, sie aber nicht unterschreiten dürfen.
- Mit Blick auf die **Richtlinie im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen** bekräftigt die Konferenz nochmals die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch in diesem Bereich und damit die Wichtigkeit der Verabschiedung einer entsprechenden Regelung.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, sich im Sinne dieser Positionen im Rat der Europäischen Union für die Belange eines harmonisierten Datenschutzrechts auf einem hohen Niveau einzusetzen.

### 17.1.15 Entschließung der 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 7./8. November 2012 in Frankfurt (Oder): Übermittlung von Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und die GEZ rechtskonform gestalten

Die Meldebehörden sind verpflichtet, regelmäßig Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und an die Gebühreneinzugszentrale (GEZ) zu übermitteln. Die zu übermittelnden Daten beinhalten u. a. Angaben über die Religionszugehörigkeit, aber auch Meldedaten, für die eine Auskunfts- und Übermittlungssperre (beispielsweise wegen Gefahr für Leib und Leben oder einer Inkognito-Adoption) im Meldedatensatz eingetragen ist. Sie sind daher besonders schutzbedürftig.

Die datenschutzrechtliche Verantwortung für den rechtmäßigen Umgang mit Meldedaten tragen allein die Meldebehörden. Eine Übermittlung in elektronischer Form ist nur dann zulässig, wenn die Identitäten von Absender und Empfänger zweifelsfrei feststehen und wenn die Daten vor dem Transport verschlüsselt werden. Diese Anforderungen werden jedoch häufig missachtet.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, für die elektronische Übertragung von Meldedaten elektronische Signaturen und geeignete Verschlüsselungsverfahren mit öffentlichen Schlüsseln zu verwenden, die der jeweils aktuellen Richtlinie des Bundesamtes für die Sicherheit in der Informationstechnik entnommen sind. Durch Zertifizierung oder Beglaubigung der eingesetzten Schlüssel lassen sich auch bei der Nutzung öffentlicher Netze Absender und Empfänger eindeutig und zuverlässig identifizieren.

Mit dem Online Services Computer Interface (OSCI) steht eine bewährte Infrastruktur für E-Government-Anwendungen zur Verfügung. Die Meldeämter setzen das Verfahren entsprechend der Bundesmeldedatenübermittlungsverordnung u. a. für den Datenabgleich zwischen Meldebehörden verschiedener Länder ein. Wird ein auch nach heutigem Kenntnisstand sicheres Verschlüsselungsverfahren eingesetzt, ist die OSCI-Infrastruktur geeignet, die Sicherheit der Meldedatenübertragung auch an GEZ und öffentlich-rechtliche Religionsgemeinschaften zu gewährleisten. Wie jedes kryptographische Verfahren ist auch das Verfahren OSCI-Transport regelmäßig einer Revision zu unterziehen und weiter zu entwickeln.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt dem Bundesministerium des Innern, die Verwendung von OSCI-Transport für die Übermittlungen an GEZ und die öffentlich-rechtlichen Religionsgemeinschaften vorzuschreiben und fordert die Kommunen und die Innenressorts der Länder auf, unverzüglich die

gesetzlichen Vorgaben bei Datenübermittlungen an die GEZ und öffentlich-rechtliche Religionsgemeinschaften umzusetzen.

### 17.1.16 Entschließung der 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 7./8. November 2012 in Frankfurt (Oder): Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist Versuche zurück, vermeintlich „überzogene“ Datenschutzanforderungen für das Versagen der Sicherheitsbehörden bei der Aufdeckung und Verfolgung rechtsextremistischer Terroristen verantwortlich zu machen und neue Datenverarbeitungsbefugnisse zu begründen.

Sie fordert die Bundesregierung und die Landesregierungen auf, vor einer Reform der Struktur und Arbeitsweise der Polizei- und Verfassungsschutzbehörden zunächst die Befugnisse, den Zuschnitt und die Zusammenarbeit der Verfassungsschutzbehörden vor dem Hintergrund der aufgetretenen Probleme zu evaluieren. Nur auf dieser Grundlage kann eine Diskussion über Reformen seriös geführt und ein Mehrwert für Grundrechtsschutz und Sicherheit erreicht werden.

In datenschutzrechtlicher Hinsicht geklärt werden muss insbesondere, ob die bestehenden Vorschriften in der Vergangenheit richtig angewandt, Arbeitsschwerpunkte richtig gesetzt und Ressourcen zielgerichtet verwendet worden sind. In diesem Zusammenhang ist auch zu untersuchen, ob die gesetzlichen Vorgaben den verfassungsrechtlichen Anforderungen genügen, also verhältnismäßig, hinreichend klar und bestimmt sind. Nur wenn Ursachen und Fehlentwicklungen bekannt sind, können Regierungen und Gesetzgeber die richtigen Schlüsse ziehen. Gründlichkeit geht dabei vor Schnelligkeit.

