Der Bayerische Landesbeauftragte für den Datenschutz informiert die Öffentlichkeit

27. Tätigkeitsbericht

Berichtszeitraum
2015/2016

27. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

(gemäß Artikel 30 Absatz 5
des Bayerischen Datenschutzgesetzes – BayDSG)

Berichtszeitraum: 2015/2016
Veröffentlichungsdatum: 31. Januar 2017

Inhaltsverzeichnis

1 Überblick ... 13

1.1 Europa ... 13

1.1.1 In Vielfalt geeint? Zur erfolgten Teilreform des EU-Datenschutzrechts ... 13

1.1.1.1 Datenschutz-Grundverordnung ... 14

1.1.1.2 Richtlinie für den Datenschutz der Strafjustiz ... 16

1.1.1.3 Wesentliche Neuerungen ... 17

1.1.1.4 Anpassung der allgemeinen Datenschutzgesetze des Bundes und des Freistaats Bayern an das neue europäische Datenschutzrecht ... 18

1.1.2 Geplante weitere EU-Reformen: Datenschutzverordnung 2001/45/EG und E-Privacy-Richtlinie ... 19

1.1.3 Safe Harbor-Abkommen ungültig – EU-US Privacy Shield in Kraft ... 19

1.1.4 Verantwortlichkeit der Anbieter von Facebook-Fanseiten ... 21

1.2 Deutschland ... 22

1.2.1 Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes ... 22

1.2.2 E-Health-Gesetz, GKV-Versorgungsverstärkungsgesetz ... 23

1.3 Freistaat Bayern ... 26

1.3.1 Bayerisches E-Government-Gesetz ... 26

1.3.2 Insbesondere: Allgemeines Auskunftsrecht ... 26

1.3.3 Änderung des Bayerischen Verfassungsschutzgesetzes ... 26

1.3.4 Regelung der Schülerunterlagen ... 27

1.3.5 Behördliche Datenschutzbeauftragte an allen bayerischen Finanzämtern ... 27

1.4 Öffentlichkeitsarbeit ... 27

1.5 Schlussbemerkungen ... 28

2 Informations- und Kommunikationstechnik und Organisation ... 29

2.1 Grundsatz- und Einzelthemen ... 29

2.1.1 Einsatz staatlich freigegebener Verfahren in den Kommunen – Gesetzesänderung ... 29

2.1.2 Schutz vor Ransomware ... 30

2.1.3 Versenden von E-Mails an mehrere Empfängerinnen und Empfänger ... 32

2.1.4 Nutzung des E-Postbriefs ... 33

2.1.5 IT-Abschottung von Statistikstellen ... 34

2.1.6 Verkehrsflussanalyse mit gekauften anonymisierten Daten ... 35

2.1.7 Veröffentlichung privater E-Mail-Adressen von Kreistags-, Stadtrats- oder Gemeinderatsmitgliedern ... 36

2.1.8 Videoüberwachung im Krankenhaus ... 36

2.1.9 Berechtigungskonzepte und Protokollierung in Krankenhäusern ... 38

2.2 Prüfungen ... 39

2.2.1 Geprüfte Einrichtungen ... 39
2.2.2 Auftragsdatenverarbeitung bei der Aktenverwaltung und Entsorgungskonzepte in Kliniken ... 40
2.2.3 Apps – Anwendungen für mobile Endgeräte ... 41
2.2.4 Spam-Abwehr auf E-Mail-Servern ... 44
2.2.5 NAKO-Gesundheitsstudie: Prüfung Studienzentrum Regensburg ... 46
2.2.6 Immatrikulationsbescheinigung online ... 47
2.3 Beanstandungen ... 48
2.4 Orientierungshilfen ... 49
3 Polizei ... 50
3.1 Allgemeines ... 50
3.1.1 Änderungsbedarf des Polizeiaufgabengesetzes ... 50
3.1.2 Precobs ... 52
3.1.3 Erlass einer neuen Meldedatenverordnung ... 54
3.2 G7-Gipfel ... 54
3.3 Polizeiliche Kontrolle von Schmuckankaufstellen ... 56
3.4 Polizeiliche Beobachtung ... 56
3.5 Einsatz von Videotechnik ... 58
3.5.1 Videoüberwachung durch Zugriff auf Kameras der Verkehrsbetriebe ... 58
3.5.2 Erhebung der Daten nichtpolizeilicher Videokameras anlässlich des G7-Gipfels ... 58
3.6 Speicherungen in polizeilichen Dateien ... 59
3.6.1 Prüfung der Speicherungsvoraussetzung „polizeilicher Restverdacht" – grundlegende Folgerungen aus meiner Prüfung ... 59
3.6.2 Bundesweite Speicherung polizeilicher Daten in PIAV ... 61
3.6.3 Speicherung von Lichtbildern ... 63
3.6.4 Löschung von IGVP-Speicherungen ... 63
3.6.5 Speicherungen im Kriminalaktennachweis trotz fehlenden Restverdachts – Einzelfälle ... 64
3.6.6 Reduzierte Dauer bei der Speicherung von Erstkonsumenten „weicher" Drogen ... 65
3.6.7 Speicherungen in der Falldatei Rauschgift (FDR) ... 65
3.6.8 Prüfung erkennungsdienstlicher Maßnahmen ... 67
3.7 Anfertigen einer Personalausweiskopie durch die Polizei ... 68
3.8 Datenübermittlungen ... 69
3.8.1 Weitergabe von Zeugendaten bei einem Verkehrsunfall ... 69
3.8.2 Datenübermittlungen an Fahrerlaubnisbehörden ... 69
3.8.3 Prüfung des Gemeinsamen Terrorismusabwehrzentrums (GTAZ) ... 70
3.9 Ermittlungen in sozialen Netzwerken ... 70

3.10 Auskunftsersuchen ... 71
3.10.1 Rücksendung von Ausweiskopien ... 71
3.10.2 Bearbeitungsdauer von Auskunfts- und Löschanträgen ... 71

4 Verfassungsschutz ... 73

4.1 Novellierung des Bayerischen Verfassungsschutzgesetzes (BayVSG) ... 73
4.2 Dokumentenmanagementsystem beim Landesamt für Verfassungsschutz ... 76
4.3 Löschmoratorien zur Unterstützung von parlamentarischen Untersuchungsausschüssen ... 77
4.4 Prüfungen ... 78
4.4.1 Prüfung des Gemeinsamen Terrorismusabwehrzentrums (GTAZ) ... 78
4.4.2 Teilnahme des Landesamts für Verfassungsschutz an einer staatsanwaltlichen Durchsuchung ... 79

5 Justiz ... 82

5.1 Gesetze, Verordnungen und Verwaltungsvorschriften ... 82
5.1.1 Künftige Auswirkungen der Richtlinie für den Datenschutz der Strafjustiz ... 82
5.1.2 Vorratsdatenspeicherung ... 83
5.1.3 Aufbewahrung von Notariatsunterlagen und Errichtung eines elektronischen Urkundenarchivs ... 84
5.1.4 Anti-Doping-Gesetz ... 85
5.1.5 Einsicht des Europäischen Komitees zur Verhütung von Folter (CPT) in die Personal- und Gesundheitsakten von Gefangenen ... 86
5.1.6 Wiedereinführung der Regelanfrage beim Landesamt für Verfassungsschutz für die Richterschaft ... 87
5.2 Auskunftsersuchen der Landesjustizkasse an Jobcenter ... 89
5.3 Strafverfolgung ... 90
5.3.1 Wiederherstellung von „gelöschten“ Fotos mit Zustimmung der Berechtigten ... 90
5.3.2 Prüfung von Funkzellenabfragen ... 90
5.3.3 Automatische Angabe des Geburtsdatums von Angeklagten in forumSTAR-Straf ... 94
5.3.4 Umfang einer Einstellungsmitteilung an Anzeigeerstatter ... 95
5.3.5 Mitteilungen der Staatsanwaltschaft zum Wählerverzeichnis ... 95
5.3.6 Beschriftung von Aktenordnern ... 96
5.4 Prüfung von Jugendarrestanstalten ... 96
5.5 Strafvollzug ... 97
5.5.1 Videoüberwachung ... 97
5.5.2 Kopieren eines unverschlossenen, nicht der Überwachung unterliegenden Briefes ... 98
5.5.3 Versand von Gesundheitsdaten per Telefax an falschen Empfänger ... 99

5.6 Bildaufnahmen zur Verfolgung von Parkverstößen ... 100

6 Kommunales ... 101

6.1 Videoüberwachung im öffentlichen Raum durch Kommunen ... 101
6.1.1 Überblick über Art. 21a BayDSG ... 101
6.1.2 Anwendbarkeit des Art. 21a BayDSG auf Kameraattrappen ... 102
6.1.3 Hinreichende Gefahr für bestimmte Rechtsgüter ... 103
6.1.4 Nachweis der Gefahr durch eine Vorfallsdokumentation ... 104

6.2 Digitalisierung von archivierten Personenstandsdaten ... 104

6.3 Einbau und Betrieb „intelligenter" Wasserzähler ... 107
6.3.1 Notwendigkeit einer formell-gesetzlichen Rechtsgrundlage ... 108
6.3.2 Freiwilliger Einbau und Betrieb von „intelligenten" Wasserzählern ... 109
6.3.3 Fazit ... 109

6.4 Bestellung eines behördlichen Datenschutzbeauftragten für mehrere öffentliche Stellen ... 109

6.5 Geschwindigkeitsanzeigetafeln ... 112

6.6 Datenschutz bei Bürgerbegehren ... 113

6.7 Datenübermittlung zur Bekämpfung von Sozialleistungsmissbrauch ... 113

6.8 Veröffentlichung von Sitzungsvorlagen im Internet ... 114

6.9 Bekanntgabe von Bauherrendaten in öffentlicher Gemeinderatssitzung und der Tagesordnung ... 116

6.10 Dauerhafte Speicherung der Aufzeichnungen von Stadt- und Gemeinderatssitzungen ... 116
6.10.1 Einrichtung einer Internet-Mediathek über aufgezeichnete Sitzungen ... 116
6.10.2 Archivierung von zur Erstellung der Niederschrift dienenden Audioaufzeichnungen ... 118

6.11 Einstellung öffentlicher Bekanntmachungen mit personenbezogenen Daten in das Internet ... 118

6.12 Schwärzung von personenbezogenen Daten bei Eingaben ... 119

6.13 Datenerhebung durch Kommunen zur Feststellung der Hundehaltung ... 120

6.14 Auskunft an die eine Anzeige erstattende Person ... 121

6.15 Kenntnisnahme des Nachbarn von den Baukosten im Baugenehmigungsverfahren ... 123

6.16 Novellierung des Melderechts ... 124
6.16.1 Melderecht als „Rückgrat" der Informationsverwaltung ... 124
6.16.2 Melderegisterauskünfte ... 125
6.16.2.1 Einfache Melderegisterauskunft ... 125
6.16.2.2 Auskunftssperre nach § 51 Abs. 1 BMG ... 125

6.17 Übermittlung von Meldedaten an den Beitragsservice der öffentlich-rechtlichen Landesrundfunkanstalten (ARD), des Zweiten Deutschen Fernsehens (ZDF) und des Deutschlandradios ... 126

7 Gesundheitswesen ... 128

7.1 Wearables und Gesundheits-Apps ... 128

7.2 Flüchtlinge und Asylsuchende ... 130

7.2.1 Videoüberwachung von Unterkünften für Asylsuchende ... 130

7.2.2 Video- und Telefondolmetscher in Aufnahmeeinrichtungen für Asylsuchende ... 132

7.2.3 Gesundheitsuntersuchung bei Flüchtlingen ... 133

7.2.4 Datenübermittlung im Rahmen der Beratung und Betreuung von Asylsuchenden durch Wohlfahrtsverbände und Helferkreise ... 134

7.2.5 Einwilligung der Asylsuchenden gegenüber dem Landratsamt zur Datenübermittlung an verschiedene Stellen ... 136

7.3 Krebsregister ... 137

7.4 Gesundheitsamt ... 141

7.4.1 Vorlage von Impfnachweisen bei Schuleingangsuntersuchungen und weiteren schulischen Impfberatungen ... 141

7.4.2 Weitergabe von Gesundheitsdaten an die Polizei ... 142

7.4.3 Gesundheits- und Entwicklungsscreening im Kindergartenalter (GESiK) ... 143

7.4.4 Leitfaden „Einhaltung datenschutzrechtlicher Bestimmungen bei Gesundheitsämtern“ ... 143

7.5 Krankenhaus ... 144

7.5.1 Externe Dienstleistungen ... 144

7.5.2 Grundsätzlich kostenfreie Auskunftserteilung ... 146

7.5.3 Verzicht auf eine Datennutzung bei Einwilligungen ... 147

7.6 Bayerisches Gesundheitsdatenzentrum ... 147

8 Sozialwesen ... 149

8.1 Gesetzliche Krankenversicherung ... 149

8.1.1 Datenschutzrechtliche Befugnisse der Krankenkassen im Rahmen des Krankengeldfallmanagements ... 149

8.1.2 Umschlagverfahren ... 151

8.1.3 Datenschutzrechtliche Befugnisse bei Anschlussrehabilitation ... 152

8.1.4 Datenschutzrechtliche Befugnisse im Rahmen der besonderen Versorgung ... 153

8.1.5 Gewinnspiele von Krankenkassen ... 153

8.1.6 Einkommensnachweise für Krankenkassen ... 154

8.1.7 Videoüberwachung einer Krankenkasse ... 155

8.2 Pflege ... 156

8.2.1 Vollzug des Pflege- und Wohnqualitätsgesetzes ... 156

8.3 Sozialbehörden ... 158
8.3.1 Anforderung von Kontounterlagen ... 158
8.3.2 Erhebung medizinischer Daten ... 159
8.3.3 Anforderung von weiteren Unterlagen ... 161
8.3.4 Erklärung über persönliche und sachliche Verhältnisse ... 163
8.3.5 Beantragung von Sozialleistungen über die Gemeinde ... 164
8.3.6 Einsatz von Sozialdetektiven, Recherche im Internet oder in Sozialen Netzwerken ... 164
8.3.7 Einsatz von E-Mail und Fax ... 167
8.3.8 Akteneinsichtsrecht und Auskunftsanspruch ... 168
8.3.8.1 Recht auf Akteneinsicht ... 168
8.3.8.2 Sozialrechtlicher Auskunftsanspruch ... 170
8.3.9 Outsourcing bei Sozialbehörden ... 171
8.3.10 Aufbewahrung von Sozialakten ... 174

8.4 Jugendhilfe ... 175
8.4.1 Anmeldung für Kindertageseinrichtungen ... 175
8.4.2 Erweitertes Führungszeugnis für Ehrenamtliche ... 176

9 Steuer- und Finanzverwaltung ... 177

9.1 Datenschutzbeauftragte an allen bayerischen Finanzämtern ... 177
9.1.1 Bisher: Gemeinsamer behördlicher Datenschutzbeauftragter der bayerischen Steuerverwaltung ... 177
9.1.2 Neu: Einrichtung von behördlichen Datenschutzbeauftragten an den Finanzbehörden vor Ort ... 179
9.1.3 Personalausstattung für Datenschutzaufgaben in der Steuerverwaltung ... 181
9.1.4 Fazit ... 182

9.2 Bekanntgabe von Steuerbescheiden an Steuerpflichtige mit Wohnsitz in der Schweiz ... 182
9.2.1 Sachverhalt ... 182
9.2.2 Rechtslage ... 183
9.2.3 Bewertung des Sachverhalts ... 185
9.2.4 Anpassung des Musterformulars ... 186

9.3 Steuerrechtliche Anforderungen an Restaurantrechnungen ... 186

9.4 ELSTER beim Betrieb von Photovoltaikanlagen durch Privatleute ... 189
9.4.1 Abgabe der Umsatzsteuererklärung ... 190
9.4.2 Abgabe der Einkommensteuererklärung ... 191

10 Schulen und Hochschulen ... 194

10.1 Umfassende Regelung der Schülerunterlagen ... 194
10.1.1 Übersicht über die neuen schuldatenschutzrechtlichen Regelungen ... 195
10.1.2 Regelungsgehalt des Art. 85 Abs. 1a BayEUG ... 196

10.1.3 Vorgaben zu Schülerunterlagen in der Bayerischen Schulordnung ... 196
10.1.4 Fazit ... 202

10.2 Digitales Lernen an bayerischen Schulen: „mebis – Landesmedienzentrum Bayern“ ... 202
10.2.1 Notwendigkeit einer Rechtsgrundlage für die mebis-Lernplattform ... 203
10.2.2 Anpassung der Anlage 10 „Passwortgeschützte Lernplattform“ DVBayDSG-KM ... 204
10.2.3 Zwischenbilanz und Ausblick ... 205

10.3 Videoaufnahmen im Schulunterricht ... 206
10.3.1 Reichweite der gesetzlichen Befugnis des Art. 85 Abs. 1 BayEUG ... 206
10.3.2 Datenschutzgerechte Einwilligung ... 209
10.3.3 Praxisrelevante Einzelfälle ... 210

10.4 „Sponsoring“ von Klassenfotos ... 211
10.4.1 Sachverhalt ... 212
10.4.2 Datenschutzrechtliche Bewertung ... 212
10.4.3 Ergebnis ... 213

10.5 Videoüberwachung des Kollegstufencafés ... 213
10.5.1 Sachverhalt ... 214
10.5.2 Rechtslage ... 214
10.5.3 Rechtsdurchsetzung ... 216
10.5.4 Fazit ... 217

10.6 Datenschutz bei der Bayerischen Landesstelle für den Schulsport ... 217
10.6.1 Ausgangssituation ... 217
10.6.2 Mängelbehebung ... 218
10.6.3 Ausblick ... 219

10.7 Staatliche Schulaufsicht über private Grundschulen und Mittelschulen ... 220
10.7.1 Gesetzliche Zuständigkeit allein bei Regierungen ... 220
10.7.2 Tatsächliche Aufgabenwahrnehmung durch Schulämter ... 221
10.7.3 Art und Umfang der Aufgabenerfüllung durch Schulämter – Erkenntnisse des Kultusministeriums ... 221
10.7.4 Rechtliche Bedenken gegenüber umfassender Aufgabenerledigung durch Schulämter ... 222
10.7.5 Schulämter als bloße Erbringer von „Hilfeleistungen“? ... 223
10.7.6 Bedenken gegenüber Heranziehung der Schulämter als „Hilfsorgane“ ... 224
10.7.7 Fazit ... 225

11 Personalwesen ... 226

11.1 Benutzung dienstlicher Telekommunikationsanlagen – Neufassung der TKBek ... 226
11.1.1 Dienstliche Telefongespräche ... 227
11.1.2 Private Telefongespräche ... 227

11.1.3 Datenschutzrelevante allgemeine Regelungen ... 228
11.2 Datenschutz bei elektronischen Schließanlagen ... 229
11.2.1 Erhebung und Verwendung von Beschäftigtendaten ... 229
11.2.2 Einwilligung im Abhängigkeitsverhältnis ... 230
11.2.3 Gesetzliche Anforderungen ... 230
11.2.4 Datenschutzrechtliche Freigabe ... 233
11.2.5 Mitbestimmung des Personalrats ... 233
11.2.6 Weiterführende Hinweise ... 234
11.3 Und nochmals: Datenschutz beim Betrieblichen Eingliederungsmanagement ... 234
11.4 Ausstattung von Dienstfahrzeugen mit Ortungssystemen ... 237
11.4.1 Erhebung personenbezogener Daten mittels Ortungssystemen ... 237
11.4.2 Einwilligung im Abhängigkeitsverhältnis ... 238
11.4.3 Datenschutzanforderungen an den Einsatz von Ortungssystemen ... 238
11.4.4 Datenschutzrechtliche Freigabe ... 240
11.4.5 Mitbestimmung des Personalrats ... 240
11.4.6 Weiterführende Hinweise ... 241
11.5 Einstellung von Bedienstetenfotos ins behördeneigene Intranet ... 242
11.6 Entgegennahme von Dienst- und Arbeitsunfähigkeitsbescheinigungen ... 243
11.7 Zeitliche Grenzen der Aufbewahrung von Arzneimittelverordnungen bei den Beihilfestellen ... 246
11.7.1 Verfahren der Arzneimittelrabattierung ... 246
11.7.2 Problematik der Aufbewahrung von Arzneimittelverordnungen ... 247
11.7.3 Keine ausdrückliche Festlegung einer Überprüfungshöchstfrist ... 248
11.7.4 Aber: Zeitliche Grenzen der Überprüfung und der Aufbewahrung ... 249
11.8 Einsicht in Personalakten durch Gemeinderats-„Referent“ ... 251
11.9 Dienstliche Beurteilung von behördlichen Datenschutzbeauftragten ... 255
11.10 Zugriff des Personalrats auf elektronische Zeiterfassungsdaten ... 257
11.10.1 Informationsanspruch des Personalrats allgemein ... 258
11.10.2 Informationsanspruch des Personalrats hinsichtlich elektronischer Zeiterfassungsdaten ... 259
12 E-Government, Telemedienrecht, Soziale Medien ... 262
12.1 E-Government-Regelungen ... 262
12.2 Plattformen und Verfahren ... 265
12.3 Verfolgung des Nutzerverhaltens im Internet ... 267
12.4 Soziale Medien, insbesondere Soziale Netzwerke ... 268

13 Spezielle datenschutzrechtliche Themen 270

13.1 Recht auf Auskunft 270

13.2 Safe Harbor – EU-US Privacy Shield 275

13.3 Cloud Computing 278

13.4 Datenübermittlungen durch die Industrie- und Handelskammern 279

13.4.1 Datenübermittlung an andere Industrie- und Handelskammern 279

13.4.2 Datenübermittlung an nichtöffentliche Stellen 279

13.5 Erhebung von Kundendaten des Antragstellers in einem Genehmigungsverfahren nach § 10 Bundesimmissionsschutzgesetz 281

13.6 Übergabe von Ausweisdokumenten an Dritte zum Zwecke der Kfz-Zulassung 282

13.7 Speicherung von durch die Polizei übermittelten Daten durch die Fahrerlaubnisbehörde 283

14 Datenschutzkommission 285

15 Abbildungen 287

Anlage 1: Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19.03.2015 Datenschutz nach „Charlie Hebdo“ Rechtsstaat und Grundrechte beweisen sich gerade in Zeiten terroristischer Bedrohung! 288

Anlage 2: Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19.03.2015 Datenschutzgrundverordnung darf keine Mogelpackung werden! 288

Anlage 3: Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19.03.2015 IT-Sicherheitsgesetz nicht ohne Datenschutz! 290

Anlage 4: Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19.03.2015 Mindestlohngesetz und Datenschutz 291

Anlage 5: Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19.03.2015 Safe Harbor bietet keinen ausreichenden Schutz für den Datentransfer in die USA 292

Anlage 6: Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19.03.2015 Verschlüsselung ohne Einschränkungen ermöglichen 292

Anlage 7: Entschließung der 90. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 30.09./01.10.2015 Cloud-unterstützte Betriebssysteme bergen Datenschutzrisiken 294

Anlage 8: Entschließung der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 06./07.04.2016
Wahrung der Freiheits- und Persönlichkeitsrechte bei der Bekämpfung des internationalen Terrorismus 295

Anlage 9: Entschließung Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 25.05.2016
EU-Datenschutz-Grundverordnung erfordert zusätzliche Ressourcen für Datenschutzbehörden! 296

Anlage 10: Entschließung der 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 09.11.2016
„Videoüberwachungsverbesserungsgesetz" zurückziehen! 297

Abkürzungsverzeichnis 299

Stichwortverzeichnis 304

1 Überblick

1.1 Europa

1.1.1 In Vielfalt geeint? Zur erfolgten Teilreform des EU-Datenschutzrechts

Der Philosoph Gottfried Wilhelm Leibniz soll seine Lehre von einer Universalharmonie mit dem Satz „Unitas in multitudine“ – Einheit in der Vielheit – zusammengefasst haben. Danach wird die Welt durch das Zusammenwirken unendlich vieler Krafteinheiten (Monaden) zusammengehalten.

Im Jahr 2003 schlug der Europäische Konvent zur Zukunft Europas den Entwurf eines Vertrags über eine Verfassung für Europa vor. In der Präambel heißt es:

„In der Gewissheit, dass Europa, „in Vielfalt geeint“, ihnen die besten Möglichkeiten bietet, unter Wahrung der Rechte des Einzelnen und im Bewusstsein ihrer Verantwortung gegenüber den künftigen Generationen und der Erde dieses große Abenteuer fortzusetzen, das einen Raum eröffnet, in dem sich die Hoffnung der Menschen entfalten kann“.

Der Leitspruch „In Vielfalt geeint“ ist heute noch ein offizielles Symbol der Europäischen Union. Gemäß der offiziellen Webseite der Europäischen Union (www.europa.eu) soll er zum Ausdruck bringen, dass sich die Mitgliedstaaten in der Europäischen Union zusammengeschlossen haben, um sich gemeinsam für Frieden und Wohlstand einzusetzen, und dass die vielen verschiedenen Kulturen, Traditionen und Sprachen in Europa den gesamten Kontinent bereichern. Unverkennbar klingt dabei der Leibniz´sche Grundgedanke eines harmonischen Zusammenwirkens eigenständiger Bestandteile zum Wohle der Gesamtheit an.

Freilich klaffen Anspruch und Wirklichkeit oft weit auseinander. Das formelle Gesetzgebungsverfahren zur Teilreform des europäischen Datenschutzrechtsrahmens etwa hat trotz umfassender Vorbereitung über vier Jahre in Anspruch genommen (siehe zuletzt meinen 26. Tätigkeitsbericht 2014 unter Nr. 1.2). Nach diesem mehrjährigen Ringen haben die drei Gesetzgebungsorgane der Europäischen Union – Kommission, Parlament und Rat – nun endlich die ersten beiden Schritte einer grundlegenden Reform des Datenschutz-Rechtsrahmens erfolgreich vollzogen. Am 27. April 2016 haben das Europäische Parlament und der Rat eine Datenschutz-Grundverordnung und eine Richtlinie über den Datenschutz der Strafjustiz erlassen, die nun im Amtsblatt der Europäischen Union vom 4. Mai 2016 (L 119) veröffentlicht sind.

1.1.1.1 Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung (DSGVO, „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG – Datenschutz-Grundverordnung“) soll die bisher geltende allgemeine Datenschutzrichtlinie 95/46/EG ersetzen.

Nach Art. 288 Vertrag über die Arbeitsweise der Europäischen Union (AEUV) haben Verordnungen grundsätzlich allgemeine und verbindliche Geltung. Sie gelten in den Mitgliedstaaten unmittelbar. Als „Grundverordnung“ sieht die Datenschutz-Grundverordnung allerdings zahlreiche Klauseln vor, die den mitgliedstaatlichen Gesetzgebern gewisse Gestaltungsmöglichkeiten eröffnen und auch einige Regelungsaufträge erteilen. Insbesondere haben nach Art. 6 Abs. 3 Satz 1, Abs. 1 Buchst. e) DSGVO die Union oder die Mitgliedstaaten die Rechtsgrundlagen für Verarbeitungen zu regeln, die zur Wahrnehmung von Aufgaben erforderlich sind, die im öffentlichen Interesse liegen oder zur Ausübung öffentlicher Gewalt erfolgen. Entsprechendes gilt für die Verarbeitung zur Erfüllung von rechtlichen Verpflichtungen, Art. 6 Abs. 3 Satz 1, Abs. 1 Buchst. c) DSGVO.

Art. 6 DSGVO Rechtmäßigkeit der Verarbeitung
(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

. . .

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

. . .

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

. . .

(3) Die Rechtsgrundlage für die Verarbeitungen nach Absatz 1 Buchstaben c und e wird festgelegt durch
a) Unionsrecht oder
b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.

Ähnlich wie die allgemeine Datenschutzrichtlinie 95/46/EG soll die Datenschutz-Grundverordnung die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Datenverarbeitung und der Gewährleistung des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten har-

monisieren (Erwägungsgrund 3 DSGVO). Entsprechend der gefestigten Rechtsprechung des Europäischen Gerichtshofs (EuGH) soll diese Harmonisierung der mitgliedstaatlichen Rechtsvorschriften nicht auf eine Mindestharmonisierung beschränkt sein, sondern – auf hohem Datenschutzniveau – zu einer grundsätzlich umfassenden Harmonisierung führen. Mit anderen Worten beschreibt die Datenschutz-Grundverordnung sowohl das Mindestschutzniveau als auch die Schutzobergrenze des Datenschutzes (vgl. etwa EuGH, Urteil vom 24. November 2011 – Rechtssache C-468, 469/10 – ASNEF, Abs. 28-30, Urteil vom 6. November 2003 – Rechtssache C-101/01 – Lindquist, Abs. 95, 96).

Die Datenschutz-Grundverordnung wird ab 25. Mai 2018 in den EU-Mitgliedstaaten und damit auch im Freistaat Bayern unmittelbar und allgemein gelten. Bis zu diesem Zeitpunkt müssen die mitgliedstaatlichen Gesetzgeber – also auch der Bund und der Freistaat Bayern – ihre jeweilige Rechtsordnung an die Vorgaben der Datenschutz-Grundverordnung anpassen. Angesichts der zahlreichen Öffnungsklauseln in der Datenschutz-Grundverordnung ist der zur Verfügung stehende Zeitraum knapp bemessen. Zur Unterstützung des bayerischen Gesetzgebers habe ich deshalb Empfehlungen zur Anpassung der allgemeinen Datenschutzvorschriften an die Datenschutz-Grundverordnung erarbeitet, die ich der Bayerischen Staatsregierung und der Datenschutzkommission beim Bayerischen Landtag zugeleitet habe. Diese Empfehlungen sind auf meiner Webseite https://www.datenschutz-bayern.de veröffentlicht.

Auch die 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 6./7. April 2016 hat sich mit der Verabschiedung der Datenschutz-Grundverordnung befasst. Sie hat an die deutschen Gesetzgeber appelliert, die durch die Öffnungsklauseln bestehenden Gestaltungsspielräume im Sinne eines effektiven Grundrechtsschutzes zu nutzen.

Entschließung der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 06./07.04.2016

Stärkung des Datenschutzes in Europa – nationale Spielräume nutzen

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

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

Nach der Einschätzung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder ist es allerdings zur Erhaltung und Verstärkung des bestehenden Datenschutzniveaus auch im Lichte der jüngeren Entscheidungen des Europäischen Gerichtshofs geboten, die in der Grundverordnung enthaltenen Öffnungs- und Konkretisierungsklauseln zu Gunsten des Rechts auf informatio-

nelle Selbstbestimmung zu nutzen. Auch die von der Grundverordnung getroffenen Weiterentwicklungen des Datenschutzes wie beispielsweise die Grundsätze des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sowie das Erfordernis von Datenschutz-Folgeabschätzungen müssen wirksam ausgestaltet werden. Die Konferenz fordert deshalb Bundes- und Landesgesetzgeber auf, in allen gesetzgeberischen Bereichen die nationalen Spielräume im Sinne des Grundrechts auf informationelle Selbstbestimmung zu nutzen.

Insbesondere folgenden Regelungen kommt in diesem Zusammenhang hohe Bedeutung zu:

- *Schaffung eines Beschäftigtendatenschutzgesetzes, mindestens jedoch Beibehaltung der §§ 3 Abs. 11, 32 BDSG (Art. 88 i.V.m. Erwägungsgrund [EG] 155),*
- *Beschränkungen für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten (Art. 9 Abs. 4 i.V.m. EG 53, letzte beide Sätze),*
- *Stärkung der Befugnisse der Aufsichtsbehörden, insbesondere Schaffung von Klagebefugnissen und effektiven Sanktionen auch gegenüber Behörden (Art. 58 und 83 Abs. 7 i.V.m. EG 150, vorletzter Satz),*
- *jedenfalls im öffentlichen Bereich durch die Nennung der Schutzziele Datensparsamkeit, Vertraulichkeit, Integrität, Verfügbarkeit, Nichtverkettbarkeit, Transparenz und Intervenierbarkeit, um einen einfachen, flexiblen und praxistauglichen technischen und organisatorischen Datenschutz zu konkretisieren (Art. 6 Abs. 2, 25, 32),*
- *Begrenzung der Zweckänderung bei Videoüberwachung öffentlich zugänglicher Räume durch Private, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist (Art. 6 Abs. 4),*
- *Beibehaltung der Verpflichtung in § 4f Abs. 1 BDSG einen betrieblichen Datenschutzbeauftragten zu bestellen (Art. 37 Abs. 4).*

1.1.1.2 Richtlinie für den Datenschutz der Strafjustiz

Bislang regelt das Recht der Europäischen Union die Verarbeitung personenbezogener Daten zu strafjustiziellen Zwecken nicht umfassend. Neben vielen Einzelrechtsakten zur Errichtung und zu Kompetenzen spezieller Institutionen (wie etwa Europol und Eurojust) und zu Verfahren (wie Schengen-Kodex oder Visa-Kodex) regelt bislang der Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 lediglich den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden. Er betrifft damit die grenzüberschreitende kriminalpolizeiliche und strafjustizielle Verarbeitung personenbezogener Daten.

Demgegenüber betrifft die Richtlinie für den Datenschutz der Strafjustiz (RLDSJ, „Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates“) auch die rein innerstaatliche strafjustizielle Datenverarbeitung.

Auch diese Richtlinie dient der Harmonisierung der strafjustiziellen Verarbeitung. So sollen die Mitgliedstaaten sicherstellen, dass der legale Austausch personenbezogener Daten zwischen den zuständigen Strafverfolgungsbehörden in der Union nicht aus Datenschutzgründen eingeschränkt oder verboten wird. Die Vorgabe soll sicherstellen, dass die Anfrage einer zuständigen Behörde nicht nur deshalb nicht beantwortet wird, weil sie nicht von einer inländischen zuständigen Behörde gestellt worden ist.

Allerdings verlangt die Richtlinie für den Datenschutz der Strafjustiz – anders wie die Datenschutz-Grundverordnung – lediglich die Herstellung eines Mindestdatenschutzniveaus.

Art. 1 RLDSJ Gegenstand und Ziele
(3) Diese Richtlinie hindert die Mitgliedstaaten nicht daran, zum Schutz der Rechte und Freiheiten der betroffenen Person bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden Garantien festzulegen, die strenger sind als die Garantien dieser Richtlinie.

Die Mitgliedstaaten haben bis zum 6. Mai 2018 die Rechts- und Verwaltungsvorschriften zu veröffentlichen, die zur Umsetzung der Richtlinie erforderlich sind. Auch hierzu beabsichtige ich, unter Berücksichtigung etwaiger Stellungnahmen der Datenschutzkonferenz Empfehlungen zu erarbeiten, die ich den zuständigen Staatsministerien zuleiten werde.

1.1.1.3 Wesentliche Neuerungen

Wer die Vorschriften über die Grundsätze in der Datenschutz-Grundverordnung mit den Vorgängervorschriften vergleicht, stellt fest: Der Gesetzgeber der Europäischen Union hat im Wesentlichen lediglich bereits bekannte und anerkannte Grundsätze weiterentwickelt und ergänzt. In Art. 6 der Richtlinie 95/46/EG gibt es bereits die Grundsätze der Rechtmäßigkeit, der Verarbeitung nach Treu und Glauben, der Zweckbindung, der Datenminimierung, der Richtigkeit und der Speicherbegrenzung. Die nun hinzugetretenen Prinzipien der Transparenz, der Integrität und Vertraulichkeit sowie der Rechenschaftspflicht des Verantwortlichen sind in Art. 5 der Richtlinie 95/46/EG zwar noch nicht ausdrücklich benannt, gleichwohl in anderen Vorschriften der Richtlinie bereits angelegt. Immerhin wertet der Verordnungsgeber sie durch die Aufnahme in die Liste der Verarbeitungsgrundsätze deutlich auf. Neuerungen bei den Grundsätzen sind also überschaubar. Nennenswert sind beispielsweise der gesteigerte Schutz von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung sowie Daten der sexuellen Orientierung einer natürlichen Person. Besonders begrüße ich, dass die Datenschutz-Grundverordnung – mehr als bisherige Datenschutzrechtsakte – den Schutz von Minderjährigen im Blick hat.

Wesentliche Änderungen betreffen also weniger Verarbeitungsgrundsätze, als vielmehr die Betroffenenrechte, Vorgaben an Technik und Verfahren sowie die Datenschutzaufsicht.

Die Betroffenenrechte werden durch das Recht auf Vergessenwerden und das Recht auf Datenübertragbarkeit ausgebaut.

Das Recht auf Vergessenwerden betrifft insbesondere Fälle, in denen die für die Verarbeitung Verantwortlichen personenbezogene Daten veröffentlicht haben.

Machen betroffene Personen Löschansprüche geltend, müssen solche Verantwortlichen im zumutbaren Umfang dafür sorgen, dass auch die Datenempfänger von dem jeweiligen Löschanspruch erfahren. Letztlich passt das Recht auf Vergessenwerden also Löschansprüche von betroffenen Personen an die arbeitsteilige digitale Verarbeitungswelt an.

Das Recht auf Datenübertragbarkeit soll insbesondere Nutzerinnen und Nutzern von Sozialen Netzwerken die Datenhoheit über ihre Daten sichern. Verantwortliche Sozialer Netzwerke sollen verpflichtet werden, interoperable Datenformate einzusetzen. Wechselt eine Nutzerin oder ein Nutzer ein Soziales Netzwerk, soll sie oder er die eigenen Daten „mitnehmen" können. Auf diese Weise soll die Abhängigkeit einer betroffenen Person von einem ganz bestimmten Dienst vermindert werden.

Was den technisch-organisatorischen Datenschutz anbelangt, werden die bisherigen Regelungen jetzt unter anderem durch Vorschriften zum Datenschutz durch Technikgestaltung (Art. 25 DSGVO), durch Meldepflichten bei Datenschutzverletzungen (Art. 33 DSGVO) sowie zur Sicherheit der Verarbeitung (Art. 32 DSGVO) ausgebaut.

Einen besonderen Schwerpunkt legt die Datenschutz-Grundverordnung schließlich auf den Ausbau der Kompetenzen der unabhängigen Datenschutzaufsichtsbehörden. Durch diesen Ausbau von Befugnissen werde ich als Landesbeauftragter für den Datenschutz zu einer Datenschutzaufsichtsbehörde mit entsprechenden Weisungs- und Verbotsbefugnissen umgestaltet. Zugleich werden die Datenschutzaufsichtsbehörden zur engen Kooperation mit den Aufsichtsbehörden anderer Mitgliedstaaten verpflichtet, die vor Allem im Rahmen eines Europäischen Datenschutzausschusses erfolgen soll.

1.1.1.4 Anpassung der allgemeinen Datenschutzgesetze des Bundes und des Freistaats Bayern an das neue europäische Datenschutzrecht

Die nachhaltige Umgestaltung der deutschen Datenschutzkontrolle wirft gewichtige Fragen auf. Wenn zentrale Datenschutzfragen künftig auf europäischer Ebene vom Europäischen Datenschutzausschuss beantworten werden sollen – wie entwickeln die deutschen Datenschutzbehörden eine einheitliche Verhandlungsposition? Wer vertritt die Datenschutzbehörden im Ausschuss und welchen innerstaatlichen Vorgaben unterliegt diese Vertretung? Unter anderem solche Fragen soll ein „Allgemeines Bundesdatenschutzgesetz" beantworten, das das bisherige Bundesdatenschutzgesetz ablösen soll.

Zur Änderung des Bayerischen Datenschutzgesetzes hat das im Freistaat Bayern federführende Staatsministerium des Innern, für Bau und Verkehr angekündigt, einen ersten Regelungsentwurf im Frühjahr 2017 vorzulegen. Angesichts der bisher sehr konstruktiven Zusammenarbeit während des EU-Datenschutzreformprozesses gehe ich davon aus, dass meine Empfehlungen zur Anpassung des allgemeinen Datenschutzrechts an die Datenschutz-Grundverordnung (siehe Nr. 1.1.1.1) bei der Ausgestaltung des künftigen Bayerischen Datenschutzgesetzes angemessen berücksichtigt werden. Beide Gesetzesvorhaben werde ich kritisch und aufmerksam begleiten.

1.1.2 Geplante weitere EU-Reformen: Datenschutzverordnung 2001/45/EG und E-Privacy-Richtlinie

Mit dem Inkrafttreten der Datenschutz-Grundverordnung und der Richtlinie für den Datenschutz der Strafjustiz ist der europäische Datenschutzreformprozess noch nicht abgeschlossen. Der Datenschutz von EU-Institutionen etwa wird durch eine Datenschutzverordnung aus dem Jahr 2001 geregelt. Diese Verordnung soll mittelfristig an die Vorgaben der Datenschutz-Grundverordnung angepasst werden.

Erwägungsgrund 17 DSGVO
Die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates gilt für die Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union. Die Verordnung (EG) Nr. 45/2001 und sonstige Rechtsakte der Union, die diese Verarbeitung personenbezogener Daten regeln, sollten an die Grundsätze und Vorschriften der vorliegenden Verordnung angepasst und im Lichte der vorliegenden Verordnung angewandt werden. Um einen soliden und kohärenten Rechtsrahmen im Bereich des Datenschutzes in der Union zu gewährleisten, sollten die erforderlichen Anpassungen der Verordnung (EG) Nr. 45/2001 im Anschluss an den Erlass der vorliegenden Verordnung vorgenommen werden, damit sie gleichzeitig mit der vorliegenden Verordnung angewandt werden können.

Bevor diese Anpassung der Datenschutzverordnung 2001/45/EG an die Datenschutz-Grundverordnung erfolgt, soll jedoch zunächst die sogenannte E-Privacy-Richtlinie überarbeitet werden. Aus meiner Sicht ist diese geplante Reform für Bayern wesentlich bedeutsamer als die Novellierung der Datenschutzverordnung 2001/45/EG, weil sie konkret die Verarbeitungspflichten von bayerischen Stellen bei der elektronischen Kommunikation betrifft.

Um die Reform der E-Privacy-Richtlinie 2002/58/EG vorzubereiten, leitete die Europäische Kommission ein öffentliches Anhörungsverfahren ein. Diese Konsultation diente dazu, die Richtlinie an die Datenschutz-Grundverordnung anzugleichen und zu überprüfen, inwiefern sie im Bereich der elektronischen Kommunikation ein hohes Schutzniveau zugunsten der Einzelnen sowie gleiche Wettbewerbsbedingungen der Marktteilnehmer gewährleistet (Mitteilung der Kommission vom 11. April 2016: „Public Consultation on the Evaluation and Review of the ePrivacy Directive“, veröffentlicht unter https://ec.europa.eu/digital-single-market/; vergleiche auch Nr. 12.3).

1.1.3 Safe Harbor-Abkommen ungültig – EU-US Privacy Shield in Kraft

Die Europäische Datenschutzrichtlinie (RL 95/46/EG) sieht vor, dass die Übermittlung personenbezogener Daten in Länder außerhalb der Europäischen Union grundsätzlich nur zulässig ist, wenn diese so genannten Drittstaaten ein angemessenes Datenschutzniveau gewährleisten. Bei der Beantwortung der Frage, ob ein Drittstaat ein angemessenes Datenschutzniveau gewährleistet, sind alle Umstände zu beurteilen, die bei einer Übermittlung oder bei einer Kategorie von Übermittlungen eine Rolle spielen, Art. 25 Abs. 2 RL 95/46/EG. Die Kommission kann feststellen, dass ein Drittstaat aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen allgemein ein angemessenes Datenschutzniveau gewährleistet (Art. 25 Abs. 6 RL 95/46/EG).

Art. 25 RL 95/46/EG
(1) Die Mitgliedstaaten sehen vor, daß die Übermittlung personenbezogener Daten, die Gegenstand einer Verarbeitung sind oder nach der Übermittlung verarbeitet werden sollen, in ein Drittland vorbehaltlich der Beachtung der aufgrund der anderen Bestimmungen dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zulässig ist, wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet.
(2) Die Angemessenheit des Schutzniveaus, das ein Drittland bietet, wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen; Nr. L 281/46 [DE Amtsblatt der Europäischen Gemeinschaften 23 . 11 . 95 insbesondere werden die Art der Daten, die Zweckbestimmung sowie die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen sowie die dort geltenden Standesregeln und Sicherheitsmaßnahmen berücksichtigt.
(3) Die Mitgliedstaaten und die Kommission unterrichten einander über die Fälle, in denen ihres Erachtens ein Drittland kein angemessenes Schutzniveau im Sinne des Absatzes 2 gewährleistet.
(4) Stellt die Kommission nach dem Verfahren des Artikels 31 Absatz 2 fest, dass ein Drittland kein angemessenes Schutzniveau im Sinne des Absatzes 2 des vorliegenden Artikels aufweist, so treffen die Mitgliedstaaten die erforderlichen Maßnahmen, damit keine gleichartige Datenübermittlung in das Drittland erfolgt.
(6) Die Kommission kann nach dem Verfahren des Artikels 31 Absatz 2 feststellen, dass ein Drittland aufgrund seiner innerstaatlichen Rechtsvorschriften oder internationaler Verpflichtungen, die es insbesondere infolge der Verhandlungen gemäß Absatz 5 eingegangen ist, hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau im Sinne des Absatzes 2 gewährleistet.

Mit ihrer Entscheidung 2000/520/EG hatte die Europäische Kommission festgestellt, dass die Vereinigten Staaten für bestimmte Datenempfänger ein angemessenes Schutzniveau gewährleisten. Von der Entscheidung erfasst waren solche amerikanische Unternehmen, die sich den sogenannten Safe Harbor-Datenschutzgrundsätzen unterworfen hatten.

Die Entscheidung der Europäischen Kommission zum sogenannten Safe Harbor-Abkommen erklärte der Europäische Gerichtshof für ungültig (Urteil vom 6. Oktober 2015, Rechtssache C-362/14 – Schrems). Sinngemäß rügte der Europäische Gerichtshof insbesondere, die Kommission hätte feststellen müssen, dass die Vereinigten Staaten von Amerika aufgrund innerstaatlichen Rechtsvorschriften oder internationalen Verpflichtungen tatsächlich ein Schutzniveau der Grundrechte gewährleisteten, das dem in der Europäischen Union aufgrund der Richtlinie im Lichte der Grundrechtecharta garantierte Niveau der Sache nach gleichwertig sei. Das habe die Kommission nicht geleistet.

Ein solches gleichwertiges Schutzniveau liege in dem Drittstaat jedenfalls nicht vor, wenn er generell die Speicherung aller personenbezogenen Daten sämtlicher Personen gestatte, deren Daten aus der Union in die Vereinigten Staaten übermittelt werden, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels vorzunehmen und ohne objektive Kriterien vorzusehen, die es ermöglichen, den Zugang der Behörden zu den Daten und deren spätere Nutzung zu beschränken. Eine Regelung, die es den Behörden gestatte, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, verletze den Wesens-

gehalt des Grundrechts auf Achtung des Privatlebens (Absatz 93 der Urteilsbegründung). Darüber hinaus verletze eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des Grundrechts auf wirksamen gerichtlichen Rechtsschutz (Absatz 95 der Urteilsbegründung).

In Bezug auf die Kompetenz der Datenschutzbehörden stellte der Gerichtshof fest, dass die Entscheidung der Kommission vom 26. Juli 2000 den nationalen Datenschutzbehörden Befugnisse entziehe, die ihnen für den Fall zustehen, dass eine Person die Vereinbarkeit der Entscheidung mit dem Schutz der Privatsphäre sowie der Freiheiten und Grundrechte von Personen in Frage stellt. Die Kommission habe keine Kompetenz gehabt, die Befugnisse der nationalen Datenschutzbehörden in dieser Weise zu beschränken (Absätze 102-104 der Urteilsbegründung).

Schließlich wies der Europäische Gerichtshof sinngemäß darauf hin, dass Art. 8 Abs. 3 der Charta der Grundrechte eine effektive Datenschutzaufsicht verlange. Halte die Kontrollstelle die Beschwerde einer betroffenen Person für begründet, müsse sie daher ein Klagerecht gegen einen Angemessenheitsbeschluss der Kommission haben. Insoweit sei es Sache des nationalen Gesetzgebers, Rechtsbehelfe vorzusehen, die es der betreffenden nationalen Kontrollstelle ermöglichten, die von ihr für begründet erachteten Rügen vor den nationalen Gerichten geltend zu machen, um gegebenenfalls ein Vorabentscheidungsverfahren zu erlangen (Absatz 66 der Urteilsbegründung).

Nach dem Urteil des Europäischen Gerichtshofs war die Übermittlung personenbezogener Daten aufgrund des Safe Harbor-Abkommens nicht mehr zulässig. In einer Pressemitteilung vom 7. Oktober 2015 wies ich die bayerischen öffentlichen Stellen deshalb darauf hin, dass sie die Zulässigkeit von Datenübermittlungen an Stellen mit Sitz in den USA nun besonders überprüfen müssten. Im besonderen Maße erheblich war die Entscheidung des Europäischen Gerichtshofs für Hochschulen, die auf vertraglicher Basis Public Cloud-Dienste mit US-amerikanischen Anbietern abgeschlossen hatten.

In der Zwischenzeit haben die Europäische Union und die Vereinigten Staaten von Amerika ein neues Abkommen zum Datenschutz abgeschlossen. Jetzt folgt ein „EU-US Privacy Shield“ dem für ungültig erklärten Safe Harbor-Abkommen nach (siehe Nr. 13.2).

1.1.4 Verantwortlichkeit der Anbieter von Facebook-Fanseiten

Mehrfach habe ich mich bereits mit der Frage auseinandergesetzt, ob und inwieweit Behörden zum Zweck der Öffentlichkeitsarbeit bei Facebook eine Fanseite einrichten und betreiben können. Zuletzt habe ich in meinem 26. Tätigkeitsbericht 2014 unter Nr. 12.4.1 über die einschlägige uneinheitliche Rechtsprechung berichtet.

Eines der Kernprobleme lautet, ob eine Behörde datenschutzrechtlich für Rechtsverstöße von Facebook mitverantwortlich ist, wenn sie eine Fanseite einrichtet und betreibt. Dies wurde vom Oberverwaltungsgericht Schleswig in einer Entscheidung vom 4. September 2014 noch verneint (Az.: 4 LB 20/13).

Im Rahmen des Revisionsverfahrens hat das Bundesverwaltungsgericht Fragen zu diesem Kernproblem dem Europäischen Gerichtshof vorgelegt (Beschluss vom 25. Februar 2016 – 1 C 28/14; siehe Nr. 12.4).

1.2 Deutschland

1.2.1 Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes

Die Aufdeckung des „Nationalsozialistischen Untergrundes" (NSU) Ende 2011 löste eine umfassende Diskussion zur Aufgabenwahrnehmung und Zusammenarbeit der Sicherheitsbehörden aus. Eine ganze Reihe von Untersuchungsausschüssen des Bundestags und mehrerer Landtage deckte Defizite bei der Zusammenarbeit der Sicherheitsbehörden, insbesondere Kooperationsdefizite bei einigen Verfassungsschutzbehörden auf. Als besonders problematisch hatten einige Untersuchungsausschüsse die Rolle von V-Leuten gesehen. V-Leute sind keine Beschäftigten der Verfassungsschutzämter. Sie sind Privatpersonen, die bereit sind, als Insider dem Verfassungsschutz Informationen über extremistische Kreise zu liefern.

Das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes vom 17. November 2015 soll die Schlussfolgerungen aus den Erkenntnissen der Untersuchungsausschüsse ziehen. Künftig soll das Bundesamt für Verfassungsschutz stärker als bisher die Zusammenarbeit der Verfassungsschutzämter koordinieren. Der Informationsfluss zwischen den Behörden soll verbessert und die Analysefähigkeit erhöht werden. Das Gesetz soll auch Rechtsklarheit zum Einsatz solcher V-Leute schaffen.

Aus Sicht der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist das neue Gesetz unter dem Gesichtspunkt des Grundrechtsschutzes verfassungsrechtlich problematisch.

Entschließung der 90. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 30.09./01.10.2015

Verfassungsschutzreform bedroht die Grundrechte

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

Das Gesetz sieht u. a. vor, Aufgaben und Informationen beim Bundesamt für Verfassungsschutz zu zentralisieren. Es erweitert die Verpflichtungen der Verfassungsschutzbehörden, Daten untereinander auszutauschen, erheblich. Zudem ermöglicht es den Austausch mit Polizeibehörden in einem Maß, welches der Rechtsprechung des Bundesverfassungsgerichtes zum informationellen Trennungsprinzip (Urteil vom 24. April 2013, 1 BvR 1215/07) widerspricht. Es schafft weiter die rechtliche Grundlage, das zentrale nachrichtendienstliche Informationssystem

(NADIS) von einem reinen Indexsystem zu einem vollumfänglichen Informationssystem auszubauen. Dies geschieht vor allem dadurch, dass nach dem Gesetzeswortlaut zu allen gespeicherten Personen und Objekten zukünftig auch die zugehörigen Dokumente, Bilder, Video- oder Audiomaterial in NADIS gespeichert werden können und sollen. Auf die erheblichen Risiken von Recherchen in solch umfassenden Dateien hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereits frühzeitig mit ihrer Entschließung vom 4. November 2010 „Keine Volltextsuche in Dateien der Sicherheitsbehörden" hingewiesen. Das Bundesamt für Verfassungsschutz erhält schließlich in Konkurrenz zu den Ländern operative Zuständigkeiten auch für nicht länderübergreifende gewaltorientierte Bestrebungen. Die Verfassungsschutzbehörden der Länder werden faktisch auf die Rolle von Datenlieferanten für das Bundesamt für Verfassungsschutz reduziert.

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

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

Die Konferenzentschließung habe ich unterstützt. Selbstverständlich habe ich keine Einwände gegen eine effektive Terrorismusbekämpfung, die dem Schutz der Bevölkerung dient. Die Verfassungsschutzbehörden nehmen insoweit als Frühwarnsystem des Rechtsstaats eine wichtige Rolle wahr. Jedoch darf eine Ausweitung der Kompetenzen nicht dazu führen, dass die Grundrechte unverhältnismäßig eingeschränkt werden. Trotz erheblicher Indizien für ein schwerwiegendes Fehlverhalten einiger Verfassungsschutzämter bei der NSU-Affäre wurden die Befugnisse des Verfassungsschutzes zwar erheblich ausgedehnt, die rechtsstaatliche Kontrolle hingegen nicht (siehe im Einzelnen Nr. 4.1).

1.2.2 E-Health-Gesetz, GKV-Versorgungsverstärkungsgesetz

Das „Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (E-Health-Gesetz)" vom 21. Dezember 2015 soll die Einführung einer digitalen Infrastruktur mit hohen Sicherheitsstandards und die Einführung nutzbringender Anwendungen auf der elektronischen Gesundheitskarte beschleunigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat das Gesetzgebungsverfahren mit einer Entschließung kritisch begleitet.

Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19.03.2015

Nachbesserungen beim eHealth-Gesetz und klare Regelungen zum Einsatz externer Dienstleister bei Berufsgeheimnisträgern erforderlich

Mit dem Entwurf eines Gesetzes für sichere und digitale Kommunikation und Anwendungen im Gesundheitswesen („eHealth-Gesetz“) würde die Bundesregierung die Gelegenheit verpassen, die zunehmende IT-Nutzung im Gesundheitswesen datenschutzgerecht auszugestalten und insbesondere die Anforderungen an die Vertraulichkeit und Transparenz der Datenverarbeitung zu regeln.

Aus diesem Grund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber insbesondere zu folgenden Ergänzungen des Gesetzentwurfs auf:

1. *Der Gesetzentwurf hat zum Ziel, die elektronische Gesundheitskarte einschließlich der Telematikinfrastruktur als zentrale Kommunikationsplattform im Gesundheitsbereich zu etablieren. So soll der Einsatz freiwilliger Anwendungen, in denen Patientendaten verarbeitet werden, forciert werden. Es muss allerdings bei dem Grundsatz bleiben, dass die Betroffenen über die Speicherung von Diagnosen und anderen medizinischen Daten auf der Gesundheitskarte selbst entscheiden können. Zur Wahrung der Transparenz ist das den Betroffenen eingeräumte Zugriffsrecht auf ihre Daten von besonderer Bedeutung. Ihnen wird damit auch die Wahrnehmung ihrer Rechte, insbesondere auf Auskunft und Löschung, ermöglicht. Entgegen der Gesetzeslage und entsprechender Ankündigungen ist eine Erprobung des Patientenzugriffs bislang unterblieben. Es ist daher sicherzustellen, dass die Versicherten ihre gesetzlich zugestandenen Rechte auch wahrnehmen können. Für den Fall, dass die notwendigen Funktionalitäten nicht zeitgerecht zur Verfügung stehen, sollte der Gesetzgeber angemessene Sanktionen festlegen.*
2. *Nach dem Gesetzentwurf richtet die Gesellschaft für Telematik zukünftig ein öffentlich über das Internet verfügbares Interoperabilitätsverzeichnis „für technische und semantische Standards, Profile und Leitfäden für informationstechnische Systeme im Gesundheitswesen“ ein. Sie wird dabei von Experten insbesondere aus dem IT-Bereich beraten. Zur Sicherung des hohen Schutzniveaus von Gesundheitsdaten sind auch Datenschutzexperten hinzuzuziehen.*
3. *Der Bundesgesetzgeber muss klare Rahmenbedingungen für die Einschaltung externer Dienstleister durch Berufsgeheimnisträger schaffen und den Vertraulichkeitsschutz bei den Dienstleistern sicherstellen. Die Einschaltung von externen Dienstleistern ist für Berufsgeheimnisträger oft ohne Alternative, wenn sie – wie auch vom Gesetzgeber beispielsweise mit dem eHealth-Gesetz gewünscht – moderne Informationstechnik nutzen wollen. Jedoch ist damit regelmäßig die Gefahr eines Verstoßes gegen die Schweigepflicht verbunden.*

Vor diesem Hintergrund muss der Gesetzgeber Rechtssicherheit schaffen, unter welchen Voraussetzungen Berufsgeheimnisträger externe Dienstleister einschalten dürfen. Die notwendige rechtliche Regelung muss (z.B. in § 203 StGB) gewährleisten, dass die Kenntnisnahme von Berufsgeheimnissen auf das unbedingt

Erforderliche beschränkt wird, die Dienstleister einer Schweigepflicht unterworfen und die Patientendaten auch bei ihnen durch ein Beschlagnahmeverbot abgesichert werden. Zudem muss durch Weisungsrechte der Berufsgeheimnisträger deren Verantwortlichkeit für die Berufsgeheimnisse gewahrt bleiben. Über technische und organisatorische Maßnahmen und über das Herstellen von Transparenz ist das für sensible Daten erforderliche Schutzniveau herzustellen.

Entsprechendes gilt für das „Gesetz zur Stärkung der Versorgung in der gesetzlichen Krankenversicherung (GKV-Versorgungsstärkungsgesetz)". Die Konferenz hat insoweit kritisiert, dass das bisherige datenschutzrechtlich problematische Vorgehen einiger Krankenkassen beim so genannten Krankengeldfallmanagement nunmehr legitimiert werden soll (Einzelheiten zu diesem Gesetz unter Nr. 8.1.1).

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. Dezember 2014

Schluss mit den datenschutzrechtlichen Missständen beim Umgang mit Krankengeldbeziehern!

Bei dem derzeit praktizierten „Krankengeldfallmanagement" lädt eine Vielzahl von Krankenkassen ihre Versicherten in der vierten Woche einer Arbeitsunfähigkeit zu einem persönlichen Gespräch ein. Die Krankenkassen stellen Fragen zur Arbeitsplatz-, Krankheits-, familiären und sozialen Situation des Versicherten. Außerdem sollen die Ärzte der Versicherten häufig medizinische Fragen beantworten sowie Arzt-, Krankenhaus- oder Rehaentlassberichte an die Krankenkasse schicken. Vielfach werden Versicherte, die im Krankengeldbezug stehen, – zum Teil mehrfach wöchentlich – von Krankenkassenmitarbeitern oder in deren Auftrag von Dritten angerufen, um sich nach dem Fortschritt der Genesung zu erkundigen.

Zudem werden nach den Prüferfahrungen der Datenschutzbeauftragten des Bundes und einiger Länder Versicherte beim „Krankengeldfallmanagement" von ihrer Krankenkasse oftmals unter Druck gesetzt. Auch der Patientenbeauftragte der Bundesregierung sowie die Unabhängige Patientenberatung Deutschland (UPD) haben an dieser Praxis starke Kritik geübt.

Die Krankenkassen sind zur Beurteilung sensibler medizinischer Daten aufgrund der bisherigen gesetzgeberischen Grundentscheidung auf ein Tätigwerden des Medizinischen Dienstes der Krankenversicherung (MDK) angewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist die Bundesregierung darauf hin, dass es nicht nachvollziehbar ist, dass mit dem Entwurf eines Gesetzes zur Stärkung der Versorgung in der gesetzlichen Krankenversicherung (GKV Versorgungsstärkungsgesetz – GKV-VSG) das bisherige datenschutzrechtlich problematische Vorgehen von vielen Krankenkassen beim sog. Krankengeldfallmanagement nunmehr legitimiert werden soll. Zukünftig sollen danach die Versicherten bei einem (absehbaren) Krankengeldbezug „Anspruch auf eine umfassende Prüfung, individuelle Beratung und Hilfestellung, welche Leistungen und unterstützende Angebote zur Wiederherstellung der Arbeitsfähigkeit erforderlich sind" gegenüber ihrer gesetzlichen Krankenkasse haben. Die Krankenkasse soll dabei die erforderlichen personenbezogenen Daten mit Einwilligung des Versicherten erheben, verarbeiten und nutzen dürfen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, von dieser Regelung Abstand zu nehmen. Vielmehr sind die derzeit bestehenden gesetzlichen Regelungen konsequent umzusetzen.

1.3 Freistaat Bayern

1.3.1 Bayerisches E-Government-Gesetz

Am 30. Dezember 2015 ist das Gesetz über die elektronische Verwaltung in Bayern (Bayerisches E-Government-Gesetz – BayEGovG) in Kraft getreten. Vorbehaltlich vorrangig anzuwendender Spezialregelungen gilt das Gesetz für die öffentlich-rechtliche Verwaltungstätigkeit der öffentlichen Stellen Bayerns.

Unter anderem soll es den Ausbau von E-Government-Anwendungen unterstützen, digitale Zugangs- und Verfahrensrechte von Bürgerinnen und Bürgern begründen und das Datenschutzrecht modernisieren. In das Gesetzgebungsverfahren wurde ich umfassend eingebunden. Gleichwohl habe ich gewisse Zweifel, ob das Gesetz die zentralen datenschutzrechtlichen Fragen des E-Government klären wird (im Einzelnen siehe Nr. 12.1).

1.3.2 Insbesondere: Allgemeines Auskunftsrecht

Mit dem Bayerischen E-Government-Gesetz hat der bayerische Gesetzgeber ein allgemeines Recht der Bürgerinnen und Bürger gegenüber bayerischen Behörden auf Auskunft eingeführt. Der neu verabschiedete Art. 36 BayDSG regelt die näheren Voraussetzungen dieses Auskunftsanspruchs. Mit dieser Vorschrift hat der bayerische Gesetzgeber Rechtssicherheit über Umfang und Grenzen des schon aus dem Rechtsstaatsprinzip abzuleitenden allgemeinen Auskunftsrechts geschaffen.

Das neu geschaffene Informationsrecht ist von den Medien kaum aufgegriffen worden und bei vielen Bürgerinnen und Bürgern ebenso wie bei einigen Behörden nach meinem Eindruck noch unbekannt. Bei mir gehen zwar durchaus zahlreiche Beschwerden und Anfragen ein, die sich auf das Auskunftsverhalten von bayerischen Behörden beziehen. Sie beziehen sich jedoch nach wie vor zumeist auf ein „Informationsfreiheitsgesetz“, das es in Bayern in dieser Form nicht gibt.

Deshalb habe ich auf meiner Webseite https://www.datenschutz-bayern.de eine neue Rubrik zum Allgemeinen Auskunftsrecht eingerichtet. Dort sind Informationen rund um den allgemeinen Auskunftsanspruch bereit gestellt (Gesetzestext und weitere Einzelheiten siehe Nr. 13.1).

1.3.3 Änderung des Bayerischen Verfassungsschutzgesetzes

Der Gesetzgeber hat das Bayerische Verfassungsschutzgesetz in erheblichem Umfang geändert. Meine Empfehlungen wurden dabei nur teilweise berücksichtigt. Verfassungsrechtlich problematisch könnte vor allem die gesetzliche Ausgestaltung grundrechtssichernder Verfahrensvorschriften sein (siehe Nr. 4.1).

1.3.4 Regelung der Schülerunterlagen

Im Rahmen von Prüfungen vor Ort habe ich immer wieder feststellen müssen, dass Schulen sich gerade mit der Aufbewahrung von Schülerunterlagen schwer tun. Zunächst nehmen die in Papierform geführten Schülerunterlagen einen erheblichen Platz in Anspruch. Zudem haben die Untersicherheiten und Auslegungsfragen mit den wachsenden informations- und kommunikationstechnischen Möglichkeiten deutlich zugenommen. Deshalb habe ich mich bereits seit Jahren dafür eingesetzt, dass die offenen Fragen insbesondere im Hinblick auf Definition und Aufbewahrung der – datenschutzrechtlich sensiblen – Schülerunterlagen durch Rechtsvorschriften klar beantwortet werden. Im Berichtszeitraum hat der bayerische Gesetz- und Verordnungsgeber meine jahrzehntelangen drängenden Empfehlungen endlich umgesetzt (zu Einzelheiten siehe Nr. 10.1).

1.3.5 Behördliche Datenschutzbeauftragte an allen bayerischen Finanzämtern

Für einen effektiven Datenschutz ist es besonders wichtig, dass Vorschriften nicht nur auf dem Papier stehen, sondern in der Praxis auch beachtet werden. Organisatorischen und verfahrensrechtlichen Vorkehrungen kommt daher seit jeher im Datenschutzrecht eine besondere Bedeutung zu. Erfreulich ist aus diesem Grund die Entscheidung des Staatsministeriums der Finanzen, für Landesentwicklung und Heimat, neben weiteren datenschutzfreundlichen Maßnahmen auch an allen bayerischen Finanzämtern behördliche Datenschutzbeauftragte einzurichten (zu Einzelheiten siehe Nr. 9.1).

1.4 Öffentlichkeitsarbeit

Öffentlichkeitsarbeit hat eine zentrale Bedeutung für den Datenschutz. Informationen und datenschutzrechtliche Positionen sollen – über den unmittelbaren Kontakt mit der Politik, der Presse, den Behörden und den im Einzelfall Betroffenen hinaus – allgemein bekannt und verfügbar gemacht werden. Auch so kann ich die Verwaltung dabei unterstützen, datenschutzkonform zu handeln. Bürgerinnen und Bürgern helfe ich damit, ihre Rechte und Schutzmöglichkeiten zu (er)kennen und wahrzunehmen. Wegen der Neuordnung des Europäischen Datenschutz-Rechtsrahmens und der daraus folgenden Änderungen wird es in den kommenden Berichtszeiträumen einen erhöhten Informationsbedarf geben.

Ein wesentlicher Baustein ist der **Internetauftritt** meiner Dienststelle (https://www.datenschutz-bayern.de). Über neue sowie aktualisierte Inhalte des Internetauftritts kann sich jeder per RSS-Feed informieren lassen.

Darüber hinaus ist es mir wichtig, auch Bevölkerungsgruppen zu erreichen, die meine Webseite normalerweise nicht besuchen. Daher ist meine **Ausstellung „Vom Eid des Hippokrates bis zu Edward Snowden – eine kleine Reise durch 2500 Jahre Datenschutz“** (siehe 26. Tätigkeitsbericht 2014 unter Nr. 1.5) weiter von Ort zu Ort gewandert. Im Berichtszeitraum war die Ausstellung bei der Stadt Weiden, der Stadt Augsburg, der Universität Passau, der Stadt Landshut, dem Landratsamt Regensburg, der Stadt Ingolstadt, der Fachhochschule für öffentliche Verwaltung und Rechtspflege (Fachbereich Polizei) in Fürstenfeldbruck, der Stadt Rosenheim, der Hochschule für angewandte Wissenschaften Coburg, der Stadtbibliothek Straubing, der Hochschule für angewandte Wissenschaften München, dem Staatsministerium für Arbeit und Soziales, Familie und Integration, der

Friedrich-Alexander-Universität Erlangen-Nürnberg, der Stadt Nördlingen, der Stadt Landsberg am Lech, der Stadt Kempten und zuletzt bei der Volkshochschule Lindau zu Gast.

Aufgrund der guten Erfahrungen werde ich auch meinen **Informationsstand** weiter nutzen, um Bürgerinnen und Bürger vor Ort zu informieren, sie darüber hinaus zu beraten und mit ihnen zu diskutieren. Im Berichtszeitraum war der Stand am 11. Oktober 2015 beim Tag der offenen Tür der Stadt Nürnberg und am 26. November 2016 beim gemeinsamen Tag der offenen Tür des Landtags, der Staatsregierung und des Verfassungsgerichtshofs.

Außerdem haben Angehörige meiner Dienststelle und ich erneut an zahlreichen **Informations- und Diskussionsveranstaltungen** als Referentinnen beziehungsweise Referenten teilgenommen und Vorlesungen oder Gastvorträge gehalten.

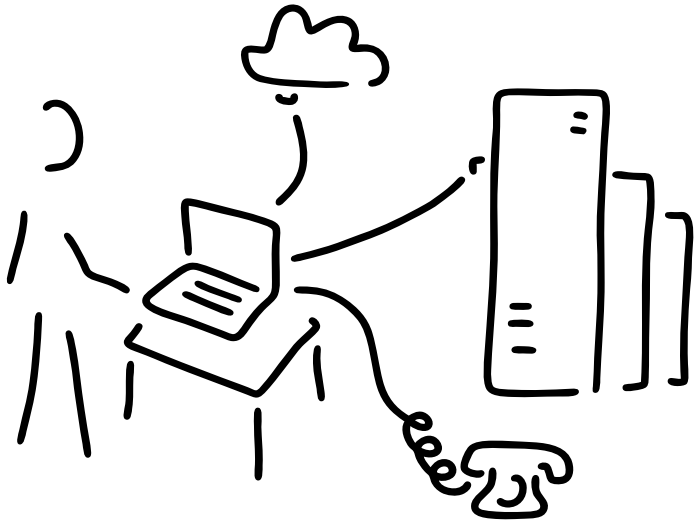
Meine **Broschüren und Informationsmaterialien** (siehe 26. Tätigkeitsbericht 2014 unter Nr. 1.5) werden weiter rege bei mir bestellt und von meiner Webseite heruntergeladen.

Pressearbeit ist besonders wichtig, um die Öffentlichkeit zu informieren und datenschutzrechtliche Positionen darzustellen. Auch in diesem Bereich verstärke ich meine Aktivitäten (siehe 26. Tätigkeitsbericht 2014 unter Nr. 1.5) stetig.

1.5 Schlussbemerkungen

Die nachfolgenden Kapitel geben unter anderem einen Überblick über meine Beteiligung an wesentlichen, hier nicht erwähnten Gesetzgebungsverfahren und meine Datenschutzkontrolle der bayerischen öffentlichen Stellen im Berichtszeitraum 2015/2016.

2 Informations- und Kommunikationstechnik und Organisation



2.1 Grundsatz- und Einzelthemen

2.1.1 Einsatz staatlich freigegebener Verfahren in den Kommunen – Gesetzesänderung

Nach Art. 26 BayDSG bedarf ein automatisiertes Verfahren, mit dem personenbezogene Daten verarbeitet werden, insbesondere vor dem erstmaligen Einsatz der schriftlichen Freigabe durch den behördlichen Datenschutzbeauftragten der das Verfahren einsetzenden öffentlichen Stelle.

Diese lokal vorzunehmende Freigabe ist nicht erforderlich bei Verfahren, welche durch das fachlich zuständige Staatsministerium oder die von ihm ermächtigte öffentliche Stelle für den landesweiten Einsatz datenschutzrechtlich freigegeben worden sind (Art. 26 Abs. 1 Satz 2 Halbsatz 2 BayDSG). Diese „Befreiung" von der Erforderlichkeit einer lokal vorzunehmenden datenschutzrechtlichen Freigabe galt bis zum 21. Dezember 2015 nur für staatliche Stellen. Kommunen hingegen, welche die gleichen Verfahren einsetzten, mussten diese Verfahren selbst prüfen und diese auch selbst datenschutzrechtlich freigeben. Kommunen konnten bis dahin nur solche Verfahren ohne eigene datenschutzrechtliche Freigabe einsetzen, wenn diese durch die Anstalt für Kommunale Datenverarbeitung in Bayern gemäß Art. 26 Abs. 1 Satz 2 Halbsatz BayDSG bereits freigegeben waren.

Mit der letzten Änderung des Bayerischen Datenschutzgesetzes am 22. Dezember 2015 ist es nunmehr auch den Kommunen möglich, derartige Verfahren einzusetzen, ohne sie erneut selbst freigeben zu müssen. Der Einsatz von bereits

staatlicherseits datenschutzrechtlich freigegebenen Verfahren ist durch diese neue Regelung für Kommunen deutlich vereinfacht worden.

Die Kommunen sind jedoch – wie auch bei den von der Anstalt für Kommunale Datenverarbeitung in Bayern freigegebenen Verfahren – gehalten, eine Kopie der datenschutzrechtlichen Freigabe des Verfahrens zum eigenen Verfahrensverzeichnis zu nehmen.

2.1.2 Schutz vor Ransomware

Seit September 2015 wird in den Medien verstärkt über Cyber-Angriffe mittels sogenannter Ransomware berichtet. Dabei handelt es sich um Schadprogramme, die den Zugang zu Computern und mobilen Geräten (etwa Tablets oder Smartphones) verhindern und/oder darauf gespeicherte Daten verschlüsseln. Benutzerinnen und Benutzer erhalten bei Zugriffsversuchen häufig lediglich eine Meldung, dass ihr Gerät gesperrt ist und die Daten verschlüsselt sind. Zusätzlich wird eingeblendet, auf welche Weise sie womit und wohin Lösegeld bezahlen müssen, um wieder auf ihre Daten zugreifen zu können.

Ransomware stellt eine neue Form der Trojanischen Pferde dar und setzt sich aus den englischen Wörtern Ransom (Lösegeld) und Software zusammen. Neben Privatpersonen und Unternehmen zählen auch Behörden, Kommunen und deren Einrichtungen zunehmend zu den auserwählten Opfern.

Um wieder Zugriff auf die von der Ransomware verschlüsselten Daten zu erhalten, werden die Geschädigten aufgefordert, eine E-Mail an eine bestimmte E-Mail-Adresse zu senden, eine Webseite aufzurufen oder eine Formularmaske auszufüllen. In allen Fällen wird eine Software zur Entschlüsselung oder die Zusendung des benötigten Passworts versprochen, falls zuvor eine Bezahlung (typischerweise in Bitcoins) erfolgt ist. Von einer Bezahlung rät aber das Bundesamt für Sicherheit in der Informationstechnik (BSI) ab, da auch nach Bezahlung des Lösegelds nicht sicher sei, ob die Daten tatsächlich wieder entschlüsselt würden. Zudem würde die Zahlungsbereitschaft der Opfer festgestellt, wodurch weitere Forderungen nicht auszuschließen seien. Bei einer Zahlung mittels Kreditkarte würden dem Kriminellen darüber hinaus weitere private Informationen zugänglich. Stattdessen rät das BSI, Anzeige zu erstatten.

Eingeschleust wird Ransomware oft durch verseuchte USB-Sticks oder infizierte E-Mail-Anhänge angeblicher Rechnungen, Bestellbestätigungen und dergleichen. Werden diese Anhänge geöffnet, startet im Hintergrund die Installation der Schadsoftware. Diese wird zumeist mit Hilfe eines Skriptes von einem Server aus dem Internet nachgeladen.

Häufig bestehen diese Anhänge aus Microsoft Office-Dokumenten, in denen Makros enthalten sind, bei deren Aufruf die Schadenssoftware installiert wird.

Eine weitere Gefahr besteht durch den Besuch kompromittierter Webseiten. Dabei wird durch das Ausnützen bekannter Sicherheitslücken (in Webbrowsern) automatisch und unbemerkt die schädliche Software auf dem Rechner der Anwenderin oder des Anwenders installiert (Drive-by-exploits).

Die folgenden Vorbeugemaßnahmen dienen nicht nur gegen Ransomware, sondern sind häufig auch dazu geeignet, einen Befall mit anderer Schadenssoftware zu vermeiden:

- Da auch der beste Virenscanner häufig eine Infektion mit Ransomware nicht verhindern kann, besteht die wichtigste Vorbeugemaßnahme in der Erstellung regelmäßiger Datenbackups auf externen, nicht dauerhaft angeschlossenen Datenträgern. Permanent angeschlossene Laufwerke oder Datenträger stellen ein Risiko dar, da Ransomware das gesamte Netzwerk einer öffentlichen Stelle – und damit auch angeschlossene Sicherungsdatenträger – befallen kann. Damit eine zentrale Datensicherung möglich ist, sind die Benutzerinnen und Benutzer anzuhalten, ihre Daten auf Netzlaufwerken abzuspeichern.

- Die eingesetzten Betriebssysteme (auch auf Tablets und Smartphones), Virenscanner, Webbrowser sowie Browser-Erweiterungen sollten immer durch das Einspielen aktueller Updates und Patches auf dem neuesten Stand gehalten werden.

- Hersteller von Antivirensoftware gehen mittlerweile dazu über, Spezialtools (auch für mobile Geräte) gegen Verschlüsselungsversuche zu entwickeln. Sobald das Tool entsprechende Versuche registriert, werden diese Vorgänge gestoppt und eine Warnmeldung erzeugt. Auch Entschlüsselungstools werden teilweise angeboten; diese sind aber selten auf dem neuesten Stand.

- Zur Vorbeugung gegen Drive-by-exploits-Angriffen sollten die Webbrowser mit Hilfe von Werbeblockern gegen die Ausführung unnötiger Scripts und anderen eingebundenen aktiven Inhalten geschützt werden.

- Da Ransomware häufig mittels Spam-Mails versendet wird, sollten diese E-Mails mit Hilfe eines Spamfilters entsprechend markiert werden. E-Mails mit ausführbaren Dateien im Anhang (beispielsweise .exe, .scr, .chm, .bat, .com, .msi, .jar, .cmd, .hta, .pif, .scf) sollten geblockt und nicht an die Empfängerin oder den Empfänger weitergeleitet werden.

- Grundsätzlich sollte die Makroausführung in Office-Programmen deaktiviert werden. Müssen Makros in Office-Dokumenten genutzt werden, sollten diese digital signiert sein und nur die Ausführung von Makros mit festgelegten digitalen Signaturen erlaubt werden.

- Selbstverständlich sollten alle Bediensteten einer öffentlichen Stelle hinsichtlich der Gefahr eines Ransomwarebefalls sensibilisiert und darauf hingewiesen werden, dass sie keinesfalls E-Mail-Anhänge öffnen dürfen, wenn sie nicht sicher sind, dass deren Inhalt unbedenklich ist.

Ich rate allen bayerischen öffentlichen Stellen dringend dazu, die angeführten Vorbeugemaßnahmen zu ergreifen, auch wenn sie natürlich keinen hundertprozentigen Schutz gegen einen Befall mit Ransomware gewährleisten können.

Weitere Informationen zu Ransomware können einem entsprechenden Themenpapier des BSI entnommen werden (abrufbar unter https://www.bsi.bund.de).

2.1.3 Versenden von E-Mails an mehrere Empfängerinnen und Empfänger

Bereits in meinem 20. Tätigkeitsbericht 2002 unter Nr. 9.10 und in meinem 22. Tätigkeitsbericht 2006 unter Nr. 8.1.3 habe ich Städte, Gemeinden und Landkreise darauf hingewiesen, dass beim Versand einer E-Mail an mehrere Empfängerinnen und/oder Empfänger darauf zu achten ist, dass nur berechtigte Personen die Adressen der anderen zur Kenntnis nehmen können. Gleichwohl erreichen mich dazu immer noch zahlreiche Eingaben.

Beim Versenden einer E-Mail gibt es – technisch gesehen – drei Möglichkeiten der Adressierung:

— Der oder die eigentlichen Empfängerinnen und Empfänger werden für alle sichtbar im „An"-Feld („To"-Feld) eingetragen.

— Eine Kopie der E-Mail kann an weitere Adressen ins „Cc"-Feld („Carbon Copy") versendet werden. Auch diese Adressen sind von allen einsehbar.

— Einen Sonderfall stellt das „Bcc"-Feld („Blind Carbon Copy", übersetzt etwa „Blindkopie") dar. Die dort eingetragenen Adressen sind für alle anderen Adressatinnen und Adressaten der E-Mail nicht sichtbar.

Wird eine E-Mail mittels „Cc" an mehrere Adressen der gleichen Behörde versendet, so wird die E-Mail grundsätzlich nur einmal an den E-Mail-Server der Behörde übertragen und dann in die Postfächer der einzelnen Empfängerinnen und Empfänger „kopiert". Wird „Bcc" verwendet, vervielfältigt der absendende E-Mail-Server die E-Mail und überträgt sie für jede Empfängeradresse eigens an den empfangenden Server. Selbst auf dem empfangenden Server ist es dann nicht mehr sofort erkennbar, dass diese (inhaltlich gleiche) E-Mail mehrfach eingegangen ist und wer genau diese erhalten hat.

Aus rechtlicher Sicht stellen die Weitergaben der E-Mail-Adressen im „An" -oder „Cc"-Modus an die einzelnen Empfängerinnen und Empfänger grundsätzlich Datenübermittlungen dar. Diese Datenübermittlungen lassen sich durch die Verwendung von „Bcc" (oder auch durch Einzel-E-Mails) vermeiden. Sie sind somit nicht erforderlich und daher regelmäßig unzulässig, zumindest wenn beim Empfängerkreis kein berechtigtes Interesse an der Kenntnis der anderen Adressen vorliegt.

Aber auch aus Sicht der IT-Sicherheit kann die Verwendung von „An" und/oder „Cc" negative Auswirkungen haben. Je größer der Adressatenkreis ist, umso größer wird die Wahrscheinlichkeit, dass wenigstens ein empfangendes IT-System mit Schadsoftware infiziert ist. Da sie sich – wie etwa Krypto-Trojaner – oft per E-Mails verbreitet, ist es für die Schadsoftware ein großer Vorteil, wenn sie „Kenntnis" von vielen aktuellen E-Mail-Adressen erhält. Anhand dieser E-Mail-Adressen kann die Schadsoftware dann versuchen, neue IT-Systeme zu infizieren. Außerdem können diese E-Mail-Adressen auch zum Spam-Versand weitergegeben werden.

Je umfangreicher also ein Empfängerkreis ist, desto höher ist die Wahrscheinlichkeit, dass dessen E-Mail-Adressen von Schadsoftware abgefangen und durch sie missbräuchlich verwendet werden. Damit einhergehend erhöht sich das Schadenspotential.

Sowohl aus datenschutzrechtlicher Sicht als auch aus Gründen der IT-Sicherheit ist daher bei jedem Versand einer E-Mail an mehrere Adressen zu prüfen, ob wirklich ein Versand mittels „An"- oder „Cc"-Adressierung nötig ist. Ansonsten empfehle ich dringend, bevorzugt „Bcc" zu verwenden oder die E-Mail an jeden einzelnen gesondert manuell zu adressieren.

2.1.4 Nutzung des E-Postbriefs

Im Berichtszeitraum erreichten mich mehrfach Anfragen von staatlichen und kommunalen Stellen, was sie bei der Nutzung des E-Postbriefes datenschutzrechtlich zu beachten haben.

Der E-Postbrief ist ein Dienst der Deutschen Post AG für den Austausch elektronischer Nachrichten über das Internet. Es handelt sich dabei regelmäßig um elektronische Datenübertragungen ohne Medienbruch. E-Postbriefe können aber auch alternativ in Papierform zugestellt werden – hierbei spricht man von einem Hybridbrief. Im Folgenden gehe ich näher auf die beiden Zustellmöglichkeiten ein.

Für die durchgängig elektronische Übertragung des E-Postbriefes ist Voraussetzung, dass sowohl Absenderinnen und Absender als auch Empfängerinnen und Empfänger zur E-Postbrief-Kundschaft der Deutschen Post AG zählen.

Aufgrund von Sicherheitsmaßnahmen (wie etwa einer Transportverschlüsselung) sowie weiterer Vorgaben an die Vertraulichkeit, Integrität und Authentizität der Kommunikation bietet der E-Postbrief ein höheres Sicherheits- und Datenschutzniveau als der herkömmliche E-Mail-Versand.

Eine verschlüsselte Datenübertragung findet standardmäßig nur zwischen der Absenderin oder dem Absender und der Betreiberin des Verfahrens (also der Deutschen Post AG) statt. Der E-Postbrief liegt bei der Betreiberin somit unverschlüsselt vor; dadurch kann dort ein unzulässiger Datenzugriff nicht (technisch) sicher ausgeschlossen werden. Die Weiterleitung des E-Postbriefs von der Betreiberin an die Empfängerin oder den Empfänger erfolgt sodann ebenfalls durch eine erneute Transportverschlüsselung geschützt.

Für den Versand von Daten mit besonders hohem Schutzbedarf (etwa Gesundheitsdaten) ist die Verwendung einer zusätzlichen Ende-zu-Ende-Verschlüsselung zur durchgängigen Sicherstellung der Vertraulichkeit notwendig. Nur dann bestehen aus datenschutzrechtlicher Sicht gegen dieses Verfahren keine Bedenken.

Der Versand eines E-Postbriefes als Hybridbrief wird gewählt, wenn zwar die Absenderin oder der Absender, nicht aber die Empfängerin oder der Empfänger zur E-Postbrief-Kundschaft der Deutschen Post AG zählt.

Beim Versand eines E-Postbriefes als Hybridbrief erfolgt zunächst wieder eine Verschlüsselung des Transportwegs zwischen der Absenderin oder dem Absender und der Betreiberin. Bei der Betreiberin wird das Dokument ausgedruckt, kuvertiert und frankiert und dann der Empfängerin oder dem Empfänger in Papierform konventionell zugestellt.

Ausdruck, Kuvertierung und Frankierung verlaufen nach Angabe der Deutschen Post AG automatisch. Ein menschliches Eingreifen sei lediglich bei Störungen erforderlich. Deren Umfang ist mir nicht bekannt. Zusätzlich werden die Ausdrucke und die Kuvertierungen durch die Deutsche Post AG stichprobenartig überprüft. Daher kann nicht gänzlich ausgeschlossen werden, dass die mit der Überprüfung beauftragten Personen diese Dokumente auch lesen und somit vom Inhalt Kenntnis nehmen können. Demzufolge müssen alle dafür eingesetzten Beschäftigten auf das Fernmelde- und Postgeheimnis verpflichtet werden.

Bei dem Versand eines Hybridbriefs mit sensiblem Inhalt sollte die absendende öffentliche Stelle zuvor die schriftliche Einwilligung der betroffenen Empfängerin oder des betroffenen Empfängers in diese Art des Versands einholen. Liegt diese Einwilligung nicht vor, sollte von einem Versand derartiger Schreiben mittels Hybridbriefs abgesehen werden.

Beim Versand eines Hybridbriefs liegt im Regelfall eine Auftragsdatenverarbeitung vor. Somit muss diese Dienstleistung in dem jeweiligen Umfeld zum einen rechtlich zulässig sein, was im Gesundheits- und Sozialbereich nicht ohne weiteres der Fall ist. Zum anderen muss ein entsprechender Vertrag abgeschlossen werden. Sofern die Deutsche Post AG sich zum Ausdrucken und Kuvertieren einer dritten Stelle bedient, handelt es sich um ein Unterauftragsverhältnis, das im Vertrag zur Auftragsdatenverarbeitung ebenfalls geregelt sein muss.

2.1.5 IT-Abschottung von Statistikstellen

Ich habe in meinem 25. Tätigkeitsbericht 2012 unter Nr. 2.2.6 Hinweise dazu gegeben, was bei dem gemäß Art. 21 Abs. 3 Satz 1 Bayerisches Statistikgesetz geforderten Abschottungsgebot kommunaler Statistikstellen vom übrigen Verwaltungsnetz zu beachten ist. Insbesondere habe ich den kreisfreien Städten und Landkreisen – in Abstimmung mit dem Landesamt für Statistik – zwei Varianten bezüglich der IT-Abschottung ihrer Statistikstellen aufgezeigt.

Bei der ersten Variante befinden sich sämtliche IT-Komponenten innerhalb der abgeschotteten Statistikstelle und werden ausschließlich vom eigenen Personal der Statistikstelle betrieben. Diese Vorgehensweise ist grundsätzlich zu bevorzugen, weil so sämtliche Zuständigkeiten in der Hand der Statistikstelle verbleiben und die Abschottung zuverlässig gewährleistet wird.

Nach der zweiten Variante werden ein oder mehrere Server, auf dem/denen statistische Einzeldaten gespeichert sind, außerhalb der abgeschotteten Statistikstellen in einem kommunalen Rechenzentrum installiert. In diesem Fall müssen die Daten verschlüsselt gespeichert werden. Die Verschlüsselung muss auch gegenüber der Systemverwaltung wirken, soweit sie nicht von Beschäftigten der Statistikstelle selbst gestellt wird. Die Verschlüsselung muss also bereits vor der Übertragung der Einzeldaten auf den Statistikdatenserver erfolgen.

Mittlerweile haben mir verschiedene Städte Konzepte vorgelegt, die eine Auslagerung der Daten der kommunalen Statistikstelle vorsehen. Bei all diesen mir vorgelegten Konzepten sollen sowohl die Datenübertragung als auch die Datenspeicherung verschlüsselt erfolgen. Ich werde mich zu gegebener Zeit von der Umsetzung dieser Maßnahmen überzeugen.

2.1.6 Verkehrsflussanalyse mit gekauften anonymisierten Daten

Anfang 2015 war den Printmedien zu entnehmen, dass die VAG Verkehrs-Aktiengesellschaft Nürnberg gemeinsam mit der Telekom Deutschland GmbH ein Pilotprojekt zur Verkehrsflussanalyse auf Basis anonymisierter Mobilfunkdaten betreibe. Das Projekt in Nürnberg wurde aufgrund der kritischen Medienresonanz wieder eingestellt. Es ist jedoch davon auszugehen, dass auch andere Städte oder Verkehrsbetriebe Interesse an einer solchen Analyse haben, um diese insbesondere für eine Optimierungs- oder Ausbauplanung der öffentlichen Nahverkehrsmittel heranzuziehen.

Das Pilotprojekt in Nürnberg basierte auf den Daten der Telekom Deutschland GmbH, die diese zum Zwecke der Abrechnung und des Managements der Telefonverbindungen erhebt und speichert. Benötigt werden diese Informationen unter anderem zur Übergabe eines Gesprächs von einer Funkzelle zur nächsten; es findet somit keine GPS-Ortung des Handys statt. Identifikationsmerkmale wie etwa TMSI und CallerID, über die eine Reidentifizierung möglich wäre, werden von der Telekom Deutschland GmbH in Hashwerte umgewandelt. Diese Umwandlung ähnelt dem Verfahren der kennzeichenbasierten oder Bluetooth-basierten Reisezeitmessung (siehe 25. Tätigkeitsbericht 2012 unter Nr. 2.1.5). Gleiche Bewegungsmuster von Hashwerten werden aggregiert.

Diese aggregierten Daten werden sodann an die Telekomtochterfirma Motionlogic GmbH übertragen, die im Kundenauftrag Auswertungen auf diesen Daten durchführt. Die Kundin VAG Verkehrs-Aktiengesellschaft Nürnberg erhält von der Motionlogic GmbH nur die Auswertungsergebnisse zu den sie interessierenden Fragen. Sie selbst hat somit keinen Zugriff auf die Daten.