Schon jetzt haben die Sicherheitsbehörden weitreichende Befugnisse zum Informationsaustausch. Die Sicherheitsgesetze verpflichten Polizei, Nachrichtendienste und andere Behörden bereits heute zu umfassenden Datenübermittlungen. Neue Gesetze können alte Vollzugsdefizite nicht beseitigen.

Bei einer Reform der Sicherheitsbehörden sind der Grundrechtsschutz der Bürgerinnen und Bürger, das Trennungsgebot, die informationelle Gewaltenteilung im Bundesstaat und eine effiziente rechtsstaatliche Kontrolle der Nachrichtendienste zu gewährleisten. Eine effiziente Kontrolle schützt die Betroffenen und verhindert, dass Prozesse sich verselbständigen, Gesetze übersehen und Ressourcen zu Lasten der Sicherheit falsch eingesetzt werden. Nur so kann das Vertrauen in die Arbeit der Sicherheitsbehörden bewahrt und gegebenenfalls wieder hergestellt werden.

Datenschutz und Sicherheit sind kein Widerspruch. Sie müssen zusammenwirken im Interesse der Bürgerinnen und Bürger.

### 17.1.17 Entschließung der 84. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 7./8. November 2012 in Frankfurt (Oder): Einführung von IPv6: Hinweise für Provider im Privatkundengeschäft und Hersteller

Viele Provider werden demnächst in ihren Netzwerken die neue Version 6 des Internet-Protokolls (IPv6) einführen. Größere Unternehmen und Verwaltungen werden ihre Netze meist schrittweise an das neue Protokoll anpassen. Privatkunden werden von dieser Umstellung zuerst betroffen sein.

Für einen datenschutzgerechten Einsatz von IPv6 empfehlen die Datenschutzbeauftragten insbesondere:

- Um das zielgerichtete Verfolgen von Nutzeraktivitäten (Tracking) zu vermeiden, müssen Adresspräfixe grundsätzlich dynamisch an Endkunden vergeben werden. Auch eine Vergabe mehrerer statischer und dynamischer Adresspräfixe kann datenschutzfreundlich sein, wenn Betriebssystem und Anwendungen den Nutzer dabei unterstützen, Adressen gezielt nach der erforderlichen Lebensdauer auszuwählen.
- Entscheidet sich ein Provider für die Vergabe statischer Präfixe an Endkunden, müssen diese Präfixe auf Wunsch des Kunden gewechselt werden können. Hierzu müssen dem Kunden einfache Bedienmöglichkeiten am Router oder am Endgerät zur Verfügung gestellt werden.
- Privacy Extensions müssen auf Endgeräten implementiert und sollten standardmäßig eingeschaltet sein. Ist dies nicht möglich, muss eine benutzerfreundliche manuelle Wechselmöglichkeit für den Interface Identifier bestehen.
- Zusätzlich sollten die Betriebssystem-Hersteller benutzerfreundliche Konfigurationsmöglichkeiten bereitstellen, mit denen Kunden die Wechselfrequenz des Interface Identifiers auf kurze Werte festlegen können bzw. einen Wechsel zu bestimmten Ereignissen anstoßen lassen können, z. B. beim Start des Browsers oder beim Start oder Aufwachen des Rechners.
- Interface Identifier und Präfix sollten synchron gewechselt werden.
- Um den Ortsbezug von Adressen zu verringern, sollten Provider die Adressen für Einwahl-Knoten und sonstige Infrastrukturkomponenten zufällig aus dem ganzen ihnen zur Verfügung stehenden Pool auswählen und regelmäßig innerhalb des Pools wechseln.