Standardmäßig werden die Daten der gesamten Mobilfunkkundschaft der Telekom Deutschland GmbH für die Auswertung herangezogen. Es besteht jedoch die Möglichkeit, der Nutzung der Mobilfunkdaten für andere Zwecke als der Abrechnung und des Managements der Telefonverbindungen zu widersprechen.

Die Frage, ob die Telekom Deutschland GmbH die Mobilfunkdaten zu anderen Zwecken als der Abrechnung und des Managements der Telefonverbindungen nutzen darf, habe nicht ich, sondern die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zu beantworten. Ebenso verhält es sich hinsichtlich der Frage, ob diese Daten dann an ein Tochterunternehmen weitergegeben werden dürfen. Ich konnte daher nur die Stelle überprüfen, die eine Verkehrsflussanalyse durchführen wollte, hier also die VAG Verkehrs-Aktiengesellschaft Nürnberg.

Im vorliegenden Fall musste ich somit klären, ob eine Reidentifizierung von Mobilfunknutzerinnen und -nutzern auf Basis der Auswertungsdaten möglich ist. Meine Prüfung hat ergeben, dass die VAG Verkehrs-Aktiengesellschaft Nürnberg ausschließlich faktisch anonymisierte Daten erhalten hatte und diese somit nutzen durfte.

Vor der abschließenden Entscheidung über den Ankauf solcher anonymisierter Analyseverfahren ist aus Datenschutzsicht zu empfehlen, beim Anbieter zu klären, wie die zuständige Datenschutzbehörde das Verfahren bewertet hat. Andernfalls kann die öffentliche Stelle, die ein nicht datenschutzkonformes Analyseverfahren mit möglicherweise noch personenbezogenen Daten einsetzt, eine datenschutz-

rechtliche Mitverantwortung treffen, die jedenfalls ab der Anwendung der Datenschutz-Grundverordnung umfassende Verpflichtungen auch unmittelbar gegenüber den Betroffenen auslöst.

2.1.7 Veröffentlichung privater E-Mail-Adressen von Kreistags-, Stadtrats- oder Gemeinderatsmitgliedern

Ein Petent hat mich darauf hingewiesen, dass einige Landratsämter auf ihren Webseiten neben anderen Kontaktdaten auch die überwiegend privat genutzten E-Mail-Adressen von Kreistagsmitgliedern veröffentlichen.

Kreistagsmitglieder sind regelmäßig keine Bediensteten des Landratsamts. Daher werden ihnen keine E-Mail-Adressen aus der E-Mail-Domäne des Landratsamts zugewiesen. Gelegentlich veröffentlichen Landratsämter auf ihrer Webseite die privaten E-Mail-Adressen der Kreistagsmitglieder, sofern sie diese dem jeweiligen Landratsamt für diesen Zweck übermittelt haben.

Das Landratsamt hat auf den E-Mail-Verkehr von und mit den Kreistagsmitgliedern über diese privaten E-Mail-Adressen keinen unmittelbaren Einfluss. Gleichwohl wird durch die Veröffentlichung auf der Webseite des Landratsamts nach außen der Anschein einer gewissen Zurechenbarkeit der privaten E-Mail-Adressen zum Landratsamt erweckt. Dem Landratsamt kommt daher gegenüber den Bürgerinnen und Bürgern, die die kommunalrechtlichen Besonderheiten in der Regel nicht kennen, eine gewisse Verantwortung zu. Denn auch Bürgerinnen und Bürger, die ein Kreistagsmitglied in dieser ehrenamtlichen Funktion erreichen wollen, müssen nicht zwingend dessen private E-Mail-Adresse benutzen. Sie können sich dazu grundsätzlich auch über die amtliche E-Mail-Adresse des Landratsamts an dieses wenden, das dann die Mitteilung an das Kreistagsmitglied weiterleitet.

Private E-Mail-Adressen und darüber laufende Kommunikation genügen meist nicht den an behördliche Kommunikation gestellten datenschutzrechtlichen Anforderungen. Sofern Landratsämter die privaten E-Mail-Adressen der Kreistagsmitglieder weiterhin als Kontaktmöglichkeit veröffentlichen wollen, sollten sie auf ihrer Webseite über mögliche Risiken und die Alternative einer behördlichen E-Mail-Adresse informieren.

Diese Empfehlung gilt entsprechend für ähnliche Veröffentlichungen, etwa von privaten E-Mail-Adressen von Stadtratsmitgliedern auf den Webseiten der jeweiligen Stadt oder von Gemeinderatsmitgliedern auf den Webseiten der jeweiligen Gemeinde.

2.1.8 Videoüberwachung im Krankenhaus

Vor-Ort-Prüfungen in Krankenhäusern haben gezeigt, dass Videoüberwachung mittlerweile Standard in bayerischen Krankenhäusern ist. Sie ist zur Absicherung des Gebäudes in den Eingangs- und Zugangsbereichen und zur Überwachung des Gesundheitszustands von Patientinnen und Patienten auch in medizinischen Bereichen zu finden.

Krankenhäuser sind ein besonders sensibler Bereich, sowohl bezüglich der Schutzwürdigkeit der verarbeiteten Daten als auch bezüglich der Patientinnen und Patienten. Krankenhäuser sind im Normalfall rund um die Uhr geöffnet, haben oft

eine Vielzahl von Eingängen und die Patientenzimmer sind nicht abschließbar, so dass im Hinblick auf die Gebäudesicherung und -überwachung besondere Schutzmaßnahmen geboten sind.

Bei anderen öffentlichen Stellen muss für jede Videoüberwachung einzeln geprüft werden, ob es in der Vergangenheit problematische Vorfälle gab oder ob es sich lediglich um eine abstrakte Gefahr handelt (Art. 21a BayDSG). Für die Krankenhäuser hingegen gibt es Bereiche, in denen eine Videoüberwachung typischerweise zulässig ist, da es im Krankenhaus immer auch um die Gesundheit und das Leben von Personen geht und daher hohe Rechtsgüter zu schützen sind.

Für die Patientensicherheit **typischerweise zulässige Bereiche für die Videoüberwachung** können sein:

- Eingänge,
- direkte Krankenhausvorplätze, wenn es sich dabei nur um den Zugangsbereich des Klinikums handelt und nicht um einen allgemeinen öffentlichen Raum,
- Notaufnahme und Zufahrt,
- Hubschrauberlandeplatz.

Die **Erforderlichkeit** der Videoüberwachung ist hingegen regelmäßig detaillierter zu prüfen und zu begründen bei:

- Parkplätzen, Schranken, Zufahrten,
- Allgemeine Aufenthaltsräume wie Cafeterien und Bistros,
- Kassenautomaten.

Folgende **weitere Bedingungen** müssen bei der Videoüberwachung stets umgesetzt werden:

- Deutlich sichtbare Beschilderung der überwachten Bereiche,

- laufende Beobachtung des Geschehens durch Beschäftigte des Klinikums, zum Beispiel an der Pforte mit dem Ziel, sofort eingreifen zu können,

- Festlegung von Bildausschnitten und Kameraeinstellungen (nicht zoom- oder schwenkbar),

- Ermöglichung zusätzlicher kurzfristiger Aufzeichnungen zu Strafverfolgungszwecken lediglich als Nebenzweck,

- Festlegung der Speicherdauer von maximal 10 Tagen mit anschließender Löschung,

- technische Verhinderung des Zugriffs auf die Aufzeichnungen, Möglichkeit zum Zugriff nur mit Beteiligung von Personalräten und behördlichen Datenschutzbeauftragten,

- Abschluss einer Dienstvereinbarung zur Videoüberwachung,

– datenschutzrechtliche Freigabe mit den Angaben gemäß Art. 21a Abs. 6 in Verbindung mit Art. 26 Abs. 3 Satz 1 BayDSG sowie Beschreibung der eingesetzten Videoaufzeichnungsanlage und der technischen und organisatorischen Maßnahmen nach Art. 7 und Art. 8 BayDSG.

Eine Videoüberwachung im medizinischen Bereich muss dagegen **immer im Einzelfall geprüft werden.** Grundsätzlich gilt:

– Nur Videobeobachtung mit laufender Beobachtung durch sachkundiges Personal, keine Aufzeichnung,

– deutlich sichtbare Beschilderung der überwachten Bereiche,

– Prüfung des Zweckes und der Erforderlichkeit gemäß Prüfschema, zu finden auf meiner Homepage https://www.datenschutz-bayern.de,

– Nutzung ausschließlich für medizinische Zwecke,

– Verhinderung von Einsichtsmöglichkeiten für Unbefugte, zum Beispiel im Vorbeigehen,

– Abschluss einer Dienstvereinbarung zur Videoüberwachung,

– datenschutzrechtliche Freigabe mit den Angaben gemäß Art. 21a Abs. 6 in Verbindung mit Art. 26 Abs. 3 Satz 1 BayDSG sowie Beschreibung der eingesetzten Videoaufzeichnungsanlage und der technischen und organisatorischen Maßnahmen nach Art. 7 und Art. 8 BayDSG.

2.1.9 Berechtigungskonzepte und Protokollierung in Krankenhäusern

Nach Katastrophenereignissen wie dem Zugunglück von Bad Aibling im Februar 2016 fragen mich Betroffene, welche Zugriffsmöglichkeiten Beschäftigte von Krankenhäusern auf Patientendaten im konkreten Fall haben und ob und wie missbräuchliche Zugriffe festgestellt werden können.

Grundsätzlich gilt, dass die Beschäftigten eines Krankenhauses nur auf die Daten zugreifen können dürfen, die sie für ihre jeweilige Aufgabenerfüllung benötigen. Wie dies genau für die verschiedenen Bereiche des Krankenhauses ausgestaltet werden muss, ist ausführlich in der „Orientierungshilfe Krankenhausinformationssysteme (2. Fassung)“ dargelegt. Diese ist abrufbar von meiner Homepage https://www.datenschutz-bayern.de. Bei der Erstellung und Umsetzungskonzepten von Berechtigungskonzepten ist zu beachten, dass keine Gruppenkennungen verwendet werden dürfen. Ansonsten wäre trotz Protokollierung nicht feststellbar, wer tatsächlich zu welchem Zeitpunkt den Computer benutzt und auf Daten zugegriffen hat.

Um überprüfen zu können, wer auf welche Daten zugegriffen hat, ist eine umfassende Protokollierung lesender Zugriffe in den Krankenhaussystemen erforderlich. So können Anschuldigungen geklärt werden, dass Beschäftigte des Krankenhauses unerlaubt Einsicht in Daten genommen hätten. Das Krankenhaus kann so auch den gesetzlichen Anspruch von Betroffenen auf Auskunft erfüllen, wer auf ihre Daten zugegriffen hat. Es müssen daher im Krankenhaus IT-Systeme zum Einsatz kommen, die eine derartige Protokollierung ermöglichen.

Diese Protokollierung kann anlassbezogen ausgewertet werden, also beispielsweise im Falle einer Beschwerde oder eines Auskunftsbegehrens. Gleichzeitig ist jedoch eine regelmäßige Auswertung in Stichproben erforderlich, um auch unbefugte Zugriffe feststellen zu können, die nicht anderweitig bekannt werden. Diese Auswertung darf allerdings nicht alle Zugriffe umfassen und auch nicht ständig stattfinden (Vollüberwachung), sondern hat in festgelegten zeitlichen Abständen und mit festgelegtem Umfang zu erfolgen.

Dazu muss das Krankenhaus ein Stichprobenkonzept erstellen, das regelt, wie ein unbefugter Zugriff erkannt werden kann, wie und durch wen die Auswertung der Protokolle erfolgen und wie häufig sowie in welchem Umfang dies geschehen soll. Es ist zudem festzulegen, dass diese Auswertungen nicht zur Verhaltens- und Leistungskontrolle verwendet werden dürfen. Daher ist auch die Personalvertretung frühzeitig zu beteiligen.

Protokollauswertungen spielen in vielen Bereichen eine zunehmende Rolle. Deswegen können die Ausführungen zum Stichprobenkonzept des Verfahrens TIZIAN im 26. Tätigkeitsbericht 2014 unter Nr. 2.3.8 auch auf Krankenhäuser übertragen werden.

2.2 Prüfungen

Im Berichtszeitraum 2015/2016 habe ich eine ganze Reihe öffentlicher Stellen unter technisch-organisatorischen Datenschutzaspekten geprüft. In vielen Fällen wurden diese Prüfungen von meinem Technikreferat gemeinsam mit dem jeweils zuständigen Rechtsreferat durchgeführt. Schwerpunkte meiner Prüfungstätigkeit im technisch-organisatorischen Bereich waren die Entsorgungskonzepte und Outsourcing-Aktivitäten im klinischen Umfeld, die Datenschutzkonformität von durch öffentliche Stellen angebotenen Apps sowie die Systemkonfigurationen von Mail-Servern (siehe Nrn. 2.2.2 mit 2.2.4).

2.2.1 Geprüfte Einrichtungen

Folgende Stellen und Systeme habe ich im Berichtszeitraum teils durch Vor-Ort-Besuche, teils durch Fragebogen mit anschließend ergänzenden Nachfragen und teils online geprüft:

- Bezirk Schwaben,
- Bezirksklinikum Mainkofen,
- BKK Stadt Augsburg,
- BRK-Pflegezentrum Donauwörth,
- Intelligente Verkehrssysteme (IVS) Testfeld Nürnberg der Obersten Baubehörde,
- Justizvollzugsanstalt Bernau,
- Kommunal BIT – IT-Dienstleister der Städte Erlangen, Fürth und Schwabach,
- NAKO-Studienzentrum Regensburg am Universitätsklinikum Regensburg,
- RoMed Klinikum Rosenheim,
- Theater Regensburg,
- VAG Verkehrs-Aktiengesellschaft Nürnberg,
- Zentrum Bayern Familie und Soziales – Informationsverarbeitungszentrum (ZBFS-IVZ) München,

- Zulassungsbehörde Stadt Ingolstadt,
- Zweckverband Zulassungsstelle Coburg,
- mehrere Apps mit den jeweils hinterlegten Systemen,
- mehrere E-Mail-Server,
- mehr als 100 Krankenhäuser und Krankenhausverbände.

2.2.2 Auftragsdatenverarbeitung bei der Aktenverwaltung und Entsorgungskonzepte in Kliniken

Anfragen und Einzelfallprüfungen haben in der Vergangenheit gezeigt, dass Outsourcing/Auftragsdatenverarbeitung ein zunehmend wichtiges Thema für Krankenhäuser ist. Insbesondere beim Verwalten und Scannen von Papierakten, wie auch bei der datenschutzgerechten Entsorgung personenbezogener Unterlagen und dem IT-Betrieb wird häufig auf externe Dienstleistungsunternehmen zurückgegriffen. Dass dies auch zu Problemen führen kann, hat sich beispielhaft im Februar 2015 gezeigt, als ein Passant hunderte Röntgenbilder aus einem bayerischen Krankenhaus auf der Straße fand. Eigentlich hätten diese über ein externes Dienstleistungsunternehmen entsorgt werden sollen (siehe Pressemitteilung vom 19. Februar 2015).

Das Bayerische Krankenhausgesetz (BayKrG) setzt dem Outsourcing in Krankenhäusern enge Grenzen und setzt den Schutzbedarf der Daten sehr hoch an. So sieht Art. 27 Abs. 4 Satz 6 BayKrG vor, dass sich ein Krankenhaus zur Verarbeitung von Patientendaten, die nicht zur verwaltungsmäßigen Abwicklung der Behandlung erforderlich sind (medizinische Patientendaten), nur anderer Krankenhäuser bedienen darf.

Sinn und Zweck dieser Regelung ist es insbesondere, den Kreis der Personen, die mit sensiblen medizinischen Daten in Berührung kommen, möglichst eng und die Qualifikation der betreffenden Personen möglichst hoch zu halten, um eine missbräuchliche Verwendung medizinischer Patientendaten möglichst auszuschließen (siehe auch Nr. 7.5.1).

Um einen Überblick über die Nutzung der Auftragsdatenverarbeitung in bayerischen Krankenhäusern zu bekommen, habe ich daher im Berichtszeitraum die öffentlichen Krankenhäuser in Bayern mittels eines Fragebogens geprüft und den Krankenhäusern die bei ihnen erkannten jeweiligen Mängel mitgeteilt.

Um eine möglichst gleiche Behandlung öffentlicher und privater Krankenhäuser zu bewerkstelligen, habe ich gemeinsam mit dem Bayerischen Landesamt für Datenschutzaufsicht einen Leitfaden erarbeitet, der genauere rechtliche Ausführungen zu den Anforderungen des Bayerischen Krankenhausgesetzes sowie mögliche Lösungen enthält. Dieser Leitfaden ist auf meiner Homepage https://www.datenschutz-bayern.de zu finden (vergleiche Pressemitteilung vom 29. Juni 2016).

Die Behebung der Mängel werde ich weiterhin intensiv begleiten und auch die gefundenen Lösungen werde ich stichprobenartig vor Ort überprüfen.

2.2.3 Apps – Anwendungen für mobile Endgeräte

Auch wenn ein großer Teil der für Mobilgeräte verfügbaren Apps von nicht-öffentlichen Stellen angeboten wird, so habe ich zum Ende des letzten Berichtszeitraums festgestellt, dass immer mehr bayerische öffentliche Stellen damit beginnen, Apps anzubieten oder entwickeln zu lassen. Wie im 26. Tätigkeitsbericht 2014 unter Nr. 2.1.2 angekündigt, habe ich deshalb eine Prüfung derartiger Apps durchgeführt.

Bei flüchtiger Betrachtung könnte man annehmen, dass eine öffentliche Stelle datenschutzrechtlich für die Verarbeitung von personenbezogenen Daten bei der Nutzung einer von ihr angebotenen App nicht verantwortlich sei. Denn die App wird vom Anwender auf einem Gerät installiert und genutzt, welches sich nicht im Verantwortungsbereich der öffentlichen Stelle befindet, und die Daten, die mit der App verarbeitet werden, gibt gegebenenfalls der Anwender selbst ein.

Bei genauerer Betrachtung sind die meisten Apps aber keine alleinstehenden Programme, wie man sie von klassischen PCs kennt. Vielmehr sind sie eine Kombination aus einem Programm (App), das auf einem mobilen Gerät betrieben wird, und beispielsweise einer Webseite (Hintergrunddienst), die auf Servern der Anbieterin oder des Anbieters gehostet wird. Zwischen der App und dem Hintergrunddienst werden Daten ausgetauscht.

Nur eine App ohne Datenaustausch über das Netzwerk (ohne das Recht überhaupt auf das Netzwerk zuzugreifen) kann aus Sicht des Datenschutzes als eigenständiges Programm in der Verantwortung der jeweiligen Anwenderin oder des jeweiligen Anwenders gesehen werden.

Unabhängig davon muss eine öffentliche Stelle für die von ihr angebotenen Apps sicherstellen, dass die in Art. 7 BayDSG geforderten technischen und organisatorischen Maßnahmen eingehalten werden – auch unabhängig davon, ob sie diese App selbst entwickelt hat oder durch Dritte hat entwickeln lassen. Eine App, die Daten außerhalb des Geräts abruft oder speichert, stellt ein Verfahren im Sinne des Bayerischen Datenschutzgesetzes dar. Dies gilt auch, wenn die App nur Daten ohne Personenbezug, etwa statische Bilder, Videos oder Texte nachlädt. Denn bei der Nutzung einer App wird aus technischen Gründen stets die als personenbezogenes Datum anzusehende IP-Adresse des verwendeten mobilen Geräts an Dritte übermittelt.

Eine vollständige technische Prüfung aller mir bekannten Apps konnte ich aus Kapazitätsgründen leider nicht leisten. Ich musste meine Prüfung von Apps daher einschränken. Neben den Apps, zu denen mir bereits Eingaben vorlagen, wählte ich aus unterschiedlichen Bereichen weitere aus Sicht des Datenschutzes interessante Apps aus, um so einen möglichst repräsentativen Überblick zu erhalten.

An die Anbieterinnen und Anbieter der ausgewählten Apps habe ich in einem ersten Prüfungsschritt einen mehrseitigen, detaillierten Fragebogen versandt, der sowohl rechtliche als auch technische Fragen enthielt. Der Fragebogen basiert auf dem „Prüfkatalog für den technischen Datenschutz bei Apps mit normalem Schutzbedarf“, den mir das Landesamt für Datenschutzaufsicht dankenswerterweise zur Verfügung gestellt hat und der auch auf dessen Webseite https://www.lda.bayern.de als Infoblatt abrufbar ist.

Die relevanten Rückläufe prüfte ich sowohl auf rechtliche als auch auf technisch-organisatorische Mängel.

In einem zweiten Prüfungsschritt unterzog ich einzelne Apps in einem Prüflabor einer konkreten technischen Prüfung. Je nach Notwendigkeit bezog diese eine Analyse des Netzwerkverkehrs, des Verhaltens der App sowohl in verschiedenen Emulatoren als auch auf echten Geräten, des Umfangs der lokal auf dem Mobilgerät gespeicherten Daten, der Sicherheit der involvierten Server, mit denen die App Daten austauschte, und in Einzelfällen auch eine „Disassemblierung" der App mit ein.

Einige der geprüften Stellen entfernten ihre App kurz nach Erhalt des Fragebogens. Auch wenn sie diese Entscheidung nicht mit der konkreten Prüfung begründet haben, so bleibt zumindest die Vermutung, dass hierfür eventuell bereits selbst erkannte Mängel in Bezug auf die Einhaltung datenschutzrechtlicher Anforderungen ein Grund gewesen sein könnten.

Fast alle angefragten öffentlichen Stellen bejahten die Frage, ob das App-Verfahren, also die App an sich, zusammen mit den dazugehörigen Hintergrunddiensten, personenbezogene Daten verarbeite. Allerdings verneinten ebenfalls fast alle dieser Stellen die Frage, ob das Verfahren nach Art. 26 BayDSG freigegeben sei. Dies hat mir die Notwendigkeit dieser Prüfung bestätigt.

Folgende grundlegenden Datenschutzanforderungen wurden häufig nicht oder nur mangelhaft umgesetzt:

— Datenschutzrechtliche Freigabe

  Nach Art. 26 BayDSG bedarf der erstmalige Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, grundsätzlich der vorherigen schriftlichen Freigabe durch die das Verfahren einsetzende öffentliche Stelle.

  Zumindest jede App, die das Recht des Netzwerkzugriffs besitzt, ist daher freizugeben. Die Freigabe darf sich nicht nur auf die App selbst beschränken, sondern muss sich auch auf alle Hintergrunddienste erstrecken, mit denen die App über Netzwerke Daten austauscht.

  Unabhängig von der Notwendigkeit einer Freigabe empfiehlt es sich, in jedem Fall die behördlichen Datenschutzbeauftragten – am besten bereits bei der Planung einer App – miteinzubeziehen.

— Impressum und Datenschutzerklärung

  Grundsätzlich ist eine App als Telemediendienst anzusehen. Daher sind die in § 5 Abs. 1 Telemediengesetz (TMG) aufgeführten Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten („Impressumspflicht").

  Weiterhin sind die Nutzerinnen und Nutzer gemäß § 13 Abs. 1 Satz 1 TMG zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verar-

beitung ihrer Daten in allgemein verständlicher Form zu unterrichten („Datenschutzerklärung"). Detaillierte Ausführungen hierzu finden sich im 26. Tätigkeitsbericht 2014 unter Nr. 2.1.2.

Insbesondere hat die Datenschutzerklärung (der App) detailliert Auskunft über die Datenverarbeitung der App Auskunft zu geben. Eine Kopie der Datenschutzerklärung des Internetauftritts genügt hierfür nicht, zumal diese meist auch nicht zutrifft.

— Verschlüsselung der Datenübertragung

Sendet oder empfängt eine App personenbezogene Daten an oder von Servern im Internet, so sind diese Daten zu verschlüsseln. Auch wenn in den übersandten Fragebogen eine Verschlüsselung bejaht wurde, so erwies sich in der konkreten technischen Prüfung mehrfach, dass tatsächlich keine oder nur eine teilweise Verschlüsselung der Daten stattfand.

Es empfiehlt sich hier, externe Entwickler ausdrücklich auf die Notwendigkeit einer Verschlüsselung hinzuweisen und dies auch zu prüfen oder prüfen zu lassen.

— Eingebundene Dienste Dritter

Einige Apps benutzen beispielsweise Kartendienste, um den Weg zu einem bestimmten Ort darzustellen. Dadurch kann der Diensteanbieter eine Vielzahl von personenbezogenen Daten erhalten, vor allem wenn er die Nutzerinnen oder Nutzer bereits durch andere genutzte Dienste eindeutig identifizieren kann. Der derart eingebundene Diensteanbieter ist für die Nutzung innerhalb der App grundsätzlich nicht für die Datenverarbeitung selbst verantwortlich; die Verantwortung verbleibt bei der öffentliche Stelle als Anbieterin der App.

Sollte der Diensteanbieter bereits umfangreiche Daten aus anderen Quellen über eine Nutzerin oder einen Nutzer besitzen, so ist die Einbindung des Dienstes analog einem „Social Plugin" zu bewerten. Ich verweise hierzu auf meine Ausführungen zu Social Plugins auf Webseiten bayerischer öffentlicher Stellen, zu finden auf meiner Homepage https://www.datenschutz-bayern.de.

— Rechte der App

Jede App darf bei der Installation nur genau die Rechte anfordern, die zum Betrieb auch nötig sind. Es ist darauf zu achten, dass eine App mit der Angabe, dass sie keinen Zugriff auf Dienste im Internet benötigt, auch kein Recht einfordern darf, auf das Internet zuzugreifen. Überschießende Rechte sind zu entziehen.

Zusammengefasst habe ich leider bei fast allen Apps Mängel gefunden, die einen Zugriff auf Hintergrunddienste nutzen. In vielen Fällen haben sich die öffentlichen Stellen als Anbieterinnen von Apps wohl darauf verlassen, dass die Entwickler (Auftragnehmer) Sicherheits- und Datenschutzaspekte selbstständig beachten und zuverlässig umsetzen. Es ist aber eine Pflicht der öffentlichen Stelle als Auftraggeberin, detaillierte Anforderungen bereits bei der Auftragsvergabe festzulegen und deren korrekte Umsetzung auch zu prüfen.

Leider scheint sich bei Apps zu wiederholen, was zu Beginn der Entwicklung von Webanwendungen ebenfalls deutlich wurde: Funktionalität und Design werden konkret beauftragt und umgesetzt, Datenschutz und Datensicherheit werden dagegen – wenn überhaupt angedacht und bedacht – wie selbstverständlich als implementiert und gegeben angenommen. Eine nachträgliche Korrektur von Mängeln kann aber – wie im Rahmen der Prüfung festgestellt – dazu führen, dass eine App kostenintensiv ein zweites Mal erneut entwickelt werden muss.

Das Landesamt für Datenschutzaufsicht hat eine „Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter" erstellt. Auch wenn diese primär die Entwicklung von Apps durch nicht-öffentliche Stellen behandelt, so kann sie doch als gute Grundlage auch für die Entwicklung von Apps durch öffentliche Stellen dienen. Bei der Auftragsvergabe empfehle ich, diese Orientierungshilfe mit einzubeziehen. Die Orientierungshilfe ist zu finden auf der Webseite des Landesamts für Datenschutzaufsicht https://www.lda.bayern.de.

2.2.4 Spam-Abwehr auf E-Mail-Servern

Die mir im Rahmen von Beschwerden mitgeteilten Bedenken bezüglich den bei einigen bayerischen öffentlichen Stellen eingesetzten Anti-Spam-Lösungen veranlassten mich dazu, einige der eingesetzten Verfahren auf technische und organisatorische Mängel umfangreich zu prüfen. Meinen Prüfungsschwerpunkt legte ich auf Verfahren, die nicht von öffentlichen Stellen selbst oder im Auftrag, sondern von nicht-öffentlichen Stellen als „Hosting"-Dienstleistung angeboten werden.

Bei einem ersten Prüfschritt mit rund 2.300 E-Mail-Domänen („MX-Einträge") von bayerischen öffentlichen Stellen wurde deutlich, dass das IT-Dienstleistungszentrum des Freistaats Bayern, die Landratsämter und die Städte die Rangliste der Betreiber von E-Mail-Domänen deutlich anführten, gefolgt von bekannten großen Hosting-Providern. Aus diesen weiteren Betreibern wählte ich einzelne für eine detaillierte Prüfung aus und bezog dabei auch die Beschwerden mit ein. Vereinzelt wurden auch Verfahren geprüft, die von den Behörden selbst betrieben wurden.

Die detaillierte Prüfung umfasste einen Fragebogen, der unter anderem folgende Fragen enthielt:

— Welche Server („MX-Hosts") werden für die jeweilig verwendeten E-Mail-Domänen als Empfänger eingesetzt?

— Welche dieser Server bieten STARTTLS mit Perfect Forward Secrecy (PFS) an?

— Wo und von wem werden diese Server betrieben und gewartet?

— Welche Software wird in welcher Version auf den Servern eingesetzt?

— Welche personenbezogenen Daten werden auf den Servern protokolliert?

— Wie lange werden die Protokolldaten gespeichert und wer hat Zugriff darauf?

— Wie ist die private E-Mail-Nutzung geregelt?

Zusätzlich wurde eine technische Prüfung der angefragten E-Mail-Domänen durchgeführt, um die gegebenen Antworten soweit möglich nachzuprüfen und die genauen technischen Eigenschaften festzustellen.

Folgende Mängel habe ich häufig festgestellt:

— Beauftragen Behörden externe Dritte mit dem Betrieb eines E-Mail-Servers, so rechtfertigen sie dies häufig mit der **Verarbeitung von personenbezogenen Daten im Auftrag,** bei der die strengen Voraussetzungen der Datenübermittlung nicht vorliegen müssen. Dann aber sind nach Art. 6 BayDSG die Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihnen getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei Datenerhebung, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Der Auftraggeber hat sich, soweit erforderlich, von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen beim Auftragnehmer zu überzeugen.

  Gerade bei den von den Petenten gemeldeten Fällen hat sich gezeigt, dass diese Anforderungen nicht erfüllt waren.

— Nach Art. 7 Abs. 2 BayDSG sind bei der automatisierten Verarbeitung von personenbezogenen Daten insbesondere Maßnahmen zu treffen, die geeignet sind zu verhindern, dass bei der Übertragung personenbezogener Daten die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle). Insofern sind Behörden bereits heute verpflichtet, dem Stand der Technik entsprechende Verschlüsselungsverfahren anzubieten. Dies betrifft nicht nur eine gegebenenfalls nötige Ende-zu-Ende-Verschlüsselung etwa mittels S/MIME, sondern auch eine **verschlüsselte Übertragung zwischen den einzelnen E-Mail-Servern mittels STARTTLS und PFS** („Leitungsverschlüsselung"). Insbesondere wenn E-Mail-Server des Auftragnehmers Daten an den E-Mail-Server der Auftraggeberin Behörde über das Internet weiterleiten, muss diese Verbindung zumindest mit STARTTLS geschützt werden.

  Grundsätzlich ist der Aufwand, diese Verschlüsselung einzusetzen, als relativ gering anzusehen. Es zeigte sich aber bei der Prüfung, dass bei einigen Anbieterinnen und Anbietern zumindest in der zum Prüfungszeitpunkt eingesetzten Software-Version STARTTLS nicht unterstützt wurde. Auch hiervon waren die mir gemeldeten Fälle betroffen.

— Einige der geprüften Behörden ersetzten zum Teil bereits nach dem Erhalt des Fragebogens und andere nach dem Erhalt des Prüfungsergebnisses die von ihnen eingesetzten Systeme beziehungsweise Verfahren. Es liegt nahe, dass eine Neubeschaffung in diesen Fällen wohl der einfachere oder auch der einzige Weg war, einen datenschutzgerechten Betrieb zu ermöglichen. Die neuen Verfahren erfüllten alle Anforderungen oder benötigten nur noch kleinere Anpassungen.

  Auch wenn noch nicht alle geprüften Stellen die festgestellten Mängel beseitigen konnten, so wurde doch in fast allen Fällen zwischenzeitlich die

Konfiguration angepasst oder die verwendeten Produkte durch neue Verfahren ersetzt. Ein datenschutzrechtlich einwandfreier Betrieb ist nun möglich.

Soweit dies nicht schon bei der Beschaffung von Anti-Spam-Lösungen geschehen ist, fordere ich alle öffentlichen Stellen dazu auf, die eigenen Verfahren bezüglich der datenschutzrechtlichen Regelungen zu prüfen und gegebenenfalls entsprechende Maßnahmen zu ergreifen.

2.2.5 NAKO-Gesundheitsstudie: Prüfung Studienzentrum Regensburg

Die NAKO-Gesundheitsstudie (kurz NAKO) ist eine deutschlandweite Studie zur Langzeitbeobachtung der Entstehung und Entwicklung von sogenannten Volkskrankheiten wie Krebs, Demenz, Diabetes, Herzinfarkt und Infektionskrankheiten. Diese Studie wird betrieben vom Verein Nationale Kohorte e.V., in dem sich mehrere Forschungseinrichtungen zusammengeschlossen haben. Hierzu werden in 18 bundesweit verteilten Studienzentren 200.000 zufällig ausgewählte Personen untersucht und zu ihren Lebensgewohnheiten befragt. In regelmäßigen Abständen sollen Nachuntersuchungen und -befragungen stattfinden. Aufgrund der geplanten Laufzeit von 20-30 Jahren und des Umfangs der erhobenen Daten wird diese Studie sehr eng von den Datenschutzaufsichtsbehörden begleitet.

Die Auswahl der potenziellen Teilnehmerinnen und Teilnehmer geschieht über eine zufällige Ziehung in den Einwohnermeldeämtern im Umfeld der 18 Studienzentren. Die gezogenen Personen werden dann vom jeweiligen Studienzentrum angeschrieben, zur Patienteneigenschaft befragt und gegebenenfalls um ihre Zustimmung zur Teilnahme gebeten. Beim ersten Untersuchungstermin im Studienzentrum erfolgt die detaillierte Patienteninformation und Einwilligung. Hierbei können die Betroffenen auch einzelne Teile der Studie auslassen. Dann werden die entsprechenden Daten nicht erhoben.

Die Studiendaten werden zwar im jeweiligen Studienzentrum erhoben, die Speicherung erfolgt jedoch in einer für alle Studienzentren einheitlichen IT-Infrastruktur. Dabei werden die medizinischen Daten und die personenidentifizierenden Daten der Teilnehmerinnen oder Teilnehmer voneinander getrennt und bei verschiedenen Einrichtungen und auf verschiedenen Servern gespeichert. Eine Zusammenführung der Daten erfolgt nur im Studienzentrum während der Untersuchung und Befragung der Teilnehmerinnen oder Teilnehmer. Für Forschungszwecke kann nur auf anonymisierte oder pseudonymisierte Daten zugegriffen werden. Die Einzelheiten sind im Datenschutzkonzept der NAKO festgelegt, das in die Zuständigkeit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) fällt.

Alle Studienzentren nehmen in regionalen Einrichtungen Auftragsdatenverarbeitungen für den Nationale Kohorte e.V. wahr. In Bayern gibt es zwei Studienzentren in Augsburg und Regensburg sowie das Zentrallager für die Bioproben. Das Studienzentrum Augsburg sowie das Zentrallager werden von der Helmholtz-Gesellschaft betrieben und fallen in die datenschutzrechtliche Zuständigkeit der BfDI. Das Studienzentrum Regensburg wird von der Universität Regensburg betrieben und untersteht somit meiner Kontrolle. Im Jahr 2016 habe ich geprüft, wie dort das Datenschutzkonzept umgesetzt wird und ob ausreichende Maßnahmen zum Schutz der sehr sensiblen Daten der Teilnehmerinnen und Teilnehmer getroffen wurden.

Im Ergebnis konnte ich feststellen, dass das Studienzentrum sich der Sensibilität der Daten bewusst und sehr bemüht ist, die Anforderungen des Datenschutzes umzusetzen. Allerdings waren zum Prüfungszeitpunkt einige Teile der zentralen Infrastruktur noch nicht voll funktionsfähig. So mussten Daten beispielsweise noch lokal zwischengespeichert werden, um Datenverluste zu verhindern. Das Studienzentrum hat hierbei allerdings sicherzustellen, dass nur wenige Personen im Bedarfsfall Zugriff auf diese Daten erhalten. Ich habe dies der BfDI mitgeteilt und werde weiterverfolgen, ob in naher Zukunft eine Löschung dieser lokal zwischengespeicherten Daten erfolgen kann.

Um die sichere Identifizierung der teilnehmenden Personen wie auch die persönliche Ansprache zu gewährleisten, arbeitet das Studienzentrum während des Patientenbesuchs sowie zur Vor- und Nachbereitung mit personenbezogenen Daten. Wichtig war mir daher besonders, dass diese temporär auch auf Papier vorhandenen Unterlagen sicher verwahrt und nach dem Besuch datenschutzgerecht entsorgt werden.

Eine interessante Frage, die im Rahmen meiner Prüfung beim Studienzentrum Regensburg aufkam und die auch schon im Zusammenhang mit anderen Studien diskutiert wurde, ist die Nutzung von Non-Responder-Fragebögen. Diese Fragebögen werden an die Personen versandt, die nicht an der Studie teilnehmen wollen. Neben der Bitte um Angabe von Gründen für die Nichtteilnahme enthält der Fragebogen auch Fragen zum gesundheitlichen Zustand, die dann ebenfalls in der Studiendatenbank gespeichert werden sollen. Dies ist aus meiner Sicht kritisch zu sehen, da nicht teilnehmende Personen keine genaueren Informationen zur Studie und zur IT-Infrastruktur erhalten haben können und auch nicht in die Datenverarbeitung durch die Studie eingewilligt haben. Zudem machte das Datenschutzkonzept der NAKO zum Prüfungszeitpunkt keine genaueren Aussagen zur Verarbeitung der Daten der nicht teilnehmenden Personen (zum Beispiel zur Anonymisierung), weswegen ich diesen Punkt ebenfalls der BfDI mitgeteilt habe. Ich werde die Entwicklung des Datenschutzkonzepts der NAKO sowie auch des Studienzentrums Regensburg weiterhin verfolgen.

2.2.6 Immatrikulationsbescheinigung online

Eine bayerische Hochschule ermöglichte ihren Studierenden, Immatrikulationsbescheinigungen über ein Webformular abzurufen und dann selbst auszudrucken. Andere Stellen, denen eine solche Bescheinigung vorgelegt wurde, konnten diese aber nur sehr schwer auf Echtheit prüfen. Da es sich hierbei um eine große Anzahl von nötigen Verifikationen handelte, schieden beispielsweise telefonische Rückfragen bei der Hochschulverwaltung aus.

Daher enthielt jede online erstellte Immatrikulationsbescheinigung einen sogenannten Verifikationscode, der aus 12 alphanumerischen Zeichen bestand und auf einer Webseite der Hochschule eingegeben werden konnte. Sofern der Verifikationscode gültig war, erhielt die anfragende Person als Bestätigung die auf der Immatrikulationsbescheinigung aufgedruckten Daten angezeigt, so dass eine Fälschung dieser Daten wirksam erschwert wurde.

Allerdings ermöglichte diese Online-Verifikation der anfragenden Person auch, zusätzliche Daten, etwa Angaben zu einer während des Gültigkeitszeitraums der Bescheinigung möglicherweise stattgefundenen Exmatrikulation, abzurufen.

Außerdem gab die Eingabe eines Verifikationscodes auch den aktuellen Studierendenstatus aus, selbst wenn sich dieser außerhalb des Gültigkeitszeitraums der Bescheinigung befand. So war es beispielsweise möglich, mit einer Bescheinigung für das erste Semester auch Jahre später noch festzustellen, ob die Studierenden immer noch immatrikuliert waren oder wann sie zwischenzeitlich exmatrikuliert wurden.

Ich habe das Verfahren im Grundsatz als zulässig erachtet – auch soweit Änderungen innerhalb des Gültigkeitszeitraums der Immatrikulationsbescheinigung im Rahmen der Online-Verifikation abrufbar gehalten werden. Sollten Studierende während des Semesters, für das die Bescheinigung erstellt wurde, exmatrikuliert werden, so darf auch dies durchaus mitgeteilt werden.

Als unzulässig erachtet habe ich aber, dass Bescheinigungen auch dafür verwendet werden konnten, den Immatrikulationsstatus außerhalb des Bescheinigungszeitraums abzufragen. Unzulässig ist auch, den Umstand mitzuteilen, dass mittels jeder Bescheinigung rückwirkend dauerhaft das Ende der – gegebenenfalls außerhalb des Bescheinigungszeitraums liegenden – Immatrikulation feststellbar war.

Die Hochschule hat daraufhin das Verfahren so angepasst, dass nur noch die zulässigen Daten mittels Online-Verifikation abgerufen und geprüft werden können.

2.3 Beanstandungen

Leider musste ich in diesem Berichtszeitraum im technisch-organisatorischen Bereich mehrere Beanstandungen nach Art. 31 Abs. 1 BayDSG aussprechen. Dabei handelte es sich jeweils um tatsächlich erfolgte Offenbarungen besonders schutzwürdiger Daten – nämlich Patientendaten und Personaldaten – in medizinischen Einrichtungen.

Eine Beanstandung musste ich aussprechen, weil ein Krankenhaus viele hundert zur Entsorgung vorgesehene Röntgenbilder sackweise an unbekannte Abholer übergeben hatte. Die Abholer hatten sich als Unterauftragnehmer des vom Klinikum beauftragten Entsorgers ausgegeben. Eine Teilmenge dieser Röntgenbilder wurde im öffentlichen Verkehrsraum aufgefunden, wodurch der Vorfall bekannt wurde. Zwar waren die Diebe wohl nicht an den patientenbezogenen Daten, sondern eher an den im Trägermaterial der Röntgenbilder enthaltenen Edelmetallen interessiert. Gleichwohl erfolgte durch den Diebstahl eine unzulässige Offenbarung patientenbezogener Daten gegenüber unberechtigten Dritten. Der Diebstahl konnte nur erfolgen, weil die vom Krankenhaus getroffenen technisch-organisatorischen Maßnahmen zur Entsorgung von Patientenunterlagen schwerwiegende Fehler und Unterlassungen aufwiesen. So enthielt der abgeschlossene Entsorgungsvertrag insbesondere keine hinreichenden Regelungen zur Sicherstellung des Gewahrsams des Krankenhauses an dem Datenmaterial, keine Festlegung von Unterauftragsverhältnissen und keine Festlegung geeigneter Transportbehältnisse. Auch für das konkrete Entsorgungsvorhaben waren vorab weder Abholberechtigte noch Abholzeitpunkt festgelegt worden. Ein Ergebnis aus diesem Vorfall ist unter anderem die Entwicklung des Leitfadens „Auftragsdatenverarbeitung bei der Aktenverwaltung in bayerischen öffentlichen und privaten Krankenhäusern“ (siehe Nr. 2.2.2).

Die zweite Beanstandung betraf ein Krankenhaus, in dem auf einem dezentralen Fileserver einer seiner Kliniken ein Unterordner zum Personal dieser Klinik eingerichtet war. Dieser Personalordner enthielt Korrespondenz zu Personalangelegenheiten von ehemaligen und aktuellen Beschäftigten. Aufgrund mangelhafter Zugriffs- und Berechtigungsverwaltung war jedem für diesen Fileserver Berechtigten auch dieser Personalordner zugänglich, selbst wenn er nicht mit der Personalsachbearbeitung der Klinik betraut war.

Die dritte Beanstandung musste ich einem Klinikum gegenüber aussprechen, weil die Daten eines dort behandelten Patienten auf dem privaten Facebook-Account eines Bediensteten des Klinikums veröffentlicht wurden. Wie diese Patientendaten aus den klinikeigenen Systemen in das Soziale Netzwerk gelangten, konnte letztendlich nicht mehr vollständig aufgeklärt werden.

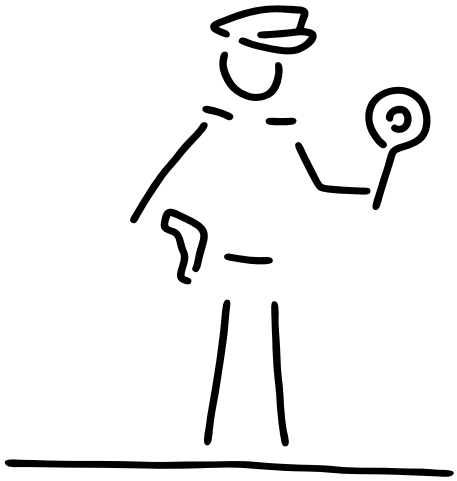
Die vierte Beanstandung betraf ein Klinikum, das seiner gesetzlichen Verpflichtung, mich – durch die Erteilung von Auskünften und Bereitstellung von Informationen – bei der Erfüllung meiner Aufgaben zu unterstützen, nicht in angemessener Weise nachgekommen war. Trotz mehrfacher Aufforderung hatte das Klinikum seit zwei Jahren meine Nachfragen zum Sachstand der weiteren Mängelbehebung bezüglich einer dort von mir durchgeführten Prüfung nicht beantwortet. Es war für mich daher auch nach so langer Zeit nicht erkennbar, ob und inwieweit seinerzeit festgestellte und noch offene Mängel behoben wurden und ob mittlerweile die dortigen IT-Systeme datenschutzkonform betrieben werden.

2.4 Orientierungshilfen

Als ein Ergebnis einer flächendeckenden Prüfung von Krankenhäusern im Berichtszeitraum (siehe Nr. 2.2.2) habe ich mit dem Bayerischen Landesamt für Datenschutzaufsicht einen Leitfaden zusammengestellt, in dem die wichtigsten Anforderungen an die Auftragsdatenverarbeitung in bayerischen Krankenhäusern sowie die Möglichkeiten und erforderlichen Maßnahmen zur gesetzeskonformen Beteiligung externer Dienstleister als Best Practice zusammengefasst sind.

Der Leitfaden „Auftragsdatenverarbeitung bei der Aktenverwaltung in bayerischen öffentlichen und privaten Krankenhäusern“ ist auf meiner Homepage https://www.datenschutz-bayern.de zu finden.

3 Polizei



3.1 Allgemeines

3.1.1 Änderungsbedarf des Polizeiaufgabengesetzes

Im Berichtszeitraum ist eine wegweisende Gerichtsentscheidung des Bundesverfassungsgerichts ergangen, die einen erheblichen Anpassungsbedarf des Polizeiaufgabengesetzes zur Folge hat:

Das Bundesverfassungsgericht hat in seinem Urteil vom 20. April 2016 – 1 BvR 966/09, 1 BvR 1140/09 – entschieden, dass die angegriffenen Regelungen des Bundeskriminalamtsgesetzes in ihrer jetzigen Ausgestaltung weitgehend verfassungswidrig sind. Die Ermittlungsbefugnisse des Bundeskriminalamts zum Einsatz von heimlichen Überwachungsmaßnahmen zur Abwehr von Gefahren des internationalen Terrorismus sind zwar im Grundsatz mit den Grundrechten vereinbar, die derzeitige Ausgestaltung verstößt aber gegen den Verhältnismäßigkeitsgrundsatz. Die beanstandeten Vorschriften gelten mit Einschränkungen überwiegend bis zum Ablauf des 30. Juni 2018 weiter.

Die Entscheidung betrifft, eine langjährige Rechtsprechung zusammenführend, sowohl die Voraussetzungen für die Durchführung von heimlichen Überwachungsmaßnahmen als auch die Frage der grundsätzlichen Verwendung der erhobenen Daten und der Datenübermittlung an andere inländische Behörden sowie schließlich erstmals auch die Anforderungen an eine Datenübermittlung an ausländische Behörden. In seiner aktuellen Entscheidung führt das Gericht seine bisherige Rechtsprechung in grundsätzlicher Weise zusammen und setzt zugleich neue Maßstäbe. Unter anderem fordert das Bundesverfassungsgericht:

- Besondere Schutzregelungen für den Kernbereich privater Lebensgestaltung,
- einen hinreichenden Schutz von Berufsgeheimnisträgern,
- eine regelmäßige effektive aufsichtliche Kontrolle. Das heißt, dass Datenerhebungen vollständig protokolliert werden müssen und es muss durch technische und organisatorische Maßnahmen sichergestellt werden, dass die Daten in praktikabler, auswertbarer Weise zur Verfügung stehen und die Protokollierung hinreichende Angaben zu dem zu kontrollierenden Vorgang enthält,
- Berichtspflichten gegenüber Parlament und Öffentlichkeit,
- umfangreiche Löschungspflichten,
- eine Unterscheidung zwischen einer grundsätzlich zulässigen weiteren Nutzung der Daten im Rahmen des ursprünglichen Erhebungszweckes (Zweckbindung) und einer Zweckänderung, die nur in bestimmten Grenzen erlaubt werden darf,
- eine Begrenzung für die Datenübermittlung an ausländische Sicherheitsbehörden.

Weiterer wesentlicher Anpassungsbedarf des Polizeiaufgabengesetzes besteht aufgrund der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI (im Folgenden „Richtlinie"), die am 4. Mai 2016 im Amtsblatt der Europäischen Union veröffentlicht wurde (siehe Nrn. 1.1.1.2, 1.1.1.4, 5.1.1). Die Richtlinie ist Teil eines Datenschutzpaketes und entfaltet im Gegensatz zur Grundverordnung keine unmittelbare Wirkung in den Mitgliedstaaten. Vielmehr legt sie einen datenschutzrechtlichen Rahmen in Form eines Mindeststandards fest. Es obliegt den Mitgliedstaaten, die Richtlinie innerhalb der vorgegebenen Zeit von zwei Jahren in nationales Recht umzusetzen. Daraus ergibt sich aber auch ein gewisser Spielraum zur Umsetzung durch die jeweiligen Gesetzgeber. Es wird klargestellt, dass die nationalen Regelungen auch ein höheres Schutzniveau als von der Richtlinie vorgegeben gewähren dürfen (vgl. Art. 1 Abs. 3 der Richtlinie und Nr. 15 der Erwägungsgründe).

Ziel der Richtlinie ist, eine wirksame justizielle Zusammenarbeit in Strafsachen und eine wirksame polizeiliche Zusammenarbeit sicherzustellen und den Austausch personenbezogener Daten zwischen den zuständigen Behörden der Mitgliedstaaten zu erleichtern. Gleichzeitig soll ein einheitlich hohes Schutzniveau für die personenbezogenen Daten natürlicher Personen gewährleistet werden. Anders als der Rahmenbeschluss 2008/977/JI des Rates, der durch die Richtlinie ersetzt wird, deckt die Richtlinie jetzt auch die innerstaatliche Verarbeitung personenbezogener Daten ab, da die Union mit Art. 16 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) über eine neue Rechtsgrundlage verfügt, die auch für die Verarbeitung personenbezogener Daten im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit gilt.

Zu den wesentlichen Vorgaben der Richtlinie gehören unter anderem:

- Bildung von Kategorien bei der Datenerhebung und Unterscheidung nach der Verfahrensrolle: Beschuldigte, Verurteilte, Geschädigte, Zeugen, sonstige Dritte; zudem Differenzierung nach Verdachtsgraden mit Pflicht zur laufenden Anpassung,

- Nachweispflicht der Behörden, dass die Datenschutzbestimmungen eingehalten werden (Dokumentation),
- Pflicht zur Einführung von Datenschutzmanagementsystemen, datenschutzfreundlicher Technik, Verzeichnissen für Datenverarbeitungsverfahren, umfassenden Protokollierungen, Folgenabschätzungen bei neuen Vorhaben,
- der Landesbeauftragte für den Datenschutz wird in eine Datenschutzaufsichtsbehörde umgestaltet, die über Untersuchungs- und Abhilfebefugnisse verfügt. Im Gegenzug sind Rechtsmittel der Behörden gegen Anordnungen des Landesbeauftragten für den Datenschutz vorgesehen.

Im Ergebnis muss daher insbesondere das Polizeiaufgabengesetz an zahlreichen Stellen angepasst werden. Dazu stehe ich im engen Austausch mit dem zuständigen Staatsministerium des Innern, für Bau und Verkehr. Über konkrete Ergebnisse, die zum Redaktionsschluss noch nicht feststanden, werde ich weiter berichten.

3.1.2 Precobs

Polizeibeamte kontrollieren Bürger, weil eine Software dies vorgibt – solche oder ähnliche Szenarien wurden in den Medien befürchtet, als das Staatsministerium des Innern, für Bau und Verkehr im Sommer 2014 eine neue Polizeisoftware der Öffentlichkeit vorstellte. Diese Aussicht ließ selbstverständlich auch mich aufhorchen. In der Folge habe ich mich mit der „Precobs" genannten Software und deren Anwendung bei der Polizei kritisch auseinandergesetzt. Hierbei kam ich zu dem Ergebnis, dass das verwendete Analysesystem in der aktuellen Ausgestaltung datenschutzrechtlich nicht zu beanstanden ist.

Abgesehen von Angaben zum Tatort, zur Tatzeit und zu besonderen Tatumständen bereits zurückliegender Einbrüche verwendet das System keine personenbezogenen Daten um die Tatvorhersagen zu berechnen. Auch muss der zuständige Lagesachbearbeiter der Polizei das Analyseergebnis der Software nochmals gegenprüfen, bevor er es freigibt. Die Einbruchsprognose für einen bestimmten Bereich wird dann den Beamtinnen und Beamten visuell dargestellt. So vorinformiert will die Polizei zukünftig zur richtigen Zeit am richtigen Ort präsent sein.

Neben den verwendeten Datenbeständen habe ich ein weiteres Augenmerk darauf gelegt, dass eine Polizeibeamtin oder ein Polizeibeamter und nicht die Software – sprich ein unbekannter Algorithmus – die Entscheidung bezüglich einer Maßnahme trifft. Bei allen Rechtseingriffen der Polizei – wie beispielsweise vermehrten Personenkontrollen in einem bestimmten Gebiet – gelten weiterhin die gesetzlichen Schranken. Prognose hin oder her, in jedem Einzelfall müssen die rechtlichen Vorgaben durch die Polizei vor Ort strikt eingehalten werden. Natürlich werde ich auch weiterhin die Entwicklung des Analysesystems genau im Auge behalten. Was nicht passieren darf, ist eine schleichende Übernahme der eigentlichen Polizeiarbeit durch einen Computer.

Auch die Datenschutzbeauftragten des Bundes und der Länder haben sich auf ihrer 89. Konferenz am 18./19. März 2015 mit dieser Thematik befasst. In der nachstehenden Entschließung werden die allgemeinen Gefahren und Risiken im Zusammenhang mit dem zunehmenden Einsatz von Datenanalysesystemen durch die Polizei kritisch hinterfragt.

Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19.03.2015 in Wiesbaden

Big Data zur Gefahrenabwehr und Strafverfolgung: Risiken und Nebenwirkungen beachten

Zunehmend sind Systeme zur Datenanalyse auch für Polizeibehörden am Markt verfügbar. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist daher frühzeitig – bevor diese Systeme in der Fläche beschafft werden – darauf hin, dass der Einsatz solcher Systeme durch die Polizei geeignet ist, elementare Grundsätze des Datenschutzes und des Rechts auf informationelle Selbstbestimmung in Frage zu stellen. Solche Verfahren können enorme Mengen von heterogenen – strukturierten wie unstrukturierten – Daten mit hoher Geschwindigkeit auswerten. Sogenannte selbst lernende Algorithmen sind in der Lage, die Kriterien für die Auswertung selbst zu entwickeln und an neue Erkenntnisse anzupassen. Damit sollen Zusammenhänge zwischen Straftaten erkannt werden und Vorhersagen über künftige Straftaten oder Gefahren bereits im Vorfeld getroffen werden ("Predictive Policing").

Dies kann zu einer weiteren Verschiebung der polizeilichen Eingriffsschwelle in das Vorfeld von Gefahren und Straftaten führen. Die Gefahr fehlerhafter Prognosen ist der Vorfeldanalyse stets immanent – mit erheblichen Auswirkungen auf die dabei in Verdacht geratenen Personen.

Besonders kritisch ist es, wenn Analysesysteme vermeintlich harmlose, allgemein zugängliche Daten aus dem Internet auswerten, etwa aus Foren oder sozialen Netzwerken. Diese können zudem mit polizeilichen Speicherungen verknüpft und einer konkreten Person zugeordnet werden. Es besteht das Risiko, dass die Systeme die Daten aus einem ganz anderen Zusammenhang verwenden, denen kein gefährdendes oder strafbares Verhalten zu Grunde liegt. Dann können Bürgerinnen und Bürger nicht mehr sicher sein, welche ihrer Handlungen von der Polizei registriert und nach welchen Kriterien bewertet werden – zumal diese stets nur auf statistischen Erfahrungswerten beruhen, die im Einzelfall nicht zutreffen müssen. Sind die Kriterien und die Funktionsweise der Auswertealgorithmen nicht bekannt, ist es den Betroffenen unmöglich, das Ergebnis mit eigenen Angaben zu widerlegen.

Auch wenn die derzeit in der Praxis bei einzelnen Länderpolizeien eingesetzten Verfahren, mit denen relevante polizeiliche Daten ausschließlich ortsbezogen und nicht personenbezogen ausgewertet werden, nicht die beschriebenen Risiken hervorrufen, kann die Bewertung bei nur geringfügigen Änderungen eine ganz andere sein. Die ständig weiterentwickelten technischen Auswertemöglichkeiten bergen schon heute das Potential dafür, dass Bürgerinnen und Bürger die Kontrolle über ihre Daten – in einem Umfang und auf eine Art und Weise – verlieren könnten, die in der Vergangenheit nicht vorstellbar gewesen ist.

Die derzeitigen gesetzlichen Vorschriften in Bund und Ländern enthalten – mit Ausnahme der Regelungen zur Rasterfahndung – keine ausdrücklichen Vorgaben für den Einsatz weit gefasster Analysesysteme. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist angesichts der beschriebenen Gefahren darauf hin, dass der Einsatz solcher Systeme durch die Polizei nur in engen Grenzen als verfassungsrechtlich zulässig zu betrachten ist.

3.1.3 Erlass einer neuen Meldedatenverordnung

Im Berichtszeitraum habe ich zur Neufassung der Verordnung zur Übermittlung von Meldedaten – Meldedatenverordnung kritisch Stellung genommen und Verbesserungen gefordert. Für den Bereich der Polizei regelt die Verordnung – wie auch ihre Vorgängerversion – insbesondere, dass dem Landeskriminalamt bei einer An- und Abmeldung, einem Sterbefall oder einer Namensänderung automatisch und tagesaktuell bestimmte Daten übermittelt werden. Diese Datenübermittlung an das Landeskriminalamt dient dem automatisierten Abgleich mit den polizeilichen Fahndungsdateien nach Art. 43 Abs. 1 Polizeiaufgabengesetz (PAG). Für die Neufassung habe ich zunächst die Aufnahme einer ausdrücklichen Zweckbestimmung für diese Datenübermittlung gefordert. Diese Forderung wurde berücksichtigt. Weiter habe ich gefordert, durch eine spezielle gesetzliche Regelung sicherzustellen, dass die übermittelten Meldedaten zwingend sofort und spurenlos gelöscht werden, sofern der automatisierte Abgleich mit den Fahndungsdateien keinen Treffer ergeben hat. Das Staatsministerium des Innern, für Bau und Verkehr hält eine ausdrückliche gesetzliche Regelung hierzu demgegenüber nicht für erforderlich. Es beruft sich auf die allgemeine Regelung des Art. 45 Abs. 2 Nr. 2 PAG, wonach personenbezogene Daten zu löschen sind, wenn festgestellt wird, dass ihre Kenntnis zur Aufgabenerfüllung nicht mehr erforderlich ist. Weiterhin beruft sich das Staatsministerium des Innern, für Bau und Verkehr darauf, dass die gebotene Löschung bereits jetzt in der entsprechenden Errichtungsanordnung vorgesehen sei. Ich habe demgegenüber an meiner Auffassung festgehalten, zumal die derzeitige Speicherungspraxis dieser Daten zeigt, dass eine klare gesetzliche Regelung sinnvoll wäre. Hierauf sicherte man mir zumindest zu, meinen diesbezüglichen Hinweisen nachzugehen und die betreffende Errichtungsanordnung zu aktualisieren.

3.2 G7-Gipfel

Anfang Juni 2015 fand in Elmau der G7-Gipfel statt. Bereits frühzeitig wurde ich vom Planungsstab der Polizei über die beabsichtigten Maßnahmen informiert. Unter anderem plante die Polizei, die Gegend um Elmau mit stationären Videokameras zu überwachen. Daneben sollten auch mobile Videokameras in Form von Fußtrupps mit Schulterkameras zum Einsatz kommen. Ich überprüfte im Vorfeld des Gipfeltreffens das Videokonzept der Polizei. Meine Anregungen und Bedenken, beispielsweise zur Notwendigkeit etwaiger Hinweisschilder, wurden weitgehend berücksichtigt.

Im Nachgang zum G7-Gipfel kontrollierte ich zudem im Zusammenhang mit dem Gipfeltreffen erstellte Videoaufzeichnungen auf deren Zulässigkeit und Einhaltung der Löschungsfristen. Erforderlich ist für jede Videoüberwachung grundsätzlich eine tragfähige Rechtsgrundlage. Die Besonderheit lag hier darin, dass die Videoaufnahmen – je nach Situation – aufgrund unterschiedlicher Rechtsgrundlagen angefertigt wurden. Neben dem Polizeiaufgabengesetz kamen das Bayerische Versammlungsgesetz, das Ordnungswidrigkeitengesetz sowie – im Falle von Straftaten – die Strafprozessordnung zur Anwendung. Die Rechtsgrundlagen knüpfen je nach Zweck an unterschiedliche Voraussetzungen an und erfordern die Beachtung verschiedentlicher Löschungsfristen, Dokumentations- und Hinweispflichten. Hierbei konnte ich jedoch keine nennenswerten Verstöße gegen die einschlägigen Bestimmungen feststellen.

Im Anschluss an den G7-Gipfel erstellte die Polizei einen Schulungsfilm über die Vorbereitung des Einsatzes und den Einsatzverlauf. Der Schulungsfilm dient in erster Linie der Aus- und Fortbildung von Polizeibeamtinnen und -beamten. Das Videomaterial dazu wurde überwiegend von der Polizei selbst erstellt. Hierbei wirkte ich darauf hin, dass die aufgezeichneten Personen durch Verpixelung unkenntlich gemacht wurden, sofern sie nicht vorab in die Videoaufnahmen eingewilligt hatten. Auch Kfz-Kennzeichen mussten verpixelt werden, da auch über sie ein Personenbezug hergestellt werden kann.

Des Weiteren hatte ich mein Augenmerk auf Speicherungen im Zusammenhang mit den Zuverlässigkeitsüberprüfungen gelegt, die im Vorfeld des G7-Gipfels vom Landeskriminalamt durchgeführt wurden. Alle Beschäftigten externer Dienstleistungsunternehmen, die Sicherheitsbereiche betreten durften, wurden hinsichtlich ihrer Zuverlässigkeit überprüft. Hierfür glich das Landeskriminalamt die vom Landratsamt Garmisch-Partenkirchen übermittelten Beschäftigtendaten mit dem polizeilichen Datenbestand, insbesondere INPOL, ab und teilte das Ergebnis in Form eines Positiv- oder Negativvotums dem Landratsamt mit. Die Speicherung der im Zusammenhang mit der Akkreditierung übermittelten Daten war nur für die Dauer von drei Monaten, in Ausnahmefällen maximal ein Jahr, ab Beendigung des G7-Gipfels vorgesehen. Auf meine Nachfrage im September 2015 teilte mir das Landeskriminalamt mit, dass mittlerweile sämtliche Personendaten in der betreffenden Datenbank gelöscht seien.

Anlässlich des G7-Gipfels setzte die Polizei erstmalig ein so genanntes elektronisches Freiheitsentziehungsbuch ein, da eine größere Zahl an Festnahmen und Ingewahrsamnahmen nicht auszuschließen war. Das elektronische Freiheitsentziehungsbuch ermöglicht es dann, die Abläufe innerhalb einer Gefangenensammelstelle für spätere gerichtliche Überprüfungen präzise zu dokumentieren. Erfasst werden unter anderem die Personalien der Beschuldigten und Betroffenen, der sachbearbeitenden Polizeibeamtinnen und –beamten sowie von Auskunftspersonen. Des Weiteren enthält es Details zum Vorfall, Angaben zur Freiheitsentziehung (Rechtsgrundlage, Dauer, Verpflegung, gerichtliche oder staatsanwaltschaftliche Entscheidung, Entlassung etc.) und zu etwaigen Besuchen. Die Einführung des elektronischen Freiheitsentziehungsbuchs habe ich kritisch begleitet, um eine überschießende Datenspeicherung zu vermeiden. So habe ich darauf hingewiesen, dass etwa Angaben zur Verfassung der Person, zu ärztlichen Untersuchungen, zur Medikamenteneinnahme oder zu vorliegenden Erkrankungen nur erfasst werden dürfen, soweit dies zur ordnungsgemäßen Durchführung des Gewahrsams erforderlich ist. Dies kann zum Beispiel der Fall sein, wenn eine in Gewahrsam genommene Person auf die Einnahme von Medikamenten angewiesen ist.

Darüber hinaus überprüfte ich im Anschluss an den G7-Gipfel die in diesem Zusammenhang getroffenen erkennungsdienstlichen Maßnahmen der Polizei. Hierbei konnte ich keine nennenswerten Mängel feststellen. Erfreulich war zudem, dass sich die Zahlen erkennungsdienstlich behandelter Personen wie auch der insgesamt (vorläufig) Festgenommenen in Grenzen hielten.

Schließlich habe ich mich noch mit der Erfassung der Videokameras von Privatpersonen in der Umgebung des G7-Gipfels durch die Polizei befasst; nähere Einzelheiten hierzu siehe Nr. 3.5.2.

3.3 Polizeiliche Kontrolle von Schmuckankaufstellen

Die Kontrolle seiner An- und Verkaufsbelege hat einen Schmuckhändler dazu veranlasst, mich um die Überprüfung der polizeilichen Vorgehensweise zu bitten. Aus seiner Sicht würden er sowie seine Kundinnen und Kunden dabei unter einen Generalverdacht gestellt. Die Polizei argumentierte hingegen, die Kontrollen dienten unter anderem der Bekämpfung der Eigentumskriminalität. Die Auswahl der in solche Kontrollmaßnahmen einbezogenen Geschäfte ergebe sich anlassbezogen, beispielsweise nach Erkenntnissen aus Ermittlungsverfahren, aus Auswertungen der täglichen Kriminalitätslageberichte oder nach Hinweisen aus der Bevölkerung. Zudem erfolgten die Recherchen grundsätzlich mit Zustimmung der jeweiligen Geschäftsleitung. Eine Datenerhebung gegen deren Willen erfolge nicht.

In der Gesamtbetrachtung halte ich die Auffassung der Polizei, die Aufforderung zur Übergabe von Geschäftsbüchern und Belegen zur Einsichtnahme an die Polizei könne auf Art. 31 Abs. 1 Nr. 1 Polizeiaufgabengesetz (PAG) gestützt werden, für vertretbar. Die Bestimmung erlaubt es der Polizei, personenbezogene Daten über Verantwortliche, Nichtverantwortliche und über „andere Personen“ zu erheben, wenn dies zur Gefahrenabwehr – insbesondere zur vorbeugenden Bekämpfung von Straftaten – „erforderlich“ ist und die Art. 11 bis 48 PAG die Befugnisse der Polizei nicht besonders regeln. Laut Vollzugsbekanntmachung zu Art. 31 Abs. 1 PAG ist eine in diesem Sinne vorgenommene Datenerhebung möglich, „auch wenn nicht oder noch nicht von dem Vorliegen einer im Einzelfall bestehenden (konkreten) Gefahr ausgegangen werden kann.“

Gerade die von der Polizei vorgelegten Fallzahlen und Kontrolltreffer konnten mich davon überzeugen, dass es sich bei den Kontrollen um ein effektives Mittel zur Gefahrenabwehr und zur Verfolgung von Straftaten (Eigentumsdelikte) handelt. Denn immer wieder werden durch diese Überprüfungen rechtmäßige Eigentümerinnen und Eigentümer abhandengekommener Wertgegenstände vor dem endgültigen Verlust der Sachen bewahrt. Gleichwohl habe ich das betroffene Polizeipräsidium darauf aufmerksam gemacht, dass, wenn eine Datenerhebung auf freiwilliger Basis erfolgt, nach Art. 30 Abs. 4 PAG auf die Freiwilligkeit der Auskunft hinzuweisen ist.

3.4 Polizeiliche Beobachtung

Als ein Pkw-Besitzer von der Fahndungsausschreibung seines Fahrzeugs erfuhr, ersuchte er mich um Rat. Auf meine Nachfrage hin erläuterte das ausschreibende Polizeipräsidium den Fall. Hintergrund der Fahndungsausschreibung war die Nutzung des Wagens durch den Sohn des Halters, der sich mutmaßlich in einem extremistischen Umfeld bewegte. Die Polizei wollte mehr über seine Kontakte zu der Szene, aber auch über Treffpunkte sowie Veranstaltungsörtlichkeiten in Erfahrung bringen. Nach polizeilicher Einschätzung lagen in dem Fall die erforderlichen Voraussetzungen für eine polizeilichen Beobachtung im Sinne des Art. 36 Abs. 1 Polizeiaufgabengesetz (PAG) jedoch nicht vor.

Art. 36 PAG Polizeiliche Beobachtung
(1) Die Polizei kann personenbezogene Daten, insbesondere die Personalien einer Person sowie das amtliche Kennzeichen des von ihr benutzten Kraftfahrzeugs, zur polizeilichen Beobachtung ausschreiben, wenn

1. die Gesamtwürdigung der Person und ihrer bisher begangenen Straftaten erwarten lassen, daß sie auch künftig Straftaten von erheblicher Bedeutung begehen wird oder
2. Tatsachen die Annahme rechtfertigen, daß die Person Straftaten von erheblicher Bedeutung begehen wird,
und die polizeiliche Beobachtung zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist.
(2) Im Fall eines Antreffens der Person oder des Kraftfahrzeugs können Erkenntnisse über das Antreffen sowie über Kontakt- und Begleitpersonen und mitgeführte Sachen an die ausschreibende Polizeidienststelle übermittelt werden.
(3) [1]Die Ausschreibung zur polizeilichen Beobachtung darf nur durch eine in Art. 33 Abs. 5 Sätze 1 und 2 genannte Stelle angeordnet werden.[2]Die Anordnung ist auf höchstens ein Jahr zu befristen.[3]Zur Verlängerung der Laufzeit bedarf es einer neuen Anordnung.
(4) Liegen die Voraussetzungen für die Anordnung nicht mehr vor, ist der Zweck der Maßnahme erreicht oder zeigt sich, daß er nicht erreicht werden kann, ist die Ausschreibung zur polizeilichen Beobachtung unverzüglich zu löschen.
(5) [1]Von Maßnahmen nach Abs. 1 sind
1. die Personen zu unterrichten, gegen die die Maßnahme gerichtet war, sowie
2. diejenigen, deren personenbezogene Daten gemeldet worden sind.
[2]Die Unterrichtung erfolgt, sobald dies ohne Gefährdung des Zwecks der Maßnahme oder der eingesetzten nicht offen ermittelnden Beamten geschehen kann.[3]Ist wegen desselben Sachverhalts ein strafrechtliches Ermittlungsverfahren gegen den Betroffenen eingeleitet worden, ist die Unterrichtung in Abstimmung mit der Staatsanwaltschaft nachzuholen, sobald dies der Stand der Ermittlungen zulässt.[4]Erfolgt die Benachrichtigung nicht binnen zwölf Monaten nach Beendigung der Maßnahme, bedarf die weitere Zurückstellung der richterlichen Zustimmung.[5] Art. 34 Abs. 6 Sätze 4 und 5 gelten entsprechend.[6]Die gerichtliche Zuständigkeit und das Verfahren richten sich im Fall des Satzes 3 nach den Regeln der Strafprozessordnung, im Übrigen ist für die richterliche Entscheidung Art. 24 Abs. 1 Satz 3 entsprechend anzuwenden; zuständig ist das Amtsgericht, in dessen Bezirk die ausschreibende Polizeidienststelle ihren Sitz hat.

Gleichwohl entschloss die Polizei sich, das Fahrzeug mit dem Zusatz, die Daten der Insassen bei einer Kontrolle an die zuständige Kriminalpolizeiinspektion zu senden, zur Fahndung auszuschreiben. Als Rechtsgrundlage hierfür zog sie die polizeiliche Generalklausel zur Datenerhebung, Art. 31 Abs. 1 PAG, heran.

Art. 31 PAG Datenerhebung
(1) Die Polizei kann personenbezogene Daten über die in Art. 7, 8 und 10 genannten Personen und über andere Personen erheben, wenn dies erforderlich ist
1. zur Gefahrenabwehr, insbesondere zur vorbeugenden Bekämpfung von Straftaten (Art. 2 Abs. 1),
2. zum Schutz privater Rechte (Art. 2 Abs. 2),
3. zur Vollzugshilfe (Art. 2 Abs. 3) oder
4. zur Erfüllung ihr durch andere Rechtsvorschriften übertragener Aufgaben (Art. 2 Abs. 4)
und die Art. 11 bis 48 die Befugnisse der Polizei nicht besonders regeln.

Betrachtet man die getroffene Maßnahme und deren Zielrichtung, ging es im vorliegenden Fall gerade um die Sammlung von Erkenntnissen (etwa durch Kontrollmitteilungen), die von der ausschreibenden Dienststelle ausgewertet und zu einem punktuellen Bewegungsbild des Fahrzeugnutzers zusammengefasst werden

sollten. Auch Zusammenhänge und Querverbindungen zwischen dem Fahrzeugnutzer und anderen Personen wollte man dabei erkennen. Entsprechend der Vollzugsbekanntmachung zu Art. 36 PAG verfolgt die Maßnahme der polizeilichen Beobachtung eben diese Zielrichtung, polizeiliche Zufallserkenntnisse über das Antreffen einer Person zusammenzutragen. Dabei kann die Polizei auch, wie im vorliegenden Fall, ein genutztes Fahrzeug im Fahndungssystem ausschreiben. Nachdem der Rahmen für diese Maßnahmen in Art. 36 PAG jedoch speziell geregelt ist, kommt ein Rückgriff auf Art. 31 Abs. 1 PAG nicht in Betracht.

Dies habe ich dem betroffenen Polizeipräsidium mitgeteilt. Es bestätigte mir, dass die auf dieser Grundlage getroffenen Ausschreibungen inzwischen gelöscht und die Betroffenen im Sinne des Art. 36 PAG über die Maßnahme unterrichtet wurden.

3.5 Einsatz von Videotechnik

3.5.1 Videoüberwachung durch Zugriff auf Kameras der Verkehrsbetriebe

Ein wiederkehrendes Thema in meinen Tätigkeitsberichten ist die präventive Videoüberwachung durch die Polizei. Ob an Kriminalitätsschwerpunkten oder bei Sport- und Großveranstaltungen, den Rechtsrahmen für solche Maßnahmen bietet in erster Linie Art. 32 Polizeiaufgabengesetz. Dabei ist es zunächst nachrangig, wem die Kamera gehört, mit der die Polizei ihre Videoüberwachung betreibt. Handelt die Polizei als die speichernde Stelle im Sinne des Art. 4 Abs. 9 BayDSG, obliegt ihr ohnehin die datenschutzrechtliche Verantwortung der Maßnahme. Aber auch bei einer Mischnutzung der Anlage muss die Polizei für einen datenschutzkonformen Umgang und für die fristgerechte Löschung ihrer Aufzeichnungen sorgen. Unter Umständen kommt der Polizei dann auch die systemtechnische und organisatorische Verantwortung für die gesamte Anlage zu. Schon bei meiner Überprüfung der polizeilichen Videoüberwachung in Fußballstadien habe ich darauf hingewirkt, eine klare Regelungslage der Nutzungs- und Überlassungsstruktur sowie der Rahmenbedingungen für den Umgang mit den Bilddaten zu schaffen. In diesem Berichtszeitraum trug ich wesentlich dazu bei, dass die Mitbenutzung einzelner Videokameras der Verkehrsbetriebe durch die Polizei neu gestaltet wurde. Die Verträge zwischen dem zuständigen Polizeipräsidium und den städtischen Verkehrsbetrieben enthalten nun alle erforderlichen technischen und organisatorischen Regelungen für den datenschutzkonformen Betrieb des Systems.

3.5.2 Erhebung der Daten nichtpolizeilicher Videokameras anlässlich des G7-Gipfels

Polizei sammelt Daten von Überwachungskameras – so und ähnlich berichteten lokale und überregionale Medien im Vorfeld des G7-Gipfels. Laut Berichterstattung sammelten Kriminalbeamtinnen und -beamte die Daten von Geschäftsleuten in Garmisch-Partenkirchen, die eine eigene Videoüberwachung betrieben. Gerüchte kamen auf, die Polizei habe Geschäftsleute aufgefordert, Kamerabereiche extra so auszurichten, dass Teile des öffentlichen Raumes mitgefilmt werden. Teilweise wurde sogar vermutet, die Polizei wolle auf diese privaten Kameras online zugreifen.

Wie sich bei meiner Überprüfung hingegen herausstellte, war die Polizei im Vorfeld des Großeinsatzes bemüht, ihre sogenannte „Objektdatenbank“ auf den aktuellen Stand zu bringen. In solchen polizeilichen Dateien können gemäß Art. 31 Abs. 2 Polizeiaufgabengesetz neben Daten über die betreffenden Objekte selbst auch Daten zu den Personen und deren Erreichbarkeit aufgenommen werden, die für gefährdete Einrichtungen verantwortlich sind. Vor dem Hintergrund der teilweise erheblichen Ausschreitungen bei ähnlichen Veranstaltungen in der Vergangenheit wurde von der Polizei vorübergehend diese Gefährdungseinschätzung für Gewerbebetriebe im Umfeld der Veranstaltung beziehungsweise der geplanten Versammlungsorte weiter gefasst. Die Begründung der Polizei hierfür erschien mir nachvollziehbar.

Im Fall von Ausschreitungen oder gar Anschlägen hätten so Verantwortliche und Ansprechpartner schneller erreicht und gegebenenfalls Fahndungsmaßnahmen durch Auswertung der privaten Videoaufzeichnungen zügiger eingeleitet werden können. Jedoch habe ich die Polizei frühzeitig darauf hingewiesen, dass – soweit die Betroffenen nicht ohnehin bereits förmlich in ihre Speicherung eingewilligt haben – die Datensätze nach dem G7-Gipfel wieder gelöscht werden müssen. Nach Angabe der Polizei ist dies bereits geschehen.

3.6 Speicherungen in polizeilichen Dateien

Die Polizei unterhält zur Erfüllung ihrer gesetzlichen Aufgaben eine Vielzahl unterschiedlicher Dateien. Von überregionaler Bedeutung ist hierbei das Informationssystem Polizei (INPOL). INPOL ist eine polizeiliche Datenbank, die für Bundes- und Länderpolizeien kriminalpolizeiliche Daten bereithält. Wichtiger Bestandteil von INPOL ist der sogenannte Kriminalaktennachweis (KAN), der Angaben zu erkennungsdienstlichen Behandlungen, Haftdaten, Strafanzeigen und Beschreibungen auffällig gewordener Personen enthält. Ebenso wichtig für die alltägliche Arbeit der Polizei ist das Integrationsverfahren der Bayerischen Polizei (IGVP), welches vor allem der Vorgangsverwaltung beim jeweiligen Polizeiverband dient. Darin sind wesentliche Vorgänge dokumentiert, die bei der polizeilichen Arbeit anfallen. Aufgrund der datenschutzrechtlichen Bedeutung polizeilicher Speicherungen beschäftige ich mich regelmäßig mit diesem Themenbereich.

3.6.1 Prüfung der Speicherungsvoraussetzung „polizeilicher Restverdacht“ – grundlegende Folgerungen aus meiner Prüfung

Im letzten Tätigkeitsbericht habe ich über die Ergebnisse meiner Prüfung der Speicherung in polizeilichen Dateien trotz Verfahrenseinstellung und der Speicherungsvoraussetzung „polizeilicher Restverdacht“ berichtet (siehe 26. Tätigkeitsbericht 2014 unter Nrn. 3.5.3 und 5.3.5). Dort habe ich auch die geltende Rechtslage zur Speicherung personenbezogener Daten nach Art. 38 Abs. 2 Polizeiaufgabengesetz (PAG) dargestellt.

Aus den damaligen Prüfungsergebnissen haben sich für mich, losgelöst von den geprüften Einzelfällen, grundlegende Schlussfolgerungen und Forderungen ergeben. Damit habe ich mich an das Staatsministerium des Innern, für Bau und Verkehr gewandt:

Zunächst habe ich die Regelungslage in den einschlägigen Verwaltungsvorschriften der Polizei kritisiert. Die Verwaltungsvorschriften können so verstanden werden, dass nur in denjenigen Fällen eine Einzelfallprüfung der Fortdauer einer Speicherung durchzuführen wäre, in denen die Staatsanwaltschaft das Verfahren nach § 170 Abs. 2 Strafprozessordnung (StPO) einstellt, weil sich herausstellt, dass Beschuldigte unschuldig sind oder kein begründeter Verdacht mehr gegen sie besteht. In den übrigen Fällen der Einstellung, insbesondere im Regelfall des § 170 Abs. 2 StPO, bei dem schlicht mangels Tatnachweises eingestellt wird, wäre danach eine Einzelfallprüfung hingegen nicht durchzuführen. Dies entspricht jedoch nicht der aktuellen Rechtslage. Eine Einzelfallprüfung der Polizei zur weiteren Speicherung (Bewertung zum Vorliegen eines Restverdachts und zusätzlich Bewertung zur Erforderlichkeit der weiteren Speicherung) ist grundsätzlich in allen Fällen der Einstellung nach § 170 Abs. 2 StPO durchzuführen. Auf eine Einzelfallprüfung zum Restverdacht kann die Polizei allenfalls verzichten, soweit die Einstellung bereits eine ausdrückliche Feststellung zum weiteren Bestehen eines Restverdachts enthält. Eine Einzelfallprüfung und damit eine eigene Bewertung hat die Polizei hingegen zu unterlassen, wenn die Staatsanwaltschaft in ihrer Einstellung ausdrücklich feststellt, dass der Tatverdacht vollständig entfallen ist (etwa weil keine Straftat vorliegt, der oder die Beschuldigte die Tat nicht oder nicht rechtswidrig begangen hat); von dieser Bewertung der Staatsanwaltschaft darf die Polizei nicht von sich aus abweichen. Nichts anderes kann im Übrigen für den Fall eines Freispruchs gelten. Auch der Bayerische Verwaltungsgerichtshof (BayVGH) hat dementsprechend entschieden, dass die Daten im Fall der Feststellung der Staatsanwaltschaft oder des Gerichts über ein vollständiges Entfallen des Verdachts zu löschen sind (Art. 38 Abs. 2 Satz 2 PAG). Eine eigenständige Prüfung der Polizei zum Restverdacht hält der Bayerische Verwaltungsgerichtshof nur in denjenigen Fällen für erforderlich, in welchen bei Einstellung gemäß § 170 Abs. 2 StPO, bei Ablehnung der Eröffnung des Hauptverfahrens oder bei rechtskräftigem Freispruch keine derartige Feststellung der Staatsanwaltschaft oder des Gerichts zum Restverdacht erfolgt (BayVGH vom 1. August 2012 – 10 ZB 11.2438, Rn. 3). Ich habe daher gefordert, die betreffenden Verwaltungsvorschriften der Rechtslage anzupassen. Das Staatsministerium des Innern, für Bau und Verkehr ist dem gefolgt und hat die Verwaltungsvorschrift entsprechend überarbeitet.

Zudem habe ich eine allgemeine Nachfragepflicht der Polizei bei der Staatsanwaltschaft über den Verfahrensausgang nach entsprechenden Zeitabläufen gefordert. Eine solche Nachfragepflicht der Polizei kann verhindern, dass Speicherungen, die aufgrund des abschließenden Ergebnisses des Strafverfahrens unzulässig werden, nur deshalb in den polizeilichen Dateien unverändert weitergespeichert werden, weil die vorgeschriebene Ausgangsmitteilung der Staatsanwaltschaft nicht bei der Polizei eingegangen ist und der Polizei Abschluss und Ausgang des Verfahrens daher noch nicht bekannt sind. Bezüglich dieses Punktes wurde mir eine Prüfung der Umsetzbarkeit zugesagt.

Besonders erfreulich ist des Weiteren, dass mir in Aussicht gestellt wurde, meine Forderung zu prüfen, in den polizeilichen Dateien wie INPOL/KAN und IGVP auch den Ausgang des jeweiligen Strafverfahrens einzutragen (soweit nach Abschluss des Verfahrens von der Zulässigkeit der fortdauernden Speicherung ausgegangen wird). Dies ist derzeit in den Vorschriften der Polizei nicht vorgesehen und wird auch nicht durchgeführt. Für eine sinnvolle und korrekte Nutzung der einzelnen präventiven Speicherungen kann jedoch gerade die Kenntnis auch des Verfahrensausgangs zur jeweiligen Speicherung von erheblicher Bedeutung sein. Schließlich macht es bei der Nutzung der Dateien für alle Betroffenen einen er-

heblichen Unterschied, ob ein Ermittlungsverfahren bei verbleibendem Restverdacht eingestellt wurde oder ob das Verfahren sogar mit einer rechtskräftigen Verurteilung endete. Eine Datei, die personenbezogene Daten aus strafrechtlichen Ermittlungen speichert, jedoch den Ausgang dieser Ermittlungen nicht in der Datei vermerkt, besitzt nur sehr eingeschränkte Aussagekraft.

Wichtig ist mir ferner, dass die Entscheidung, ob ein Restverdacht besteht, nachvollziehbar zu dokumentieren ist. Auch diesbezüglich wurde mir eine Umsetzung zugesagt.

Insgesamt gestützt werde ich in meiner Haltung von der Richtlinie über den Datenschutz der Strafjustiz (RLDSJ, Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI). Diese sieht in Art. 4 Abs. 1 Buchst. d) vor, dass personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein müssen.

3.6.2 Bundesweite Speicherung polizeilicher Daten in PIAV

Wie in meinem 26. Tätigkeitsbericht 2014 erwähnt, planen die Polizeien der Länder und des Bundes seit geraumer Zeit, mit dem neuen Polizeilichen Informations- und Analyseverbund (PIAV) Personen-, Fall- und Sachdaten aus der Kriminalitätsbekämpfung in einem neuen präventiven Dateisystem zusammenzufassen. Seit Bekanntwerden dieser Absicht habe ich mich auf Bundes- und Landesebene für eine datenschutzkonforme Entwicklung des PIAV-Systems eingesetzt. Nicht zuletzt sehe ich in der Neustrukturierung – beispielsweise der bisherigen INPOL-Falldateien – aber auch eine günstige Gelegenheit, schon länger gebotene Nachbesserungen beim Umgang mit personenbezogenen Daten in bundesweiten polizeilichen Verbundsystemen vorzunehmen. Ganz wesentlich scheint dabei, den Betroffenenkreis für solche Speicherungen einzugrenzen.

In der Praxis sieht das übergreifende PIAV-Konzept vor, je Deliktsbereich eine eigene Datei einzurichten, für die jeweils auch eine eigene Errichtungsanordnung zu erstellen ist. Die Bereitstellung der Daten aus den Bundesländern wird dann über sogenannte Quelldateien gewährleistet. In Bayern stellt das Fallbearbeitungssystem EASy mit seinen verschiedenen delikts- beziehungsweise phänomenologisch strukturierten Arbeitsdateien die Basis für die Datenübertragung in das bundesweite Verbundsystem dar. Dementsprechend ist es vorgesehen, die PIAV-Quelldateien in Bayern deckungsgleich zu den PIAV-Zentraldateien beim Bundeskriminalamt aufzugliedern.

Mittlerweile konnte ich mit dem Staatsministerium des Innern, für Bau und Verkehr und mit dem in Dateiangelegenheiten federführendem Landeskriminalamt übereinkommen, bei der Neukonzeption der Quelldateien ein besonderes Augenmerk darauf zu legen, dass bei der Datenspeicherung nicht nur die Bestimmungen des Landesrechts, sondern auch die einschlägigen Vorschriften des Bundeskriminalamtsgesetzes (BKAG) beachtet werden. Dies umfasst insbesondere die in § 8 BKAG vorgegebene negative Prognoseentscheidung, die entsprechend nachvollziehbar dokumentiert werden muss.

§ 8 BKAG Dateien der Zentralstelle

(1) Das Bundeskriminalamt kann zur Erfüllung seiner Aufgaben nach § 2 Abs. 1 bis 3

1. *die Personendaten von Beschuldigten und, soweit erforderlich, andere zur Identifizierung geeignete Merkmale,*
2. *die kriminalaktenführende Polizeidienststelle und die Kriminalaktennummer,*
3. *die Tatzeiten und Tatorte und*
4. *die Tatvorwürfe durch Angabe der gesetzlichen Vorschriften und die nähere Bezeichnung der Straftaten*

in Dateien speichern, verändern und nutzen.

(2) Weitere personenbezogene Daten von Beschuldigten und personenbezogene Daten von Personen, die einer Straftat verdächtig sind, kann das Bundeskriminalamt nur speichern, verändern und nutzen, soweit dies erforderlich ist, weil wegen der Art oder Ausführung der Tat, der Persönlichkeit des Betroffenen oder sonstiger Erkenntnisse Grund zu der Annahme besteht, daß Strafverfahren gegen den Beschuldigten oder Tatverdächtigen zu führen sind.

(3) Wird der Beschuldigte rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens gegen ihn unanfechtbar abgelehnt oder das Verfahren nicht nur vorläufig eingestellt, so ist die Speicherung, Veränderung und Nutzung unzulässig, wenn sich aus den Gründen der Entscheidung ergibt, daß der Betroffene die Tat nicht oder nicht rechtswidrig begangen hat.

(4) Personenbezogene Daten solcher Personen, die bei einer künftigen Strafverfolgung als Zeugen in Betracht kommen oder bei denen Anhaltspunkte bestehen, daß sie Opfer einer künftigen Straftat werden könnten, sowie von Kontakt- und Begleitpersonen der in Absatz 2 bezeichneten Personen, Hinweisgebern und sonstigen Auskunftspersonen können nur gespeichert, verändert und genutzt werden, soweit dies zur Verhütung oder zur Vorsorge für die künftige Verfolgung einer Straftat mit erheblicher Bedeutung erforderlich ist. Die Speicherung nach Satz 1 ist zu beschränken auf die in Absatz 1 Nr. 1 und 2 bezeichneten Daten sowie auf die Angabe, in welcher Eigenschaft der Person und in Bezug auf welchen Sachverhalt die Speicherung der Daten erfolgt. Personenbezogene Daten über Zeugen, mögliche Opfer, Hinweisgeber und sonstige Auskunftspersonen nach Satz 1 dürfen nur mit Einwilligung des Betroffenen gespeichert werden. Die Einwilligung ist nicht erforderlich, wenn das Bekanntwerden der Speicherungsabsicht den mit der Speicherung verfolgten Zweck gefährden würde.

(5) Personenbezogene Daten sonstiger Personen kann das Bundeskriminalamt in Dateien speichern, verändern und nutzen, soweit dies erforderlich ist, weil bestimmte Tatsachen die Annahme rechtfertigen, daß die Betroffenen Straftaten von erheblicher Bedeutung begehen werden.

(6) Das Bundeskriminalamt kann zur Erfüllung seiner Aufgaben nach § 2 Abs. 4 personenbezogene Daten, die bei der Durchführung erkennungsdienstlicher Maßnahmen erhoben worden sind, in Dateien speichern, verändern und nutzen, wenn eine andere Rechtsvorschrift dies erlaubt oder dies erforderlich ist,

1. *weil bei Beschuldigten und Personen, die einer Straftat verdächtig sind, wegen der Art oder Ausführung der Tat, der Persönlichkeit des Betroffenen oder sonstiger Erkenntnisse Grund zu der Annahme besteht, daß gegen ihn Strafverfahren zu führen sind, oder*
2. *zur Abwehr erheblicher Gefahren.*

Absatz 3 gilt entsprechend.

Des Weiteren dürfen aus den PIAV-Quelldateien nur Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung zur Übertragung in den PIAV-Verbund freigegeben werden. Zu beachten ist dabei, dass die PIAV-Relevanz eines Vorganges nicht mit den rechtlichen Voraussetzungen einer Speicherung, insbesondere der oben genannten Negativprognose, gleichgesetzt werden darf.

3.6.3 Speicherung von Lichtbildern

Im vorangegangenen Tätigkeitsbericht habe ich mich ausführlich mit den rechtlichen Hürden bei der Erhebung und Speicherung erkennungsdienstlicher Daten (ED-Daten) befasst. Gewöhnlich erfolgt die Speicherung dieser ED-Daten bei der Bayerischen Polizei in einem Verfahren mit der Bezeichnung Erkennungsdienst Digital (ED-DI). Von dort werden die ED-Daten dann in das INPOL-System übertragen und stehen im Grunde jeder Polizeibeamtin und jedem Polizeibeamten zum Abruf zur Verfügung.

Mit der fortwährenden Entwicklung des Fallbearbeitungssystem EASy eröffnet sich zunehmend die Möglichkeit, Bilder von Betroffenen als Dateianhänge auch in sonstigen polizeilichen Dateien (etwa in PIAV-Quelldateien) recherchierbar vorzuhalten. Aus datenschutzrechtlicher Sicht bedürfen diese Bildspeicherungen einer näheren Betrachtung.

Erfolgen Zuordnungen oder Verknüpfungen der Bilddaten mit sonstigen Personendaten in einer präventiv ausgerichteten Datei, ist dies durchaus mit der allgemeinen Bereithaltung von erkennungsdienstlichen Unterlagen vergleichbar. Die dann zu beachtenden rechtlichen Voraussetzungen sind dabei nicht an ein bestimmtes Dateisystem gebunden. Ob die Voraussetzungen für die Speicherung solcher (erkennungsdienstlicher) Daten gegeben sind, richtet sich nach denselben Kriterien wie die Entscheidung, ob eine erkennungsdienstliche Behandlung angeordnet werden darf.

In meinen Vorbereitungsgesprächen auf Landes- und Bundesebene zum polizeilichen Informations- und Analyseverbund PIAV löste diese Auslegung zunächst Diskussionen aus. Gleichwohl habe ich inzwischen mit dem Landeskriminalamt vereinbart, dass zukünftig bei der Erfassung von Lichtbildern in bayerischen Quelldateien zu PIAV grundsätzlich die rechtlichen Voraussetzungen für eine erkennungsdienstliche Behandlung vorliegen müssen. Dies ist in den entsprechenden Errichtungsanordnungen ausdrücklich vorzusehen.

3.6.4 Löschung von IGVP-Speicherungen

„Keine Volltextsuche in Dateien der Sicherheitsbehörden“ war die Überschrift einer Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Jahr 2010 in Freiburg. Diese Forderung habe ich in der Folge gegenüber dem Staatsministerium des Innern, für Bau und Verkehr immer wieder hervorgehoben, insbesondere als es um die Realisierung der Freitextsuche im Integrationsverfahren der Bayerischen Polizei (IGVP) ging (siehe 24. Tätigkeitsbericht 2010 unter Nr. 3.5.2 und 26. Tätigkeitsbericht 2014 unter Nr. 3.5.2). Meine konkrete Befürchtung war, die Einhaltung von Prüfungs- und Löschungsterminen für die suchfähige Speicherung personenbezogener Daten in Dateien könne

möglicherweise ausgehebelt werden, da diese Löschvorgaben regelmäßig nur bezüglich festgelegter Datenfelder greifen.

Aus diesem Grund ist es wichtig, auf die Nennung von Namen im Freitextfeld „Kurzsachverhalt“ zu verzichten und nur auf die dafür vorgesehenen Datenfelder zu verweisen. Dies wird nach meiner Erfahrung zwar weitgehend beachtet, aber eben nur weitgehend. Auch in diesem Berichtszeitraum wurde ich wieder auf Speicherungen von Klarnamen in IGVP-Kurzsachverhalten aufmerksam. In einem Fall hatte das betreffende Polizeipräsidium gegenüber der betroffenen Person sogar schon die Löschung der Daten schriftlich bestätigt. Trotzdem blieben der Name der Person und weitere Daten im Kurzsachverhalt gespeichert. Von einer tatsächlich vollzogenen Datenlöschung konnte insoweit nicht gesprochen werden. Auf meinen Einwand hin löschte die Polizei die Namensdaten aus dem Kurzsachverhalt umgehend.

3.6.5 Speicherungen im Kriminalaktennachweis trotz fehlenden Restverdachts – Einzelfälle

Grundsätzlich ist es der Polizei nach Art. 38 Abs. 2 Polizeiaufgabengesetz (PAG) erlaubt, personenbezogene Daten auch nach Abschluss eines Strafverfahrens zu speichern soweit dies zur Gefahrenabwehr erforderlich ist. Selbst wenn die Staatsanwaltschaft ein Verfahren einstellt oder ein gerichtlicher Freispruch ergeht, kann die Polizei die erhobenen personenbezogenen Daten weiterhin speichern. Voraussetzung hierfür ist, dass ein Tatverdacht von ausreichender Substanz verbleibt und nicht auszuschließen ist, dass die Datenspeicherung künftig bei der vorbeugenden Straftatenbekämpfung von Nutzen sein könnte (sogenannter Restverdacht). Der für eine weitere Speicherung erforderliche polizeiliche Restverdacht ist von dem hinreichenden Tatverdacht im Sinne der Strafprozessordnung zu unterscheiden. Die Einstellung eines Verfahrens für sich alleine beseitigt den Tatverdacht grundsätzlich nicht. Es gelten für die polizeilichen Dateien im Sinne des Art. 38 PAG im Hinblick auf die Speicherung und Löschung damit andere Voraussetzungen als etwa für die Ermittlungsakten der Staatsanwaltschaft oder Eintragungen im Bundeszentralregister (siehe zu den Voraussetzungen der Restverdachtsspeicherung auch ausführlich 26. Tätigkeitsbericht 2014 unter Nr. 3.5.3; siehe zu meinen grundlegenden Forderungen in diesem Zusammenhang Nr. 3.6.1).

Auch in diesem Berichtszeitraum konnte ich bei meinen Überprüfungen Fälle feststellen, in denen die Polizei im Kriminalaktennachweis Daten von Personen gespeichert hatte, obwohl kein polizeilicher Restverdacht bestand.

So kam beispielsweise in einem Fall der zuständige Polizeiverband aufgrund der von mir angestoßenen Überprüfung selbst zu dem Ergebnis, dass für insgesamt vier Eintragungen zu einer Person keine Notwendigkeit für eine weitere Speicherung dieser Daten im Kriminalaktennachweis bestand. Bei einer weiteren Speicherung war zudem der Ausgang des zugrundeliegenden Verfahrens nicht bekannt. Da eine Beurteilung des Restverdachts somit nicht möglich und nicht begründbar war, mussten auch diese Daten gelöscht werden.

In einem anderen Fall etwa musste ich eine Speicherung wegen Nötigung im Kriminalaktennachweis feststellen, obwohl die zuständige Staatsanwaltschaft der Polizei bereits im Vorfeld ihre Zweifel an der Strafbarkeit des Handelns der Petentin mitgeteilt hatte. Auch in diesem Fall veranlasste der zuständige Polizeiverband

im Rahmen der von mir angestoßenen Überprüfung die Löschung dieser Speicherung.

3.6.6 Reduzierte Dauer bei der Speicherung von Erstkonsumenten „weicher" Drogen

Über die vergangenen Jahre hinweg erreichten mich immer wieder Eingaben von Betroffenen, die als Jugendliche (14 bis 18 Jahre) oder Heranwachsende (18 bis 21 Jahre) wegen eines einmaligen Erwerbs oder Besitzes von Marihuana im Bagatellbereich langfristig im Kriminalaktennachweis der Polizei gespeichert wurden.

Soweit sich in diesen Fällen der Tatverdacht als solcher nicht ausreichend belegen lässt, muss die Polizei die Speicherung im Kriminalaktennachweis sofort löschen.

Aber auch bei nachweisbaren Verstößen empfinde ich die Anwendung der ungekürzten Regelspeicherfrist in diesen Fällen oftmals als zu einschneidend. Das Polizeiaufgabengesetz sieht bei Erwachsenen immerhin eine Regelspeicherungsdauer von zehn Jahren vor. Dabei schildern mir die Betroffenen oft, welche Auswirkungen solche Speicherungen bei Polizeikontrollen noch über Jahre hinweg hervorrufen. Vor diesem Hintergrund habe ich mich wiederholt dafür eingesetzt, bei jugendlichen und heranwachsenden Ersttäterinnen und -tätern, die lediglich eine geringe Menge „weicher" Drogen wie Marihuana für ihren Eigenkonsum erwerben oder besitzen, eine reduzierte Speicherfrist anzusetzen.

Im vergangenen Jahr ist nun ein Polizeipräsidium dieser Bitte gefolgt und hat meine Anregung aufgenommen. Bei jugendlichen und heranwachsenden Ersttäterinnen und -tätern im Zusammenhang mit dem Erwerb und Besitz von sogenannten „weichen" Drogen wird dort nun die Regelspeicherfrist für Speicherungen im Kriminalaktennachweis grundsätzlich auf zwei Jahre reduziert. Ich begrüße diese Entwicklung ausdrücklich und werde mich in den kommenden Jahren dafür einsetzen, dass auch die anderen Polizeipräsidien eine ähnliche Verfahrensweise übernehmen.

3.6.7 Speicherungen in der Falldatei Rauschgift (FDR)

Seit der Einführung der bundesweiten Falldatei Rauschgift (FDR) vor über 30 Jahren entbrennt regelmäßig zwischen Polizei und Datenschutzbehörden eine Diskussion um den zulässigen Umfang des Personenkreises, der in diese Datei aufgenommen werden darf.

Unterschiedliche Meinungen bestehen immer wieder bei der Frage, ob die Polizei zur umfassenden Rauschgift-Lagedarstellung auch Fälle in die FDR aufnehmen darf, die gerade keine erhebliche, länderübergreifende oder internationale Bedeutung haben. Betroffen sind beispielsweise die Daten von erstauffälligen Beschuldigten, die mit einer geringen Menge sogenannter „weicher" Drogen – teilweise auch lediglich für den Eigenkonsum – aufgegriffen werden.

Bereits vor einigen Jahren hatte sich das Bundeskriminalamt nach längeren Verhandlungen der Rechtsauffassung der Datenschutzbeauftragten des Bundes und der Länder angeschlossen und in die Errichtungsanordnung für die Datei ausdrücklich die Einschränkung auf Taten mit erheblicher, länderübergreifender oder

internationaler Bedeutung eingefügt. Anders als in Arbeits- und Ermittlungsdateien, die unter Umständen auch noch unbestätigte Ermittlungserkenntnisse enthalten können, dürfen in die FDR zudem nur sogenannte „gesicherte" Daten einfließen. Die Datengrundlage der FDR soll hierdurch den beteiligten Behörden die Erstellung von belastbaren Statistiken und Analysen ermöglichen, in Einzelfällen aber auch den Rückgriff auf täterbezogene Auskünfte im Bereich der Betäubungsmittelkriminalität erlauben.

Wie sich nun bei einer gemeinsamen Prüfung der Bundes- und der Landesbeauftragten für den Datenschutz zeigte, gelangen trotz der oben genannten Vorgaben und der erfolgten Klarstellung in der Errichtungsanordnung weiterhin Sachverhalte in die Datei, die den festgelegten Kriterien nicht entsprechen. So konnte ich bei der Durchsicht der ausgewählten Prüffälle zahlreiche Speicherungen entdecken, bei denen sich kein ausreichender Tatverdacht belegen lässt oder die eben gerade keinen erheblichen, länderübergreifenden oder internationalen Bezug haben. Die fraglichen Fälle wurden nach Auskunft der Polizei inzwischen gelöscht.

Von Beginn an positiv stellte sich bei meiner Prüfung die konstruktive Zusammenarbeit mit dem Landeskriminalamt dar. Auch wenn dort, nach der bisherigen Interpretation der Errichtungsanordnung, zur Erstellung eines umfassenden und überregionalen Rauschgiftlagebildes sämtliche Rauschgiftmeldungen der Polizeipräsidien in der FDR erfasst wurden, wird diese Verfahrensweise durch das Landeskriminalamt nunmehr neu bewertet.

Mit der Einführung des „Polizeilichen Informations- und Analyseverbundes (PIAV)" sowie der damit einhergehenden Umstellung des kriminalpolizeilichen Meldedienstes Rauschgift scheint eine Erfassung von Personendaten unter einer festgelegten Relevanzschwelle nicht mehr erforderlich. Derzeit erarbeitet eine Bund-Länder-Arbeitsgruppe unter Mitwirkung Bayerns entsprechende Regelungen. Wie mir das Landeskriminalamt dazu versicherte, ist die Umsetzung der datenschutzrechtlichen Vorgaben ein wesentliches Ziel dieser Arbeitsgruppe.

Im Rahmen der 92. Konferenz haben sich die Datenschutzbeauftragten des Bundes und der Länder am 9./10. November 2016 mit dieser Thematik befasst und gemeinsam folgende Entschließung verabschiedet:

Entschließung der 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 10.11.2016

Gemeinsame Prüfung der Falldatei Rauschgift deckt gravierende Mängel auf Konsequenzen für polizeiliche Datenverarbeitung notwendig

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

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

Datenschutzbeauftragten haben im Rahmen ihrer Kontrollen sowohl die Struktur der Datei als auch Einzelspeicherungen überprüft.

Die Prüfung hat im Wesentlichen folgende Mängel aufgedeckt:

- *Vielfach haben die Behörden nicht ausreichend geprüft, ob die Voraussetzungen des § 2 BKAG (Straftat von länderübergreifender oder erheblicher Bedeutung) und des § 8 Abs. 2 BKAG (Negativprognose) vorliegen.*

- *Verbreitet fehlt es an einer nachvollziehbaren Dokumentation des Vorliegens der gesetzlichen Speicherungsvoraussetzungen.*

- *Dementsprechend fanden sich in der bundesweit abrufbaren Datei vielfach Speicherungen, die dem Bereich der Bagatellkriminalität zuzuordnen sind. Auch wurden Personen gespeichert, bei denen kein hinreichender polizeilicher Restverdacht festzustellen war.*

- *Das Ergebnis des jeweiligen Strafverfahrens war bei vielen Einträgen nicht berücksichtigt – entweder aufgrund organisatorischer Mängel oder weil die nach § 482 Absatz 2 Strafprozessordnung (StPO) notwendige Mitteilung der Staatsanwaltschaft unterblieb.*

Die Ergebnisse machen deutlich:

1. *Es ist wichtig, die konkrete Zwecksetzung jeder Datei in einer Errichtungsanordnung festzulegen. Die Voraussetzungen, wann welche Daten für den jeweiligen Zweck erforderlich sind und welcher Personenkreis erfasst werden darf, müssen genau definiert werden.*
2. *Bagatellfälle in Verbunddateien zu speichern, ist auch im Hinblick auf die bundesweite Abrufbarkeit der Daten unverhältnismäßig.*
3. *In der Praxis ist sicherzustellen, dass in Verbunddateien alle Speichervoraussetzungen, vor allem die Negativprognose, durchgehend und gründlich bezogen auf den jeweiligen Einzelfall dokumentiert werden.*

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

3.6.8 Prüfung erkennungsdienstlicher Maßnahmen

Einen besonderen Stellenwert bei meinen datenschutzrechtlichen Überprüfungen nehmen immer wieder die erkennungsdienstlichen Maßnahmen der Polizei ein. Auch in diesem Berichtszeitraum konnte ich bei meinen Überprüfungen erkennungsdienstliche Maßnahmen feststellen, die nicht den erforderlichen Vorgaben entsprachen und die daher gelöscht werden mussten. Zu den Voraussetzungen im Allgemeinen darf ich auf meine zurückliegenden Tätigkeitsberichte verweisen (siehe 25. Tätigkeitsbericht 2012 unter Nr. 3.5.5 sowie 26. Tätigkeitsbericht

2014 unter Nr. 3.5.4). Im Folgenden schildere ich zwei Beispielsfälle aus meiner Prüfpraxis:

In einem Fall behandelte die Polizei eine Person erkennungsdienstlich, nachdem sie in einem Supermarkt Süßigkeiten im Wert von 7,76 Euro gestohlen hatte. Zwar war sie bereits wenige Monate zuvor in eine wechselseitige Körperverletzung verwickelt. Bei diesem Sachverhalt konnte aber bis zuletzt nicht nachvollzogen werden, wer die Auseinandersetzung tatsächlich begonnen hatte. In der Gesamtbetrachtung folgte das zuständige Polizeipräsidium dann auch ohne Widerspruch meiner Auffassung, dass in diesem Fall eine erkennungsdienstliche Behandlung zur künftigen Aufklärung von Straftaten nicht erforderlich war.

Bei einem weiteren Fall war nach Auffassung der Staatsanwaltschaft schon der Straftatbestand als solcher entfallen. In der Einstellungsverfügung kam sie daher zu dem Ergebnis, dass keine Bedrohung stattgefunden habe. Auch andere Straftatbestände sah die Staatsanwaltschaft als nicht erfüllt an. Das zuständige Polizeipräsidium veranlasste daher nach meinem Einwand die Löschung der erkennungsdienstlichen Unterlagen sowie der Speicherung im Kriminalaktennachweis.

3.7 Anfertigen einer Personalausweiskopie durch die Polizei

Eine Petentin wandte sich an mich, nachdem ihr Personalausweis von einem Ladendetektiv und der Polizei kopiert worden war. Sie teilte mir mit, dass sie eines Ladendiebstahls verdächtigt worden sei und sich daraufhin mit ihrem Personalausweis habe ausweisen müssen. Zusätzlich seien jedoch auch noch Kopien von ihrem Ausweis gefertigt worden.

Ich habe der Petentin die strengen Maßstäbe, die für die Anfertigung von Personalausweiskopien gelten, dargelegt. Die Rechtslage stellt sich hierzu folgendermaßen dar: Nach dem Personalausweisgesetz (PAuswG) ist insbesondere zu prüfen, ob nicht bereits die Vorlage des Ausweises an sich und gegebenenfalls die Anfertigung eines entsprechenden Vermerks über die Personalien ausreichend ist. Die Erforderlichkeit der Ausweiskopie wird – abgesehen von gesetzlichen Sonderregelungen wie etwa § 64 Abs. 1 Nr. 2 Fahrerlaubnis-Verordnung oder § 8 Abs. 1 Satz 3 Geldwäschegesetz – bei einer Identifizierung unter Anwesenden in der Regel nicht vorliegen. Auch wenn die Notwendigkeit der Vervielfältigung gegeben sein sollte, ist weiter insbesondere darauf zu achten, dass dem Betroffenen ermöglicht wird, diejenigen Daten zu schwärzen, die nicht zur Identifizierung benötigt werden. Letzteres gilt insbesondere für die Zugangs- und Seriennummer des Personalausweises. Zudem sind die Kopien regelmäßig unverzüglich zu vernichten, sobald der mit der Kopie verfolgte Zweck der Identitätsfeststellung erreicht ist (siehe zum Anfertigen von Personalausweiskopien auch 26. Tätigkeitsbericht 2014 unter Nrn. 2.1.5 und 3.7).

Die Petentin hatte bereits vor ihrer Eingabe die betreffende Polizeiinspektion um Vernichtung der Ausweiskopie gebeten. Noch ehe ich mich in dieser Angelegenheit an das zuständige Polizeipräsidium wenden konnte, informierte mich die Petentin darüber, dass ihre Ausweiskopie von der Polizei zwischenzeitlich vernichtet worden sei. Zudem habe ihr der stellvertretende Polizeiinspektionsleiter mitgeteilt, dass er den Supermarkt zur Herausgabe der dort verbliebenen weiteren Ausweiskopie aufgefordert habe.

Positiv hervorzuheben ist in diesem Fall, dass die Polizei von sich aus gegenüber der Petentin den Fehler umgehend eingeräumt und beseitigt hat.

3.8 Datenübermittlungen

3.8.1 Weitergabe von Zeugendaten bei einem Verkehrsunfall

Kurze Zeit nachdem ein Bürger sich als Zeuge eines Verkehrsunfalles, an dem er nicht beteiligt war, der Polizei zur Verfügung gestellt hatte, bekam er auf seinem Handy einen Anruf des Unfallverursachers. An die Telefonnummer war der Unfallverursacher über eine von der Polizei ausgefüllte Personalienaustauschkarte gelangt, die auch die Daten und die Telefonnummer des Zeugen enthielt. Wenig begeistert über die Weitergabe seiner privaten Handynummer, bat mich der Zeuge um eine datenschutzrechtliche Abklärung des Sachverhalts. Ich habe mich daher an das betreffende Polizeipräsidium gewandt und mir zu der Verfahrensweise in diesem Fall berichten lassen.

Grundsätzlich erachte ich es als zulässig, wenn die Polizei als Serviceleistung den Personalienaustausch nach einem Verkehrsunfall unterstützt und dabei die Daten der Unfallbeteiligten untereinander weitergibt. Sie unterstützt dabei letztlich nur die rechtliche Verpflichtung der Unfallbeteiligten, selbst nach § 34 Straßenverkehrsordnung anderen am Unfallort anwesenden Beteiligten und Geschädigten gegenüber den eigenen Namen und die eigene Anschrift anzugeben (siehe auch § 142 Strafgesetzbuch). Insoweit wird sich gegen die Befugnis der polizeilichen Datenübermittlung nach Art. 41 Abs. 2 Nr. 1 Polizeiaufgabengesetz im Regelfall auch kein schutzwürdiges Interesse eines Unfallbeteiligten am Ausschluss der Übermittlung seiner Daten herleiten lassen. Zu beachten ist jedoch, dass sich dieser Personenkreis in der Regel auf die Unfallbeteiligten beschränkt. Folgt man der Definition aus § 142 Strafgesetzbuch, so ist Unfallbeteiligter jeder, dessen Verhalten nach den Umständen zur Verursachung des Unfalls beigetragen haben kann. Ein Zeuge kann zu diesem Personenkreis zunächst nicht zugerechnet werden.

Im oben genannten Fall hat das betreffende Polizeipräsidium dann auch festgestellt, dass die Polizeistreife vor der Weitergabe der Zeugendaten zunächst dessen Einverständnis hätte einholen müssen. Im vorliegenden Fall unterblieb dies. Die Polizei nahm den Vorfall daher zum Anlass, die Personalienaustauschkarte, die sie in solchen Fällen verwendet, zu ergänzen und darin auf die entsprechenden datenschutzrechtlichen Vorgaben hinzuweisen. Die Änderung wird derzeit noch mit den anderen Polizeiverbänden und dem Staatsministerium des Innern, für Bau und Verkehr abgestimmt. Zu Redaktionsschluss lag mir noch kein Entwurf für die angepasste Personalienaustauschkarte vor.

3.8.2 Datenübermittlungen an Fahrerlaubnisbehörden

Um den Fahrerlaubnisbehörden die Überprüfung hinsichtlich der Nichteignung oder Nichtbefähigung zum Führen von Kraftfahrzeugen zu ermöglichen, hat die Polizei den Fahrerlaubnisbehörden ihr bekannt gewordene Informationen über Tatsachen zu übermitteln, die auf nicht nur vorübergehende Mängel hinsichtlich der Eignung oder auf Mängel hinsichtlich der Befähigung einer Person zum Führen von Kraftfahrzeugen schließen lassen. Diese Verpflichtung findet ihre gesetzliche Grundlage in § 2 Abs. 12 Satz 1 Straßenverkehrsgesetz (StVG).

§ 2 StVG Fahrerlaubnis und Führerschein
(12) Die Polizei hat Informationen über Tatsachen, die auf nicht nur vorübergehende Mängel hinsichtlich der Eignung oder auf Mängel hinsichtlich der Befähigung einer Person zum Führen von Kraftfahrzeugen schließen lassen, den Fahrerlaubnisbehörden zu übermitteln, soweit dies für die Überprüfung der Eignung oder Befähigung aus der Sicht der übermittelnden Stelle erforderlich ist. Soweit die mitgeteilten Informationen für die Beurteilung der Eignung oder Befähigung nicht erforderlich sind, sind die Unterlagen unverzüglich zu vernichten.

Meine datenschutzrechtliche Prüfung polizeilicher Mitteilungen an Fahrerlaubnisbehörden ergab keine Hinweise auf wesentliche datenschutzrechtliche Verstöße der Polizei. Die geprüften Behörden orientierten sich regelmäßig an einem – im Grundsatz die Rechtslage zutreffend würdigenden – Rundschreiben des Innenministeriums (IMS) aus dem Jahr 2001. Gleichwohl nutzte ich die Gelegenheit, beim Staatsministerium des Innern, für Bau und Verkehr eine Aktualisierung dieses Rundschreibens anzustoßen. Hierbei konnte ich erfreulicherweise einige datenschutzrechtliche Verbesserungen erreichen: So wurde etwa eine Empfehlung aufgenommen, in Zweifelsfällen vor einer Datenübermittlung den Sachverhalt zunächst in anonymisierter Form mit der Fahrerlaubnisbehörde zu klären. Auch wird künftig darauf hingewiesen, dass die gelegentliche Einnahme von Cannabis alleine noch nicht die Annahme von Eignungszweifeln rechtfertigt, sondern noch weitere Umstände (zum Beispiel kein Trennen zwischen Konsum und Fahren) hinzukommen müssen. Ähnliches gilt bei Straftaten, die im Zusammenhang mit dem Straßenverkehr und der Kraftfahreignung stehen. Auch diesbezüglich wird nunmehr klargestellt, dass in jedem Einzelfall zu prüfen ist, ob Tatsachen vorliegen, die den Verdacht auf einen Mangel im Sinne von § 2 Abs. 12 StVG rechtfertigen.

Hinsichtlich der Speicherung der von der Polizei übermittelten Daten bei den Fahrerlaubnisbehörden darf ich auf Nr. 13.7 verweisen.

3.8.3 Prüfung des Gemeinsamen Terrorismusabwehrzentrums (GTAZ)

Im Rahmen einer datenschutzrechtlichen Prüfung des Gemeinsamen Terrorismusabwehrzentrums (GTAZ) habe ich unter anderem die Datenübermittlungen der meiner Kontrollkompetenz unterliegenden bayerischen Behörden – dies sind das Landeskriminalamt und das Landesamt für Verfassungsschutz – näher untersucht.

Hintergründe zum GTAZ sowie das Ergebnis meiner Prüfung sind unter Nr. 4.4.1 zu finden.

3.9 Ermittlungen in sozialen Netzwerken

Für polizeiliche Ermittlungen in sozialen Netzwerken hat das Staatsministerium des Innern, für Bau und Verkehr einen Leitfaden für die Polizeibehörden entwickelt. Zu diesem Leitfaden habe ich im Berichtszeitraum wiederholt kritisch Stellung bezogen. Das Innenministerium hat einige meiner Hinweise aufgegriffen und diverse Ausführungen im Leitfaden ergänzt beziehungsweise präzisiert.

Eine sehr grundrechtssensible Form der Ermittlung in sozialen Netzwerken ist die verdeckte polizeiliche Kommunikation im nicht-öffentlichen Bereich, also in ge-

schlossenen Benutzergruppen. Dabei nimmt die Polizei heimlich, etwa unter Verwendung eines Ermittlungsaccounts, an der Kommunikation innerhalb einer Gruppe teil, die die Erteilung einer Zugangsberechtigung, die Bestätigung einer Freundschaftsanfrage oder ähnliches voraussetzt. Hier konnte ich mich mit meiner Forderung nicht durchsetzen, diesen heimlichen Eingriff aufgrund seiner Intensität in jedem Fall den Regelungen über den Einsatz eines verdeckten Ermittlers (§ 110a Strafprozessordnung beziehungsweise Art. 33 Polizeiaufgabengesetz) zu unterstellen statt in gewissen Fallgestaltungen lediglich die gesetzlichen Ermittlungsgeneralklauseln als Rechtsgrundlage ausreichen zu lassen. Die Anwendung der Vorschriften über verdeckte Ermittler hätte den Vorteil, dass besondere grundrechtssichernde Verfahrensregelungen, wie etwa die nachträgliche Benachrichtigungspflicht der Betroffenen, gelten.

3.10 Auskunftsersuchen

3.10.1 Rücksendung von Ausweiskopien

Im 26. Tätigkeitsbericht 2014 unter Nr. 3.7 habe ich mich mit dem Thema „Ausweiskopien zum Identitätsnachweis bei Auskunftsersuchen“ befasst. In diesem Berichtszeitraum hat sich nun ein Bürger an mich gewandt und hinterfragt, was bei der Polizei mit seiner Ausweiskopie, die er als Identitätsnachweis an die Polizei senden sollte, geschehe. Er erhielt von dem betroffenen Polizeipräsidium die Antwort, dass seine Ausweiskopie dort aufbewahrt und frühestens nach fünf Jahren vernichtet werde.

An der Zweckmäßigkeit einer so langen Aufbewahrung habe ich große Zweifel und teilte dies der Behörde mit. Wie bereits in meinem letzten Tätigkeitsbericht erläutert, halte ich die Einforderung einer Ausweiskopie zum Zwecke der Identitätsfeststellung zwar nicht grundsätzlich für unzulässig. Ihre längere Aufbewahrung ist jedoch nicht notwendig. Schließlich muss die Behörde auch darauf achten, dass ihre Verfahrensweise nicht als Hemmnis für einen Auskunftsantrag gesehen wird. Eine überlange Aufbewahrung der Ausweiskopie könnte von vielen Auskunftssuchenden sicherlich negativ aufgefasst werden. Ich habe daher das Polizeipräsidium gebeten, seine diesbezügliche Verfahrensweise zu überdenken und anzupassen.

Mit dem Ergebnis bin ich sehr zufrieden. So sollen bei dem Polizeipräsidium zukünftig Ausweiskopien, die für einen Identitätsnachweis übersandt werden, mit den Auskunftsschreiben an die Betroffenen zurückgesandt werden. Ausweiskopien, die aus zurückliegenden Anträgen noch vorliegen, wurden zudem bereits vernichtet. Diese Regelung scheint insgesamt eine sinnvolle und datenschutzfreundliche Ergänzung zu dem bislang bereits praktizierten Verfahren.

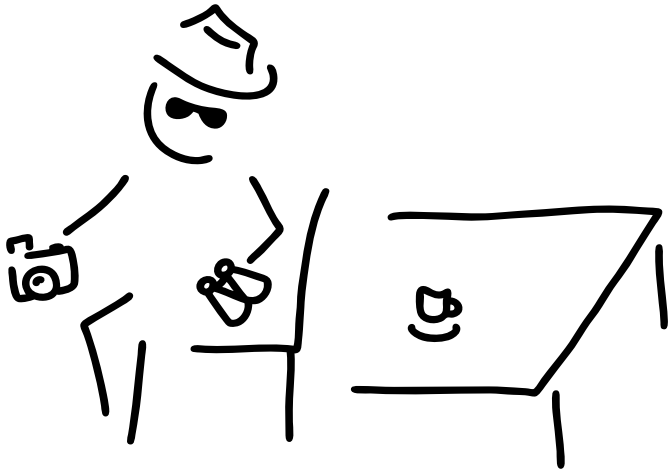
3.10.2 Bearbeitungsdauer von Auskunfts- und Löschanträgen

Regelmäßig wenden sich Bürgerinnen und Bürger an mich, da ihnen die Bearbeitungsdauer ihrer Auskunfts- und Löschungsanträge zu lange erscheint. Dies habe ich zum Anlass genommen, die Verfahrenspraxis des Landeskriminalamts hinsichtlich der Bearbeitungsdauer von Auskunfts- und Löschungsanträgen von Amts wegen datenschutzrechtlich zu überprüfen.

Im Ergebnis konnte ich feststellen, dass die Polizei bereits unterschiedliche strukturelle und organisatorische Maßnahmen ergriffen beziehungsweise angeregt hat, um die Bearbeitungsdauer von Auskunfts- und Löschungsanträgen zu verbessern. Dies kann ich aus datenschutzrechtlicher Sicht nur begrüßen. Ob diese Maßnahmen tatsächlich zu einer Verbesserung führen, wird die weitere Entwicklung zeigen.

Gleichwohl habe ich dem Landeskriminalamt mitgeteilt, dass die Bearbeitung sowohl von Auskunfts- als auch von Löschungsanträgen in der Regel nicht länger als drei Monate dauern darf. Maßgeblich hierfür ist zum einen die allgemeine Entscheidung des Gesetzgebers, nach drei Monaten grundsätzlich den Weg für eine Untätigkeitsklage zu öffnen (siehe § 75 Verwaltungsgerichtsordnung). Zum anderen sieht die Richtlinie über den Datenschutz der Strafjustiz (RL 2016/680/EU) im Speziellen vor, dass derartige Anträge grundsätzlich unverzüglich zu beantworten sind (siehe Erwägungsgrund 40 RL 2016/680/EU).

4 Verfassungsschutz



4.1 Novellierung des Bayerischen Verfassungsschutzgesetzes (BayVSG)

Im Berichtszeitraum wurde das Bayerische Verfassungsschutzgesetz umfassend reformiert. Das neue Bayerische Verfassungsschutzgesetz wurde am 7. Juli 2016 vom Landtag verabschiedet und ist am 1. August 2016 in Kraft getreten. Grund für die Novellierung war unter anderem das Urteil des Bundesverfassungsgerichts vom 24. April 2013 (BVerfGE 133, 277) zum Antiterrordateigesetz (ATDG), das der Informationsübermittlung zwischen den Verfassungsschutzbehörden und der Polizei enge Grenzen gesetzt hat (siehe zu den Folgen aus dem ATDG-Urteil bereits 26. Tätigkeitsbericht 2014 unter Nr. 4.2.1). Zudem ist am 21. November 2015 das Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes in Kraft getreten, in welchem erstmals der Einsatz von Verdeckten Mitarbeitern und Vertrauensleuten im Bereich des Verfassungsschutzes geregelt wird. Ausweislich der Gesetzesbegründung sollten zudem die Ergebnisse der Bund-Länder-Kommission „Rechtsterrorismus“ (Bundestags-Drucksache 17/14600) und des NSU-Untersuchungsausschusses des Bayerischen Landtags (Landtags-Drucksache 16/17740) im neuen Bayerischen Verfassungsschutzgesetz berücksichtigt werden.

Die Staatsregierung hat den Reformbedarf schließlich zum Anlass genommen, das Bayerische Verfassungsschutzgesetz grundlegend zu novellieren. Im Zuge dessen wurde auch erstmalig die Möglichkeit des Abrufs von gespeicherten Verkehrsdaten („Vorratsdatenspeicherung“) durch das Landesamt für Verfassungsschutz geschaffen.

Bereits frühzeitig wurde ich vom Staatsministerium des Innern, für Bau und Verkehr über das Reformvorhaben informiert. Ich erhielt Gelegenheit, zum Gesetzentwurf (Landtags-Drucksache 17/10014) ausführlich Stellung zu beziehen. Mein Hauptaugenmerk lag hierbei auf den datenschutzrechtlichen Defiziten, die

die Novellierung mit sich bringt. Im Vergleich zur bisherigen Fassung enthält das neue Bayerische Verfassungsschutzgesetz einige erhebliche Verschlechterungen.

Insbesondere folgende Punkte sehe ich sehr kritisch:

— Bei den grundrechtssichernden Verfahrensvorschriften ist eine generelle Absenkung des Schutzniveaus zu verzeichnen. So regelt das novellierte Bayerische Verfassungsschutzgesetz etwa das Abhören und Aufzeichnen des außerhalb von Wohnungen gesprochenen Wortes (Art. 6d BayVSG a.F.) nicht mehr, obwohl diese Maßnahme sehr eingriffsintensiv ist. Insbesondere entfallen dadurch die besonderen Verfahrensvorschriften des Art. 6f Abs. 4 BayVSG a.F. (zum Beispiel Schutz von Berufsgeheimnisträgern). Zudem begegnet es verfassungsrechtlichen Bedenken, dass die nachrichtendienstlichen Mittel lediglich in einer Dienstvorschrift und nicht im Gesetz selbst aufgeführt sind. Art. 7 Abs. 2 Satz 1 BayVSG-E (jetzt Art. 8 Satz 1 BayVSG) genügt damit nach meiner Auffassung den vom Bundesverfassungsgericht aufgestellten Anforderungen an die Grundsätze der Normenbestimmtheit und Normenklarheit nicht.

— Für den Abruf der nach § 113b Telekommunikationsgesetz gespeicherten Verkehrsdaten („Vorratsdatenspeicherung“) ist der Schutz der Berufsgeheimnisträger zu verbessern und die Abrufbefugnis entsprechend den Vorgaben des Bundesverfassungsgerichts aus dem Urteil zur Vorratsdatenspeicherung vom 2. März 2010 (BVerfGE 125, 260) verfassungskonform auszugestalten (Art. 13 Abs. 3 BayVSG-E, jetzt Art. 15 Abs. 3 BayVSG). Nach meiner Einschätzung wird die Regelung derzeit den vom Bundesverfassungsgericht festgestellten verfassungsrechtlichen Anforderungen ebenfalls nicht gerecht.

— Für den neu geregelten Einsatz von Verdeckten Mitarbeitern und Vertrauensleuten (Art. 16, 17 BayVSG-E, jetzt Art. 18, 19 BayVSG) fehlen grundrechtssichernde Verfahrensvorschriften (etwa hinsichtlich des Kernbereichsschutzes und der Benachrichtigungspflicht), obwohl es sich um eingriffsintensive verdeckte Maßnahmen handelt.

— Die Novellierung des Bayerischen Verfassungsschutzgesetzes darf den Schutz von Minderjährigen nicht herabsetzen (Art. 5 Abs. 1 Satz 4 BayVSG und Art. 19 Abs. 1 Satz 3 BayVSG-E, jetzt Art. 21 Abs. 1 Satz 3 BayVSG). Eine Absenkung des Schutzniveaus an dieser Stelle sehe ich äußerst kritisch, weil gerade Minderjährige in ihrer Persönlichkeit noch nicht ausgereift sind und die Tragweite ihrer Handlungen altersbedingt regelmäßig nicht überblicken können.

— Die unverhältnismäßig lange Löschfrist des Art. 19 Abs. 1 Satz 1 Nr. 3 BayVSG-E (jetzt Art. 21 Abs. 1 Satz 1 Nr. 3 BayVSG) von 15 Jahren ist angesichts der Regelungslage auf Bundesebene nicht nachvollziehbar. Auch das Bundesverfassungsschutzgesetz geht in § 12 Abs. 3 von nur zehn Jahren aus.

— Bei den Datenübermittlungsvorschriften sind die Vorgaben des Bundesverfassungsgerichts aus dem ATDG-Urteil vom 24. April 2013 (BVerfGE 133, 277) nicht vollständig umgesetzt (siehe Art. 22, 23 BayVSG-E,

jetzt Art. 24, 25 BayVSG). Insbesondere wird dem so genannten informationellen Trennungsprinzip zwischen den Verfassungsschutz- und Polizeibehörden nicht ausreichend Rechnung getragen.

— Die Novellierung des Bayerischen Verfassungsschutzgesetzes darf die Kontrollmöglichkeiten durch staatliche Stellen nicht einschränken. Die bestehenden Kontrollrechte des Parlamentarischen Kontrollgremiums werden jedoch teilweise reduziert (Art. 18 BayVSG-E, jetzt Art. 20 BayVSG).

Im Rahmen der Ressortanhörung konnte ich aber auch einige datenschutzrechtliche Verbesserungen bewirken. Unter anderem konnte ich erreichen, dass der Aufgabenbereich des Landesamts für Verfassungsschutz in Art. 3 Satz 2 BayVSG ausdrücklich auf die Beobachtung von Bestrebungen und Tätigkeiten Organisierter Kriminalität „zum Schutz der verfassungsmäßigen Ordnung" beschränkt wird. Damit wird dem informationellen Trennungsprinzip eher Rechnung getragen und der Beobachtungsauftrag des Verfassungsschutzes zugunsten der klassischen Aufgaben eingegrenzt. Zudem konnte ich hinsichtlich des Auskunftsanspruchs nach Art. 21 BayVSG-E (jetzt Art. 23 BayVSG) durchsetzen, dass in der Gesetzesbegründung festgelegt wird, dass das Landesamt für Verfassungsschutz zumindest zur ermessensgerechten Entscheidung über die Auskunftserteilung verpflichtet ist, wenn der Auskunftsantrag unzureichend begründet ist (siehe Landtags-Drucksache 16/17740, S. 47).

Meine ausführliche Stellungnahme zur BayVSG-Novelle ist auf meiner Homepage https://www.datenschutz-bayern.de eingestellt und ist auch auf der Internetseite des Landtags (https://www.bayern.landtag.de/dokumente) unter „Protokolle" abrufbar.

In diesem Zusammenhang möchte ich zudem auf die Entschließung der 90. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 30. September/1. Oktober 2015 zum bereits oben erwähnten Gesetz zur Verbesserung der Zusammenarbeit im Bereich des Verfassungsschutzes verweisen. In dieser Entschließung lehnt die Konferenz die vom Bundesgesetzgeber verabschiedete Reform des Verfassungsschutzes ab, weil sie mit der föderalen Ordnung der Bundesrepublik nicht vereinbar ist und die Grundrechte der Bürgerinnen und Bürger bedroht:

Entschließung der 90. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 30.09./01.10.2015

Verfassungsschutzreform bedroht die Grundrechte

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

Das Gesetz sieht u. a. vor, Aufgaben und Informationen beim Bundesamt für Verfassungsschutz zu zentralisieren. Es erweitert die Verpflichtungen der Verfassungsschutzbehörden, Daten untereinander auszutauschen, erheblich. Zudem er-

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

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

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

4.2 Dokumentenmanagementsystem beim Landesamt für Verfassungsschutz

Nachdem bei der Einführung einer neuen Dokumentenmanagementsoftware beim Landesamt für Verfassungsschutz keine spezifischen Regularien zur Aussonderung des elektronisch vorgehaltenen Aktenbestandes getroffen wurden, war eine meiner zentralen Forderungen an das Landesamt für Verfassungsschutz, für das neue System ein abgestuftes Löschkonzept zu erstellen. Das Landesamt für Verfassungsschutz ist meiner Argumentation gefolgt und hat inzwischen einen Entwurf für eine Errichtungsanordnung vorgelegt, der meine Forderungen weitgehend berücksichtigt. Gerade für einfach gelagerten Schriftverkehr mit Bürgerinnen und Bürgern oder mit anderen Behörden sind darin nunmehr wesentlich kürzere Aufbewahrungszeiten als bislang vorgesehen. Weiterhin wurde in dem System nun die Möglichkeit implementiert, unzulässige Datenspeicherungen durch den behördlichen Datenschutzbeauftragten unverzüglich löschen zu lassen.

4.3 Löschmoratorien zur Unterstützung von parlamentarischen Untersuchungsausschüssen

Im Rahmen der Tätigkeit des Untersuchungsausschusses „Rechtsterrorismus in Bayern – NSU“ des Bayerischen Landtags hatte der Vorsitzende das Staatsministerium des Innern, für Bau und Verkehr gebeten, dafür Sorge zu tragen, dass weder im Landesamt für Verfassungsschutz noch in bayerischen Polizeibehörden Akten, Dateien und sonstige Unterlagen, die für den Untersuchungsauftrag relevant sein können, unwiederbringlich gelöscht werden. Eine ähnliche Bitte erreichte die bayerischen Behörden auch durch den Vorsitzenden des parallel laufenden Untersuchungsausschusses des Deutschen Bundestags.

Um diesen Anliegen zu entsprechen, verfügte das Staatsministerium des Innern, für Bau und Verkehr gegenüber dem Landesamt für Verfassungsschutz und den Polizeiverbänden, vorerst die Aussonderung und Löschung von polizeilichen Akten, Dateien und sonstigen Unterlagen zu unterlassen – unabhängig von den bis dahin erkennbaren Bezügen zum Untersuchungsgegenstand. Die Anordnung hierfür stützte das Landesamt für Verfassungsschutz auf Art. 7 Bayerisches Verfassungsschutzgesetz in Verbindung mit den jeweiligen Arbeitsanweisungen für die Speicherung und Löschung personenbezogener Daten. Im Bereich der polizeilichen Speicherungen/Akten wurde auf Art. 45 Abs. 3 Nr. 2 Polizeiaufgabengesetz zurückgegriffen.

Nachdem mich das Staatsministerium des Innern, für Bau und Verkehr über die Vorgehensweise informiert hat, habe ich darauf hingewiesen, dass die hierdurch länger aufbewahrten Daten ausschließlich dem oben genannten Zweck des Untersuchungsausschuss dienen dürften. Ebenso sollte auch der Personenkreis mit Zugriffsmöglichkeit auf diese Daten weitgehend eingeschränkt werden. Nach Abstimmung mit dem Staatsministerium für Justiz wurde zudem klargestellt, dass zwingende gesetzliche Löschungsverpflichtungen (wie zum Beispiel bei Erkenntnissen aus dem Kernbereich privater Lebensgestaltung) weiterhin unverzüglich zu erfüllen sind. Unter den vorgenannten Voraussetzungen habe ich den Regelungen und später auch der Verlängerung des Löschmoratoriums sowie einem weiteren Löschmoratorium beim Landesamt für Verfassungsschutz im Zusammenhang mit dem NSA-Untersuchungsausschuss des Deutschen Bundestages zugestimmt. Meine datenschutzrechtlichen Bedenken gegenüber den umfassenden Speicherungs- und Aufbewahrungsverlängerungen der personenbezogenen Daten einer Vielzahl von unbeteiligten Betroffenen habe ich gerade auch im Hinblick auf die verfassungsrechtlich gebotene Aufklärungsarbeit solcher Untersuchungsausschüsse vorerst zurückgestellt.

Grundsätzlich sehe ich jedoch die Zunahme von Löschmoratorien kritisch. So habe ich bei der Übertragung der oben genannten Verfahrensweise zur Unterstützung parlamentarischer Untersuchungsausschüsse auf strafrechtliche Ermittlungsverfahren (beispielsweise anlässlich der Ermittlungen des Generalbundesanwaltes zum Oktoberfestattentat) meine datenschutzrechtlichen Bedenken dem Staatsministerium des Innern, für Bau und Verkehr mitgeteilt.

4.4 Prüfungen

4.4.1 Prüfung des Gemeinsamen Terrorismusabwehrzentrums (GTAZ)

Das Gemeinsame Terrorismusabwehrzentrum beschäftigt sich mit der Bekämpfung des islamistischen Terrorismus. Es hat seinen Sitz beim Bundeskriminalamt am Standort Berlin-Treptow und nahm Ende 2004 seine Arbeit auf. Im GTAZ sind folgende Behörden vertreten:

- Bundeskriminalamt (BKA),
- Bundesamt für Verfassungsschutz (BfV),
- alle Landeskriminalämter,
- alle Landesämter für Verfassungsschutz,
- Bundenachrichtendienst (BND),
- Militärischer Abschirmdienst (MAD),
- Bundespolizei,
- Generalbundesanwalt (GBA),
- Zollkriminalamt (ZKA),
- Bundesamt für Migration und Flüchtlinge (BAMF).

Von den meiner Kontrollkompetenz unterliegenden bayerischen Behörden sind demnach das Bayerische Landeskriminalamt (LKA) sowie das Bayerische Landesamt für Verfassungsschutz (LfV) mit jeweils einem Verbindungsbeamten vor Ort vertreten. Entsprechend meinem gesetzlichen Kontrollauftrag habe ich ausschließlich die Datenerhebung, -verarbeitung und -nutzung durch die Verbindungsbeamten dieser beiden bayerischen Behörden geprüft.

Es handelt sich beim GTAZ wie auch bei den weiteren gemeinsamen Zentren des Bundes (etwa dem Gemeinsamen Extremismus- und Terrorismusabwehrzentrum GETZ) nicht um eine eigenständige Behörde, sondern um eine Plattform, die dem wechselseitigen länder- und behördenübergreifenden Informationsaustausch und der persönlichen Vernetzung dient. Demzufolge existieren keine gesonderten Rechtsgrundlagen speziell für das GTAZ. Vielmehr werden für die dortigen Datenübermittlungen die für die dort vertretenen Behörden jeweils einschlägigen Datenübermittlungsbefugnisse herangezogen. Vor allem die wechselseitige Datenübermittlung zwischen den Polizeibehörden und den Nachrichtendiensten unterliegt aufgrund des informationellen Trennungsprinzips jedoch besonderen Voraussetzungen (ATDG-Urteil des Bundesverfassungsgerichts vom 24. April 2013 – 1 BvR 1215/07; siehe hierzu näher 26. Tätigkeitsbericht 2014 unter Nr. 4.2.1).

Diese besondere Konstruktion des GTAZ und die Anforderungen des Bundesverfassungsgerichts in seinem ATDG-Urteil habe ich zum Anlass für meine Prüfung des LKA und des LfV genommen. Dabei habe ich Protokolle der Besprechungen der Verbindungsbeamtinnen und -beamten im GTAZ gesichtet und sie dazu befragt. In diesem Zusammenhang habe ich Gespräche mit weiteren Vertretern des LKA und des LfV über die Tätigkeit im GTAZ geführt. Auch habe ich das GTAZ vor Ort besucht und an dortigen Besprechungen teilgenommen.

Jeder Beitrag einer Verbindungsbeamtin oder eines Verbindungsbeamten des LKA oder des LfV in einem Gremium des GTAZ stellt datenschutzrechtlich bereits eine Datenübermittlung an sämtliche im dortigen Gremium vertretenen Behörden dar, weshalb die Voraussetzungen der jeweiligen Datenübermittlungsbefugnis

auch im Hinblick auf jede einzelne Empfangsbehörde vorliegen müssen. Insbesondere muss die Erforderlichkeit einer personenbezogenen Datenübermittlung an alle dort jeweils vertretenen Behörden und damit gegebenenfalls an alle im GTAZ vertretenen Behörden vorliegen.

Auf diese Rechtslage habe ich hingewiesen. Wie mir versichert wurde, teilen die beiden betreffenden Behörden meine Auffassung. Ich habe darum gebeten, die Voraussetzungen einer Datenübermittlung mit Personenbezug in jedem konkreten Einzelfall auch künftig sorgfältig zu prüfen. Verbesserungen konnte ich dahingehend erreichen, dass diese Prüfung der Datenübermittlungsvoraussetzungen nunmehr dokumentiert werden wird. Konkrete Beiträge der bayerischen Verbindungsbeamtinnen und -beamten im GTAZ, für welche die rechtlichen Voraussetzungen der Datenübermittlung an die übrigen Behörden des GTAZ im Einzelfall nicht vorgelegen hätten, habe ich im Rahmen meiner Prüfung nicht festgestellt.

Weiter konnte ich erreichen, dass für den Bereich der beiden bayerischen Behörden LKA und LfV nunmehr ausdrücklich und verbindlich geregelt wird, wo und wie lange sie die GTAZ-Unterlagen (Protokolle und ähnliches) aufbewahren beziehungsweise speichern. Insbesondere habe ich darauf geachtet, dass bestehende Höchstspeicherfristen in den übrigen Dateien der genannten Behörden durch die Aufbewahrung der GTAZ-Unterlagen nicht umgangen werden. Die in diesem Rahmen getroffenen Regelungen von LKA und LfV habe ich als ausreichend und verhältnismäßig beurteilt.

4.4.2 Teilnahme des Landesamts für Verfassungsschutz an einer staatsanwaltlichen Durchsuchung

Im Rahmen einer Prüfung habe ich von einem Vorgang erfahren, in welchem das Landesamt für Verfassungsschutz an einer staatsanwaltlichen Durchsuchung teilgenommen hatte. Der Beschuldigte dieses Ermittlungsverfahrens war bereits zuvor den Polizei – sowie auch den Verfassungsschutzbehörden bekannt. Die mit Zustimmung der Staatsanwaltschaft erfolgte Teilnahme der Beschäftigten des Landessamts für Verfassungsschutz diente dem Zweck, beratende Unterstützung für das Ermittlungsverfahren zu leisten, insbesondere im Hinblick auf die extremistische Gruppierung, der der Beschuldigte angehören soll. Die Beschäftigten des Landesamts für Verfassungsschutz traten dabei – wie den von mir eingesehenen Akten zu entnehmen war – offen als Angehörige des Landesamts für Verfassungsschutz auf. Im Rahmen ihrer beratenden Teilnahme an der Durchsuchungsmaßnahme haben die Beschäftigten des Landesamts für Verfassungsschutz jedoch in einem Fall auch eigenständig personenbezogene Daten erhoben. Dies habe ich zum Anlass genommen, mich grundsätzlich mit dieser Thematik zu beschäftigen.

Anerkanntermaßen kann die Staatsanwaltschaft zwar zu Ermittlungshandlungen – wie etwa Durchsuchungen – grundsätzlich Sachverständige oder sachkundige Dritte zu ihrer Unterstützung hinzuziehen, soweit dies zur Förderung der Ermittlungshandlung erforderlich ist. Darunter können auch Beschäftigte des Landesamts für Verfassungsschutz fallen (siehe Nr. 205 Abs. 5 der Richtlinien für das Straf- und Bußgeldverfahren – RiStBV), auch wenn ich dies datenschutzrechtlich aufgrund des Trennungsgebots (siehe Urteil des Bundesverfassungsgerichts vom 24. April 2013 – 1 BvR 1215/07) kritisch sehe. Es handelt sich auch in diesen Fällen jedoch stets um eine Ermittlungshandlung der Staatsanwaltschaft. Hinzugezo-

gene Sachverständige oder sachkundige Dritte werden nur beratend oder unterstützend tätig; eine eigene Ermittlungshandlung von Dritten ist damit nicht verbunden.

Erhebliche datenschutzrechtliche Bedenken ergeben sich, wenn die zur Durchsuchung – gegebenenfalls zudem verdeckt – hinzugezogenen Beschäftigten des Landesamts für Verfassungsschutz eigene Datenerhebungen durchführen und nicht nur die Datenerhebungen der Staatsanwaltschaft beratend unterstützen. In diesem Fall verlassen sie den Bereich der bloßen Unterstützung der Ermittlungsbehörden. Es bedarf daher für die eigene Datenerhebung des Landesamts für Verfassungsschutz bei der Teilnahme an der Durchsuchung auch einer eigenen Befugnis zur Datenerhebung.

Unabhängig davon habe ich aber darüber hinaus grundlegende Bedenken, wenn das Landesamt für Verfassungsschutz anlässlich einer unterstützenden Teilnahme an Wohnungsdurchsuchungen selbst Daten erhebt:

Das Bayerische Verfassungsschutzgesetz (BayVSG) räumt dem Landesamt für Verfassungsschutz bewusst keine Befugnis zu einer zwangsweise durchsetzbaren Wohnungsdurchsuchung wie in §§ 102, 103 Strafprozessordnung oder Art. 23 Polizeiaufgabengesetz ein. Diese gesetzgeberische Entscheidung droht, in Fällen der eigenen Datenerhebungen im Rahmen einer Teilnahme an Durchsuchungsmaßnahmen hierzu befugter Behörden umgangen zu werden. Damit wird Art. 13 Grundgesetz (GG) nicht gewahrt. Hinzu kommt, dass die Wohnungsinhaberin oder der Wohnungsinhaber regelmäßig das Betreten der Wohnung nur unter dem Eindruck und dem Zwang des richterlichen Durchsuchungsbeschlusses gestattet, der das Betreten zum Zwecke der Strafverfolgung (vor allem Auffinden von Beweismitteln oder Ergreifung des Beschuldigten) erlaubt. Diese Zweckbindung wird bei anschließenden eigenen Datenerhebungen des Landesamts für Verfassungsschutz jedoch nicht gewahrt. Vielmehr wird der Zweck „Strafverfolgung“ in den Zweck „Aufgabenerfüllung nach Art. 3 BayVSG“ geändert, ohne dass dies den Betroffenen bei Bekanntgabe des Durchsuchungsbeschlusses bewusst war und sie ihre Entscheidungen danach ausrichten konnten.

Sofern daher das Landesamt für Verfassungsschutz an einer Wohnungsdurchsuchung bereits in der vorgefassten Absicht beziehungsweise – zumindest auch – zu dem Zweck teilnehmen würde, eigene Datenerhebungen durchführen zu wollen, wäre aus datenschutzrechtlicher Sicht von vornherein der Bereich der bloßen sachkundigen Unterstützung im Sinne von Nr. 205 Abs. 5 RiStBV überschritten. Die Teilnahme zur Unterstützung der Ermittlungsbehörde würde in diesen Fällen nur als vorgeschobene Konstruktion dienen, um das Fehlen einer Befugnis zur Wohnungsdurchsuchung im Bayerischen Verfassungsschutzgesetz und damit den Schutz des Art. 13 GG zu umgehen. Zudem bestünde auch die Gefahr, dass die Wohnungsinhaberin oder der Wohnungsinhaber durch die Teilnahme des Verfassungsschutzes an der Durchsuchung über die Reichweite und Bedeutung des richterlichen Durchsuchungsbeschlusses getäuscht wird.

Deshalb kommt auch eine lediglich beratende Teilnahme des Landesamts für Verfassungsschutz an Wohnungsdurchsuchungsmaßnahmen nur in Betracht, soweit die durchsuchende Behörde bereits selbst – unabhängig von etwaigen Wünschen des Landesamts für Verfassungsschutz – die Entscheidung zu einer Wohnungsdurchsuchung getroffen hat.

Im konkreten Fall habe ich zwar nicht festgestellt, dass sich das Landesamt für Verfassungsschutz bewusst die Gelegenheit einer eigenen Datenerhebung verschaffen wollte. Jedoch ging die Zusammenarbeit im Laufe der Durchsuchungsmaßnahme über eine bloß beratende Unterstützung hinaus. Aus datenschutzrechtlicher Sicht handelte es sich daher um eine unzulässige Datenerhebung durch das Landesamt für Verfassungsschutz anlässlich einer Wohnungsdurchsuchung.

Meine Einschätzung habe ich dem Landesamt für Verfassungsschutz mitgeteilt. Das Landesamt für Verfassungsschutz hat seine Beschäftigten gebeten, die in meiner Bewertung zum Ausdruck gebrachten rechtlichen Grenzen der Teilnahme an staatsanwaltlichen Durchsuchungen künftig zu beachten.

5 Justiz

5.1 Gesetze, Verordnungen und Verwaltungsvorschriften

5.1.1 Künftige Auswirkungen der Richtlinie für den Datenschutz der Strafjustiz

Am 27. April 2016 erließen das Europäische Parlament und der Rat die Richtlinie 2016/680/EU zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI. Anders als die am gleichen Tag erlassene Datenschutz-Grundverordnung (siehe hierzu Nr. 1.1.1.1) berücksichtigt diese Richtlinie für den Datenschutz der Strafjustiz – als spezifischeres Regelungsinstrument – die Besonderheiten der Kriminalitätsbekämpfung.

Ziel der Richtlinie ist, eine effektive Zusammenarbeit in Strafsachen und Polizeiangelegenheiten und den Austausch personenbezogener Daten zwischen den zuständigen Behörden der Mitgliedstaaten zu erleichtern. Gleichzeitig soll ein einheitlich hohes Schutzniveau für die personenbezogenen Daten gewährleistet werden. Hierzu räumt die Richtlinie den Betroffenen weitreichende Rechte ein, stattet die Aufsichtsbehörden mit zahlreichen Befugnissen (insbesondere Untersuchungs- und Abhilfebefugnissen) aus und schränkt die Datenverarbeitung an entscheidenden Stellen ein. So ist etwa zukünftig eine Datenverarbeitung allein mit Einwilligung der betroffenen Personen nur noch zulässig, wenn die Einwilligungsmöglichkeit gesetzlich normiert ist (siehe Erwägungsgrund 35 der Richtlinie). Dies betrifft die immer wieder praktizierten „Einwilligungslösungen“, bei denen eine Datenverarbeitung gesetzlich nicht geregelt ist. In diesen Fällen ist zukünftig eine Datenverarbeitung nur noch dann zulässig, wenn eine Rechtsvorschrift die Einwilligung ausdrücklich vorsieht (siehe zu den weiteren Neuerungen auch Nr. 3.1.1).

Die Richtlinie ist bis zum 6. Mai 2018 in nationales Recht umzusetzen. Sie erfordert zahlreiche Anpassungen von Rechtsvorschriften.

Wegen des notwendigen Anpassungsbedarfs stehe ich im engen Austausch mit dem zuständigen Staatsministerium der Justiz. Über konkrete Ergebnisse, die zum Redaktionsschluss noch nicht feststanden, werde ich weiter berichten.

5.1.2 Vorratsdatenspeicherung

Mit der Vorratsspeicherung von Telekommunikationsdaten habe ich mich in den letzten Jahren regelmäßig auseinandergesetzt (siehe 24. Tätigkeitsbericht 2010 unter Nr. 3.3, 25. Tätigkeitsbericht 2012 unter Nr. 3.1, 26. Tätigkeitsbericht 2014 unter Nr. 1.2.2). Mein letzter Tätigkeitsberichtsbeitrag zu diesem Thema hatte die Überschrift „Ende der Vorratsdatenspeicherung?“. Diese Frage knüpfte an die Entscheidung des Europäischen Gerichtshofs vom 8. April 2014 an, in der dieser die Richtlinie 2006/24/EG zur Vorratsspeicherung von Telekommunikationsdaten für ungültig erklärte. Leider hat sich die mit dieser Entscheidung verbundene Hoffnung auf ein Ende der Vorratsdatenspeicherung nicht erfüllt. Vielmehr hat der deutsche Gesetzgeber mit dem Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherpflicht für Verkehrsdaten vom 10. Dezember 2015 (BGBl. 2015 I S. 2218) die Vorratsdatenspeicherung abermals eingeführt. Die gegen dieses Gesetz bestehenden Bedenken hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 9. Juni 2015 zum Ausdruck gebracht.

Umlaufentschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 09.06.2015

Gegen den Gesetzentwurf zur Vorratsspeicherung von Telekommunikationsverkehrsdaten bestehen erhebliche verfassungsrechtliche Bedenken

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

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

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

Mit einer Vorratsdatenspeicherung wird massiv in Freiheitsrechte von allen Menschen unabhängig von einem konkreten Verdacht eingegriffen. Deshalb müssen derartige Maßnahmen, die nur als absolute Ausnahme überhaupt zulässig sein können, einer strengen Erforderlichkeits- und Verhältnismäßigkeitsprüfung unterzogen und durch technische, organisatorische und verfahrensrechtliche Vorkeh-

rungen abgesichert werden. Die Konferenz kann nicht erkennen, dass die Regelungen grundrechtlichen Anforderungen genügen. Dies gilt namentlich für die Kommunikation mit Berufsgeheimnisträgern (z.B. Abgeordneten, Ärzten, Rechtsanwälten und Journalisten). Auch die Vorgaben des Europäischen Gerichtshofs sind nicht vollumfänglich berücksichtigt.

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

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

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

5.1.3 Aufbewahrung von Notariatsunterlagen und Errichtung eines elektronischen Urkundenarchivs

Im Berichtszeitraum habe ich zum Entwurf eines Gesetzes zur Neuordnung der Aufbewahrung von Notariatsunterlagen und Errichtung eines elektronischen Urkundenarchivs bei der Bundesnotarkammer kritisch Stellung genommen. Neben verschiedenen technisch-organisatorischen Aspekten habe ich mich vor allem dagegen ausgesprochen, die Notarinnen und Notare von der Pflicht zur Bestellung von Datenschutzbeauftragten auszunehmen. Bislang sind in Bayern auch die Notariate als öffentliche Stellen zur Bestellung von Datenschutzbeauftragten verpflichtet (Art. 25 Abs. 2 BayDSG). Zur effektiven Sicherung der Datenschutzrechte der Bürgerinnen und Bürger halte ich es für geboten, diese Bestellungspflicht beizubehalten.

Nachdrücklich habe ich mich daher gegen die geplante Änderung des § 92 Bundesnotarordnung (BNotO) gewandt. Beabsichtigt war, die Notariate von der Kontrolle durch die Landesbeauftragten für den Datenschutz vollständig auszunehmen. Die Datenschutzkontrolle sollte danach nur noch durch die aufsichtführenden Stellen der Justizverwaltung durchgeführt werden. Eine solche umfassende Herausnahme der Notariate aus meiner Kontrollzuständigkeit konnte ich nicht hinnehmen. Die auch schon bislang bestehende Aufsicht durch die Justizverwaltung stellt keine gänzlich unabhängige Datenschutzkontrolle dar, wie sie durch Vorgaben des Europarechts verlangt wird. Die Justizverwaltung wird zudem bei ihrer Aufsichtstätigkeit den Fokus auf unterschiedliche Bereiche der Notariatstätig-

keit legen, wohingegen ich mich ausschließlich auf den Schutz des Rechts auf informationelle Selbstbestimmung konzentriere und dabei von meiner langjährigen Prüferfahrung aus diesem Bereich profitieren kann.

Die mit dem ersten Entwurf befasste Bund-Länder-Arbeitsgruppe unter Beteiligung der Bundesnotarkammer nahm meine Kritik auf und überarbeitete den Entwurf in den entscheidenden Punkten. Insbesondere wurde die geplante Regelung komplett gestrichen, wonach die Notariate von der Pflicht zur Bestellung von behördlichen Datenschutzbeauftragten befreit sein sollten. Zudem wird die beabsichtigte Änderung des § 92 BNotO nicht weiter verfolgt. Damit unterstehen Notariate auch künftig der Kontrolle der Landesbeauftragten für den Datenschutz. Das begrüße ich, denn so wird auch im Notariatswesen der Datenschutz weiterhin zuverlässig und kompetent sichergestellt.

Das Bundesministerium der Justiz und für Verbraucherschutz hat auf Grundlage des Entwurfs eine Gesetzesinitiative der Bundesregierung vorzubereitet. Am 12. Oktober 2016 hat das Bundeskabinett den Gesetzentwurf beschlossen (BR-Drs. 602/16). Dieser soll noch in der laufenden Legislaturperiode vom Bundestag verabschiedet werden.

5.1.4 Anti-Doping-Gesetz

Dem Staatsministerium der Justiz gegenüber habe ich zu einem Referentenentwurf der Bundesministerien der Justiz und für Verbraucherschutz, des Innern und für Gesundheit für ein Bundesgesetz zur Bekämpfung von Doping im Sport (Anti-Doping-Gesetz) Stellung genommen. Eine zentrale Rolle spielt in diesem Gesetzesentwurf die Zusammenarbeit öffentlicher Stellen mit der privatrechtlich organisierten Stiftung Nationale Anti Doping Agentur Deutschland (NADA). § 8 des Gesetzentwurfs regelt die Übermittlung personenbezogener Daten von Amts wegen durch Gerichte und Staatsanwaltschaften an die Stiftung NADA zum Zwecke disziplinarrechtlicher Maßnahmen im Rahmen des Dopingkontrollsystems der Stiftung. Eine derartige Übermittlung personenbezogener Daten durch die genannten Stellen greift in erheblichem Maße in das Recht auf informationelle Selbstbestimmung der Betroffenen ein. Dementsprechend kann nach der ausdrücklichen Regelung in § 8 Abs. 1 des Gesetzentwurfs ein schutzwürdiges Interesse der betroffenen Personen einer Übermittlung an die Stiftung entgegenstehen. Ein eventuell entgegenstehendes schutzwürdiges Interesse ist daher von der übermittelnden Stelle vor der Übermittlung im jeweiligen konkreten Einzelfall näher zu bestimmen und gegebenenfalls gegen den Zweck der Maßnahmen im Dopingkontrollsystem abzuwägen. Diese erforderliche Bestimmung und Abwägung der schutzwürdigen Interessen der betroffenen Personen setzt aus datenschutzrechtlicher Sicht jedoch voraus, dass den Betroffenen jedenfalls im Regelfall seitens der übermittelnden Stelle Gelegenheit zur Äußerung im Hinblick auf ihre entgegenstehenden schutzwürdigen Interessen gegeben wird. Nur durch eine solche Gelegenheit zur Äußerung ist gewährleistet, dass die möglichen schutzwürdigen Interessen der Betroffenen vollständig und zutreffend erfasst werden können. Auf diese Problematik habe ich das Staatsministerium der Justiz hingewiesen.

Dieses hat meine Hinweise in seiner Stellungnahme gegenüber dem Bundesministerium der Justiz und für Verbraucherschutz aufgenommen und meine Hinweise wurden in der Gesetzesbegründung aufgegriffen. Dort wird ausgeführt, dass die Betroffenen vor der Datenübermittlung in der Regel angehört werden

müssen. Sofern die vorherige Anhörung die Durchführung des Disziplinarverfahrens gefährden würde, sind die Betroffenen jedenfalls nachträglich zu unterrichten.

5.1.5 Einsicht des Europäischen Komitees zur Verhütung von Folter (CPT) in die Personal- und Gesundheitsakten von Gefangenen

Das Europäische Komitee zu Verhütung von Folter (European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment – CPT) ist ein Gremium des Europarats. Es findet seine Rechtsgrundlage im Europäischen Übereinkommen zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe (im Folgenden: Übereinkommen). Das Übereinkommen wurde von allen Mitgliedstaaten des Europarats ratifiziert und ist am 1. März 2002 in Kraft getreten. Das CPT besucht Hafteinrichtungen, um zu prüfen, wie Menschen behandelt werden, denen die Freiheit entzogen ist. Solche Einrichtungen sind Gefängnisse, Jugendhaftanstalten, Polizeidienststellen, Abschiebehafteinrichtungen und psychiatrische Kliniken. Delegationen des CPT haben unbeschränkten Zugang zu diesen Hafteinrichtungen einschließlich des Rechts, sich innerhalb dieser Orte ungehindert zu bewegen. Sie befragen Personen, denen die Freiheit entzogen ist, ohne Zeugen und können sich ungehindert mit jeder Person in Verbindung setzen, die ihnen sachdienliche Auskünfte geben kann. Nach jedem Besuch übermittelt das CPT einen detaillierten Bericht an den betroffenen Staat. Dieser Bericht beinhaltet die festgestellten Tatsachen sowie Empfehlungen, Kommentare und Auskunftsersuchen. Das CPT fordert darüber hinaus die jeweils betroffene Regierung auf, eine ausführliche Antwort auf seinen Bericht zu übermitteln. Die Berichte und Antworten sind die zentralen Elemente für einen kontinuierlichen Dialog mit dem betreffenden Staat.

Art. 8 Nr. 2 Übereinkommen
Eine Vertragspartei hat dem Ausschuss zur Erfüllung seiner Aufgabe folgende Erleichterungen zu gewähren:

a. Zugang zu ihrem Hoheitsgebiet und das Recht, sich dort uneingeschränkt zu bewegen;
b. alle Auskünfte über die Orte, an denen sich Personen befinden, denen die Freiheit entzogen ist;
c. unbeschränkten Zugang zu allen Orten, an denen sich Personen befinden, denen die Freiheit entzogen ist, einschließlich des Rechts, sich innerhalb dieser Orte ungehindert zu bewegen;
d. alle sonstigen der Vertragspartei zur Verfügung stehenden Auskünfte, die der Ausschuss zur Erfüllung seiner Aufgabe benötigt. Bei der Beschaffung solcher Auskünfte beachtet der Ausschuss die innerstaatlichen Rechtsvorschriften einschließlich des Standesrechts.

Umstritten ist die Frage, ob das CPT bereits auf der Grundlage des Art. 8 Nr. 2 Buchst. d) des Übereinkommens auch ein eigenes Recht auf Einsicht in die Personal- und Gesundheitsakten der Gefangenen besitzt oder ob hierfür eine eigenständige Rechtsgrundlage im deutschen Recht erforderlich ist. Während man teilweise eine eigene Rechtsgrundlage fordert und daher versucht, jeweils eine Einwilligung der betroffenen Person in die Einsichtnahme einzuholen, lassen andere die zitierten Passagen aus dem Übereinkommen für die Akteneinsicht grundsätzlich ausreichen.

Zu dieser Frage habe ich gegenüber dem Staatsministerium der Justiz Stellung bezogen. Art. 8 Abs. 2 Buchst. d) des Übereinkommens als alleinige Rechtsgrundlage für eine Einsicht in die Akten der Gefangenen halte ich aufgrund der dort formulierten Einschränkung in Satz 2 nicht für überzeugend. Eine solche Auslegung wird dem Recht der betroffenen Gefangenen auf informationelle Selbstbestimmung trotz der Aufgabe und Bedeutung des CPT nicht gerecht.

Zur Lösung über eine – den Anforderungen an die Freiwilligkeit genügende – Einwilligung der Betroffenen teile ich uneingeschränkt die hiergegen vom CPT geäußerte Befürchtung, die Gefangenen könnten sich gegenüber der Einrichtung dem Zwang ausgesetzt fühlen, ihre Einwilligung nicht zu erteilen.

Nicht zuletzt aus Gründen der Rechtssicherheit halte demnach auch ich die Schaffung einer eigenen gesetzlichen Rechtsgrundlage für die Gewährung der Akteneinsicht zugunsten des CPT zur Erfüllung der vertraglichen Verpflichtungen aus Art. 8 des Übereinkommens für vorzugswürdig. Grundsätzliche Bedenken gegen eine spezielle gesetzliche Regelung der Einsichtnahme des CPT in die Gefangenenpersonal- und -gesundheitsakten habe ich nicht, soweit die Einsicht für die Aufgabenerfüllung des CPT im Rahmen des Übereinkommens erforderlich ist. Dem CPT als Einrichtung des Europarats kommt im völkerrechtlichen System des Menschenrechtsschutzes in Europa eine tragende Rolle zu. Ich würde daher die Einführung einer eigenen Rechtsgrundlage begrüßen, wie dies bereits einige andere Bundesländer in ihren Strafvollzugsgesetzen vorgesehen haben.

5.1.6 Wiedereinführung der Regelanfrage beim Landesamt für Verfassungsschutz für die Richterschaft

Genau 25 Jahre nach Abschaffung der Regelanfrage in Bayern führt die Staatsregierung diese für angehende Richterinnen und Richter zum 1. November 2016 wieder ein. Die – auch unter dem Stichwort „Radikalenerlass“ bekannte – Regelanfrage soll vor jeder Einstellung eine routinemäßige Anfrage beim Landesamt für Verfassungsschutz nach Erkenntnissen ermöglichen, die gegebenenfalls auf eine verfassungsfeindliche Gesinnung schließen lassen. Anlass für die jetzige Wiedereinführung ist der Fall eines Richters, der am Amtsgericht Lichtenfels zum Proberichter ernannt wurde und zuvor in rechtsextremen Kreisen aktiv war.

Die Wiedereinführung der Regelanfrage lehne ich als unnötigen und erheblichen Grundrechtseingriff entschieden ab. Bereits heute bestehen hinreichende Möglichkeiten, die Verfassungstreue von Bewerberinnen und Bewerbern zu überprüfen. So erhalten diese Bewerberinnen und Bewerber bereits vor ihrer Bewerbung einen Fragebogen zur Prüfung der Verfassungstreue sowie eine gesonderte Erklärung hierzu, die sie auszufüllen und zu unterzeichnen haben.

Sollte eine betroffene Person diese Unterlagen zur Verfassungstreueprüfung wahrheitswidrig ausfüllen, ist ihre Ernennung zur Richterin oder zum Richter auf Lebenszeit gemäß § 19 Abs. 1 Nr. 3 Deutsches Richtergesetz (DRiG) – wegen arglistiger Täuschung – in der Regel zurückzunehmen.

Bei Richterinnen und Richtern auf Probe ist die Entfernung aus dem Dienstverhältnis sogar unter leichteren Voraussetzungen möglich. Nach § 22 Abs. 1 DRiG kann ein Probeverhältnis während der ersten zwei Jahre nach Ernennung zu bestimmten Zeitpunkten ohne weitere Vorbedingung, lediglich nach pflichtgemäßem Ermessen, beendet werden. Daran anschließend gestattet § 22 Abs. 2 DRiG

die Entlassung eines Richters auf Probe zum Ablauf des dritten oder vierten Jahres, wenn er für das Richteramt nicht geeignet ist oder wenn der Richterwahlausschuss seine Übernahme in das Richterverhältnis auf Lebenszeit ablehnt. Nach § 22 Abs. 3 DRiG kann ein Proberichter außerdem aus disziplinären Gründen entlassen werden, was auch eine vorläufige Dienstenthebung rechtfertigt (Art. 69 Abs. 1 Nr. 2 Bayerisches Richtergesetz). Die Entlassung von Richterinnen und Richtern auf Probe setzt im Übrigen keine Gerichtsentscheidung voraus, sondern erfolgt durch bloße Verfügung der jeweiligen Behörde.

Des Weiteren steht den bayerischen Staatsministerien als oberste Landesbehörden zusätzlich ein unbeschränktes Auskunftsrecht aus dem Bundeszentralregister zu (§ 41 Abs. 1 Nr. 2 Bundeszentralregistergesetz), wovon auch bereits im Bewerbungsverfahren Gebrauch gemacht werden kann. Aus dem Bundeszentralregister können sich ebenfalls Hinweise auf eine fehlende Verfassungstreue ergeben, insbesondere bei Eintragungen von Verurteilungen aus dem Staatsschutzbereich.

Neben den genannten Überprüfungsmöglichkeiten und Entlassungstatbeständen bieten die jeweiligen Prozessordnungen selbst ausreichend Sicherungsmechanismen, um etwaig politisch beeinflusste Entscheidungen zu verhindern:

Zu nennen sind hier an erster Stelle die Vorschriften über die Ablehnung eines Richters wegen Befangenheit (etwa § 24 Strafprozessordnung, § 42 Zivilprozessordnung, § 54 Verwaltungsgerichtsordnung, § 60 Sozialgerichtsgesetz). Diese ermöglichen bereits während eines laufenden Gerichtsverfahrens die Ablehnung eines Richters, „wenn ein Grund vorliegt, der geeignet ist, Misstrauen gegen die Unparteilichkeit eines Richters zu rechtfertigen“ (§ 24 Abs. 2 Strafprozessordnung, § 42 Abs. 2 Zivilprozessordnung).

Weiterhin sieht grundsätzlich jede Prozessordnung vor, gerichtliche Entscheidungen durch das Einlegen von Rechtsmitteln überprüfen zu lassen. Die Rechtsmitteleinlegung hat zur Folge, dass das Verfahren zur Entscheidung in eine höhere Instanz gehoben und darüber hinaus die Rechtskraft bis zur endgültigen Entscheidung gehemmt wird.

Zudem kommt dem Öffentlichkeitsgrundsatz (§§ 69 ff. Gerichtsverfassungsgesetz, § 55 Verwaltungsgerichtsordnung, § 52 Arbeitsgerichtsgesetz, § 61 Sozialgerichtsgesetz) als einem der tragenden Verfahrensgrundsätze eine Transparenz- und Überwachungsfunktion zu. Hiernach finden Gerichtsverhandlungen einschließlich der Beweisaufnahme und Urteilsverkündung grundsätzlich öffentlich statt und sind jedermann zugänglich. Dies erlaubt eine Kontrolle durch die Allgemeinheit und die Medien.

Aufgrund dieser Schutzmechanismen und Kontrollinstrumente sehe ich keine Notwendigkeit, Bewerberinnen und Bewerber für ein Richteramt einer verschärften Prüfung zu unterziehen. Insbesondere sollten nicht wegen eines Einzelfalls nunmehr alle Bewerberinnen und Bewerber unter Generalverdacht gestellt werden.

Meine ablehnende Haltung habe ich gegenüber der Staatsregierung deutlich zum Ausdruck gebracht. Leider hat sie meinen grundsätzlichen Bedenken keine Rechnung getragen. Ich konnte lediglich die Aufnahme einiger Verfahrensgrundsätze erreichen, die bei Durchführung der Regelanfrage zukünftig zu beachten sind:

So dürfen Anfragen beim Landesamt für Verfassungsschutz erst erfolgen, wenn die Einstellung tatsächlich beabsichtigt ist und die Verfassungstreue – gegebenenfalls neben der gesundheitlichen Eignung – die letzte zu prüfende Einstellungsvoraussetzung ist. Weiterhin ist die Einstellungsbehörde verpflichtet, Bedenken, die gegen die Einstellung sprechen und die dafür erheblichen Tatsachen der betroffenen Person schriftlich mitzuteilen, um eine Überprüfung der Richtigkeit der Erkenntnisse zu ermöglichen. Findet ein Anhörungsgespräch statt, ist ein Protokoll zu führen, in das der Bewerberin oder dem Bewerber auf Antrag Einsicht zu gewähren ist.

5.2 Auskunftsersuchen der Landesjustizkasse an Jobcenter

Die Landesjustizkasse Bamberg ist bayernweit unter anderem mit der Beitreibung von Gerichtskosten betraut. Ein Jobcenter unterrichtete mich darüber, dass die Landesjustizkasse das Jobcenter per Formblatt um Auskunft über die Leistungen an einen Betroffenen sowie über dessen Arbeitgeber ersucht hat. Wie ich feststellen musste, besitzt die Landesjustizkasse jedoch keine gesetzliche Befugnis zur Datenerhebung bei einem Jobcenter.

Das Bundesverfassungsgericht geht für den Datenaustausch zwischen Behörden vom sogenannten Doppeltürmodell aus (Entscheidungen vom 24. Januar 2012 – 1 BvR 1299/05 sowie vom 6. März 2014 – 1 BvR 3541/13). Dies bedeutet, dass bei einem Austausch von Daten sowohl für die Datenerhebung einerseits als auch für die Übermittlung der Daten andererseits jeweils eine eigene Rechtsgrundlage vorliegen muss.

Die für die Landesjustizkasse maßgebliche Justizbeitreibungsordnung sieht über die Verweisung auf einzelne Vorschriften der Zivilprozessordnung eine Befugnis zur Erhebung bestimmter Daten (wie etwa des aktuellen Arbeitgebers) nur bei den Trägern der gesetzlichen Rentenversicherung vor. Eine Datenerhebung bei Jobcentern ist von der Justizbeitreibungsordnung jedoch nicht abgedeckt. Die sozialgesetzlichen Vorschriften wiederum regeln zwar die Datenübermittlung, jedoch nicht die Datenerhebung durch die Landesjustizkasse. Schließlich ersetzt auch eine Berufung auf die Amtshilfevorschriften die notwendige gesonderte Rechtsgrundlage für die Datenerhebung nicht. Die Amtshilfe betrifft allein die Frage, ob eine um Information ersuchte Stelle bei Vorliegen einer Datenübermittlungsbefugnis auch verpflichtet ist, die ersuchten Daten zu übermitteln, nicht jedoch die Frage, ob die ersuchende Behörde zur Erhebung dieser Daten überhaupt befugt ist.

Die Landesjustizkasse hat sich meiner Rechtsauffassung zur fehlenden gesetzlichen Datenerhebungsbefugnis bei Jobcentern angeschlossen. Die Datenerhebung bei Jobcentern wurde eingestellt; die Beschäftigten wurden auf deren Unzulässigkeit hingewiesen.

5.3 Strafverfolgung

5.3.1 Wiederherstellung von „gelöschten“ Fotos mit Zustimmung der Berechtigten

Eine Petentin wurde zufällig Zeugin einer massiven Schlägerei auf dem Oktoberfest. Sie machte davon Fotos und bot der Polizei diese Fotos an. Nachdem die Polizei deswegen jedoch zunächst nicht mehr an sie herantrat, löschte sie die Fotos von der Speicherkarte. Erst einige Monate später kam die Polizei auf das Angebot der Petentin zurück. Aufgrund ihrer Bedenken, dass auch rein private Fotos ohne Relevanz für das Strafverfahren auf der Speicherkarte enthalten seien, sicherte man der Petentin zu, nur die tatrelevanten Aufnahmen, nicht jedoch die sonstigen Privatfotos auf dem Speichermedium wiederherzustellen und zu verwenden. Damit erklärte sie sich pauschal einverstanden. Der polizeiliche Sachbearbeiter beauftragte die technische Auswertestelle der Polizei zunächst, alle Fotos mit Bezug zum Oktoberfest wiederherzustellen. Die Auswertestelle stellte daher insgesamt fünf Aufnahmen vom Oktoberfest wieder her.

Dieses Vorgehen habe ich als vertretbar bewertet. Die erste Eingrenzung des Auftrags, Bilder mit Oktoberfestbezug wiederherzustellen, war zunächst ausreichend, da die technische Stelle mit dem Gegenstand und dem Stand der Ermittlungen nicht im Detail vertraut war und daher die konkrete Tatrelevanz nicht hinreichend beurteilen konnte. Die weitere Prüfung, ob sämtliche wiederhergestellten Oktoberfestbilder auch tatsächlich einen relevanten Bezug zur konkreten Tat aufweisen und daher für das Strafverfahren von Bedeutung sind, hatte der polizeiliche Sachbearbeiter anhand des Standes seiner Ermittlungen zu treffen.

Datenschutzrechtlichen Einwänden begegnete jedoch das weitere Vorgehen. Der polizeiliche Sachbearbeiter erkannte offenbar bereits selbst, dass lediglich drei der wiederhergestellten Fotos tatrelevant waren. Diese drei Fotos legte er der Petentin vor, die den Tatbezug bestätigte und ihre Zustimmung zur Verwendung dieser Fotos erklärte. Die übrigen beiden Fotos vom Oktoberfest wurden der Petentin nicht vorgelegt; von deren Wiederherstellung wusste sie nichts. Dennoch gelangten auch diese beiden Fotos ohne Tatrelevanz zur Strafakte und wurden so in das Verfahren eingeführt. Dafür holte man aber weder eine Zustimmung der Petentin ein noch veranlasste man gegebenenfalls eine Beschlagnahme oder ähnliches.

Die Beinahme auch der nichttatrelevanten Fotos zur Akte habe ich kritisiert. Die zuständige Staatsanwaltschaft hat im Rahmen meiner Prüfung die betreffenden Fotos der Akte entnommen und in einen Sonderband übernommen, der einer Akteneinsicht grundsätzlich nicht unterliegt. Dadurch wird die besondere Sensibilität der beiden rein privaten Fotos beachtet. Eine nachträgliche Entnahme und Vernichtung der beiden Fotos konnte ich hingegen wegen des Grundsatzes der Aktenvollständigkeit hier nicht erreichen. Immerhin habe ich veranlasst, dafür Sorge zu tragen, dass die Fotos auch bei der Polizei nicht mehr gespeichert oder sonst aufbewahrt werden.

5.3.2 Prüfung von Funkzellenabfragen

Im Berichtszeitraum habe ich bei zwei Staatsanwaltschaften sogenannte nichtindividualisierte Funkzellenabfragen geprüft. Mit dieser Maßnahme können bei

Straftaten von auch im Einzelfall erheblicher Bedeutung die Verbindungsdaten aller Mobilfunkgeräte, die sich in einem bestimmten Zeitraum in einer bestimmten räumlichen Funkzelle aufgehalten haben, von den Telekommunikationsanbietern abgefragt werden. Voraussetzung ist weiterhin, dass die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts von Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Rechtsgrundlage für eine Funkzellenabfrage war bis zum 17. Dezember 2015 § 100g Abs. 2 Satz 2, Abs. 1 Strafprozessordnung (StPO). Mit dem Gesetz zur Einführung einer Speicherfrist und Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 (BGBl. I, S. 2218) wurde die Funkzellenabfrage nunmehr ausdrücklich in § 100g Abs. 3 StPO n.F. geregelt. Da die Prüfung der Funkzellenabfragen noch vor Inkrafttreten der Gesetzesänderung durchgeführt wurde, waren bezüglich der rechtlichen Anforderungen noch die bis zum 17. Dezember 2015 geltenden Bestimmungen zu beachten. Die Funkzellenabfrage ist aus datenschutzrechtlicher Sicht grundsätzlich kritisch zu sehen, da regelmäßig eine Vielzahl von Daten abgefragt werden und die weit überwiegende Zahl der Betroffenen der Funkzellenabfrage mit der verfolgten Tat meistens nicht in Verbindung steht. Die Einhaltung der grundrechtssichernden Verfahrensvorschriften ist daher von besonderer Bedeutung für die Betroffenen einer solchen Funkzellenabfrage.

Meine Prüfung hat zunächst gezeigt, dass in allen geprüften Verfahren die erforderliche richterliche Anordnung eingeholt wurde. Da ich die richterliche Anordnung selbst aufgrund der richterlichen Unabhängigkeit nicht überprüfen kann (Art. 2 Abs. 6 BayDSG), habe ich bei meiner weiteren Prüfung mein Augenmerk auf die grundrechtssichernden Verfahrensregelungen – wie etwa die Benachrichtigungs- und die Löschungspflicht – gelegt.

Die Strafprozessordnung bestimmt zur Absicherung der Grundechte der Betroffenen insbesondere, dass die an der betroffenen Telekommunikation Beteiligten von der Maßnahme der Funkzellenabfrage zu beachrichtigen sind § 101 Abs. 4 bis 6 StPO (jetzt: § 101a Abs. 6 StPO n.F. wobei dieser die Regelungen des § 101 Abs. 4 bis 6 StPO für weitgehend anwendbar erklärt.

§ 101 StPO Verfahrensregelungen bei verdeckten Maßnahmen
(4) Von den in Absatz 1 genannten Maßnahmen sind im Falle

1. *des § 98a die betroffenen Personen, gegen die nach Auswertung der Daten weitere Ermittlungen geführt wurden,*
2. *des § 99 der Absender und der Adressat der Postsendung,*
3. *des § 100a die Beteiligten der überwachten Telekommunikation,*
4. *des § 100c*
   a) *der Beschuldigte, gegen den sich die Maßnahme richtete,*
   b) *sonstige überwachte Personen,*
   c) *Personen, die die überwachte Wohnung zur Zeit der Durchführung der Maßnahme innehatten oder bewohnten,*
5. *des § 100f die Zielperson sowie die erheblich mitbetroffenen Personen,*
6. *des § 100h Abs. 1 die Zielperson sowie die erheblich mitbetroffenen Personen,*
7. *des § 100i die Zielperson,*
8. *des § 110a*
   a) *die Zielperson,*
   b) *die erheblich mitbetroffenen Personen,*
   c) *die Personen, deren nicht allgemein zugängliche Wohnung der Verdeckte Ermittler betreten hat,*

9. des § 163d die betroffenen Personen, gegen die nach Auswertung der Daten weitere Ermittlungen geführt wurden,
10. des § 163e die Zielperson und die Person, deren personenbezogene Daten gemeldet worden sind,
11. des § 163f die Zielperson sowie die erheblich mitbetroffenen Personen
zu benachrichtigen. Dabei ist auf die Möglichkeit nachträglichen Rechtsschutzes nach Absatz 7 und die dafür vorgesehene Frist hinzuweisen. Die Benachrichtigung unterbleibt, wenn ihr überwiegende schutzwürdige Belange einer betroffenen Person entgegenstehen. Zudem kann die Benachrichtigung einer in Satz 1 Nummer 2 und 3 bezeichneten Person, gegen die sich die Maßnahme nicht gerichtet hat, unterbleiben, wenn diese von der Maßnahme nur unerheblich betroffen wurde und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung hat. Nachforschungen zur Feststellung der Identität einer in Satz 1 bezeichneten Person sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist.
(5) Die Benachrichtigung erfolgt, sobald dies ohne Gefährdung des Untersuchungszwecks, des Lebens, der körperlichen Unversehrtheit und der persönlichen Freiheit einer Person und von bedeutenden Vermögenswerten, im Fall des § 110a auch der Möglichkeit der weiteren Verwendung des Verdeckten Ermittlers möglich ist. Wird die Benachrichtigung nach Satz 1 zurückgestellt, sind die Gründe aktenkundig zu machen.
(6) Erfolgt die nach Absatz 5 zurückgestellte Benachrichtigung nicht binnen zwölf Monaten nach Beendigung der Maßnahme, bedürfen weitere Zurückstellungen der gerichtlichen Zustimmung. Das Gericht bestimmt die Dauer weiterer Zurückstellungen. Es kann dem endgültigen Absehen von der Benachrichtigung zustimmen, wenn die Voraussetzungen für eine Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden. Sind mehrere Maßnahmen in einem engen zeitlichen Zusammenhang durchgeführt worden, so beginnt die in Satz 1 genannte Frist mit der Beendigung der letzten Maßnahme. Im Fall des § 100c beträgt die in Satz 1 genannte Frist sechs Monate.