- Damit eine sichere und vertrauenswürdige Ende-zu-Ende-Kommunikation mit IPv6 unter Nutzung des Sicherheitsprotokolls IPsec möglich ist, müssen Hersteller von Betriebssystemen starke Verschlüsselungsalgorithmen im TCP/IP-Protokollstack implementieren.
- Die Endgerätehersteller sollten ihre Produkte mit korrekt und sinnvoll vorkonfigurierten IPv6-fähigen Paketfiltern ausstatten und diese über eine leicht zu bedienende Oberfläche zugänglich machen. Bei der Aktivierung der IPv6-Unterstützung im Router sollte die Aktivierung des Paketfilters automatisch stattfinden, dem Nutzer aber zumindest empfohlen werden.
- Hersteller von nicht IPv6-fähigen Firewalls (Firmware und Systemsoftware) sollten entsprechende Updates anbieten. Hersteller von IPv6-fähigen Firewalls sollten den Reifegrad ihrer Produkte regelmäßig prüfen und soweit erforderlich verbessern.
- IPv6-Adressen sind ebenso wie IPv4-Adressen personenbezogene Daten. Sofern eine Speicherung der Adressen über das Ende der Erbringung des Dienstes hinaus unzulässig ist, dürfen Provider und Diensteanbieter IPv6-Adressen allenfalls nach einer Anonymisierung speichern und verarbeiten. Ebenso ist die Ermittlung des ungefähren Standorts eines Endgerätes anhand der IPv6-Adresse für Provider und Diensteanbieter nur nach Anonymisierung der Adresse zulässig. Zur wirkungsvollen Anonymisierung der IPv6-Adressen sollten nach derzeitigem Kenntnisstand mindestens die unteren 88 Bit jeder Adresse gelöscht werden, d. h. der gesamte Interface Identifier sowie 24 Bit des Präfix.
- Der gemeinsame Betrieb von IPv6 und IPv4 auf einem Gerät (Dual-Stack-Betrieb) führt zu erhöhtem Gefahrenpotenzial und sollte daher vermieden werden. Dies gilt auch für die als Übergangslösung gedachten Tunnelprotokolle.
- Bestimmte Arten von Anonymisierungsdiensten sind dazu geeignet, die IP-Adressen von Nutzern wirksam zu verbergen. Auch Peer-to-Peer-Anwendungen können zu einem robusten und datenschutzfreundlichen, weil nicht an einzelnen Punkten stör- und überwachbaren Internet beitragen. Netzbetreiber können die Forschung auf diesem Gebiet unterstützen und selbst Anonymisierungsdienste anbieten. Die Verwendung von Anonymisierungsdiensten und Peer-to-Peer-Anwendungen darf durch Netzbetreiber nicht blockiert werden.

Mit der Orientierungshilfe „Datenschutz bei IPv6 - Hinweise für Hersteller und Provider im Privatkundengeschäft“ präzisieren die Datenschutzbeauftragten des Bundes und der Länder ihre Hinweise vom September 2011.

### 17.1.18 Entschließung zwischen der 84. und 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. Januar 2013: Beschäftigtendatenschutz nicht abbauen, sondern stärken!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erinnert an ihre Entschließung vom 16./17. März 2011 und ihre Forderung nach speziellen Regelungen zum Beschäftigtendatenschutz. Bei einer Gesamtbetrachtung ist die Konferenz enttäuscht von dem jetzt veröffentlichten Änderungsentwurf der Koalitionsfraktionen.

Bereits der ursprünglich von der Bundesregierung vorgelegte Entwurf enthielt aus Datenschutzsicht erhebliche Mängel. Der nun vorgelegte Änderungsentwurf nimmt zwar einzelne Forderungen - etwa zum Konzerndatenschutz - auf und stärkt das informationelle Selbstbestimmungsrecht auch gegenüber Tarifverträgen und Betriebsvereinbarungen. Das Datenschutzniveau für die Beschäftigten soll jedoch in einigen wesentlichen Bereichen sogar noch weiter abgesenkt werden.

Besonders bedenklich sind die folgenden Regelungsvorschläge:

- Die Möglichkeiten der offenen Videoüberwachung am Arbeitsplatz sollen noch über das bisher Geplante hinaus ausgeweitet werden. Überdies ist die Beschreibung der zuzulassenden Überwachungszwecke unverständlich und würde deshalb nicht zur Rechtssicherheit beitragen.
- Beschäftigte in Call-Centern sollen noch stärker überwacht werden können, als dies der Regierungsentwurf ohnehin schon vorsah. Die Beschäftigten müssen sich nunmehr auf eine jederzeit mögliche, unbemerkte Überwachung einstellen. Hierdurch kann ein unzumutbarer Überwachungsdruck entstehen.
- Die Datenerhebungsbefugnisse im Bewerbungsverfahren sollen erweitert werden. Der noch im Regierungsentwurf vorgesehene Ausschluss von Arbeitgeberrecherchen über Bewerberinnen und Bewerber in sozialen Netzwerken außerhalb spezieller Bewerbungsportale wurde gestrichen. Damit wird der Grundsatz der Direkterhebung bei den Betroffenen weiter unterlaufen.
- Dem Arbeitgeber soll es gestattet sein, auch nicht allgemein zugängliche Beschäftigtendaten bei Dritten zu erheben, wenn die Beschäftigten eingewilligt haben. Die tatsächliche Freiwilligkeit einer solchen Einwilligung ist fraglich.
- Die im Regierungsentwurf enthaltene Vorgabe, Eignungstests grundsätzlich nach wissenschaftlich anerkannten Methoden durchzuführen, soll wieder entfallen.

Die Konferenz appelliert an den Bundestag, bei seinen Beratungen zum Gesetz den Forderungen der Datenschutzbeauftragten Rechnung zu tragen.

### 17.1.19 Entschließung der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 13./14. März 2013 in Bremerhaven: Europa muss den Datenschutz stärken

Das Europäische Parlament und der Rat der Europäischen Union bereiten derzeit ihre Änderungsvorschläge für den von der Europäischen Kommission vor einem Jahr vorgelegten Entwurf einer Datenschutz-Grundverordnung für Europa vor. Aktuelle Diskussionen und Äußerungen aus dem Europäischen Parlament und dem Rat lassen die Absenkung des derzeitigen Datenschutzniveaus der Europäischen Datenschutzrichtlinie von 1995 befürchten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erinnert alle Beteiligten des Gesetzgebungsverfahrens daran, dass das Europäische Parlament in seiner Entschließung vom 6. Juli 2011 zum damaligen Gesamtkonzept für Datenschutz in der Europäischen Union (2011/2025(INI)) sich unter Hinweis auf die Charta der Grundrechte der Europäischen Union und insbesondere auf Artikel 7 und 8 der Charta einhellig dafür ausgesprochen hat, die Grundsätze und Standards der Richtlinie 95/46/EG zu einem modernen Datenschutzrecht weiterzuentwickeln, zu erweitern und zu stärken. Das Europäische Parlament hat eine volle Harmonisierung des Datenschutzrechts auf höchstem Niveau gefordert.

Die Datenschutzbeauftragten von Bund und Ländern setzen sich dafür ein, dass die wesentlichen Grundpfeiler des Datenschutzes erhalten und ausgebaut werden. Sie wenden sich entschieden gegen Bestrebungen, den Datenschutz zu schwächen. Insbesondere fordern sie:

- Jedes personenbeziehbare Datum muss geschützt werden: Das europäische Datenschutzrecht muss unterschiedslos alle Daten erfassen, die einer natürlichen Person zugeordnet werden können. Dies schließt auch pseudonyme Daten oder Identifizierungsmerkmale wie beispielsweise IP-Adressen ein.
- Es darf keine grundrechtsfreien Räume geben: Die generelle Herausnahme von bestimmten Datenkategorien und Berufs- und Unternehmensgruppen ist daher abzulehnen.
- Einwilligungen müssen ausdrücklich erteilt werden: Einwilligungen in die Verarbeitung personenbezogener Daten dürfen nur dann rechtswirksam sein, wenn sie auf einer eindeutigen, freiwilligen und informierten Willensbekundung der Betroffenen beruhen. Auch deshalb muss eine gesetzliche Pflicht geschaffen werden, die Kompetenz zum Selbstdatenschutz zu fördern.

- Datenverarbeiter dürfen ihre Ziele nicht eigenmächtig verändern: Die Zweckbindung als zentraler Baustein zur Gewährleistung der Transparenz und Vorhersehbarkeit der Datenverarbeitung muss ohne Abstriche erhalten bleiben.
- Profilbildung muss beschränkt werden: Für die Zusammenführung und Auswertung vieler Daten über eine Person müssen enge Grenzen gelten.
- Stärkung der Eigenverantwortung der Datenverarbeiter durch betriebliche Datenschutzbeauftragte: Betriebliche Datenschutzbeauftragte sollten europaweit eingeführt, obligatorisch bestellt und in ihrer Stellung gestärkt werden. Sie sind ein wesentlicher Bestandteil der Gesamtstruktur einer effektiven Datenschutzkontrolle.
- Datenverarbeiter dürfen sich ihre Aufsichtsbehörde nicht aussuchen können: Es ist auszuschließen, dass sich Datenverarbeiter ihre Aufsichtsbehörde durch die Festlegung ihrer Hauptniederlassung aussuchen. Neben der federführenden Aufsichtsbehörde des Hauptsitzlandes müssen auch die anderen jeweils örtlich zuständigen Kontrollbehörden inhaltlich beteiligt werden.
- Völlige Unabhängigkeit der Aufsichtsbehörden auch gegenüber der Kommission: Die Datenschutz-Aufsichtsbehörden müssen unabhängig und verbindlich über die Einhaltung des Datenschutzes entscheiden. Ein Letztentscheidungsrecht der Kommission verletzt die Unabhängigkeit der Aufsichtsbehörden und des künftigen Europäischen Datenschutzausschusses.
- Grundrechtsschutz braucht effektive Kontrollen: Um die datenschutzrechtliche Kontrolle in Europa zu stärken, müssen die Aufsichtsbehörden mit wirksamen und flexiblen Durchsetzungsbefugnissen ausgestattet werden. Die Sanktionen müssen effektiv und geeignet sein, damit die Verantwortlichen und Datenverarbeiter die Datenschutzvorschriften nachhaltig beachten. Ohne spürbare Bußgelddrohungen bleibt die Datenschutzkontrolle gegen Unternehmen zahnlos.
- Hoher Datenschutzstandard für ganz Europa: Soweit etwa im Hinblick auf die Sensitivität der Daten oder sonstige Umstände ein über die Datenschutz-Grundverordnung hinausgehender Schutz durch nationale Gesetzgebung erforderlich ist, muss dies möglich bleiben. Jedenfalls hinsichtlich der Datenverarbeitung durch die öffentliche Verwaltung müssen die Mitgliedstaaten auch zukünftig strengere Regelungen und damit ein höheres Datenschutzniveau in ihrem nationalen Recht vorsehen können.