Ohne eine solche Benachrichtigung erfahren gerade die an der Tat unbeteiligten Betroffenen in der Regel nichts von der Maßnahme, die jedoch mitunter erheblich in ihre Privatsphäre eingreift. Die Benachrichtigung ist daher Voraussetzung für das Recht der Betroffenen, auch nach Beendigung der Maßnahme deren Rechtmäßigkeit sowie die Art und Weise ihres Vollzugs bei Gericht überprüfen zu lassen (§ 101 Abs. 7 Satz 2 StPO, jetzt: § 101a Abs. 6 Satz 2 StPO n.F. i.V.m. § 101 Abs. 7 Satz 2 StPO). Das Gesetz lässt allerdings zahlreiche Ausnahmen von der Benachrichtigungspflicht zu.

Während eine der beiden Staatsanwaltschaften in den meisten der geprüften Verfahren über die Notwendigkeit einer Benachrichtigung entschieden und diese Entscheidung in der Akte dokumentiert hatte, war eine solche aktenmäßig dokumentierte Entscheidung den Akten der anderen Staatsanwaltschaft in keinem der geprüften Fälle zu entnehmen. Auch falls im konkreten Einzelfall eine gesetzliche Ausnahme von der Benachrichtigungspflicht greift, halte ich es jedoch für erforderlich, die getroffene Entscheidung – sei es über die Benachrichtigung, deren Unterbleiben oder deren Zurückstellung – und die Gründe hierfür aktenkundig zu machen. Zwar ist dies gesetzlich nur für das Zurückstellen der Benachrichtigung nach § 101 Abs. 5 StPO, nicht aber für das gänzliche Unterbleiben gemäß Abs. 4 vorgeschrieben. Ein entsprechender Vermerk in den Akten nach Abschluss des Verfahrens dient jedoch der Übersichtlichkeit sowie der Nachvollziehbarkeit der

Entscheidungen der Staatsanwaltschaft im Nachhinein. Zudem fördert eine Pflicht, die eigene Entscheidung aktenkundig zu machen, die Sensibilität für diese Thematik und verhindert, dass die Problematik der Benachrichtigung schlichtweg übersehen und damit das Grundrecht auf informationelle Selbstbestimmung der überwiegend unbeteiligt Betroffenen nicht hinreichend beachtet wird.

Ein ganz ähnliches Ergebnis zeigte meine Prüfung auch im Bereich der Löschungspflicht nach § 101 Abs. 8 StPO (jetzt: § 101a Abs. 3 Satz 4 StPO n.F. der jedoch § 101 Abs. 8 StPO ebenfalls für entsprechend anwendbar erklärt).

§ 101 StPO Verfahrensregelungen bei verdeckten Maßnahmen
(8) Sind die durch die Maßnahme erlangten personenbezogenen Daten zur Strafverfolgung und für eine etwaige gerichtliche Überprüfung der Maßnahme nicht mehr erforderlich, so sind sie unverzüglich zu löschen. Die Löschung ist aktenkundig zu machen.

Naturgemäß betrifft die Funkzellenabfrage Personen die weit überwiegend keinerlei Verfahrensbezug zur Tat haben. Deshalb halte ich es aufgrund der Bedeutung der Löschpflicht für erforderlich, die getroffene Entscheidung über die Löschung aktenkundig zu machen. Ansonsten besteht die Gefahr, dass die Löschung übersehen wird oder in Vergessenheit gerät. Zwar bestimmt § 101 Abs. 8 Satz 2 StPO ausdrücklich nur, dass die Löschung an sich aktenkundig zu machen ist. Gleiches muss sich jedoch aus den genannten Gründen des Grundrechtsschutzes auch ergeben, wenn die erforderliche Prüfung der Löschungspflicht nicht die Löschung zum Ergebnis hat, sondern die Feststellung, dass die erhobenen Daten zunächst weiterhin zur Strafverfolgung erforderlich sind. Jedenfalls sollte spätestens nach Abschluss des Verfahrens ein solcher Vermerk erfolgen. Soweit die erhobenen Daten als weiterhin zur Strafverfolgung erforderlich im Sinne von § 101 Abs. 8 StPO angesehen werden (unter Umständen etwa bei Verfahren mit unbekannten Täterinnen oder Tätern), ist dieses Ergebnis regelmäßig in angemessenen Zeitabständen zu überprüfen und das Ergebnis dieser Überprüfung der Erforderlichkeit ebenfalls in den Akten festzuhalten.

Den beiden geprüften Staatsanwaltschaften habe ich meine Rechtsauffassung mitgeteilt und sie aufgefordert, die in den betreffenden Verfahren bislang nicht aktenkundigen Entscheidungen über die Benachrichtigung der Betroffenen und die Löschung der Daten nachzuholen und in den Akten zu dokumentieren.

Ich habe zudem auch die weitere Verarbeitung der mit der Funkzellenabfrage erhobenen Daten geprüft. In Betracht kommen hierfür insbesondere die Maßnahmen der Rasterfahndung nach § 98a StPO sowie des maschinellen Datenabgleichs im Sinne von § 98c StPO.

§ 98a StPO Rasterfahndung
(1) Liegen zureichende tatsächliche Anhaltspunkte dafür vor, daß eine Straftat von erheblicher Bedeutung
1. auf dem Gebiet des unerlaubten Betäubungsmittel- oder Waffenverkehrs, der Geld- oder Wertzeichenfälschung,
2. auf dem Gebiet des Staatsschutzes (§§ 74a, 120 des Gerichtsverfassungsgesetzes),
3. auf dem Gebiet der gemeingefährlichen Straftaten,
4. gegen Leib oder Leben, die sexuelle Selbstbestimmung oder die persönliche Freiheit,
5. gewerbs- oder gewohnheitsmäßig oder

6. von einem Bandenmitglied oder in anderer Weise organisiert
begangen worden ist, so dürfen, unbeschadet §§ 94, 110, 161, personenbezogene Daten von Personen, die bestimmte, auf den Täter vermutlich zutreffende Prüfungsmerkmale erfüllen, mit anderen Daten maschinell abgeglichen werden, um Nichtverdächtige auszuschließen oder Personen festzustellen, die weitere für die Ermittlungen bedeutsame Prüfungsmerkmale erfüllen. Die Maßnahme darf nur angeordnet werden, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise erheblich weniger erfolgversprechend oder wesentlich erschwert wäre.

§ 98c StPO Maschineller Abgleich mit vorhandenen Daten
Zur Aufklärung einer Straftat oder zur Ermittlung des Aufenthaltsortes einer Person, nach der für Zwecke eines Strafverfahrens gefahndet wird, dürfen personenbezogene Daten aus einem Strafverfahren mit anderen zur Strafverfolgung oder Strafvollstreckung oder zur Gefahrenabwehr gespeicherten Daten maschinell abgeglichen werden. Entgegenstehende besondere bundesgesetzliche oder entsprechende landesgesetzliche Verwendungsregelungen bleiben unberührt.

Meine Prüfung hat gezeigt, dass die erforderliche Abgrenzung zwischen einer Rasterfahndung, die den speziellen Voraussetzungen und Regelungen der §§ 98a und § 98b StPO unterliegt, und dem bloßen Datenabgleich nach § 98c StPO nicht immer trennscharf möglich und daher nicht immer leicht zu finden ist. Dabei steht die Rasterfahndung im Gegensatz zum Datenabgleich unter einem gesetzlichen Richtervorbehalt. Zudem bestimmt § 98b Abs. 4 StPO für die Rasterfahndung, dass die jeweils zuständige Datenschutzbehörde über diese Maßnahme nach ihrer Beendigung zu unterrichten ist. Insbesondere wenn in einem Strafverfahren die erhobenen Funkzellendaten mit Funkzellendaten aus anderen ähnlichen gelagerten Strafverfahren maschinell abgeglichen werden, stellt sich die Frage, ob ein solcher Abgleich noch auf § 98c StPO gestützt werden kann oder ob eine Rasterfahndung vorliegt. In derartigen Konstellationen holen einige Staatsanwaltschaften mitunter Rasterfahndungsbeschlüsse ein und gehen damit der Abgrenzungsproblematik im Einzelfall und somit einer eventuell später auftretenden Verwertungsproblematik aus dem Weg. Auch ich halte diesen Weg für vorzugswürdig. Hierauf habe ich die geprüften Staatsanwaltschaften hingewiesen.

5.3.3 Automatische Angabe des Geburtsdatums von Angeklagten in forumSTAR-Straf

Die Strafgerichte in Bayern arbeiten mit dem EDV-Programm forumSTAR-Straf. Dieses Programm ermöglicht die Erstellung von Schreiben mit Textbausteinen. Dabei werden bestimmte Daten zum Betreff des Verfahrens jeweils automatisch aus den Grunddaten übernommen. Wie ich erfahren habe, wird dabei neben dem Namen von Angeklagten und dem Tatvorwurf auch das Geburtsdatum von Angeklagten automatisch in die mit Hilfe dieses Programms erstellten Schreiben, wie etwa Zeugenladungen, übernommen. Auch wenn ich die konkrete Gestaltung von Zeugenladungen durch ein Gericht in einem gerichtlichen Verfahren im Einzelnen nicht überprüfen kann (Art. 2 Abs. 6 BayDSG), so habe ich die generelle automatische Übernahme des Geburtsdatums durch das Programm forumSTAR-Straf gegenüber dem Staatsministerium der Justiz problematisiert. Zwar kann das Geburtsdatum von Angeklagten ein erforderliches und sachgerechtes Unterscheidungskriterium darstellen, um die jeweiligen Angeklagten eindeutig identifizieren zu können. Dies ist etwa bei Ladungen von Zeuginnen und Zeugen der Fall, die

aufgrund ihrer beruflichen Tätigkeit mit einer Vielzahl von Verfahren und Zeugenaussagen in Berührung kommen, wie zum Beispiel Polizeibeamtinnen und -beamten oder Beschäftigten bestimmter Ämter. In vielen anderen Fällen halte ich jedoch die Angabe des Geburtsdatums insbesondere auf Zeugenladungen nicht für erforderlich. Besonders problematisch war die Tatsache, dass forumSTAR-Straf eine manuelle Verhinderung der automatischen Übernahme des Geburtsdatums oder dessen nachträgliche Löschung bislang nicht vorsah. Mit meinem Wunsch, auf die automatische Übernahme des Geburtsdatums zu verzichten, konnte ich mich zwar nicht durchsetzen. Das Justizministerium ist meiner Bitte gefolgt und hat das Programm in einem ersten Schritt so geändert, dass das zunächst in den Textbaustein übernommene Geburtsdatum entfernt werden konnte. In einem zweiten Schritt wurde das Geburtsdatum aus den entsprechenden Textbausteinen entfernt. Es ist nun durch die Anwenderin oder den Anwender zu ergänzen, soweit es für erforderlich angesehen wird. Sämtliche Anwenderinnen und Anwender wurden auf diese neu geschaffenen Möglichkeiten hingewiesen. Durch diese Neuerung kann bei sachgemäßer Handhabung das informationelle Selbstbestimmungsrecht der Angeklagten mit dem Interesse der Justiz an einer funktionsfähigen Rechtspflege im jeweiligen Einzelfall zu einem angemessenen Ausgleich gebracht werden.

5.3.4 Umfang einer Einstellungsmitteilung an Anzeigeerstatter

Ein Autohaus erstattete Strafanzeige wegen Unterschlagung eines Fahrzeugs. Von der Staatsanwaltschaft erhielt das Autohaus nach einiger Zeit eine Mitteilung über eine Teileinstellung des Verfahrens. Die Gründe der Mitteilung standen jedoch nicht nur in Zusammenhang mit der Strafanzeige des Autohauses. Vielmehr waren darin auch Ausführungen zu ebenfalls eingestellten Tatvorwürfen wie versuchter Schwangerschaftsabbruch, versuchte Körperverletzung und versuchter Einbruchsdiebstahl enthalten. Diese bezogen sich offenkundig auf andere Strafanzeigen und andere Sachverhalte. Ich habe darin eine unzulässige Übermittlung von Daten des Beschuldigten an das Autohaus gesehen. Die verschiedenen Anzeigen gegen den Beschuldigten wurden von der Staatsanwaltschaft in einem einheitlichen Ermittlungsverfahren behandelt und in eine einheitliche Einstellungsbegründung zusammengefasst. Dagegen bestehen an sich keine Einwände. Jedoch muss im Zuge der Mitteilung der Einstellung und ihrer Gründe darauf geachtet werden, dass an unterschiedliche Anzeigeerstatter jeweils nur diejenigen Teile mitgeteilt werden, die den jeweils angezeigten Sachverhalt betreffen und keine Informationen übermittelt werden, die allein andere Anzeigeerstatter betreffen. Erleichtert wird diese notwendige Differenzierung bei der Übermittlung der Einstellung, wenn bereits bei Gestaltung der Einstellung und ihrer Gründe zwischen den einzelnen voneinander getrennten Anzeigen unterschieden wird. Um künftig derartige Fälle zu vermeiden hat die betroffene Staatsanwaltschaft ihre Beschäftigten bezüglich der geschilderten Problematik entsprechend sensibilisiert.

5.3.5 Mitteilungen der Staatsanwaltschaft zum Wählerverzeichnis

Nach § 45 Strafgesetzbuch verliert die Person, die wegen eines Verbrechens zu einer Freiheitsstrafe von mindestens einem Jahr verurteilt wurde, automatisch für eine bestimmte Zeit ihr passives Wahlrecht. Darüber hinaus kann das Strafgericht in bestimmten Fällen den Verlust des aktiven wie auch des passiven Wahlrechts für eine bestimmte Zeit aussprechen. In all diesen Fällen teilt die Staatsanwalt-

schaft diese Tatsache – ohne Bezeichnung der Tat – derjenigen Verwaltungsbehörde mit, die das Wählerverzeichnis führt. Diese sogenannte Mitteilung zum Wählerverzeichnis hat ihre gesetzliche Rechtsgrundlage in § 13 Abs. 1 Nr. 5 Einführungsgesetz zum Gerichtsverfassungsgesetz und ist in Nr. 12 der Anordnung über Mitteilungen in Strafsachen (MiStra) näher geregelt. In Bayern sind die Gemeinden für die Führung des Wählerverzeichnisses zuständig. Wie mir jedoch ein Landratsamt mitteilte, erhielt man dort bereits wiederholt derartige Mitteilungen einer bestimmten Staatsanwaltschaft zum Wählerverzeichnis, obwohl die Mitteilung an die jeweilige kreisangehörige Gemeinde zu richten gewesen wäre. Ich habe die Staatsanwaltschaft auf diese Sachlage hingewiesen, da die Mitteilung an eine unzuständige Behörde regelmäßig eine nicht erforderliche Datenübermittlung darstellt. Die Staatsanwaltschaft hat sich meiner Auffassung zur zuständigen Empfangsbehörde für die Mitteilungen zum Wählerverzeichnis angeschlossen. Sie hat aufgrund meines Hinweises von sich aus organisatorische Maßnahmen ergriffen, um eine Versendung der Mitteilungen an eine unzuständige Behörde künftig zu vermeiden.

5.3.6 Beschriftung von Aktenordnern

Im Zuge der Prüfung einer Eingabe habe ich von einer Staatsanwaltschaft die entsprechenden Strafakten angefordert und eingesehen. Dabei musste ich feststellen, dass die mir übersandten Aktenordner teilweise noch Beschriftungen aus einer vorherigen Verwendung der Ordner in anderen Verfahren enthielten. So konnte man auf dem Aktenrücken ohne weiteres Namen und Geburtsdatum von Beschuldigten und Geschädigten sowie die dazugehörigen Tatvorwürfe aus anderen Verfahren ablesen, die mit dem aktuellen Verfahren und dem Akteninhalt in keiner Verbindung standen. Eine solche Beschriftung mit Daten der Verfahrensbeteiligten aus früheren Verfahren bei der Wiederverwendung von Aktenordnern für neue Verfahren kann zu einer unzulässigen Datenübermittlung führen. Bei einer Aktenversendung – gleich an welche Stelle oder welche Person – ist stets sorgfältig darauf zu achten, dass die Aktenordner nur die zutreffende Beschriftung enthalten. Sofern Aktenordner für neue Verfahren wiederverwendet werden, ist darauf zu achten, dass bisherige Beschriftungen der Ordner mit personenbezogenen Daten gänzlich unkenntlich gemacht werden. Ich habe die betreffende Staatsanwaltschaft aufgefordert, die betroffenen Aktenrücken zu ändern und die oben genannten Ausführungen künftig zu beachten.

5.4 Prüfung von Jugendarrestanstalten

Im Berichtszeitraum habe ich zwei Jugendarrestanstalten geprüft. Die Verhängung von Jugendarrest ist in § 13 und § 16 Jugendgerichtsgesetz (JGG) geregelt. Er wird in Bayern in speziellen Jugendarrestanstalten vollzogen. Jugendarrest wird in denjenigen Fällen verhängt, in denen eine Jugendstrafe nicht geboten ist, dem Jugendlichen jedoch eindringlich zum Bewusstsein gebracht werden muss, dass er für das von ihm begangene Unrecht einzustehen hat (§ 13 Abs. 1 JGG). Jugendarrest stellt keine Strafe wie etwa die Jugendstrafe dar, sondern ein Zuchtmittel, das nicht die Rechtswirkungen einer Strafe besitzt (§ 13 Abs. 3 JGG). Dieses Wesen des Jugendarrestes hat auch auf die datenschutzrechtlichen Bewertungen Einfluss. Zudem ist der Jugendarrest im Gegensatz zum sonstigen Strafvollzug von vornherein stets auf eine relativ kurze Zeit bemessen; so kann auch der Dauerarrest für nur höchstens 4 Wochen angeordnet werden.

Der Vollzug des Jugendarrests ist zunächst in § 90 JGG geregelt.

§ 90 JGG Jugendarrest
(1) Der Vollzug des Jugendarrestes soll das Ehrgefühl des Jugendlichen wecken und ihm eindringlich zum Bewußtsein bringen, daß er für das von ihm begangene Unrecht einzustehen hat. Der Vollzug des Jugendarrestes soll erzieherisch gestaltet werden. Er soll dem Jugendlichen helfen, die Schwierigkeiten zu bewältigen, die zur Begehung der Straftat beigetragen haben.
(2) Der Jugendarrest wird in Jugendarrestanstalten oder Freizeitarresträumen der Landesjustizverwaltung vollzogen. Vollzugsleiter ist der Jugendrichter am Ort des Vollzugs.

Weitere Rechtsgrundlage des Vollzugs des Jugendarrests im Rahmen des § 90 JGG ist – bis zur Schaffung einer näheren gesetzlichen Vollzugsregelung – lediglich die Jugendarrestvollzugsordnung (JAVollzO), eine Rechtsverordnung in der Fassung der Bekanntmachung vom 30. Januar 1976. Die ergänzenden, bundesweit einheitlichen Verwaltungsvorschriften hierzu, die Richtlinien zur Jugendarrestvollzugsordnung (RiJAVollzO), stammen für Bayern aus dem Jahr 1977.

Wie ich im Rahmen meiner Prüfung von Arrestanstalten feststellen konnte, genügt die Jugendarrestvollzugsordnung im Vergleich zu den Vollzugsgesetzen für die Strafhaft und die Untersuchungshaft den Anforderungen an einen modernen Jugendarrestvollzug nicht mehr durchgehend. Beispielhaft sei nur auf die Regelung des § 20 JAVollzO zum Verkehr mit der Außenwelt verwiesen. Außer in dringenden Fällen geht sie von der grundsätzlichen Unzulässigkeit des Außenkontakts aus und sieht sogar hinsichtlich eines nicht überwachten Außenkontakts keine privilegierten Stellen vor, wie es etwa im Bereich des Strafvollzugs üblich ist (vgl. Art. 32 Abs. 2 Bayerisches Strafvollzugsgesetz – BayStVollzG). Gleichfalls fehlen in der Jugendarrestvollzugsordnung auf den Jugendarrestvollzug zugeschnittene allgemeine Regelungen zur Erhebung, Nutzung und Verarbeitung personenbezogener Daten, etwa vergleichbar mit Art. 196 ff. BayStVollzG. Der Vollzug des Jugendarrests bringt zwangsläufig zahlreiche Grundrechtseingriffe von erheblichem Gewicht mit sich. Diese Eingriffe erfordern mit Blick auf die Wesentlichkeitstheorie des Bundesverfassungsgerichts jeweils eine normenklare und ausreichend bestimmte gesetzliche Rechtsgrundlage in Gestalt eines förmlichen Gesetzes. Ein solches modernes Gesetz für den Jugendarrestvollzug würde im Übrigen auch über den Datenschutz hinaus sowohl den Arrestanten als auch den Bediensteten im Jugendarrest mehr Rechtssicherheit in Fragen des Vollzugs geben als die vergleichsweise nur rudimentär ausgestaltete Jugendarrestvollzugsordnung. Dies habe ich auch dem Staatsministerium der Justiz mitgeteilt und die Schaffung eines modernen Vollzugsgesetzes für den Jugendarrest gefordert. Das Justizministerium hat mir mitgeteilt, es werde bei der anstehenden Erarbeitung eines modernen Jugendarrestvollzugsgesetzes meine Hinweise berücksichtigen.

5.5 Strafvollzug

5.5.1 Videoüberwachung

Meine regelmäßigen Prüfungen von Justizvollzugsanstalten habe ich auch in diesem Berichtszeitraum fortgeführt. Dabei habe ich wiederum auch die dortigen Videoüberwachungsmaßnahmen geprüft (zu den wichtigsten Gesichtspunkten siehe 26. Tätigkeitsbericht 2014 unter Nr. 5.4.4).

In einer Justizvollzugsanstalt habe ich auch dieses Mal die Videoüberwachung der Außenmauern kritisiert. Einige der schwenkbaren Kameras mit Zoom-Funktion konnten auch Privathäuser in der Nachbarschaft erfassen. Der hierdurch mögliche, mitunter deutliche Einblick in die Privatsphäre dritter Personen war nicht zulässig. Ich habe die Justizvollzugsanstalt daher aufgefordert, die Erfassung der Privathäuser durch geeignete technische Maßnahmen zu unterbinden. Die Anstalt ist dem durch eine entsprechende Einschränkung des Schwenkbereichs nachgekommen. Weiterhin habe ich bei zwei Justizvollzugsanstalten festgestellt, dass auf die Videoüberwachung erst unmittelbar am Eingang zur Justizvollzugsanstalt hingewiesen wurde. Ein Hinweis bereits an der Einfahrt zum Besucherparkplatz, der von der Videoüberwachung miterfasst wurde, fehlte hingegen. Damit war nicht gewährleistet, dass Besucherinnen und Besucher der Justizvollzugsanstalt rechtzeitig mit Betreten der videoüberwachten Bereiche auf die durchgeführte Videoüberwachung aufmerksam wurden und ihr Verhalten demgemäß daran ausrichten konnten. Die geprüften Justizvollzugsanstalten haben auf meine Bitte hin die erforderlichen Hinweisschilder angebracht.

5.5.2 Kopieren eines unverschlossenen, nicht der Überwachung unterliegenden Briefes

Nach Art. 32 Abs. 3 Bayerisches Strafvollzugsgesetz (BayStVollzG) darf der Schriftwechsel eines Gefangenen im Strafvollzug überwacht werden, soweit es aus Gründen der Behandlung oder der Sicherheit oder Ordnung der Anstalt erforderlich ist.

Davon ausgenommen ist der Schriftwechsel mit bestimmten im Gesetz ausdrücklich benannten Stellen, wie insbesondere dem Verteidiger des Gefangenen und den Datenschutzbeauftragten des Bundes und der Länder (Art. 32 Abs. 1 und 2 BayStVollzG). Ebenso von der Briefüberwachung ausgenommen ist der Schriftwechsel von Gefangenen mit den Mitgliedern des Anstaltsbeirats (siehe Art. 187 Abs. 2 Satz 2 BayStVollzG).

Mit dem Thema der Überwachung des Schriftwechsels mit dem Anstaltsbeirat war ich in folgendem Fall befasst: Ein Gefangener gab einen Brief mit einer Beschwerde an den Anstaltsbeirat unverschlossen bei einem Vollzugsbediensteten zur Weiterleitung ab. Wie mir mitgeteilt wurde, äußerte der Gefangene den Wunsch, den Inhalt seiner Beschwerde auch mit dem Leiter des Vollzugsdienstes zu besprechen. Für das Gespräch mit dem Gefangenen fertigte der Leiter des Vollzugsdienstes als Gedächtnisstütze eine Kopie dieses unverschlossenen Briefes an und brachte das Original auf den Postweg. Der Gefangene willigte in die Anfertigung einer Kopie nicht ein; vielmehr erfuhr er davon erst viel später. Die Briefkopie gelangte in der Folgezeit zur Gefangenenpersonalakte. Aus welchen Gründen dies geschah, konnte nicht mehr aufgeklärt werden. Die Justizvollzugsanstalt hat auf meine Nachfrage hin eingeräumt, dass das Anfertigen der Kopie in diesem Fall unzulässig war, da der Brief an den Anstaltsbeirat nicht der Briefüberwachung unterlag. Daran ändert auch der Umstand nichts, dass sich der Gefangene mit dem unverschlossenen Brief von sich aus an den Bediensteten gewandt hat, um den Inhalt des Briefes auch mit diesem zu besprechen. Auch die spätere Beinahme zur Gefangenenpersonalakte war dementsprechend unzulässig. Die Kopie wurde aus der Gefangenenpersonalakte entnommen und vernichtet. Die Justizvollzugsanstalt hat zudem ihre Bediensteten auf diese Thematik hingewiesen.

5.5.3 Versand von Gesundheitsdaten per Telefax an falschen Empfänger

Nach seiner Haftentlassung bat ein Petent die Justizvollzugsanstalt (JVA) schriftlich um Übersendung bestimmter ärztlicher Unterlagen an seinen namentlich mit Postanschrift benannten Hausarzt. Kurz darauf erhielt er die Nachricht seines Rechtsanwalts, dass die angeforderten Unterlagen des Anstaltsarztes per Fax in der Kanzlei statt beim Hausarzt eingegangen waren. Das Ersuchen des Petenten an die JVA wies jedoch den Petenten selbst als Absender aus, seine Anwaltskanzlei war darin in keiner Weise genannt. Wie sich im Rahmen meiner Prüfung herausstellte, hatte der Petent offenbar veranlasst, dass die Versendung seines Anschreibens an die JVA vom Telefaxgerät seines Rechtsanwalts aus vorgenommen wurde. Der Anstaltsarzt wiederum ging davon aus, dass es sich bei der im Empfangsexemplar automatisch aufgedruckten Faxnummer um die Faxnummer des Petenten oder seines Hausarztes handele. Er hatte daher die ärztlichen Unterlagen an die dort angegebene Faxnummer versandt. Durch die Versendung der Unterlagen an den Rechtsanwalt gegen den Willen des Petenten wurde gegen Datenschutzvorschriften verstoßen. Der Anstaltsarzt bedauerte sein Versehen ausdrücklich und sicherte mir künftig eine erhöhte Sorgfalt in derartigen Fällen zu.

Mit der Übermittlung personenbezogener Daten per Telefax habe ich mich bereits mehrfach befasst. Diese weist in datenschutzrechtlicher Hinsicht immer wieder erhebliche Probleme und Risiken auf. Da Verschlüsselungstechniken bei einem Telefax-Versand – ob konventionell oder auch mittels PC – aufgrund des verwendeten Protokolls derzeit nicht zur Verfügung stehen, sollte zur Gewährleistung der Vertraulichkeit – außer wenn dadurch in einem Notfall eine nicht zumutbare Zeitverzögerung entstehen würde – ein Versand sensibler personenbezogener Daten per Telefax grundsätzlich unterbleiben (siehe 21. Tätigkeitsbericht 2004 unter Nr. 22.2.24). Dies gilt umso mehr, soweit es sich um besonders sensible Daten wie vorliegend Gesundheitsdaten im Sinne von Art. 200 Abs. 2 Bayerisches Strafvollzugsgesetz handelt. Es wäre daher vom Anstaltsarzt zunächst sorgfältig zu prüfen gewesen, ob nicht ein Versand der angeforderten Daten per Post gegenüber einem Versand per Telefax vorzuziehen gewesen wäre. Hier lag die Besonderheit vor, dass der Petent zwar einerseits keine Telefaxnummer seines Hausarztes angegeben, andererseits jedoch unter Fristsetzung ausdrücklich darauf hingewiesen hat, dass die angeforderten Befunde ärztlicherseits dringend benötigt werden.

Weiterhin sind bei der Ermittlung der zutreffenden Telefaxnummer besondere Anforderungen an die Sorgfalt zu wahren. Diese Sorgfaltspflichten hat der Anstaltsarzt nicht eingehalten, weshalb ein Datenschutzverstoß zum Nachteil des Petenten vorlag. Bei Anwendung der gebotenen Sorgfalt kann nicht ohne weiteres davon ausgegangen werden, dass die beim Empfang des Telefaxes in der Absenderzeile automatisch aufgedruckte Faxnummer eindeutig und ausschließlich dem Absender zuzuordnen ist, sofern der Absender sie nicht als eigene Faxnummer bezeichnet. Vorliegend kommt hinzu, dass der Petent die Versendung nicht an sich selbst, sondern ausdrücklich an seinen Hausarzt wünschte. Zu den Risiken bei der Ermittlung der zutreffenden Faxnummer siehe bereits meinen 26. Tätigkeitsbericht 2014 unter Nr. 5.2.3. Zu diesen und weiteren Gesichtspunkten beim Telefaxversand halte ich zudem weitere Hinweise („Datensicherheit beim Telefax-Dienst“) auf meiner Homepage https://www.datenschutz-bayern.de bereit.

5.6 Bildaufnahmen zur Verfolgung von Parkverstößen

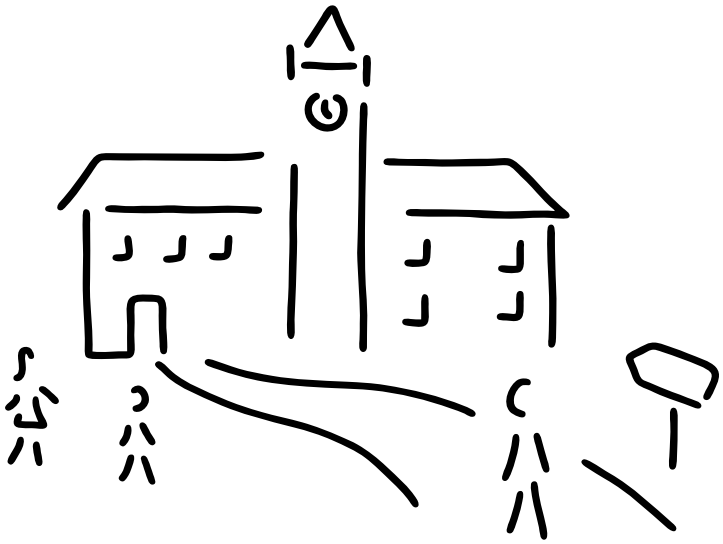
Ausgehend von Bürgereingaben und Behördenanfragen habe ich mich mit der Frage beschäftigt, ob und unter welchen Voraussetzungen bei der Verfolgung von Verkehrsordnungswidrigkeiten im Zusammenhang mit Parkverstößen von den Behörden Bildaufnahmen angefertigt werden dürfen. Grundsätzlich begegnet die Anfertigung von Lichtbildern der betreffenden Fahrzeuge oder des betreffenden Umfeldes bei Parkverstößen durch die Verfolgungsbehörden an sich keinen Einwänden. Dies gilt jedenfalls, soweit Lichtbilder von dem betreffenden Fahrzeug und der konkreten Verkehrssituation angefertigt werden, die zur Verfolgung des konkreten Vorwurfs erforderlich sind und nicht gezielt etwa Personen oder Fahrzeuge erfasst werden, die mit der Verfolgung des Verkehrsverstoßes in keinerlei Zusammenhang stehen.

Die Anfertigung von Lichtbildern zur Verfolgung von Parkverstößen findet ihre Rechtsgrundlage in der Generalklausel des § 161 Abs. 1 Strafprozessordnung (StPO) in Verbindung mit § 46 Abs. 1 Ordnungswidrigkeitengesetz. Zudem kommt wie bei der Verkehrsüberwachung im fließenden Verkehr § 100h Abs. 1 Nr. 1 StPO in Betracht. Das Anfertigen von Lichtbildaufnahmen zur Feststellung und Dokumentation von Parkverstößen kann auch zusätzlich zu einer Zeugenaussage grundsätzlich als erforderlich angesehen werden. Die Lichtbilder sind als Augenscheinobjekt im Bußgeldverfahren – auch vor Gericht – grundsätzlich verwertbar und stellen damit neben der Zeugenaussage der Beschäftigten der Verkehrsüberwachung ein weiteres Beweismittel dar, welches zudem von anderer Art (Augenschein statt Zeugenbeweis) und damit anderer Qualität ist.

Hinsichtlich des technisch-organisatorischen Verfahrens der Erstellung und Speicherung der Fotos sind dem Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen, die insbesondere die Vertraulichkeit und die Unversehrtheit der Daten gewährleisten.

Grundlegende datenschutzrechtliche Bedenken habe ich hingegen, soweit personenbezogene Inhalte der – gegebenenfalls zulässig angefertigten – Lichtbilder, welche zur Verfolgung des Parkverstoßes nicht erforderlich sind, nicht unkenntlich gemacht werden. Dazu zählen insbesondere Passanten im Hintergrund oder Kennzeichen anderer unbeteiligter Fahrzeuge. Bereits bei der Anfertigung der Lichtbilder ist darauf zu achten, solche überschießenden Datenerhebungen zu vermeiden. Gelingt dies im Einzelfall nicht, ist eine entsprechende Schwärzung von unbeteiligten Personen (Gesichter) und unbeteiligten Fahrzeugen (Kennzeichen) auf den Fotos erforderlich. Dabei ist die gebotene Schwärzung zur Sicherung des Rechts auf informationelle Selbstbestimmung so früh als möglich und damit nicht erst auf den eventuellen Ausdrucken der Fotos, sondern grundsätzlich bereits im elektronischen Bearbeitungssystem selbst durchzuführen.

6 Kommunales



6.1 Videoüberwachung im öffentlichen Raum durch Kommunen

Die Zulässigkeit von Videoüberwachung im öffentlichen Raum durch Kommunen ist seit Jahren immer wieder Gegenstand meiner Beratungs- und Kontrollpraxis. Es wenden sich sowohl Behörden als auch betroffene Bürgerinnen und Bürger an mich. Die Videoüberwachung ist – abgesehen von einzelnen Sondervorschriften etwa für die Polizei – in Art. 21a BayDSG geregelt. Bei vielen Vor-Ort-Prüfungen stellt sich heraus, dass bereits installierte Kameras gar nicht oder jedenfalls nicht im beabsichtigten Umfang zulässig sind. Vereinzelt hat bereits alleine die Ankündigung einer Prüfung zum Abbau der Kameras geführt. Das ist einerseits erfreulich, andererseits wäre es wünschenswert, wenn die verantwortlichen Stellen vor Ort bei der Installation einer Kamera sich vorab mit der Rechtslage intensiver befassen würden, als dies mitunter der Fall ist.

Erneut war ich besonders häufig mit der Frage konfrontiert, ob auch Kameraattrappen in den Anwendungsbereich des Art. 21a BayDSG fallen und wie die Gefahren, die mittels Videoüberwachung abgewehrt werden sollen, eigentlich nachgewiesen und dokumentiert werden sollen.

6.1.1 Überblick über Art. 21a BayDSG

Art. 21a Abs. 1 BayDSG regelt die materiell rechtlichen Anforderungen an eine Videoüberwachung. Hierunter ist sowohl die (speicherlose) Videobeobachtung als auch die Videoaufzeichnung zu verstehen. Im Ergebnis muss die Überwachung dazu dienen, bestehende Gefahren für die im Wortlaut des Art. 21a Abs. 1 BayDSG genannten Rechtsgüter (insbesondere: Leben, Gesundheit, Eigentum) abzuwehren. Art. 21a Abs. 2 BayDSG enthält das Transparenzgebot, wonach die

Videoüberwachung als solche und die erhebende Stelle durch geeignete Maßnahmen erkennbar zu machen sind („Hinweisschilder"). Art. 21a Abs. 3 BayDSG regelt die Zweckbindung der gespeicherten Daten. Art. 21a Abs. 4 BayDSG schreibt für bestimmte, seltene Fälle eine Information der Betroffenen vor. Art. 21a Abs. 5 BayDSG enthält eine Speicherungs- und Löschungsvorschrift. Art. 21a Abs. 6 BayDSG ordnet schließlich die entsprechende Geltung des datenschutzrechtlichen Freigabeerfordernisses und das Führen eines Verfahrensverzeichnisses für den Fall der Videoaufzeichnung an; außerdem regelt er die Details der Beteiligung der behördlichen Datenschutzbeauftragten, die alle Behörden nach Art. 25 Abs. 2 BayDSG zu bestellen haben.

Art. 21a BayDSG Videobeobachtung und Videoaufzeichnung (Videoüberwachung)
(1) [1]Mit Hilfe von optisch-elektronischen Einrichtungen sind die Erhebung (Videobeobachtung) und die Speicherung (Videoaufzeichnung) personenbezogener Daten zulässig, wenn dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts erforderlich ist,

1. *um Leben, Gesundheit, Freiheit oder Eigentum von Personen, die sich im Bereich öffentlicher Einrichtungen, öffentlicher Verkehrsmittel, von Dienstgebäuden oder sonstigen baulichen Anlagen öffentlicher Stellen oder in deren unmittelbarer Nähe aufhalten, oder*
2. *um Kulturgüter, öffentliche Einrichtungen, öffentliche Verkehrsmittel, Dienstgebäude oder sonstige bauliche Anlagen öffentlicher Stellen sowie die dort oder in deren unmittelbarer Nähe befindlichen Sachen*

zu schützen. [2]Es dürfen keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen der Betroffenen beeinträchtigt werden.
(2) Die Videoüberwachung und die erhebende Stelle sind durch geeignete Maßnahmen erkennbar zu machen.
(3) Die Daten dürfen für den Zweck verarbeitet und genutzt werden, für den sie erhoben worden sind, für einen anderen Zweck nur, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten erforderlich ist.
(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über die Tatsache der Speicherung entsprechend Art. 10 Abs. 8 zu benachrichtigen.
(5) Die Videoaufzeichnungen und daraus gefertigte Unterlagen sind spätestens drei Wochen nach der Datenerhebung zu löschen, soweit sie nicht zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten oder zur Geltendmachung von Rechtsansprüchen benötigt werden.
(6) [1]Art. 26 bis 28 gelten für die Videoaufzeichnung entsprechend. [2]Öffentliche Stellen haben ihren behördlichen Datenschutzbeauftragten rechtzeitig vor dem Einsatz einer Videoaufzeichnung neben den in Art. 26 Abs. 3 Satz 1 genannten Beschreibungen die räumliche Ausdehnung und Dauer der Videoaufzeichnung, die Maßnahmen nach Abs. 2 und die vorgesehenen Auswertungen mitzuteilen.

6.1.2 Anwendbarkeit des Art. 21a BayDSG auf Kameraattrappen

Da bayerische öffentliche Stellen gelegentlich auch Kameraattrappen installieren, stellt sich die Frage, ob Art. 21a BayDSG auch in diesen Fällen anwendbar ist. Ich vertrete dazu die folgende Auffassung:

Die bereichsspezifische Regelung in Art. 21a BayDSG ist eine unmittelbare Folge der Entscheidung des Bundesverfassungsgerichts vom 23. Februar 2007 –

1 BvR 2368/06 – wonach eine Videoüberwachung öffentlicher Orte und Einrichtungen eine erhebliche Grundrechtsbeeinträchtigung darstellt und deshalb nicht auf die allgemeinen Bestimmungen des Bayerischen Datenschutzgesetzes zur Erhebung und Nutzung personenbezogener Daten gestützt werden kann. Das Bundesverfassungsgericht stellt in diesem Beschluss fest, dass maßgebend für die rechtliche Beurteilung der Intensität eines Eingriffs in das Recht auf informationelle Selbstbestimmung die Art der Beeinträchtigung ist. Insofern könne auch von Belang sein, ob die betroffenen Personen für die Maßnahme einen Anlass geben würden und wie dieser beschaffen sei. Verdachtslose Eingriffe mit großer Streubreite, bei denen zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stünden und den Eingriff durch ihr Verhalten nicht veranlasst hätten, würden grundsätzlich eine hohe Eingriffsintensität aufweisen.

Zwar findet bei Kameraattrappen keine tatsächliche Datenerhebung und -speicherung statt. Durch – deutlich sichtbar angebrachte – Kameraattrappen wird jedoch infolge der vorgetäuschten Überwachung, wie bei der tatsächlichen Überwachung, ein verhaltenslenkender Zweck verfolgt. Dieser Anpassungsdruck, der bei Kameraattrappen im öffentlichen Raum wie bei echten Videokameras zahlreiche Personen trifft, die für eine solche Maßnahme keinen Anlass gegeben haben, rechtfertigt und gebietet es, Art. 21a BayDSG hinsichtlich der Tatbestandsvoraussetzungen analog anzuwenden. Ich verweise dazu auch auf meinen, zusammen mit dem Staatsministerium des Innern, für Bau und Verkehr, erarbeiteten Leitfaden zur Videoüberwachung durch bayerische Kommunen, den das Ministerium mit Rundschreiben vom 9. April 2014 an die nachgeordneten Behörden zur Beachtung versandt hat. Den Leitfaden und meine Presseerklärung dazu habe ich auch auf meiner Homepage https://www.datenschutz-bayern.de veröffentlicht.

6.1.3 Hinreichende Gefahr für bestimmte Rechtsgüter

Art. 21a BayDSG soll die öffentlichen Stellen in die Lage versetzen, bestimmte Gefahren für die in Art. 21a Abs. 1 BayDSG genannten Rechtsgüter durch den Einsatz von Videoüberwachungsanlagen abzuwehren. Eine Gefahr liegt vor, wenn auf Grund bestimmter und konkreter Tatsachen der Schluss auf den Eintritt eines Schadens für die Rechtsgüter mit hinreichender Wahrscheinlichkeit gezogen werden kann. Der erforderliche Grad der Wahrscheinlichkeit hängt wiederum maßgebend von dem Gewicht des gefährdeten Rechtsguts und dem Ausmaß des drohenden Schadens ab. Maßgebend ist daher der Einzelfall. Allgemein kann man jedoch sagen, dass es grundsätzlich konkreter, ortsbezogener Tatsachen bedarf, aus denen man auf die künftige Schäden schlussfolgern kann.

In der Regel bedeutet dies, dass es bereits zuvor einschlägige Vorfälle am Ort der Kameraeinrichtung gegeben haben muss. Allerdings kann es auch zulässig sein, eine Gefährdungslage zu bejahen, wenn eine Situation typischerweise gefährlich ist. Es können also durchaus auch ausreichende Gefahrenlagen mit der allgemeinen Lebenserfahrung begründet werden (siehe 26. Tätigkeitsbericht 2014 unter Nr. 6.3). Hier ist allerdings Vorsicht geboten, weil die Versuchung naheliegt, solche Erfahrungssätze leichthin zu behaupten anstatt sie zu belegen und einen Bezug zum konkreten Überwachungsbereich festzustellen.

6.1.4 Nachweis der Gefahr durch eine Vorfallsdokumentation

Die gemeindliche Einschätzung, dass für die Rechtsgüter am konkreten Kamerastandort eine ausreichende Gefahr vorliegt, ist zu Kontrollzwecken zu dokumentieren. Die überprüfbaren Tatsachen sind plausibel darzulegen. Hierzu empfehle ich, eine sogenannte Vorfallsdokumentation anzulegen. Um die Kommunen hierbei zu unterstützen, habe ich auf meiner Homepage https://www.datenschutz-bayern.de ein entsprechendes Muster samt Erläuterungen eingestellt. Im Rahmen der Vorfallsdokumentation sind die Anzeigen, Polizeiberichte, Beschwerden, Beschädigungen und andere Ereignisse zu dokumentieren, damit der Umfang, die Häufigkeit und die Intensität der Schadensereignisse, die nun die Gefahrenprognose tragen sollen, dargelegt werden können. Der allgemeine Verweis, an diesem oder jenem Ort sei „schon mal etwas passiert", vage Erinnerung des Verwaltungspersonals oder die allgemeine Annahme eines vermeintlichen Unsicherheitsgefühls der Bevölkerung stellen keine ausreichende Plausibilisierung einer Gefahr dar.

6.2 Digitalisierung von archivierten Personenstandsdaten

Durch Berichterstattung in der Tagespresse wurde ich darauf aufmerksam, dass eine große bayerische Stadt plant, in ihrem Stadtarchiv aufbewahrte Personenstandsregister und Polizeimeldebögen digitalisieren zu lassen. Die Stadt verfolgt das Ziel, die auf Papier vorliegenden Bestände konservatorisch zu schonen und eine bequeme Einsichtnahme zu ermöglichen. In den Personenstandsregistern sind Geburten, Eheschließungen und Sterbefälle seit dem Jahr 1876 beurkundet. Auf Grund der bestehenden Anzeigepflichten ist das Register seinem Anspruch nach lückenlos. Bei den Polizeimeldebögen handelt es sich um die Bestandteile eines weiteren Registers, das Vorläufer des heutigen Melderegisters war.

Einen solchen Datenbestand zu digitalisieren, kostet viel Geld. Die Stadt beabsichtigte daher, einen externen Anbieter in das Projekt einzubinden. Solche Kooperationen werden scheinbar kostenfrei angeboten. Allerdings verlangen die externen Anbieter üblicherweise Nutzungsrechte, um die entstehenden Digitalisate (das sind die Dateien, in welche die einzelnen Registereinträge, etwa Seiten in einem Geburtenbuch, mittels Scanner überführt werden) im eigenen Interesse verwerten zu können. Ein am Markt prominent vertretener Anbieter nutzt die Digitalisierung beispielsweise als Grundlage für die „Bestückung" einer genealogischen Datenbank. Für diese Datenbank eröffnet er dann entgeltlich Recherchemöglichkeiten.

Aus datenschutzrechtlicher Sicht ist an einem solchen Projekt insbesondere problematisch, dass Personenstandsregister Aussagen (auch) über heute lebende Personen zulassen, weil aus ihnen familiäre Zusammenhänge bei bestimmten Merkmalen erschlossen werden können.

Nach Einholung einer Stellungnahme der Stadt und eingehender Prüfung gelangte ich zu dem Ergebnis, dass das konkrete Projekt **unzulässig ist**.

Die Entscheidung für ein solches Projekt bedarf nach meiner Auffassung einer **parlamentsgesetzlichen Ermächtigung,** die das geltende Recht gegenwärtig nicht vorsieht . Im Einzelnen ist zu bemerken:

— Verfassungsrechtlicher Maßstab für die Beurteilung von Digitalisierungsprojekten, die Personenstandsregister betreffen, ist ein von Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz für die Bundesrepublik Deutschland (GG) geschütztes, hier so bezeichnetes **Recht auf Vertraulichkeit von Abstammungsinformationen**. Dieses Recht ergibt sich aus einer Gesamtschau mehrerer Teilaussagen des allgemeinen Persönlichkeitsrechts. Das Grundrecht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG gewährleistet Rechte auf informationelle Selbstbestimmung sowie auf Kenntnis der eigenen Abstammung. Das Recht auf informationelle Selbstbestimmung bewahrt die Einzelnen vor der unbeschränkten Weitergabe ihrer persönlichen Daten durch öffentliche Stellen. Das Recht auf Kenntnis der eigenen Abstammung verweist darauf, dass insbesondere Informationen über die biologische Einbindung in einen familiären Zusammenhang solche persönlichen Daten sind. Das Grundrecht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG schützt ferner die eigene Darstellung in der Öffentlichkeit, auch im Hinblick auf die Herkunft. Familiäre Beziehungen sind für die Beschreibung der „Herkunft“ wesentlich. Daher ist die Entscheidung, inwiefern die entsprechenden Informationen in die Öffentlichkeit getragen werden, den Einzelnen und nicht öffentlichen Stellen zugeordnet.

  Das Recht auf Vertraulichkeit von Abstammungsinformationen greift zeitlich zwar nicht „ewig“ in die Vergangenheit zurück, immerhin aber so weit, wie dies erforderlich ist, Zuordnungen von persönlichen Daten nicht mehr lebender Vorfahren zu heute lebenden Personen verlässlich zu unterbinden. Dieser Zeitraum ist so zu bemessen, dass bei typisierender Betrachtungsweise eine für die „Unterbrechung“ von Zuordnungen ausreichende Zahl generativer Schritte stattgefunden hat.

— Der durch das Recht auf Vertraulichkeit von Abstammungsinformationen vermittelte Schutz verfolgt keinen Selbstzweck, sondern das **Ziel, die Einzelnen vor einer unerwünschten „Zuschreibung“ von persönlichen Daten ihrer Vorfahren zu schützen**.

  Hier ist insbesondere zu berücksichtigen, dass die Eintragungen in Personenstandsregistern je nach Rechtsstand Angaben zur **Religionszugehörigkeit**, zum **Beruf** und zur **Wohnanschrift** der Beurkundungsbetroffenen ausweisen. Bei Sterbefällen wird neben dem erreichten **Lebensalter** auch der **Ort des Todes** ersichtlich, unter der Geltung des Personenstandsgesetzes von 1937 zudem die **Todesursache** (siehe dort § 38).

  Gerade bei Erfassung eines großstädtischen Datenbestands können generationsübergreifend familiäre Kontinuitäten sichtbar gemacht werden. Auf dieser Grundlage lassen sich zu **heute lebenden Personen** etwa Schlüsse auf die **Religionszugehörigkeit** ziehen, ferner können **Vermögensverhältnisse von Familien** rekonstruiert werden. So ließe sich – gegebenenfalls nach Verknüpfung mit anderen bereits öffentlich zugänglichen Erkenntnismitteln oder auch den „Polizeimeldebögen“ – die Zugehörigkeit zu einer Familie erkennen, in der viele Mitglieder bestimmte „einkommensstarke“ Berufe ausüben, oder zu einer Familie, in der Grundbesitz oder Gewerbebetriebe vererbt werden.

  Ein **familiär gesteigertes Risiko von Frühversterben** kann ebenso zutage treten wie **familiäre Häufungen von Todesfällen in Einrichtungen wie Nervenheil- oder Justizvollzugsanstalten**. Soweit bei der Beurkundung

das Personenstandsgesetz von 1937 zugrunde lag und deshalb die Todesursache ausgewiesen ist, können zudem konkrete **erbbiologische Belastungen** offenbar werden. Gesundheitsbezogene Auswertungsmöglichkeiten mögen bei einer genealogischen Datenbank zunächst nicht im Vordergrund stehen, werden durch die Digitalisierung aber geschaffen. Insofern kann nicht überraschen, dass zumindest ein einschlägiger Anbieter derzeit ein **Angebot erbbiologischer Informationen** erprobt.

Eine Überlassung von Personenstandsregistern an einen kommerziellen Anbieter wäre vor diesem Hintergrund als **Eingriff in das Recht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG** zu werten. Entsprechenden Bedenken begegnet sowohl eine Verpflichtung hierzu wie auch die Grundsatzentscheidung für ein Digitalisierungsprojekt, das eine solche Überlassung vorsieht. Der Eingriff hätte ein **erhebliches Gewicht**.

In diesem Zusammenhang ist zum einen festzuhalten, dass die einschlägigen Geschäftsmodelle erkennbar auf ein Ideal von „Vollständigkeit“ angelegt sind. Die Datenbanken sind für die Kundinnen und Kunden umso „interessanter“, je mehr Elemente eines bisher im Verborgenen liegenden Stammbaums aufgedeckt werden können. Für das Gewicht des Eingriffs ist vor diesem Hintergrund eine „**Summenwirkung**“ zu berücksichtigen: Auf Grund einer Vielzahl systematischer und geschlossener „Datenabgriffe“ werden Verknüpfungs- und Auswertungsmöglichkeiten geschaffen, die zuvor nicht bestanden und eine eigenständige Gefährdung für die Rechte heute lebender Personen begründen.

Weiterhin fällt der Einbezug auch der „Polizeimeldebögen“ ins Gewicht. Deren „Einknüpfung“ in das „Datennetz“ sorgt dafür, dass für die personenstandsrechtlich erfassten Bürgerinnen und Bürger zusätzlich mindestens auch noch innerstädtische „Umzugsbiografien“ rekonstruierbar werden. Entsprechendes gilt für die übrigen Personen, die nicht in den Personenstandsregistern der Stadt erfasst sind, weil sie nicht dort geboren oder verstorben sind beziehungsweise geheiratet haben. Zudem können – über den personenstandsrechtlich verfestigten Bereich hinaus – Nachbarschaften ermittelt werden. Problematisch erscheint dabei insbesondere der durch das geltende Recht aus guten Gründen nicht hergestellte **Registerverbund** von Personenstands- und Melderegister.

Schließlich bestehen Zweifel, ob Verträge mit kommerziellen Anbietern eine Zweckbindung dahin enthalten, dass die Digitalisate nur für die genealogische Arbeit von Privatpersonen zur Verfügung gestellt werden dürfen, und ob sie Beschränkungen zu Umfang und Kriterien einer Indizierung formulieren. Vielmehr erscheint nicht ausgeschlossen, dass der Anbieter vertraglich berechtigt sein soll, die Digitalisate auch außerhalb eines solchen Zwecks zu nutzen, insbesondere kommerziell weiterzuverwerten, und sie beliebig auswertbar zu machen. Auf diese Weise würde ein nicht übersehbares, auch zeitlich uneingeschränktes **Missbrauchsrisiko** geschaffen, das sich bei anfallenden gesundheitsbezogenen Angaben etwa in einer **„Kooperation“ mit Versicherungen oder Arbeitgebern heute lebender Personen** nachteilig bemerkbar machen könnte.

– Der Eingriff ist nach geltendem Recht **nicht gerechtfertigt**. Insbesondere kann die Überlassung der Personenstandsregister nicht auf Art. 10 Abs. 2 Bayerisches Archivgesetz (BayArchivG) gestützt werden. Die Erstellung

kompletter elektronischer Abbilder von „analogen Datenbanken“ mit dem Ziel, im Verbund mit entsprechenden Abbildern aus anderen Archiven ein „Meta-Archiv“ zu errichten, ist bereits keine Benützung. Art. 10 Abs. 2 BayArchivG verschafft einen Benützungsanspruch, über dessen Erfüllung das zuständige Archiv entscheidet. Bei dieser Entscheidung sind nach Maßgabe des gesetzlichen Prüfprogramms Vertraulichkeitsinteressen zu verarbeiten. Das entstehende „Meta-Archiv“ kann weder die behördliche Entscheidung über den Zugang sicherstellen, noch ist es verpflichtet, Vertraulichkeitsinteressen zu berücksichtigen. Es wird vielmehr den Zugang nach den Grundsätzen ökonomischer Opportunität organisieren. Zu einem solchen „Austausch“ des Zugangsregimes hat der Gesetzgeber die Archive nicht ermächtigt.

6.3 Einbau und Betrieb „intelligenter“ Wasserzähler

Im Berichtszeitraum haben sich zahlreiche Bürgerinnen und Bürger bei mir darüber beschwert, dass Stadtwerke und Zweckverbände dazu übergehen, bisherige „analoge“ Wasserzähler durch „intelligente“ Wasserzähler – auch gegen ihren Willen – zu ersetzen.

Auf dem Markt werden verschiedene Modelle an „intelligenten“ Wasserzählern angeboten. Im Wesentlichen speichern sie aber nach den mir bisher vorliegenden Informationen zumindest den jeweiligen Wasserdurchfluss und -verbrauch in kurzen Zeitabschnitten (beispielsweise mehrfach pro Minute), alle 24 Stunden den Zählerstand für mehrere Hundert Tage im sogenannten Tagesregister, einmal im Monat zu einem Stichtag den jeweiligen Monatsverbrauch für mehrere Jahre im sogenannten Monatsregister und Informationen zum Höchst- und Mindestdurchfluss, mit der Folge, dass bei atypischen Abweichungen das Gerät eine Fehlermeldung generiert (beispielsweise „Verdacht auf Rohrbruch“).

Diese gespeicherten Daten sind jedenfalls über ein Lesegerät vor Ort am Wasserzähler auslesbar. Ferner senden die „intelligenten“ Wasserzähler innerhalb eines festgelegten Zeitraums (beispielsweise mehrfach pro Minute) Signale aus, die von außerhalb des Gebäudes erfasst und ausgewertet werden können. Dies geschieht regelmäßig ohne Mitwirkung und ohne Kenntnis der Verbraucherinnen und Verbraucher. Typischerweise werden offenbar nicht alle gespeicherten Daten übermittelt, sondern insbesondere „nur“ der aktuelle Zählerstand, der Zählerstand des vergangenen Monats und mögliche Fehlermeldungen.

Die Auslesung von außen findet durch den Wasserversorger zum einem jeweils zum Zwecke der Jahresabrechnung statt, zum anderen, wenn er in konkreten Verdachtsfällen Wasserlecks aufspüren möchte.

Ich habe mich anlässlich der bei mir erhobenen Beschwerden mit der – umstrittenen – rechtlichen Zulässigkeit insbesondere einer „Zwangsdigitalisierung“ näher befasst und versucht, in einem Diskussionsprozess mit dem für die Kommunalaufsicht zuständigen Innenministerium zu einer gemeinsamen Rechtsauffassung zu gelangen.

Das ist im Wesentlichen gelungen:

6.3.1 Notwendigkeit einer formell-gesetzlichen Rechtsgrundlage

Für die Beurteilung der Zulässigkeit des Einbaus und Betriebs von „intelligenten“ Wasserzählern stellt sich zunächst aus Sicht des Verfassungsrechts die Frage, ob es hierfür einer formell-gesetzlichen Rechtsgrundlage – also einer Entscheidung des Parlamentsgesetzgebers – bedarf oder ob möglicherweise entsprechende Satzungsregelungen vor Ort genügen. Eine formell-gesetzliche Rechtsgrundlage gibt es im Moment nicht.

Der rechtliche Hintergrund für diese Frage ist, dass die ständige Rechtsprechung des Bundesverfassungsgerichts den Gesetzgeber (das Parlament) verpflichtet, die für Grundrechtseingriffe **wesentlichen** Regelungen **selbst** und **durch Gesetz** zu treffen. Das Parlament hat dabei nicht nur „irgendein“ Gesetz zu beschließen, sondern muss in diesem Gesetz auch die wichtigsten Aspekte inhaltlich regeln.

Im vorliegenden Zusammenhang lautet demnach die **entscheidende Frage**: Betrifft der Einbau und Betrieb von „intelligenten“ Wasserzählern eine so **wesentliche** Frage, dass es zunächst einer Entscheidung des Parlamentsgesetzgebers bedarf oder eine nur satzungsmäßige Entscheidung vor Ort genügt?

Diese Frage lässt sich für den Einbau und Betrieb von jedem „intelligenten“ Wasserzähler nicht pauschal beantworten. Die Antwort hängt davon ab, wie intensiv der mit dem Einbau und Betrieb verbundene Eingriff in das **Grundrecht auf informationelle Selbstbestimmung** ausfällt. Die Intensität des Eingriffs wiederum hängt von den konkreten Funktionsmöglichkeiten des jeweiligen Zählers ab, insbesondere davon, welche Daten wie lange gespeichert werden.

Beim Einsatz von „intelligenten“ Wasserzählern geht es jedenfalls um Eingriffe in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz – GG), möglicherweise sogar um Eingriffe in die Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG). Das informationelle Selbstbestimmungsrecht hat das Bundesverfassungsgericht im bekannten Volkszählungsurteil im Jahr 1983 entwickelt. Es gibt jedem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Das informationelle Selbstbestimmungsrecht ist im Zusammenhang mit „intelligenten“ Wasserzählern deshalb betroffen, weil sämtliche im Wasserzähler gespeicherten Verbrauchsdaten einen Personenbezug aufweisen und die Bildung eines Verbrauchsprofils ermöglichen.

Auch wenn die Frage nicht pauschal zu beantworten ist, so ist jedenfalls dann eine formell-gesetzliche Grundlage notwendig, wenn

— die Bürgerinnen und Bürger die **Pflicht** auferlegt bekommen, den Einbau und Betrieb eines „intelligenten“ Wasserzählers zu dulden, und

— durch den Wasserzähler personenbezogene Daten erhoben werden, die **nicht zu Abrechnungszwecken notwendig** sind, insbesondere wenn eine sehr „kleinteilige“ Erfassung von Verbrauchswerten mit einer langen Speicherdauer zusammentrifft, oder

— solche personenbezogenen Daten in regelmäßigen Abständen ohne Einflussmöglichkeit der Betroffenen „auf die Straße“ übertragen und über die Ferne **unbemerkt und ohne Mitwirkung der Betroffenen abgelesen** werden können.

Liegen diese Voraussetzungen vor, so bedeutet das, dass es eine Verpflichtung vor Ort zum Einbau und Betrieb solcher Zähler erst dann geben darf, wenn der **Gesetzgeber** eine **konkrete** Regelung über die Einsatz- und Betriebsvoraussetzungen von „intelligenten" Wasserzählern geschaffen hat. **Im Moment gibt es eine solche spezielle gesetzliche Grundlage nicht.** Die manchmal vor Ort geschaffenen Regelungen für „intelligente" Wasserzähler **in einer Satzung** genügen **nicht.**

6.3.2 Freiwilliger Einbau und Betrieb von „intelligenten" Wasserzählern

Umgekehrt wird man **keine** gesonderte gesetzliche Rechtsgrundlage verlangen müssen, wenn der Einsatz bei den Betroffenen **freiwillig** erfolgt. Dann reicht eine Satzungsregelung vor Ort aus.

Die Freiwilligkeit hinsichtlich des Betriebs eines solchen Zählers ist dabei freilich mit Schwierigkeiten im Falle eines Eigentümer- und/oder Mieterwechsels verbunden und erscheint daher nicht sonderlich praxisrelevant.

Von größerer Bedeutung könnte die Freiwilligkeit allerdings sein, wenn jedenfalls die Übertragung der personenbezogenen Daten „auf die Straße" und die damit verbundene unbemerkte Fernablesemöglichkeit durch die jeweils Betroffenen jederzeit leicht an- und ausgeschaltet werden könnte (und sie hierüber belehrt worden sind). Es wäre daher beispielsweise datenschutzrechtlich nicht bedenklich, wenn ein Funksignal zum angekündigten Ablesetermin freiwillig aktiviert wird. So wäre eine „unbürokratische" Fernablese ohne Beeinträchtigung des informationellen Selbstbestimmungsrechts möglich.

6.3.3 Fazit

Der Parlamentsgesetzgeber hat zu entscheiden, ob es Gründe gibt, eine Rechtsgrundlage für einen „unfreiwilligen" Einbau und Betrieb von „intelligenten" Wasserzählern zu schaffen. Bis dahin werde ich die weitere Entwicklung in den Gemeinden sorgfältig beobachten und insbesondere darauf hinwirken, dass jedenfalls keine solchen Wasserzähler mehr eingebaut werden, für die eine formell-gesetzliche Rechtsgrundlage erforderlich ist.

6.4 Bestellung eines behördlichen Datenschutzbeauftragten für mehrere öffentliche Stellen

Nach Art. 25 Abs. 2 BayDSG sind die meisten öffentlichen Stellen verpflichtet, einen behördlichen Datenschutzbeauftragten zu bestellen. Viele öffentliche Stellen – wie zum Beispiel kleine Gemeinden – haben aber nur wenige Bedienstete. Andere widmen sich Tätigkeitsbereichen, die nicht schwerpunktmäßig mit personenbezogener Datenverarbeitung verbunden sind. Die sachgerechte Wahrnehmung der Aufgaben eines behördlichen Datenschutzbeauftragten erfordert ein hohes Maß von Fachkunde hinsichtlich rechtlicher wie technisch-organisatorischer Anforderungen des Datenschutzes. Die nötigen Fähigkeiten vorzuhalten, ist für manche öffentliche Stellen nicht wirtschaftlich möglich. Vor diesem Hintergrund lässt das Gesetz die Bestellung gemeinsamer behördlicher Datenschutzbeauftragter für mehrere öffentliche Stellen zu.

Art. 25 BayDSG Sicherstellung des Datenschutzes, behördliche Datenschutzbeauftragte
(2) [1]Öffentliche Stellen, die personenbezogene Daten mit Hilfe von automatisierten Verfahren verarbeiten oder nutzen, haben einen ihrer Beschäftigten zum behördlichen Datenschutzbeauftragten zu bestellen. [2]Mehrere öffentliche Stellen können gemeinsam einen ihrer Beschäftigten bestellen; bei Staatsbehörden kann die Bestellung auch durch eine höhere Behörde erfolgen.

Im Berichtszeitraum war ich unter anderem mit zwei (geplanten) Kooperationen von Landkreisen mit kreisangehörigen Gemeinden, Verwaltungsgemeinschaften und Zweckverbänden befasst. Bei solchen Kooperationen sollte stets zunächst ein **Konzept** ausgearbeitet werden, das sich zur Art und Weise der Zusammenarbeit und zum Ressourceneinsatz verhält. Auf dieser Grundlage lässt sich dann eine **Zweckvereinbarung** erarbeiten. Ich habe den betroffenen öffentlichen Stellen aus datenschutzrechtlicher Sicht folgende Hinweise gegeben:

— Der gemeinsame behördliche Datenschutzbeauftragte wird nach Art. 25 Abs. 2 Satz 2 Halbsatz 1 BayDSG gemeinsam bestellt. Nach meiner Auffassung liegt eine **gemeinsame Bestellung** nur vor, wenn **alle Mitglieder der „Bestellungsgemeinschaft"** für sich den Bestellungsakt vornehmen. Dafür ist jeweils ein auf eine konkrete Person bezogener Rechtsakt des kollegialen Hauptorgans (etwa des Gemeinderats) erforderlich. Nicht zulässig ist ein Modell, in welchem der Landkreis kreisangehörigen Gemeinden gegen anteilige Kostenerstattung einen gemeindlichen behördlichen Datenschutzbeauftragten stellt, der beim Kreis beschäftigt ist, nicht jedoch auch für diesen die Aufgabe des behördlichen Datenschutzbeauftragten wahrnimmt.

— Die in einem Projekt gefundene Lösung, für den gemeinsamen behördlichen Datenschutzbeauftragten bei jeder der beteiligten öffentlichen Stellen einen **„Vor-Ort-Vertreter"** zu bestellen, habe ich positiv bewertet.

  Voraussetzung für eine solche Lösung ist allerdings, dass sich die Zusammenarbeit des gemeinsamen behördlichen Datenschutzbeauftragten mit seinen „Vor-Ort-Vertretern" nicht als eine reine Verhinderungsvertretung gestaltet, sondern dass sich die kommunale „Bestellungsgemeinschaft" als ein „**kommunales Netzwerk Datenschutz**" formiert. Erforderlich ist dabei eine klare Aufgabenverteilung zwischen dem gemeinsamen behördlichen Datenschutzbeauftragten und seinen „Vor-Ort-Vertretern". Der gemeinsame behördliche Datenschutzbeauftragte könnte im regelmäßigen **Erfahrungsaustausch** mit seinen „Vor-Ort-Vertretern" relevantes Datenschutzwissen in die Verwaltungen weitergeben und von ihnen Rückmeldungen zu aktuellen Problemstellungen erhalten. Die „Vor-Ort-Vertreter" könnten dann zum einen als **Multiplikatoren**, zum anderen als erste Ansprechpartner wirken und so eine **Schlüsselfunktion** zwischen ihrer jeweiligen öffentliche Stelle und dem gemeinsamen behördlichen Datenschutzbeauftragten einnehmen. Ein „kommunales Netzwerk Datenschutz" beruht auf dem Gedanken einer **Aufgabenteilung**. Die Mitglieder der „Bestellungsgemeinschaft" finanzieren gemeinsam eine Fachkraft, ohne aber den Datenschutz thematisch zu „entsorgen".

  Das „kommunale Netzwerk Datenschutz" ist in **einer Zweckvereinbarung** zu konkretisieren. In ihr ist zunächst klar zu regeln, dass alle beteiligten öffentlichen Stellen die Funktion „behördlicher Datenschutzbeauftragter"

in **gemeinsamer Verantwortung** gewährleisten. Dabei hat eine Stelle die Beschäftigung einer datenschutzrechtlichen Fachkraft zu übernehmen, um eine professionelle Datenschutzkontrolle zu gewährleisten. Zu regeln ist ferner, dass diese Fachkraft die Funktion des gemeinsamen behördlichen Datenschutzbeauftragten im Zusammenwirken mit ihren Vor-Ort-Vertretern wahrnimmt. Daran anknüpfend ist die Figur der Fachkraft und ihrer „Vor-Ort-Vertreter" nach den **Aufgaben und Befugnissen** zu beschreiben, weiterhin ist festzulegen, auf welche Art und Weise sich die **Kooperation** des gemeinsamen behördlichen Datenschutzbeauftragten mit seinen Vor-Ort-Vertretern gestalten soll. Ich empfehle, die Kooperation für die wichtigsten „**Verwaltungsprodukte**" des gemeinsamen behördlichen Datenschutzbeauftragten zu **standardisieren**, um ein „Herausreden" auf die eigene Unzuständigkeit von vornherein auszuschließen.

— Die Aufgabenteilung ist auch Voraussetzung dafür, **dass kommunalrechtliche Bedenken gegen eine Kooperation von Landkreis und Gemeinden** gegen den Abschluss der Zweckvereinbarung zurückgestellt werden können. Zur gemeinsamen Aufgabenerledigung „verbünden" sich hier kommunale Körperschaften unterschiedlicher Stufen. So nimmt der behördliche Datenschutzbeauftragte des Landkreises beziehungsweise staatlichen Landratsamts seine Funktion im Hinblick auf den Tätigkeitsbereich dieser Stellen wahr, der behördliche Datenschutzbeauftragte einer Gemeinde in Bezug auf deren Wirkungskreis. Ein solches Bündnis mit ungleichartigen Aufgaben entspricht nicht dem gesetzlichen Leitbild. Im Hinblick darauf hat der Gesetzgeber den Fall einer Übernahme von Gemeindeaufgaben durch den Landkreis an die (engen) Voraussetzungen des Art. 52 Landkreisordnung für den Freistaat Bayern gebunden.

— Soll ein gemeinsamer behördlicher Datenschutzbeauftragter eingeführt werden, ist besonders auf das **Arbeitszeitdeputat** zu achten. Ein behördlicher Datenschutzbeauftragter hat nicht die Funktion eines „Feigenblatts", sondern seine gesetzlichen Aufgaben wahrzunehmen. Sein Wert für die betreuten öffentlichen Stellen liegt insbesondere darin, bei datenschutzrechtlichen Problemen in kurzer Zeit qualifiziert Beratung erlangen zu können. Dies erfordert eine gute Kenntnis der Situation an Ort und Stelle, auch was die eingesetzten Fachverfahren und ihre jeweiligen Eigenheiten betrifft.

  Im Rahmen des Konzepts sollten für die Sicherstellung der Kontrollfunktion sowie eines bedarfsgerechten Beratungsangebots geeignete Vorkehrungen getroffen werden. Nach meiner Auffassung bietet sich eine **„Experimentierphase" mit Evaluierung** nach angemessener Zeit (etwa: zwei Jahre) an. Dabei wäre unter Mitwirkung aller öffentlichen Stellen der „Bestellungsgemeinschaft" zu ermitteln, wie sich die Beratungs- und Kontrollbedarfe entwickelt haben, ob die aufgetretenen „Beratungsfälle" innerhalb überschaubarer Zeit und mit zufriedenstellender Qualität abgearbeitet und welche Kontrollaktivitäten entfaltet werden konnten, weiterhin, inwiefern es möglich war, aus der Vergangenheit überkommene datenschutzrechtliche Defizite festzustellen und zu beseitigen. Eine solche Evaluierung sollte in der Zweckvereinbarung geregelt und auch hinsichtlich des Zeitplans sowie der wesentlichen Parameter bereits vorab festgelegt werden.

– Ich empfehle außerdem, in der Zweckvereinbarung für den gemeinsamen behördlichen Datenschutzbeauftragten die **Pflicht zur Erstellung eines Tätigkeitsberichts** vorzusehen.

6.5 Geschwindigkeitsanzeigetafeln

Mit Geschwindigkeitsanzeigetafeln wollen Sicherheitsbehörden Fahrzeugführerinnen und -führern die aktuell gefahrene Geschwindigkeit bewusst machen und sie zu einem verkehrsgerechten Verhalten anhalten. Da die Geschwindigkeit aber auch anwesenden Dritten angezeigt wird, stellt sich die Frage nach der datenschutzrechtlichen Zulässigkeit dieses Vorgangs. Im Ergebnis stellt das Anzeigen der Geschwindigkeit eine zulässige Datenübermittlung dar.

Dabei ist zunächst zu prüfen, ob mit der Anzeige der Geschwindigkeit des Kraftfahrzeugs der Begriff des personenbezogenen Datums erfüllt wird. Personenbezogene Daten sind nach Art. 4 Abs. 1 BayDSG Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen. Die Anzeige der Geschwindigkeit trifft eine Aussage über das Fahrverhalten. Jedenfalls Personen, die die Fahrzeugführerin oder den Fahrzeugführer aus anderem Zusammenhang kennen, können diese Aussage auch ihr oder ihm konkret zuordnen. Daher ist die Anzeige der Geschwindigkeit jedenfalls manchmal ein personenbezogenes Datum.

Die Anzeige der Geschwindigkeit wird auch im Sinne des Art. 4 Abs. 6 Satz 2 Nr. 3 Buchst. a BayDSG übermittelt, da sie für anwesende Dritte erkennbar ist.

Gesetzlich zugelassen ist eine solche Übermittlung an nicht-öffentliche Stellen nach Art. 19 Abs. 1 Nr. 1 BayDSG, wenn die Übermittlung zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und – verkürzt formuliert – die Voraussetzungen des Art. 17 BayDSG vorliegen. Dies ist der Fall:

– Die Anzeige der Geschwindigkeit dient dazu, auf die Beachtung der jeweils bestehenden Geschwindigkeitsbegrenzung hinzuweisen und so einerseits Ordnungswidrigkeiten vorzubeugen (die Anzeigetafeln stehen verbreitet kurz vor Beginn der entsprechenden Geschwindigkeitszone) und andererseits die mit erhöhter Geschwindigkeit verbundenen Gefahren für andere Verkehrsteilnehmerinnen und -teilnehmer zu verringern. Dieser präventive Charakter macht die Geschwindigkeitsanzeige insgesamt zu einem Instrument der Gefahrenabwehr. Für Gefahrenabwehr sind auch die Gemeinden zuständig, die vielfach solche Anzeigetafeln aufstellen. Die Tafeln dienen insoweit der gemeindlichen Aufgabenerfüllung.

– Die Anzeige kann auch erforderlich sein. Zwar können unter Umständen auch Dritte erkennen, wie schnell eine konkrete (ihnen bekannte) Person fährt, doch wären Alternativen, die die Kenntnisnahme Dritter vermeiden, insgesamt mit erheblicheren Grundrechtseingriffen und datenschutzrechtlich relevanten Maßnahmen verbunden. Denn würde von der Gemeinde verlangt, die jeweilige fahrzeugführende Person individuell anzusprechen, müsste sie diese – auch für jedermann sichtbar – anhalten. Alternativ müsste sie über eine Speicherung des Kennzeichens die Halterin oder den Halter ermitteln und darüber hinaus die konkrete fahrzeugführende Person feststellen. Solche Maßnahmen wären jeweils Eingriffe, die keineswegs

milder als die Geschwindigkeitsanzeige sind. Dabei ist zu bedenken, dass es Passantinnen und Passanten mangels entsprechenden Zusatzwissens zumeist gar nicht möglich sein wird, einen Personenbezug herzustellen und private Halterabfragen nicht ohne weiteres möglich sind (vgl. § 39 Straßenverkehrsgesetz).

— Die Voraussetzungen des Art. 17 Abs. 1 Nr. 2 BayDSG liegen ebenfalls vor, weil die Daten gerade für den Zweck erhoben wurden, für den sie auch übermittelt werden, also kein Fall einer (erhöhten Anforderungen unterliegenden) Zweckänderung vorliegt.

6.6 Datenschutz bei Bürgerbegehren

Durch eine Beschwerde wurde mir bekannt, dass eine Gemeinde im Rahmen der Prüfung der Zulässigkeit eines Bürgerbegehrens die Unterzeichnerinnen und Unterzeichner angerufen und befragt hat. Ziel der Befragung war vornehmlich herauszufinden, ob sie das Anliegen des Bürgerbegehrens verstanden hatten. Nach Mitteilung der Gemeinde wurde das Ergebnis der Befragung auch bei der Zulässigkeitsprüfung nach Art. 18a Abs. 8 Satz 1 Gemeindeordnung (GO) berücksichtigt.

Diese Nutzung der personenbezogenen Daten der Unterzeichnerinnen und Unterzeichner ist unzulässig. Es handelt sich um einen gravierenden Verstoß der Gemeinde gegen kommunal- und datenschutzrechtliche Vorschriften, den ich auch deshalb förmlich beanstandet habe, weil der ordnungsgemäße Umgang mit eingereichten Unterschriften eines Bürgerbegehrens seit langem geklärt ist (siehe nur meinen 17. Tätigkeitsbericht 1996 unter Nr. 8.4.2 und meinen 21. Tätigkeitsbericht 2004 unter Nr. 11.11).

Gemeinden müssen bei der Auswertung der für ein Bürgerbegehren abgegebenen Unterschriftenlisten den Grundsatz der Zweckbindung (Art. 17 Abs. 1 Nr. 2 BayDSG) strikt beachten. Die Unterschriften dürfen ausschließlich hinsichtlich der Frage ausgewertet werden, ob das Bürgerbegehren von einer ausreichenden Zahl antragsberechtigter Gemeindebürger (Art. 18a Abs. 6 GO) unterschrieben worden ist. Dies kann mit Hilfe des nach Art. 18a Abs. 5 Satz 2 GO anzulegenden Bürgerverzeichnisses überprüft werden.

Eine Kontaktaufnahme mit den Unterzeichnerinnen und Unterzeichnern ist demgegenüber hierfür nicht erforderlich. Es ist insbesondere **unzulässig**, bei den Unterzeichnerinnen und Unterzeichnern inhaltliche Aspekte des Bürgerbegehrens abzufragen oder mit diesen zu erörtern. Es steht der Gemeinde nicht zu, mit Hilfe der ihr unweigerlich zukommenden Amtsautorität die Motivation und Gründe für eine Unterzeichnung des Bürgerbegehrens zu erforschen. Darüber hinaus ist es nicht ersichtlich, inwiefern die durch die Befragungen gewonnenen Erkenntnisse für die Beurteilung der Zulässigkeit des Bürgerbegehrens relevant sein könnten.

6.7 Datenübermittlung zur Bekämpfung von Sozialleistungsmissbrauch

Die behördliche Datenschutzbeauftragte einer Stadt hat sich an mich mit der Frage gewandt, ob städtische Ämter, die bei Bürgerinnen und Bürgern Sozialleistungsbetrug vermuten, das Sozialamt der Stadt darüber informieren dürfen.

Soweit keine vorrangigen bereichsspezifischen Datenschutzbestimmungen anwendbar sind, richtet sich eine Datenweitergabe nach den allgemeinen Vorschriften des Bayerischen Datenschutzgesetzes. Die Weitergabe von Daten innerhalb der speichernden Stelle (hier von einem städtischen Amt an das Sozialamt der Kommune) stellt nach Art. 4 Abs. 7 BayDSG eine Datennutzung dar. Diese ist nach Art. 17 BayDSG (nur) zulässig, wenn erstens die Weitergabe zur Erfüllung der in der Zuständigkeit der empfangenen Stelle liegenden Aufgaben erforderlich ist (Art. 17 Abs. 1 Nr. 1 BayDSG) und zweitens die Voraussetzungen für eine Zweckänderung nach Art. 17 Abs. 1 Nr. 2, Abs. 2 bis 4 BayDSG vorliegen.

Grundsätzlich ist es Aufgabe der Sozialbehörden, Sozialleistungsmissbrauch zu bekämpfen.

Im vorliegenden Fall waren im Bereich des Melde- und Passwesens Hinweise auf einen Sozialleistungsmissbrauch bekannt geworden. Eine Weitergabe dieser Hinweise an den Sozialbereich kann dann erforderlich und damit zulässig sein, wenn der Sozialleistungsmissbrauch entweder sicher feststeht oder jedenfalls mit hinreichender Wahrscheinlichkeit anzunehmen ist. Sofern die Melde- oder Passbehörde nicht selbst beurteilen kann, ob die Weitergabe im konkreten Fall nach diesen Maßstäben zur Aufgabenerfüllung der Sozialbehörden erforderlich ist, kann sie – in einem ersten Schritt – ihre Erkenntnisse in anonymisierter Form bei den Sozialbehörden vortragen und anfragen, ob nähere Informationen über den Fall zur Überprüfung eines Sozialleistungsmissbrauchs benötigt werden. Bejahendenfalls ist – in einem zweiten Schritt – die Weitergabe in nichtanonymisierter Form erforderlich.

Die mit der Weitergabe verbundene Zweckänderung kann – abhängig vom jeweiligen Einzelfall – gemäß Art. 17 Abs. 2 Nr. 5 BayDSG gerechtfertigt sein. Hiernach ist sie zulässig, wenn Angaben der Betroffenen überprüft werden sollen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen. Für die Beurteilung, ob tatsächliche Anhaltspunkte vorliegen, ist wiederum das Ergebnis der vorherigen Anfrage in anonymisierter Form bei den Sozialbehörden maßgeblich. Möglicherweise kann auch ein Fall des Art. 17 Abs. 2 Nr. 6 BayDSG vorliegen, wonach die Weitergabe für einen anderen Zweck zulässig ist, wenn Angaben der Betroffenen zur Erlangung von finanziellen Leistungen öffentlicher Stellen mit anderen derartigen Angaben verglichen werden sollen.

Aufgrund des Erforderlichkeitsprinzips muss die Weitergabe auf die für die Einleitung eines entsprechenden Überprüfungsverfahrens durch die Sozialbehörden notwendigen Daten beschränkt werden. Deshalb sind beispielsweise nicht notwendige Aktenbestandteile zu schwärzen.

6.8 Veröffentlichung von Sitzungsvorlagen im Internet

Viele Gemeinden nutzen das World Wide Web, um die Gemeinderatsarbeit transparent zu machen. Der Gewinn bei den Informationsmöglichkeiten für die örtliche Gemeinschaft wird dabei mit der weltweiten Verfügbarkeit der auf einer Homepage, einer Facebook-Präsenz oder in einem Ratsinformationssystem publizierten Dokumente erkauft. Im Berichtszeitraum erreichten mich zahlreiche Anfragen von Bürgerinnen und Bürgern und Gemeinden, die diesen Aspekt von Transparenz betrafen.

Aus einer niederbayerischen Stadt gingen mehrere Eingaben von Stadtratsmitgliedern ein, die feststellen mussten, dass der erste Bürgermeister einen von ihnen für eine Sitzung des Stadtrats gestellten Antrag im Rahmen seiner Facebook-Präsenz veröffentlicht hatte. Der Antrag war – wie von der Geschäftsordnung für den Stadtrat vorgesehen – von den ihn unterstützenden Stadtratsmitgliedern handschriftlich unterzeichnet. Für die Veröffentlichung war der Antrag offenkundig eingescannt worden, sodass die Unterschriften gleichsam im Faksimile weltweit abrufbar waren. Betroffene Stadtratsmitglieder wiesen in ihren Eingaben auf Missbrauchsrisiken hin.

Die unter dem Namen des ersten Bürgermeisters geführte Facebook-Präsenz wies im Impressum Kontaktdaten der Stadtverwaltung aus und war daher der Stadt zuzuordnen. Der erste Bürgermeister räumte auf mein Ersuchen um Stellungnahme auch ein, dass es sich bei der Seite um eine Präsenz der Stadt handle.

Ich habe den Sachverhalt datenschutzrechtlich folgendermaßen gewürdigt:

Indem die Stadträte einen Antrag stellen, nehmen sie ein mandatsbezogenes Recht wahr. Gleichwohl sind die Schriftzüge, mit denen sie den Antrag unterzeichnet haben, personenbezogene Daten im Sinne von Art. 4 Abs. 1 BayDSG. Die Einstellung auf einer amtlichen Facebook-Präsenz ist als Datenübermittlung zu werten, die nach Art. 15 Abs. 1 Nr. 1, Art. 4 Abs. 6 Satz 1 BayDSG einer Rechtsgrundlage bedarf. Eine solche Rechtsgrundlage ist in den kommunalrechtlichen Vorschriften zur Öffentlichkeit (Art. 52 Gemeindeordnung für den Freistaat Bayern – GO) nicht enthalten.

Als Rechtsgrundlage kommt Art. 21 Abs. 2 Satz 1, Art. 19 Abs. 1 Nr. 1 BayDSG in Betracht, weil die entsprechende Datei mit dem Einstellen auf einer Facebook-Präsenz an eine nicht-öffentliche Stelle in einem Drittland (Standort der Server von Facebook) übermittelt wird. Die Voraussetzungen dieser Rechtsgrundlage sind aber nicht erfüllt.

Die Übermittlung ist nicht – wie von Art. 19 Abs. 1 Nr. 1 BayDSG gefordert – zur Erfüllung von Aufgaben der öffentlichen Stelle erforderlich. Der erste Bürgermeister hat nach Art. 46 Abs. 2 Satz 1 GO die Beratungsgegenstände für die Sitzungen des Stadtrats vorzubereiten. Die Erledigung dieser Aufgabe bedingt nicht einmal in jedem Fall den Versand von Sitzungsunterlagen an die Stadtratsmitglieder.

Eine Aufgabe, Stadtratsanträge im Faksimile Außenstehenden und zudem weltweit verfügbar zu machen, stellt sich bayerischen Gemeinden überhaupt nicht. Eine andere Sichtweise wäre im Übrigen auch mit Art. 6 Abs. 1 Satz 1 GO unvereinbar.

Ich habe den festgestellten Datenschutzverstoß beanstandet.

Der Fall zeigt, dass bei der Publikation von Sitzungsunterlagen im World Wide Web Vorsicht geboten ist. Das Einstellen von eingescannten Dokumenten, die handschriftlich unterzeichnet sind, ist grundsätzlich unzulässig. Dies gilt nicht nur für Anträge aus der Mitte des Gemeinderats, sondern auch für Schreiben, welche die Gemeinde von Bürgerinnen und Bürgern oder von Behörden (wie etwa Recht- oder Fachaufsichtsbehörden, benachbarten Gemeinden oder dem Bayerischen Kommunalen Prüfungsverband) erhält.

6.9 Bekanntgabe von Bauherrendaten in öffentlicher Gemeinderatssitzung und der Tagesordnung

Gemeinden, Bürgerinnen und Bürger haben sich mit der Frage an mich gewandt, welche Daten der Bauherrinnen und Bauherren bei der Behandlung ihrer Bauanträge in öffentlicher Gemeinderatssitzung und der Tagesordnung dazu veröffentlicht werden dürfen. Ich vertrete dazu die folgende Rechtsauffassung:

Bauanträge sind grundsätzlich in öffentlicher Gemeinderatssitzung zu behandeln (Art. 52 Abs. 2 Satz 1 Gemeindeordnung für den Freistaat Bayern – GO). In der Tagesordnung zu der Gemeinderatssitzung sowie bei der Behandlung der Angelegenheit in der Sitzung sind dabei die Bauherrendaten bekannt zu geben, die zur Bezeichnung des Bauvorhabens erforderlich sind. Zur ordnungsgemäßen Bezeichnung des Tagesordnungspunktes ist es im Regelfall erforderlich, dass der Bauort (Straße und Hausnummer oder Flurstücknummer) und die Art des Bauvorhabens genannt werden. Fraglich ist, ob darüber hinaus der Name der Bauherrin beziehungsweise des Bauherren genannt werden muss, da es sich bei dem Bauvorhaben um eine sachbezogene Angelegenheit handelt. Hierzu wird vorgetragen, dass die mit der Veröffentlichung der Tagesordnung und der Behandlung in öffentlicher Sitzung verbundene Kontrollfunktion, beispielsweise im Hinblick auf eine mögliche Bevorzugung einzelner Bauherrinnen und Bauherren, nicht ausgeübt werden können, wenn die Namen nicht genannt würden. Das halte ich für nachvollziehbar und erhebe gegen die Namensnennung keine Einwände. Nicht notwendig ist allerdings die Bekanntgabe der Anschrift oder des Wohnorts der Bauherrin oder des Bauherren. Diese Daten dürfen daher in der Tagesordnung und in der Sitzung nicht bekanntgegeben werden. Haben Bauplatz und Bauherrin beziehungsweise Bauherr dieselbe Anschrift, ist die Veröffentlichung unter der Bezeichnung des Bauplatzes aber hinzunehmen.

Soll die Tagesordnung zusätzlich im Internet, etwa auf der Homepage der Gemeinde, veröffentlicht werden, ist der Name der Bauherrin oder des Bauherren entweder wegzulassen oder zu anonymisieren, soweit dieser Name für die Information der Öffentlichkeit nicht zwingend erforderlich ist. Dies ist bei der Behandlung von Bauanträgen regelmäßig der Fall.

Der Bayerische Gemeindetag hat seine Mitglieder in einem Rundschreiben auf meine Rechtsauffassung hingewiesen.

6.10 Dauerhafte Speicherung der Aufzeichnungen von Stadt- und Gemeinderatssitzungen

6.10.1 Einrichtung einer Internet-Mediathek über aufgezeichnete Sitzungen

Im Rahmen ihrer Transparenzbemühungen übertragen Kommunen Stadt- oder Gemeinderatssitzungen nicht nur als „Livestream“ direkt über das Internet, sondern wollen diese teilweise auch als in Form einer Mediathek unbegrenzt oder zumindest für einige Zeit auf den jeweiligen kommunalen Internetseiten – vergleichbar den Mediatheken der öffentlich-rechtlichen Rundfunkanstalten – „archivieren“ und damit für alle Interessierten weltweit einsehbar und abrufbar machen.

Zur Frage der Zulässigkeit einer Liveübertragung von Sitzungen habe ich mich bereits in der Vergangenheit geäußert (siehe 21. Tätigkeitsbericht 2004 unter Nr. 11.2). Die dort näher beschriebenen strengen datenschutzrechtlichen Rahmenbedingungen zur Direktübertragung deuten bereits darauf hin, dass die Einrichtung einer Mediathek ebenfalls datenschutzrechtlich problematisch ist. Im Ergebnis halte ich sie für unzulässig.

Lässt man die Frage, ob das Kommunalrecht wegen seiner Regelung in Art. 54 Abs. 3 Gemeindeordnung für den Freistaat Bayern (GO) nicht schon von vornherein der Einrichtung einer Mediathek entgegensteht, außer Betracht, so gilt Folgendes: Die Datenübermittlung in Gestalt einer Mediathek bedarf nach Art. 15 BayDSG einer Rechtsgrundlage, soweit davon personenbezogene Daten betroffen sind. Bereits die aufgezeichneten Äußerungen und die bildhafte Darstellung der Mitglieder des Stadt- oder Gemeinderats betreffen personenbezogene Daten. Erst Recht gilt das, wenn Gegenstand der Sitzung Anträge von Bürgerinnen und Bürgern sind und etwa deren Namen erwähnt werden.

Eine spezielle gesetzliche Rechtsgrundlage besteht nicht. Auch Art. 19 Abs. 1 Nr. 2 BayDSG scheidet als Rechtsgrundlage aus. Stellt diese Norm schon für den „Livestream“ keine geeignete Grundlage dar (siehe 21. Tätigkeitsbericht 2004 unter Nr. 11.2), so gilt dies erst Recht für die Einrichtung einer Mediathek.

Schließlich scheidet auch eine Einwilligung der Mitglieder des Stadt- oder Gemeinderats, die sich im Übrigen ausdrücklich auf die Archivierung beziehen müsste und vornherein personenbezogene Daten von Bürgerinnen und Bürgern nicht umfassen könnte, als Rechtsgrundlage (vgl. Art. 15 Abs. 1 Nr. 2 BayDSG) ebenfalls aus. Im Vergleich zum „Livestream“ stellt eine „Archivierung“ – auch wenn sie nur vorübergehend erfolgt – eine Datenübermittlung von besonderer Tragweite dar. Alle gegebenenfalls auch spontanen oder möglicherweise „ungeschickten“ Verhaltensweisen oder Äußerungen der Stadtratsmitglieder wären nicht nur im Moment der Übertragung in Bild und Ton, sondern sogar für längeren Zeitraum oder dauerhaft weltweit abrufbar und auswertbar. Unabhängig davon, wie lange und in welchem Umfang eine Archivierung erfolgt, ist die nachträgliche Auswertung der so entstandenen Bild- und Tondokumente noch weniger kontrollier- und steuerbar, als das bei einem „Livestream“ der Fall ist. Je nach Beratungsgegenstand können die damit verbundenen Einschüchterungseffekte und die deshalb schwindende Unbefangenheit sich nicht nur auf die Persönlichkeitsrechte des Betroffenen auswirken, sondern auch die Arbeit des Gremiums und auf lange Sicht sogar die Funktionsfähigkeit des Stadtrats beeinträchtigen. Mit Blick hierauf dürften die einzelnen Stadtratsmitglieder bereits nicht befugt sein, mittels Einwilligung über diese zu disponieren. Jedenfalls aber dient das Instrument der Einwilligung nicht dazu, den Vorrang des Gesetzes zu unterlaufen, das über die grundsätzliche Frage der Art und Weise der Herstellung von Öffentlichkeit in Stadtratssitzungen zu entscheiden hat. Insoweit stehen die in Art. 15 Abs. 1 BayDSG genannten Rechtsgrundlagen – Rechtsvorschrift oder Einwilligung – in einem gewissen Spannungsverhältnis.

Eine Gemeinde kann ihre gesetzlichen Befugnisse nicht beliebig mit Hilfe von Einwilligungen erweitern. Der Gesetzgeber hat schon die Live-Übertragung öffentlicher Stadtrats- und Ausschusssitzungen im Internet nicht geregelt. Wie im 21. Tätigkeitsbericht 2004 unter Nr. 11.2 dargestellt, kann sie mit Hilfe von Einwilligungen unter bestimmten Voraussetzungen noch gerechtfertigt sein. Im Gegensatz zu einer solchen flüchtigen Momentaufnahme hat eine dauerhafte Archivierung

weitergehende Auswirkungen auf die Persönlichkeitsrechte und die Funktionsfähigkeit des Gremiums. Daher sehe ich ohne gesonderte gesetzliche Regelung keinen Raum, auf Basis einer Einwilligung diese Datenübermittlung für zulässig zu halten. Die Einwilligung ist als Instrument nicht geeignet, sich derart weit vom gesetzlichen Regelungsmodell – Öffentlichkeit der Stadtratssitzung nur nach Maßgabe von Art. 52 Abs. 2 GO – zu entfernen.

6.10.2 Archivierung von zur Erstellung der Niederschrift dienenden Audioaufzeichnungen

Eine Stadt hat mir mitgeteilt, der erste Bürgermeister habe im Zusammenhang mit der Erstellung von Niederschriften über die Sitzungen des Stadtrats angedacht, künftig neben der Niederschrift mit dem Mindestinhalt nach Art. 54 Abs. 1 Gemeindeordnung für den Freistaat Bayern (GO) noch Audiodateien, auf denen die vollständige Sitzung gespeichert ist, dauerhaft zu archivieren. Bei den Audiodateien handele es sich um Tonbandaufnahmen, die als Hilfsmittel zur Erstellung von Sitzungsniederschriften angefertigt wurden. Die Stadt selbst hat Bedenken gegen eine dauerhafte Speicherung derartiger Aufnahmen geäußert, die ich aus den folgenden Gründen teile:

Tonbandaufnahmen von Wortbeiträgen greifen in das Recht auf informationelle Selbstbestimmung der Gemeinderatsmitglieder und sonstiger betroffener Personen ein. Sie gehen weit über das hinaus, was in Art. 54 Abs. 1 GO als Mindest- (und praktisch als Regel-) Inhalt einer Niederschrift vorgesehen ist und geben beispielsweise auch die Einzelheiten und die Lautstärke der in der Sitzung geführten Debatten wieder. Sie können selbst rein private, etwas zu laut geführte Unterhaltungen zwischen Sitzungsteilnehmern festhalten (Widtmann/Grasser/Glaser, Bayerische Gemeindeordnung, Art. 54 Rn. 2). Die Tonbandaufnahmen sind daher gemäß Art. 12 Abs. 4 Satz 2 BayDSG zu löschen, sobald sie als Hilfsmittel zur Anfertigung der Sitzungsniederschriften nicht mehr erforderlich sind. Das ist in der Regel mit der Genehmigung der Niederschrift der Fall (siehe Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Teil C Handbuch, Abschnitt XII Nr. 5a). § 34 Abs. 2 Satz 2 der Mustergeschäftsordnung des Bayerischen Gemeindetages sieht daher vor, dass Tonbandaufnahmen unverzüglich nach Genehmigung der Niederschrift zu löschen sind und Außenstehenden nicht zugänglich gemacht werden dürfen.

6.11 Einstellung öffentlicher Bekanntmachungen mit personenbezogenen Daten in das Internet

Mit dem Gesetz zur Änderung des Bayerischen Verwaltungsverfahrensgesetzes und anderer Rechtsvorschriften vom 22. Mai 2015 (GVBl. S. 154) hat der Gesetzgeber einen neuen Art. 27a mit der Überschrift „Öffentliche Bekanntmachung im Internet“ in das Bayerische Verwaltungsverfahrensgesetz (BayVwVfG) eingefügt. Mit dieser Vorschrift soll erreicht werden, dass öffentliche oder ortsübliche Bekanntmachungen im Rahmen eines Verwaltungsverfahrens ergänzend auch im Internet erfolgen.

Bereits in der Vergangenheit habe ich festgestellt, dass viele Gemeinden ihre Amtsblätter, die teilweise auch öffentliche Bekanntmachungen mit personenbezogenen Daten enthalten, im Internet dauerhaft veröffentlichen. Deshalb habe ich in meinem 25. Tätigkeitsbericht 2012 unter Nr. 6.1 darauf hingewiesen, dass mit

Blick auf die unterschiedlichen Wirkungen einer Veröffentlichung in Papierform (in einem archivierten Amtsblatt) und einer allzeit verfügbaren Veröffentlichung im Internet stets sorgfältig zu prüfen ist, ob gerade eine Internetveröffentlichung (dieses jeweils konkreten Teils des Amtsblatts) zur Aufgabenerfüllung erforderlich ist.

An dieser notwendigen einzelfall- und inhaltsbezogenen Abwägung der zu veröffentlichenden Informationen ändert auch die Einführung des Art. 27a BayVwVfG nichts.

Zwar sieht Art. 27a Abs. 1 BayVwVfG vor, dass Behörden den Inhalt einer (durch Rechtsvorschrift – etwa aus dem Baurecht – angeordneten) öffentlichen oder ortsüblichen Bekanntmachung zusätzlich im Internet veröffentlichen sollen. Es handelt sich jedoch ausdrücklich um eine „Soll-Vorschrift". Damit lässt der Wortlaut nach dem Willen des Gesetzgebers Raum für die Berücksichtigung des Datenschutzes: „Datenschutzrechtliche Belange sind in besonderem Maße im Rahmen einer Einzelfallprüfung gerade auch bei ortsüblichen oder öffentlichen Bekanntmachungen von an Einzelpersonen gerichteten Verwaltungsakten zu beachten" (Landtags-Drucksache 17/2820, S. 13 f.).

Wird eine Information nach der entsprechenden Abwägung in das Internet eingestellt, so ist gleichzeitig zu prüfen, wie lange die Information im Internet eingestellt werden darf. Auch hierzu enthält Art. 27a Abs. 1 BayVwVfG keine Vorgaben. Für die Dauer einer Interneteinstellung ist die jeweilige Funktion der Internetveröffentlichung maßgebend. Geht es etwa um eine öffentliche Bekanntmachung mit „Einladungs- oder Anstoßcharakter" (vgl. Art. 66 Abs. 2 Satz 4 Bayerische Bauordnung), so muss die Internetveröffentlichung der Bekanntmachung bis zum Ablauf des Termins – aber eben auch nicht länger – zugänglich gemacht werden. Das genügt, um die Handlung wirksam vorzunehmen, zu der „eingeladen" oder „angestoßen" werden soll.

Art. 27a BayVwVfG Öffentliche Bekanntmachung im Internet
(1) [1]Ist durch Rechtsvorschrift eine öffentliche oder ortsübliche Bekanntmachung angeordnet, soll die Behörde deren Inhalt zusätzlich im Internet veröffentlichen. [2]Dies wird dadurch bewirkt, dass der Inhalt der Bekanntmachung auf einer Internetseite der Behörde oder ihres Verwaltungsträgers zugänglich gemacht wird. [3]Bezieht sich die Bekanntmachung auf zur Einsicht auszulegende Unterlagen, sollen auch diese über das Internet zugänglich gemacht werden. [4]Soweit durch Rechtsvorschrift nichts anderes geregelt ist, ist der Inhalt der zur Einsicht ausgelegten Unterlagen maßgeblich.
(2) In der öffentlichen oder ortsüblichen Bekanntmachung ist die Internetseite anzugeben.

6.12 Schwärzung von personenbezogenen Daten bei Eingaben

Ein Bürger hat sich an mich gewandt und gerügt, dass es im Zusammenhang mit Debatten im Stadtrat einer Kommune zur Umsetzung eines bestehenden Bebauungsplans zu Datenschutzverstößen gekommen sei. Er teilte mit, dass Eingaben von Bürgerinnen und Bürgern, die als Anlage zu Beschlussvorlagen an den zuständigen Ausschuss beilagen, zwar von der Verwaltung geschwärzt worden seien. Diese Schwärzungen hätten allerdings mithilfe einfacher technischer Möglichkeiten beseitigt werden können. Dadurch seien die eingabeführenden Personen erkennbar geworden. Diesen Umstand hätten sich offenbar einzelne Mitglieder ei-

ner Fraktion des Stadtrats zunutze gemacht. Sie hätten die so unzureichend anonymisierten betroffenen Personen angeschrieben, um sie aus der Sicht der Fraktionsmitglieder über den Stand der Dinge zu informieren.

Die mir vorgelegten Dokumente sprachen dafür, dass sich der geschilderte Sachverhalt tatsächlich so zugetragen hat. Ich habe die betroffene Kommune darauf hingewiesen, dass erstens die gebotenen Schwärzungen stets so vorzunehmen sind, dass sie unumkehrbar und auch mutwillig nicht zu umgehen sind, und zweitens, dass die Verschwiegenheitspflicht von Stadtratsmitgliedern sich auch auf solche Informationen und personenbezogene Daten erstreckt, von denen sie Kenntnis erhalten, weil eine Schwärzung unzureichend vorgenommen wurde.

Nach Art. 20 Abs. 2 Satz 2 Gemeindeordnung für den Freistaat Bayern (GO) dürfen Stadtratsmitglieder die Kenntnis der geheimzuhaltenden Angelegenheiten nicht unbefugt verwerten. Es ist in Ordnung, wenn Stadtratsmitglieder die Irreversibilität der Schwärzungen kritisch überprüfen, die die Verwaltung bei Anlagen für Beschlussvorlagen vornimmt. Keinesfalls ist es aber hinzunehmen, wenn Stadtratsmitglieder sich die technische Reversibilität einer Schwärzung zunutze machen. Hierin liegt ein – mit Ordnungsgeld belegbarer – Verstoß gegen das Verwertungsverbot des Art. 20 Abs. 2 Satz 2 GO. Es ist bereits ein Verstoß, die Adressen zu verwenden und Bürgerinnen und Bürger anzuschreiben. Es kommt nicht darauf an, ob die Betroffenen – etwa durch Verwendung eines offenen E-Mail-Verteilers – wechselseitig die personenbezogenen Daten erhalten. Nach Art. 20 Abs. 4 Satz 1 GO kann, wer den Verpflichtungen der Absätze 1, 2 oder 3 Satz 1 schuldhaft zuwiderhandelt, im Einzelfall mit Ordnungsgeld bis zu zweihundertfünfzig Euro, bei unbefugter Offenbarung personenbezogener Daten bis zu fünfhundert Euro, belegt werden.

Zwar hat die Stadt hier keinen Datenschutzverstoß begangen, da ihr das beschriebene Verhalten der Stadtratsmitglieder wegen mutmaßlich fehlender Billigung nicht zugerechnet werden konnte. Ich habe sie gleichwohl gebeten, alle Stadtratsmitglieder darauf hinzuweisen, dass unzureichende Schwärzungen von den Mitgliedern des Stadtrats nicht zur Gewinnung von personenbezogenen Daten ausgenutzt werden dürfen.

6.13 Datenerhebung durch Kommunen zur Feststellung der Hundehaltung

Durch Eingaben war ich mit der Frage befasst, ob Kommunen ihre Bürgerinnen und Bürger danach befragen dürfen, ob sie Hunde halten. In der Regel beauftragen die Kommunen damit private Unternehmen, die die Befragung vor Ort durchführen.

Geht man davon aus, dass das Kontrollpersonal lediglich an der Haustür klingelt und sich nach einer Hundehaltung erkundigt, nicht aber die Wohnung betritt, so dürfte zwar kein Eingriff in das Grundrecht der Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 Grundgesetz – GG) vorliegen. Es liegt jedoch auf jeden Fall ein Eingriff in das – ebenfalls verfassungsrechtlich gewährleistete – informationelle Selbstbestimmungsrecht (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) vor. Auch für solche Eingriffe bedarf es einer Rechtsgrundlage.

Eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch öffentliche Stellen ist nach Art. 15 Abs. 1 BayDSG zulässig, wenn das Bayerische Datenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet (Nr. 1) oder der Betroffene eingewilligt hat (Nr. 2).

Eine vorrangige Spezialregelung gibt es nicht. Der Gesetzgeber hat in Art. 13 Abs. 6 Satz 1 Kommunalabgabengesetz (KAG) ausdrücklich in Bezug auf die Hundesteuer die Anwendung des Bayerischen Datenschutzgesetzes angeordnet. Mangels einer Spezialregelung ist daher die Datenerhebung zulässig, wenn die Voraussetzungen des Art. 16 Abs. 1 BayDSG vorliegen. Denn diese Vorschrift gestattet Datenerhebungen im Sinne des oben genannten Art. 15 Abs. 1 Nr. 1 BayDSG. Voraussetzung des Art. 16 Abs. 1 BayDSG ist, dass die Kenntnis der Daten zur Erfüllung der in der Zuständigkeit der erhebenden Stelle liegenden Aufgaben erforderlich ist.

Die genannten Voraussetzungen des Art. 16 Abs. 1 BayDSG liegen vor. Die Hundesteuer ist eine örtliche Aufwandsteuer, die die Gemeinden nach Art. 3 KAG erheben können. Die Beitreibung der Steuer gehört insoweit zur Aufgabe der Gemeinde. Hierzu dient das Erheben der personenbezogenen Daten über die Hundehalterinnen und Hundehalter. Zudem ist die Erhebung der Daten erforderlich. Erforderlich ist eine Datenerhebung nach Art. 16 Abs. 1 BayDSG bereits dann, wenn die Kenntnis der Daten zur Erreichung des Zwecks objektiv geeignet und im Verhältnis zu dem angestrebten Zweck angemessen ist. Die Kenntnis von der Hundehaltung ist für die Verwirklichung des Steuertatbestandes und die Möglichkeit seiner Beitreibung geeignet und grundsätzlich auch angemessen. Die erhobenen Daten sind nicht sonderlich sensibel und offenbaren keine höchstpersönlichen Informationen.

Nach Art. 16 Abs. 3 BayDSG ist allerdings bei der Erhebung der Daten der Erhebungszweck der betroffenen Personen gegenüber anzugeben und darauf hinzuweisen, dass die Angaben freiwillig sind oder die Rechtsvorschrift zu nennen, der zufolge eine Verpflichtung zur Auskunftserteilung steht. Eine Pflicht zur Auskunftserteilung besteht im vorliegenden Fall nach § 93 Abgabenordnung. Hiernach haben die Beteiligten der Finanzbehörde die zur Feststellung eines für die Besteuerung erheblichen Sachverhalts – hier die Hundehaltung – erforderlichen Auskünfte zu erteilen. Diese Regelung gilt nach Art. 13 Abs. 1 Nr. 3 Buchst. a) KAG im vorliegenden Zusammenhang entsprechend und damit besteht bezüglich der Hundesteuer die Auskunftspflicht gegenüber der zuständigen Gemeinde.

Dass die Gemeinde nicht mit eigenen Bediensteten, sondern mit privaten Stellen die Datenerhebung durchführt, ist grundsätzlich nach Art. 6 BayDSG möglich. Art. 6 BayDSG gestattet unter Beachtung bestimmter Voraussetzungen, dass personenbezogene Daten durch andere (private) Stellen im Auftrag der öffentlichen Stelle erhoben werden.

6.14 Auskunft an die eine Anzeige erstattende Person

Zu der Frage, unter welchen Voraussetzungen eine Behörde der angezeigten Person den Namen einer Behördeninformantin oder eines Behördeninformanten mitteilen darf, habe ich mich wiederholt geäußert, zuletzt im 26. Tätigkeitsbericht 2014 unter Nr. 6.11. Es haben sich aber auch Bürgerinnen und Bürger an mich

gewandt, die Anzeige erstattet hatten und wissen wollten, wie die Behörde mit ihrer Anzeige umgegangen ist. Ein solches Begehren ist aus datenschutzrechtlicher Sicht wie folgt zu bewerten:

Die eine Anzeige erstattende Person hat als solche keinen Rechtsanspruch gegen die Behörde auf Mitteilung, ob, gegen wen und welche Maßnahmen diese aufgrund der Anzeige ergriffen hat. Die Anzeige stellt eine bloße Anregung und Information gegenüber der Behörde dar, aus der sich keine Rechtspositionen ableiten lassen.

Eine Auskunftserteilung kommt regelmäßig auch nicht im Rahmen einer Ermessensausübung nach Art. 19 Abs. 1 Nr. 2 BayDSG in Betracht, da die schutzwürdigen Belange der von der Anzeige betroffenen Person an einem Ausschluss der Übermittlung ihrer personenbezogenen Daten das bloße Informationsinteresse der die Anzeige erstattenden Person überwiegen. Diese kann jedoch erwarten, dass die Behörde auf eine entsprechende Anfrage hin den Eingang der Anzeige bestätigt. Insoweit liegt jedoch kein datenschutzrechtlicher Bezug vor.

Eine andere Situation liegt vor, wenn die Behörde auf die Anzeige hin ein Verwaltungsverfahren nach dem Bayerischen Verwaltungsverfahrensgesetz (BayVwVfG) durchführt und die eine Anzeige erstattende Person in diesem Verfahren Beteiligte ist. Ob eine Behörde ein Verwaltungsverfahren durchführt, entscheidet sie im Rahmen ihrer Aufgabenerfüllung in eigener Zuständigkeit. Diese Entscheidung ist keine datenschutzrechtliche Frage, sondern eine solche des fachlichen Aufgabenvollzugs. Beteiligte eines Verwaltungsverfahrens sind nach Art. 13 Abs. 1 BayVwVfG unter anderem Antragsteller und Antragsgegner sowie diejenigen, an die die Behörde den Verwaltungsakt richten will oder gerichtet hat. Nach Art. 13 Abs. 2 BayVwVfG kann die Behörde außerdem diejenigen, deren rechtliche Interessen durch den Ausgang des Verfahrens berührt werden können, als Beteiligte hinzuziehen.

Die Erteilung von Auskünften aus einem Verwaltungsverfahren stellt eine besondere Form der Akteneinsicht nach Art. 29 Abs. 1 BayVwVfG dar. Danach hat die Behörde den Beteiligten (zum Begriff siehe oben) Einsicht in die einzelnen Teile der das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist.

Außerhalb eines Verwaltungsverfahrens kann Akteneinsicht im Rahmen einer Ermessensentscheidung gewährt werden, wenn die antragstellende Person ein berechtigtes Interesse hieran geltend macht. Das ist dann der Fall, wenn die Kenntnis des Akteninhalts Voraussetzung für eine wirksame Rechtsverfolgung ist.

Art. 29 BayVwVfG Akteneinsicht durch Beteiligte
(1) [1]Die Behörde hat den Beteiligten Einsicht in die einzelnen Teile der das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. [2]Satz 1 gilt bis zum Abschluß des Verwaltungsverfahrens nicht für Entwürfe zu Entscheidungen sowie die Arbeiten zu ihrer unmittelbaren Vorbereitung. [3]Soweit nach den Art. 17 und 18 eine Vertretung stattfindet, haben nur die Vertreter Anspruch auf Akteneinsicht.

6.15 Kenntnisnahme des Nachbarn von den Baukosten im Baugenehmigungsverfahren

Im Verfahren auf Erteilung einer Baugenehmigung schreibt die Bayerische Bauordnung (BayBO) auch die Beteiligung des Nachbarn vor. Der Bauherr legt dem Nachbarn den Lageplan und die Bauzeichnungen vor. Ist der Nachbar mit dem Vorhaben einverstanden, bringt er dies mit seiner Unterschrift zum Ausdruck. In diesem Fall erhält der Nachbar keine Ausfertigung der Baugenehmigung. Eine Nachbarklage ist grundsätzlich ausgeschlossen. Hat der Nachbar nicht zugestimmt oder wird seinen Einwendungen nicht entsprochen, ist ihm eine Ausfertigung der Baugenehmigung zuzustellen (Art. 66 Abs. 1 Satz 6 BayBO). Diese Ausfertigung benötigt der Nachbar, um die Erfolgsaussichten einer Nachbarklage überprüfen (lassen) zu können.

In einem Baugenehmigungsverfahren, das bei einem Landratsamt anhängig war, hatte ein Nachbar die Unterschriftsleistung verweigert. Folglich war ihm eine Ausfertigung der Baugenehmigung zuzustellen. Damit war allerdings der Bauherr nicht einverstanden, weil er befürchtete, der Nachbar werde durch die mit der Baugenehmigung getroffene Kostenentscheidung und eine diesbezügliche Begründung Details über die Baukosten und so mittelbar über die Vermögensverhältnisse des Bauherrn erfahren. Das Landratsamt suchte bei mir um Beratung nach.

Ausgangspunkt für die rechtliche Würdigung ist die erwähnte Vorschrift des Art. 66 Abs. 1 Satz 6 BayBO. Danach ist „eine Ausfertigung der Baugenehmigung“ zuzustellen. Wie Art. 68 Abs. 1 und 2 BayBO zeigen, verwendet der Gesetzgeber den Begriff „Baugenehmigung“ (auch) für die Urkunde (den Baubescheid). Die Erteilung der Baugenehmigung ist kostenpflichtig. Die Kostenentscheidung wird in der Verwaltungspraxis üblicherweise mit der Baufreigabe getroffen und verbreitet im Baubescheid mit dieser verbunden. Zugestellt wird aber – auch an den Nachbarn – der vollständige Baubescheid.

Der Nachbar kann bei dieser Rechtslage durch die Zustellung des vollständigen Baubescheids jedenfalls bei Uneinigkeit von Bauherr und Bauaufsichtsbehörde über die Baukosten Kenntnis der entsprechenden Ansätze erlangen, weil in dieser Konstellation eine Begründung der Kostenentscheidung hinsichtlich der nach Tarifstellen 1.24 ff. Kostenverzeichnis maßgeblichen Berechnungsgrundlage (den Baukosten) erforderlich ist.

Dass der Bauherr nicht beanspruchen kann, sein Vorhaben gleichsam „heimlich“ realisieren zu können, entspricht der Einbindung des Grundeigentums in ein Gemeinschaftsverhältnis. Nachbarn erhalten im Rahmen der Nachbarbeteiligung bereits vor Erteilung der Baugenehmigung Kenntnis auch von Einzelheiten des Vorhabens, wie sie sich aus Lageplan und Bauzeichnungen (Art. 66 Abs. 1 Satz 1 BayBO) ergeben. Aus diesen Unterlagen lässt sich ohne Schwierigkeit ersehen, ob eine größere oder kleinere Baumasse, eine aufwändige oder weniger aufwändige Bauausführung beabsichtigt ist. Die für den Bauantrag üblicherweise anhand eines Baukostenindex errechneten Baukosten geben einen Anhaltspunkt über die für den Bauherrn bei Durchführung des Vorhabens in Aussicht stehende finanzielle Belastung; dadurch wird jedoch nur das Bild abgerundet, welches der Nachbar durch Einblick in die Baupläne ohnehin bereits gewinnen konnte.

Um einen ihm möglicherweise zustehenden Nachbarrechtsbehelf prüfen und einlegen zu können, benötigt der Nachbar indes nur Kenntnis von der zur Sache (Baufreigabe) getroffenen Entscheidung. Die Baukosten sind für den Nachbarn

nicht relevant. Er kann mangels Beschwer weder die Kostenentscheidung angreifen noch hängt die gerichtliche Kostenentscheidung hinsichtlich des Nachbarrechtsbehelfs von den Baukosten ab. Der Streitwertkatalog 2013 für die Verwaltungsgerichtsbarkeit – Internet: http://www.bverwg.de/informationen/streitwertkatalog.php – nennt hier unter Nr. 9.7.1 einen Rahmen von 7.500 bis 15.000 Euro, soweit nicht ein höherer wirtschaftlicher Schaden feststellbar ist.

Vor diesem Hintergrund habe ich dem Landratsamt geraten, der Kostenentscheidung zugrunde gelegte Baukosten möglichst (nur) in einer separaten, dem Nachbarn nicht zuzustellenden Kostenrechnung zu nennen. Eine mir bekannte Verwaltungspraxis formuliert die Kostenentscheidung im Baubescheid folgendermaßen:

„Der Antragsteller hat die Kosten des Verfahrens zu tragen. Für diesen Bescheid werden gemäß beiliegender Kostenrechnung Kosten in Höhe von … Euro erhoben."

Alternativ könnte auch – wie von Art. 12 Abs. 1 Kostengesetz vorausgesetzt – eine vom Baubescheid getrennte Kostenentscheidung ergehen.

6.16 Novellierung des Melderechts

Im Zuge der Föderalismusreform im Jahr 2006 wurde das Meldewesen in die ausschließliche Gesetzgebungskompetenz des Bundes überführt. Von dieser hat der Bund zwischenzeitlich durch das Bundesmeldegesetz Gebrauch gemacht, das zum Teil am 26. November 2014, überwiegend aber am 1. November 2015 in Kraft getreten ist (BGBl. I 2013, 1084; BGBl. I 2014, 1738). Es hat das Melderechtsrahmengesetz des Bundes und in Bayern das bisherige Gesetz über das Meldewesen (Meldegesetz – MeldeG) vom 8. Dezember 2006 abgelöst.

Für das Melderecht sind daher in Bayern seit dem 1. November 2015 im Wesentlichen maßgeblich das Bundesmeldegesetz (BMG), das Bayerische Gesetz zur Ausführung des Bundesmeldegesetzes (BayAGBMG) und die Verordnung zur Übermittlung von Meldedaten (Meldedatenverordnung – MeldDV).

Ein besonders häufiger Anwendungsfall des Melderechts sind Melderegisterauskünfte. Immer wieder wenden sich Bürgerinnen und Bürger an mich, die sich darüber beschweren, dass die Meldebehörden privaten Dritten über Meldedaten Auskunft erteilen, teilweise sogar, obwohl die Betroffenen im Melderegister eine Auskunftssperre eingetragen haben. In aller Regel sind die von den Meldebehörden gegebenen Auskünfte angesichts der Rechtslage rechtmäßig.

6.16.1 Melderecht als „Rückgrat" der Informationsverwaltung

Der Bundesgesetzgeber hat sich wie bisher schon die Landesgesetzgeber dafür entschieden, das Melderegister als „Rückgrat" einer auf Informationen angewiesenen Verwaltung einzurichten. Entsprechend hält das Melderegister für die Meldebehörde wie auch eine Vielzahl von anderen Behörden einen in § 3 BMG näher beschriebenen, recht umfassenden Datenbestand über jede meldepflichtige Person bereit. Die Einzelheiten der Datenübermittlung an öffentliche Stellen lassen sich den §§ 34 ff. BMG entnehmen; welche (bayerischen) Behörden unter welchen Voraussetzungen welche Daten aus dem Melderegister erhalten können, ist

dabei im Einzelnen vor allem durch die Meldedatenverordnung spezifisch geregelt worden.

6.16.2 Melderegisterauskünfte

Seit alters her dient das Melderegister aber nicht allein behördlichen Zwecken, sondern auch den Interessen von Privatpersonen. Hintergrund dieser Entscheidung des Gesetzgebers ist die Annahme, dass es ohne triftigen Grund niemandem möglich sein soll, sich jeder Form von Kontaktaufnahme durch private Dritte zu entziehen. Das Interesse von Einzelnen, sich gegenüber jedermann persönlich unerreichbar zu machen, ist hiernach – vorbehaltlich bestimmter Ausnahmefälle – nicht schutzwürdig.

6.16.2.1 Einfache Melderegisterauskunft

Die wichtigste Form der Melderegisterauskunft ist die einfache Melderegisterauskunft. Sie ist in § 44 BMG geregelt. Hiernach kann eine Person über eine andere Person bestimmte „Basisdaten" (nämlich Vornamen, Familienname, Doktorgrad und derzeitige Anschrift) von der Meldebehörde gegen Gebühr erhalten, wenn die gesuchte Person dort gemeldet ist und die antragstellende Person diese mittels bestimmter Angaben gegenüber der Meldebehörde eindeutig identifizieren kann. Auf das Einverständnis der betroffenen Person kommt es nicht an. Es gibt auch keine Möglichkeit, der Erteilung einer einfachen Melderegisterauskunft zu widersprechen.

§ 44 BMG Einfache Melderegisterauskunft
(3) [1]Die Erteilung einer einfachen Melderegisterauskunft ist nur zulässig, wenn
1. die Identität der Person, über die eine Auskunft begehrt wird, auf Grund der in der Anfrage mitgeteilten Angaben über den Familiennamen, den früheren Namen, die Vornamen, das Geburtsdatum, das Geschlecht oder eine Anschrift eindeutig festgestellt werden kann, und
2. die Auskunft verlangende Person oder Stelle erklärt, die Daten nicht zu verwenden für Zwecke
a) der Werbung oder
b) des Adresshandels,
es sei denn, die betroffene Person hat in die Übermittlung für jeweils diesen Zweck ausdrücklich eingewilligt.

Auskünfte nach diesen Regeln können in Bayern nicht nur bei der jeweiligen Meldebehörde eingeholt werden, sondern sie kann **automatisiert** auch über das **Bürgerservice-Portal** der **Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB)** eingeholt werden. Nach Art. 7 Abs. 1 BayAGBMG übermitteln die Meldebehörden tagesaktuell die Einwohnerdaten an die Anstalt für Kommunale Datenverarbeitung in Bayern. Diese darf wiederum nach Art. 9 BayAGBMG aus diesem geschaffenen Datenbestand ein Portal betreiben und hieraus gegen ein privatrechtliches Entgelt Melderegisterauskünfte erteilen.

6.16.2.2 Auskunftssperre nach § 51 Abs. 1 BMG

Eine einfache Melderegisterauskunft ist nur dann unzulässig, wenn erstens die betroffene Person für sich eine Auskunftssperre wegen einer nachgewiesenen besonderen Gefahrenlage hat eintragen lassen und zweitens anlässlich eines kon-

kreten Antrags auf Erteilung einer einfachen Melderegisterauskunft nach Anhörung der betroffenen Person eine entsprechende Gefahr nicht ausgeschlossen werden kann.

§ 51 BMG Auskunftssperren
(1) Liegen Tatsachen vor, die die Annahme rechtfertigen, dass der betroffenen oder einer anderen Person durch eine Melderegisterauskunft eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen erwachsen kann, hat die Meldebehörde auf Antrag oder von Amts wegen eine Auskunftssperre im Melderegister einzutragen.
(2) [1]Sofern nach Anhörung der betroffenen Person eine Gefahr nach Absatz 1 nicht ausgeschlossen werden kann, ist eine Melderegisterauskunft nicht zulässig. (…) [3]Sofern eine Auskunft nicht erteilt wird, erhält die ersuchende Person oder Stelle eine Mitteilung, die keine Rückschlüsse darauf zulassen darf, ob zu der betroffenen Person keine Daten vorhanden sind oder eine Auskunftssperre besteht.

Eine Auskunftssperre nach § 51 Abs. 1 BMG darf also nicht schon dann eingetragen werden, wenn die betroffene Person – aus welchen Gründen auch immer – nicht möchte, dass ihre Melderegisterdaten („Basisdaten") an Dritte auf Anfrage herausgegeben werden; denn ein allgemeines Widerspruchsrecht gibt es gerade nicht.

Sie kann nur dann eingetragen werden, wenn Tatsachen vorgetragen werden, die die Annahme rechtfertigen, dass der betroffenen Person durch die Erteilung von einfachen Melderegisterauskünften Gefahren für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen erwachsen können. Entsprechend hoch sind die Anforderungen, die für die Eintragung einer solchen Sperre erfüllt werden müssen. Im Regelfall ist daher die Eintragung einer Auskunftssperre durch die Meldebehörde nicht möglich.

Ist für eine betroffene Person nach diesen strengen Maßstäben eine Auskunftssperre eingetragen worden, darf eine Auskunft grundsätzlich nur nach ihrer Anhörung und nur dann erteilt werden, wenn diese Anhörung ergibt, dass durch die erteilte Auskunft keine entsprechende Gesundheits- oder Lebensgefahr entsteht. Entscheidend ist hier die Bewertung der Behörde, nicht die der betroffenen Person.

Wichtig zu wissen ist auch, dass die Auskunftssperre grundsätzlich nur Auskünfte an Private, nicht aber Datenübermittlungen an öffentliche Stellen verhindert. Eine Übermittlung der Daten an – verkürzt und vereinfacht formuliert – den ARD ZDF Deutschlandradio Beitragsservice (vormals Gebühreneinzugszentrale – GEZ) – nach § 35 MeldDV kann durch eine Auskunftssperre daher nicht verhindert werden.

6.17 Übermittlung von Meldedaten an den Beitragsservice der öffentlich-rechtlichen Landesrundfunkanstalten (ARD), des Zweiten Deutschen Fernsehens (ZDF) und des Deutschlandradios

Ich erhalte immer wieder Anfragen von Bürgerinnen und Bürgern, die wissen wollen, wie die öffentlich-rechtlichen Rundfunkanstalten an ihre Meldedaten gelangt sind. Dazu weise ich auf Folgendes hin:

Zum 1. Januar 2013 wurde die GEZ (Gebühreneinzugszentrale) durch den Beitragsservice der öffentlich-rechtlichen Rundfunkanstalten – dies sind die in der ARD verbundenen Landesrundfunkanstalten, ferner das ZDF und das Deutschlandradio – abgelöst. Der Beitragsservice ist eine im Rahmen einer nicht rechtsfähigen öffentlich-rechtlichen Verwaltungsgemeinschaft nach § 10 Abs. 7 Satz 1 Rundfunkbeitragsstaatsvertrag errichtete Stelle mit der Aufgabe, Rundfunkbeiträge einzuziehen.

Regelmäßige Datenübermittlungen der bayerischen Meldebehörden an den Bayerischen Rundfunk oder die gemeinsame Verwaltungsstelle nach § 10 Abs. 7 Satz 1 Rundfunkbeitragsstaatsvertrag – damit ist der Beitragsservice gemeint – richten sich nach § 36 Abs. 1 Bundesmeldegesetz in Verbindung mit § 35 der Meldedatenverordnung – MeldDV. Danach können die Meldebehörden dem Bayerischen Rundfunk oder der gemeinsamen Verwaltungsstelle bei einer Anmeldung, Abmeldung oder einem Todesfall unter anderem den Vor- und Familiennamen, den Geburtstag und die (derzeitige und letzte frühere) Anschrift volljähriger Einwohner übermitteln.

Nach § 35 Abs. 2 MeldDV dürfen die übermittelten Daten nur für Zwecke der Beitragserhebung sowie zur Feststellung, ob eine Beitragspflicht nach dem Rundfunkbeitragsstaatsvertrag besteht, erhoben, verarbeitet oder genutzt werden. Der Bayerische Rundfunk und die gemeinsame Verwaltungsstelle haben die Daten unverzüglich zu löschen, wenn feststeht, dass sie nicht mehr benötigt werden.

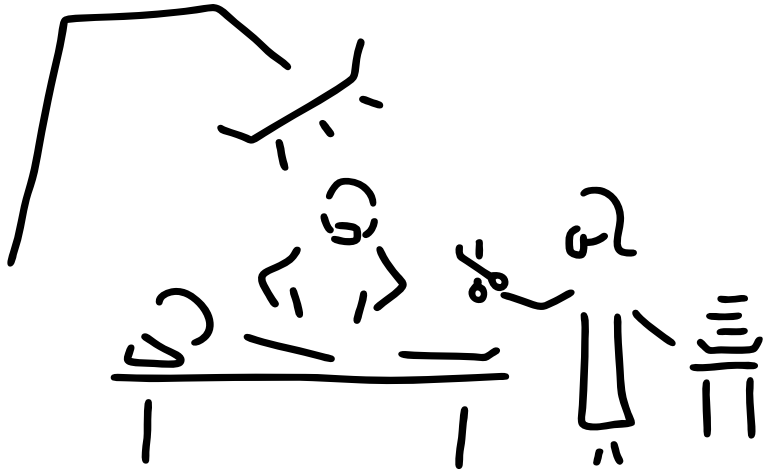
Ein Widerspruchsrecht für Datenübermittlungen an den Beitragsservice von ARD, ZDF und Deutschlandradio ist nicht vorgesehen, weshalb die Eintragung einer melderechtlichen Übermittlungssperre insoweit nicht möglich ist.

§ 35 MeldDV Datenübermittlungen an den Bayerischen Rundfunk
(1) [1]Die Meldebehörden der Haupt- und Nebenwohnung können dem Bayerischen Rundfunk oder der gemeinsamen Verwaltungsstelle nach § 10 Abs. 7 Satz 1 des Rundfunkbeitragsstaatsvertrags vom 7. Juni 2011 (GVBl. S. 258, BayRS 2251-17-S) in der jeweils geltenden Fassung bei einer Anmeldung, Abmeldung oder einem Todesfall folgende Daten volljähriger Einwohner übermitteln:

1. *Familienname*
2. *Vorname*
3. *Doktorgrad*
4. *Geburtsdatum*
5. *derzeitige und letzte frühere Anschrift*
6. *Einzugsdatum und Auszugsdatum, Datum der Anmeldung oder Abmeldung von Amts wegen*
7. *Sterbedatum*

[2]Bei Vorliegen einer Auskunftssperre nach § 51 BMG ist die Übermittlung ausgeschlossen.
(2) [1]Die übermittelten Daten dürfen nur für Zwecke der Beitragserhebung sowie zur Feststellung, ob eine Beitragspflicht nach dem Rundfunkbeitragsstaatsvertrag besteht, erhoben, verarbeitet oder genutzt werden. [2]Der Bayerische Rundfunk und die gemeinsame Verwaltungsstelle haben die Daten unverzüglich zu löschen, wenn feststeht, dass sie nicht mehr benötigt werden. [3]Nicht überprüfte Daten sind spätestens nach zwölf Monaten zu löschen.

7 Gesundheitswesen



7.1 Wearables und Gesundheits-Apps

Wearables und Gesundheits-Apps sind aufgrund ihrer raschen Verbreitung derzeit ein Schwerpunktthema im Gesundheitswesen, das zahlreiche datenschutzrechtliche aber auch ethische Fragen zur Selbstbestimmtheit des Menschen in der Gesellschaft aufwirft. Folgerichtig hat unter meinem Vorsitz der Arbeitskreis Gesundheit und Soziales der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder das Thema ausführlich diskutiert. Die Konferenz hat dazu eine Entschließung „Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen!“ verabschiedet, die am Ende dieses Beitrags im Wortlaut angefügt ist. Darüber hinaus verweise ich auf Nr. 2.2.3 in diesem Tätigkeitsbericht.

Nach meiner Einschätzung dürfte es schwer fallen, die Anforderungen einer wirksamen Einwilligung von Nutzerinnen und Nutzern für Datenverarbeitungsprozesse, insbesondere für die Weitergabe von Gesundheits- und Verhaltensdaten an Dritte, zu erfüllen. Regelmäßig wird zwischen Herstellern, Anbietern oder Verwendern auf der einen und den Nutzerinnen und Nutzern auf der anderen Seite ein erhebliches Verhandlungsungleichgewicht bestehen, so dass Einwilligungserklärungen unwirksam sind. Darüber hinaus befürchte ich, dass aufgrund gesellschaftlicher oder ökonomischer Zwänge nicht jede betroffene Person frei über die Nutzung derartiger Technologien entscheiden kann. Ich habe mich deshalb dahingehend geäußert, dass jedenfalls im Bereich der gesetzlichen Krankenversicherung Vorteile, beispielsweise bei der Tarifgestaltung oder bei Gesundheitsangeboten, nicht von der Einwilligung in die Verwendung solcher Daten abhängig gemacht werden dürfen.

Die Konferenzentschließung berücksichtigt die derzeit relevanten datenschutzrechtlichen Aspekte. Sie lautet:

Entschließung der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 06./07.04.2016

Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen!

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

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

Allerdings stehen diesen Chancen auch Risiken, insbesondere für das Persönlichkeitsrecht, gegenüber. Zahlreiche Wearables und Gesundheits-Apps geben die aufgezeichneten Daten an andere Personen oder Stellen weiter, ohne dass die betroffenen Personen hiervon wissen oder dazu eine bewusste Entscheidung treffen. Darüber hinaus können Bedienungsfehler oder unzureichende technische Funktionalitäten dazu führen, dass Gesundheitsinformationen ungewollt preisgegeben werden. Einige Angebote weisen erhebliche Sicherheitsdefizite auf, so dass auch Unbefugte sich Zugriff auf die Gesundheitsdaten verschaffen können. Für bestimmte Situationen besteht überdies das Risiko, dass Einzelne aufgrund massiver gesellschaftlicher, sozialer oder ökonomischer Zwänge nicht frei über die Nutzung derartiger Technologien entscheiden können. Zum notwendigen Schutz von Gesundheitsdaten bei Wearables und Gesundheits-Apps weist die Datenschutzkonferenz auf folgende Gesichtspunkte hin:

- *Die Grundsätze der Datenvermeidung und Datensparsamkeit sind zu beachten. Insbesondere Hersteller von Wearables und Gesundheits-Apps sind aufgerufen, datenschutzfreundliche Technologien und Voreinstellungen einzusetzen (Privacy by Design and Default). Hierzu gehören Möglichkeiten zur anonymen bzw. pseudonymen Datenverarbeitung. Soweit eine Weitergabe von Gesundheits- und Verhaltensdaten an Dritte nicht wegen einer medizinischen Behandlung geboten ist, sollten Betroffene sie technisch unterbinden können (lediglich lokale Speicherung).*

- *Die Datenverarbeitungsprozesse, insbesondere die Weitergabe von Gesundheits- und Verhaltensdaten an Dritte, bedürfen einer gesetzlichen Grundlage oder einer wirksamen und informierten Einwilligung. Sie sind transparent zu gestalten. Für das Persönlichkeitsrecht riskante Datenverwendungen, insbesondere Datenflüsse an Dritte, sollten für die Nutzerinnen und Nutzer auf einen Blick erkennbar sein. Beispielsweise könnte die Anzeige des Vernetzungsstatus die aktuellen Weitergabe-Einstellungen veranschaulichen. Eine solche Verpflichtung zur erhöhten Transparenz sollte gesetzlich verankert werden.*

- *Einwilligungserklärungen und Verträge, die unter Ausnutzung eines erheblichen Verhandlungsungleichgewichts zwischen Verwendern und den betroffenen Personen zustande kommen, sind unwirksam und liefern keine Rechtsgrundlage für Verarbeitungen. Das gilt namentlich für besonders risikoträchtige Verwendungszusammenhänge, etwa in Beschäftigungs- und Versicherungsverhältnissen.*

- *Verbindliche gesetzliche Vorschriften zur Datensicherheit, insbesondere zur Integrität und Vertraulichkeit von Daten, können nicht durch Verträge oder durch Einwilligungserklärungen abbedungen werden.*

- *Wer aus eigenen Geschäftsinteressen gezielt bestimmte Wearables und Gesundheits-Apps in den Umlauf bringt oder ihren Vertrieb systematisch unterstützt, trägt eine Mitverantwortlichkeit für die rechtmäßige Ausgestaltung solcher Angebote. In diesem Sinne Mitverantwortliche haben sich zu vergewissern, dass die Produkte verbindlichen Qualitätsstandards an IT-Sicherheit, Funktionsfähigkeit sowie an Transparenz der Datenverarbeitung genügen.*

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

7.2 Flüchtlinge und Asylsuchende

Die vor allem in der zweiten Jahreshälfte 2015 stark ansteigende Zahl von Asylsuchenden führte vermehrt auch zu datenschutzrechtlichen Anfragen rund um deren Aufnahme, Unterbringung und Betreuung.

Flüchtlinge unterscheiden sich von Asylbewerberinnen und -bewerbern dadurch, dass ihr Status als Flüchtling von einer nationalen Regierung anerkannt wurde. Asylbewerberinnen und -bewerber sind Personen, die internationalen Schutz suchen, ihn aber noch nicht bekommen haben. Oft handelt es sich um Menschen, die noch auf die Entscheidung einer Regierung warten, ob ihnen der Flüchtlingsstatus zuerkannt wird oder nicht.

7.2.1 Videoüberwachung von Unterkünften für Asylsuchende

Die Unterbringung von Asylsuchenden erfolgt regelmäßig in staatlich betriebenen Aufnahmeeinrichtungen und Gemeinschaftsunterkünften.

Auf Anfragen zur Zulässigkeit einer Videoüberwachung solcher Unterkünfte habe ich unter Hinweis auf das von meiner Homepage https://www.datenschutz-bayern.de abrufbare Prüfungsschema zur Videobeobachtung und Videoaufzeichnung (Videoüberwachung) wie folgt geantwortet:

Zunächst ist der Schutz der Bewohnerinnen und Bewohner dieser Unterkünfte ein Zweck, der mit den in Art. 21a Abs. 1 Satz 1 BayDSG genannten schutzwürdigen Rechtsgütern wie Leben und Gesundheit vereinbar ist. Weiter muss die Videoüberwachung zum Schutz der genannten Rechtsgüter im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts erforderlich sein.

Der Schutz der Asylsuchenden als öffentliche Aufgabe der „Gefahrenabwehr“ ist grundsätzlich ein Überwachungszweck, der eine Videoüberwachung rechtfertigen kann.

Die Ausübung des Hausrechts dagegen kann regelmäßig – wenn überhaupt – nur die Videoüberwachung eines engen Bereichs im unmittelbaren Umgriff der Einrichtung rechtfertigen, insbesondere der Eingangsbereiche. Das Hausrecht ist das Recht der öffentlichen Stelle, über die Benutzung eines geschützten Raumes zu bestimmen und insbesondere auch jemanden aus einem Gebäude beziehungsweise von einem Grundstück der öffentlichen Stelle zu verweisen oder ihm den Zutritt hierzu zu verweigern (siehe Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Art. 21a Rn. 17). Eine unbeschränkte und womöglich personenscharfe Erfassung und Speicherung des Geschehens etwa auf der gesamten Fahrbahnbreite inklusive der Gehwege vor der Einrichtung ist kritisch zu beurteilen. Es besteht die Gefahr, dass eine Videoüberwachung in diesem Ausmaß zu einer unzulässigen Beeinträchtigung überwiegender schutzwürdiger Interessen von Betroffenen führt (siehe Art. 21a Abs. 1 Satz 2 BayDSG). Bewohnerinnen und Bewohner, aber auch Beschäftigte haben häufig die öffentlichen Straßen und Gehwege zu nutzen, beispielsweise um den täglichen Weg zur Arbeitsstelle zurückzulegen.

Ich habe angeregt, bei der Ausübung des Ermessens- und Beurteilungsspielraums folgende Fragen einzubeziehen:

— Ist die Videoüberwachung neben anderen vorrangigen Sicherungsmaßnahmen (Einzäunung des Geländes oder Einsatz eines Sicherheitsdienstes) erforderlich?

— Gibt es Zeiten, in denen auf einen Betrieb der Videoüberwachungsanlage verzichtet werden kann? Dies könnte der Fall sein, wenn zu bestimmten Tages- oder Nachtzeiten in einem ausreichenden Maß Sicherheitspersonal vor Ort anwesend ist, das in Gefährdungssituationen einschreiten oder weitere Hilfe anfordern kann.

— Ist die (bloße) Videobeobachtung ausreichend oder bedarf es auch einer zusätzlichen Videoaufzeichnung?

Bei Videoaufzeichnungen (= Speicherung) ist eine Verfahrensbeschreibung und eine Freigabe durch die jeweiligen behördlichen Datenschutzbeauftragten erforderlich. Dabei sind zusätzliche Angaben zu machen (Art. 21a Abs. 6 BayDSG), insbesondere zur Speicherdauer und zu Einsichts- und Auswertungsrechten.

Videoüberwachungsmaßnahmen sind nach Art. 21a Abs. 2 BayDSG transparent zu gestalten, indem die Tatsache der Videoüberwachung und die erhebende Stelle auf geeignete Weise erkennbar gemacht werden. In der Praxis bewährt hat sich dabei das Anbringen entsprechender Hinweisschilder.

Nach Art. 75a Abs. 1 Nr. 1 Bayerisches Personalvertretungsgesetz hat der Personalrat sowohl bei Einführung als auch bei Anwendung und erheblicher Änderung technischer Einrichtungen mitzubestimmen, die an sich – was nach der Rechtsprechung bereits ausreichend ist – zur Überwachung des Verhaltens oder der Leistung der Beschäftigten geeignet sind. Darunter fallen auch Maßnahmen der Videoüberwachung, wenn die Bediensteten sich (auch) in Bereichen bewegen, von denen mit den Kameras Bilder erzeugt werden.

7.2.2 Video- und Telefondolmetscher in Aufnahmeeinrichtungen für Asylsuchende

Bei der Aufnahme, Registrierung und Erstuntersuchung von Asylbewerberinnen und -bewerbern spielt die Verständigung zwischen Behörden und Betroffenen eine wichtige Rolle. In diesem Zusammenhang hat mich folgende Anfrage erreicht:

Der Einsatz von Präsenzdolmetscherinnen und -dolmetschern bringe einen erheblichen Kosten- und Koordinierungsaufwand mit sich. Dieser könne durch video- oder telefongestützte Übersetzungen verringert werden. Dabei sollten über eine Software verschiedene Sprachen angeboten werden. Bei Auswahl einer bestimmten Sprache werde bereits nach kurzer Zeit eine entsprechende Dolmetscherin oder ein entsprechender Dolmetscher über Videochat oder Telefon zur Verfügung gestellt. Zur Frage, ob und gegebenenfalls welche datenschutzrechtlichen Vorgaben zu beachten seien, habe ich mich wie folgt geäußert:

Das Dolmetschen im Auftrag öffentlicher Stellen ist nur in Teilbereichen gesetzlich geregelt. In Gerichtsverfahren (§ 185 Abs. 1 Satz 1 Gerichtsverfassungsgesetz – GVG) und in Asylverfahren (§ 17 Abs. 1 Asylgesetz – AsylG) ist die Zuziehung von Sprachmittlerinnen und Sprachmittlern verpflichtend, wenn die betroffene Person der deutschen Sprache nicht mächtig oder nicht hinreichend kundig ist. Gemäß § 189 Abs. 4 Satz 1 GVG soll der Hinzugezogene über Umstände, die ihm bei seiner Tätigkeit zur Kenntnis gelangen, Verschwiegenheit wahren.

Entsprechende Vorschriften für die Registrierung und Erstuntersuchung von Asylsuchenden gibt es nicht. Da hierbei regelmäßig besonders sensible personenbezogene Daten anfallen (vgl. Art. 15 Abs. 7 BayDSG), kommt der Qualität der Dolmetscherleistung und der Verschwiegenheit der Dolmetscherinnen und Dolmetscher entscheidende Bedeutung zu.

Ich habe deshalb angeregt, bei der Personalauswahl entsprechend der Bekanntmachung des Staatsministeriums der Justiz und für Verbraucherschutz zur Ausführung des Dolmetschergesetzes (Dolmetschergesetzausführungsbekanntmachung – DolmGABek) vom 11. März 2010 zu verfahren. Nr. 8 DolmGABek bestimmt zur Heranziehung von Dolmetschern und Übersetzern Folgendes:

8.1 Sprachübertragungen für gerichtliche und behördliche Zwecke sollen grundsätzlich nur Dolmetscher und Übersetzer vornehmen, die in der länderübergreifenden Dolmetscher- und Übersetzerdatenbank eingetragen sind. Aus der Datenbank geht hervor, in welchem Land ein öffentlich bestellter und allgemein beeidigter Dolmetscher (Übersetzer) tätig ist. Bei nur vorübergehend und gelegentlich tätigen Dolmetschern und Übersetzern ist die Bestellungs- oder Anerkennungsbehörde des Niederlassungsstaats aus der Datenbank ersichtlich.

8.2 Andere geeignete Dolmetscher und Übersetzer können herangezogen werden, wenn eingetragene Dolmetscher und Übersetzer nicht zur Verfügung stehen oder wenn deren Heranziehung unverhältnismäßig hohe Kosten verursachen würde. Ohne ausdrückliche Zustimmung des zuständigen Richters, Staatsanwalts oder Rechtspflegers sollen die Geschäftsstellen die Ladung oder Beauftragung eines nicht eingetragenen Dolmetschers oder Übersetzers nicht bewirken.

Öffentlich bestellte und allgemein beeidigte Dolmetscherinnen und Dolmetscher haben ihre fachliche und persönliche Eignung nachgewiesen und sind nach dem Dolmetschergesetz (DolmG) zur Verschwiegenheit verpflichtet.

Art. 10 DolmG
Dem Dolmetscher (Übersetzer) ist es untersagt, Tatsachen, die ihm bei der Ausübung seiner Tätigkeit zur Kenntnis gelangen, Dritten unbefugt mitzuteilen oder sie zum Nachteil anderer zu verwerten.

Über diese allgemeinen Anforderungen hinaus konnte ich zum geplanten Einsatz von Video- oder Telefondolmetscherinnen und -dolmetschern keine datenschutzrechtliche Einschätzung abgeben, da mir der Sachverhalt nicht hinreichend klar war.

Offen war zum Beispiel, wer verantwortliche Stelle für die Auswahl und den Einsatz der Video- oder Telefondolmetscherinnen und -dolmetschern sein würde: Das fachlich zuständige Staatsministerium, die Regierungen als Betreiberinnen der Aufnahmeeinrichtungen oder die Gesundheitsämter als zuständige Behörden für die Erstuntersuchung?

Die Beauftragung von Video- oder Telefondolmetscherinnen und -dolmetschern bedarf eines Datenschutzkonzepts, das über die genannten Punkte (Qualität, Verschwiegenheit, verantwortliche Stelle) hinaus insbesondere auch auf die Rechtsgrundlagen für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten eingeht.

Auch technisch-organisatorische Fragestellungen sollte das Datenschutzkonzept aufgreifen, zum Beispiel:

- Wer stellt die erforderlichen technischen Kommunikationsmittel zur Verfügung?
- Wie findet die Datenübertragung statt (IP, ISDN)?
- Wer ist für die Sicherheit der Komponenten verantwortlich?
- Können Dritte die Gespräche mithören (etwa in Einzel- oder Großraumbüros)?
- Werden Dolmetschergespräche aufgenommen oder zwischengespeichert? Gegebenenfalls bedarf es dann einer datenschutzrechtlichen Freigabe im Sinne des Art. 26 BayDSG.

7.2.3 Gesundheitsuntersuchung bei Flüchtlingen

Nach § 62 Asylgesetz (AsylG) sind Ausländer, die in einer Aufnahmeeinrichtung oder Gemeinschaftsunterkunft zu wohnen haben, verpflichtet, eine ärztliche Untersuchung auf übertragbare Krankheiten einschließlich einer Röntgenaufnahme der Atmungsorgane zu dulden. Die oberste Landesgesundheitsbehörde oder die von ihr bestimmte Stelle legt den Umfang der Untersuchung fest (in Bayern im Hinblick auf übertragbare Krankheiten, Tuberkulose, Ruhr, Cholera, Hepatitis B, Lues, HIV I und II) und benennt den Arzt, der die Untersuchung durchführt.

Eine Information der Betroffenen war in Bayern bisher grundsätzlich nicht vorgesehen. Konkret bedeutete das in der Vergangenheit zumeist, dass Flüchtlinge Stuhl, Urin und Blut zur Untersuchung abgaben, ohne zu wissen, welche Untersuchungen mit diesen Proben durchgeführt werden.

Eine bereichsspezifische datenschutzrechtliche Regelung für die mit der Untersuchung einhergehenden Datenerhebungen besteht nicht. Deren Zulässigkeit richtet sich demnach nach der im allgemeinen Datenschutzrecht enthaltenen Regelung des Art. 16 Abs. 3 BayDSG, auf die ich das Staatsministerium für Gesundheit und Pflege hingewiesen habe.

Art. 16 BayDSG Erhebung
(3) Werden personenbezogene Daten beim Betroffenen mit seiner Kenntnis erhoben, so ist der Erhebungszweck ihm gegenüber anzugeben. Werden sie beim Betroffenen auf Grund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Auf Verlangen ist der Betroffene über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären. Bei einer Datenerhebung auf schriftlichem Weg ist die Rechtsvorschrift stets anzugeben.

Das Gesundheitsministerium hat ein mit mir abgestimmtes Merkblatt „Informationen zu Ihrer Gesundheitsuntersuchung" erstellt und mit Piktogrammen versehen. Dieses Merkblatt wird in zehn Sprachen übersetzt. Es soll im Vorfeld der Gesundheitsuntersuchung den Asylsuchenden ausgehändigt werden. Auf diese Weise werden die Betroffenen über die mit der Gesundheitsuntersuchung einhergehende Datenerhebung sowie den Zweck der Untersuchung entsprechend der datenschutzrechtlichen Vorgaben informiert.

Darüber hinaus hat das Gesundheitsministerium eine Bekanntmachung zum Vollzug des § 62 AsylG sowie weitere Vollzugshinweise erlassen, die mit mir ebenfalls abgestimmt wurden.

7.2.4 Datenübermittlung im Rahmen der Beratung und Betreuung von Asylsuchenden durch Wohlfahrtsverbände und Helferkreise

Im Berichtszeitraum war ich wiederholt auch mit Fragen rund um die Beratung und Betreuung von Asylsuchenden befasst.

Die soziale Beratung und Betreuung von Asylsuchenden ist keine staatliche Aufgabe. Träger der Asylsozialberatung in Bayern sind regelmäßig die Verbände der freien Wohlfahrtspflege, also Caritasverband, Diakonisches Werk, Bayerisches Rotes Kreuz, Arbeiterwohlfahrt und Paritätischer Wohlfahrtsverband. Dies ergibt sich aus der Asylsozialberatungs-Richtlinie (Richtlinie für die Förderung der sozialen Beratung und Betreuung von Leistungsberechtigten nach dem Asylbewerberleistungsgesetz und von Ausländerinnen und Ausländern in staatlichen Unterkünften), die auch Grundlage ist für die finanzielle Förderung durch den Freistaat Bayern. Neben den Wohlfahrtsverbänden kümmern sich auch viele Ehrenamtliche und Helferkreise um die Beratung und Betreuung der Asylsuchenden.

— Dürfen Behörden personenbezogene Daten von Asylsuchenden an Wohlfahrtsverbände und ehrenamtliche Helferkreise herausgeben?

  Helferkreise und Wohlfahrtsverbände argumentieren, dass sie durch die Übermittlung entsprechender Listen die Asylsuchenden schneller, individueller und bedarfsgerechter beraten und betreuen könnten.

Ohne wirksame Einwilligung der Betroffenen halte ich dies für nicht zulässig, da weder das Bayerische Datenschutzgesetz noch eine andere Rechtsvorschrift die Übermittlung erlaubt oder anordnet. Insbesondere erfordert es die Unterstützung der Neuankömmlinge bei der Erfüllung melderechtlicher Pflichten nicht, einen Überblick über alle etwa im Landkreis untergebrachten Asylsuchenden zu haben. Insoweit wäre die Übermittlung der vom Landratsamt geführten Listen unverhältnismäßig. Angesichts des Umfangs und der Sensibilität der in solchen Listen aufgeführten personenbezogenen Daten halte ich es für angezeigt, den Kreis der Listeninhaberinnen und -inhaber so klein wie möglich zu halten, auch um der Gefahr eines etwaigen Missbrauchs zu begegnen.

Selbstverständlich dürfen die Wohlfahrtsverbände und ehrenamtlichen Helferkreise ihre Hilfsangebote in allgemeiner Form an die Asylsuchenden herantragen. Diese können dann selbst darüber entscheiden, ob und inwieweit sie eine Kontaktaufnahme oder eine Unterstützung wünschen. Insoweit halte ich es für vertretbar, dass die Anschriften der dezentralen Unterkünfte an die Wohlfahrtsverbände weitergegeben werden, gegebenenfalls verbunden mit der Angabe, wie viele Personen aus welchen Nationen dort jeweils untergebracht sind.

— Dürfen Helferkreise eine eigene Datenbank aufbauen?

Ob und unter welchen Voraussetzungen die Helferkreise eine eigene Datenbank aufbauen dürfen, kann ich als Landesbeauftragter für den Datenschutz nicht beurteilen. Da es sich bei den ehrenamtlichen Helferkreisen um nicht-öffentliche Stellen handelt, obliegt die Prüfung einer entsprechenden Datenerhebung, -verarbeitung und -nutzung dem Landesamt für Datenschutzaufsicht als zuständiger Datenschutzbehörde für den nicht-öffentlichen Bereich.

— Dürfen Krankenhäuser Patientendaten von Asylsuchenden an Sozialbetreuerinnen oder -betreuer herausgeben?

Die soziale Betreuung von Asylsuchenden durch Angehörige von Wohlfahrtsverbänden oder von ehrenamtlichen Helferkreisen ist nicht mit der rechtlichen Betreuung im Sinne der §§ 1896 ff. Bürgerliches Gesetzbuch vergleichbar. Insbesondere ergibt sich aus einem freiwilligen Betreuungsverhältnis – anders als bei der gerichtlich angeordneten Betreuung – regelmäßig keine Vertretungsmacht nach außen.

Insofern besteht für die Sozialbetreuerinnen und -betreuer auch keine generelle Vollmacht zur Entgegennahme von Auskünften über den Gesundheitszustand der von ihnen Betreuten. Stehen die Auskünfte im Zusammenhang mit einem Krankenhausaufenthalt, müssen die Asylsuchenden grundsätzlich ausdrücklich in die Übermittlung von Patientendaten an Sozialbetreuerinnen oder -betreuer einwilligen. Kommen Asylsuchende in deren Begleitung zur Behandlung ins Krankenhaus, kann je nach den Umständen des Einzelfalls auch eine konkludente Einwilligung in Betracht kommen.

7.2.5 Einwilligung der Asylsuchenden gegenüber dem Landratsamt zur Datenübermittlung an verschiedene Stellen

Das Sachgebiet „Asylbewerberleistungen und -betreuung“ eines Landratsamts wurde von verschiedenen Stellen um die Übermittlung personenbezogener Daten von Asylsuchenden gebeten. Bei den anfragenden Stellen handelte es sich unter anderem um Schulamt, Gesundheitsamt, Ausländerbehörde, Jugendamt, Schulen, medizinische Leistungserbringer, Gemeinden, Bezirksregierung, Bundesamt für Migration und Flüchtlinge, Jobcenter, Wohlfahrtsverbände, Bundesagentur für Arbeit und Unterkunftsbetreiber. Um die Vielzahl der Anfragen zeitnah bearbeiten zu können, war geplant, die Betroffenen allgemein verfasste Einwilligungserklärungen unterschreiben zu lassen. Dadurch sollte die Weitergabe personenbezogener Daten etwa für Zwecke der Gesundheitsversorgung, der sozialen Betreuung, für schulische Zwecke oder zur Beschleunigung des Asylverfahrens ermöglicht werden.

Bei den anfragenden Stellen handelte es sich teils um öffentliche, teils um nichtöffentliche Stellen, teils um Landesbehörden und teils um Bundesbehörden. Das wirkt sich unmittelbar auf die Frage nach den einschlägigen datenschutzrechtlichen Regelungen, aber auch auf die Frage nach der zuständigen Datenschutzaufsicht aus, zumindest was die Beurteilung der Erhebungsbefugnis der anfragenden Stellen anbelangt. Für Bundesbehörden ist insoweit die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, für nicht-öffentliche Stellen in Bayern ist grundsätzlich das Landesamt für Datenschutzaufsicht und für kirchliche Wohlfahrtsverbände (Caritas, Diakonie) sind die kircheninternen Datenschutzbeauftragten zuständig.

Im Ergebnis muss jeder Datenfluss für sich betrachtet werden, etwa um beurteilen zu können, ob eine Datenübermittlung nicht bereits gesetzlich erlaubt oder angeordnet ist. In diesen Fällen kommt es auf eine Einwilligung der Betroffenen gar nicht mehr an.

Beispielsweise regelt § 11 Abs. 3 Asylbewerberleistungsgesetz den Datenabgleich mit den Ausländerbehörden. Demnach überprüft die zuständige Behörde die Personen, die Leistungen nach diesem Gesetz beziehen, auf Übereinstimmung der ihr vorliegenden Daten mit den der Ausländerbehörde über diese Personen vorliegenden Daten und darf dafür der zuständigen Ausländerbehörde unter anderem Name, Vorname (Rufname), Geburtsdatum, Geburtsort, Staatsangehörigkeiten, Geschlecht, Familienstand, Anschrift, Aufenthaltsstatus und Aufenthaltszeiten dieser Personen übermitteln.

Weitere Beispiele für spezialgesetzliche Regelungen sind § 87 Aufenthaltsgesetz (Übermittlungen an Ausländerbehörden) und § 8 Asylgesetz (Übermittlung personenbezogener Daten an das Bundesamt für Migration und Flüchtlinge).

Im Übrigen richtet sich die Zulässigkeit von Datenübermittlungen durch das Sachgebiet „Asylbewerberleistungen und -betreuung“ grundsätzlich nach den allgemeinen Vorschriften des Bayerischen Datenschutzgesetzes.

Fehlt es im Verhältnis der anfragenden Stellen zum Sachgebiet „Asylbewerberleistungen und -betreuung“ an entsprechenden gesetzlichen Erhebungs- und Übermittlungsbefugnissen, ist die Übermittlung personenbezogener Daten nur zulässig, wenn die Betroffenen eingewilligt haben (siehe Art. 15 Abs. 1 BayDSG).

Die geplante Einwilligungserklärung war aber aus mehreren Gründen nicht datenschutzkonform. Weder die Adressaten der Datenübermittlung noch der konkrete Verwendungsweck wurden abschließend benannt, sondern nur beispielhaft aufgezählt („etc."). Die Betroffenen konnten deshalb nicht erkennen, welche Daten an welche Stelle zu welchem Zweck übermittelt werden sollen.

Die Einwilligung muss stets freiwillig sein. Das setzt voraus, dass sich die Betroffenen über die Tragweite ihrer Einwilligung im Klaren sind, insbesondere über den Verarbeitungszweck bei der anfragenden Stelle. Auch müssen die Asylsuchenden die Möglichkeit haben, nur in einzelne Datenübermittlungen einwilligen beziehungsweise in der Folge diese auch widerrufen zu können. Eine pauschale Einwilligungserklärung in alle relevanten Datenübermittlungen scheidet von vornherein aus. Die Betroffenen sind auch darüber zu informieren, was geschieht, wenn sie nicht einwilligen. Die Folgen einer ablehnenden Entscheidung dürfen für die Betroffenen nicht unzumutbar sein, so dass aus diesem Grunde die Freiwilligkeit fraglich wäre.

In den Einwilligungserklärungen muss der jeweilige Datenstrom verständlich beschrieben werden. Das setzt in diesem sensiblen Bereich Formulare in den maßgeblichen Fremdsprachen voraus. Nur so kann gewährleistet werden, dass die Einwilligung tatsächlich informiert und freiwillig erfolgt. Je nach anfragender Stelle bedarf die entsprechende Einwilligungserklärung auch der Abstimmung mit den weiteren Datenschutzbehörden.

7.3 Krebsregister

Das Thema Krebsregister beschäftigt mich seit vielen Jahren. Im 26. Tätigkeitsbericht 2014 unter Nr. 7.3, der auf weitere Tätigkeitsberichte in den zurückliegenden Jahren verweist, habe ich mich bereit erklärt, auch weiterhin meine Expertise einzubringen, um insbesondere den derzeitigen rechtswidrigen Zustand in einigen klinischen Krebsregistern zu beenden. Im Berichtszeitraum wurde nun erstmals ein Gesetzentwurf vorgelegt, dessen Eckpunkte zuvor von der Staatsregierung beschlossen worden waren. Ich hätte mir gewünscht, auch bei der Erarbeitung der Eckpunkte bereits frühzeitiger eingebunden zu werden, zumal eine Neuausrichtung im Verfahren der Krebsregistrierung festgelegt werden soll. Bislang haben viele voneinander unabhängige Stellen das Bayerische Krebsregister getragen; nun soll es zentral am Landesamt für Gesundheit und Lebensmittelsicherheit (LGL) eingerichtet werden. Auch die bisher klinischen Krebsregister und Tumorzentren sollen als Regionalzentren Teil des LGL werden. Die Zuständigkeit einer öffentlichen Stelle hat den Vorzug, dass diese für die Beachtung sämtlicher datenschutzrechtlicher Vorschriften in der Krebsregistrierung verantwortlich sein wird und mir bei Kontrollen mit Weisungs- und Durchsetzungskompetenzen gegenüber den nach wie vor zahlreichen beteiligten Stellen (unter dem Dach des LGL) zur Verfügung stehen wird.

Eine zentrale Registerstruktur wird aber auch erhebliche Risiken für die Sicherheit und Vertraulichkeit von Patientendaten beinhalten.

Ich habe es daher für dringend erforderlich angesehen, meine wesentlichen Standpunkte zur Neustrukturierung der Bayerischen Krebsregistrierung durch ein Bayerisches Krebsregistergesetz sehr deutlich zum Ausdruck zu bringen.

- Die in datenschutzrechtlicher Hinsicht grundsätzlich problematische Zentralisierung des Bayerischen Krebsregisters am LGL erfordert rechtliche, technische und organisatorische Regelungen, die einen umfassenden Schutz der im Mittelpunkt stehenden Patientendaten gewährleisten müssen.

- Die Einführung einer Meldepflicht stellt einen erheblichen Eingriff in das Grundrecht der Patientinnen und Patienten auf informationelle Selbstbestimmung dar (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz). Darüber hinaus bedeutet eine Meldepflicht für die Ärzteschaft eine erhebliche Belastung des durch die ärztliche Schweigepflicht geschützten Vertrauensverhältnisses zu den Patientinnen und Patienten. Verfassungsrechtlich hinnehmbar ist dieser Eingriff lediglich unter den Voraussetzungen, dass insbesondere die Transparenz des Verfahrens, eine umfassende Information der Betroffenen über die wesentlichen Datenflüsse, ein effektives Widerspruchsrecht, ein Auskunftsrecht über alle zur Person gespeicherten Daten und die Einhaltung von Löschungspflichten gewährleistet werden.

- Der Grundsatz der Transparenz und die Grundsätze der Normbestimmtheit und Normenklarheit geben verfassungsrechtlich zwingend vor, dass das Bayerische Krebsregistergesetz aus sich heraus für die betroffenen Patientinnen und Patienten verständlich ist: Einschränkungen des Grundrechts auf informationelle Selbstbestimmung bedürfen einer gesetzlichen Grundlage, aus der sich deren Voraussetzungen und Umfang klar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entsprechen – siehe bereits das Urteil des Bundesverfassungsgerichts vom 23. Februar 2007 (1 BvR 2368/06).

Ich habe im Rahmen der Beteiligung am Gesetzgebungsprozess Zweifel geäußert, ob der Entwurf eines Bayerischen Krebsregistergesetzes (BayKRegG-E) diese Grundsätze erfüllt:

- Die Struktur beziehungsweise Organisation der Krebsregistrierung in Bayern ist aus dem Gesetz nicht klar erkennbar. Art. 2 BayKRegG-E enthält lediglich rudimentäre Regelungen. So ist definiert, dass das Bayerische Krebsregister vom LGL geführt wird, und dass eine landesweit tätige Vertrauensstelle eingerichtet wird, die dauerhaft Klardaten speichern darf. Der patienten- und meldernahe Vollzug wird über Dienststellen des LGL sichergestellt. In Art. 17b BayKRegG-E werden die zum Vollzug des Bayerischen Krebsregistergesetzes unterhaltenen weiteren Dienststellen des LGL aufgeführt: die Regionalzentren und die bayernweit tätige Servicestelle. Die Aufgaben sowie die Aufgabenverteilung auf die verschiedenen Stellen werden nicht dargelegt. Insbesondere wird nicht deutlich, wo genau personenbezogene Patientendaten (Klarnamen und Anschriften) gespeichert werden. Ich habe darauf hingewiesen, dass eine mehrfache Datenhaltung unterbleiben muss. Die identifizierenden Daten der Patientinnen und Patienten dürfen dauerhaft entweder nur in den Regionalzentren oder in der zentralen Dienststelle der Vertrauensstelle gespeichert werden. Das Zentrum für Krebsfrüherkennung und -krebsregistrierung wird im Gesetz überhaupt nicht erwähnt.

Die wesentlichen Regelungsgegenstände müssen jedoch im Gesetz enthalten sein (Wesentlichkeitstheorie des Bundesverfassungsgerichts, vgl. BVerfGE 33, 303; BVerfGE 47, 46; BVerfGE 49, 89). Es ist auch nicht erkennbar, dass die Verordnungsermächtigungen nähere Regelungen für die Organisation und Struktur des Bayerischen Krebsregisters in Form von Rechtsverordnungen ermöglichen. Zumindest müsste zu den gesetzlichen Regelungen zugleich eine Rechtsverordnung vorliegen, die mindestens in der Zusammenschau klar erkennen lässt, wie das Bayerische Krebsregister organisiert ist und welche Stellen welche Aufgaben und Befugnisse, insbesondere datenschutzrechtliche Befugnisse, innehaben. Dies ist nicht der Fall.

— Für die Patientinnen und Patienten besteht nur ein eingeschränktes Widerspruchsrecht. Sie haben keine Möglichkeit, ihre Daten vollständig löschen oder anonymisieren zu lassen. Art. 5 BayKRegG-E sieht nur das Recht zum Widerspruch gegen eine dauerhafte Speicherung der Identitätsdaten vor. Laut Protokoll habe ich im Gesundheitsausschuss des Bayerischen Landtags am 31. Mai 2016 ausgeführt: „Der betroffene Patient müsse zum Zeitpunkt der Befunderstellung vom Arzt über die Registrierung unterrichtet werden, sodass er entscheiden könne, ob er der Erfassung seiner Daten durch das Klinikregister zustimme oder widerspreche. Widerspreche er einer Weiterleitung, so müssten seine Daten komplett gelöscht werden.“ (Protokoll des Bayerischen Landtags, Ausschuss für Gesundheit und Pflege, 44. Sitzung, Seite 7).

  Das nicht umfassend gewährte Widerspruchsrecht greift in das Allgemeine Persönlichkeitsrecht der Betroffenen in massiver Weise ein. Dieses Recht umfasst die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden, und daher grundsätzlich selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen (vgl. BVerfGE 65, 1 <42 f.>; 67, 100 <143>). Bereits mit der Einführung der Meldepflicht wird dieser Grundsatz umgangen. Insoweit würde ich meine Bedenken zwar zurückstellen, sofern ein Widerspruch der Betroffenen im Ergebnis dazu führt, dass alle ihre Daten nicht mehr für die Krebsregistrierung verwendet werden dürfen. Dies ist jedoch nicht der Fall. Es wurde auf meinen Vorschlag hin zumindest eine Evaluationsklausel über das Widerspruchsverfahren eingefügt. Sollte sich zeigen, dass die Widerspruchsquote gering ist und die Funktionsfähigkeit der Krebsregistrierung dadurch nicht beeinträchtigt wird, sollten in diesen Fällen nicht nur die Identitätsdaten der Widersprechenden, sondern auch sämtliche Daten zur Krankheitsgeschichte gelöscht werden.

  Mein darüber hinaus gehender Vorschlag, den ich zum ersten Mal dem Landesgesundheitsrat vorgestellt habe, lautet allerdings wie folgt:

  Vorschlag zu Art. 5 BayKRegG-E Widerspruchsrecht:

  (1) [1]Jeder kann der dauerhaften Speicherung der Daten im Bayerischen Krebsregister widersprechen, soweit sie ihn selbst oder eine seiner Personensorge oder Betreuung unterstehende Person betreffen. [2]Diese Daten sind unverzüglich und vollständig zu löschen, sobald sie für Zwecke der verpflichtenden Qualitätssicherung, Abrechnung

oder auf Grund anderer gesetzlicher Vorschriften nicht mehr benötigt werden. … [5]Der Widerspruch betrifft bereits erfasste sowie künftig eingehende Daten. …

(3) [1]Das für die Gesundheit zuständige Staatsministerium (Staatsministerium) überprüft zwei Jahre nach Inkrafttreten dieses Gesetzes die Regelungen der Abs. 1 und 2 unter den Gesichtspunkten eines wirksamen Datenschutzes und einer ausreichenden Qualitätssicherung für die Zwecke des Bayerischen Krebsregisters. [2]Ergibt die Überprüfung eine Beeinträchtigung der Funktionsfähigkeit der Krebsregistrierung, wird das Staatsministerium ermächtigt, die unverzügliche und vollständige Löschung von Daten nach Abs. 1 Satz 2 auf die Identitätsdaten zu beschränken. [3]Die Beschränkung ist nach zwei Jahren zu überprüfen.

Begründung:
Ein effektives Widerspruchsrecht für Patientinnen und Patienten ist nur sichergestellt, wenn die Identitätsdaten und die Krankheitsdaten vollständig gelöscht werden. Für den Fall, dass eine hohe Widerspruchsquote dazu führt, dass die Funktionsfähigkeit der Krebsregistrierung beeinträchtigt wird und das Ziel einer möglichst flächendeckenden Erfassung nicht mehr erreicht werden kann, wird das Staatsministerium ermächtigt, die Krankheitsdaten weiterhin zu verwenden und die Löschung auf die Identitätsdaten zu begrenzen. Nach zwei Jahren ist die Beschränkung des Widerspruchsrechts erneut zu überprüfen.

– Im Gesetzentwurf ist eine Trennung von Identitätsdaten und medizinischen Daten nicht mehr verwirklicht; insbesondere in der Vertrauensstelle sind keine getrennten Vertrauens- und Registerbereiche erkennbar. Dies ist jedoch Voraussetzung für die Datennutzung zu eigenen Forschungszwecken. Für die Forschung mit Patientendaten gilt der Grundsatz, dass diese im Regelfall nur mit pseudonymisierten oder anonymisierten Daten betrieben werden darf. Daher ist zwischen den verschiedenen Stellen der Vertrauensstelle sowie den sonstigen Stellen des Bayerischen Krebsregisters eine räumliche, personelle, technische und organisatorische Trennung nötig. Dies betrifft auch eine Datentrennung, wie sie früher über Vertrauensbereiche und Registerbereiche der klinischen Krebsregister realisiert war. Auch in diesem Zusammenhang möchte ich auf meine Ausführungen im Gesundheitsausschuss des Bayerischen Landtags hinweisen (Protokoll, a.a.O., Seite 9).

Der Gesetzentwurf, der auf Ebene der Staatsregierung immer wieder erhebliche Veränderungen erfahren hat, ist nun sehr schlank gehalten. Ich gehe davon aus, dass mich das Krebsregister auch weiterhin stark beschäftigen wird. Denn erst mit dem Erlass von Rechtsverordnungen und weiteren Ausführungsbestimmungen, die bei Redaktionsschluss des Tätigkeitsberichts noch nicht vorlagen, werden die Aufgaben und Befugnisse der beteiligten Stellen konkretisiert. Ich habe darum gebeten, hier frühzeitig die Möglichkeit zur Stellungnahme zu erhalten. Wichtig ist mir auch die Mitarbeit an einem Informationsblatt für Patientinnen und Patienten. Es sollte allgemein verständlich über den Zweck der Meldung und das Widerspruchsrecht der Betroffenen, aber auch über Auskunftsrechte, Löschfristen und über die an dem Bayerischen Krebsregister beteiligten Stellen sowie über die Datenflüsse informieren.

7.4 Gesundheitsamt

7.4.1 Vorlage von Impfnachweisen bei Schuleingangsuntersuchungen und weiteren schulischen Impfberatungen

Im 26. Tätigkeitsbericht 2014 unter Nr. 7.1.2 habe ich über die zum 1. Januar 2013 eingeführte gesetzliche Verpflichtung zur Vorlage von Impfdokumenten bei Schuleingangsuntersuchungen und weiteren schulischen Impfberatungen berichtet. Die in Art. 14 Abs. 5 Satz 8 des Gesundheitsdienst- und Verbraucherschutzgesetzes (GDVG) getroffene Neureglung verfolgte das Ziel, Impflücken insbesondere auch bei jungen Menschen zu begegnen.

Art. 14 GDVG Schutz der Gesundheit von Kindern und Jugendlichen
(5) … [8]Bei der Schuleingangsuntersuchung nach Satz 4 und bei weiteren schulischen Impfberatungen sind vorhandene Impfausweise und Impfbescheinigungen (§ 22 IfSG) der Kinder durch die Personensorgeberechtigten vorzulegen. …

Die Pflicht zur Vorlage von Impfausweisen und Impfbescheinigungen wurde auf meine Empfehlung hin zunächst auf drei Jahre begrenzt.

Nachdem eine vom Landesamt für Gesundheit und Lebensmittelsicherheit vorgenommene Evaluation zu dem Ergebnis geführt hat, dass die Einführung der Impfbuchvorlagepflicht zu einem Anstieg der Impfaufklärung und einer Erhöhung der Durchimpfungsrate beigetragen habe, wurde die zeitliche Befristung der Regelung zwischenzeitlich durch das Gesetz zur Änderung des Gesundheitsdienst- und Verbraucherschutzgesetzes und weiterer Rechtsvorschriften vom 28. Oktober 2015 aufgehoben.

Gegenüber dem Staatsministerium für Gesundheit und Pflege habe ich betont, dass die Impfpässe bei Schuleingangsuntersuchungen und weiteren schulischen Impfberatungen vor einer unbefugten Einsichtnahme zu schützen sind. Dieser Schutz kann wie folgt gewährleistet werden:

In den betroffenen Schulklassen wird zunächst ein Informationsblatt für die Eltern ausgeteilt. Die Erziehungsberechtigten werden darin gebeten, den Kindern deren Impfausweise oder Kopien hiervon in die Schule mitzugeben. Die mitgebrachten Dokumente werden dann von der Klassenleitung eingesammelt und bis zu dem Tag, an dem die Einsichtnahme durch Bedienstete des Gesundheitsamts stattfindet oder die Impfausweise vom Gesundheitsamt abgeholt werden, in der Schule verwahrt. Danach werden sie mit eingelegten Hinweisblättern zum Impfstatus wiederum über die Schule an die Schulkinder zurückgegeben.

Die Impfdokumente müssen dabei in verschlossenen, an das Gesundheitsamt adressierten Umschlägen in der Schule abgegeben werden können. Nach der Durchsicht durch Bedienstete des Gesundheitsamts müssen sie in verschlossenen Umschlägen, die mit dem Namen der jeweiligen Schülerinnen und Schüler versehen sind, an das Schulpersonal übergeben werden. Dieses reicht die Impfdokumente an die Schülerinnen und Schüler weiter. Die an die Erziehungsberechtigten gerichteten Informationsblätter, die die Gesundheitsämter vor der Impfausweiskontrolle austeilen, müssen Hinweise auf dieses Verfahren, insbesondere auf die Verwendung von verschlossenen Umschlägen, enthalten.

Bislang habe ich keine Hinweise darauf, dass diese Vorgaben strukturell missachtet werden. Ich werde jedoch auch in Zukunft darauf achten, dass bei der Durchführung der schulischen Impfberatungen die Belange des Datenschutzes nicht außer Acht gelassen werden.

Ein Informationsangebot mit datenschutzrechtlichen Hinweisen zur Impfberatung der Gesundheitsämter in Schulen habe ich auch auf meiner Homepage https://www.datenschutz-bayern.de bereitgestellt.

7.4.2 Weitergabe von Gesundheitsdaten an die Polizei

Das Infektionsschutzgesetz gibt den Gesundheitsämtern die Befugnis, Patientinnen und Patienten, die in Verdacht stehen, an einer übertragbaren Krankheit zu leiden, vorzuladen und ärztlich zu untersuchen. Infektionen sollen so frühzeitig erkannt und ihre Weiterverbreitung möglichst verhindert werden.

Leisten die Betroffenen einer solchen Vorladung nicht freiwillig Folge, so kann die Abklärung des Krankheitsverdachts auch durch eine zwangsweise Vorführung der Patientinnen und Patienten durch die Polizei im Rahmen der Vollzugshilfe durchgesetzt werden.

Das Staatsministerium für Gesundheit und Pflege hat mich um eine Stellungnahme zu der Frage gebeten, ob ein Gesundheitsamt im Falle einer zwangsweisen Vorführung auch Angaben über (möglicherweise) bestehende infektiöse Erkrankungen der oder des Betroffenen an die Polizei machen darf.

Maßgeblich für die Übermittlung personenbezogener Daten durch die Gesundheitsbehörden (hier durch die Gesundheitsämter) an andere öffentliche Stellen (hier an die Polizei) sind Art. 30, 31 Gesundheitsdienst- und Verbraucherschutzgesetz (GDVG).

Danach dürfen personenbezogene Daten übermittelt werden, wenn dies zur Abwehr von Gefahren für Freiheit, Leben oder Gesundheit Dritter erforderlich ist (Art. 31 Abs. 8 Nr. 1, 30 Abs. 2 Satz 2 GDVG).

Art. 31 GDVG Mitteilungen, Datenübermittlungen
(8) Außer in den hier genannten Fällen dürfen die Behörden für Gesundheit, Veterinärwesen, Ernährung und Verbraucherschutz sowie die in Abs. 3 und 4 genannten Behörden personenbezogene Daten an öffentliche Stellen nur übermitteln oder an andere Teile der öffentlichen Stelle, deren Bestandteil die Behörde für Gesundheit, Veterinärwesen, Ernährung und Verbraucherschutz ist, weitergeben
1. in den Fällen des Art. 30 Abs. 2,
2. …

Art. 30 GDVG Datenschutz, Geheimhaltungspflichten
(2) … [2]Abweichend von Abs. 1 dürfen personenbezogene Daten von den Behörden für Gesundheit, Veterinärwesen, Ernährung und Verbraucherschutz an öffentliche Stellen übermittelt oder an andere Teile der öffentlichen Stelle, deren Bestandteil die Behörde für Gesundheit, Veterinärwesen, Ernährung und Verbraucherschutz ist, weitergegeben werden, wenn dies zur Abwehr von Gefahren für Freiheit, Leben oder Gesundheit Dritter erforderlich ist; die betroffene Person soll hierauf hingewiesen werden.

Nach der gesetzlichen Regelung kommt es entscheidend darauf an, ob die Mitteilung der konkreten Krankheit beziehungsweise des konkreten Krankheitsverdachts erforderlich ist, um Gefahren für die Gesundheit der begleitenden Polizeikräfte abzuwehren.

Eine generelle Kenntnis der Polizei über die konkrete Krankheit oder den konkreten Krankheitsverdacht erscheint mir allerdings nicht generell erforderlich zu sein. Hier gebe ich zu bedenken, dass für medizinische Laien die bloße Kenntnis von der konkreten übertragbaren Krankheit oder von dem Verdacht auf eine konkrete übertragbare Krankheit noch nicht geeignet ist, sich angemessen vor einer Ansteckung zu schützen. Vielmehr werden die Polizeikräfte erst durch Hinweise zum Übertragungsweg und zu notwendigen Schutzmaßnahmen in die Lage versetzt, sich vor einer Ansteckung zu schützen und auf diese Weise die Gefahr für die Gesundheit abzuwehren. Letztlich kann nur dieses Wissen vor einer Ansteckung schützen.

Notwendig, aber im Regelfall auch ausreichend sind daher die Mitteilung, dass eine Patientin oder ein Patient im Verdacht steht, an einer übertragbaren Krankheit zu leiden, und die Information, welche Maßnahmen die Polizeikräfte zum Schutz vor Ansteckung ergreifen können.

Damit schließe ich nicht aus, dass in Einzelfällen konkrete Umstände die Übermittlung weiterer Daten durch das Gesundheitsamt an die Polizei ausnahmsweise rechtfertigen können. Dies könnte beispielsweise dann der Fall sein, wenn es – trotz ergriffener Schutzmaßnahmen – zur Ansteckung einer Polizistin oder eines Polizisten kam oder ein konkreter Verdacht hierfür vorliegt.

7.4.3 Gesundheits- und Entwicklungsscreening im Kindergartenalter (GESiK)

Die Staatsregierung will zukünftig Kinder mit Lern- und Entwicklungsdefiziten früher als bisher fördern. Aus diesem Grund soll durch das Pilotprojekt „Gesundheits- und Entwicklungsscreening im Kindergartenalter (GESiK)“ die Schuleingangsuntersuchung zeitlich vorgezogen und ihr Umfang erweitert werden.

Ich habe die Planungen dieses Projekts begleitet und dabei insbesondere auf die Notwendigkeit einer Rechtsgrundlage hingewiesen. Daraufhin wurde die Meldedatenverordnung durch die Vorschrift des § 27 Abs. 3 ergänzt, wonach die Gesundheitsämter die Daten von Kindern etwa ein Jahr vor deren Schulpflicht erhalten. Zudem konnte ich Änderungen bei der Elterninformation sowie der Einwilligungserklärung erwirken. Dies hat dazu geführt, dass die Eltern transparenter über mögliche datenschutzrechtliche Vorgänge informiert werden.

7.4.4 Leitfaden „Einhaltung datenschutzrechtlicher Bestimmungen bei Gesundheitsämtern“

Im 26. Tätigkeitsbericht 2014 unter Nr. 7.1.1 habe ich darüber berichtet, dass ich den Schwerpunkt meiner Prüfungen darauf gelegt habe, mir einen aktuellen Überblick über die Einhaltung datenschutzrechtlicher Bestimmungen bei den Gesundheitsämtern zu verschaffen.

Ich habe im Nachgang zu den datenschutzrechtlichen Prüfungen bei Gesundheitsämtern sowie im Interesse einer einheitlichen Vorgehensweise der Gesundheitsämter gebeten, standardisierte und datenschutzgerechte Lösungen, insbesondere bei der Aktenverwahrung, Aussonderung und Löschung von Akten, zu erarbeiten.