**Erläuterungen zur Entschließung: „Europa muss den Datenschutz stärken“**

**- Jedes personenbeziehbare Datum muss geschützt werden**

Nach Artikel 8 Abs. 1 der Charta der Grundrechte der Europäischen Union (Grundrechtecharta) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Daher muss das europäische Datenschutzrecht unterschiedslos alle Da-

ten erfassen, die einer natürlichen Person zugeordnet werden können. Personenbezogene Daten sollten als Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person definiert werden. Dies schließt auch pseudonyme Daten oder Identifizierungsmerkmale wie z. B. IP-Adressen, Kenn-Nummern, Standortdaten ein.

**- Es darf keine grundrechtsfreien Räume geben**

Die Bestrebungen, ganze Datenkategorien wie etwa Beschäftigtendaten und ganze Berufsgruppen wie Freiberufler aus dem Anwendungsbereich des Datenschutzgrundrechtes herauszunehmen, kollidiert mit dem Grundsatz der universalen Geltung von Grundrechten. Die pauschale Entbindung von kleinen, mittleren und Kleinstunternehmen von zentralen datenschutzrechtlichen Verpflichtungen verkennt, dass es für den Grad des Eingriffes in das Grundrecht unerheblich ist, wie viele Beschäftigte das in dieses Recht eingreifende Unternehmen hat.

**- Einwilligungen müssen ausdrücklich erteilt werden**

Die Einwilligung in die Verarbeitung personenbezogener Daten kann nur dann rechtswirksam sein, wenn sie auf einer eindeutigen und ausdrücklichen Willensbekundung des Betroffenen in Kenntnis der Sachlage beruht. An der Anforderung, dass eine wirksame Einwilligung auf tatsächlich freiwilliger Entscheidung beruhen muss, darf es keine Abstriche geben. Eine unter faktischem Zwang abgegebene Erklärung muss auch weiterhin unwirksam sein. Aufweichungen der Vorschläge der Kommission und des Berichterstatters im federführenden Ausschuss für Bürgerrechte sowie der Forderungen des Europäischen Parlaments in dessen Entschließung vom 6. Juli 2011 (Punkte 11, 12) darf es - auch mit Blick auf Artikel 8 Abs. 2 der Grundrechtecharta - nicht geben. Es gilt, die Kompetenz zum Selbstdatenschutz zu fördern.

**- Datenverarbeiter dürfen ihre Ziele nicht eigenmächtig verändern**

Der bestehende Grundsatz der Zweckbindung ist ein zentraler Baustein zur Gewährleistung der Transparenz und Vorhersehbarkeit der Datenverarbeitung und muss erhalten bleiben, so wie es auch - in Anlehnung an Artikel 8 Abs. 2 der Grundrechtecharta - das Europäische Parlament in der Entschließung vom 6. Juli 2011 (Punkt 11) gefordert hat. Daten sollen auch zukünftig nur für den Zweck verarbeitet werden dürfen, zu dem sie erhoben wurden. Ergänzend sollte geregelt werden, dass die Zwecke, für die personenbezogene Daten erhoben werden, konkret festzulegen sind.

**- Profilbildung muss beschränkt werden**

Die Profilbildung, also die Zusammenführung vieler Daten über eine bestimmte Person, muss effektiv beschränkt werden. Die vorgelegten Vorschläge dürfen nicht minimiert werden. Die Anforderungen an die Rechtmäßigkeit der Profilbildung müssen

vielmehr erhöht und festgelegt werden, dass besondere Kategorien personenbezogener Daten wegen ihrer hohen Sensitivität nicht in eine Profilbildung einfließen dürfen. Die Profilbildungsregelung muss auf jede systematische Verarbeitung zur Profilbildung Anwendung finden. Zudem muss klargestellt werden, dass auch der Online-Bereich, beispielsweise die Auswertung des Nutzerverhaltens oder die Bildung von Sozialprofilen in sozialen Netzwerken zur adressatengerechten Werbung und Scoring-Verfahren mit erfasst sind.