Um den Gesundheitsämtern ein geeignetes Instrument zur Überprüfung an die Hand zu geben, ob die jeweiligen datenschutzrechtlichen Anforderungen erfüllt werden, hat das Staatsministerium für Gesundheit und Pflege einen Leitfaden „Einhaltung datenschutzrechtlicher Bestimmungen bei Gesundheitsämtern – Hinweise und Leitfaden auf Grundlage der Empfehlungen des Bayerischen Landesbeauftragten für den Datenschutz“ erstellt. Dieser wurde mit dem Staatsministerium für Arbeit und Soziales, Familie und Integration und mit mir abgestimmt.

Der Leitfaden enthält Hinweise über datenschutzrechtliche Grundlagen, Geheimhaltungspflichten, Übermittlungsbefugnisse, Aufbewahrungsdauer und -pflichten sowie eine Checkliste zur Überprüfung spezifischer datenschutzrechtlicher Anforderungen. Er wurde allen Gesundheitsämtern zur Verfügung gestellt. Die Gesundheitsämter sind nun aufgefordert, eigenverantwortlich unter Einbindung der behördlichen Datenschutzbeauftragten die Empfehlungen des Leitfadens umzusetzen, im Sinne des Qualitätsmanagements zu evaluieren und fortzuschreiben.

7.5 Krankenhaus

7.5.1 Externe Dienstleistungen

Immer wieder ist zu hören, Art. 27 Abs. 4 Bayerisches Krankenhausgesetz (BayKrG) sei in Zeiten von Cloud Computing und Big Data veraltet und unbrauchbar, da er einer Auftragsdatenverarbeitung im Bereich der Krankenhäuser zu enge Grenzen setze.

Art. 27 BayKrG Datenschutz
(4) …[5]Das Krankenhaus kann sich zur Verarbeitung und Mikroverfilmung von Patientendaten anderer Personen oder Stellen bedienen, wenn es sicherstellt, dass beim Auftragnehmer die besonderen Schutzmaßnahmen nach Abs. 6 eingehalten werden, und solange keine Anhaltspunkte dafür bestehen, dass durch die Art und Ausführung der Auftragsdatenverarbeitung schutzwürdige Belange von Patienten beeinträchtigt werden. [6]Zur Verarbeitung oder Mikroverfilmung von Patientendaten, die nicht zur verwaltungsmäßigen Abwicklung der Behandlung der Patienten erforderlich sind, darf sich das Krankenhaus jedoch nur anderer Krankenhäuser bedienen.
(6) Es sind besondere Schutzmaßnahmen technischer und organisatorischer Art zu treffen, dass Patientendaten nicht unberechtigt verwendet oder übermittelt werden können.

Gerade in Krankenhäusern entstehen zunehmend große Mengen an Daten, die die Gesundheit der Patientinnen und Patienten und damit deren intimsten Lebensbereich betreffen. Für diese Daten ist es durchaus angemessen, strengere Schutzmaßnahmen zu fordern. Durch die Beteiligung externer Stellen wird der Kreis derer größer, die mit sensiblen medizinischen Daten in Berührung kommen. Gleichzeitig sinken die direkten Einflussmöglichkeiten der Krankenhäuser auf den Umgang mit den Daten ihrer Patientinnen und Patienten. Das kann das Risiko von

Datenmissbrauch und Datenverlust in einem besonders sensiblen Bereich erhöhen.

Deshalb hat Art. 27 Abs. 4 BayKrG auch weiterhin seine Berechtigung. Er sorgt dafür, dass externe Dienstleister nur mit zusätzlichen Sicherheitsmaßnahmen zum Einsatz kommen dürfen. Eine elektronische Archivierung beispielsweise darf nur erfolgen, wenn die Daten im Krankenhaus verschlüsselt werden oder Klinikbeschäftigte die Papierentsorgung durch einen externen Entsorger begleiten. Dies sorgt dafür, dass die Daten jederzeit unter Aufsicht und im Gewahrsam des Klinikums stehen.

Dass es möglich ist, die strengen Anforderungen des Art. 27 Abs. 4 BayKrG einzuhalten, hat eine flächendeckende Prüfung im Jahr 2015 gezeigt. Zwar habe ich in den Krankenhäusern Mängel bei der Umsetzung gefunden; gleichzeitig konnte ich jedoch auch feststellen, dass es für alle Konstellationen sehr wohl datenschutzgerechte Lösungen gibt. Zur Unterstützung der Krankenhäuser habe ich die Ergebnisse der Prüfung in einen Leitfaden zusammengefasst. Dieser ist auf meiner Homepage https://www.datenschutz-bayern.de zu finden (siehe Pressemitteilung vom 29. Juni 2016).

Art. 27 Abs. 4 Satz 6 BayKrG sieht vor, dass sich ein Krankenhaus zur Verarbeitung medizinischer Patientendaten nur anderer Krankenhäuser bedienen darf. Sinn und Zweck des Art. 27 Abs. 4 Satz 6 BayKrG ist es insbesondere, den Kreis der Personen möglichst eng zu halten, die mit sensiblen medizinischen Daten in Berührung kommen. Gleichzeitig soll die Qualifikation der zugriffsberechtigten Personen möglichst hoch gehalten werden. Die Aufsichtsbefugnisse der Krankenhäuser auch während der Datenverarbeitung sollen gestärkt, die Kenntnisnahme durch Unbefugte soll vermieden und die missbräuchliche Verwendung medizinischer Patientendaten damit soweit wie möglich ausgeschlossen werden.

Art. 27 Abs. 4 Satz 6 BayKrG ist nach der Entscheidung des Bayerischen Verfassungsgerichtshofs vom 6. April 1989 (Vf. 2-VII-87) verfassungsgemäß. Die gegen diese Entscheidung gerichtete Verfassungsbeschwerde wurde vom Bundesverfassungsgericht nicht zur Entscheidung angenommen (Beschluss vom 25. September 1990 – 1 BvR 1555/87).

Allerdings hat der Bayerische Verfassungsgerichtshof unter anderem ausgeführt, dass es den Krankenhäusern nicht verwehrt sei, medizinische Daten in einer dem Art. 26 Abs. 4 Satz 5 BayKrG a.F. (jetzt: Art. 27 Abs. 4 Satz 6 BayKrG) entsprechenden Ausgestaltung innerhalb des Krankenhauses durch Dritte mikroverfilmen (archivieren) zu lassen. Dem Gesetzgeber sei es entscheidend darauf angekommen, dass die medizinischen Patientendaten nicht aus dem Gewahrsam des Krankenhauses herausgegeben werden.

Eine Beteiligung externer Dienstleister ist demnach möglich, wenn die Datenverarbeitung im Gewahrsam des Klinikums stattfindet oder diese keine Kenntnis von den Daten nehmen können (etwa durch Verschlüsselung). Gewahrsam bedeutet dabei nicht nur die räumliche Zuordnung zum Krankenhaus (beispielsweise die Nutzung von Räumen auf dem Gelände des Krankenhauses), sondern auch die ausschließliche Verfügungsgewalt über die Patientendaten. So muss die Schlüsselgewalt beim Krankenhaus verbleiben, eine Weisungsbefugnis gegenüber den Beschäftigten des Dienstleisters bestehen und eine effektive Aufsicht durch das Klinikum erfolgen. Die entsprechenden Punkte müssen ausdrücklich in einem schriftlichen Vertrag zur Auftragsdatenverarbeitung geregelt werden.

7.5.2 Grundsätzlich kostenfreie Auskunftserteilung

Das Auskunftsrecht gegenüber öffentlichen Stellen ist ein wichtiges Element des Grundrechts auf Datenschutz. Es macht die Erhebung, Verarbeitung und Nutzung der Daten transparent und versetzt Betroffene in die Lage, wenn nötig, weitere Schutzrechte (beispielsweise das Recht auf Berichtigung oder das Recht auf Löschung) geltend zu machen. Dies gilt insbesondere auch gegenüber Krankenhäusern.

Zwei Fragen werden mir häufig gestellt: Auf welcher Rechtsgrundlage können Patientinnen und Patienten Auskunft verlangen und inwieweit können sie an den mit einer Auskunftserteilung verbundenen Kosten beteiligt werden?

Insoweit ist zu unterscheiden nach zivilrechtlichen Ansprüchen und öffentlich-rechtlichen Auskunftsansprüchen:

– Beim zivilrechtlichen Anspruch auf Einsicht in die Patientenakte und beim Recht der Patientinnen und Patienten, elektronische Abschriften zu verlangen (§ 630g Abs. 1 und 2 Bürgerliches Gesetzbuch – BGB), hat der Gesetzgeber nur für elektronische Abschriften eine Kostenerstattung vorgesehen. Er hat keine generelle Gebührenpflicht von Auskunftsbegehren geregelt. Behandelnde können Kostenerstattung deshalb meines Erachtens allenfalls verlangen, wenn eine elektronische Abschrift der Patientenakte verlangt wird. Meine Auffassung deckt sich insoweit mit der in der in § 10 Abs. 2 Berufsordnung für die Ärzte Bayerns (BOÄ) enthaltenen Regelung.

  § 630g BGB Einsichtnahme in die Patientenakte
  (1) Dem Patienten ist auf Verlangen unverzüglich Einsicht in die vollständige, ihn betreffende Patientenakte zu gewähren, soweit der Einsichtnahme nicht erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen. Die Ablehnung der Einsichtnahme ist zu begründen….
  (2) Der Patient kann auch elektronische Abschriften von der Patientenakte verlangen. Er hat dem Behandelnden die entstandenen Kosten zu erstatten….

  § 10 BOÄ Dokumentationspflicht
  (2) Ärztinnen und Ärzte haben Patientinnen und Patienten auf deren Verlangen in die sie betreffende Dokumentation Einsicht zu gewähren, soweit der Einsichtnahme nicht erhebliche therapeutische Gründe oder erhebliche Rechte der Ärztin, des Arztes oder Dritter entgegenstehen. Auf Verlangen sind der Patientin oder dem Patienten Kopien der Unterlagen gegen Erstattung der Kosten herauszugeben.

– Stützen Betroffene ihr Auskunftsrecht auf die in den allgemeinen Datenschutzgesetzen enthaltenen öffentlich-rechtlichen Auskunftsansprüche nach Art. 10 Abs. 2 BayDSG oder § 34 Abs. 8 Satz 1 Bundesdatenschutzgesetz, so sehen diese Regelungen im Grundsatz die Unentgeltlichkeit der Auskunft vor. Der spezielle Auskunftsanspruch für Patientinnen und Patienten im Krankenhaus ist in Art. 27 Abs. 3 Bayerisches Krankenhausgesetz (BayKrG) enthalten. Da abweichende Festlegungen zum allgemeinen Datenschutzrecht dort nicht getroffen wurden, kommt man auch hier zu dem Ergebnis, dass die Auskunft grundsätzlich kostenfrei zu erteilen ist.

Art. 27 BayKrG Datenschutz
(3) [1]Die Patienten haben Anspruch auf Auskunft über die zu ihrer Person aufbewahrten Daten, über die Personen und Stellen außerhalb des Krankenhauses, an die ihre Daten übermittelt wurden, sowie darüber, welche Daten zu anderen Zwecken als zur Behandlung und deren verwaltungsmäßiger Abwicklung übermittelt wurden. [2]Auskunft darüber, welche Patientendaten zur Behandlung oder zu deren verwaltungsmäßiger Abwicklung übermittelt wurden, ist zu erteilen, soweit die Unterlagen des Krankenhauses hierzu Angaben enthalten. [3]Die Auskunft soll im Einzelfall durch Ärzte vermittelt werden, soweit dies mit Rücksicht auf den Gesundheitszustand der Patienten dringend geboten ist. [4]Eine Beschränkung der Auskunft nach Satz 1 hinsichtlich ärztlicher Beurteilungen oder Wertungen ist zulässig.

Die grundsätzliche Unentgeltlichkeit der Auskunft schließt allerdings nicht generell aus, dass eine Klinik für die Anfertigung von Kopien Kostenerstattung ausnahmsweise verlangen kann. Dies ist beispielsweise der Fall, wenn dem Auskunftsanspruch bereits nachgekommen wurde und eine verlangte zusätzliche Erstellung von Ausdrucken oder Kopien mit einem besonderen Verwaltungsaufwand – der im Einzelfall zu prüfen wäre – verbunden ist.

7.5.3 Verzicht auf eine Datennutzung bei Einwilligungen

Ein Universitätsklinikum hatte sich die Verwendung von Patientendaten für den Versand von Spendenbriefen ausdrücklich erlauben und dies auf einem gesonderten Formular bestätigen lassen. Rund drei Jahre später beschwerte sich ein Patient, als er (erstmals) einen entsprechenden Spendenaufruf erhielt. An seine ausdrücklich erteilte Einwilligung konnte er sich offenbar nicht mehr erinnern. Das Klinikum hat die Eingabe zum Anlass genommen, den Prozess zu überdenken und künftig alle Einwilligungen, die älter als 18 Monate sind, nicht mehr zu verwenden.

Die Entscheidung des Klinikums habe ich unter dem Gesichtspunkt der Datensparsamkeit begrüßt. Gleichzeitig habe ich angeregt, im Formular ausdrücklich vorzusehen, dass das Klinikum nach Ablauf von eineinhalb Jahren von der Einwilligung in die Datennutzung keinen Gebrauch mehr macht.

Das Formular trägt dann der Tatsache Rechnung, dass Betroffene regelmäßig einige Zeit nach erteilter Einwilligung nicht mehr nachvollziehen können, ob und wann sie eine entsprechende Erklärung abgegeben haben. Je nach Umständen des Einzelfalls verliert eine ungenutzte Einwilligung durch Zeitablauf ihre Wirkung.

7.6 Bayerisches Gesundheitsdatenzentrum

Wichtig erscheint mir ein Hinweis auf eine Diskussion, die derzeit im Gesundheitswesen in Bayern geführt wird. Der Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF) hatte im Auftrag des Gesundheitsministeriums eine Machbarkeitsstudie für ein Bayerisches Gesundheitsdatenzentrum erstellt. Die Studie des TMF hatte bereits viele Ausführungen zu datenschutzrechtlichen Anforderungen zur Errichtung eines solchen Datenzentrums enthalten. Am 16. Juni 2016 fand dazu auf Einladung des Arbeitskreises Gesundheit der CSU-Fraktion eine öffentliche Anhörung „Wege zur Errichtung eines Bayerischen Gesundheitsdatenzentrums“ im Bayerischen Landtag statt. Alle relevanten Institutionen im Gesundheitswesen haben daran teilgenommen.

Das Gutachten beleuchtet allerdings die ab Mai 2018 geltende Datenschutz-Grundverordnung (DSGVO) nicht näher. Deshalb habe ich mich den künftig geltenden europäischen Datenschutzvorschriften besonders gewidmet und die Errichtung eines Bayerischen Gesundheitsdatenzentrums anhand dieser Regelungen erörtert. Dabei habe ich besonderes Augenmerk auf die vom TMF entwickelten Modelle „Elektronische Patientenakte“ und „Versorgungsforschung“ gelegt. Für eine auf eine Einwilligung gestützte bayerische Patientenakte müssten insbesondere die Anforderungen der Art. 5, 7 und 9 DSGVO beachtet werden. Es müsste ein eigenes Netzwerk, wie beispielsweise KVSafenet, geschaffen werden, um die Sicherheit zu gewährleisten (siehe Art. 24, 25 DSGVO). Ein Austausch sensibler Gesundheitsdaten über das allgemeine Internet käme keinesfalls in Betracht. Im Übrigen wäre eine Kooperation mit der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) anzuraten, die mit der Einführung der elektronischen Gesundheitskarte im Bundesgebiet beauftragt ist. Für die Versorgungsforschung wäre eine gesetzliche Grundlage erforderlich (Einwilligung allenfalls begleitend). Notwendig wären ferner die Einbindung von ärztlichem Fachpersonal, die Pseudonymisierung von Daten und eine Vertrauensstelle. Auf Bund- und Länderebene wären Gesetzesänderungen erforderlich, insbesondere die Änderung von Sozialgesetzbüchern.

Für die Errichtung eines Bayerischen Gesundheitsdatenzentrums wären zwingend insbesondere folgende Bedingungen zu erfüllen:

— Ein förmlicher Rechtsakt wäre unerlässlich.

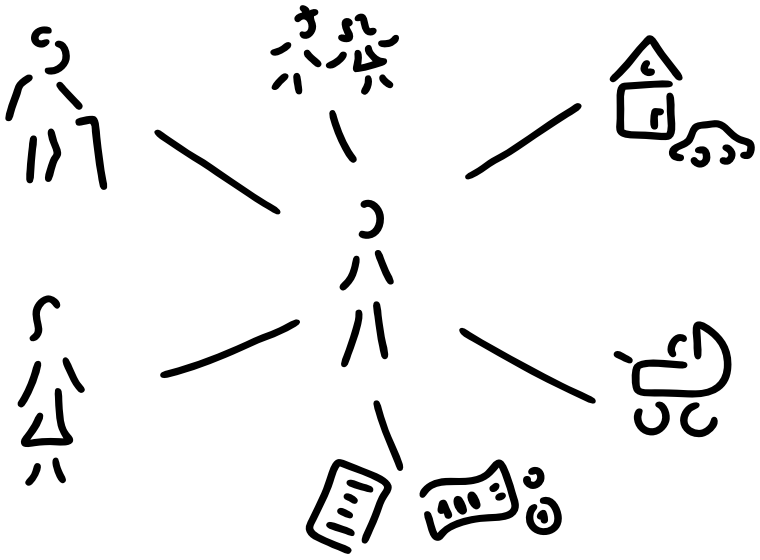
— Die Qualitätssicherung der Daten müsste gewährleistet sein.

— Die technischen Anforderungen zur Sicherung der Daten müssten beachtet werden.

— Die Datensouveränität müsste bei den Patienten bleiben, ohne deren Einverständnis eine Datennutzung nicht möglich wäre.

In Übereinstimmung mit den Gesundheitsexperten bin ich weiterhin skeptisch zu Sinn und Zweck eines Bayerischen Gesundheitsdatenzentrums.

8 Sozialwesen



8.1 Gesetzliche Krankenversicherung

8.1.1 Datenschutzrechtliche Befugnisse der Krankenkassen im Rahmen des Krankengeldfallmanagements

In den vergangenen Jahren war das Krankengeldfallmanagement der Krankenkassen einer meiner Prüfungsschwerpunkte (siehe 25. Tätigkeitsbericht 2012 unter Nr. 8.11 und 26. Tätigkeitsbericht 2014 unter Nr. 8.1.4). Zu Beginn meiner Prüfungsreihe musste ich eine Vielzahl von Datenschutzverstößen feststellen. Insbesondere nahm eine große bayerische Krankenkasse unzulässigerweise sensible medizinische Daten (insbesondere Behandlungsunterlagen) zur Kenntnis. Dies wäre jedoch allein dem Medizinischen Dienst der Krankenversicherung (MDK) vorbehalten gewesen. Gemeinsam mit dieser Krankenkasse konnte ich zunächst datenschutzrechtliche Verbesserungen erreichen.

Bedauerlicherweise hat die Krankenkasse jedoch eine Gesetzesänderung zum Anlass genommen, die erreichten datenschutzrechtlichen Verbesserungen größtenteils wieder zu revidieren. Dabei berief sie sich auf den vermeintlichen Willen des Gesetzgebers. Zwar hat dieser tatsächlich zum 23. Juli 2015 die Vorschrift des § 44 Abs. 4 Sozialgesetzbuch Fünftes Buch (SGB V) neu eingefügt – trotz großer Bedenken der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16.12.2014

Schluss mit den datenschutzrechtlichen Missständen beim Umgang mit Krankengeldbeziehern!

Bei dem derzeit praktizierten „Krankengeldfallmanagement" lädt eine Vielzahl von Krankenkassen ihre Versicherten in der vierten Woche einer Arbeitsunfähigkeit zu einem persönlichen Gespräch ein. Die Krankenkassen stellen Fragen zur Arbeitsplatz-, Krankheits-, familiären und sozialen Situation des Versicherten. Außerdem sollen die Ärzte der Versicherten häufig medizinische Fragen beantworten sowie Arzt-, Krankenhaus- oder Rehaentlassberichte an die Krankenkasse schicken. Vielfach werden Versicherte, die im Krankengeldbezug stehen, – zum Teil mehrfach wöchentlich – von Krankenkassenmitarbeitern oder in deren Auftrag von Dritten angerufen, um sich nach dem Fortschritt der Genesung zu erkundigen.
Zudem werden nach den Prüferfahrungen der Datenschutzbeauftragten des Bundes und einiger Länder Versicherte beim „Krankengeldfallmanagement" von ihrer Krankenkasse oftmals unter Druck gesetzt. Auch der Patientenbeauftragte der Bundesregierung sowie die Unabhängige Patientenberatung Deutschland (UPD) haben an dieser Praxis starke Kritik geübt.

Die Krankenkassen sind zur Beurteilung sensibler medizinischer Daten aufgrund der bisherigen gesetzgeberischen Grundentscheidung auf ein Tätigwerden des Medizinischen Dienstes der Krankenversicherung (MDK) angewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist die Bundesregierung darauf hin, dass es nicht nachvollziehbar ist, dass mit dem Entwurf eines Gesetzes zur Stärkung der Versorgung in der gesetzlichen Krankenversicherung (GKV Versorgungsstärkungsgesetz – GKV-VSG) das bisherige datenschutzrechtlich problematische Vorgehen von vielen Krankenkassen beim sog. Krankengeldfallmanagement nunmehr legitimiert werden soll. Zukünftig sollen danach die Versicherten bei einem (absehbaren) Krankengeldbezug „Anspruch auf eine umfassende Prüfung, individuelle Beratung und Hilfestellung, welche Leistungen und unterstützende Angebote zur Wiederherstellung der Arbeitsfähigkeit erforderlich sind" gegenüber ihrer gesetzlichen Krankenkasse haben. Die Krankenkasse soll dabei die erforderlichen personenbezogenen Daten mit Einwilligung des Versicherten erheben, verarbeiten und nutzen dürfen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, von dieser Regelung Abstand zu nehmen. Vielmehr sind die derzeit bestehenden gesetzlichen Regelungen konsequent umzusetzen.

Nach § 44 SGB V können Krankenkassen nun lediglich unter bestimmten engen Voraussetzungen sensible medizinische Daten zur eigenen Kenntnisnahme erheben.

§ 44 SGB V Krankengeld
(4) Versicherte haben Anspruch auf individuelle Beratung und Hilfestellung durch die Krankenkasse, welche Leistungen und unterstützende Angebote zur Wiederherstellung der Arbeitsfähigkeit erforderlich sind. Maßnahmen nach Satz 1 und die dazu erforderliche Erhebung, Verarbeitung und Nutzung personenbezogener Da-

ten dürfen nur mit schriftlicher Einwilligung und nach vorheriger schriftlicher Information des Versicherten erfolgen. Die Einwilligung kann jederzeit schriftlich widerrufen werden. …

Die geprüfte Krankenkasse erfüllt diese Anforderungen in vielen Punkten gegenwärtig noch nicht: Dies betrifft zum einen den eindeutigen Gesetzeswortlaut. Die Krankenkasse begrenzt ihre Datenerhebungen nicht auf den einschlägigen Zweck der Wiederherstellung der Arbeitsfähigkeit. Hinzu kommt, dass nach der Rechtsprechung Beschäftigte einer Krankenkasse grundsätzlich nicht über die notwendige medizinische Ausbildung verfügen (Entscheidungen des Bundessozialgerichts vom 16. Mai 2012 – B 3 KR 14/11 R – und des Bayerischen Verwaltungsgerichtshofs vom 31. Januar 2013 – 12 B 12.860; siehe auch Nr. 8.3.2). Daher ist es grundsätzlich nicht erforderlich, dass sie sensible medizinische Daten zur Kenntnis nehmen. Außerdem liegt keine vorherige schriftliche Information des Versicherten vor. Ferner berücksichtigt die Krankenkasse nicht die klarstellenden Hinweise in der Gesetzesbegründung. Insbesondere ist die derzeitige Einwilligungserklärung zu pauschal. Dadurch ist den Versicherten in der Regel nicht klar, in welcher Art und Weise die Krankenkasse in ihr Recht auf informationelle Selbstbestimmung eingreift.

Trotz mehrfacher Vorschläge für schriftliche Informationen und Einwilligungserklärungen in diesem Bereich hat die Krankenkasse ihr Vorgehen im Wesentlichen beibehalten, obwohl sie die datenschutzrechtlichen Verstöße im Grundsatz einräumt. Begründet wird dies insbesondere mit Abstimmungsbedarf auf Bundesebene. Ich werde deshalb den Dialog mit der Krankenkasse fortsetzen und mich weiterhin für eine datenschutzfreundliche Umsetzung des gesetzgeberischen Willens einsetzen.

8.1.2 Umschlagverfahren

Mit dem so genannten Umschlagverfahren in der gesetzlichen Krankenversicherung war ich in der Vergangenheit mehrfach befasst. Ich hatte seit Jahren die Auffassung vertreten, dass die für den Medizinischen Dienst der Krankenversicherung (MDK) bestimmten Daten zwar auch über die Krankenkassen zugeleitet werden können. Dabei musste aber (beispielsweise durch einen verschlossenen Umschlag) ausgeschlossen sein, dass die Krankenkasse vom Inhalt der Daten für den MDK Kenntnis nimmt (siehe 17. Tätigkeitsbericht 1996 unter Nr. 4.4.2, 25. Tätigkeitsbericht 2012 unter Nr. 8.11 sowie 26. Tätigkeitsbericht 2014 unter Nrn. 8.1.2 und 8.1.4).

Zum 1. Januar 2016 ist jedoch eine Änderung des einschlägigen § 276 Abs. 2 Sozialgesetzbuch Fünftes Buch (SGB V) in Kraft getreten, die das Ende des Umschlagverfahrens eingeläutet haben dürfte.

§ 276 SGB V Zusammenarbeit
(2) Der Medizinische Dienst darf Sozialdaten nur erheben und speichern, soweit dies für die Prüfungen, Beratungen und gutachtlichen Stellungnahmen … und für die Modellvorhaben … erforderlich ist; haben die Krankenkassen … eine gutachtliche Stellungnahme oder Prüfung durch den Medizinischen Dienst veranlasst, sind die Leistungserbringer verpflichtet, Sozialdaten auf Anforderung des Medizinischen Dienstes unmittelbar an diesen zu übermitteln, soweit dies für die gutachtliche Stellungnahme und Prüfung erforderlich ist.

Derzeit arbeiten Krankenkassen und MDK an einer technischen Lösung zur Umsetzung dieser Gesetzesänderung. Die Krankenkasse soll den MDK zeitnah beauftragen können. Außerdem kann die Krankenkasse den Eingang und die Art der Unterlagen beim MDK einsehen.

Mit einer flächendeckenden Umsetzung dieser technischen Lösung ist im Jahr 2017 zu rechnen. Aus diesem Grund habe ich im Jahr 2016 nicht beanstandet, sofern ein ordnungsgemäßes Umschlagverfahren durchgeführt wurde.

Ohne weitere Nutzung des Umschlagverfahrens wären nach Angaben der Krankenkassen und des MDK Probleme im Vollzug zu befürchten: Der MDK würde Unterlagen von Leistungserbringern erhalten, die er aufgrund der noch nicht erfolgten Beauftragung durch die Krankenkasse nicht zuordnen kann. Eine Datenspeicherung „auf Vorrat" ist aber problematisch. Außerdem haben die Krankenkassen eigenen Angaben zufolge nicht den Überblick, ob Leistungserbringer ihren Pflichten nachgekommen sind.

Derartige Duldungslösungen im Sinne einer praxisgerechten Verfahrensweise zur Umstellung eines langjährigen Verfahrens können nur ausnahmsweise und zeitlich begrenzt herangezogen werden, weil die geänderte Gesetzeslage in solchen Fällen stets zu einer gewissen Rechtsunsicherheit bei den Beteiligten führen kann.

8.1.3 Datenschutzrechtliche Befugnisse bei Anschlussrehabilitation

Im Rahmen einer datenschutzrechtlichen Prüfung im Krankenhausbereich habe ich mich auch ausführlich mit einem Antrag der Versicherten auf eine Anschlussrehabilitation auseinandergesetzt.

Hier habe ich zunächst auf die Rechtsprechung des Bundessozialgerichts im Krankenhausbereich (Bundessozialgericht, Urteil vom 16. Mai 2013 – B 3 KR 32/12 R) verwiesen. Danach dürfen Krankenkassen selbst grundsätzlich keine medizinischen Erhebungen durchführen und von den Leistungserbringern auch keine entsprechenden Auskünfte einholen.

Dieses Ergebnis wirkte jedoch befremdlich. Schließlich können Vertragsärztinnen und -ärzte bei einer Anschlussrehabilitation bestimmte medizinische Daten mit Hilfe des Vordrucks „Muster 61" an die Krankenkasse übermitteln. In diesem Fall besteht jedoch meiner Ansicht nach mit dem Bundesmantelvertrag Ärzte und der Vordruckvereinbarung eine datenschutzrechtliche Befugnis (siehe 26. Tätigkeitsbericht 2014 unter Nr. 8.1.1).

Nach ständiger Rechtsprechung kommt als datenschutzrechtliche Rechtsgrundlage jedoch auch ein Vertrag zwischen der Landeskrankenhausgesellschaft und den zuständigen Verbänden der Krankenkassen in Betracht. Schließlich handelt es sich hier um Normenverträge (siehe auch 26. Tätigkeitsbericht 2014 unter Nr. 8.1.1). Auf meine Anregung hin sind die Vordrucke in Bayern inzwischen Anlage zu einem derartigen bereits bestehenden Vertrag. Damit sind Erhebungen medizinischer Daten entsprechend diesen Vordrucken inzwischen sowohl im Vertragsarzt- als auch im Krankenhausbereich zulässig.

Allerdings sind zum 23. Juli 2015 unter anderem auch neue Vorschriften zur Erhebung, Verarbeitung und Nutzung von Daten beim Entlassmanagement im Krankenhaus (§ 39 Abs. 1a Sozialgesetzbuch Fünftes Buch – SGB V) in Kraft getreten.

Diese Regelungen entsprechen in etwa denjenigen des Krankengeldfallmanagements (siehe Nr. 8.1.1). Auch hier ist insbesondere eine enge Begrenzung auf den einschlägigen Zweck sowie eine ausreichende schriftliche Information beziehungsweise Einwilligungserklärung notwendig. Ich gehe davon aus, dass hier vergleichbare Probleme auftreten werden.

8.1.4 Datenschutzrechtliche Befugnisse im Rahmen der besonderen Versorgung

Auch in diesem Berichtszeitraum war ich mit verschiedenen Programmen zur besonderen Versorgung nach § 140a Sozialgesetzbuch Fünftes Buch (SGB V) befasst (siehe schon 23. Tätigkeitsbericht 2008, Anlage 24; 26. Tätigkeitsbericht 2014 unter Nr. 8.1.10). Die Kassen sind hier bemüht und vom Gesetzgeber angehalten, ihre Versicherten durch verschiedene Programme zu „steuern". Zum 23. Juli 2015 ist auch hier eine gesetzliche Änderung in Kraft getreten:

§ 140a SGB V Besondere Versorgung
(5) Die Erhebung, Verarbeitung und Nutzung der für die Durchführung der Verträge … erforderlichen personenbezogenen Daten durch die Vertragspartner … darf nur mit Einwilligung und nach vorheriger Information der Versicherten erfolgen. …

Diese Regelungen entsprechen nun in etwa denjenigen des Krankengeldfall- beziehungsweise Krankenhausentlassmanagements (siehe Nrn. 8.1.1 und 8.1.3). Auch hier musste ich schon mehrfach auf eine enge Begrenzung des einschlägigen Zwecks, den Grundsatz der Erforderlichkeit sowie eine ausreichende schriftliche Information beziehungsweise Einwilligungserklärung hinwirken.

Insbesondere so genannte Managementgesellschaften versuchen, sowohl im Vorfeld der Versichertenauswahl als auch im Rahmen der Steuerung eine Vielzahl von Daten zu erhalten. Außerdem werden hier häufig medizinische Forschung und die „Steuerung" von Versicherten unzulässigerweise miteinander verwoben.

8.1.5 Gewinnspiele von Krankenkassen

Mit der datenschutzrechtlichen Problematik von Gewinnspielen bei Krankenkassen war ich bereits in der Vergangenheit befasst (siehe 22. Tätigkeitsbericht 2006 unter Nr. 14.1.4; 26. Tätigkeitsbericht 2014 unter Nr. 8.1.8). Zwar ist es angesichts des Wettbewerbs zwischen den gesetzlichen Krankenkassen nachvollziehbar, dass diese versuchen, neue Mitglieder zu werben oder an die personenbezogenen Daten potenzieller Neumitglieder zu gelangen. Dabei müssen sie jedoch die datenschutzrechtlichen Vorschriften einhalten.

In einem Einzelfall hat eine Krankenkasse bei einem Gewinnspiel mithilfe eines Coupons Daten eines Minderjährigen erhoben. Aufgrund von Skrupeln gab dieser Jugendliche dabei insbesondere eine falsche Wohnadresse an. Nach Angaben der Krankenkasse stellte sich erst bei einem Hausbesuch unter dieser Adresse heraus, dass die Wohnanschrift und das Geburtsdatum des Minderjährigen nicht mit den Couponangaben übereinstimmten. Aus diesem Grund hat die Krankenkasse Daten über das Bayerische Behördeninformationssystem (BayBIS) erhoben.

Nach der Rechtsprechung des Bundesgerichtshofs (Urteil vom 22. Januar 2014 – IZR 218/12) sind die Erhebung, Verarbeitung und Nutzung von Daten von Minderjährigen durch Krankenkassen bei Gewinnspielen zum Zwecke der Mitgliederwerbung schon aus wettbewerbsrechtlichen Gründen unzulässig.

Des Weiteren war der Abruf über BayBIS unzulässig. Melderegisterauskünfte über BayBIS dürfen nur aus Anlass einer Beantragung, der Erbringung oder der Erstattung einer Sozialleistung erfolgen. Datenabrufe für andere Zwecke (zum Beispiel Mitgliederwerbung, abstrakt-generelle Informationen für die Versicherten) sind nicht von der Genehmigung umfasst.

Ich habe diese datenschutzrechtlichen Verstöße beanstandet. Zum einen handelt es sich hier um Sozialdaten eines Minderjährigen. Zum anderen musste ich in den letzten Jahren vielfach Verstöße dieser Krankenkasse bei der Erhebung, Verarbeitung und Nutzung von Daten von Minderjährigen im Rahmen der Mitgliederwerbung feststellen. Vor einem Jahrzehnt führten derartige datenschutzrechtliche Verstöße in zwei Fällen bereits zu einer Beanstandung. Zudem hatte sich die Krankenkasse zunächst geweigert, ein mit mir abgestimmtes Datenschutzkonzept mit Kriterien zur Erhebung von Daten von Minderjährigen im Rahmen der Mitgliederwerbung zu erarbeiten.

Auch in der näheren Vergangenheit war ich mit der Mitgliederwerbung dieser Krankenkasse in mehrfacher Hinsicht befasst. Obwohl ich gegenüber der Krankenkasse eine entsprechende Änderung der einschlägigen Einwilligungserklärungen angeregt hatte, hat diese die Vereinbarungen in der Praxis vielfach nicht eingehalten. So hat die Krankenkasse unter anderem die Erhebung, Verarbeitung und Nutzung von Daten von Minderjährigen im Rahmen von Gewinnspielen erst eingestellt, als auch der Bundesgerichtshof entsprechend entschieden hatte.

Diese Rechtsprechung umgeht die Krankenkasse aktuell immer noch dadurch, dass sie statt eines Gewinnspiels für die Minderjährigen vergleichbare Anreize schafft. Meiner Einschätzung nach beachtet diese Krankenkasse damit auch nicht die Vorgaben des Staatsministeriums für Gesundheit und Pflege, nach denen die Datenerhebung in der konkreten durchgeführten Art und Weise nicht geeignet sein darf, die gesetzliche Unerfahrenheit von Jugendlichen auszunutzen.

8.1.6 Einkommensnachweise für Krankenkassen

Zu Zwecken der Beitragsermittlung sind die Krankenkassen insbesondere bei freiwillig versicherten Mitgliedern auf die Erhebung bestimmter Daten angewiesen. Dies war im Berichtszeitraum Thema verschiedener Nachfragen:

Nach § 206 Abs. 1 Satz 2 Sozialgesetzbuch Fünftes Buch (SGB V) dürfen die Krankenkassen verlangen, dass ihnen die Originale der Einkommensteuerbescheide in ihren Geschäftsräumen vorgelegt (nicht ausgehändigt) werden (siehe auch Bundessozialgericht, Urteil vom 26. September 1996 – 12 RK 46/95 – BSGE 79, 133, 139). Auch bei der Zusammenveranlagung von Ehegatten sind die Krankenkassen auf die Vorlage des Steuerbescheides angewiesen.

Allerdings dürfen die Krankenkassen nur die für die Beitragsfestsetzung erforderlichen Daten erheben und speichern. Bei nicht benötigten Daten ist eine Schwärzung möglich (siehe auch Nr. 8.3.1).

8.1.7 Videoüberwachung einer Krankenkasse

Aufwändig gestaltete sich die Prüfung einer Videoüberwachung in der Tiefgarage einer Krankenkasse. Die Verantwortlichen hatten sich mit den einschlägigen Vorschriften (Art. 21a BayDSG, siehe 23. Tätigkeitsbericht 2008 unter Nr. 9.2) nicht eingehend befasst.

Der Einsatz der Videoüberwachungsanlage war nicht vom behördlichen Datenschutzbeauftragten freigegeben worden (Art. 21a Abs. 6 Satz 1 in Verbindung mit Art. 26 BayDSG). Ihm lagen die benötigten Unterlagen auch nicht vor, um eine derartige Entscheidung überhaupt treffen zu können (Art. 21a Abs. 6 Satz 2 BayDSG). Auch die örtliche Personalvertretung wurde im Vorfeld nicht beteiligt (Art. 75a Abs.1 Nr. 1 Bayerisches Personalvertretungsgesetz).

Im Nachgang waren die vorgelegten Unterlagen zunächst dürftig, so dass ich keine abschließende Bewertung vornehmen konnte. Ich habe daher darum gebeten, hier die von mir entwickelten Unterlagen zur Videoüberwachung (Leitfaden, Muster und Prüfschema siehe 26. Tätigkeitsbericht 2014 unter Nr. 6.2) zu verwenden. Ich bat die Krankenkasse, einen Lageplan der einzelnen Kameras vorzulegen, aus dem das jeweilige Sichtfeld zu entnehmen ist, um die mit Hilfe der Kameras vorgenommenen Datenerhebungen und -verarbeitungen beurteilen zu können.

Die Videobeobachtung und -aufzeichnung musste im konkreten Einzelfall in Ausübung des Hausrechts entweder zum Schutz von Leben, Gesundheit, Freiheit oder Eigentum der Personen, die sich im Bereich der öffentlichen Stelle oder in deren unmittelbarer Nähe aufhalten, oder zum Schutz der Einrichtung der öffentlichen Stelle, des Dienstgebäudes oder der in deren unmittelbarer Nähe befindlichen Sachen erforderlich sein (Art. 21a Abs. 1 Satz 1 BayDSG).

Datenschutzrechtlich eher unproblematisch war die optisch-elektronische Klingelanlage, die sich im Bereich der Einfahrt zur Tiefgarage an der Schranke befindet. Deren Kamera schaltet sich erst ein, wenn eine Besucherin oder ein Besucher den Klingelknopf betätigt. Derartige Lösungen begegnen regelmäßig keinen datenschutzrechtlichen Bedenken (siehe 26. Tätigkeitsbericht 2014 unter Nr. 7.1.3).

Problematischer hingegen war der Einsatz von Kameras, die ausgewählte Parkplätze sowie den Verkehrsraum in der Tiefgarage beobachten oder aufzeichnen. Klärungsbedürftig war zunächst, wie gefährdet die eben genannten Rechtsgüter sind. Von einer Gefahrensituation ist in der Regel auszugehen, wenn bereits in der Vergangenheit Vorfälle auftraten, die eine Videoüberwachung rechtfertigen können. Dazu bedarf es einer aussagekräftigen Vorfalldokumentation, die erkennen lässt, an welchen Stellen es wann in der Vergangenheit welche Schadensfälle gab (siehe 26. Tätigkeitsbericht 2014 unter Nr. 10.10.2). Eine mögliche Strafverfolgung, ein subjektives Empfinden oder eine reine „Drohkulisse“ allein reichen zum Nachweis der Erforderlichkeit von Videoüberwachungsmaßnahmen dagegen nicht aus (siehe 26. Tätigkeitsbericht 2014 unter Nr. 10.10.2). Nach Aussage der Krankenkasse hat es in der Vergangenheit mehrere Fälle mit gezielter Sachbeschädigung gegeben. Außerdem gebe es gelegentlich Bedrohungen durch Kundinnen und Kunden. Allerdings seien entsprechende Aufzeichnungen inzwischen bereits vernichtet. Für die Zukunft werde aber eine (nicht personenbezogene) Dokumentation vorgenommen.

Zudem hatte die Krankenkasse zu prüfen, ob nicht weniger eingriffsintensive Mittel der Aufsicht beziehungsweise Überwachung ausreichen. Auch dürfen keine Anhaltspunkte dafür bestehen, dass durch die Videoüberwachung überwiegende schutzwürdige Interessen der Betroffenen beeinträchtigt werden (Art. 21a Abs. 1 Satz 2 BayDSG). Im konkreten Fall war sichergestellt, dass die Kameras für die Beschäftigten am Kundenempfang nicht zoom- oder schwenkbar sind, das heißt Personen in der Tiefgarage nicht näher beobachtet werden können.

Ich wirkte darauf hin, dass Hinweisschilder deutlich auf den Einsatz der Kameras hinweisen (Art. 21a Abs. 2 BayDSG). Zudem sind die Videoaufzeichnungen nach drei Wochen zu löschen, soweit sie nicht zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung und von Straftaten oder zur Geltendmachung von Rechtsansprüchen benötigt werden (Art. 21a Abs. 5 BayDSG). Letztlich konnte ich auch eine Reduzierung der Zugriffsberechtigungen erreichen.

Aufgrund des bekannt gewordenen Sachverhalts habe ich mit der Krankenkasse vereinbart, dass die Kameras in zwei Jahren abgebaut werden, wenn bis dahin keine weiteren Schadensfälle eingetreten sind und sich die Gefährdungslage entspannt hat.

8.2 Pflege

8.2.1 Vollzug des Pflege- und Wohnqualitätsgesetzes

Bereits in den letzten Berichtszeiträumen hatte ich mich intensiv mit dem Vollzug des Pflege- und Wohnqualitätsgesetzes (PfleWoqG) auseinandergesetzt (siehe 23. Tätigkeitsbericht 2008 unter Nr. 17.7.1 und 26. Tätigkeitsbericht 2014 unter Nr. 8.2.1). Auf meine Anregung hin war das Staatsministerium für Gesundheit und Pflege bereit, seine Rechtsauffassung zum Zustimmungserfordernis bei Qualitätsprüfungen weiterzuentwickeln:

— Bei Qualitätsprüfungen hat die Zustimmung der Bewohnerin oder des Bewohners beziehungsweise der Betreuerin oder des Betreuers zu bestimmten Fällen der Erhebung, Verarbeitung und Nutzung der Daten vor der Prüfung im absoluten Regelfall in schriftlicher oder in sonstiger Textform zu erfolgen (Art. 11 Abs. 2 Satz 2 ff. PfleWoqG).

— Die in diesen Fällen an sich nicht zulässige mündliche Form der Zustimmung vor der Prüfung werde ich jedoch unter bestimmten Umständen nicht beanstanden. Dann müsste allerdings zum einen festgehalten sein, aus welchen Gründen eine Zustimmung in schriftlicher oder sonstiger Textform nicht abgegeben werden kann. Zum anderen müsste die mündliche Einwilligung sogleich durch eine dritte Person – die jedoch nicht die Prüfinstitution selbst sein kann – in Textform dokumentiert werden.

Die Einhaltung dieses vereinbarten Verfahrens habe ich im Berichtszeitraum durch eine Umfrage überprüft. Die Ergebnisse waren allerdings nicht zufriedenstellend:

Mit der Umfrage wollte ich insbesondere erfahren, in welchen Konstellationen die Fachstellen für Pflege und Behinderteneinrichtungen – Qualitätsentwicklung und

Aufsicht (FQAs) in der Praxis tatsächlich lediglich mündliche Einwilligungserklärungen einholen. Nur etwa zwei Drittel der angeschriebenen Stellen machen von dieser Möglichkeit – absprachegemäß – allein dann Gebrauch, wenn eine Einwilligungserklärung in Schrift- oder sonstiger Textform bei den Betreuerinnen oder Betreuern nicht eingeholt werden kann.

Etwa ein Drittel der geprüften FQAs hingegen geht unzulässigerweise über die Grenzen des vereinbarten Verfahrens hinaus. Knapp zehn Prozent der FQAs holen ausschließlich mündliche Einwilligungserklärungen ein. Zum Teil räumen die FQAs den Betroffenen aber auch ein Wahlrecht ein, ob sie ihre Einwilligungserklärungen mündlich oder schriftlich abgeben möchten. Sie begründen dieses Wahlrecht mit dem Unwillen vieler Betroffener, Erklärungen zu unterschreiben. Dies kann aber kein Argument dafür sein, die gesetzlichen Vorschriften außer Acht zu lassen. Teilweise holen die Behörden aber auch bei Betreuerinnen und Betreuern generell und ohne Ausnahme mündliche Einwilligungserklärungen ein.

Die Auswertung hat allerdings auch ergeben, dass weniger als zehn Prozent der FQAs überhaupt Kommunikationsmittel wie E-Mail, Fax oder SMS verwenden. Dies deutet darauf hin, dass mit dem Einsatz zeitgemäßer Kommunikationsmittel zumindest die Erteilung der Einwilligung in Textform deutlich erhöht werden könnte.

An sich kennt das Pflege- und Wohnqualitätsgesetz keine mündlichen Einwilligungserklärungen. Allerdings habe ich jedoch gemeinsam mit dem Staatsministerium für Gesundheit und Pflege eine „Duldungslösung“ erarbeitet. Danach sehe ich ausnahmsweise unter bestimmten Umständen von einer Beanstandung ab, wenn eine Einwilligungserklärung in Schrift- oder sonstiger Textform bei Betreuerinnen und Betreuern faktisch nicht in Betracht kommt (siehe oben).

Leider dokumentiert aber nur etwa die Hälfte der FQAs schriftlich, warum eine mündliche Einwilligungserklärung eingeholt wurde. In diesen Fällen ließen zudem lediglich 40 Prozent der FQAs die eigentlich gebotene Dokumentation durch einen Dritten (beispielsweise Pflegepersonal, Einrichtungsleitung) vornehmen. Bei den übrigen 60 Prozent hingegen dokumentierte ein Mitglied der FQAs selbst.

Diese datenschutzrechtlichen Verstöße sind umso bedauerlicher, da sowohl das Formular als auch das Schreiben des Staatsministeriums für Gesundheit und Pflege diese Dokumentationspflichten vorsehen. Diese sollen der Gefahr eines Missbrauchs der genannten Duldungslösung entgegenwirken. Allerdings verwenden lediglich etwa zwei Drittel der angeschriebenen Stellen das aktuelle, mit mir abgestimmte Formular des Staatsministeriums für Gesundheit und Pflege.

Nach meinen Hinweisen haben mir mehrere FQAs zugesichert, das vereinbarte Verfahren umzusetzen. Ich werde weiterhin auf dessen konsequente Umsetzung hinwirken. Dies gilt auch für Qualitätsprüfungen des Medizinischen Dienstes der Krankenversicherung (§§ 114 ff. Sozialgesetzbuch Elftes Buch) und der Bezirke (§§ 75 ff. Sozialgesetzbuch Zwölftes Buch).

8.3 Sozialbehörden

8.3.1 Anforderung von Kontounterlagen

Im Berichtszeitraum habe ich bei etwa 120 bayerischen Sozialbehörden geprüft, ob sie bei der Anforderung von Kontounterlagen die Vorgaben des Sozialgesetzbuchs und der Rechtsprechung (siehe Bundessozialgericht, Urteile vom 19. September 2008 – B 14 AS 45/07 R – sowie vom 19. Februar 2009 – B 4 AS 10/08 R; 24. Tätigkeitsbericht 2010 unter Nr. 8.15) einhalten. Die Prüfung betraf unter anderem den Vollzug des Sozialgesetzbuchs Zweites Buch (SGB II, Grundsicherung für Arbeitssuchende), des Sozialgesetzbuchs Achtes Buch (SGB VIII, Kinder- und Jugendhilfe), des Sozialgesetzbuchs Zwölftes Buch (SGB XII, Sozialhilfe), des Wohngeldgesetzes, des Unterhaltsvorschussgesetzes, des Bundesausbildungsförderungsgesetzes und des Asylbewerberleistungsgesetzes.

Sozialbehörden fordern von Personen, die Sozialleistungen beantragt haben, Kontounterlagen für zurückliegende Zeiträume an, beispielsweise um deren Angaben zum Einkommen zu kontrollieren.

Die Prüfungen haben gezeigt, dass die Sozialbehörden sehr unterschiedlich vorgehen und die meisten von ihnen jedenfalls nicht alle datenschutzrechtlichen Vorgaben einhalten:

Nach der Rechtsprechung dürfen Sozialbehörden von Antragstellerinnen und Antragstellern grundsätzlich Kontounterlagen von bis zu drei Monaten anfordern (siehe auch Landessozialgericht Bayern, Urteil vom 13. Juli 2012 – L 7 AS 492/12 B ER; 24. Tätigkeitsbericht 2010 unter Nr. 8.15). Insoweit besteht eine entsprechende Mitwirkungspflicht der Betroffenen. Die Anforderung von Kontounterlagen der letzten sechs Monate ist lediglich ausnahmsweise erforderlich (siehe Entscheidungen des Bundessozialgerichts vom 15. Juli 2010 – B 14 AS 45/10 – und des Landessozialgerichts Nordrhein-Westfalen vom 3. März 2010 – L 12 AS 15/08 – sowie des Landessozialgerichts Bayern vom 24. September 2012 – L 7 AS 660/12 ER: unregelmäßige Einkünfte, des Landessozialgerichts Nordrhein-Westfalen vom 19. Dezember 2014 – L 2 AS 267/13: Verdacht des Leistungsmissbrauchs). In solchen Ausnahmefällen sollte die Behörde die Gründe schon aus Nachweisgründen dokumentieren. Lediglich in ganz besonders gearteten Fällen sind Anforderungen über längere Zeiträume denkbar (siehe Landessozialgericht Sachsen-Anhalt, Urteil vom 19. Januar 2011 – L 5 AS 452/10 B ER: Verdacht einer Erbschaft). Demgegenüber forderte eine Reihe der geprüften Sozialbehörden Kontounterlagen pauschal für deutlich längere Zeiträume an, ohne dass ein Ausnahmegrund vorlag. Zeiträume von mehreren Jahren oder – wie vereinzelt festgestellt – sogar von bis zu zehn Jahren sind hingegen grundsätzlich nicht erforderlich. Außerdem ist grundsätzlich nicht zwischen Erst- und Weiterbewilligungsanträgen sowie unterschiedlichen Bewilligungszeiträumen zu unterscheiden.

Die den Sozialantrag stellenden Personen dürfen auf ihren Kontounterlagen bei den Ausgaben (nicht jedoch bei Einnahmen) den Überweisungszweck beziehungsweise den Empfänger (nicht aber deren Höhe) schwärzen, sofern es sich um „besondere Arten personenbezogener Daten“ (§ 67 Abs. 12 Sozialgesetzbuch Zehntes Buch – SGB X) handelt. Dies sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Nur

etwa die Hälfte der Sozialbehörden hielt sich an diese rechtlichen Vorgaben; die Übrigen wollten ausdrücklich keinerlei Schwärzungen akzeptieren. Diese Haltung zahlreicher Sozialbehörden verstößt gegen geltendes Recht. Die besonders sensiblen Daten dürfen geschwärzt werden.

Die Rechtsprechung hat betont, dass Sozialbehörden die Antragstellerinnen und Antragsteller auf die Möglichkeit zur Schwärzung der besonderen Datenarten hinweisen müssen. Dies sollte schon aus Nachweisgründen schriftlich erfolgen. Nur wenige der von mir überprüften Behörden kamen dieser Pflicht nach. Dadurch ist das Recht zur Schwärzung dieser Daten oftmals leergelaufen, weil die Betroffenen ohne entsprechende Hinweise häufig keine Kenntnis von diesem Recht haben.

Die Rechtsprechung kann nicht dadurch umgangen werden, dass die jeweiligen Stellen beispielsweise „geeignete Nachweise“ oder „Bankauskünfte“ verlangen. Hier sind die eben genannten Grundsätze anzuwenden.

Sollte sich jedoch aus den geschwärzten Kontoauszügen ergeben, dass in auffälliger Häufung oder Höhe Beträge überwiesen werden, so ist nach der Rechtsprechung jeweils im Einzelfall zu entscheiden, inwieweit die Sozialbehörde ausnahmsweise eine Offenlegung auch des bislang geschwärzten Adressaten fordern kann. Antragstellerinnen und Antragsteller können jedoch auch auf ihre Schwärzungsmöglichkeit verzichten und ungeschwärzte Kontoauszüge vorlegen. In diesen Fällen bietet sich eine Erklärung an, dass die Antragstellenden auf ihr Recht zur Schwärzung verzichten, sowie eine schriftliche Einwilligung, dass auch ungeschwärzte Kontoauszüge zu den Akten genommen werden dürfen (§ 67b SGB X).

Inzwischen haben die meisten Sozialbehörden die jeweils festgestellten Mängel behoben. Mit den jeweiligen Staatsministerien befinde ich mich derzeit im Austausch. Punktuelle Überprüfungen vor Ort behalte ich mir vor.

Bei Kontounterlagen ist zwischen Erhebung und Speicherung zu unterscheiden. Inzwischen hat das Landessozialgericht Bayern (Beschluss vom 21. Mai 2014 – L 7 AS 347/14 B ER) entschieden, dass eine Speicherung von Kontounterlagen dann zulässig ist, wenn deren Erhebung zulässig war.

8.3.2 Erhebung medizinischer Daten

Im Berichtszeitraum habe ich mehrfach – wie bereits in der Vergangenheit (siehe 25. Tätigkeitsbericht 2012 unter Nr. 8.12) – die Erhebung medizinischer Daten durch Sozialbehörden überprüft. Betroffen war insbesondere der Vollzug des Sozialgesetzbuchs Zweites Buch (SGB II – Grundsicherung für Arbeitssuchende), des Sozialgesetzbuchs Neuntes Buch (SGB IX – Rehabilitation und Teilhabe behinderter Menschen), des Sozialgesetzbuchs Zwölftes Buch (SGB XII – Sozialhilfe) und des Wohngeldgesetzes. Die Sozialbehörden haben sich dabei häufig für Diagnosen, gesundheitliche Beeinträchtigungen, ärztliche Behandlungen, Arzt-, Krankenhaus-, Rehaentlass- und Therapieberichte, Gutachten und Atteste interessiert. Bei den geprüften, aber auch bei anderen Sozialleistungsbehörden vertrete ich folgende Auffassung, die die geprüften Sozialbehörden zunächst in sehr unterschiedlicher Art und Weise erfüllt haben:

Die Erhebung der medizinischen Daten muss in jedem Fall für die Erfüllung der jeweiligen Aufgabe erforderlich sein. Es müssen also konkrete Anhaltspunkte für

eine Beeinträchtigung der Betroffenen vorliegen. Die „Krankengeschichte“ der Betroffenen ist dabei grundsätzlich nur mittelbar relevant. Entscheidend ist vielmehr, welche konkreten Beeinträchtigungen diese aktuell für die Betroffenen zur Folge hat. Daher sollte der Schwerpunkt bei entsprechenden Abfragen auf den jeweiligen Einschränkungen bei den Betroffenen liegen und nicht auf deren Krankheiten. Erforderlich dürften in der Regel auch nur medizinische Daten der letzten Jahre sein. Berichte, die sich auch mit weit zurückliegenden Gesundheitsproblemen auseinandersetzen, sind daher datenschutzrechtlich problematisch. Dies gilt insbesondere auch für Berichte von Psychotherapeutinnen und -therapeuten, die sich in der Regel sogar mit der Kindheit der jeweiligen Betroffenen auseinandersetzen. Allein die Tatsache, dass derartige Berichte bestimmte erforderliche Daten enthalten, rechtfertigt nicht deren Anforderung in Gänze. Vielmehr ist hier zu prüfen, ob nicht lediglich Teile dieser Berichte zu erheben oder zur Akte zu nehmen sind. Unter Umständen kommen auch Schwärzungen in Betracht (siehe Nr. 8.3.1).

Klärungsbedarf besteht hinsichtlich der Frage, wer insbesondere die sensiblen medizinischen Daten überhaupt zur Kenntnis nehmen darf. Nach der Rechtsprechung verfügen Sachbearbeiter einer Sozialbehörde grundsätzlich nicht über die notwendige medizinische Ausbildung (Entscheidungen des Bayerischen Verwaltungsgerichtshofs vom 31. Januar 2013 – 12 B 12.860 – und des Bundessozialgerichts vom 16. Mai 2012 – B 3 KR 14/11 R, siehe auch Nr. 8.1.1). Daher ist es grundsätzlich nicht erforderlich, dass sie sensible medizinische Daten zur Kenntnis nehmen. Vorbehalten ist dies in der Regel ausschließlich den durch die Sozialbehörde beauftragten begutachtenden Ärztinnen und Ärzten (siehe auch Nr. 8.3.9). Die Tatsache, dass die Sozialbehörde über keinen oder nur über einen unzureichend ausgestatteten ärztlichen Dienst verfügt, ist datenschutzrechtlich ohne Belang. Für zulässig erachte ich es jedoch, wenn die sensiblen medizinischen Daten der Sozialbehörde im verschlossenen Umschlag zur ausschließlichen ärztlichen Kenntnisnahme zur Verfügung gestellt werden. Ein derartiges Verfahren war bisher auch im Bereich der gesetzlichen Krankenversicherung vorgesehen (siehe Nr. 8.1.2). Hier bietet sich ein farbiger Umschlag mit dem Aufdruck „Nur vom Ärztlichen Dienst zu öffnen“ an, um versehentliches Öffnen zu verhindern.

Sachbearbeiterinnen und Sachbearbeiter der Sozialbehörde hingegen haben lediglich ein Interesse an der Klärung von Fragen, die im Hinblick auf ihre jeweilige Aufgabe konkret erforderlich ist. Dementsprechend dürfen Beratungsärztinnen und Beratungsärzte allenfalls punktuell Angaben zu Krankheitsdaten machen. Grundsätzlich unzulässig ist jedoch die Übermittlung der „Krankengeschichte“ der jeweils Betroffenen. Mehr ist für eine Plausibilitätsprüfung der Sachbearbeiterin oder des Sachbearbeiters beziehungsweise zur Begründung eines Verwaltungsakts nicht erforderlich. Ausführliche allgemeine globale Fragen oder Beschreibungen des Krankheitsbilds der Betroffenen sind hingegen datenschutzrechtlich problematisch. Grundsätzlich sind die Daten bei den Betroffenen selbst zu erheben. Dabei sind die Betroffenen auf etwaige Pflichten und Mitwirkungsvorschriften (§§ 60 ff. Sozialgesetzbuch Erstes Buch – SGB I), insbesondere auf mögliche Folgen der Verweigerung hinzuweisen (§ 67a Abs. 3 Satz 3 Sozialgesetzbuch Zehntes Buch –SGB X). Dies sollte grundsätzlich schon aus Nachweisgründen schriftlich erfolgen.

Lediglich in Ausnahmefällen ist eine Datenerhebung bei Dritten vorgesehen (siehe Nr. 8.3.6).

Häufig kommt daher eine schriftliche Einwilligungs- beziehungsweise Schweigepflichtentbindungserklärung in Betracht. Diese ist laut Rechtsprechung etwa zwei Jahre gültig (vgl. Landgericht Berlin, Beschluss vom 2. Juli 2004 – 15 O 653/03). Vielfach verwenden Behörden allzu pauschale und umfassende Einwilligungserklärungen. Hier hat nicht zuletzt das Bundesverfassungsgericht Bedenken geäußert. Vielmehr seien die erforderlichen Daten im Dialog zu ermitteln (Beschluss vom 17. Juli 2013 – 1 BvR 3167/08). Datenschutzrechtlich wünschenswert wäre an sich eine namentliche Auflistung der betroffenen Stellen/Personen und der Auskünfte/Unterlagen. In jedem Fall muss aber der zeitliche Umfang der Datenerhebung in den Erklärungen begrenzt werden. Außerdem sollten die Betroffenen die Möglichkeit haben, bestimmte Stellen/Personen und Auskünfte/Unterlagen von ihrer Einwilligungserklärung auszunehmen.

Bei der Einwilligungserklärung ist die betroffene Person auf die Folgen der Verweigerung der Einwilligung hinzuweisen (§ 67b Abs. 2 Satz 1 SGB X). Wird die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt, so ist sie aufgrund zwingender gesetzlicher Vorgaben im äußeren Erscheinungsbild der Erklärung hervorzuheben (§ 67b Abs. 2 Satz 4 SGB X).

Zudem sollte die Sozialbehörde in der Erklärung gegebenenfalls darauf hinweisen, dass die Erhebung auch medizinische Unterlagen betreffen kann, die nicht nur von der jeweiligen Ärztin oder dem jeweiligen Arzt, sondern auch von Dritten (etwa Laboren) erstellt worden sind. Des Weiteren sollte eine Klarstellung erfolgen, wenn die Schweigepflichtentbindung auch psychologische Unterlagen umfassen kann. Die Erklärungen sollen auch darauf hinweisen, dass die Betroffenen sie jederzeit widerrufen können.

Bei der Information über die Weitergabe von medizinischen Unterlagen durch die Sozialbehörde sind sozialdatenschutzrechtliche Vorgaben zu berücksichtigen. So sind die Betroffenen zu Beginn des Verwaltungsverfahrens in allgemeiner Form schriftlich auf ihr Widerspruchsrecht hinzuweisen (§ 76 Abs. 2 Nr. 1 SGB X). Eine mündliche Belehrung reicht nicht aus. Hier sollte das einschlägige Formular vielmehr eine Ankreuzmöglichkeit für einen etwaigen Widerspruch hinsichtlich der Übermittlung vorsehen. Des Weiteren ist klarzustellen, dass eine Übermittlung an andere Sozialleistungsträger lediglich dann zulässig ist, soweit dies erforderlich ist.

Bei den Anschreiben an Dritte haben die geprüften Behörden nicht immer den Datenschutz beachtet. Auch hier ist auf eine Pflicht zur Auskunft oder Vorlage von Unterlagen beziehungsweise die Freiwilligkeit der Mitwirkung hinzuweisen (§ 67a Abs. 4 SGB X). Allgemeine Verweise auf den Untersuchungsgrundsatz oder die Amtshilfe sind nicht ausreichend. Außerdem ist bei den anzugebenden Befugnissen darauf zu achten, ob sie lediglich Auskünfte (etwa § 100 SGB X) oder auch die Vorlage von Unterlagen ermöglichen.

8.3.3 Anforderung von weiteren Unterlagen

Im Berichtszeitraum habe ich mich vielfach damit beschäftigt, inwiefern die Anforderung bestimmter weiterer Unterlagen für den Vollzug der jeweiligen Sozialleistung erforderlich ist. Dies betraf unter anderem den Vollzug des Sozialgesetzbuchs Zweites Buch (SGB II – Grundsicherung für Arbeitssuchende), des Sozialgesetzbuchs Zwölftes Buch (SGB XII – Sozialhilfe) und des Bundeselterngeld- und Elternzeitgesetzes. Dabei konnte ich mit dem Staatsministerium für Arbeit

und Soziales, Familie und Integration bestimmte Regeln festlegen, die bei der Erhebung der weiteren Unterlagen in jedem Fall zu beachten sind. In diesen Fällen besteht auch eine Mitwirkungspflicht der Betroffenen (§§ 60 ff. Sozialgesetzbuch Erstes Buch – SGB I). Die folgenden Punkte gelten grundsätzlich auch für andere Sozialleistungsbereiche.

— Personalausweis (siehe auch 25. Tätigkeitsbericht 2012 unter Nr. 8.9):

  Bei einer Identifizierung unter Anwesenden ist die Erstellung einer Kopie des Personalausweises grundsätzlich unzulässig, weil regelmäßig kein Bedarf dafür besteht. Die Sachlage ist jedoch anders zu beurteilen, wenn Leistungen für Nichtanwesende (etwa Ehepartner, volljährige Kinder) beantragt werden.

  Bei einer Kopie des Personalausweises sind nichtrelevante Daten wie etwa Größe oder Augenfarbe abzudecken oder auf der Kopie zu schwärzen. Die Antragstellenden sind auf diese Möglichkeit des Abdeckens oder Schwärzens schriftlich hinzuweisen (siehe Nr. 8.3.1).

— Anmeldebestätigung :

  Die Vorlage der Anmeldebestätigung der Antragstellenden bei der Meldebehörde ist nur in Ausnahmefällen erforderlich. Da die Begründung des gewöhnlichen Aufenthalts nicht von der Meldung bei der Einwohnermeldebehörde abhängt, bedarf es dieser grundsätzlich auch nicht. In der Regel kann der gewöhnliche Aufenthalt auch anderweitig nachgewiesen werden.

— Arbeitsvertrag:

  Die Datenspeicherung und -nutzung sollte sich auf die Teile des Arbeitsvertrages beschränken, die für die Berechnung der Sozialleistungen konkret erforderlich sind. Nur diese Teile dürfen in Kopie zu den Akten genommen werden. Hier ist meiner Ansicht nach schon bei der Erhebung eine Schwärzung der nicht relevanten Teile möglich.

— Mietvertrag:

  Es ist nicht erforderlich, den gesamten Mietvertrag, sondern lediglich die für die Leistungsgewährung erforderlichen Teile in Kopie zu den Akten zu nehmen. Meiner Ansicht nach ist auch hier schon bei der Erhebung eine Schwärzung der nicht relevanten Teile möglich.

  Die Sozialbehörde darf grundsätzlich Vermieterinnen und Vermietern (etwa durch Mietbescheinigung oder unmittelbare Überweisung; siehe 22. Tätigkeitsbericht 2006 unter Nr. 14.4.2, 23. Tätigkeitsbericht 2008 unter Nr. 17.6.1, 25. Tätigkeitsbericht 2012 unter Nr. 8.18; Bundessozialgericht, Entscheidung vom 25. Januar 2012 – B 14 AS 65/11 R 1) oder einen sonstigen Dritten (siehe auch 21. Tätigkeitsbericht 2004 unter Nr. 6.4; 24. Tätigkeitsbericht 2010 unter Nr. 8.21) nicht darüber informieren, dass die jeweiligen Betroffenen Sozialleistungen erhalten. Eine Ausnahme besteht nur bei einer ausdrücklichen Rechtsgrundlage oder einer Einwilligung der betroffenen Personen.

— Gas- und Stromliefervertrag:

  Es ist ausreichend, wenn für die Leistungsgewährung die Teile des Gas- und Stromliefervertrags vorgelegt werden, aus denen die anfallenden Kosten ersichtlich sind, beispielsweise Jahresabrechnungen.

— Kfz-Haftpflichtversicherungsvertrag:

  Die Erhebung und Nutzung vollständiger Kfz-Haftpflichtversicherungsverträge ist nicht erforderlich. Zwar können derartige Beiträge unter Umständen einkommensmindernd berücksichtigt werden; die Höhe der Beiträge kann aber mittels der (jährlichen) Mitteilung über die Beitragshöhe festgestellt werden.

— Scheidungsurteil:

  Die Vorlage von Scheidungsurteilen (ohne Unterhaltsfestsetzung) ist für eine Leistungsgewährung und die Leistungshöhe nicht von Belang. Von Bedeutung ist vielmehr, welche Personen einer Bedarfsgemeinschaft angehören.

8.3.4 Erklärung über persönliche und sachliche Verhältnisse

Im Berichtszeitraum habe ich mich mit einem datenschutzrechtlich bedenklichen Formular verschiedener Wohngeldbehörden auseinander gesetzt. Danach sollten die Antragstellerinnen oder Antragsteller darlegen, wieviel sie durchschnittlich monatlich jeweils beispielsweise für die Bereiche Ernährung, Unterkunft, Neuanschaffung von Bekleidung, Reinigung und Reparatur von Kleidung, Haushaltsgegenstände und Möbel, persönliche Dinge des täglichen Lebens (etwa Kosmetik, Körperpflege, Bücher, Zeitschriften, Vereine), Telefon/Rundfunk/Fernsehen, Versicherungen und Kraftfahrzeug ausgegeben haben. Begründet haben diese Behörden die Datenerhebung damit, es sei nicht nachvollziehbar, wie die Antragstellenden mit den von ihnen angegebenen geringen Einnahmen bislang ihren Lebensunterhalt bestreiten konnten.

Ich bin der Auffassung, dass solche generalisierten Datenerhebungen zu weitgehend sind. Wenn berechtigte Zweifel an der Glaubhaftigkeit und Vollständigkeit der Angaben bestehen, kann die jeweilige Sozialbehörde weitere Angaben verlangen, um die Einkommenssituation der antragstellenden Person zu klären. Für den Nachweis der Plausibilität kommen auch andere Möglichkeiten in Betracht.

Letztlich hat auch das Staatsministerium des Innern, für Bau und Verkehr meine Auffassung bestätigt. Sollten derartige Formulare in Ausnahmefällen überhaupt Verwendung finden, ist zukünftig deutlich schriftlich darauf hinzuweisen, dass das Ausfüllen nicht verpflichtend ist und andere Möglichkeiten der Glaubhaftmachung unbenommen bleiben.

Im Rahmen dieses Vorgangs hatte ich mich auch mit der Problematik zu beschäftigen, dass eine Behörde veraltete Antragsformulare verwendet hat. Ein „Aufbrauchen“ noch vorhandener – überholter – Leerformulare kann sich aus Datenschutzsicht allerdings dann als problematisch erweisen, wenn sich die Ausgangssituation verändert hat und bestimmte Angaben nicht mehr erforderlich sind. Deshalb appelliere ich an die zuständigen Behörden, stets nur aktuelle Formulare zu

verwenden und im Interesse der Betroffenen an dieser Stelle keine „falsche" Sparsamkeit walten zu lassen. Auch im Internet vorgehaltene Formulare sind regelmäßig daraufhin zu überprüfen, ob sie dem aktuellen Stand entsprechen.

8.3.5 Beantragung von Sozialleistungen über die Gemeinde

Im Berichtszeitraum habe ich – wie bereits in der Vergangenheit (siehe 24. Tätigkeitsbericht 2010 unter Nr. 8.20, 25. Tätigkeitsbericht 2012 unter Nr. 8.7) – auch Antragsformulare im Bereich der Sozialhilfe geprüft. Bei einigen Formularen wurde die Wohnsitzgemeinde beispielsweise aufgefordert mitzuteilen, ob die vorstehenden Angaben der Wahrheit entsprechen, ob sie die Notlage bestätigt und seit wann diese Notlage der Gemeinde bekannt ist.

§ 16 Sozialgesetzbuch Erstes Buch (SGB I) begründet aber lediglich die Möglichkeit, Anträge auf Sozialleistungen auch vor Ort bei der Gemeinde zu stellen. Zweck dieser Regelung ist es, den Bürgerinnen und Bürgern die Antragstellung zu erleichtern und ihnen größeren Aufwand und längere Anreisewege zu ersparen. Ob Antragstellerinnen oder Antragsteller von dieser Möglichkeit Gebrauch machen, ist ihre eigene Entscheidung. Auch haben Wohnsitzgemeinden grundsätzlich keine eigene Prüfzuständigkeit hinsichtlich der Antragsvoraussetzungen.

Daher ist es zum einen unzulässig, die Betroffenen zu einer Antragstellung bei der Gemeinde zu verpflichten. Zum anderen ist die oben genannte Aufforderung an die Wohnsitzgemeinde zur inhaltlichen Prüfung grundsätzlich unzulässig. Diese Problematik ist auch bei anderen Sozialleistungen oder anderen Behörden denkbar (siehe 23. Tätigkeitsbericht 2008 unter Nr. 17.6.1).

Auch eine regelmäßige, anlassunabhängige Übersendung von Sozialhilfebescheiden (Abdrucken) an kreisangehörige Gemeinden und Städte durch einen Landkreis ist aus diesem Grund unzulässig (siehe schon 21. Tätigkeitsbericht 2004 unter Nr. 6.4).

8.3.6 Einsatz von Sozialdetektiven, Recherche im Internet oder in Sozialen Netzwerken

Im Berichtszeitraum musste ich mehrfach sehr weitgehende Nachforschungen von Sozialbehörden überprüfen. In einem Fall ließ eine Krankenkasse einen Versicherten durch einen Detektiv verdeckt observieren. In einem weiteren Fall hat ein Sozialamt durch einen Ermittler im Umfeld eines Leistungsbeziehers Befragungen durchgeführt. Dazu habe ich mich bereits in der Vergangenheit in Abstimmung mit den kommunalen Spitzenverbänden sehr kritisch geäußert (siehe 18. Tätigkeitsbericht 1998 unter Nr. 4.5.4). Außerdem war ich mehrfach mit der Recherche von Sozialbehörden im Internet oder in Sozialen Netzwerken befasst. Zu diesen Themenkomplexen habe ich im Berichtszeitraum nachfolgende Ansicht vertreten:

— Eingriff in das Recht auf informationelle Selbstbestimmung

  Ein Eingriff in das Recht auf informationelle Selbstbestimmung liegt schon dann vor, wenn Informationen, die durch die Sichtung allgemein zugänglicher Inhalte gewonnen wurden, gezielt zusammengetragen, gespeichert

und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich daraus eine besondere Gefahrenlage für die Persönlichkeit der Betroffenen ergibt (siehe Bundesverfassungsgericht, Urteil vom 27. Februar 2008 – 1 BvR 370/07, 1 BvR 595/07). In den geschilderten Fällen haben die jeweiligen Sozialbehörden bestimmte, bereits vorliegende Anhaltspunkte für einen Leistungsmissbrauch mit weiteren gezielt recherchierten Daten (aus Beobachtungen, Befragungen, Internet und Sozialen Netzwerken) abgeglichen.

— Spezielle Befugnis

Im ersten Fall hatte ich schon Zweifel, ob das Sozialrecht überhaupt Observationen oder „verdeckte Ermittler" zulässt (vgl. Entscheidung des Oberverwaltungsgerichts Thüringen vom 25. November 2010 – 3 KO 527/08; 18. Tätigkeitsbericht 1998 unter Nr. 4.5.4). Schließlich sehen andere Rechtsgebiete dafür bereichsspezifische Datenschutzregelungen vor. Zudem handelt es sich bei Sozialdaten grundsätzlich um besonders sensible Daten.

— Allgemeine Befugnis

Außerdem hatte ich bei der Recherche im Internet oder in Sozialen Netzwerken schon Zweifel an der Eignung der Maßnahme. Schließlich entsprechen Angaben in Sozialen Netzwerken aus verschiedenen Gründen häufig nicht der Realität. Beispielsweise können Nutzende ihre Profile lange nicht mehr aktualisiert haben oder sie möchten Änderungen ihrer Lebensumstände absichtlich nicht einstellen, damit sie anderen Nutzenden nicht bekannt werden. Da somit die inhaltliche Richtigkeit, Vollständigkeit und Aktualität der eingestellten Daten nicht sichergestellt sind, ist auch die Geeignetheit der Erhebung entsprechender Daten fraglich. Dies gilt umso mehr, wenn Dritte die Informationen ins Internet gestellt haben.

Grundsätzlich besteht eine allgemeine Befugnis zur Erhebung von Daten, soweit dies zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist (§ 67a Abs. 1 Satz 1 Sozialgesetzbuch Zehntes Buch – SGB X).

Allerdings hatte ich schon Zweifel an der Erforderlichkeit der getroffenen Maßnahmen. Der Eingriff muss von der Reichweite und Intensität her in einem ausgewogenen Verhältnis stehen zu dem im überwiegenden öffentlichen Interesse liegenden Gebot, Sozialleistungsmissbrauch vorzubeugen und gegebenenfalls zu unterbinden. In den konkreten Einzelfällen bestanden jeweils zwar durchaus tatsächliche Anhaltspunkte für einen Leistungsmissbrauch. Das Gesetz sieht in derartigen Fällen als mögliche „Erkenntnisquellen" allerdings die Angabe von Tatsachen (§ 60 SGB I) sowie ein persönliches Erscheinen (§ 61 SGB I) vor.

Außerdem wäre es als milderes Mittel denkbar gewesen, die jeweils Betroffenen mit den Verdachtsmomenten zu konfrontieren.

Zudem enthalten schon das Internet und Soziale Netzwerke personenbezogene Daten, die mehr oder weniger die Privatsphäre der Betroffenen tangieren. Jedenfalls sind sie regelmäßig nicht eindeutig getrennt von Daten, die hinsichtlich eines Sozialleistungsbezugs relevant sein könnten. In-

soweit erhalten Behörden bei der Recherche beabsichtigt oder unbeabsichtigt, jedenfalls unvermeidbar eine Vielzahl von Daten über die Betroffenen, obwohl sie für den konkreten Sozialleistungsbezug nicht erforderlich sind.

Auch die „Beschattung" führt regelmäßig zu zusätzlichen Erkenntnissen aus der Privatsphäre der Betroffenen, die nicht Gegenstand der Ermittlungen sind (siehe 18. Tätigkeitsbericht 1998 unter Nr. 4.5.4). Auch bei dieser Observation wurde „über das Ziel hinaus geschossen": Zum einen erfolgte sie nicht zielgerichtet und punktgenau, sondern an mehreren Orten, zu verschiedenen Uhrzeiten und in verschiedenen Situationen. Außerdem war auch eine Vielzahl unbeteiligter Personen betroffen. Zum anderen wurden Videos und Bilder aufgenommen, obwohl dies nicht notwendig gewesen wäre. Zudem wäre es als mildere Maßnahme denkbar gewesen, Beschäftigte des Außendienstes einzusetzen.

Letzteres gilt auch für die zweite hier geschilderte Problemstellung. Ermittlungen bei Dritten sind ebenfalls nur unter engen Voraussetzungen zulässig: Schließlich ist mit der Befragung anderer Personen oder Stellen regelmäßig die Mitteilung verbunden, dass die Hilfeempfangenden Kontakt zu einem Sozialleistungsträger haben und es dort Anlass für Nachfragen gibt. Keinesfalls darf ein Sozialdetektiv – wie im zweiten Fall – einfach an eine Person aus dem Umfeld des Hilfeempfängers herantreten, der er bei seinem Einsatz gerade begegnet. Auch muss der Sozialdetektiv – anders als hier – seine Fragen so beschränken, dass er möglichst nur die erforderlichen Informationen erhält. Außerdem muss der Sozialdetektiv darauf hinweisen, dass es den Befragten freisteht, Angaben zu machen, und dass ihnen andernfalls keine Nachteile entstehen. Hierzu muss sich der Ermittler als Außendienstmitarbeiter des Sozialamts zu erkennen geben und darf seine Gesprächspartner nicht unter falschen Angaben oder sonstigen Vorwänden zu Äußerungen über den Hilfeempfänger verleiten. Zudem bestehen Mindeststandards für die Auftragserteilung und Dokumentation. Sozialdetektive, die nicht selbst für die Sachbearbeitung zuständig sind, sind über die Rechtslage zu informieren. Sie müssen schriftlich genau definierte Aufträge und Regeln zum Vorgehen erhalten. Außerdem sind Auftragserteilung und Einsätze auch in der Akte der jeweils Betroffenen genau zu dokumentieren (siehe 18. Tätigkeitsbericht 1998 unter Nr. 4.5.4).

— Mitwirkung der Betroffenen

Grundsätzlich sind die Daten nur beim Betroffenen zu erheben. Eine Erhebung ohne Mitwirkung des Betroffenen ist nur unter engen Voraussetzungen möglich (siehe § 67a Abs. 2 Satz 2 Nr. 2 Buchst. b Doppelbuchst. aa SGB X).

§ 67a SGB X Datenerhebung
(2) Sozialdaten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden …
2. bei anderen Personen oder Stellen, wenn
b) aa) die Aufgaben nach diesem Gesetzbuch ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich machen …
und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

Voraussetzung dafür ist, dass die ordnungsgemäße Aufgabenerfüllung ohne die Information durch Dritte typischerweise nicht möglich ist. Maßgeblich ist die Art der Aufgabe, aus der sich allein die Erforderlichkeit der Datenerhebung ohne Mitwirkung der betroffenen Person begründen muss. Diese Erforderlichkeit lässt sich nur bejahen, wenn die betroffene Person die Informationen etwa im Hinblick auf die Art der Daten selbst nicht geben kann, insbesondere die angeforderten Unterlagen nicht hat und auch nicht beibringen kann. Schon diese Voraussetzung war im zweiten Fall nicht erfüllt.

Zudem dürfen keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen der Betroffenen beeinträchtigt werden.

— Unterrichtung der Betroffenen

Im Übrigen hätte der Betroffene jeweils von der Speicherung, der Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung unterrichtet werden müssen (§ 67a Abs. 5 SGB X).

In beiden Fällen habe ich die datenschutzrechtlichen Verstöße beanstandet. Zwar gab es durchaus Anhaltspunkte für einen Leistungsmissbrauch. Dies rechtfertigt jedoch nicht die massiven Eingriffe in das Recht auf informationelle Selbstbestimmung. Durch die Maßnahmen dürften auch Dritten unbefugt Sozialgeheimnisse offenbart worden sein (etwa Detektiven, Nachbarn, Vermietern; vgl. Entscheidung des Bundessozialgerichts vom 25. Januar 2012 – B 14 AS 65/11 R; 23. Tätigkeitsbericht 2008 unter Nr. 17.6.1). Vielmehr hätten andere, mildere Mittel zur Verfügung gestanden.

8.3.7 Einsatz von E-Mail und Fax

Elektronische Post wird inzwischen auch dienstlich häufig als Kommunikationsmittel genutzt. Dabei können insbesondere vertrauliche Dokumente Angriffsmöglichkeiten ausgesetzt sein. Der ungesicherte E-Mail-Versand ist vergleichbar mit dem Verschicken einer Postkarte. E-Mails können eingesehen, verändert oder verfälscht werden. Dies ist insbesondere dann ein Risiko, wenn die E-Mails über ungesicherte Netze wie das Internet übertragen werden.

In den meisten Behörden gehört auch das Faxgerät zu den gängigen Kommunikationsmitteln. Dass allerdings auch die Telefax-Nutzung Sicherheitsrisiken birgt, ist des Öfteren nicht bekannt. Zum einen kann man sich verwählen und die Daten geraten an eine falsche Adresse. Das wird insbesondere dann zu einem Risiko, wenn mit dem Fax personenbezogene Daten versendet werden. So sind bei dem Verlust von sensiblen Daten unter Umständen die zuständige Aufsichts- und die Datenschutzbehörde sowie die Betroffenen zu informieren, sofern diesen schwerwiegende Beeinträchtigungen drohen (§ 83 Sozialgesetzbuch Zehntes Buch – SGB X). Zum anderen sind Faxgeräte oft so aufgestellt, dass auch Unbefugte auf die dort ankommenden Dokumente zugreifen können. Dementsprechend sollten Faxgeräte so aufgestellt werden, dass Unbefugte die übermittelten Informationen nicht erlangen können. Im Gegensatz zu E-Mails werden Faxe (Ausnahme Computerfax) nicht über das Internet übertragen und sind zumindest auf dem Übertragungsweg besser geschützt.

Hinzu kommt, dass Sozialbehörden in der Regel Sozialdaten erheben, verarbeiten und nutzen, die grundsätzlich einen hohen Schutzbedarf haben. Folglich sind besondere technische und organisatorische Schutzmaßnahmen zu ergreifen (§ 78a SGB X). Bei der Übermittlung von schutzwürdigen Informationen über das Internet sind daher Verschlüsselungen einzusetzen. Eine Verschlüsselung von Datenübertragungen über das Internet ist heutzutage durchaus üblich und wird von Stellen wie dem Bundesamt für Sicherheit in der Informationstechnik regelmäßig gefordert. Davon kann lediglich in Ausnahmefällen abgesehen werden, in denen von einem normalen Schutzbedarf auszugehen ist (beispielsweise bei allgemeinen Informationsfragen, Fragen nach dem Verfahrensstand, sachleitenden Informationen) oder die in besonderem Maße eilbedürftig sind. In letztem Fall sind aber zusätzlich geeignete technisch-organisatorische Maßnahmen zu treffen (beispielsweise bei telefonischer Vorankündigung der Nachricht). Insoweit verweise ich auf die Orientierungshilfen auf meiner Homepage https://www.datenschutz-bayern.de.

Weitere Ausnahmen sind auch mit Einwilligung der Betroffenen regelmäßig nicht akzeptabel, da jede öffentliche Stelle dem Grundrechtsschutz und damit der Einhaltung gewisser technischer Mindeststandards verpflichtet ist. Diese Grundrechte dürfen auch nicht durch die massenhafte Einholung von Einwilligungen umgangen werden. Zudem sind Einwilligungen im Bereich des Sozialdatenschutzes nur dort zulässig, wo der Gesetzgeber sie ausdrücklich vorgesehen hat (vgl. Entscheidung des Bundessozialgerichts vom 10. Dezember 2008 – B 6 KA 37/07 R). Dies ist im Anwendungsbereich des § 78a SGB X nicht der Fall.

Aus diesem Grund dürfte auch für Sozialbehörden die Nutzung des „BayernPortals“ interessant sein. Sie ist datenschutzrechtlich im Grundsatz auch nicht unzulässig, soweit das Sozialgesetzbuch keine abschließenden oder entgegenstehenden Regeln enthält. Allerdings hat die Sozialbehörde mit dem Betreiber des „BayernPortals“ einen Vertrag zur Auftragsdatenverarbeitung nach § 80 SGB X abzuschließen.

8.3.8 Akteneinsichtsrecht und Auskunftsanspruch

Akteneinsichten und die damit verbundenen Probleme nehmen einen immer größer werdenden Teil meiner Arbeit ein. Häufig betrafen Beschwerden die Jugendhilfe; allerdings waren auch andere Sozialleistungen betroffen (etwa Grundsicherung, Sozialhilfe).

Für den Zugang zu Akteninformationen gibt es verschiedene Grundlagen (beispielsweise § 25 Sozialgesetzbuch Zehntes Buch – SGB X, § 83 SGB X, Art. 36 BayDSG; siehe auch 20. Tätigkeitsbericht 2002 unter Nr. 5.1; 22. Tätigkeitsbericht 2006 unter Nr. 14.1.3).

8.3.8.1 Recht auf Akteneinsicht

Das Recht auf Akteneinsicht nach § 25 Sozialgesetzbuch Zehntes Buch (SGB X) dient dem Zugang zu Behördeninformationen, soweit dies zur Geltendmachung oder Verteidigung der rechtlichen Interessen der Antragstellerin oder des Antragstellers erforderlich ist. Hintergrund dieser Regelung ist die Gewährleistung des Rechtsstaatsprinzips, das den Beteiligten Anspruch auf rechtliches Gehör und ein faires Verfahren zusichert.

§ 25 SGB X Akteneinsicht durch Beteiligte
(1) Die Behörde hat den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. Satz 1 gilt bis zum Abschluss des Verwaltungsverfahrens nicht für Entwürfe zu Entscheidungen sowie die Arbeiten zu ihrer unmittelbaren Vorbereitung.
(2) Soweit die Akten Angaben über gesundheitliche Verhältnisse eines Beteiligten enthalten, kann die Behörde stattdessen den Inhalt der Akten dem Beteiligten durch einen Arzt vermitteln lassen. Sie soll den Inhalt der Akten durch einen Arzt vermitteln lassen, soweit zu befürchten ist, dass die Akteneinsicht dem Beteiligten einen unverhältnismäßigen Nachteil, insbesondere an der Gesundheit, zufügen würde. ....
(3) Die Behörde ist zur Gestattung der Akteneinsicht nicht verpflichtet, soweit die Vorgänge wegen der berechtigten Interessen der Beteiligten oder dritter Personen geheim gehalten werden müssen.
(4) Die Akteneinsicht erfolgt bei der Behörde, die die Akten führt. Im Einzelfall kann die Einsicht auch bei einer anderen Behörde ... erfolgen; weitere Ausnahmen kann die Behörde, die die Akten führt, gestatten.
(5) Soweit die Akteneinsicht zu gestatten ist, können die Beteiligten Auszüge oder Abschriften selbst fertigen oder sich Ablichtungen durch die Behörde erteilen lassen. Soweit die Akteneinsicht in eine elektronische Akte zu gestatten ist, kann die Behörde Akteneinsicht gewähren, indem sie Unterlagen ganz oder teilweise ausdruckt, elektronische Dokumente auf einem Bildschirm wiedergibt, elektronische Dokumente zur Verfügung stellt oder den elektronischen Zugriff auf den Inhalt der Akte gestattet. Die Behörde kann Ersatz ihrer Aufwendungen in angemessenem Umfang verlangen.

Dass dieses Recht nicht durch überzogene Kosten (beispielsweise Kopien über 0,30 Euro) faktisch ausgehöhlt wird, sollte sich beinahe von selbst verstehen. Aber bereits bezüglich der Frage des „Ob" einer Akteneinsicht ging eine Vielzahl von Beschwerden von Bürgerinnen und Bürgern ein:

Das Recht auf Akteneinsicht ist nicht schon deshalb ausgeschlossen, weil die betroffenen Sozialdaten einen Doppelbezug aufweisen, also auch einen Bezug zu anderen Personen haben. Dies ist häufig bei Dreiecksverhältnissen der Fall (beispielsweise Mutter – Vater – Kind bei Sorgerechts- oder Umgangsverfahren).

Auch der Einwand, dass die Weitergabe von Informationen, beispielsweise an einen antragstellenden Kindsvater, nicht möglich sei, da es sich um „anvertraute" Daten handele, geht zumeist fehl. Anvertraute Daten liegen erst dann vor, wenn die Mitteilung der Daten im Vertrauen und in der Erwartung erfolgt ist, dass diese Informationen Dritten nicht zugänglich sind. Ein „Anvertrauen" liegt aber nicht vor, wenn die betroffene Person weiß oder wissen muss, dass die mitgeteilten Informationen im Rahmen der Aufgabenstellung (beispielsweise einem Gericht) mitzuteilen sind.

Vielmehr hat die Behörde zu prüfen, ob durch das Akteneinsichtsrecht schutzwürdige Belange Dritter berührt sind. Gegebenenfalls ist das Antragsinteresse mit den berechtigten Interessen Dritter abzuwägen (zu Informanten siehe 23. Tätigkeitsbericht 2008 unter Nr. 17.8). Bei einem überwiegenden Interesse Dritter ist von einer Akteneinsicht in Teilen, soweit die Interessen der Dritten reichen, in Ausnahmefällen auch ganz abzusehen.

Zur Vermeidung von Problemen bei später durchzuführenden Akteneinsichten sollte die Behörde daher versuchen, bei der Aktenführung konkret zu differenzieren und die wenigen tatsächlich besonders vertrauenswürdigen Teile schon vorab zu trennen.

Entwürfe fallen nicht unter das Akteneinsichtsrecht. Aktenvermerke, Berichte, Gutachten oder Stellungnahmen anderer Behörden sind hingegen keine Entwürfe. Handschriftliche „persönliche" Vermerke oder Notizen (beispielsweise auf Klebezetteln) oder gar „Handakten" sind nur dann der Akteneinsicht entzogen, wenn die vorgangsrelevanten Tatsachen (beispielsweise in einem abgetippten Vermerk) tatsächlich inhaltlich umfassend formal der Akte zugefügt werden. Dies entspricht der gebotenen Dokumentation des Verwaltungshandelns.