- **Stärkung der Eigenverantwortung der Datenverarbeiter durch betriebliche Datenschutzbeauftragte**
  Die Konferenz weist auf die positiven Erfahrungen mit den betrieblichen Datenschutzbeauftragten in Deutschland hin. Das Vorhaben der Kommission, eine Bestellungspflicht für einen Datenschutzbeauftragten erst ab 250 Beschäftigten zu normieren, bedroht insofern eine gewachsene und erfolgreiche Struktur des betrieblichen Datenschutzes in Deutschland. Bei risikobehafteter Datenverarbeitung sollte die Bestellungspflicht unabhängig von der Mitarbeiterzahl bestehen. Die Eigenverantwortung der Datenverarbeiter darf auch nicht dadurch abgeschwächt werden, dass die Aufsichtsbehörden Verfahren in großem Umfang vorab genehmigen oder dazu vorab zu Rate gezogen werden müssen. Vielmehr muss die Eigenverantwortlichkeit zunächst durch eine leistungsfähige Selbstkontrolle gewährleistet werden.

- **Datenverarbeiter dürfen sich ihre Aufsichtsbehörde nicht aussuchen können**
  Ein kohärenter Datenschutz in der EU setzt neben einer einheitlichen Regelung auch eine einheitliche Auslegung und einen einheitlichen Rechtsvollzug durch die Aufsichtsbehörden voraus. Bei einer ausschließlichen Zuständigkeit einer Aufsichtsbehörde ist zu befürchten, dass das Unternehmen seine Hauptniederlassung jeweils in dem Mitgliedstaat nimmt, in dem mit einem geringeren Grad an Durchsetzungsfähigkeit oder Durchsetzungswillen der jeweiligen Aufsichtsbehörde gerechnet wird. Eine Aufweichung der Datenschutzstandards wäre die Folge. Für den Fall der Untätigkeit einer federführenden Behörde müssen rechtliche Strukturen gefunden werden, die einen effektiven Vollzug des Datenschutzrechts gewährleisten.

- **Völlige Unabhängigkeit der Aufsichtsbehörden auch gegenüber der Kommission**
  Ein Letztentscheidungsrecht der Kommission bei der Rechtsdurchsetzung, wie im Kommissionsentwurf vorgesehen, verletzt die Unabhängigkeit der datenschutzrechtlichen Aufsichtsbehörden und des europäischen Datenschutzausschusses und ist daher abzulehnen. Diese Kompetenzen der Kommission sind mit Artikel 8 Abs. 3 der Grundrechtecharta und Art. 16 Abs. 2 Satz 2 des Vertrages über die Arbeitsweise der EU (AEUV) nicht vereinbar, wonach die Einhaltung des EU-Datenschutzes unabhängigen Aufsichtsbehörden übertragen ist. In Anlehnung an die Forderungen des

Europäischen Parlaments in der Entschließung vom 6. Juli 2011 (Punkte 42 bis 44) sollte als Folge der Unabhängigkeit der Aufsichtsbehörden statt der Kommission ausschließlich der Europäische Datenschutzausschuss über Sachverhalte und Maßnahmen, die dem Kohärenzverfahren unterfallen, entscheiden.

**- Grundrechtsschutz braucht effektive Kontrollen**

Die Sanktionen müssen - wie schon das Europäische Parlament in der Entschließung vom 6. Juli 2011 (Punkt 33) deutlich gemacht hat - abschreckend und damit geeignet sein, dass die Verantwortlichen und Datenverarbeiter die Datenschutzvorschriften nachhaltig einhalten. Die Aufsichtsbehörden müssen im Rahmen ihrer Unabhängigkeit darüber entscheiden können, ob und inwieweit sie von den Sanktionsmöglichkeiten Gebrauch machen. Ohne spürbare Bußgelddrohungen würde die Datenschutzkontrolle gegen Unternehmen zahnlos bleiben. Die von der Kommission vorgesehenen Sanktionsmöglichkeiten sollten daher auf jeden Fall beibehalten werden.

**- Hoher Datenschutzstandard für ganz Europa**

Für Bereiche ohne konkreten Bezug zum Binnenmarkt sehen einige Mitgliedstaaten bereits heute zahlreiche Regelungen vor, die über den Datenschutzstandard der allgemeinen Datenschutzrichtlinie 95/46 EG hinausgehen. Sie berücksichtigen unter anderem besondere Schutzbedarfe und haben maßgeblich zur Fortentwicklung des europäischen Datenschutz-Rechtsrahmens beigetragen. Deshalb sollte eine Datenschutz-Grundverordnung Gestaltungsspielräume für einen weitergehenden Datenschutz eröffnen.

### 17.1.20 Entschließung der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 13./14 März 2013 in Bremerhaven: Datenschutz auch in einer transatlantischen Freihandelszone gewährleisten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist auf die Notwendigkeit hin, bei den angekündigten Verhandlungen zwischen der Europäischen Union und der Regierung der Vereinigten Staaten über eine transatlantische Freihandelszone auch die unterschiedlichen datenschutzrechtlichen Rahmenbedingungen zu thematisieren. Dabei muss sichergestellt werden, dass das durch die Europäische Grundrechtecharta verbriefte Grundrecht auf Datenschutz und die daraus abgeleiteten Standards gewahrt bleiben.

Von der Kommission erwartet die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass sie bei den Verhandlungen das Ziel einer grundrechtsorientierten Wertegemeinschaft nicht aus dem Auge verliert. Keineswegs dürfen durch die angestrebte transatlantische Wirtschaftsunion europäische Grundrechtsgewährleistungen

abgeschwächt werden. Auch wäre es nicht hinzunehmen, wenn sich die Verhandlungen negativ auf den durch die Europäische Kommission angestoßenen Reformprozess des EU-Datenschutzrechts auswirken würden.

Die Konferenz sieht in der vom US-Präsidenten vorgeschlagenen Freihandelszone die Chance, international eine Erhöhung des Datenschutzniveaus zu bewirken. Sie begrüßt daher die vom US-Präsidenten angekündigte Initiative für verbindliche Vorgaben zum Datenschutz in der Wirtschaft. Sie erinnert daran, dass nach den Vorgaben der Welthandelsorganisation der Datenschutz kein Handelshindernis darstellt.

### 17.1.21 Entschließung der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 13./14. März 2013 in Bremerhaven: Soziale Netzwerke brauchen Leitplanken - Datenschutzbeauftragte legen Orientierungshilfe vor

Angesichts der zunehmenden Bedeutung sozialer Netzwerke erinnert die Datenschutzkonferenz deren Betreiber an ihre Verpflichtung, die Einhaltung datenschutzrechtlicher Anforderungen sicherzustellen. Auch Unternehmen und öffentliche Stellen, die soziale Netzwerke nutzen, müssen diesen Anforderungen Rechnung tragen. Die Erfahrung der Aufsichtsbehörden zeigt, dass der Schutz der Privatsphäre von den Betreibern sozialer Netzwerke nicht immer hinreichend beachtet wird.

Häufig vertrauen die Nutzenden den Betreibern dieser Dienste sehr persönliche Informationen an. Auch die Vielfalt der Informationen, die innerhalb eines Netzwerkes aktiv eingestellt oder über die Nutzerinnen und Nutzer erhoben werden, ermöglicht einen tiefen Einblick in deren persönliche Lebensgestaltung.

Es zeichnet sich ab, dass die angekündigte Selbstregulierung für soziale Netzwerke - insbesondere auf Grund der mangelnden Bereitschaft einiger großer Netzwerk-Betreiber - den erforderlichen Datenschutzstandard nicht gewährleisten kann. Deshalb haben die Datenschutzbeauftragten des Bundes und der Länder die Orientierungshilfe „Soziale Netzwerke“ erarbeitet. Sie soll die Betreiber sozialer Netzwerke und die die Netzwerke nutzenden öffentlichen und privaten Stellen bei der datenschutzgerechten Gestaltung und Nutzung der Angebote unterstützen. Die Konferenz weist darauf hin, dass der vorhandene Rechtsrahmen zur Gewährleistung eines angemessenen Datenschutzes bei sozialen Netzwerken weiterentwickelt werden muss, insbesondere in Bezug auf konkrete und präzise Vorgaben zu datenschutzfreundlichen Voreinstellungen, zum Minderjährigenschutz, zur Löschungsverpflichtung bei Dritten und zum Verhältnis von Meinungsfreiheit und Persönlichkeitsrecht. Ferner wird die Verantwortlichkeit für den Umgang mit Nutzungsdaten in Bezug auf Social Plug-Ins, Fanpages sowie für den

Einsatz von Cookies von vielen Unternehmen und Behörden in Abrede gestellt. Der europäische und nationale Gesetzgeber bleiben aufgefordert, für die notwendige Klarheit zu sorgen und damit einen ausreichenden Datenschutzstandard zu sichern. Darauf weist die Konferenz der Datenschutzbeauftragten erneut nachdrücklich hin.

### 17.1.22 Entschließung der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 13./14. März 2013 in Bremerhaven: Pseudonymisierung von Krebsregisterdaten verbessern

In allen Ländern werden Daten über individuelle Fälle von Krebserkrankungen in Krebsregistern gespeichert, um sie der epidemiologischen Forschung zur Verfügung zu stellen. Zum Schutz der Betroffenen werden die Daten in allen Ländern (außer Hamburg) mit Kontrollnummern nach § 4 Bundeskrebsregisterdatengesetz (BKRG) pseudonymisiert gespeichert. Als Pseudonyme werden so genannte Kontrollnummern verwendet. Kontrollnummern werden darüber hinaus von allen Ländern zum Abgleich der Daten der epidemiologischen Krebsregister untereinander und mit dem Zentrum für Krebsregisterdaten nach § 4 BKRG verwendet.