Das Recht auf Akteneinsicht steht aber nur den Beteiligten eines laufenden Verwaltungsverfahrens zu. Dies betrifft grundsätzlich die Antragstellerin oder den Antragsteller beziehungsweise die jeweiligen Adressaten eines beabsichtigten Verwaltungsaktes. Bei der häufig problematisierten Mitwirkung des Jugendamts vor dem Familiengericht liegt tatsächlich schon kein Verwaltungsverfahren vor. Manchmal wird den Betroffenen auch die Akteneinsicht mit der Begründung verwehrt, das Verfahren sei schon abgeschlossen.

8.3.8.2 Sozialrechtlicher Auskunftsanspruch

Häufig kommt es allerdings nicht darauf an, ob ein Verwaltungsverfahren überhaupt vorliegt, noch andauert oder bereits abgeschlossen ist. Das Begehren der auskunftssuchenden Person ist nämlich auszulegen, wie Treu und Glauben mit Rücksicht auf die Verkehrssitte dies erfordern. Dabei ist der wirkliche Wille zu erforschen.

Daher ist ein Begehr auf Akteneinsicht oder nach Informationsfreiheit (die in Bayern so nicht besteht) grundsätzlich auch als Auskunftsanspruch nach § 83 Sozialgesetzbuch Zehntes Buch (SGB X) auszulegen. Dieser Anspruch basiert auf dem Grundrecht auf informationelle Selbstbestimmung, das den Betroffenen das Recht gibt zu wissen, welche Informationen eine öffentliche Stelle über sie hat. Nur dadurch können Betroffene die Informationen erhalten, um möglicherweise Ansprüche auf Berichtigung, Sperrung und Löschung geltend zu machen. Bei diesem Auskunftsanspruch muss die antragstellende Person lediglich Betroffene und nicht Beteiligte sein. Außerdem erscheint dieser Anspruch häufig auch aufgrund seiner Unentgeltlichkeit attraktiv. Hinsichtlich der überwiegend berechtigten Interessen von Dritten gilt das eben Gesagte entsprechend. Bei einer solchen Auskunftserteilung bestimmt aber die verantwortliche speichernde Stelle das Verfahren nach pflichtgemäßem Ermessen, insbesondere die Form der Auskunftserteilung. Eine solche Auskunft kann durch Gewährung von Akteneinsicht erfolgen, aber auch auf andere Weise (siehe 22. Tätigkeitsbericht 2006 unter Nr. 14.1.3).

§ 83 SGB X Auskunft an den Betroffenen
(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über
1. die zu seiner Person gespeicherten Sozialdaten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
2. die Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und
3. den Zweck der Speicherung.
In dem Antrag soll die Art der Sozialdaten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die Sozialdaten nicht automatisiert oder nicht in

nicht automatisierten Dateien gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Die verantwortliche Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen. …
(2) Für Sozialdaten, die nur deshalb gespeichert sind, weil sie auf Grund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder die ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen, gilt Absatz 1 nicht, wenn eine Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.
(3) Bezieht sich die Auskunftserteilung auf die Übermittlung von Sozialdaten an Staatsanwaltschaften und Gerichte im Bereich der Strafverfolgung, an Polizeibehörden, Verfassungsschutzbehörden, den Bundesnachrichtendienst und den Militärischen Abschirmdienst, ist sie nur mit Zustimmung dieser Stellen zulässig.
(4) Die Auskunftserteilung unterbleibt, soweit
1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährden würde,
2. die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder
3. 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,
und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.
(5) Die Ablehnung der Auskunftserteilung bedarf keiner Begründung, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall ist der Betroffene darauf hinzuweisen, dass er sich an … (die Bundes- oder die Landesdatenschutzbeauftragten) wenden kann.
(6) Wird einem Auskunftsberechtigten keine Auskunft erteilt, so kann … (die Bundes- oder die Landesdatenschutzbeauftragten) prüfen, ob die Ablehnung der Auskunftserteilung rechtmäßig war.
(7) Die Auskunft ist unentgeltlich.

Das Recht der gesetzlichen Krankenversicherung sieht mit § 305 Sozialgesetzbuch Fünftes Buch (SGB V) einen weiteren Auskunftsanspruch vor, der neben § 83 SGB X anwendbar ist (siehe auch 19. Tätigkeitsbericht 2000 unter Nr. 4.4.3; 20. Tätigkeitsbericht 2002 unter Nr. 5.4.2).

Theoretisch kommt auch ein allgemeiner Auskunftsanspruch nach Art. 36 BayDSG in Betracht. Danach müsste die antragstellende Person lediglich ein berechtigtes Interesse glaubhaft darlegen. Angesichts des Sozialgeheimnisses (Art. 36 Abs. 3 Nr. 3 BayDSG in Verbindung mit § 35 Sozialgesetzbuch Erstes Buch – SGB I) ist dieser Anspruch jedoch regelmäßig kraft Gesetzes ausgeschlossen.

8.3.9 Outsourcing bei Sozialbehörden

„Outsourcing" – also die Auslagerung von bisher in einem Unternehmen oder einer Behörde selbst erbrachten Leistungen an externe Auftragnehmer oder Dienstleister – beschäftigt mich nicht erst seit diesem Berichtszeitraum (siehe 24. Tätigkeitsbericht 2010 unter Nrn. 2.1.5, 2.2.13 und 8.3; 25. Tätigkeitsbericht

2012 unter Nrn. 2.1.6 und 2.3.1; 26. Tätigkeitsbericht 2014 unter Nrn. 8.4.4 und 13.1). Auch Sozialbehörden bedienen sich immer mehr dieses Instrumentariums. Allerdings beachten sie dabei nicht immer die rechtlichen Vorgaben. Je nach Konstellation sind die Unterschiede in der datenschutzrechtlichen Verantwortlichkeit und Haftung erheblich:

— Eine datenverarbeitende Stelle

  Im einfachsten Fall gibt es eine verantwortliche Stelle, die die personenbezogenen Daten selbst (für eigene Zwecke) erhebt, verarbeitet und nutzt. Da die Daten hier innerhalb der verantwortlichen Stelle verbleiben, liegt keine Übermittlung von Daten vor.

— Dienstverhältnis höherer Art

  Inzwischen beauftragen aber auch immer mehr Sozialbehörden Dienstleister mit der Erbringung bestimmter Leistungen. Dabei werden auch personenbezogene Daten übertragen. Unter bestimmten Umständen kann dieser Dienstleister zumindest rechtlich „Teil der Verwaltung" und damit kein Dritter im Sinne des Datenschutzrechts sein. Damit würde wie im ersten Fall auch keine Datenübermittlung vorliegen.

  Dies ist nach Feststellung des Bundessozialgerichts unter anderem bei Dienstverhältnissen höherer Art der Fall (siehe Urteil vom 5. Februar 2008 – B 2 U 8/07 R). Hierzu zählen Tätigkeiten, die ein überdurchschnittliches Maß an Fachkenntnissen, Kunstfertigkeit oder wissenschaftlicher Bildung, eine hohe geistige Fantasie oder Flexibilität und ein besonderes Maß an persönlichem Vertrauen voraussetzen. Darunter fallen insbesondere Ärzte, Rechtsanwälte, Wirtschaftsberater/-prüfer und Steuerberater, aber unter bestimmten Umständen auch Gutachter und Sachverständige. Ich habe mich im Berichtszeitraum vielfach mit dem Einsatz von Beratungsärztinnen und -ärzten auseinandergesetzt (beispielsweise bei Optionskommunen oder Versorgungsämtern, siehe unter Nr. 8.3.2). Dabei habe ich den Grundsatz der Erforderlichkeit insbesondere unter der Prämisse beleuchtet, dass tatsächlich eine entsprechende medizinische Sachkunde besteht. In den von mir geprüften Fällen lagen hingegen häufig Konstellationen vor, in denen Beschäftigte von Sozialbehörden derartige Fragestellungen selbst entschieden haben (siehe Nr. 8.3.2).

— Auftragsdatenverarbeitung

  Im rechtlichen Ergebnis vergleichbar (lediglich Nutzung, keine Übermittlung von Daten) ist die Auftragsdatenverarbeitung (siehe 26. Tätigkeitsbericht 2014 unter Nr. 8.3). Auch hier beauftragt eine Behörde einen Dienstleister mit einer Datenverarbeitung. Dieser ist aber bei der Auftragsdatenverarbeitung lediglich „ausführendes Werkzeug" der Auftraggeberin Behörde. Für eine Auftragsdatenverarbeitung sprechen folgende „Erkennungsmerkmale":

  — Der Auftraggeber bleibt für die Zulässigkeit der Datenverarbeitung verantwortlich.

  — Dem Auftragnehmer fehlt jegliche Entscheidungsbefugnis.

— Der Auftragnehmer ist strikt an Weisungen des Auftraggebers dahingehend gebunden, was mit den Daten zu geschehen hat.

— Grundsätzlich hat der Auftragnehmer nur mit Daten umzugehen, welche der Auftraggeber zur Verfügung stellt, außer die Beauftragung des Auftragnehmers ist auch auf die Erhebung personenbezogener Daten gerichtet.

— Eine Verarbeitung oder Nutzung der Daten zu eigenen Zwecken des Auftragnehmers ist ausgeschlossen.

— Es besteht keine (vertragliche) Beziehung des Auftragnehmers zu derjenigen Person, deren personenbezogene Daten verarbeitet werden.

— Der Auftragnehmer tritt (gegenüber dem Betroffenen) nicht in eigenem Namen auf.

Liegen diese Kriterien vor, liegt auch keine Übermittlung von Daten vor. Kennt man die einschlägigen Merkmale, lässt sich durch juristische Ausgestaltung durchaus häufig eine Auftragsdatenverarbeitung „formen". Dazu sollte der Auftraggeber die Weisungen und Aufgaben des Auftragnehmers präzise in einer Vereinbarung zur Auftragsdatenverarbeitung definieren, in der mindestens die Punkte des Katalogs aus § 80 Sozialgesetzbuch Zehntes Buch (SGB X) geregelt sein müssen. Vorab müssten insbesondere die Voraussetzungen des § 80 Abs. 5 SGB X bei der Vergabe an nichtöffentliche Stellen beachtet werden (Störungen im Betriebsablauf, Kostenvergleich und Beibehaltung eines Datenbestandes). Wegen der datenschutzrechtlichen Verantwortung sollte der Auftraggeber ferner die vom Gesetz geforderte Überwachungs- und Kontrollpflicht gegenüber dem Auftragnehmer berücksichtigen. Im Berichtszeitraum habe ich hier viele Sozialbehörden beraten (beispielsweise in Bezug auf die Beauftragung von IT- und -Postdienstleistern sowie von Callcentern, siehe auch 26. Tätigkeitsbericht 2014 unter Nr. 8.1.9). Dabei hat sich gezeigt, dass nicht immer alle Anforderungen des § 80 SGB X erfüllt und hinreichend spezifiziert werden (siehe 25. Tätigkeitsbericht 2012 unter Nr. 2.1.6; 26. Tätigkeitsbericht 2014 unter Nr. 8.4.4).

Die sensiblen personenbezogenen Daten unterliegen aber nicht nur dem Sozialdatenschutz, sondern vielfach auch dem besonderen strafrechtlichen Schutz der Verletzung von Privatgeheimnissen (§ 203 Strafgesetzbuch). Allerdings ist eine Auftragsdatenverarbeitung keine Offenbarungsbefugnis im Sinne dieser Vorschrift. Hier ist an sich der Gesetzgeber gefragt (siehe Entschließung der 89. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 18./19. März 2016 in Wiesbaden: Nachbesserungen beim eHealth-Gesetz und klare Regelungen zum Einsatz externer Dienstleister bei Berufsgeheimnisträgern erforderlich, Text siehe Nr. 1.2.2). Notwendig ist daher derzeit in diesen Fällen an sich eine Schweigepflichtentbindungserklärung der Betroffenen. Der Dienstleister kann jedoch unter bestimmten Umständen als berufsmäßig tätiger Gehilfe angesehen werden. Gehilfe ist, wer einen Schweigepflichtigen in dessen beruflicher Funktion unterstützt. Rein vertraglich eingeräumte Steuerungs-, Weisungs- oder Kontrollbefugnisse des Auftraggebers sind dafür aber nicht ausreichend. Zum einen ist ein umfassendes Direktionsrecht erforderlich.

Zum anderen muss ein Gewahrsam des Auftraggebers hinsichtlich der schutzwürdigen Daten bestehen. Faktisch gehen also die Anforderungen im Fall einer Schweigepflicht über die Voraussetzungen einer „normalen" sozialdatenschutzrechtlichen Auftragsdatenverarbeitung hinaus; man könnte also von einer „Auftragsdatenverarbeitung plus" sprechen.

— Funktionsübertragung

Eine Funktionsübertragung hingegen liegt immer dann vor, wenn der Auftragnehmer „eigenverantwortlich" personenbezogene Daten verarbeitet (siehe 26. Tätigkeitsbericht 2014 unter Nr. 8.3). Einschlägig sind dabei folgende „Erkennungsmerkmale":

- Der Auftragnehmer ist frei von Weisungen dahingehend, was mit den Daten geschieht.
- Dem Auftragnehmer werden eigene Nutzungsrechte an den Daten eingeräumt.
- Der Auftragnehmer ist selbst für die Sicherstellung der Zulässigkeit und Richtigkeit der Daten verantwortlich und sichert auch eigenverantwortlich die Betroffenenrechte.
- Der Auftragnehmer tritt gegenüber dem Betroffenen – also dessen Daten verarbeitet werden, im eigenen Namen auf.
- Dem Auftragnehmer verbleibt eine Entscheidungsbefugnis in der Sache selbst.

Liegt eine Funktionsübertragung vor, werden personenbezogene Daten an den Dienstleister übermittelt. Zulässig ist dies grundsätzlich dann, wenn dies zur Aufgabenerfüllung erforderlich ist oder eine Einwilligung vorliegt.

8.3.10 Aufbewahrung von Sozialakten

Im Rahmen verschiedener Vor-Ort-Prüfungen habe ich festgestellt, dass bei der Aufbewahrung von Sozialdaten häufig nicht die datenschutzrechtlichen Bestimmungen eingehalten werden.

Zum Teil befanden sich die Akten unverschlossen in den Büroräumen. Vereinzelt blieben letztere auch nach Dienstschluss unverschlossen. In einem Fall steckten sogar durchgängig die Büroschlüssel außen an den Türen. Auch bei den „Archivräumen" musste ich Mängel feststellen. Diese sind in der Regel nicht verschlossen oder allen Beschäftigten zugänglich. Auch befanden sich teilweise (wohl zur Aussonderung vorgesehene) Akten unverschlossen in und auf Schränken, die entlang der Kellerflure standen. Begründet haben die Behörden diese Praxis häufig damit, dass die Bearbeiterinnen und Bearbeiter einander zu vertreten haben und daher auch Zugang zu den Akten haben müssten.

In der Regel dürfte es sich hier jedoch um Sozialdaten mit hohem Schutzbedarf handeln. Daher sind besondere technische und organisatorische Maßnahmen zu ergreifen (§ 78a Sozialgesetzbuch Zehntes Buch – SGB X). Diese gelten sowohl für die Büroräume als auch für die „Archivräume". Insbesondere sind die Daten vor

unbefugtem Zugriff zu schützen, also verschlossen aufzubewahren (siehe 18. Tätigkeitsbericht 1998 unter Nr. 19.3.13). Dies gilt insbesondere dann, wenn die Akten besonders sensible Daten (etwa Gesundheitsdaten) enthalten. Idealerweise sollten die Akten in verschließbaren Schränken gelagert werden. Dabei ist der Zugang zu beschränken, so dass nur ein kleiner Kreis von Beschäftigten, die sich auch tatsächlich vertreten, auf diese Akten zugreifen kann. Zudem sollte nachvollziehbar sein, wer welche Akten gerade bearbeitet. Nicht zulässig ist eine Konstellation, nach der jeder Bedienstete über den Schlüssel und damit über die Akten verfügen kann.

Diese Maßnahmen sind insbesondere zu beachten, wenn sich externe Personen in der Behörde aufhalten. Zum einen sind die jeweiligen Info-, Beratungs-, Besprechungs- und Wartebereiche nicht nur durchgängig mit einem geeigneten Sicht- und Schallschutz voneinander abzuschirmen. Vielmehr muss auch hier gewährleistet sein, dass keine Kenntnisnahme von Sozialdaten möglich ist. Zum anderen sind auch im Hinblick auf externe Reinigungsfirmen datenschutzrechtliche Vorgaben zu beachten (siehe 18. Tätigkeitsbericht 1998 unter Nr. 19.3.13). Unter Umständen liegt hier auch eine Erhebung, Verarbeitung und Nutzung von Daten vor. In diesem Fall wäre ein Vertrag zur Auftragsdatenverarbeitung notwendig (vgl. zu externen Wäschereidienstleistern 25. Tätigkeitsbericht 2012 unter Nr. 2.2.3; siehe auch Nr. 8.3.9). Selbiges gilt auch für die Einschaltung eines privaten Sicherheitsdienstes (siehe 26. Tätigkeitsbericht 2014 unter Nr. 3.6.1). Grundsätzlich sollte jedoch darauf geachtet werden, dass Externe keine Sozialdaten zur Kenntnis nehmen.

Angesichts dieser Vorgaben sollte jede Behörde ein Aufbewahrungskonzept entwickeln. Dieses sollte sich auch mit den Aufbewahrungsfristen für Unterlagen sowie deren Vernichtung auseinandersetzen. Schließlich sind Sozialdaten zu löschen, wenn ihre Kenntnis für die Behörde nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen der Betroffenen beeinträchtigt werden (§ 84 Abs. 2 SGB X). Dieses Konzept sollte auch die Anbietung dieser Unterlagen an ein Archiv berücksichtigen. Unter Umständen ist eine Übermittlung von Sozialdaten zulässig, soweit sie erforderlich ist für die Erfüllung der gesetzlichen Pflichten zur Sicherung und Nutzung von Archivgut (§ 71 Abs. 1 Satz 3 SGB X).

8.4 Jugendhilfe

8.4.1 Anmeldung für Kindertageseinrichtungen

Bereits in der Vergangenheit hatte ich mich mehrfach mit der Anmeldung für Kindertageseinrichtungen beschäftigt (17. Tätigkeitsbericht 1996 unter Nr. 4.8.1; 26. Tätigkeitsbericht 2014 unter Nr. 8.3.2). Im Berichtszeitraum hatte ich insbesondere mehrere zentrale Anmelde- und Informationssysteme für die Kinderbetreuung zu überprüfen. Dabei habe ich nachfolgende Auffassungen vertreten:

Bei noch nicht betreuten Kindern sind die Erhebungen, Verarbeitungen und Nutzungen von Daten zur Erfüllung der Aufgabe der Sicherstellung und Planung (siehe auch 22. Tätigkeitsbericht 2006 unter Nr. 14.6.1) beziehungsweise des Anspruchs auf Förderung in Tageseinrichtungen und in der Kindertagespflege grundsätzlich erforderlich und damit zulässig.

Für die Einführung und den Betrieb eines zentralen Anmelde- und Informationssystems für die Kinderbetreuung dürften personenbezogene Daten von aktuell betreuten Kindern nicht erforderlich sein. Für die Erhebung und Speicherung ist daher grundsätzlich eine Einwilligung der Betroffenen notwendig. Voraussetzung dafür ist jedoch insbesondere ein Hinweis, dass die betroffene Person die Einwilligung verweigern kann.

Ein Versand der Anmeldedaten per unverschlüsselter E-Mail ist aber nicht akzeptabel, da die Daten hierbei ungesichert über das Internet übertragen werden (siehe Nr. 8.3.7).

8.4.2 Erweitertes Führungszeugnis für Ehrenamtliche

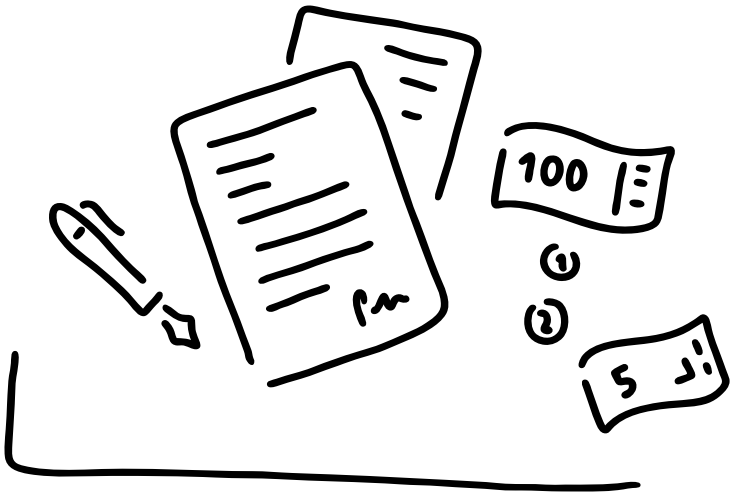
Meine Rechtsauffassung zur Vorlage eines erweiterten Führungszeugnisses durch Ehrenamtliche in der Jugendhilfe hatte ich schon in meinem 26. Tätigkeitsbericht 2014 unter Nr. 8.4.1 ausführlich dargelegt (siehe auch 25. Tätigkeitsbericht 2012 unter Nr. 8.8). Da jedoch § 72a Sozialgesetzbuch Achtes Buch (SGB VIII) erheblich in das Recht auf informationelle Selbstbestimmung eingreift, kann ich nachvollziehen, dass insbesondere Betroffene den vom Gesetzgeber vorgegebenen Weg kritisch sehen.

Inzwischen hat sich daher in der Praxis vielfach das so genannte „Regensburger Modell“ durchgesetzt. Danach beantragen ehrenamtlich Tätige beim Bundesamt der Justiz ein erweitertes Führungszeugnis. Das Zeugnis legen sie der Gemeinde vor. Diese bestätigt ihnen auf einem gesonderten Formular, dass im Führungszeugnis keine Straftaten im Sinne des § 72a SGB VIII eingetragen sind. Diese so genannte „Unbedenklichkeitsbescheinigung“ übergeben die Betroffenen dann dem Träger der Jugendhilfe. Manchmal übersendet auch das Bundesamt der Justiz das von der betroffenen Person beantragte Führungszeugnis direkt an die Gemeinde. Diese Modelle sollen sicherstellen, dass der Jugendhilfeträger keinen „überschießenden Einblick“ in das erweiterte Führungszeugnis erhält. Er soll dadurch keine Kenntnis von Eintragungen erhalten, die für das Beurteilen eines Tätigkeitsausschlusses nach § 72a SGB VIII nicht relevant sind.

Das „Regensburger Modell“ steht in einem gewissen Spannungsverhältnis zum Wortlaut des § 72a SGB VIII. Es berücksichtigt jedoch angemessen das Recht der Betroffenen auf informationelle Selbstbestimmung. Außerdem sind sie jederzeit „Herren des Verfahrens“. Daher erscheint mir das „Regensburger Modell“ derzeit ausnahmsweise hinnehmbar, sofern die dargestellten Vorgaben auch tatsächlich eingehalten werden.

Ich habe die Staatsministerien des Innern, für Bau und Verkehr sowie für Arbeit und Soziales, Familie und Integration gebeten, zeitnah auf eine entsprechende Gesetzesänderung auf Bundesebene hinzuwirken.

9 Steuer- und Finanzverwaltung



9.1 Datenschutzbeauftragte an allen bayerischen Finanzämtern

Mit der Vorschrift des Art. 25 Abs. 2 Satz 1 BayDSG hat der **bayerische Gesetzgeber alle bayerischen öffentlichen** – insbesondere staatlichen und kommunalen – **Stellen**, die personenbezogene Daten mit Hilfe von automatisierten Verfahren verarbeiten oder nutzen, gesetzlich **verpflichtet**, einen ihrer Beschäftigten zum **behördlichen Datenschutzbeauftragten zu bestellen**. Dennoch waren bei den rund 100 bayerischen Finanzämtern und Finanzamtsaußenstellen bisher keine eigenen behördlichen Datenschutzbeauftragten eingerichtet worden. Vielmehr hatte die bayerische Steuerverwaltung unter Berufung auf die Ausnahmevorschrift des Art. 25 Abs. 2 Satz 2 BayDSG für alle bayerischen Finanzbehörden lediglich einen gemeinsamen behördlichen Datenschutzbeauftragten beim Bayerischen Landesamt für Steuern bestellt.

9.1.1 Bisher: Gemeinsamer behördlicher Datenschutzbeauftragter der bayerischen Steuerverwaltung

Zwar ist es nach dem bloßen Wortlaut des Art. 25 Abs. 2 Satz 2 BayDSG zulässig, für mehrere bayerische staatliche Stellen – auch durch eine übergeordnete Behörde – einen **gemeinsamen behördlichen Datenschutzbeauftragten** zu bestellen. Allerdings ist diese Ausnahmevorschrift europarechtskonform eng auszulegen. So sieht die – bereits im Jahre 1995 erlassene – europarechtliche Vorgabe des Art. 18 Abs. 1 Richtlinie 95/46/EG (EG-Datenschutzrichtlinie) für automatisierte Datenverarbeitungsvorgänge eine Meldepflicht bei der Datenschutzkontrollstelle vor. Eine Ausnahme von dieser Meldepflicht ist nach Art. 18 Abs. 2 EG-Datenschutzrichtlinie im Wesentlichen nur dann zulässig, wenn durch die Einrichtung eines behördlichen Datenschutzbeauftragten vor Ort sichergestellt ist, dass „die Rechte und Freiheiten der betroffenen Personen durch die Verarbeitung nicht

beeinträchtigt werden." Voraussetzung für die damit geforderte effektive Datenschutzkontrolle vor Ort ist allerdings eine entsprechende personelle Ausstattung. Vor diesem Hintergrund wollte – und durfte – der bayerische Gesetzgeber mit der Einfügung der Ausnahmevorschrift des Art. 25 Abs. 2 Satz 2 BayDSG **lediglich** der Arbeitssituation **bei kleineren Behörden und bei Behörden mit wenigen personenbezogenen Daten** Rechnung tragen (vgl. auch den Standardkommentar Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Art. 25 BayDSG Rn. 21a). Eine solche Situation ist allerdings bei den bayerischen Finanzbehörden nicht gegeben: Mit **durchschnittlich deutlich über 100 Beschäftigten** erheben, verarbeiten und nutzen die **rund 100 bayerischen Finanzämter** und Außenstellen **in weitem Umfang** dem Steuergeheimnis gemäß § 30 Abgabenordnung unterfallende, überwiegend personenbezogene – und damit auch **datenschutzrechtlich** (oftmals sogar sehr) **sensible** – **Steuerdaten**.

So hat schon vor über 30 Jahren das Bundesverfassungsgericht in seinem Urteil vom 17. Juli 1984 (2 BvE 11, 15/83) sehr zutreffend formuliert:

„Die Angaben, die ein Steuerpflichtiger aufgrund des geltenden Abgabenrechts zu machen hat, ermöglichen weitreichende Einblicke in die persönlichen Verhältnisse, die persönliche Lebensführung (bis hin beispielsweise zu gesundheitlichen Gebrechen, religiösen Bindungen, Ehe- und Familienverhältnissen oder politischen Verbindungen) und in die beruflichen, betrieblichen, unternehmerischen oder sonstigen wirtschaftlichen Verhältnisse. Über ihre zeitlich kontinuierliche Erfassung, Speicherung und ständige Abrufbarkeit ermöglichen sie demjenigen, der über diese Daten verfügt, ein Wissen außerordentlichen Ausmaßes über die Betroffenen, das unter den gegenwärtigen Lebensverhältnissen in entsprechende Macht über die Betroffenen umschlagen kann."

Um den **verfassungsrechtlich gebotenen wirksamen Schutz der Steuerdaten** zu gewährleisten, sind **umfangreiche Maßnahmen auf mehreren Ebenen notwendig**:

— Zunächst hat der **Gesetzgeber** die grundlegenden gesetzlichen Schutznormen zu erlassen. Im Steuerbereich ist diesem Schutzauftrag der Bundesgesetzgeber durch Erlass insbesondere der Abgabenordnung und der Steuerdaten-Abrufverordnung nachgekommen; der bayerische Gesetzgeber hat ergänzend das Bayerische Datenschutzgesetz verabschiedet.

— Die **Steuerverwaltung** hat sodann die gesetzlichen Vorgaben in der Praxis wirksam umzusetzen. Dies kann etwa durch den Erlass konkretisierender Verwaltungsvorschriften geschehen. Vor allem sind aber die steuerlichen Informations- und Kommunikationssysteme datenschutzgerecht zu programmieren und zu sichern.

— Diese Umsetzung ist schließlich durch die steuerverwaltungsinternen technischen Systeme sowie durch die Vorgesetzten sicherzustellen und insbesondere von den **Datenschutzbeauftragten** zu kontrollieren.

Für einen wirksamen Schutz der Steuerdaten ist es deshalb **im Bereich der Steuerverwaltung insbesondere erforderlich**, dass

— die **Berechtigungen** der Finanzbeamtinnen und -beamten, in Ausübung ihrer Tätigkeit in den elektronischen Steuerbearbeitungsprogrammen **Steuerdaten der Bürgerinnen und Bürger abzurufen, sachgerecht begrenzt** werden,

— die getätigten elektronischen **Steuerdatenabrufe** zum Zwecke der Datenschutzkontrolle **protokolliert** werden und

— die **Zulässigkeit der elektronischen Steuerdatenzugriffe** durch Auswertung der Protokolldaten **zeitnah und angemessen überprüft** wird.

Vor diesem rechtlichen und tatsächlichen Hintergrund habe ich die **Bestellung nur eines gemeinsamen behördlichen Datenschutzbeauftragten** im gesamten Bereich der – etwa 20.000 Beschäftigte zählenden – bayerischen Steuerverwaltung **nie gut geheißen**.

9.1.2 Neu: Einrichtung von behördlichen Datenschutzbeauftragten an den Finanzbehörden vor Ort

Im Berichtszeitraum ist das Staatsministerium der Finanzen, für Landesentwicklung und Heimat meinen Argumenten endlich gefolgt.

In enger Abstimmung mit mir hat das **Finanzministerium** nunmehr wichtige Maßnahmen ergriffen, um den **Datenschutz gerade im Bereich der elektronischen Datenverarbeitung** bei der bayerischen Steuerverwaltung zu **verbessern**:

— So hat es die **Zugriffsberechtigungen** der Finanzbeamtinnen und -beamten auf die in den elektronischen Steuerbearbeitungsprogrammen gespeicherten Steuerdaten der Bürgerinnen und Bürger übergreifend neu und strenger geordnet. Die elektronischen Abrufberechtigungen wurden dabei insgesamt **restriktiver ausgestaltet und zurückhaltender vergeben.**

— Die Protokollierungen der elektronischen Steuerdatenabrufe hat das Finanzministerium zudem stark ausgeweitet. Nunmehr erfolgt eine **weitgehend umfassende Protokollierung** der elektronischen Zugriffe auf Steuerdaten.

— Um die Zulässigkeit der elektronischen Steuerdatenabrufe zeitnah und angemessen zu überprüfen, hat das Finanzministerium darüber hinaus eine **Zentrale Stelle beim Bayerischen Landesamt für Steuern eingerichtet**.

  Diese Zentrale Stelle **überprüft überregional die Zulässigkeit aller bayernweit protokollierten Steuerdatenabrufe und Steuerdatenabrufversuche in allen bayerischen Finanzbehörden**. Die Prüfung erfolgt systematisch nach bestimmten Kriterien, wie beispielsweise Abrufe zu ungewöhnlichen Zeiten oder in ungewöhnlicher Häufigkeit. Ergibt die automatisierte Überprüfung den Verdacht, dass ein bestimmter Steuerdatenabruf nicht mit den gesetzlichen Vorgaben im Einklang steht, findet eine individuelle Überprüfung statt. Diese erfolgt zunächst durch die Zentrale Stelle

selbst und gegebenenfalls sodann durch die Personalabteilung des Landesamts für Steuern.

Leiter der Zentralen Stelle ist der **behördliche Datenschutzbeauftragte des Bayerischen Landesamts für Steuern**.

– Schließlich hat das Finanzministerium ab dem 1. November 2014 **an allen rund 100 bayerischen Finanzämtern und Finanzamtsaußenstellen** jeweils **behördliche Datenschutzbeauftragte eingerichtet**.

In einer Verfügung hat das Landesamt für Steuern das **Aufgabengebiet der behördlichen Datenschutzbeauftragten an den Finanzämtern und Außenstellen** zutreffend wie folgt beschrieben:

- Selbstständige und eigenverantwortliche **Bearbeitung datenschutzrechtlicher Anfragen von Bürgerinnen und Bürgern**.

- **Ansprechperson für die Beschäftigten** der Finanzbehörde in Angelegenheiten des Datenschutzes gemäß Art. 25 Abs. 3 Satz 6 BayDSG.

- **Kontaktperson für den behördlichen Datenschutzbeauftragten des Landesamts für Steuern**, vor allem bei Vorgängen von überregionaler Bedeutung.

- **Stichprobenweise Überprüfung der elektronischen Steuerdatenabrufe innerhalb des Finanzamts**.

  Anfänglich bestand zwischen dem Finanzministerium und mir Uneinigkeit hinsichtlich der Frage, wie viele **verdachtsunabhängige Überprüfungen** von elektronischen Steuerdatenabrufen die behördlichen Datenschutzbeauftragten vor Ort zusätzlich zu den Überprüfungen der Zentralen Stelle (noch) durchführen müssen. Im Zuge einer langen und intensiven Diskussion konnte diese Meinungsverschiedenheit aber (jedenfalls vorerst) beseitigt werden. Die behördlichen Datenschutzbeauftragten vor Ort haben danach jeweils – gestaffelt nach der Größe der Finanzbehörden – **in 60 bis 120 Fällen pro Monat eine stichprobenweise Überprüfung von zufällig ausgewählten elektronischen Steuerdatenzugriffen** vorzunehmen.

- **Erteilung datenschutzrechtlicher Freigaben** nach Art. 26 BayDSG.

  Entsprechend ihrer gesetzlich in den Art. 25 ff. BayDSG festgelegten Aufgabenstellung sind die behördlichen Datenschutzbeauftragten **auch vor dem Einsatz** anderer, **nicht steuerlich relevanter automatisierter Verfahren, mit denen personenbezogene Daten verarbeitet werden**, in der jeweiligen Finanzbehörde zu beteiligen.

  Findet in einem Finanzamt beispielsweise eine **Videoaufzeichnung** statt, so hat der oder die behördliche Datenschutzbeauftragte nach Art. 21a Abs. 6 Satz 1 in Verbindung mit Art. 26 bis 28 BayDSG die

Videoaufzeichnungsanlage – auf Basis der ihm oder ihr vorzulegenden Unterlagen – datenschutzrechtlich zu prüfen und gegebenenfalls freizugeben.

— **Führung des Verfahrensverzeichnisses** gemäß Art. 27 BayDSG.

Schließlich haben die behördlichen Datenschutzbeauftragten nach Maßgabe des Art. 27 BayDSG ein Verzeichnis der bei der Finanzbehörde eingesetzten und datenschutzrechtlich freigegebenen automatisierten Verfahren, mit welchen personenbezogene Daten verarbeitet werden, zu führen.

9.1.3 Personalausstattung für Datenschutzaufgaben in der Steuerverwaltung

Die dargestellten Maßnahmen können sicherlich erhebliche Beiträge zu einer Verbesserung des Datenschutzes in der bayerischen Steuerverwaltung leisten. Der Grad und die Nachhaltigkeit dieser datenschutzrechtlichen Verbesserungen hängen in der Praxis allerdings maßgeblich von den personellen Kapazitäten ab, die an den Finanzämtern und Finanzamtsaußenstellen für Datenschutzaufgaben vorgesehen sind.

Mit der Vorschrift des Art. 25 Abs. 3 Satz 5 BayDSG hat der **bayerische Gesetzgeber** daher **alle bayerischen öffentlichen Stellen zu einer angemessen Freistellung der behördlichen Datenschutzbeauftragten** von der Erfüllung sonstiger dienstlicher Aufgaben **verpflichtet**. Die behördlichen Datenschutzbeauftragten – so der klare und ausdrückliche Gesetzeswortlaut – „**sind** im erforderlichen Umfang von der Erfüllung sonstiger dienstlicher Aufgaben freizustellen." Die Freistellung soll gewährleisten, dass die behördlichen Datenschutzbeauftragten alle ihre Datenschutzaufgaben auch tatsächlich und effektiv wahrnehmen können.

Lange Zeit hatten allerdings das **Staatsministerium der Finanzen, für Landesentwicklung und Heimat und das Bayerische Landesamt für Steuern** bei der Personal- und Stellenplanung in Bezug auf die behördlichen Datenschutzbeauftragten in der bayerischen Steuerverwaltung einen **äußerst restriktiven Ansatz** verfolgt. Aus meiner Sicht bestand daher zeitweise sogar die Gefahr, dass die dargestellten Datenschutzmaßnahmen zumindest teilweise unterlaufen worden wären. So wäre der rechnerische Zeitanteil, der den zu behördlichen Datenschutzbeauftragten bestellten Finanzamtsbediensteten – in der Regel den Hauptsachgebietsleitern Abgabenordnung – für die Erfüllung der Datenschutzaufgaben anfänglich zugemessen werden sollte, im Alltag wohl durch die Wahrnehmung der sonstigen dienstlichen Aufgaben aufgezehrt worden.

Erfreulicherweise konnte ich in einem intensiven Diskussionsprozess jedoch erreichen, dass als „Mitarbeiterkapazitäten" **für die Aufgaben des Datenschutzes in der bayerischen Steuerverwaltung** im Finanzministerium, am Landesamt für Steuern und an allen 76 bayerischen Finanzämtern und seinen 25 Außenstellen zusammen rechnerisch **nun (zunächst) immerhin 16 Vollzeitstellen** vorgesehen wurden. Diese „Mitarbeiterkapazitäten" wurden sodann bayernweit auf die Finanzbehörden – im Wesentlichen differenziert nach der Behördengröße – verteilt.

Auf Basis einer solchen (Anfangs-)Ausstattung bin ich **zuversichtlich**, dass die vereinbarten Verbesserungen des Datenschutzes in der bayerischen Steuerverwaltung nun auch in der Praxis Wirkung entfalten können.

9.1.4 Fazit

Die Zusammenschau der dargestellten Veränderungen zeigt, dass sich der mehrjährige, intensive und zum Teil auch schwierige Diskussionsprozess mit dem Staatsministerium der Finanzen, für Landesentwicklung und Heimat sowie dem Bayerischen Landesamt für Steuern gelohnt hat. Im Ergebnis konnte eine **längst überfällige Verbesserung der datenschutzrechtlichen Sicherungsmechanismen im gesamten Bereich der bayerischen Steuerverwaltung erreicht** werden.

Im Rahmen meiner datenschutzrechtlichen Beratungs- und Kontrolltätigkeit werde ich insbesondere die begonnene Implementierung der behördlichen Datenschutzbeauftragten an den bayerischen Finanzämtern und Finanzamtsaußenstellen **weiterhin konstruktiv begleiten**.

9.2 Bekanntgabe von Steuerbescheiden an Steuerpflichtige mit Wohnsitz in der Schweiz

Im Berichtszeitraum beschwerte sich ein Petent bei mir darüber, dass das für ihn zuständige bayerische Finanzamt seinen **Einkommensteuerbescheid durch Aushang im Dienstgebäude des Finanzamts öffentlich zugestellt** hatte. Der Eingabeführer hatte seinen Wohnsitz schon seit Jahren in der Schweiz, war in Deutschland aber – da er inländische Einkünfte im Sinne des § 49 Einkommensteuergesetz (EStG) erzielt hatte – gemäß § 1 Abs. 4 EStG beschränkt einkommensteuerpflichtig.

9.2.1 Sachverhalt

Dem Aushang des Einkommensteuerbescheides im Dienstgebäude des Finanzamts war folgender Sachverhalt vorausgegangen:

Das Finanzamt hatte dem Petenten mitgeteilt, dass er im Hinblick auf inländische Einkünfte in der Bundesrepublik Deutschland steuerpflichtig sei. Aus diesem Grund hatte das Finanzamt den Petenten aufgefordert, innerhalb einer vom Finanzamt gesetzten Frist einen Empfangsbevollmächtigten in der Bundesrepublik Deutschland zu benennen, der sämtliche vom Finanzamt übersandten Schriftstücke, insbesondere Steuerbescheide, für den Eingabeführer in Empfang nehmen sollte. Der Petent bestritt seine Steuerpflicht und ließ die Frist verstreichen, ohne dem Finanzamt einen inländischen Empfangsbevollmächtigten zu benennen.

Einige Monate später erhielt der Petent ein weiteres Schreiben des Finanzamts, in dem ihm mitgeteilt wurde, dass die öffentliche Zustellung seines Einkommensteuerbescheides „am heutigen Tag“ erfolge. Da – wie das Finanzamt ausführt – der Petent leider bisher keinen inländischen Empfangsbevollmächtigten benannt habe und die Bekanntgabe von Steuerbescheiden mit einfachem Brief in die Schweiz nicht zulässig sei, sei der Steuerbescheid nach § 10 Verwaltungszustellungsgesetz (VwZG) – durch Aushang im Dienstgebäude des Finanzamts – öffentlich zuzustellen. Dem Schreiben war eine Kopie des entsprechenden Steuerbescheides beigefügt.

Einen – warnenden – Hinweis, dass im Falle der Nicht-Benennung eines inländischen Empfangsbevollmächtigten eine öffentliche Zustellung des Einkommensteuerbescheides durch Aushang im Dienstgebäude des Finanzamts erfolge, hatte das Finanzamt dem Petenten zuvor nicht gegeben.

9.2.2 Rechtslage

In steuer- wie datenschutzrechtlicher Hinsicht gilt für die Bekanntgabe von Einkommensteuerbescheiden an Steuerpflichtige mit Wohnsitz in der Schweiz – wie im Übrigen auch in Liechtenstein – Folgendes:

Die Bekanntgabe von Steuerverwaltungsakten – dazu gehören vor allem auch Steuerbescheide – an **Empfänger im Ausland** richtet sich nach den gesetzlichen Vorgaben der §§ 122, 123 Abgabenordnung (AO) in Verbindung mit §§ 9, 10 VwZG. Nähere Bestimmungen trifft hierzu der Anwendungserlass zur Abgabenordnung (AEAO) zu § 122 AO.

Im Grundsatz ist ein Steuerverwaltungsakt nach § 122 Abs. 1 Satz 1 AO denjenigen Beteiligten bekannt zu geben, für die er bestimmt ist oder die von ihm betroffen sind.

Ein Beteiligter ohne Wohnsitz oder gewöhnlichen Aufenthalt, Sitz oder Geschäftsleitung im Inland hat allerdings gemäß § 123 Satz 1 AO der Finanzbehörde auf Verlangen innerhalb einer angemessenen Frist einen **Empfangsbevollmächtigten im Inland** zu benennen.

Gerade für die Bekanntgabe von Steuerbescheiden an **Empfänger in der Schweiz** (und auch in Liechtenstein) gelten jedoch einige **Besonderheiten**:

— So ist die Bekanntgabe von Steuerverwaltungsakten durch **einfachen Brief**, durch **Telefax** oder – unter den Voraussetzungen des § 87a AO – durch **elektronische Übermittlung** in die Schweiz nach den derzeit geltenden steuerrechtlichen Bestimmungen **nicht zulässig** (siehe Nr. 1.8.4 in Verbindung mit Nr. 3.1.4.1 Satz 4 AEAO zu § 122 AO).

— Auch kommt eine förmliche Zustellung von Steuerverwaltungsakten gemäß § 9 Abs. 1 VwZG in der Schweiz nicht in Betracht.

  So sind die Zustellung durch **Einschreiben mit Rückschein** (§ 9 Abs. 1 Nr. 1 VwZG) sowie die Zustellung durch **Übermittlung elektronischer Dokumente** in die Schweiz (§ 9 Abs. 1 Nr. 4 VwZG) **völkerrechtlich nicht zulässig** (siehe Nr. 3.1.4.1 AEAO zu § 122 AO).

  Zudem sind Zustellungen über **Schweizer Behörden** ebenso wie Zustellungen über die **zuständigen diplomatischen oder konsularischen Vertretungen** der Bundesrepublik Deutschland (§ 9 Abs. 1 Nr. 2 VwZG) in der Schweiz **nicht möglich**. Die Auslandsvertretungen dürfen Zustellungen in Fiskalsachen weder an eigene noch an fremde Staatsangehörige oder an Staatenlose bewirken (siehe Bayerisches Landesamt für Steuern, AO-Kartei, § 122 AO, Karte 2, Nr. 8).

Zustellungen über das **Auswärtige Amt** an Personen, die das Recht der Immunität genießen und zu einer Vertretung der Bundesrepublik Deutschland in der Schweiz gehören, sowie an deren Familienangehörige, wenn diese das Recht der Immunität genießen, (§ 9 Abs. 1 Nr. 3 VwZG) sind praktisch nicht von Relevanz.

– Da die Zustellung von Steuerverwaltungsakten gemäß § 9 Abs. 1 VwZG somit ausscheidet, müssen die Finanzämter bei Zustellungen an Empfänger in der Schweiz von der Möglichkeit der **öffentlichen Zustellung gemäß § 10 VwZG** Gebrauch machen, falls – wie hier – kein inländischer Empfangsbevollmächtigter benannt ist und auch nicht nach § 123 AO verfahren werden kann.

  In derartigen Fällen ist der **Empfänger** allerdings zunächst **nicht nur aufzufordern**, dem Finanzamt einen **inländischen Empfangsbevollmächtigten zu benennen, sondern auch** darauf **hinzuweisen, dass die öffentliche Zustellung erfolgen muss, wenn dieser Aufforderung nicht nachgekommen wird**.

  Erst wenn der Empfänger dieser Aufforderung innerhalb einer angemessenen Frist nicht Folge leistet, ist die öffentliche Zustellung nach § 10 VwZG vorzunehmen (siehe Bayerisches Landesamt für Steuern, AO-Kartei, § 122 AO, Karte 2, Nrn. 7 und 8).

AO-Kartei, § 122 AO, Karte 2, Nr. 7 Öffentliche Zustellung
Nur wenn ein Schriftstück nicht auf andere Weise zugestellt oder bekannt gegeben werden kann – auch nicht durch Zustellung nach § 9 Abs. 1 Nr. 2 VwZG, vgl. z.B. Tz 8 zur Schweiz und zu Liechtenstein – ist eine öffentliche Zustellung nach § 10 Abs. 1 Nr. 2 VwZG vorzunehmen. In derartigen Fällen ist der Empfänger zunächst aufzufordern, dem Finanzamt einen inländischen Empfangsbevollmächtigten zu benennen (vgl. Tz 6) und darauf hinzuweisen, dass die öffentliche Zustellung erfolgen muss, wenn dieser Aufforderung nicht nachgekommen wird. Erst wenn der Empfänger dieser Aufforderung innerhalb einer angemessenen Frist nicht Folge leistet, ist die öffentliche Zustellung nach § 10 VwZG vorzunehmen. Dem Empfänger ist durch einfachen Brief die öffentliche Zustellung sowie der Tag der Zustellung mitzuteilen und eine Kopie des Verwaltungsakts zu übersenden. Es ist zweckmäßig, den Brief bereits abzusenden, wenn die Benachrichtigung nach § 10 Abs. 2 VwZG durch Aushang bekannt gemacht wird.

– Nach § 10 Abs. 2 Satz 1 VwZG erfolgt die öffentliche Zustellung durch **Bekanntmachung einer Benachrichtigung an der Stelle, die von der Behörde hierfür allgemein bestimmt ist** – also wie hier etwa an einer Aushangtafel im Dienstgebäude des Finanzamts –, oder durch Veröffentlichung einer Benachrichtigung im Bundesanzeiger.

  Aus datenschutzrechtlicher Sicht mache ich in diesem Zusammenhang auf folgende Bestimmung besonders aufmerksam:

  Im Hinblick auf die öffentliche Zustellung von Steuerbescheiden ist in Nr. 3.1.5.4 Satz 1 AEAO zu § 122 AO ausdrücklich vorgegeben, dass **nicht der Inhalt – auch nicht der verfügende Teil – des zuzustellenden Verwaltungsakts öffentlich bekannt zu geben** ist, **sondern lediglich eine Benachrichtigung mit weitgehend neutralem Inhalt**. Dies bedeutet also,

dass insbesondere weder die Art der erzielten Einkünfte noch die Höhe einer etwaigen Steuerschuld oder eines eventuellen Steuerguthabens veröffentlicht werden. Diese Vorgabe ist aus Datenschutzsicht nachdrücklich zu begrüßen.

Nr. 3.1.5.4 AEAO zu § 122 AO Öffentliche Zustellung (§ 10 VwZG)
Zur Durchführung der öffentlichen Zustellung ist nicht der Inhalt (auch nicht der verfügende Teil) des zuzustellenden Verwaltungsakts öffentlich bekannt zu geben, sondern lediglich eine Benachrichtigung mit weitgehend neutralem Inhalt (§ 10 Abs. 2 VwZG). Die Benachrichtigung muss die Behörde, für die zugestellt wird, den Namen und die letzte bekannte Anschrift des Zustellungsempfängers, das Datum und das Aktenzeichen des Dokuments sowie die Stelle, wo das Dokument eingesehen werden kann, erkennen lassen (§ 10 Abs. 2 Satz 2 VwZG). Für das in der Benachrichtigung anzugebende Aktenzeichen des zuzustellenden Dokuments (§ 10 Abs. 2 Satz 2 Nr. 3 VwZG) gelten die Ausführungen in Nr. 3.1.1.1 des AEAO zu § 122 entsprechend. Die Benachrichtigung muss ferner den Hinweis enthalten, dass das Dokument öffentlich zugestellt wird und Fristen in Lauf gesetzt werden können, nach deren Ablauf Rechtsverluste eintreten können (§ 10 Abs. 2 Satz 3 VwZG). … Die Benachrichtigung ist an der Stelle bekannt zu machen, die von der Behörde hierfür allgemein bestimmt ist (z.B. durch Aushang im Dienstgebäude). Alternativ hierzu kann die Benachrichtigung auch durch Veröffentlichung im Bundesanzeiger bekannt gemacht werden (§ 10 Abs. 2 Satz 1 VwZG). In den Akten ist zu vermerken, wann und in welcher Weise die Benachrichtigung bekannt gemacht wurde (§ 10 Abs. 2 Satz 5 VwZG).
Wird die Benachrichtigung über die öffentliche Zustellung durch Aushang bekannt gemacht, ist sie stets bis zu dem Zeitpunkt auszuhängen, zu dem die Zustellung nach § 10 Abs. 2 Satz 6 VwZG als bewirkt anzusehen ist. Das gilt auch dann, wenn der Empfänger vor Fristablauf bei der Finanzbehörde erscheint und ihm das zuzustellende Schriftstück ausgehändigt wird (vgl. AEAO zu § 122, Nr. 3.1.5.5). Die Aushändigung ist in den Akten zu vermerken.

9.2.3 Bewertung des Sachverhalts

Nachdem der Petent dem Finanzamt gegenüber keinen inländischen Empfangsbevollmächtigten benannt hatte, hatte das Finanzamt somit nach der Rechtslage eine öffentliche Zustellung des Einkommensteuerbescheides vorzunehmen. Allerdings hat es das Finanzamt versäumt, den Eingabeführer auf diese Auswirkung (rechtzeitig) hinzuweisen.

Der **Hinweis auf die öffentliche Zustellung dient** der Warnung, vor allem aber dem **Schutz des allgemeinen Persönlichkeitsrechts der Betroffenen**. Sie müssen wissen, welche Folgen sich aus der nicht fristgemäßen Benennung eines inländischen Empfangsbevollmächtigten ergeben. Die Steuerpflichtigen sollen die Gelegenheit haben, durch die Benennung eines inländischen Empfangsbevollmächtigten eine öffentliche Zustellung der sie betreffenden Steuerverwaltungsakte – und damit eine mögliche Bloßstellung oder befürchtete Rufschädigung – abzuwenden.

9.2.4 Anpassung des Musterformulars

Auf Nachfrage teilte mir das betreffende Finanzamt mit, dass **für die Aufforderung zur Benennung eines inländischen Empfangsbevollmächtigten ein Musterformular verwendet** wird, das das **Bayerische Landesamt für Steuern** allen bayerischen Finanzämtern landesweit zur Verfügung stellt. Einen Hinweis, dass an Empfänger mit Wohnsitz in der Schweiz und in Liechtenstein gerichtete Steuerverwaltungsakte öffentlich zuzustellen sind, wenn ein inländischer Empfangsbevollmächtigter nicht (rechtzeitig) benannt wird, enthält dieses Musterformular allerdings nicht.

Ich habe mich deswegen an das Bayerische Landesamt für Steuern gewandt und **vorgeschlagen**, für Steuerpflichtige mit Wohnsitz in der Schweiz und in Liechtenstein **in das Musterformular** den **Hinweis aufzunehmen**, dass im Falle nicht fristgemäßer Benennung eines inländischen Empfangsbevollmächtigten eine **öffentliche Zustellung** durch das Finanzamt erfolgen muss.

Nach eingehender Prüfung hat das **Bayerische Landesamt für Steuern meinen Vorschlag leider nicht vollständig umgesetzt**. Es hat in einer ausführlichen Stellungnahme insbesondere auf den **Sinn und Zweck des Musterformulars** hingewiesen, möglichst viele, aber nicht jeden einzelnen der in Frage kommenden Fälle abzudecken. Aus diesem Grund bilde das Musterformular allein den gesetzlich in § 123 AO normierten **Regelfall** der Benennung eines inländischen Empfangsbevollmächtigten ab. Schließlich hat das Bayerische Landesamt für Steuern darauf aufmerksam gemacht, dass es sich bei dem gegenständlichen Musterformular um einen **bundeseinheitlich abgestimmten und verwendeten Vordruck** handelt.

Allerdings hat mir das **Bayerische Landesamt für Steuern** versichert, die an den bayerischen Finanzämtern neu bestellten **behördlichen Datenschutzbeauftragten** (siehe Nr. 9.1) im Rahmen der datenschutzrechtlichen Schulungen **für die vorliegende Problematik – als Multiplikatoren – besonders sensibilisiert** zu haben. In diesem Zusammenhang hat das Landesamt die Multiplikatoren ausdrücklich darauf hingewiesen, dass das Musterformular – gemäß seiner Zweckbestimmung – „nur" für den Regelfall, aber nicht durchgängig und unverändert verwendet werden darf. Das Landesamt hat daher gegenüber den behördlichen Datenschutzbeauftragten **deutlich gemacht**, dass die **Finanzamtsbediensteten bei Zustellungen an Empfänger in der Schweiz und in Liechtenstein den rechtlich notwendigen Hinweis**, dass im Falle nicht fristgemäßer Benennung eines inländischen Empfangsbevollmächtigten eine **öffentliche Zustellung** durch das Finanzamt erfolgen muss, **in das (Word-)Formular manuell einzutragen haben**.

Die aufgezeigte Problematik werde ich weiterhin im Auge behalten.

9.3 Steuerrechtliche Anforderungen an Restaurantrechnungen

Ein Familienvater berichtete mir, dass er seine Familie zur Feier seines Geburtstags in ein Restaurant zum Essen eingeladen habe. Als er habe zahlen wollen, habe ihn die Bedienung gebeten, auf einem formellen Rechnungsbeleg seinen Namen und seine Adresse anzugeben. Dies sei ab einem Rechnungsbetrag von 150 Euro eine vom Finanzamt auferlegte Verpflichtung. Eine weitere Restaurantangestellte habe ihm ausdrücklich versichert, dass das Finanzamt diese Anforderung stelle.

Da dem Gastgeber an den folgenden Tagen hieran immer stärkere Zweifel kamen, wandte er sich schließlich an mich und erkundigte sich bei mir, ob er tatsächlich bei einem einfachen Essen mit seiner Familie in einem Restaurant seinen Namen und seine Adresse angeben müsse oder ob ein derartiges Vorgehen der Finanzbehörden nicht „dem Datenschutz" widerspreche.

Zu der **Frage, ob Kundinnen und Kunden eines Restaurants auf der Rechnung über verzehrte Speisen und Getränke ihren Namen und ihre Adresse angeben müssen**, konnte ich dem Familienvater aus steuerdatenschutzrechtlicher Sicht Folgendes mitteilen:

– Soweit Restaurantrechnungen gegenüber dem Finanzamt als Nachweis für entstandene Bewirtungsaufwendungen – mit dem Ziel der steuerlichen Absetzbarkeit – dienen sollen, müssen sie aufgrund steuerrechtlicher Vorgaben bestimmte Pflichtangaben enthalten.

  Nach § 4 Abs. 5 Satz 1 Nr. 2 Einkommensteuergesetz (EStG) dürfen Aufwendungen für die Bewirtung von Personen **aus geschäftlichem Anlass**, soweit sie 70 Prozent der Aufwendungen übersteigen, die nach der allgemeinen Verkehrsauffassung als angemessen anzusehen und deren **Höhe und betriebliche Veranlassung** nachgewiesen sind, den Gewinn nicht mindern.

  Welche Anforderungen im Einzelnen an diesen Nachweis zu stellen sind, ergibt sich – grundlegend – aus § 4 Abs. 5 Satz 1 Nr. 2 Sätze 2 und 3 EStG sowie – im Detail – aus R 4.10 (5-9) „Geschenke, Bewirtung, andere die Lebensführung berührende Betriebsausgaben" der Einkommensteuer-Richtlinien 2012 (EStR 2012). Nach R 4.10 (8) Sätze 1 bis 3 EStR 2012 genügen bei Bewirtung in einer Gaststätte neben der beizufügenden Rechnung – mit Angaben zu Name und Anschrift der Gaststätte, zum Tag der Bewirtung und zur Höhe der Aufwendungen – Angaben zu dem Anlass und den Teilnehmern der Bewirtung.

  Erhöhte Nachweispflichten bestehen hingegen, wenn der Gesamtbetrag der **Rechnung 150 Euro übersteigt**; in diesem Fall muss die Rechnung auch den Namen der bewirtenden steuerpflichtigen Person enthalten (siehe R 4.10 (8) Satz 4 EStR 2012).

R 4.10 (5-9) EStR 2012 Geschenke, Bewirtung, andere die Lebensführung berührende Betriebsausgaben
Nachweis
(8) [1]Der Nachweis der Höhe und der betrieblichen Veranlassung der Aufwendungen durch schriftliche Angaben zu Ort, Tag, Teilnehmer und Anlass der Bewirtung sowie Höhe der Aufwendungen ist gesetzliches Tatbestandsmerkmal für den Abzug der Bewirtungsaufwendungen als Betriebsausgaben. [2]Bei Bewirtung in einer Gaststätte genügen neben der beizufügenden Rechnung Angaben zu dem Anlass und den Teilnehmern der Bewirtung; auch hierbei handelt es sich um ein gesetzliches Tatbestandsmerkmal für den Abzug der Bewirtungsaufwendungen als Betriebsausgaben. [3]Aus der Rechnung müssen sich Name und Anschrift der Gaststätte sowie der Tag der Bewirtung ergeben. [4]Die Rechnung muss auch den Namen des bewirtenden Stpfl. enthalten; dies gilt nicht, wenn der Gesamtbetrag der Rechnung 150 Euro nicht übersteigt. [5]Die schriftlichen Angaben können auf der Rechnung oder getrennt gemacht werden. [6]Erfolgen die Angaben getrennt von der Rechnung, müssen das Schriftstück über die Angaben und die Rechnung

grundsätzlich zusammengefügt werden. [7]Ausnahmsweise genügt es, den Zusammenhang dadurch darzustellen, dass auf der Rechnung und dem Schriftstück über die Angaben Gegenseitigkeitshinweise angebracht werden, so dass Rechnung und Schriftstück jederzeit zusammengefügt werden können. [8]Die Rechnung muss den Anforderungen des § 14 UStG genügen und maschinell erstellt und registriert sein. [9]Die in Anspruch genommenen Leistungen sind nach Art, Umfang, Entgelt und Tag der Bewirtung in der Rechnung gesondert zu bezeichnen; die für den Vorsteuerabzug ausreichende Angabe „Speisen und Getränke" und die Angabe der für die Bewirtung in Rechnung gestellten Gesamtsumme sind für den Betriebsausgabenabzug nicht ausreichend.

Ferner muss eine Rechnung, deren Gesamtbetrag 150 Euro übersteigt, den strengen Anforderungen des § 14 Umsatzsteuergesetz (UStG) genügen (siehe R 4.10 (8) Satz 8 EStR 2012). Unter anderem muss nach § 14 Abs. 4 Satz 1 Nr. 1 UStG eine solche **Rechnung den vollständigen Namen und die vollständige Anschrift des leistenden Unternehmers** – hier also des Restaurants – **sowie des Leistungsempfängers** – hier also des Gastgebers – **enthalten**.

Die umsatzsteuerrechtliche Vereinfachungsregelung des § 14 Abs. 6 Nr. 3 UStG in Verbindung mit § 33 Umsatzsteuer-Durchführungsverordnung (UStDV), nach der auf die Angabe des vollständigen Namens und der vollständigen Anschrift des Leistungsempfängers verzichtet werden kann, gilt dagegen nur für „Rechnungen über Kleinbeträge", also – so der Wortlaut des § 33 UStDV – für Rechnungen, deren Gesamtbetrag 150 Euro nicht übersteigt.

§ 33 UStDV Rechnungen über Kleinbeträge
[1]Eine Rechnung, deren Gesamtbetrag 150 Euro nicht übersteigt, muss mindestens folgende Angaben enthalten:
1. *den vollständigen Namen und die vollständige Anschrift des leistenden Unternehmers,*
2. *das Ausstellungsdatum,*
3. *die Menge und die Art der gelieferten Gegenstände oder den Umfang und die Art der sonstigen Leistung und*
4. *das Entgelt und den darauf entfallenden Steuerbetrag für die Lieferung oder sonstige Leistung in einer Summe sowie den anzuwendenden Steuersatz oder im Fall einer Steuerbefreiung einen Hinweis darauf, dass für die Lieferung oder sonstige Leistung eine Steuerbefreiung gilt.*

[2]Die §§ 31 und 32 sind entsprechend anzuwenden. [3]Die Sätze 1 und 2 gelten nicht für Rechnungen über Leistungen im Sinne der §§ 3c, 6a und 13b des Gesetzes.

– Wenn ein Familienvater seine Familie anlässlich seines Geburtstags zum Essen in ein Restaurant einlädt, liegt allerdings kein geschäftlicher, sondern vielmehr ein **privater Anlass** vor.

  In einem solchen Fall sind die Vorschrift des § 4 Abs. 5 Satz 1 Nr. 2 EStG und die ergänzenden Regelungen der R 4.10 (5-9) „Bewirtung und Bewirtungsaufwendungen" EStR 2012 von vornherein nicht anwendbar.

  Bei den **Aufwendungen für die Familienfeier in einem Restaurant** handelt es sich daher nicht um Betriebsausgaben im Sinne von § 4 Abs. 4 EStG – also um Aufwendungen, die durch den Betrieb veranlasst sind –, sondern

um **rein privat veranlasste Aufwendungen**. Derartige privat veranlasste Aufwendungen sind allerdings steuerlich nicht absetzbar.

Eine (steuer)rechtliche Pflicht zur Angabe von Namen und Adresse auf der Rechnung ist in einem solchen Fall nicht ersichtlich.

Im Übrigen habe ich den Familienvater ausdrücklich darauf aufmerksam gemacht, dass es – generell – **allein der Entscheidung und der Verantwortung des Steuerpflichtigen selbst vorbehalten** bleibt, ob und gegebenenfalls inwieweit er gesetzlich zulässige **Steuervergünstigungen im Rahmen seiner Einkommensteuererklärung in Anspruch nehmen** will.

Daher kann – auch und gerade bei der steuerlich allein berücksichtigungsfähigen Bewirtung von Personen aus geschäftlichem Anlass – die Angabe von Kundennamen und -adresse auf Restaurantrechnungen **vom Restaurantbetreiber ohnehin nicht verlangt werden**.

9.4 ELSTER beim Betrieb von Photovoltaikanlagen durch Privatleute

Aus Umweltschutzgründen, aber oftmals auch mitveranlasst durch staatliche und kommunale Fördermaßnahmen, haben in den vergangenen Jahren zahlreiche bayerische Bürgerinnen und Bürger vor allem auf den Dächern ihrer Einfamilienhäuser Photovoltaikanlagen installieren lassen. Den **mittels der Photovoltaikanlagen erzeugten, nicht selbst verbrauchten Strom** haben sie sodann **zu gesetzlich garantierten festen Einspeisevergütungen ins Stromnetz eingespeist**.

Einkommensteuerrechtlich erzielen Privatleute mit dem Betrieb einer Photovoltaikanlage **Einkünfte aus Gewerbebetrieb** im Sinne des § 2 Abs. 1 Satz 1 Nr. 2 in Verbindung mit § 15 Abs. 1 Satz 1 Nr. 1 Einkommensteuergesetz (EStG). **Umsatzsteuerrechtlich** gilt dagegen bei einem Jahresumsatz bis 17.500 Euro die **„Kleinunternehmerregelung"** gemäß § 19 Abs. 1 Umsatzsteuergesetz (UStG), so dass in diesem Fall keine Umsatzsteuer entrichtet werden muss. Allerdings können die Betreiber einer Photovoltaikanlage nach § 19 Abs. 2 UStG auf diese Regelung verzichten und dadurch auch die Vorsteuer auf alle mit der Installation der Photovoltaikanlage verbundenen Investitionen erstattet bekommen. Aufgrund des **hohen Freibetrags** von 24.500 Euro unterliegen private Photovoltaikanlagen in der Regel nicht der **Gewerbesteuer** (siehe § 11 Abs. 1 Satz 3 Nr. 1 Gewerbesteuergesetz).

Im Berichtszeitraum haben sich nun mehrere private Betreiberinnen und Betreiber von Photovoltaikanlagen – vorwiegend ältere Bürgerinnen und Bürger – bei mir darüber beschwert, dass sie **vom Finanzamt dazu aufgefordert** worden seien, ihre **Umsatz- und Einkommensteuererklärungen** (vgl. §§ 149 ff. Abgabenordnung – AO) **künftig ausschließlich mittels des Verfahrens ELSTER** (Elektronische Steuererklärung) **beim Finanzamt abzugeben**, also elektronisch über das Internet an das Finanzamt zu übermitteln. Einige Betroffene brachten dabei vor, dass sie schon nicht über die dafür notwendige gerätetechnische Ausstattung, geschweige denn über einen Internetanschluss verfügten. Alle Bürgerinnen und Bürger wollten freilich von mir wissen, ob und inwieweit die im Zusammenhang mit dem Betrieb von Photovoltaikanlagen anfallenden Steuererklärungen tatsächlich nur noch elektronisch abgegeben werden könnten. Schließlich warfen die Betroffenen auch die Frage auf, ob das Finanzamt sie wirklich – faktisch – dazu zwingen könne, nicht nur die für die elektronische Abgabe der Steuererklärungen

notwendigen, kostspieligen informationstechnischen Gerätschaften einschließlich eines eigenen Internetanschlusses anzuschaffen, sondern sich auch (mühsam) die zur Bedienung nötigen Kenntnisse und Fertigkeiten anzueignen.

Die betroffenen Bürgerinnen und Bürger konnte ich im Wesentlichen beruhigen. Aus datenschutzrechtlicher Sicht ist im Hinblick auf den privaten Betrieb einer Photovoltaikanlage allerdings genau **zwischen der Abgabe der Umsatzsteuererklärung und der Abgabe der Einkommensteuererklärung zu differenzieren**:

9.4.1 Abgabe der Umsatzsteuererklärung

Mit der gesetzlichen Regelung des § 18 UStG hat der Bundesgesetzgeber die **Steuerpflichtigen im Bereich der Umsatzsteuer grundsätzlich zur elektronischen Kommunikation mit dem Finanzamt verpflichtet**.

§ 18 UStG Besteuerungsverfahren
(3) [1]Der Unternehmer hat für das Kalenderjahr oder für den kürzeren Besteuerungszeitraum eine Steuererklärung nach amtlich vorgeschriebenem Datensatz durch Datenfernübertragung nach Maßgabe der Steuerdaten-Übermittlungsverordnung zu übermitteln, in der er die zu entrichtende Steuer oder den Überschuss, der sich zu seinen Gunsten ergibt, nach § 16 Absatz 1 bis 4 und § 17 selbst zu berechnen hat (Steueranmeldung). [2]In den Fällen des § 16 Absatz 3 und 4 ist die Steueranmeldung binnen einem Monat nach Ablauf des kürzeren Besteuerungszeitraums zu übermitteln. [3]Auf Antrag kann das Finanzamt zur Vermeidung von unbilligen Härten auf eine elektronische Übermittlung verzichten; in diesem Fall hat der Unternehmer eine Steueranmeldung nach amtlich vorgeschriebenem Vordruck abzugeben und eigenhändig zu unterschreiben.

So hat der Unternehmer gemäß § 18 Abs. 3 Satz 1 UStG für das Kalenderjahr eine **Steuererklärung** nach amtlich vorgeschriebenem Datensatz durch Datenfernübertragung – also **elektronisch** – nach Maßgabe der Steuerdaten-Übermittlungsverordnung **an das Finanzamt zu übermitteln**, in der er die zu entrichtende Steuer oder den Überschuss, der sich zu seinen Gunsten ergibt, nach § 16 Abs. 1 bis 4 und § 17 UStG selbst zu berechnen hat (Steueranmeldung).

Darauf hinzuweisen ist allerdings, dass das Finanzamt nach der **Ausnahmeregelung** des § 18 Abs. 3 Satz 3 UStG auf Antrag zur Vermeidung von unbilligen Härten auf eine elektronische Übermittlung verzichten kann; in diesem Fall hat der Unternehmer eine Steueranmeldung nach amtlich vorgeschriebenem Vordruck abzugeben und eigenhändig zu unterschreiben.

In diesem Zusammenhang ist die allgemeine steuerverfahrensrechtliche Vorschrift des § 150 Abs. 8 Satz 1 AO zu beachten: Danach ist einem solchen Antrag zu entsprechen, wenn eine Erklärungsabgabe nach amtlich vorgeschriebenem Datensatz durch Datenfernübertragung für den Steuerpflichtigen **wirtschaftlich oder persönlich unzumutbar** ist. Nach § 150 Abs. 8 Satz 2 AO ist dies insbesondere der Fall, wenn die Schaffung der technischen Möglichkeiten für eine Datenfernübertragung des amtlich vorgeschriebenen Datensatzes nur mit einem **nicht unerheblichen finanziellen Aufwand** möglich wäre oder wenn der Steuerpflichtige **nach seinen individuellen Kenntnissen und Fähigkeiten nicht oder nur eingeschränkt in der Lage** ist, die Möglichkeiten der Datenfernübertragung zu nutzen. In der Praxis dürften diese Voraussetzungen vor allem bei **Kleinstbetrie-**

ben gegeben sein (siehe Bundestags-Drucksache 16/10940, Seite 13). Die Aufzählung in § 150 Abs. 8 Satz 2 AO ist nicht abschließend („insbesondere"), so dass das Finanzamt im Einzelfall auch aus anderen Gründen auf eine elektronische Übermittlung der Steuererklärung verzichten kann.

§ 150 AO Form und Inhalt der Steuererklärungen
(8) [1]Ordnen die Steuergesetze an, dass die Finanzbehörde auf Antrag zur Vermeidung unbilliger Härten auf eine Übermittlung der Steuererklärung nach amtlich vorgeschriebenem Datensatz durch Datenfernübertragung verzichten kann, ist einem solchen Antrag zu entsprechen, wenn eine Erklärungsabgabe nach amtlich vorgeschriebenem Datensatz durch Datenfernübertragung für den Steuerpflichtigen wirtschaftlich oder persönlich unzumutbar ist. [2]Dies ist insbesondere der Fall, wenn die Schaffung der technischen Möglichkeiten für eine Datenfernübertragung des amtlich vorgeschriebenen Datensatzes nur mit einem nicht unerheblichen finanziellen Aufwand möglich wäre oder wenn der Steuerpflichtige nach seinen individuellen Kenntnissen und Fähigkeiten nicht oder nur eingeschränkt in der Lage ist, die Möglichkeiten der Datenfernübertragung zu nutzen.

Gerade Steuerpflichtige, die über keine entsprechende informationstechnische Ausstattung verfügen oder im Umgang mit der Informations- und Kommunikationstechnik nicht geübt sind, können beim Finanzamt gemäß § 18 Abs. 3 Satz 3 UStG in Verbindung mit § 150 Abs. 8 AO **beantragen**, zur Vermeidung unbilliger Härten auf eine elektronische Übermittlung der Steuererklärung zu verzichten. Andernfalls sind sie gemäß § 18 Abs. 3 Satz 1 UStG dazu verpflichtet, ihre Umsatzsteuererklärung elektronisch an das Finanzamt zu übermitteln.

9.4.2 Abgabe der Einkommensteuererklärung

Anders als im Bereich der Umsatzsteuer hat der Bundesgesetzgeber im Bereich der Einkommensteuer die Steuerpflichtigen überwiegend nicht zur elektronischen Kommunikation mit dem Finanzamt verpflichtet. Jedoch ist die **Einkommensteuererklärung** gemäß § 25 Abs. 4 Satz 1 EStG dann nach amtlich vorgeschriebenem Datensatz durch Datenfernübertragung – also **elektronisch** – **an das Finanzamt zu übermitteln**, wenn Einkünfte nach § 2 Abs. 1 Satz 1 Nrn. 1 bis 3 EStG erzielt werden und es sich nicht um einen der Veranlagungsfälle gemäß § 46 Abs. 2 Nrn. 2 bis 8 EStG handelt.

§ 25 EStG Veranlagungszeitraum, Steuererklärungspflicht
(3) [1]Die steuerpflichtige Person hat für den Veranlagungszeitraum eine eigenhändig unterschriebene Einkommensteuererklärung abzugeben. [2]Wählen Ehegatten die Zusammenveranlagung (§ 26b), haben sie eine gemeinsame Steuererklärung abzugeben, die von beiden eigenhändig zu unterschreiben ist.
(4) [1]Die Erklärung nach Absatz 3 ist nach amtlich vorgeschriebenem Datensatz durch Datenfernübertragung zu übermitteln, wenn Einkünfte nach § 2 Absatz 1 Satz 1 Nummer 1 bis 3 erzielt werden und es sich nicht um einen der Veranlagungsfälle gemäß § 46 Absatz 2 Nummer 2 bis 8 handelt. [2]Auf Antrag kann die Finanzbehörde zur Vermeidung unbilliger Härten auf eine Übermittlung durch Datenfernübertragung verzichten.

Einkünfte nach § 2 Abs. 1 Satz 1 Nrn. 1 bis 3 EStG sind

— Einkünfte aus Land- und Forstwirtschaft,

— Einkünfte aus Gewerbebetrieb und

— Einkünfte aus selbständiger Arbeit.

Diese Einkünfte werden steuerrechtlich als **„Gewinneinkünfte"** bezeichnet (vgl. § 2 Abs. 2 Satz 1 Nr. 1 EStG). Bei den Veranlagungsfällen gemäß § 46 Abs. 2 Nrn. 2 bis 8 EStG handelt es sich im Wesentlichen um „Kleinfälle".

Die Pflicht zur elektronischen Übermittlung der Steuererklärung für die genannten Gewinneinkünfte greift danach – verkürzt und vereinfachend gesagt – **nur dann nicht, wenn die Einkünfte** aus den genannten Gewinneinkunftsarten – wie hier etwa aus Gewerbebetrieb – jährlich den **Betrag von 410 Euro nicht übersteigen und neben diesen Gewinneinkünften Einkünfte aus nichtselbständiger Arbeit** mit Steuerabzug erzielt werden. Zu den Einkünften aus nichtselbständiger Arbeit im Sinne des § 2 Abs. 1 Satz 1 Nr. 4 in Verbindung mit § 19 EStG gehören insbesondere Gehälter und Löhne für eine Beschäftigung im öffentlichen oder privaten Dienst (§ 19 Abs. 1 Satz 1 Nr. 1 EStG) sowie Beamtenpensionen (§ 19 Abs. 1 Satz 1 Nr. 2, Abs. 2 EStG). Steuerrechtlich handelt es sich bei diesen Einkünften um **„Überschusseinkünfte"** (vgl. § 2 Abs. 2 Satz 1 Nr. 2 EStG).

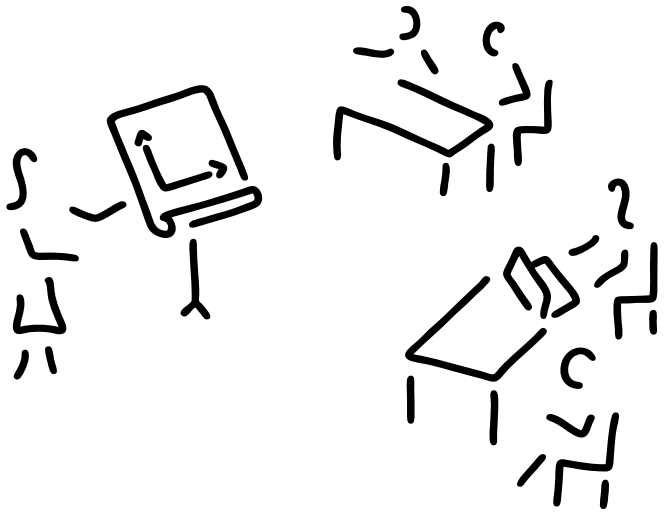
Liegt ein solcher „Kleinfall" nicht vor, besteht gemäß § 25 Abs. 4 Satz 1 EStG eine Pflicht zur elektronischen Übermittlung der Steuererklärung an das Finanzamt.

Allerdings sieht das Gesetz in § 25 Abs. 4 Satz 2 EStG eine **Ausnahmeregelung** vor: Danach kann die Finanzbehörde auf Antrag zur Vermeidung unbilliger Härten auf eine elektronische Übermittlung der Einkommensteuererklärung verzichten. Auch hier ist wiederum die allgemeine steuerverfahrensrechtliche Vorschrift des § 150 Abs. 8 Satz 1 AO zu beachten. Nach dieser Regelung ist einem solchen Antrag zu entsprechen, wenn eine Erklärungsabgabe nach amtlich vorgeschriebenem Datensatz durch Datenfernübertragung für den Steuerpflichtigen **wirtschaftlich oder persönlich unzumutbar** ist. Dies ist nach § 150 Abs. 8 Satz 2 AO insbesondere der Fall, wenn die Schaffung der technischen Möglichkeiten für eine Datenfernübertragung des amtlich vorgeschriebenen Datensatzes nur mit einem **nicht unerheblichen finanziellen Aufwand** möglich wäre oder wenn der Steuerpflichtige **nach seinen individuellen Kenntnissen und Fähigkeiten nicht oder nur eingeschränkt in der Lage** ist, die Möglichkeiten der Datenfernübertragung zu nutzen.

Im Ergebnis haben somit gerade Steuerpflichtige, die über keine entsprechende informationstechnische Ausstattung verfügen oder im Umgang mit der notwendigen Informations- und Kommunikationstechnik nicht geübt sind, die Möglichkeit, beim Finanzamt gemäß § 25 Abs. 4 Satz 2 EStG in Verbindung mit § 150 Abs. 8 AO zu **beantragen**, zur Vermeidung unbilliger Härten auf eine elektronische Übermittlung der Steuererklärung zu verzichten. Ansonsten sind sie gemäß § 25 Abs. 4 Satz 1 EStG bei Gewinneinkünften (wie beispielweise Einkünften aus Gewerbebetrieb beim Betrieb einer Photovoltaikanlage) in Höhe von über 410 Euro – neben Einkünften aus nichtselbständiger Arbeit – dazu verpflichtet, ihre Einkommensteuererklärung – im Hinblick auf die Gewinneinkünfte – elektronisch an das Finanzamt zu übermitteln.

In diesem Zusammenhang weise ich allerdings darauf hin, dass von der grundsätzlichen elektronischen Übermittlungspflicht des § 25 Abs. 4 Satz 1 EStG nur die oben genannten Gewinneinkünfte nach § 2 Abs. 1 Satz 1 Nrn. 1 bis 3 EStG, nicht aber die **Überschusseinkünfte** nach § 2 Abs. 1 Satz 1 Nrn. 4 bis 7 EStG **– wie insbesondere die Einkünfte aus nichtselbständiger Arbeit –** betroffen sind. Insoweit besteht nach wie vor **keine gesetzliche Verpflichtung zur elektronischen Übermittlung der Einkommensteuererklärung** an das Finanzamt.

10 Schulen und Hochschulen



10.1 Umfassende Regelung der Schülerunterlagen

Seit alters her führen Schulen über ihre Schülerinnen und Schüler Akten. Darin werden traditionell insbesondere Kontaktdaten wie Namen und Anschriften vermerkt, Noten eingetragen, Zeugnisse und Leistungsnachweise aufbewahrt, Schulwechsel und Ordnungsmaßnahmen dokumentiert sowie andere aus Sicht der Schule maßgebliche Ereignisse und Entwicklungen im Schülerleben beurteilt und festgehalten. In datenschutzrechtlicher Hinsicht enthalten somit **Schülerunterlagen umfangreiche Sammlungen von – teilweise sogar sehr sensiblen – personenbezogenen Daten**, die mit jedem absolvierten Schuljahr aussagekräftiger werden und einen zunehmend informativeren Überblick über wesentliche Aspekte der Entwicklung von Kindern, Jugendlichen und jungen Erwachsenen geben.

In deutlichem Kontrast zu Umfang und Sensibilität dieser Datensammlungen stand allerdings jahrzehntelang die geringe Dichte der schulrechtlichen Vorgaben. Die Rechtslage war lückenhaft und wenig übersichtlich. Nur Teilfragen des Umgangs mit Schülerunterlagen – insbesondere in Bezug auf den Schülerbogen – waren in einzelnen Vorschriften der Schulordnungen sowie in einigen Schreiben des Kultusministeriums geregelt. Keine spezifischen parlamentsgesetzlichen Regelungen gab es aber insbesondere zum Inhalt und zur Aufbewahrung der Schülerakte. Daher war hier den Schulen **allein** ein **Rückgriff auf die – naturgemäß sehr abstrakt gefasste – schuldatenschutzrechtliche Generalklausel** des Art. 85 Abs. 1 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG) sowie auf die subsidiären, ebenfalls abstrakten Regelungen des Bayerischen Datenschutzgesetzes möglich.

Diese zwar teilweise auf Schulen, nicht aber auf Schülerunterlagen zugeschnittenen Regelungen führten schon seit Langem, in Anbetracht der stetig wachsenden informations- und kommunikationstechnischen Möglichkeiten aber **zunehmend** in jüngster Zeit **Unsicherheiten und Auslegungsfragen** herbei. Im Rahmen meiner datenschutzrechtlichen Kontrolltätigkeit, insbesondere bei meinen zahlreichen Außenprüfungen öffentlicher – staatlicher wie kommunaler – Schulen, musste ich daher immer wieder feststellen, dass diese allgemein-abstrakten Regelungen bei den Schulen einen **bayernweit uneinheitlichen und teils unreflektierten Umgang mit den sensiblen Schülerunterlagen** begünstigten.

Bereits seit den frühen 1990er Jahren habe ich mich daher dafür eingesetzt, datenschutzgerechte, detaillierte und bayernweit einheitliche Vorgaben für die Führung von und den Umgang mit Schülerunterlagen zu schaffen. Verstärkt seit dem Beginn des neuen Jahrtausends habe ich das **Kultusministerium von einer klaren, umfassenden und schulartübergreifenden rechtlichen Gesamtregelung der Schülerunterlagen zu überzeugen versucht**. Diese sollte von den Schulen vor Ort umsetzbar sein und damit auch bayernweit die Schulen und Schulaufwandsträger – personell wie finanziell – entlasten.

Besonderen Wert habe ich darauf gelegt, dass die mit der Anlage, Führung, Verwendung und Aufbewahrung der Schülerunterlagen verbundene Beschränkung des Grundrechts der Schülerinnen und Schüler auf informationelle Selbstbestimmung gemäß Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 Grundgesetz für die Bundesrepublik Deutschland (GG) schon aus verfassungsrechtlichen Gründen eine **grundlegende parlamentsgesetzliche Regelung** erfährt.

Im Berichtszeitraum waren meine langjährigen Bemühungen **endlich erfolgreich**.

10.1.1 Übersicht über die neuen schuldatenschutzrechtlichen Regelungen

— Zunächst hat der bayerische Gesetzgeber mit Wirkung vom 1. August 2015 in einem **neuen Art. 85 Abs. 1a BayEUG** eine grundlegende und schulartübergreifende parlamentsgesetzliche Regelung der Schülerunterlagen geschaffen. Diese Rechtsnorm enthält nicht nur die zentralen Vorgaben zu den Schülerunterlagen, sondern auch eine Ermächtigung für den Erlass einer diese gesetzlichen Vorgaben – insbesondere im Hinblick auf Inhalt, Verwendung (vor allem Zugriff und Weitergabe) sowie Art und Dauer der Aufbewahrung der Schülerunterlagen – konkretisierenden Rechtsverordnung.

— Auf Basis dieser Rechtsverordnungsermächtigung hat sodann das Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst in enger Abstimmung mit mir die Verordnung über Schülerunterlagen (**Schülerunterlagenverordnung**) erlassen, die am 1. Oktober 2015 in Kraft getreten ist. Im Zuge der Harmonisierung des Schulrechts hat das Kultusministerium diese Verordnung mit Wirkung vom 1. August 2016 – im Wesentlichen unverändert – als **Teil 5** in die neu geschaffene Schulordnung für schulartübergreifende Regelungen an Schulen in Bayern (**Bayerische Schulordnung** – BaySchO) überführt.

  Für einen einheitlichen Vollzug der Schülerunterlagenverordnung hat das Kultusministerium den Schulen zudem – ebenfalls nach Abstimmung mit

mir – umfangreiche **„Durchführungshinweise zum Umgang mit Schülerunterlagen“** (Bekanntmachung vom 13. Oktober 2015, Az.: II.1-BS4310.1/1/1/4, KWMBl. S. 221, geändert am 30. Juni 2016, Az.: II.1-BS4310.1/7/3, KWMBl. S. 151, im Folgenden: Durchführungshinweise) mit zahlreichen Musterformularen an die Hand gegeben. Die Durchführungshinweise sind am 8. Dezember 2015 in Kraft getreten.

— Schließlich haben das Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst und die Generaldirektion der Staatlichen Archive Bayerns auf der Grundlage von Art. 6 Abs. 2 Bayerisches Archivgesetz (BayArchivG) **im Hinblick auf die Aussonderung von Schülerunterlagen der staatlichen Schulen in Bayern** eine **Archivierungsvereinbarung** (Bekanntmachung vom 14. April 2016, Az.: II.1-BS4310.1/1/6, KWMBl. S. 92, im Folgenden: Archivierungsvereinbarung) geschlossen, die mit Wirkung vom 14. April 2016 in Kraft getreten ist.

10.1.2 Regelungsgehalt des Art. 85 Abs. 1a BayEUG

Art. 85 Abs. 1a Satz 1 BayEUG verpflichtet die Schulen ausdrücklich dazu, für jede Schülerin und jeden Schüler **die für das Schulverhältnis wesentlichen Unterlagen** als **Schülerunterlagen** zu führen. Art. 85 Abs. 1a Satz 2 BayEUG hebt hervor, dass die Schülerunterlagen **vertraulich zu behandeln und** durch geeignete technische und organisatorische Maßnahmen **vor unberechtigtem Zugriff zu sichern** sind. Art. 85 Abs. 1a Satz 3 BayEUG **ermächtigt das zuständige Staatsministerium**, durch **Rechtsverordnung** insbesondere den Inhalt, die Verwendung, vor allem den Zugriff und die Weitergabe, sowie die Art und Dauer der Aufbewahrung der Schülerunterlagen zu regeln.

Art. 85 BayEUG Erhebung, Verarbeitung und Nutzung von Daten
(1a) [1]Für jede Schülerin und jeden Schüler führen die Schulen die für das Schulverhältnis wesentlichen Unterlagen als Schülerunterlagen. [2]Die Schülerunterlagen sind vertraulich zu behandeln und durch geeignete technische und organisatorische Maßnahmen vor unberechtigtem Zugriff zu sichern. [3]Das zuständige Staatsministerium regelt durch Rechtsverordnung insbesondere den Inhalt, die Verwendung, vor allem den Zugriff und die Weitergabe, sowie die Art und Dauer der Aufbewahrung der Schülerunterlagen.

Da die Schülerunterlagen für den gesamten (schulischen) Lebensweg der Schülerinnen und Schüler besonders bedeutsam sind, begrüße ich es, dass der **bayerische Gesetzgeber** durch Erlass dieser Rechtsnorm **seiner Regelungsverantwortung für einen wichtigen Lebensbereich von Kindern, Jugendlichen und jungen Erwachsenen gerecht geworden** ist.

10.1.3 Vorgaben zu Schülerunterlagen in der Bayerischen Schulordnung

Die neue Bayerische Schulordnung legt in ihrem Teil 5 – Schülerunterlagen (vergleiche Art. 85 Abs. 1a BayEUG) – zunächst fest, dass die Schülerunterlagen die in Papierform zu führende Schülerakte und die (schriftlichen sowie praktischen) Leistungsnachweise umfassen. Sodann bestimmt sie abschließend und schulartübergreifend, welche Unterlagen generell in der Schülerakte geführt werden dürfen. Anschließend normiert sie, welche Personen in welchen Fällen Zugriff auf die Schülerunterlagen haben dürfen und welche Schülerunterlagen in welchen

Fällen weitergegeben werden dürfen. Danach wird geregelt, für welche Zeiträume die Schülerunterlagen aufzubewahren sind und wer unter welchen Bedingungen zur Einsichtnahme in die Schülerunterlagen berechtigt ist. Zuletzt wird festgelegt, wie im Falle der Auflösung, Zusammenlegung oder Teilung der Schule mit den Schülerunterlagen zu verfahren ist.

Auf folgende **bedeutsame Vorgaben zum Umgang mit Schülerunterlagen** mache ich besonders aufmerksam:

– **Begriff und Inhalt der Schülerunterlagen** (§ 37 BaySchO)

  Klarheit schafft die Verordnung zunächst in begrifflicher Hinsicht. Vorweg legt § 37 Satz 1 BaySchO fest, dass die **Schülerunterlagen die für das Schulverhältnis jeder Schülerin und jedes Schülers wesentlichen Unterlagen** umfassen. Sodann bestimmt § 37 Satz 2 BaySchO grundlegend, dass die Schülerunterlagen **aus der in Papierform zu führenden Schülerakte** (§ 37 Satz 2 Nr. 1 BaySchO) **und den** schriftlichen sowie praktischen **Leistungsnachweisen** (§ 37 Satz 2 Nr. 2 BaySchO) bestehen.

  Die einzelnen (möglichen) **Bestandteile der Schülerakte** sind wiederum in § 37 Satz 2 Nr. 1 Buchstaben a) bis o) BaySchO **abschließend und schulartübergreifend** aufgeführt. So darf die Schülerakte – je nach Schulart – beispielsweise enthalten:

  – das **Schülerstammblatt**, das unter anderem Angaben über die Schülerin oder den Schüler, die Erziehungsberechtigten, die Berufsausbildung und die Schullaufbahn enthält und nach dem vom Kultusministerium in Anlage I der Durchführungshinweise vorgegebenen Muster zu führen ist,

  – die **Abschlusszeugnisse** und anderen wichtigen Zeugnisse,

  – den **Schullaufbahnbogen**, in dem die für den schulischen Bildungsweg wesentlichen Feststellungen, Beobachtungen und Empfehlungen einschließlich einer Übersicht über die ausgesprochenen Ordnungsmaßnahmen nach Art. 86 Abs. 2 Nrn. 6 bis 12 BayEUG aufgenommen werden und der nach dem vom Kultusministerium in Anlage II der Durchführungshinweise vorgegebenen Muster zu führen ist,

  – die **Notenbögen**, in die insbesondere die Ergebnisse der schriftlichen, mündlichen und praktischen Leistungsnachweise der einzelnen Schülerin oder des einzelnen Schülers sowie damit zusammenhängende Bemerkungen aufgenommen werden,

  – die **schriftlichen Angaben über** bereits erfolgte Maßnahmen und diagnostische Grundlagen bei Schülerinnen und Schülern mit besonderem **Förderbedarf sowie** Unterlagen zum **Nachteilsausgleich und Notenschutz**,

  – **alle sonstigen schriftlichen**, die einzelne Schülerin oder den einzelnen Schüler betreffenden **wesentlichen Vorgänge**, die zur nachvollziehbaren und transparenten Dokumentation der Schullaufbahn

zwingend notwendig sind. Dabei ist gemäß Nr. 2.9 Durchführungshinweise für die Einordnung als wesentlicher Vorgang – datenschutzrechtlich begrüßenswert – ein **strenger Maßstab** anzulegen.