Die Datenschutzbeauftragten von Bund und Ländern sind der Auffassung, dass das vor ca. 20 Jahren entwickelte Verfahren zur Bildung der Kontrollnummer den erforderlichen Schutz dieser höchst sensiblen Daten nicht mehr in ausreichendem Maße gewährleisten kann. Dies ist auf die folgenden Entwicklungen zurückzuführen:

- Das Anwachsen der für eine Depseudonymisierung verfügbaren Rechenkapazität hat die Schutzwirkung der bei den Krebsregistern genutzten kryptographischen Hashfunktion aufgehoben, die derzeit als erste Komponente bei der Kontrollnummernbildung verwendet wird.
- Die Wechselwirkungen zwischen mehreren Verfahren im Umfeld der epidemiologischen Krebsregistrierung verursachen Risiken im Zuge der erforderlichen Entschlüsselungen und der gemeinsamen Verwendung von geheimen Schlüsseln, die bisher nicht berücksichtigt wurden.

Diese Entwicklungen machen es erforderlich, die Regeln zur Bildung der Kontrollnummern zu überarbeiten. Hierbei ist das Umfeld aller Verfahren in Betracht zu ziehen, in dem Kontrollnummern zum Einsatz kommen bzw. absehbar kommen sollen. Hierzu hat der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzkonferenz einen entsprechenden Anforderungskatalog formuliert (siehe Anlage zu dieser Entschließung).

Die Datenschutzkonferenz fordert die zuständigen Fachaufsichtsbehörden der Länder auf, für eine koordinierte Umstellung des Verfahrens bei den ihrer Aufsicht unterstehen-

den Stellen zu sorgen, die Kontrollnummern bilden oder verwenden. Sie empfiehlt den Ländern, für den Datenaustausch klinischer Krebsregister mit den Auswertungsstellen der klinischen Krebsregistrierung auf Landesebene nach dem Krebsfrüherkennungs- und -registergesetz ein Pseudonymisierungsverfahren anzuwenden, das im Wesentlichen den gleichen Anforderungen genügt.

Die entsprechenden Vorgaben für den Datenabgleich nach § 4 BKRG sollten durch das Bundesministerium für Gesundheit in einer Verordnung nach § 4 Abs. 3 BKRG festgelegt werden.

**Anforderungen an die Bildung von Kontrollnummern zur Pseudonymisierung von Daten über individuelle Fälle von Krebserkrankungen (Anlage zur Entschließung „Pseudonymisierung von Krebsregisterdaten verbessern“)**

Mindestens folgende Anforderungen sind an die zukünftige Gestaltung und den Einsatz des Algorithmus zur Bildung von Kontrollnummern zur Pseudonymisierung von Daten über individuelle Fälle von Krebserkrankungen zu stellen:

- Die kryptografischen Komponenten sind unter Berücksichtigung der Empfehlungen des BSI gemäß dem derzeitigen Stand der Technik zu wählen. Ihre Sicherheitseigenschaften sollen auf unabhängigen kryptografischen Annahmen beruhen. Beide Komponenten müssen sich durch geheim zu haltende Schlüssel parametrisieren lassen.
- Zur Wahrung der Verknüpfbarkeit des derzeitigen Datenbestandes mit zukünftigen Meldungen kann eine Überverschlüsselung der ersten Stufe der derzeitigen Kontrollnummern (dem Ergebnis der Anwendung einer Hashfunktion auf Bestandteile der Identitätsdaten) erfolgen.
- Eine flexible Ausgestaltung des Verfahrens soll vorausschauend berücksichtigen, dass auch in Zukunft mit der Notwendigkeit des Austauschs von kryptografischen Methoden zu rechnen ist.
- Die Sicherheit des verwendeten Schlüsselmaterials wie auch seiner Nutzung ist bei allen Beteiligten durch Maßnahmen der Systemsicherheit, den Einsatz von dem Stand der Technik entsprechenden Kryptomodulen und die Protokollierung von Einsatz und Administration auf einheitlichem Schutzniveau zu gewährleisten.
- Für jedes Register und jedes Abgleichverfahren sind zumindest in der zweiten Stufe der Kontrollnummernbildung spezifische Schlüssel einzusetzen.
- Bei einem Abgleich von Registerdaten ist zu gewährleisten, dass keine Zwischenwerte gebildet werden, aus denen Rückschlüsse auf Identitätsdaten möglich sind.

# Stichwortverzeichnis