Aus Datenschutzsicht verdient schließlich die Vorschrift des § 37 Satz 3 BaySchO besondere Hervorhebung. Diese Norm stellt klar, dass **Schülerunterlagen, die einer Schweigepflicht unterliegen** – etwa Aufzeichnungen einer Schulpsychologin oder eines Schulpsychologen – nicht in die Schülerakte aufgenommen werden dürfen. Diese Unterlagen **verbleiben** vielmehr **außerhalb der Schülerakte bei den jeweiligen Schweigeverpflichteten** (siehe Nr. 2.10 Durchführungshinweise).

– **Verwendung der Schülerunterlagen** (§ 38 BaySchO)

Nach § 38 Abs. 1 BaySchO dürfen die Schülerunterlagen **ohne Einwilligung der Betroffenen nur** verwendet werden, **soweit** dies **zur Erfüllung der den Schulen durch Rechtsvorschriften zugewiesenen Aufgaben erforderlich** ist. Bei minderjährigen Schülerinnen und Schülern müssen die Erziehungsberechtigten einwilligen, ab Vollendung des 14. Lebensjahres zusätzlich auch die Minderjährigen selbst; die Einwilligung ist schriftlich zu erteilen und muss sich auf einen konkret benannten Zweck beziehen (siehe § 38 Abs. 3 BaySchO).

Der **Zugriff auf die Schülerunterlagen** ist gemäß § 38 Abs. 2 Satz 1 BaySchO jeweils **auf den konkreten Einzelfall zu beschränken**. Zugriff auf die Schülerunterlagen dürfen nach § 38 Abs. 2 Satz 2 BaySchO insbesondere erhalten:

– **Lehrkräfte** für die jeweils von ihnen unterrichteten Schülerinnen und Schüler, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist,

– die **Schulleitung**, soweit dies zur Erfüllung ihrer pädagogischen, organisatorischen und rechtlichen Aufgaben erforderlich ist,

– **Beratungslehrkräfte, Schulpsychologinnen** und **Schulpsychologen**, soweit dies zur Erfüllung ihrer pädagogisch-psychologischen und rechtlichen Aufgaben im Rahmen der Schulberatung erforderlich ist.

Nach Beendigung des Schulbesuchs darf gemäß § 38 Abs. 2 Satz 3 BaySchO Zugriff auf die Schülerunterlagen **nur die Schulleitung im konkreten Einzelfall** erhalten, soweit dies zur Erfüllung ihrer rechtlichen Aufgaben erforderlich ist oder die Betroffenen eingewilligt haben. Solche „Einwilligungsfälle“ können in der Praxis etwa auftreten, wenn ein ehemaliger Schüler oder eine ehemalige Schülerin eine Zweitschrift seines/ihres Abschlusszeugnisses oder eine Schulbesuchsbescheinigung benötigt. Die Einwilligung ist immer schriftlich zu erteilen und muss sich auf einen konkret benannten Zweck – wie etwa den Nachweis beruflicher Qualifikationen oder die Belegung sozialversicherungsrechtlicher Ansprüche – beziehen. Das Schriftformerfordernis dient nicht allein dem Schutz der betroffenen Schülerin oder des betroffenen Schülers, sondern auch der Absicherung der Schule. Allerdings kann das Schriftformerfordernis nicht nur – idealerweise – schon bei Antragstellung, sondern auch erst bei Abholung der

Zweitschrift oder der Bescheinigung erfüllt werden (siehe Nr. 3.3 Durchführungshinweise).

— **Aufbewahrung der Schülerunterlagen** (§ 40 BaySchO)

Aus Datenschutzsicht von besonderer Bedeutung ist die Dauer der Aufbewahrung der Schülerunterlagen. § 40 BaySchO sieht hierzu eine ausdifferenzierte Regelung vor, die sich – vereinfachend – wie folgt zusammenfassen lässt:

— Das Schülerstammblatt mit seinen Basisdaten sowie wichtige (Abschluss-)Zeugnisse und Urkunden sind **50 Jahre**,

— sonstige Unterlagen der Schülerakte **ein Jahr** und

— Leistungsnachweise **zwei Jahre**

aufzubewahren. Die Fristen beginnen mit Ablauf des Schuljahres, in dem die Schülerin oder der Schüler die Schule verlässt, beziehungsweise mit Ablauf des Schuljahres, in dem die Leistungsnachweise angefertigt wurden.

Auch bei der Aufbewahrung haben die Schulen die erforderlichen technischen und organisatorischen Vorkehrungen zu treffen, damit der **Schutz der Schülerunterlagen vor unbefugten Zugriffen** sichergestellt ist (siehe Art. 85 Abs. 1a Satz 2 BayEUG und Nr. 5.2 Durchführungshinweise).

Aus datenschutzrechtlicher Sicht ist insbesondere die in § 40 Satz 1 Nr. 1 BaySchO für die genannten Unterlagen festgesetzte **50jährige Aufbewahrungsfrist viel zu lang bemessen**. Für mich ist kein überzeugender Grund ersichtlich, weshalb die gesetzgeberische Wertentscheidung des Art. 6 Abs. 1 Satz 2 BayArchivG, die für alle anderen Zweige der staatlichen Verwaltung maßgebend ist, im Schulbereich nicht sachgerecht sein sollte. Hiernach sind für die Aufbewahrung **maximal 30 Jahre** vorgesehen. Die Aufarbeitung kriegsbedingter Dokumentenverluste – oft ein Argument für die längere Aufbewahrung im Schulbereich – dürfte über 70 Jahre nach Kriegsende bei den Sozialversicherungsträgern endgültig abgeschlossen sein. Die für die Anrechnung rentenversicherungsrechtlicher Zeiten notwendigen Ausbildungsdaten derzeit noch aktiver, pflicht- oder freiwillig versicherter Personen werden im Rahmen der von der Rentenversicherung regelmäßig gesetzlich verpflichtend durchgeführten Kontenklärungsverfahren (siehe § 149 Sozialgesetzbuch Sechstes Buch – Gesetzliche Rentenversicherung –) ohnehin bereits frühzeitig erfasst und nachgewiesen. Für eine 50jährige Aufbewahrung der Schülerunterlagen bei den Schulen vermag ich daher **weder ein tatsächliches Bedürfnis noch eine entsprechende rechtliche Aufgabenzuweisung** zu erkennen. Im Verordnungserlassverfahren konnte ich mich insoweit aber leider nicht durchsetzen. Allerdings zeigen mir bereits erste Rückmeldungen im Rahmen meiner bayernweiten datenschutzrechtlichen Kontroll- und Beratungstätigkeit, dass auch die schulische Praxis gerade diese Frist – in Übereinstimmung mit den kommunalen Sachaufwandsträgern – als unangemessen und viel zu lang bewertet.

In Anbetracht dieser ohnehin schon deutlich zu langen Frist ist die in § 40 Satz 4 BaySchO im Einzelfall zusätzlich bestehende **Abweichungsmöglichkeit „nach oben“** besonders problematisch. Es besteht die Gefahr, dass § 40 Satz 4 BaySchO nicht nur die festgelegten Aufbewahrungsfristen entwertet, sondern auch ein bedeutsames Ziel der Verordnung – den bayernweit schulartübergreifend einheitlichen Umgang mit Schülerunterlagen – konterkariert. Bei der Prüfung des Vorliegens der Gründe für eine mögliche Fristverlängerung ist daher gemäß Nr. 5.1 Satz 2 Durchführungshinweise ein **strenger Maßstab** anzulegen. So kommt ein Ausnahmefall etwa in Betracht, soweit die Unterlagen **im Einzelfall** für eine Rechtsstreitigkeit benötigt werden. In jedem Einzelfall sind die Gründe nach § 40 Satz 5 BaySchO allerdings nachvollziehbar zu dokumentieren.

— **Aussonderung der Schülerunterlagen** (Nr. 9 Durchführungshinweise)

Nach Ablauf der Aufbewahrungsfristen sind die Schülerunterlagen auszusondern, also aus den entsprechenden schulischen Aufbewahrungseinrichtungen herauszunehmen und dem zuständigen Archiv anzubieten oder zu vernichten.

Insoweit gelten **für staatliche Schulen** die **Vorgaben der Nr. 9 Durchführungshinweise**, die insbesondere auf die zwischen dem Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst auf der einen Seite und der Generaldirektion der Staatlichen Archive Bayerns auf der anderen Seite abgeschlossene Archivierungsvereinbarung verweisen.

In Anbetracht der großen Anzahl an staatlichen Schulen und der demgegenüber sehr begrenzten Kapazitäten der staatlichen Archive werden danach **nur ausgewählte Schulen** (siehe Anlage 1 der Archivierungsvereinbarung) **sowie besonders bedeutsame Schülerunterlagen** – etwa Schülerunterlagen von bedeutenden Persönlichkeiten oder von besonderem geschichtlichem Interesse – in die **Archivierung** einbezogen. Um im Einzelfall lokalen und regionalen Bedürfnissen nach einer Archivierung der örtlichen Überlieferung entgegenzukommen, können die **aus örtlicher Sicht archivwürdigen**, von den staatlichen Archiven nicht übernommenen **Schülerunterlagen** mit Einverständnis des Sachaufwandsträgers und unter Vorbehalt des Eigentums des Freistaates Bayern allerdings **nach Abschluss eines Archivierungsvertrags** (siehe Anlage 2 der Archivierungsvereinbarung) dauerhaft **in einem anderen öffentlichen – insbesondere kommunalen – Archiv verwahrt** werden.

Schülerunterlagen staatlicher Schulen, die weder dem zuständigen staatlichen Archiv noch einem anderen öffentlichen Archiv zur Archivierung übergeben werden, sind **datenschutzgerecht zu vernichten**. Dabei ist sicherzustellen und zu überwachen, dass nach dem aktuellen Stand der Technik Unbefugte keinen Einblick in die Unterlagen erhalten und das Papier der Rohstoffverwertung zugeführt wird (siehe Nr. 9.2.3 Durchführungshinweise).

— **Einsichtnahme in die Schülerunterlagen** (§ 41 BaySchO)

§ 41 BaySchO regelt die **Einsichtnahme in die eigene Schülerakte und die eigenen Leistungsnachweise**. Hier geht es nicht um die Verwendung der Schülerakte (insbesondere den Zugriff durch Lehrkräfte, hierzu siehe

die Ausführungen oben zu § 38 BaySchO), sondern um die Voraussetzungen, unter denen die Betroffenen Kenntnis über den Inhalt der sie selbst betreffenden Akte erlangen können. Ein solches Informationsrecht ist ein fundamentales Datenschutzrecht. Es ist Voraussetzung und zugleich Bestandteil des Rechts auf informationelle Selbstbestimmung nach Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 GG.

Im Einzelnen:

- § 41 Abs. 1 Nr. 1 BaySchO gewährt den **Schülerinnen und Schülern ab dem 14. Lebensjahr –** auch wenn sie die Schule verlassen haben – ein eigenständiges Einsichtsrecht.

- § 41 Abs. 1 Nr. 2 BaySchO vermittelt außerdem den **Erziehungsberechtigten** – also gemäß Art. 74 Abs. 2 BayEUG den Personen, die (für minderjährige Schülerinnen und Schüler) sorgeberechtigt sind – ein eigenes originäres Einsichtsrecht, das von den Regelungen zur Ausübung der gemeinsamen Sorge bei getrenntlebenden Ehegatten unabhängig ist (siehe Nr. 6.2 Satz 7 Durchführungshinweise).

- Unter den in § 41 Abs. 1 Nr. 3 BaySchO genannten Voraussetzungen dürfen zudem die **früheren Erziehungsberechtigten** bei Schülerinnen und Schülern ab der Vollendung des 18. Lebensjahres bis zur Vollendung des 21. Lebensjahres Einsicht in die Schülerunterlagen nehmen.

In seltenen Ausnahmefällen kann das **Einsichtsrecht** nach Maßgabe des – eng auszulegenden – § 41 Abs. 2 BaySchO **beschränkt** werden. Soweit möglich, ist eine Einsichtnahme in die Schülerunterlagen allerdings zu gewähren; dabei haben die Schulen gegebenenfalls die **Daten, in welche eine Einsicht unzulässig ist, zu schwärzen**. Eine pauschale Verweigerung der Einsichtnahme ist in jedem Fall unzulässig (siehe zum Ganzen Nr. 6.2 Durchführungshinweise).

Für die Gewährung von Einsichtnahme und die Anfertigung von Ablichtungen können die öffentlichen Schulen nach Art. 16 Abs. 3 Kostengesetz **auf die Erhebung von Kosten verzichten**. Bei staatlichen Schulen ist gemäß Nr. 6.4 Satz 2 Durchführungshinweise ein solcher Verzicht im Regelfall möglich.

- Übergangsvorschriften (§ 44a BaySchO)

In vollem Umfang gelten die **neuen Vorgaben erst für die Schülerunterlagen, die ab dem Schuljahr 2016/2017 angelegt werden**. Die zuvor angelegten Schülerunterlagen dürfen aus Gründen der Verwaltungsvereinfachung im Grundsatz in ihrem bisherigen „Aufbau“ fortgeführt werden. Die neuen Vorschriften – insbesondere zu Verwendung, Aufbewahrung und Einsichtnahme – sind aber gemäß § 44a Abs. 1 BaySchO auch hier vollumfänglich zu beachten.

– Geltungsbereich der Verordnung (§ 1 BaySchO)

Wie alle anderen Vorschriften der Bayerischen Schulordnung gelten auch die Vorgaben zu den Schülerunterlagen nach § 1 Satz 1 BaySchO in vollem Umfang **für alle bayerischen öffentlichen – also staatlichen und kommunalen – Schulen** (siehe Art. 3 Abs. 1 BayEUG) **und die staatlich anerkannten Ersatzschulen mit dem Charakter einer öffentlichen Schule** (siehe Art. 101 BayEUG), soweit sie der Aufsicht des Staatsministeriums für Bildung und Kultus, Wissenschaft und Kunst unterliegen.

Mit Blick auf die verfassungsrechtlich in Art. 7 Abs. 4 GG gewährleistete Privatschulfreiheit gilt die Verordnung nach § 1 Satz 2 BaySchO **überdies für staatlich genehmigte und staatlich anerkannte Ersatzschulen** im Rahmen der Art. 90, 92 Abs. 2 Nr. 2 und Abs. 5 und Art. 93 BayEUG, für letztere darüber hinaus im Rahmen des Art. 100 Abs. 2 BayEUG.

10.1.4 Fazit

Mit den vorgestellten Regelungen kennt das Schul(datenschutz)recht in Bayern nun **erstmals einheitliche, klare, umfassende und schulartübergreifende Vorgaben**, die insbesondere den genauen Inhalt der **Schülerunterlagen**, ihre Verwendung (vor allem den Zugriff und die Weitergabe) und die Art und Dauer der Aufbewahrung sowie die bestehenden Einsichtsrechte rechtssicher festlegen.

Auch wenn die aufgezeigten Vorschriften zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Schülerdaten aus Datenschutzsicht **zum Teil durchaus noch verbesserungsfähig** sind, tragen sie den Grundrechten der Schülerinnen und Schüler sowie der Erziehungsberechtigten beim Umgang mit Schülerunterlagen im Grundsatz ebenso Rechnung wie den organisatorischen und pädagogischen Interessen gerade der bayerischen öffentlichen – staatlichen wie kommunalen – Schulen.

10.2 Digitales Lernen an bayerischen Schulen: „mebis – Landesmedienzentrum Bayern“

Bereits im September 2011 hat das damalige Staatsministerium für Unterricht und Kultus das Projekt „Digitales Lernen Bayern“ gestartet, um den **informations- und kommunikationstechnisch gestützten**, also den **digitalen Unterricht an bayerischen Schulen** gezielt zu fördern. Dieses Ziel hat der Ministerpräsident in seiner Regierungserklärung „Bayern. Die Zukunft“ am 12. November 2013 aufgegriffen, indem er ankündigte, ein virtuelles Bildungsmedienzentrum einzurichten, die rund 6.100 bayerischen Schulen an ein zentrales Bildungsnetz anzubinden und damit die Medienkompetenz der bayerischen Schülerinnen und Schüler weiter auszubauen.

Gewissermaßen als „Kernstück“ des Projektes „Digitales Lernen Bayern“ hat das Kultusministerium ein **Dachportal** mit der Bezeichnung **„mebis – Landesmedienzentrum Bayern“** geschaffen, unter dem bereits bestehende Maßnahmen gebündelt und mit weiteren, neuen Angeboten zusammengeführt wurden. **Wesentliche Bestandteile** von „mebis – Landesmedienzentrum Bayern“ sind das **mebis-Infoportal**, die **mebis-Mediathek**, das **mebis-Prüfungsarchiv** und die **mebis-Lernplattform.**

In das Projekt „Digitales Lernen Bayern“ war ich von Anfang an eingebunden. Insbesondere während der Entwicklungsphase habe ich es intensiv datenschutzrechtlich begleitet. Durch meine frühe Beteiligung konnte ich **rechtzeitig datenschutzrechtlich kritische Punkte identifizieren und auf Verbesserungen hinwirken**. Es ist auf diese Weise gelungen, ein für die Schulen in ganz Bayern auch unter Datenschutzaspekten attraktives Online-Angebot zu entwickeln. Nach Angaben des Kultusministeriums haben Mitte 2016 bereits mehr als 2.900 Schulen in Bayern mit über 550.000 registrierten Nutzerinnen und Nutzern – Schülerinnen und Schülern ebenso wie Lehrkräften – die Angebote von „mebis – Landesmedienzentrum Bayern“ eingesetzt.

10.2.1 Notwendigkeit einer Rechtsgrundlage für die mebis-Lernplattform

Unter den vielen Angeboten, die „mebis – Landesmedienzentrum Bayern“ bereithält, ist aus datenschutzrechtlicher Sicht die **mebis-Lernplattform** besonders bedeutsam. Denn aufgrund der regelmäßig personalisierten Anmeldung und der regelmäßigen Protokollierung aller Nutzungsbewegungen besteht hier die Möglichkeit, detaillierte Verhaltensprofile der einzelnen Nutzerinnen und Nutzer anzufertigen.

Die **wesentlichen schul- und datenschutzrechtlichen Vorgaben** zum Betrieb und zur Nutzung von Lernplattformen an bayerischen öffentlichen Schulen enthält die **Anlage 10 „Passwortgeschützte Lernplattform“ der** vom Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst erlassenen **Verordnung zur Durchführung des Art. 28 Abs. 2 des Bayerischen Datenschutzgesetzes (DVBayDSG-KM)**. Diese Anlage legt insbesondere den zulässigen Umfang der Daten fest, der beim Einsatz passwortgeschützter Lernplattformen von Schülerinnen und Schülern sowie von Lehrkräften gespeichert werden darf, sieht aber auch Regelungen zur Nutzungsberechtigung, zum Nutzungsumfang und zu den Löschfristen vor. In diesem Zusammenhang möchte ich auch auf den Beitrag Nr. 10.1.2 meines 26. Tätigkeitsberichts 2014 aufmerksam machen, in dem ich mich zuletzt zu Anlage 10 DVBayDSG-KM ausführlich geäußert habe.

Die personenbezogenen Schüler- und Lehrerdaten, die in der **mebis-Lernplattform** nach der Vorstellung des Kultusministeriums gespeichert werden sollten, gingen jedoch **über den Rahmen**, der in der damaligen – bis zum 31. Mai 2014 geltenden – Fassung **der Anlage 10 DVBayDSG-KM** vorgegeben war, **deutlich hinaus**. So sollten hier zahlreiche zusätzliche personenbezogene Schüler- und Lehrerdaten gespeichert werden und damit auch die Nutzungs- und Verarbeitungsrechte der Lehrkräfte sowie der Schülerinnen und Schüler erheblich ausgeweitet werden. Das Kultusministerium vertrat dennoch die Auffassung, den Einsatz der mebis-Lernplattform rechtlich allein auf eine bloße (landesweite) datenschutzrechtliche Freigabe im Sinne von Art. 26 Abs. 1 Satz 2 Halbsatz 2 Fall 1 BayDSG stützen zu können.

Gegen dieses Vorhaben habe ich jedoch erhebliche verfassungsrechtliche Bedenken erhoben. Seit dem „Volkszählungsurteil“ des Bundesverfassungsgerichts (Urteil vom 15. Dezember 1983 – 1 BvR 209/83 u.a.) ist es anerkannt, dass Einschränkungen des Grundrechts auf informationelle Selbstbestimmung gemäß Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 Grundgesetz für die Bundesrepublik Deutschland einer **verfassungsgemäßen gesetzlichen Grundlage** bedürfen. Gerade in dem besonders grundrechtsrelevanten Bereich der öffentlichen Schulen muss daher der Gesetz- und Verordnungsgeber selbst für den Einsatz von

passwortgeschützten Lernplattformen den in aller Regel als ausreichend – und damit auch nur insoweit als datenschutzrechtlich erforderlich – bewerteten Rahmen vorgeben. Eine **deutliche inhaltliche Ausweitung** dieser gesetzlichen Festlegung ist folglich **nicht im Wege einer bloßen (landesweiten) datenschutzrechtlichen Freigabe** möglich. Vielmehr bedarf es insoweit einer Änderung der Anlage 10 DVBayDSG-KM in dem hierfür vorgeschriebenen Verfahrensweg.

10.2.2 Anpassung der Anlage 10 „Passwortgeschützte Lernplattform“ DVBayDSG-KM

Erfreulicherweise hat das Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst meine Argumente aufgegriffen.

Nach mehrmonatiger intensiver, teilweise kontroverser Diskussion hat es die **Anlage 10 „Passwortgeschützte Lernplattform“ DVBayDSG-KM** schließlich in Abstimmung mit mir **mit Wirkung vom 1. Juni 2014 angepasst**.

Hinsichtlich der Erhebung, Verarbeitung und Nutzung von personenbezogenen Schüler- und Lehrerdaten beim Einsatz von Lernplattformen hat das Kultusministerium dabei **unter anderem folgende Ergänzungen und Änderungen** vorgenommen:

- Benutzername, Nutzerrolle, lokale User-ID, Passwort, Stimme (im Rahmen von Audiobeiträgen) dürfen **zusätzlich gespeichert** werden;
- Korrekturzeichen und -anmerkungen, Mitgliedschaften in virtuellen Kursen/Räumen der Lernplattform (auch im Rahmen einer Schulpartnerschaft) sowie in der Lernplattform veröffentlichte Audiobeiträge dürfen **nunmehr ebenfalls gespeichert** werden;
- die **Lehrkräfte** dürfen unter anderem die Daten ihrer Schülerinnen und Schüler in den virtuellen Kursen/Räumen der Lernplattform (mit Ausnahme der lokalen User-ID und des Passwortes) **nutzen und verarbeiten**;
- umgekehrt steht auch den **Schülerinnen und Schülern** – neben dem Zugriff auf ihre eigenen Daten – ein **Leserecht beziehungsweise Hörrecht** bezüglich bestimmter, auf den jeweiligen virtuellen Kurs/Raum bezogener Daten der Lehrkräfte (etwa in der Lernplattform veröffentlichte Beiträge und Lektionen) zu;
- außerdem wurden die **Regelfristen für die Löschung oder die Prüfung der Löschung angepasst**. Danach ist ein Großteil der Daten spätestens am Ende des laufenden Schuljahres zu löschen.

Nichts geändert hat die Ergänzung der Anlage 10 DVBayDSG-KM aber an einem aus datenschutzrechtlicher Sicht **besonders wichtigen Grundsatz** (siehe Anlage 10 Nrn. 3.2 und 3.3 DVBayDSG-KM):

Die **Speicherung von Schüler- und Lehrerdaten** ist weiterhin regelmäßig **– in der mebis-Lernplattform** ebenso wie auch bei anderen passwortgeschützten Lernplattformen – **von der wirksamen Einwilligung der jeweils Betroffenen abhängig**. Zur Einholung der erforderlichen Einwilligungen der Betroffenen – Lehr-

kräfte, volljährige Schülerinnen und Schüler, Erziehungsberechtigte bei minderjährigen Schülerinnen und Schülern, diese zusätzlich ab Vollendung des 14. Lebensjahres – hat das Kultusministerium den Schulen verbindliche Muster vorgegeben (siehe die Anlagen 5.1 und 5.2 der von der Homepage des Kultusministeriums www.km.bayern.de unter „Ministerium“ – „Recht“ – „Datenschutz“ abrufbaren „Handreichung für Datenschutzbeauftragte an bayerischen staatlichen Schulen mit Formularsammlung“).

Einer Einwilligung bedarf es nur dann nicht, wenn – und soweit – die Lernplattform auf Grund von Regelungen des Kultusministeriums, wie etwa Lehrplänen, **verpflichtender Bestandteil des Unterrichts** ist. So kann der Einsatz passwortgeschützter Lernplattformen unter den sehr engen, kumulativ zu erfüllenden Voraussetzungen der Nr. 4.3 Abs. 3 der vom Kultusministerium erlassenen **Bekanntmachung „Medienbildung. Medienerziehung und informationstechnische Bildung in Schule“** vom 24. Oktober 2012 (Az.: III.4-5 S 1356-3.18 725) auch dezentral von der jeweiligen Schule vor Ort zum verpflichtenden Bestandteil des Unterrichts erklärt werden (siehe dazu im Einzelnen meinen 26. Tätigkeitsbericht 2014 unter Nr. 10.3). Im Fall des verpflichtenden schulischen Einsatzes hat die Schule die Betroffenen zuvor über Art und Umfang der Datenverarbeitung umfassend zu informieren.

10.2.3 Zwischenbilanz und Ausblick

Der Unterricht in virtuellen Klassenräumen ist aus dem heutigen Schulalltag nicht mehr wegzudenken. Im Gegenteil: er wird in der schulischen Praxis künftig weiter an Bedeutung gewinnen. Die **positive Resonanz**, die die **Einführung von „mebis – Landesmedienzentrum Bayern“** bei den bayerischen Schulen, Lehrkräften, Schülerinnen und Schülern hervorgerufen hat, spricht für sich. Nur konsequent und nachvollziehbar ist daher das Begehren gerade der Schulen, die inhaltlichen und technischen Möglichkeiten, die ein virtuelles Bildungsmedienzentrum bietet, stetig zu verfeinern und zu erweitern.

Soweit eine Fortentwicklung und Erweiterung virtueller Bildungsräume aber mit der Erhebung, Verarbeitung und Nutzung zusätzlicher personenbezogener Daten von Schülerinnen und Schülern sowie von Lehrkräften verbunden ist, müssen das Kultusministerium ebenso wie die Schulen darauf achten, dass die **Datenschutzrechte der Betroffenen – Schülerinnen und Schüler ebenso wie Lehrkräfte – gewahrt** werden.

In einer zunehmend digitalisierten Welt müssen gerade die **Schulen** hier ein **Vorbild** sein. In Wahrnehmung des gesetzlichen Bildungs- und Erziehungsauftrags (siehe Art. 1 und Art. 2 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen) sind die Schulen gehalten, ihren Schülerinnen und Schülern zu **vermitteln**, dass der Schutz personenbezogener Daten kein Selbstzweck ist, sondern dem **Schutz der Persönlichkeit** dient. Kinder und Jugendliche müssen den **bewussten und sorgfältigen Umgang mit „ihren“ Daten** lernen – nicht nur, aber auch gegenüber der Schule und ihren digitalen Unterrichtsprojekten.

Die weitere Entwicklung von „mebis – Landesmedienzentrum Bayern“ werde ich daher aus datenschutzrechtlicher Sicht aufmerksam verfolgen.

10.3 Videoaufnahmen im Schulunterricht

Im Berichtszeitraum haben viele Anfragen von öffentlichen – staatlichen wie kommunalen – Schulen, aber auch zahlreiche Eingaben von betroffenen Schulangehörigen bei mir den Eindruck der letzten Jahre weiter verstärkt, dass **Schulen in beständig zunehmendem Umfang Videotechnik im Unterricht einsetzen**. Dahinter steht zumeist eine anerkennenswerte pädagogische Absicht: Sei es, dass der Schulunterricht belebt, moderne Technik zur Wissensbildung in den Unterricht integriert und die Schülerinnen und Schüler motiviert werden sollen, sei es, dass die Videografie als Instrument der Professionalisierung des Lehrerberufs – gerade auch bei angehenden Lehrerinnen und Lehrern – eingesetzt werden soll.

Aus Datenschutzsicht darf dabei aber nicht übersehen werden, dass im Zuge von Videoaufnahmen im Unterricht regelmäßig Schülerinnen und Schüler ebenso wie Lehrkräfte selbst – optisch und gegebenenfalls auch akustisch – aufgezeichnet und damit **oftmals sensible personenbezogene Daten in erheblichem Umfang erhoben und möglicherweise auch für längere Zeit gespeichert und anderweitig verwendet werden**. Auch ohne Namensnennung oder -einblendung liegt allein schon im – vollständigen oder auch nur ausschnittsweisen – Aufzeichnen der an Schulen stets identifizierbaren Schulangehörigen eine Erhebung personenbezogener Daten.

Videografie greift daher in das verfassungsrechtlich verankerte **Allgemeine Persönlichkeitsrecht** aus Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 Grundgesetz für die Bundesrepublik Deutschland (GG) ein. Es ist allgemein anerkannt, dass sich der Schutz des Allgemeinen Persönlichkeitsrechts auch auf Abbildungen einer Person durch Dritte erstreckt. Dieses **Recht am eigenen Bild** gewährleistet nach der Rechtsprechung des Bundesverfassungsgerichts „dem Einzelnen Einfluß- und Entscheidungsmöglichkeiten, soweit es um die Anfertigung und Verwendung von (…) Aufzeichnungen seiner Person durch andere geht. Ob diese den Einzelnen in privaten oder öffentlichen Zusammenhängen zeigen, spielt dabei grundsätzlich keine Rolle. Das Schutzbedürfnis ergibt sich vielmehr (…) vor allem aus der Möglichkeit, das Erscheinungsbild eines Menschen in einer bestimmten Situation von diesem abzulösen, datenmäßig zu fixieren und jederzeit vor einem unüberschaubaren Personenkreis zu reproduzieren“ (so beispielsweise Bundesverfassungsgericht (BVerfG), Urteil vom 15. Dezember 1999 – 1 BvR 653/96 –, BVerfGE 101, 361, 381).

Eingriffe in das Recht am eigenen Bild **dürfen die Schulen allerdings nur vornehmen, wenn sie der Gesetzgeber hierzu ermächtigt hat**. Maßgeblich sind in diesem Zusammenhang die Bestimmungen des Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen (BayEUG) und des Bayerischen Datenschutzgesetzes (BayDSG).

10.3.1 Reichweite der gesetzlichen Befugnis des Art. 85 Abs. 1 BayEUG

Nach Art. 85 Abs. 1 Sätze 1 und 2 BayEUG dürfen die Schulen die zur Erfüllung der ihnen durch Rechtsvorschriften zugewiesenen Aufgaben erforderlichen personenbezogenen Daten der Schülerinnen und Schüler, deren Erziehungsberechtigten, der Lehrkräfte und des nicht unterrichtenden Personals erheben, verarbeiten und nutzen.

Art. 85 BayEUG Erhebung, Verarbeitung und Nutzung von Daten
(1) [1]Die Schulen dürfen die zur Erfüllung der ihnen durch Rechtsvorschriften zugewiesenen Aufgaben erforderlichen Daten erheben, verarbeiten und nutzen. [2]Dazu gehören personenbezogene Daten der Schülerinnen und Schüler und deren Erziehungsberechtigten, der Lehrkräfte und des nicht unterrichtenden Personals. . . .

— Erfüllung einer durch Rechtsvorschrift zugewiesenen Aufgabe

Verfolgt die Schule mit dem Einsatz der Videotechnik pädagogische Zwecke – wie etwa die Vermittlung von Wissen und Technikkompetenz –, kommt sie damit grundsätzlich ihrem **gesetzlichen Bildungs- und Erziehungsauftrag** und somit einer ihr durch Rechtsvorschrift zugewiesenen Aufgabe nach (siehe Art. 1 und 2 BayEUG sowie Art. 131 Verfassung des Freistaates Bayern). Videografie als Instrument der Professionalisierung des Lehrerberufs, ein weiterer (Neben-)Anlass für den Einsatz von Videotechnik, wird sich häufig – gerade bei angehenden Lehrerinnen und Lehrern – ebenfalls noch als Wahrnehmung dieses gesetzlichen Auftrags verstehen lassen.

Anders verhält es sich jedoch, wenn die Schule Filme von (besonderen) Schulveranstaltungen oder Projektgruppen zu **Werbe- und Imageförderungszwecken** anfertigen und – etwa durch den Abdruck von QR-Codes im schulischen **Jahresbericht** oder durch die Einstellung in die **Schulhomepage** – einem breiten Adressatenkreis zugänglich machen will. Öffentlichkeitsarbeit und Außendarstellung können hier nur selten und allenfalls in begrenztem Umfang als dem gesetzlichen Bildungs- und Erziehungsauftrag unterfallende Aufgaben angesehen werden.

— Erforderlichkeit der Videoaufzeichnung für die Aufgabenerfüllung

Kommt die Schule mit dem Einsatz der Videotechnik ihrem gesetzlichen Bildungs- und Erziehungsauftrag an sich nach, ist die damit einhergehende Datenerhebung und -verwendung jedoch **stets unzulässig, wenn** sie für die Aufgabenerfüllung **nicht erforderlich** ist.

Die Erforderlichkeit liegt dabei nur vor, wenn die Videoaufzeichnung erstens einen legitimen Zweck verfolgt, zweitens zu dessen Verwirklichung geeignet ist, drittens kein milderes, ebenso gut zur Zweckerreichung führendes Mittel besteht und viertens angemessen ist.

Im Rahmen der Prüfung der Erforderlichkeit ist durchaus der pädagogischen Einschätzung der Lehrkraft Rechnung zu tragen. Allerdings ist die Erforderlichkeit ein **Rechtsbegriff**. Sie kann nicht (allein) mit der pädagogischen Notwendigkeit begründet werden. Vielmehr kommt es zur Beurteilung der Erforderlichkeit auf die gesamten Umstände des konkreten Einzelfalles an, wobei insbesondere stets kritisch zu hinterfragen ist, ob im Einsatz der Videografie ein anderweitig nicht erzielbarer pädagogischer Mehrwert liegt.

Im Grundsatz zu bejahen ist die **Erforderlichkeit bei Videoaufnahmen während des Unterrichts für die Zwecke des Unterrichts**. Hierzu gehört etwa die Videoaufzeichnung von Übungen im Rahmen des **Rhetorik-Unterrichts** oder des **Sportunterrichts**, damit die Schülerinnen oder Schüler

durch wiederholtes Ansehen der Aufnahmen ihre (Rhetorik-, Präsentations- oder Bewegungs-)Techniken verbessern können. Ebenso gehört hierzu die Videoaufzeichnung von **Unterrichtsstunden angehender Lehrerinnen und Lehrer**, damit diese ihre **Unterrichtsgestaltung optimieren** können.

Erforderlich können hierbei **allerdings nur gelegentliche Videoaufzeichnungen** sein. Keinesfalls darf die Aufzeichnung der Unterrichtsstunden von angehenden Lehrerinnen und Lehrern, der Rhetorik-Unterrichtsstunden oder der Sportunterrichtsstunden zum Regelfall – oder auch nur zum häufigen Fall – werden.

Nicht erforderlich ist etwa auch das Filmen der Klasse, um **Fehlverhalten** (insbesondere in Abwesenheit der Lehrkraft) vorzubeugen oder zumindest aufzuklären. Hier scheint schon die Legitimität des verfolgten Ziels zweifelhaft; jedenfalls sind mildere – pädagogische – Mittel ohne weiteres denkbar.

Videografien während des Unterrichts für die Zwecke des Unterrichts **fehlt** allerdings dann regelmäßig die – als Teil der Erforderlichkeit zu prüfende – **Angemessenheit, wenn die Aufnahmen** längerfristig gespeichert und **nicht nach Beendigung der Unterrichtsstunde oder jedenfalls der** (auch mehrere Unterrichtsstunden umfassenden, thematisch zusammengehörenden) **Unterrichtseinheit gelöscht** werden. Ansonsten besteht die erhebliche Gefahr, dass die Aufnahmen ohne Einfluss- und Kontrollmöglichkeiten verbreitet werden und – gegebenenfalls auch in anderen Zusammenhängen – das Persönlichkeitsrecht der Schülerinnen und Schüler oder auch der angehenden Lehrerinnen und Lehrer beeinträchtigen.

Die Angemessenheit **fehlt** infolgedessen auch dann, wenn Videoaufnahmen im Schulunterricht Bestandteil der **Zulassungsarbeiten oder anderer Prüfungsleistungen von angehenden Lehrerinnen und Lehrern** sein sollen. Erst recht gilt dies, wenn Videografien zu **Werbe- und Imageförderungszwecken** (im Internet oder andernorts) veröffentlicht werden sollen. Schließlich fehlt die Angemessenheit, wenn beim Einsatz von Videotechnik **gänzlich unbeteiligte Schulangehörige** möglicherweise sogar unbemerkt – etwa beim Filmen innerhalb des Schulgebäudes im Rahmen eines Kunstprojekts – aufgenommen werden. Hier haben die unbeteiligten Personen auf den Umgang mit den erhobenen Daten noch weniger Einfluss als die am Projekt beteiligten Schülerinnen und Schüler oder Lehrkräfte.

Aber auch bei nur kurzfristig gespeicherten Videoaufnahmen ist die Angemessenheit **zweifelhaft**, wenn die Aufzeichnungen mit einem **Privatgerät der (angehenden) Lehrkraft** angefertigt werden oder ein schulisches Gerät zur Auswertung mit nach Hause genommen werden darf. Hier ist das Missbrauchsrisiko ebenso wie das (auch unbewusste) Verbreitungsrisiko – etwa bei Verlieren des Geräts oder bloß des Speichermediums – regelmäßig zu hoch.

— Keine Weitergabe der Videoaufzeichnung an Dritte

Art. 85 Abs. 2 BayEUG präzisiert Art. 85 Abs. 1 BayEUG dahingehend, dass die Weitergabe von Daten über Schülerinnen und Schüler und Erziehungsberechtigte an außerschulische Stellen **im Grundsatz untersagt** ist.

Ohne entsprechende datenschutzgerechte Einwilligung ist es daher regelmäßig unzulässig, dass die Schule **Videoaufzeichnungen an Dritte** herausgibt oder es gestattet, dass Dritte – etwa Sponsoren der Schule – die Schülerinnen und Schüler im Unterricht selbst filmen. Hier bildet auch das Hausrecht keine Rechtsgrundlage.

— **Keine Speicherung der Videoaufzeichnung bei Dritten**

Die Speicherung von Videoaufnahmen bei externen (Cloud-)Anbietern stellt eine **Datenverarbeitung im Auftrag** dar, die nach Art. 6 BayDSG **nur unter sehr erschwerten – tatsächlichen wie rechtlichen – Voraussetzungen zulässig** ist (siehe dazu im Einzelnen Nr. 13.3 sowie meinen 26. Tätigkeitsbericht 2014 unter Nr. 13.1). Im Schulalltag ist kaum vorstellbar, dass die vom Gesetzgeber aufgestellten hohen Anforderungen erfüllt werden können.

Ich **rate** daher allen Schulen **nachdrücklich davon ab**, im Rahmen der ohnehin datenschutzrechtlich sensiblen Videografie Dritte einzubinden.

10.3.2 Datenschutzgerechte Einwilligung

Fehlt es an den Voraussetzungen des Art. 85 Abs. 1 BayEUG, so gibt es keine Videoaufnahmen im Schulunterricht ermöglichende Rechtsvorschrift im Sinne des Art. 15 Abs. 1 Nr. 1 BayDSG. Eine Datenerhebung und -verwendung im Wege der Videografie kann daher allenfalls dann rechtmäßig sein, wenn gemäß Art. 15 Abs. 1 Nr. 2 BayDSG eine **datenschutzgerechte Einwilligung** der jeweils betroffenen Schulangehörigen vor Anfertigung der Aufnahmen eingeholt wird. Bei minderjährigen Schülerinnen und Schülern müssen dabei die Erziehungsberechtigten einwilligen, ab Vollendung des 14. Lebensjahres zusätzlich auch die Minderjährigen selbst.

Allerdings dürfen die Schulen das Instrument der Einwilligung nicht dazu nutzen, um unter **Umgehung des verfassungsrechtlichen Grundsatzes vom Vorbehalt des Gesetzes** (siehe Art. 20 Abs. 3 GG) die bestehende Befugnis des Art. 85 Abs. 1 BayEUG zu erweitern oder das Fehlen dieser Befugnis zu kompensieren. Zwischen Art. 15 Abs. 1 Nr. 1 und Nr. 2 BayDSG besteht ein **Spannungsverhältnis**. Nicht jede Datenerhebung und -verwendung, für die eine gesetzliche Rechtsgrundlage im Sinne des Art. 15 Abs. 1 Nr. 1 BayDSG fehlt, kann im Wege einer Einwilligung gemäß Art. 15 Abs. 1 Nr. 2 BayDSG gerechtfertigt werden.

Je tiefer der schulische Eingriff in das Recht am eigenen Bild ist, umso eher verbietet sich die Einholung einer Einwilligung schon deshalb, weil es in diesen Fällen dem Gesetzgeber obliegt zu entscheiden, ob die Schule einen solchen Eingriff vornehmen darf.

Liegt nach diesen Maßgaben ein Sachverhalt vor, bei dem eine Einwilligung an sich möglich ist, so muss sie insbesondere freiwillig, informiert und grundsätzlich **schriftlich** erteilt werden (Art. 15 Abs. 2 bis 4 und 7 BayDSG). An der **Freiwilligkeit** fehlt es beispielsweise, wenn die Betroffenen einem starken Gruppendruck ausgesetzt sind. Im Rahmen der **vollständigen Aufklärung** müssen die Betroffenen insbesondere darüber informiert werden, zu welchem konkreten Zweck die Videoaufnahmen gefertigt werden, in welcher Form und wie lange die Aufnahmen

gespeichert werden, wer darauf Zugriff hat und an wen sie unter Umständen weitergegeben werden. Die Betroffenen müssen somit eine konkrete Vorstellung über Ziel, Inhalt, Ablauf und Umfang der Datenerhebung und -verwendung erhalten können. Besonders wichtig ist zudem gerade in einem Abhängigkeitsverhältnis – in dem sich Schülerinnen und Schüler in der Schule stets befinden – der Hinweis darauf, dass die Einwilligung ohne Angabe von Gründen und **ohne nachteilige Folgen verweigert sowie jederzeit widerrufen** werden kann. Dies gilt insbesondere bei Schulveranstaltungen mit Teilnahmepflicht.

Allerdings rate ich von der Einholung entsprechender Einwilligungen generell ab. Aus diesem Grund stellen auch die mit mir abgestimmten, vom Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst den staatlichen Schulen zur Verwendung vorgegebenen und den kommunalen Schulen sowie den staatlich anerkannten Ersatzschulen zur Verwendung empfohlenen **Musterformulare für die Einwilligung in die Veröffentlichung von personenbezogenen Daten (einschließlich Fotos)** jeweils ausdrücklich klar, dass „Ton-, Video- und Filmaufnahmen … von dieser Einwilligung nicht umfasst" sind.

Meine ablehnende Haltung begründe ich damit, dass der Grundrechtseingriff durch Videografie – also die grundsätzlich dauerhafte Erhebung und Speicherung bewegter Bilder – stets einen **erheblichen Eingriff** in das Recht am eigenen Bild darstellt. Bewegte Bilder sind in der Regel aussagekräftiger als (bloße) Fotoaufnahmen. Der durch sie transportierte Informationsgehalt ist aus der Kombination von Bild, Ton und Bewegung über einen längeren Zeitraum besonders hoch. Gerade die Aufzeichnung von Wortbeiträgen der Schülerinnen und Schüler während des Unterrichts, die möglicherweise in Art. 15 Abs. 7 BayDSG besonders geschützte politische Meinungsäußerungen sowie religiöse oder philosophische Überzeugungen berühren, kann **tiefgehende Einblicke in die „Innenwelt" der Betroffenen** geben und deren ungestörte Überzeugungs- und Meinungsbildung erheblich beeinträchtigen. Videoaufzeichnungen sind gerade auch in diesen Fällen geeignet, die Wahrnehmung der gefilmten Person durch andere auf Dauer zu festigen und ein Vergessen ebenso wie eine spätere Distanzierung des Betroffenen „von sich selbst" zu erschweren.

10.3.3 Praxisrelevante Einzelfälle

Schließlich möchte ich noch auf folgende Fallgestaltungen, die mir im Rahmen meiner Kontrolltätigkeit im gegenständlichen Zusammenhang bekannt geworden sind, näher eingehen:

– Überraschende Videoaufzeichnung im Rahmen eines Kunstprojekts

  Im Rahmen eines schulischen Kunstprojekts wurden die Gänge des Schulgebäudes und die sich dort vereinzelt aufhaltenden Lehrkräfte sowie Schülerinnen und Schüler „überfallartig" gefilmt. Teilweise öffnete die Projektgruppe auch überraschend die Türen der Klassenzimmer und zeichnete die Lehrkraft sowie die Schülerinnen und Schüler im Unterricht „blitzartig" auf. Dass in solchen Fällen jedenfalls die **Erforderlichkeit** der Datenerhebung und -verwendung im Sinne des Art. 85 Abs. 1 Satz 1 BayEUG **fehlt**, habe ich bereits oben unter Nr. 10.3.1 dargelegt.

  Ohne Einwilligung aller erfassten – genauer: potentiell erfassbaren – Personen ist daher eine Videoaufzeichnung keinesfalls zulässig. Allerdings

dürfte die Einholung aller notwendigen Einwilligungen in der Praxis schon tatsächlich kaum möglich sein. Der Eingriff wiegt zudem so schwer, dass vieles dafür spricht, dass die fehlende gesetzliche Rechtsgrundlage im Sinne des Art. 15 Abs. 1 Nr. 1 BayDSG auch rechtlich **nicht** durch eine **Einwilligung** gemäß Art. 15 Abs. 1 Nr. 2 BayDSG „aufgefangen" werden kann.

Die besondere Schwere des Eingriffs resultiert gerade aus der **überraschenden, oftmals sogar (zunächst) unbemerkten filmischen Erfassung unbeteiligter Schulangehöriger**. Diese Vorgehensweise ist besonders geeignet, einen nicht gewollten und ungünstigen Eindruck von den Betroffenen entstehen zu lassen und zu verfestigen. Hinzu kommt, dass die Kontrolle über die Aufzeichnung denkbar gering ist. Schülerinnen und Schüler einer anderen Klasse und andere Lehrkräfte haben das Projekt zu verantworten. Die Gefahr ist groß, dass allein durch den Zugriff aller Projektteilnehmerinnen und -teilnehmer die Filme zweckwidrig verwendet werden.

— **Aufzeichnung der Mitglieder einer Filmprojektgruppe**

Dreht eine Projektgruppe mit und über ihre Mitglieder einen Film – etwa um andere Schülerinnen und Schüler zu werben oder um die thematische Breite der eigenen Schule einer größeren Öffentlichkeit zu präsentieren –, so ist der Eingriff ebenfalls erheblich. Zwar ist die Aufnahme nicht überraschend, so dass jede betroffene Person über die Art und Weise ihrer Erfassung und ihrer Handlungen eine gewisse Kontrolle ausüben kann. Ein unkontrolliertes Verbreitungsrisiko besteht aber dennoch, da die Filme gerade längerfristig gespeichert und im Zweifel andernorts auch vorgeführt werden sollen.

Soweit aber Unbeteiligte nicht aufgezeichnet werden, die Teilnahme an der Projektgruppe nicht Pflicht ist und besonders darauf geachtet wird, dass kein auf die Einwilligungserteilung gerichteter Gruppendruck entsteht, ist eine **datenschutzgerechte Einwilligung** bei Beachtung der übrigen, oben unter Nr. 10.3.2 im Einzelnen dargestellten Vorgaben **grundsätzlich möglich**.

Dennoch rate ich aus den genannten Gründen von der Einholung entsprechender Einwilligungen auch in diesen Fällen ab.

— **Videoaufnahmen im Schulunterricht durch Dritte (Sponsoren)**

Sollen Aufzeichnungen über besondere Schulveranstaltungen oder schulische Projektgruppen durch Dritte – wie etwa Sponsoren – angefertigt werden und diesen sogar die Verwertungsrechte übertragen werden, so ist hierin eine **Einwilligung im Hinblick auf das umfassende Kontrolldefizit nicht möglich**.

10.4 „Sponsoring" von Klassenfotos

Mit der datenschutzrechtlichen Problematik der **Weitergabe von Schülerdaten zu Werbezwecken** habe ich mich bereits in meinem 24. Tätigkeitsbericht 2010 unter Nr. 10.4 kritisch auseinandergesetzt. Den Themenkomplex der **Erstellung**

und Verwendung von Schülerfotos habe ich zuletzt in meinem 26. Tätigkeitsbericht 2014 unter Nr. 10.4 aus Datenschutzsicht umfassend beleuchtet.

Zu den in diesen beiden Beiträgen behandelten Fragestellungen erreichten mich auch im aktuellen Berichtszeitraum wieder **zahlreiche schriftliche und telefonische Eingaben und Anfragen**.

An dieser Stelle greife ich nur eine **besonders bemerkenswerte Fallkonstellation** heraus, die beide Themenkreise gleichermaßen betrifft.

10.4.1 Sachverhalt

Eine besorgte Mutter schilderte mir, dass ihr Sohn, ein Schüler der ersten Klasse einer staatlichen Grundschule, eines Tages einen von einer örtlichen Bank ausgestellten „Abholschein" mit nach Hause brachte. **Bei Vorlage des „Abholscheins"** sollte die Mutter **von der Bank kostenlos ein Klassenfoto** ihres Sohnes erhalten. Das Klassenfoto war zuvor in der Schule **von einem professionellen Fotografen auf Kosten der Bank angefertigt** worden. Auf dem „Abholschein" waren allerdings **der Name und der Vorname, die Anschrift, die Grundschule und die Klasse sowie das Geburtsdatum des Schülers einzutragen**. Ein Vermerk im „Kleingedruckten" besagte zudem, dass mit der Vorlage des „Abholscheins" **gegenüber der Bank das Einverständnis mit der Speicherung dieser Schülerdaten** erteilt wird.

10.4.2 Datenschutzrechtliche Bewertung

Ebenso wie für die Bank mag auch für die Grundschule die geschilderte Vorgehensweise **auf den ersten Blick** als eine **„Win-win-Situation"** erscheinen: Die Schule eröffnet ohne großen Aufwand den Erstklässlern und deren Erziehungsberechtigten die Möglichkeit, kostenfrei hochwertige Klassenfotos zu beziehen. Die Bank erhält im Gegenzug – neben der Möglichkeit, sich in der Grundschule darzustellen – zahlreiche Schülerdaten zur späteren Ansprache und Kontaktpflege.

Bei genauer Betrachtung erweist sich das dargestellte **„Sponsoring" von Klassenfotos durch die Bank** jedoch als **rechtlich sehr bedenklich**. Gegenüber der Grundschule habe ich daher dieses „Sponsoring" von Klassenfotos datenschutzrechtlich – kurz zusammengefasst – wie folgt bewertet:

– **Klassenfotos** enthalten umfangreiche **personenbezogene Daten** im Sinne des Art. 4 Abs. 1 BayDSG. Die schulische Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind gemäß Art. 15 Abs. 1 BayDSG nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder anordnet (Nr. 1) oder der Betroffene eingewilligt hat (Nr. 2).

  Eine **gesetzliche Verpflichtung der Erstklässler, sich von einem** – zudem auch noch im Auftrag einer Bank handelnden – **Fotografen** ohne Einwilligung ihrer Eltern **aufnehmen zu lassen, besteht nicht**. Für die damit verbundenen Erhebungen und Verwendungen von Schülerdaten existiert keine Rechtsgrundlage; insbesondere liegen hier die Voraussetzungen des Art. 85 Abs. 1 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG) nicht vor.

— Zwar gibt die Grundschule die **mittels der „Abholscheine“** geforderten personenbezogenen Schülerdaten nicht direkt an die Bank weiter. Allerdings veranlasst sie die Erziehungsberechtigten, mit den Schülerdaten zu „bezahlen“, um an das Bild des eigenen Kindes zu gelangen. Diese Vorgehensweise ist einer **Übermittlung der Schülerdaten durch die Grundschule an die Bank** gleichzustellen.

  Im Hinblick auf das in Art. 84 Abs. 1 BayEUG vom bayerischen Gesetzgeber aufgestellte Verbot der kommerziellen Werbung an Schulen ist eine solche Datenübermittlung an eine außerschulische Stelle gemäß Art. 85 Abs. 2 BayEUG allerdings ohne Einwilligung der Eltern **unzulässig**.

— Die mit der „Sponsoring“-Aktion verbundenen vielfältigen Erhebungen und Verwendungen von Schülerdaten könnten daher **allenfalls mit datenschutzgerechter** – also schriftlicher, informierter, freiwilliger und widerruflicher – **Einwilligung** der Betroffenen im Sinne des Art. 15 Abs. 2 bis 4 und 7 BayDSG zulässig sein. Bei Erstklässlern können allein die **Erziehungsberechtigten** einwilligen. Die Einwilligungen müssen dabei **im Vorhinein** erteilt werden.

  Entsprechende Einwilligungen hat die Grundschule bei den Eltern jedoch **nicht eingeholt**.

  Insbesondere konnte eine datenschutzgerechte Einwilligung **nicht mit dem Ausfüllen des „Abholscheins“** erteilt werden. Zum einen wäre eine solche Erklärung zu spät gekommen, weil sie dem Fotografieren zeitlich nachgelagert ist. Zum anderen wäre diese Erklärung auch nicht freiwillig gewesen, weil die Erziehungsberechtigten von der Schule einer **„Nötigungssituation“** ausgesetzt wurden. Ohne Ausfüllen des „Abholscheins“ bliebe das rechtswidrig gefertigte Bild ihres Kindes nämlich vollständig im Einflussbereich der Bank. Darüber hinaus würden die Eltern dann auch **überhaupt kein Klassenfoto** ihres Kindes erhalten; denn anderweitig ist das Klassenfoto nicht – auch nicht gegen Entgelt – erhältlich.

10.4.3 Ergebnis

Aufgrund meiner datenschutzrechtlichen Bewertung trat die Grundschule umgehend an die Bank heran. Sie konnte erreichen, dass **die bei der Bank noch vorhandenen Klassenfotos und die bereits eingereichten „Abholscheine“ vernichtet** wurden.

In den folgenden Schuljahren nahm die Grundschule sodann **bei der Erstellung von Klassenfotos das „Sponsoring“ der Bank nicht mehr** in Anspruch.

10.5 Videoüberwachung des Kollegstufencafés

Mit der datenschutzrechtlichen Problematik der Videoüberwachung an bayerischen öffentlichen – staatlichen wie kommunalen – Schulen habe ich mich in meinen Tätigkeitsberichten bereits mehrfach eingehend auseinandergesetzt (siehe 26. Tätigkeitsbericht 2014 unter Nr. 10.9, 25. Tätigkeitsbericht 2012 unter Nr. 10.5 sowie 23. Tätigkeitsbericht 2008 unter Nr. 12.2). Dabei habe ich stets auf

die engen rechtlichen Voraussetzungen hingewiesen, unter denen Videoüberwachung an Schulen überhaupt möglich ist. **In meiner Kontroll- und Beratungspraxis muss ich** jedoch immer wieder **feststellen, dass Schulen bei der Videoüberwachung die strengen rechtlichen Vorgaben nicht – oder jedenfalls nicht vollumfänglich – beachten**.

Aus dem aktuellen Berichtszeitraum greife ich nur einen **besonders markanten Einzelfall** heraus, auf den mich ein besorgter Erziehungsberechtigter aufmerksam gemacht hatte:

10.5.1 Sachverhalt

Ein staatliches Gymnasium hatte gleich in mehreren Bereichen des Schulgebäudes – darunter insbesondere auch **im Kollegstufencafé – Videokameras installiert**. Die von den Videokameras erzeugten **Bilder** wurden dabei **direkt auf** einen **Bildschirm im Eingangsbereich der Schule übertragen**, sodass sie für einen unüberschaubaren Personenkreis – Schülerinnen und Schüler, Lehrkräfte und Verwaltungspersonal, Reinigungskräfte und Lieferanten, Erziehungsberechtigte und weitere Personen – uneingeschränkt einsehbar waren.

Bereits nach kurzer Zeit waren daher die Aufnahme und die Übertragung der Videobilder **schulintern** auf **erheblichen Widerstand** gestoßen. Daraufhin hatte die Schulleitung die **Übertragung der Bilder in den Eingangsbereich eingestellt**. **Stattdessen** erfolgte nun während des Unterrichts eine **Direktübertragung des Videosignals auf einen Monitor in den Räumen der Schulleitung**; außerhalb der Unterrichtszeiten wurde das Videosignal aufgezeichnet und drei Wochen lang gespeichert.

Insoweit hielt die Schulleitung die Videoüberwachung des Kollegstufencafés weiterhin mit der Begründung für geboten, man könne die Schülerinnen und Schüler dort schließlich „nicht sich selbst überlassen“, aber auch „nicht dauernd Lehrer patrouillieren lassen“. Vielmehr sei die Videoüberwachung zur Erfüllung der Aufsichtspflicht und damit zum Schutz der Personen, die sich im Kollegstufencafé aufhielten, unerlässlich. Mit dem bestehenden, ohnehin knappen Stundenkontingent der Lehrerschaft könne die Beaufsichtigung aus Sicht der Schulleitung nicht abgedeckt werden.

10.5.2 Rechtslage

In schul- und datenschutzrechtlicher Hinsicht ist eine **Videoüberwachung an öffentlichen** – staatlichen wie kommunalen – **Schulen** von vornherein **nur in engen Grenzen zulässig**. Insbesondere gilt hier:

— Sowohl die Videobeobachtung als auch die Videoaufzeichnung unterliegen zunächst den **strengen gesetzlichen Voraussetzungen des Art. 21a BayDSG**.

  So sind nach Art. 21a Abs. 1 Satz 1 BayDSG die Videobeobachtung und die Videoaufzeichnung nur zulässig, soweit dies **zum Schutz der dort aufgezählten Rechtsgüter erforderlich** ist.

Art. 21a BayDSG Videobeobachtung und Videoaufzeichnung (Videoüberwachung)
(1) [1]Mit Hilfe von optisch-elektronischen Einrichtungen sind die Erhebung (Videobeobachtung) und die Speicherung (Videoaufzeichnung) personenbezogener Daten zulässig, wenn dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts erforderlich ist,

1. *um Leben, Gesundheit, Freiheit oder Eigentum von Personen, die sich im Bereich öffentlicher Einrichtungen, öffentlicher Verkehrsmittel, von Dienstgebäuden oder sonstigen baulichen Anlagen öffentlicher Stellen oder in deren unmittelbarer Nähe aufhalten, oder*
2. *um Kulturgüter, öffentliche Einrichtungen, öffentliche Verkehrsmittel, Dienstgebäude oder sonstige bauliche Anlagen öffentlicher Stellen sowie die dort oder in deren unmittelbarer Nähe befindlichen Sachen*

zu schützen. [2]Es dürfen keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen der Betroffenen beeinträchtigt werden.

— Weitere Einschränkungen für die Videoaufzeichnung an öffentlichen Schulen legt die **Anlage 8 „Videoaufzeichnung an Schulen" der** vom Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst erlassenen **Verordnung zur Durchführung des Art. 28 Abs. 2 des Bayerischen Datenschutzgesetzes (DVBayDSG-KM)** fest.

  Danach darf eine Videoaufzeichnung beispielsweise nur Personen betreffen, die sich im **Eingangsbereich der Schule** aufhalten oder sich zwischen 22:00 Uhr und 6:30 Uhr außerhalb von schulischen oder sonstigen von der Schule zugelassenen Veranstaltungen auf dem Schulgelände befinden; darüber hinaus ist eine Aufzeichnung nur außerhalb von schulischen oder sonstigen von der Schule zugelassenen Veranstaltungen an Feiertagen, an Wochenenden oder in den Ferien auf dem Schulgelände zulässig (siehe Nr. 2.5 der Anlage 8 DVBayDSG-KM).

— Im Hinblick darauf, dass die Videoüberwachung nach Art. 21a Abs. 1 Satz 1 BayDSG zum Schutz der dort genannten Rechtsgüter erforderlich sein muss, hat die Schule aufgrund ihrer pädagogischen Verantwortung ein hohes Maß an Sensibilität zu zeigen und insbesondere **sorgfältig zu prüfen, ob nicht andere Aufsichts- und Überwachungsmaßnahmen sowie sonstige – insbesondere pädagogische – Mittel ausreichen**.

— Darüber hinaus dürfen **keine Anhaltspunkte** dafür bestehen, dass durch die Videoüberwachung **überwiegende schutzwürdige Interessen** insbesondere der Schülerinnen und Schüler sowie der Lehrkräfte **beeinträchtigt** werden (Art. 21a Abs. 1 Satz 2 BayDSG).

— Die **Videoüberwachung** und die erhebende Stelle sind zudem gemäß Art. 21a Abs. 2 BayDSG **durch geeignete Maßnahmen** (vor allem Hinweisschilder) **erkennbar zu machen**.

— **Spätestens drei Wochen nach der Datenerhebung** sind die **Videoaufzeichnungen** und daraus gefertigte Unterlagen **zu löschen**, soweit sie nicht zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten oder zur Geltendmachung von Rechtsansprüchen benötigt werden (siehe Art. 21a Abs. 5 BayDSG sowie Nr. 5 der Anlage 8 DVBayDSG-KM).

– Schließlich ist es aus Gründen der Transparenz und zur Förderung der Akzeptanz einer derart gravierenden Maßnahme ratsam, den **Elternbeirat** – und gegebenenfalls auch das **Schulforum** – rechtzeitig in den Entscheidungsprozess **einzubeziehen**.

  Dem **Personalrat** steht in der Regel ohnehin nach Art. 75a Abs. 1 Nr. 1 Bayerisches Personalvertretungsgesetz (BayPVG) bei der Videoüberwachung ein **gesetzliches Mitbestimmungsrecht** zu. Wie stets empfehle ich in einem solchen Mitbestimmungsfall den Abschluss einer **Dienstvereinbarung** im Sinne des Art. 73 BayPVG.

10.5.3 Rechtsdurchsetzung

Im eingangs geschilderten Fall habe ich umgehend das **Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst gebeten**, aufgrund seiner datenschutzrechtlichen Gesamtverantwortung für den Geschäftsbereich gemäß Art. 25 Abs. 1 BayDSG auf die Einhaltung der schuldatenschutzrechtlichen Vorgaben für die Videoüberwachung bei dem betroffenen staatlichen Gymnasium hinzuwirken.

Im Rahmen seiner ausführlichen rechtlichen Hinweise gab das Kultusministerium daraufhin der Schulleitung konkret in Bezug auf die **Videoüberwachung im Kollegstufencafé** auf, eingehend zu prüfen, ob **aufgrund von Erfahrungswerten aus der Vergangenheit** tatsächlich der Schluss gerechtfertigt ist, dass gerade hier eine **Verletzung von Rechtsgütern wahrscheinlich** ist. Hierfür wäre erforderlich, dass es in der Vergangenheit im Kollegstufencafé selbst zu erheblichen Rechtsgutsverletzungen gekommen ist. Die **geforderten Angaben** konnte die **Schulleitung** allerdings – auch nach wiederholter Aufforderung durch das Kultusministerium – **nicht beibringen**.

Zudem forderte das Kultusministerium die Schulleitung auf, die **Angemessenheit der Videoüberwachung zu begründen**. Dabei gab das Kultusministerium der Schulleitung insbesondere zu bedenken, dass sich in einem Kollegstufencafé Schülerinnen und Schüler **typischerweise über einen längeren Zeitraum aufhalten und auch private Verhaltensweisen zeigen**. Der Eingriff in das Recht auf informationelle Selbstbestimmung sei daher ungleich gewichtiger als beispielsweise bei einer Videoüberwachung des Eingangsbereichs, in welchem sich die betroffenen Personen regelmäßig nur kurzzeitig aufhalten. Zu der entsprechenden Begründung sah sich die **Schulleitung** wiederum **nicht im Stande**.

Aber auch im Übrigen konnte die **Schulleitung** die **Erforderlichkeit einer Videoüberwachung** des Kollegstufencafés **nicht nachvollziehbar darlegen**. Insoweit hielt das **Kultusministerium** der Schulleitung vor allem entgegen, dass es schon **aus pädagogischen Erwägungen möglich sein müsse, der schulischen Aufsichtspflicht auf andere Weise zu genügen**.

Nach geraumer Zeit teilte mir das Kultusministerium schließlich mit, dass das **betreffende staatliche Gymnasium** nicht nur die Videoüberwachung des Kollegstufencafés eingestellt habe, sondern **künftig generell auf dem gesamten Schulgelände sowohl auf Videobeobachtungen als auch auf Videoaufzeichnungen verzichte**.

10.5.4 Fazit

Abschließend möchte ich aus Datenschutzsicht noch einmal betonen, dass die **Installation von Videokameras im Schulbereich** einen **intensiven Eingriff in das Persönlichkeitsrecht** insbesondere der Schülerinnen und Schüler sowie der Lehrerinnen und Lehrer bedeutet und ein **nicht unproblematisches Signal an die Schulgemeinschaft, aber auch an die Öffentlichkeit** sendet.

Die **Schulen müssen** daher bei der Beurteilung der Frage, ob die Anbringung einer Kamera im konkreten Fall tatsächlich erforderlich ist – also objektiv geeignet und im Verhältnis zu dem angestrebten Zweck auch angemessen – oder ob nicht andere, insbesondere pädagogische Maßnahmen ausreichen, gerade **aufgrund ihrer pädagogischen Verantwortung** ein **hohes Maß an Sensibilität** zeigen.

Gerade vor diesem Hintergrund freue ich mich, dass das **Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst meine Haltung** zur Videoüberwachung an Schulen – nicht nur in dem geschilderten Fall – **vollumfänglich teilt**.

10.6 Datenschutz bei der Bayerischen Landesstelle für den Schulsport

Die Bayerische Landesstelle für den Schulsport (im Folgenden: Landesstelle) ist eine bayernweit zentrale, dem Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst direkt nachgeordnete staatliche Behörde. Sie versteht sich als Serviceeinrichtung für die Schulen – für Schulleitungen und für Sportlehrkräfte ebenso wie für Schülerinnen und Schüler. Zu den **Kernaufgaben der Landesstelle** gehört die **bayernweite Steuerung und Koordinierung der schulsportlichen Wettbewerbe**. Die Landesstelle wird dabei von etwa 90 Arbeitskreisen auf Schulamtsebene sowie von Bezirksausschüssen und von einem Landesausschuss unterstützt. Mitglieder der Arbeitskreise sind jeweils mehrere Kreisschulobleute, die als Ansprechpartner für die jeweilige Sportart fungieren und jährlich die schulsportlichen Wettbewerbe auf Kreisebene planen, organisieren und durchführen.

Im Berichtszeitraum wandte sich nun ein Sportlehrer einer bayerischen öffentlichen Schule an mich, der für seine Schule bei der Landesstelle Schulsportmannschaften zu schulsportlichen Wettbewerben anmelden wollte.

10.6.1 Ausgangssituation

— Wie der Sportlehrer schilderte, erfolge die **Anmeldung der Schulsportmannschaften** zu den schulsportlichen Wettbewerben mittels eines Online-Verfahrens, das **in einem internen, passwortgeschützten Bereich der Homepage der Landesstelle** bereitgestellt werde.

  Der Zugang zu diesem internen Bereich erfordere zwar die Eingabe eines Usernamens und eines Passwortes. Allerdings werde in den Anmeldehinweisen auf dem weltweit frei einsehbaren Bereich der Homepage der für alle Anmeldungen einheitlich vorgegebene und ausschließlich zu verwendende Username ausdrücklich genannt. Da zudem als Passwort nur die jeweilige Schulnummer einzugeben sei, die etwa über die Homepage des Kultusministeriums ebenfalls frei in Erfahrung zu bringen sei, könne sich **faktisch jedermann ohne größeren Aufwand Zugang zu dem internen**

Bereich der Homepage verschaffen und Einsicht in die dort vorgehaltenen Dokumente nehmen.

— Der Sportlehrer führte weiter aus, dass jede betreuende Lehrkraft **für die Anmeldung** einer Schulsportmannschaft zu einem schulsportlichen Wettbewerb in einem Online-Formular auf der Homepage der Landesstelle zahlreiche personenbezogene Daten angeben müsse.

  Abgefragt würden unter anderem – als Pflichtfelder gekennzeichnet – **Name und Privatdresse sowie private Telefonnummer(n) und private E-Mail-Adresse der betreuenden Lehrkraft**.

  Zudem müssten die Lehrkräfte **zwingend auch in die Veröffentlichung ihrer privaten Kommunikationsdaten** auf der Homepage der Landesstelle **einwilligen**.

— Nach weiterer Darstellung des Sportlehrers könnten über den internen Bereich der Homepage der Landesstelle aber nicht nur Schulsportmannschaften für Schulsportwettbewerbe angemeldet werden. Vielmehr sei hier unter anderem auch der **Zugriff auf einen sogenannten Personenpool** möglich.

  In diesem Personenpool würden – unabhängig davon, mit welcher Schulnummer man sich angemeldet habe – **bayernweit die Namen aller Kreisschulobleute mit privaten Telefonnummern, Privatadressen und privaten E-Mail-Adressen** aufgelistet. **Insgesamt über 1.700 Datensätze** seien damit ohne größeren Aufwand **weltweit frei einsehbar**.

Aufgrund der detaillierten Schilderungen des Sportlehrers erschien mir bereits zweifelhaft, ob die Erhebung der genannten personenbezogenen Daten der betreuenden Lehrkräfte in dem dargestellten Umfang tatsächlich für die Aufgabenerfüllung der Landesstelle erforderlich war. Vor allem hielt ich es aber für fraglich, ob tatsächlich sämtliche Betroffenen in die faktisch weltweite Veröffentlichung ihrer privaten Kommunikationsdaten wirksam eingewilligt hatten.

10.6.2 Mängelbehebung

Unter Darstellung der genannten Problempunkte habe ich mich umgehend an das **Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst** gewandt. Dabei habe ich das Kultusministerium gebeten, aufgrund seiner datenschutzrechtlichen Gesamtverantwortung für den Geschäftsbereich gemäß Art. 25 Abs. 1 BayDSG die Beachtung der datenschutzrechtlichen Vorschriften bei der Landesstelle sicherzustellen.

Nach mehrjährigem Abstimmungsprozess mit der Landesstelle hat mir das Kultusministerium schließlich mitgeteilt, dass als Reaktion auf mein Tätigwerden **insbesondere folgende Maßnahmen umgesetzt** worden seien:

— Für die **Anmeldung einer Schulsportmannschaft** zu einem schulsportlichen Wettbewerb sei künftig lediglich die Angabe der dienstlichen Kommunikationsdaten der betreuenden Lehrkraft notwendig.

Hinsichtlich der **Angabe privater Daten** der betreuenden Lehrkraft werde nunmehr explizit auf die **Freiwilligkeit** hingewiesen.

Der **Einblick** in die Meldungen der Schulsportmannschaften sei im Übrigen **nur noch mit Administratorrechten** möglich.

— Im **Personenpool** sei künftig lediglich die Veröffentlichung der dienstlichen Kontaktdaten der Kreisschulobleute verpflichtend.

Die **Angabe privater Daten** sei hingegen **freiwillig**. Vor der Veröffentlichung privater Daten müssten daher entsprechende Einwilligungen eingeholt werden.

— Zunächst offen blieb indes die Frage nach dem **Zugangsschutz des internen Bereichs** der Homepage der Landesstelle. Dies betraf insbesondere den Personenpool, der zwischenzeitlich sogar zeitweise von dem öffentlich zugänglichen Bereich der Homepage – also ohne jegliche vorherige Anmeldung (!) – abrufbar war.

Zwar konnte mir das Kultusministerium die Erforderlichkeit der Vorhaltung des Personenpools auf der Homepage der Landesstelle zur Planung, Organisation und Durchführung der Schulsportwettbewerbe nachvollziehbar darlegen. Ich musste aber mehrfach anmahnen, den Personenpool in einen auch tatsächlich wirksam passwortgeschützten Bereich der Homepage einzustellen.

Die Landesstelle ist dem schließlich nachgekommen und hält (jedenfalls) den **Personenpool** nunmehr **in einem (neuen) internen passwortgeschützten Bereich** vor, auf den nur noch über ein Double-Opt-In-Verfahren per zertifizierter E-Mail-Adresse nach vorheriger Anmeldung zugegriffen werden kann.

10.6.3 Ausblick

Gegen Ende des Berichtszeitraums hat mir das Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst mitgeteilt, dass der **Zugang zum Anmeldeverfahren** – zur Erhöhung der Datensicherheit – **künftig völlig neu gestaltet** werden soll. Ich habe insoweit empfohlen, zumindest schulbezogene Benutzerkennungen und für Außenstehende nicht erschließbare, mindestens jährlich zu wechselnde Passwörter zu verwenden. Ferner habe ich geraten, die Kenntnis der Zugangsdaten innerhalb der jeweiligen Schule zuverlässig auf die Personen zu beschränken, welche das betreffende Angebot der Landesstelle jeweils für ihre konkrete Aufgabenstellung benötigen.

Insgesamt konnte durch kontinuierliche Begleitung und Beratung der beteiligten öffentlichen Stellen **letztlich** eine **aus Datenschutzsicht befriedigende Situation** erreicht werden. Gleichwohl zeigt der Fall beispielhaft, dass die Sensibilität für Fragen des Datenschutzes mancherorts noch ausbaubar ist.

10.7 Staatliche Schulaufsicht über private Grundschulen und Mittelschulen

Im Rahmen meiner datenschutzrechtlichen Kontrolltätigkeit bin ich darauf aufmerksam gemacht worden, dass **offenbar bayernweit seit Jahren wesentliche Aufgaben der staatlichen Schulaufsicht über private Grundschulen und Mittelschulen statt von den gesetzlich dafür zuständigen Regierungen faktisch von den Staatlichen Schulämtern wahrgenommen** werden. Mit der Erfüllung der vielfältigen Aufgaben der staatlichen Schulaufsicht sind insbesondere umfangreiche Erhebungen, Nutzungen und Verarbeitungen von zahlreichen Lehrer-, Eltern- und Schülerdaten verbunden. Daher ist eine solche Verfahrensweise auch unter Datenschutzaspekten problematisch.

Im Einzelnen:

10.7.1 Gesetzliche Zuständigkeit allein bei Regierungen

Nach der abschließenden gesetzlichen Zuständigkeitsregelung des Art. 114 Abs. 1 Nr. 4 Buchst. b) Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen (BayEUG) **obliegt die unmittelbare staatliche Schulaufsicht bei privaten Grundschulen und Mittelschulen den Regierungen**. Für die unmittelbare staatliche Schulaufsicht bei öffentlichen Grundschulen und Mittelschulen sind dagegen gemäß Art. 114 Abs. 1 Nr. 5 Buchst. a) BayEUG die Staatlichen Schulämter zuständig.

Art. 114 BayEUG Sachliche Zuständigkeit
(1) Die unmittelbare staatliche Schulaufsicht obliegt
1. dem Staatsministerium bei Gymnasien, Fachoberschulen, Berufsoberschulen, Realschulen einschließlich der entsprechenden Schulen zur sonderpädagogischen Förderung und der Schulen, die ganz oder teilweise die Lernziele der vorgenannten Schulen verfolgen,
2. dem Staatsministerium für Ernährung, Landwirtschaft und Forsten bei Schulen in seinem Geschäftsbereich,
3. dem Staatsministerium der Justiz im Einvernehmen mit dem Staatsministerium bei Unterrichtseinrichtungen in Justizvollzugsanstalten sowie in haftersetzenden Maßnahmen nach §§ 71, 72 des Jugendgerichtsgesetzes,
4. den Regierungen
a) bei öffentlichen Grundschulen und Mittelschulen für die schulaufsichtliche Genehmigung von Neu-, Um- und Erweiterungsbauten,
b) bei privaten Grundschulen und Mittelschulen,
c) bei Förderschulen (einschließlich der zugehörigen Einrichtungen der Mittagsbetreuung), soweit die Schulaufsicht nicht durch Nr. 1 oder 4 Buchst. d geregelt ist,
d) bei Berufsschulen, Berufsfachschulen, Wirtschaftsschulen, Fachschulen und Fachakademien einschließlich der entsprechenden Schulen zur sonderpädagogischen Förderung,
e) bei Schulen für Kranke,
f) bei Ergänzungsschulen unbeschadet der Regelung in Nr. 1,
g) bei Sing- und Musikschulen,
h) bei Lehrgängen in Verbindung mit dem Bayerischen Rundfunk (Telekolleg),
i) bei Lehrgängen, wenn diese von kommunalen Trägern oder von staatlich verwalteten Stiftungen errichtet oder betrieben werden,
5. den Schulämtern

a) bei öffentlichen Grundschulen und Mittelschulen,
b) bei Einrichtungen der Mittagsbetreuung, soweit nicht in Nr. 4 Buchst. c geregelt,

6. den Kreisverwaltungsbehörden bei Lehrgängen, soweit sie nicht in Nr. 4 Buchst. g, h und i und Abs. 2 genannt sind.

10.7.2 Tatsächliche Aufgabenwahrnehmung durch Schulämter

Nach meinen Informationen bedienen sich allerdings **in der Praxis** die Regierungen bei der Wahrnehmung ihrer schulaufsichtlichen Tätigkeit über private Grundschulen und Mittelschulen in weitem Umfang der Staatlichen Schulämter.

Wie mir aus dem Kreis der Regierungen ausdrücklich bestätigt wurde, würden in Anbetracht der Vielzahl der vorhandenen privaten Grundschulen und Mittelschulen, die zudem oftmals räumlich weiter entfernt von der jeweiligen Regierung gelegen seien, die **örtlichen Schulämter aus Praktikabilitätsgründen „gebeten", verschiedene Aufgaben der Schulaufsicht „für die Regierung" wahrzunehmen**.

Die Tätigkeit der Schulämter reiche dabei von **Ortsbesichtigungen** über **unangekündigte Besuche**, etwa aufgrund von Beschwerden, bis hin zur **Bearbeitung sensibler Vorgänge**, bei denen die Schulämter insbesondere auch mit personenbezogenen Daten sowohl von Lehrkräften als auch von Schülerinnen und Schülern sowie von Erziehungsberechtigten der privaten Grundschulen und Mittelschulen umgehen würden. Die Schulämter nähmen etwa **Einsicht in Schülerakten**; sie würden aber beispielsweise auch bei der **Feststellung der persönlichen Eignung von Lehrkräften** tätig.

10.7.3 Art und Umfang der Aufgabenerfüllung durch Schulämter – Erkenntnisse des Kultusministeriums

Aufgrund dieser auch datenschutzrechtlich bedeutsamen Informationen habe ich das Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst um Stellungnahme zu der Frage gebeten, inwieweit nach dortigen Erkenntnissen die Staatlichen Schulämter im Bereich der den Regierungen obliegenden Schulaufsicht über private Grundschulen und Mittelschulen tätig sind.

Das **Kultusministerium** hat in seiner ausführlichen Stellungnahme **bestätigt**, dass die **Staatlichen Schulämter** die Regierungen **bei der Schulaufsicht über private Grundschulen und Mittelschulen** in **zahlreichen, wesentlichen Aufgaben** unterstützen. Nach Befragung aller Regierungen nannte das Kultusministerium dabei in einer – nicht abschließenden – Aufzählung **insbesondere folgende Tätigkeitsbereiche**:

— Beratung der Träger und Leitungen privater Grundschulen und Mittelschulen vor Ort und Inanspruchnahme von staatlichen Beratungsdiensten,

— Überprüfung der fachlichen Qualifikation und pädagogischen Eignung des privat angestellten Lehrpersonals,

— Zuständigkeit für an private Schulen zugeordnetes staatliches Lehrpersonal (einschließlich Beurteilung),

- Versorgung der Schule mit Lehrpersonal zur fachgerechten Umsetzung des Lehrplans,

- Umsetzung des schulaufsichtlich genehmigten pädagogischen Konzepts,

- Mitwirkung bei Fragen zur Erfüllung der Tatbestandsvoraussetzungen einer staatlichen Anerkennung,

- Überprüfung von Auflagen aus den Genehmigungsbescheiden vor Ort,

- Überprüfung von Ergänzungsschulen im Hinblick auf die Eignung zur Erfüllung der Schulpflicht,

- Besichtigungen und Schulbesuche bei Eingaben und Beschwerden,

- Beantwortung/Bearbeitung von Anfragen oder Beschwerden von Erziehungsberechtigten.

10.7.4 Rechtliche Bedenken gegenüber umfassender Aufgabenerledigung durch Schulämter

In Anbetracht dieser **umfassenden Erfüllung einer Vielzahl wesentlicher Aufgaben der staatlichen Schulaufsicht** über private Grundschulen und Mittelschulen **durch die Staatlichen Schulämter** habe ich dem Kultusministerium meine **erheblichen Zweifel an der (datenschutzrechtlichen) Rechtmäßigkeit** dieser in Bayern offenbar seit Jahren bestehenden Praxis mitgeteilt:

- Soweit sich die Regierungen bei der Ausübung der unmittelbaren staatlichen Schulaufsicht über private Grundschulen und Mittelschulen der Schulämter bedienen, bestehen rechtliche Bedenken zunächst im Hinblick auf die **eindeutige gesetzliche Zuständigkeitsregelung** des Art. 114 Abs. 1 Nr. 4 Buchst. b) BayEUG, der für die Schulämter in Bezug auf private Grundschulen und Mittelschulen keine Zuständigkeit vorsieht.

  Eine andere gesetzliche Regelung, die eine – wenn auch nur auf bestimmte (Teil-)Bereiche beschränkte – (Mit-)Zuständigkeit der Schulämter bei der staatlichen Schulaufsicht über private Grundschulen und Mittelschulen begründet, ist nicht ersichtlich. Vielmehr hat der bayerische Gesetzgeber in Art. 114 Abs. 1 Nr. 5 Buchst. a) BayEUG die **schulaufsichtliche Zuständigkeit der Schulämter ausdrücklich und ausschließlich auf öffentliche Grundschulen und Mittelschulen beschränkt**.

- Fehlt eine Rechtsgrundlage für die Aufgabenerfüllung der Schulämter bei der staatlichen Schulaufsicht über private Grundschulen und Mittelschulen, liegt zugleich ein **Verstoß gegen den institutionellen Gesetzesvorbehalt** des Art. 77 Abs. 1 Satz 1 Fall 2 Verfassung des Freistaates Bayern vor.

  Danach darf die Regelung der Zuständigkeiten der staatlichen Organe nicht durch die Verwaltung selbst vorgenommen werden, sondern hat ausschließlich durch den Landtag im Wege eines formellen Gesetzes zu erfolgen. Eine **faktische (Modifizierung dieser) Zuständigkeitsregelung durch die Verwaltungspraxis** ist **verfassungsrechtlich unzulässig**.

— Die Einhaltung der sachlichen, örtlichen und funktionalen Zuständigkeit ist Bestandteil des Gebots gesetzmäßiger Verwaltung (vgl. Art. 20 Abs. 3 Grundgesetz für die Bundesrepublik Deutschland). Damit besteht eine Rechtspflicht der Behörden zur Wahrung der gesetzlichen Kompetenzordnung, welche in jeder Lage des Verfahrens von Amts wegen zu beachten ist.

  Die **Beachtung der Kompetenzordnung** dient der Vermeidung von Mehrfachzuständigkeiten und damit der Rechtssicherheit. Gleichzeitig hat sie eine **Schutzfunktion für die vom Behördenhandeln Betroffenen**, weil damit eine beliebige Zuständigkeitswahrnehmung durch andere Behörden ausgeschlossen werden soll. Auch hat der Bürger grundsätzlich einen Anspruch auf das Handeln der zuständigen Behörde (vgl. Stelkens/Bonk/Sachs, Verwaltungsverfahrensgesetz, 8. Auflage 2014, § 3 Rn. 5 f.).

— In Anbetracht der verfassungsrechtlich vorgeschriebenen Bindung der Verwaltung an Gesetz und Recht und der gesetzlich normierten Kompetenzordnung sind **Zuständigkeitsvereinbarungen zwischen Behörden** (oder zwischen Behörde und Bürgerinnen/Bürgern) grundsätzlich **unzulässig** und nur bei gesetzlicher Ermächtigung wirksam.

  Auch eine **einseitige Zuständigkeitsübertragung** – beispielsweise durch Delegation – ist ohne ausdrückliche gesetzliche Grundlage **unzulässig** (vgl. Stelkens/Bonk/Sachs, a.a.O., § 3 Rn. 13).

— Aus spezifisch datenschutzrechtlicher Sicht habe ich zudem darauf hingewiesen, dass die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch bayerische öffentliche Stellen nur dann zulässig sind, wenn dies zur Erfüllung der in der Zuständigkeit der erhebenden, verarbeitenden oder nutzenden öffentlichen Stelle liegenden Aufgaben erforderlich ist (so ausdrücklich Art. 16 ff. BayDSG). Die Aufgabenerfüllung muss freilich rechtmäßig sein. Die **Rechtmäßigkeit der Aufgabenerfüllung** hängt jedoch **grundlegend** von der **sachlichen, örtlichen und funktionellen Zuständigkeit der Daten erhebenden, verarbeitenden oder nutzenden öffentlichen Stelle** ab (vgl. nur den Standardkommentar Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Art. 16 Rn. 15 ff.).

  Damit ist der **Umgang mit personenbezogenen Daten** von Lehrkräften, Schülerinnen und Schülern sowie Erziehungsberechtigten privater Grundschulen und Mittelschulen **durch ein unzuständiges Schulamt** auch **datenschutzrechtlich unzulässig**.

10.7.5 Schulämter als bloße Erbringer von „Hilfeleistungen“?

Das Kultusministerium hat mir versichert, dass es die Zuständigkeit der Regierungen für die unmittelbare staatliche Schulaufsicht bei privaten Grundschulen und Mittelschulen nicht in Zweifel ziehe. Vielmehr würden die **Staatlichen Schulämter nach Auffassung des Kultusministeriums von den Regierungen lediglich „als Hilfsorgane zur Erfüllung der jeweiligen Aufgaben der Schulaufsicht“ herangezogen**.

Nach Darstellung des Kultusministeriums hätten die Regierungen deutlich gemacht, dass sie die Schulaufsicht über die große Anzahl an privaten Grund-, Haupt- und Mittelschulen in Bayern (ca. 200) ohne die Mitwirkung der Staatlichen Schulämter nicht sachgerecht ausüben könnten. **Schließlich hätten nur die Schulämter die notwendigen lokalen Kenntnisse und seien im engen Kontakt mit den Schulleitungen der Privatschulen.** Ein Miteinander von öffentlichen und privaten Schulen vor Ort sei ohne unterstützenden Einsatz des Bindeglieds der Staatlichen Schulämter nicht realisierbar.

Als rechtliche Grundlage für diese „Hilfeleistung" nannte das Kultusministerium die Vorschrift des Art. 116 Abs. 4 BayEUG. Danach können die Schulaufsichtsbehörden zur Ausübung der Aufsicht die ihnen nachgeordneten Behörden und besondere Beauftragte heranziehen. Nach Auffassung des Kultusministeriums verbleibt demnach die Zuständigkeit für die unmittelbare staatliche Schulaufsicht über private Grundschulen und Mittelschulen zwar bei den Regierungen. Die Regierungen zögen jedoch im Rahmen der Ausübung ihrer Aufsicht auf der Grundlage des Art. 116 Abs. 4 BayEUG die Staatlichen Schulämter als Hilfsorgane heran.

Art. 116 BayEUG Beteiligung an der Schulaufsicht
(4) Die Schulaufsichtsbehörden können zur Ausübung der Aufsicht die ihnen nachgeordneten Behörden und besondere Beauftragte heranziehen.

10.7.6 Bedenken gegenüber Heranziehung der Schulämter als „Hilfsorgane"

Gerade in Anbetracht des oben skizzierten **weiten Umfangs der Aufgabenerledigung** bestehen **gegenüber einer Einbeziehung der Staatlichen Schulämter in die staatliche Schulaufsicht über private Grundschulen und Mittelschulen** auf der Grundlage des Art. 116 Abs. 4 BayEUG jedoch **erhebliche rechtliche Bedenken**:

— Zunächst ist festzuhalten, dass Art. 116 Abs. 4 BayEUG die gesetzliche Regelung über die sachliche Zuständigkeit in Art. 114 BayEUG unberührt lässt. Insbesondere ermöglicht Art. 116 Abs. 4 BayEUG keine – auch nicht teilweise – Übertragung von gesetzlichen Zuständigkeiten auf nachgeordnete Behörden. Vielmehr **gestattet** die Vorschrift des **Art. 116 Abs. 4 BayEUG** den Schulaufsichtsbehörden **nur, nachgeordnete Behörden** und besondere Beauftragte **als Hilfsorgane** zur Erfüllung der jeweiligen Aufgabe der Schulaufsicht **im Einzelfall heranzuziehen** (so auch der Standardkommentar Lindner/Stahl, Das Schulrecht in Bayern, Band 1, Art. 116 BayEUG Anm. 6, sowie Dirnaichner, Praxis der Kommunalverwaltung, Erläuterungen zu Art. 116 BayEUG).

  Somit ist es auf der Basis des Art. 116 Abs. 4 BayEUG lediglich zulässig, nachgeordnete Behörden im Rahmen der Schulaufsicht zu Hilfstätigkeiten im Einzelfall heranzuziehen, ohne dass sich die gesetzlich zuständigen Schulaufsichtsbehörden dadurch ihrer schulaufsichtlichen Aufgaben und damit auch ihrer Verantwortung entledigen könnten.

— **In der Praxis** werden die **Staatlichen Schulämter** im Rahmen der staatlichen Schulaufsicht über private Grundschulen und Mittelschulen jedoch **bayernweit** mit der Erledigung einer Vielzahl von – oben unter Nr. 10.7.2 und Nr. 10.7.3 nicht einmal abschließend aufgezählter – Aufgaben betraut.

Die Staatlichen Schulämter nehmen hierbei oftmals sogar **bedeutsame Aufgaben** wahr, **deren Inhalte über bloße Hilfstätigkeiten weit hinausgehen**. So führen die Schulämter zahlreiche Tätigkeiten aus, die eine **eigenverantwortliche Prüfung und Bewertung fachbezogener und – auch datenschutzrechtlich – sensibler Sachverhalte** erfordern **und damit** zu den **elementaren Aufgaben der Schulaufsicht** gehören.

Hierzu zählen etwa die **Überprüfung** der fachlichen Qualifikation und pädagogischen Eignung des privat angestellten Lehrpersonals, die **Beurteilung** von Lehrpersonal, die **Überprüfung** von Ergänzungsschulen im Hinblick auf die Eignung zur Erfüllung der Schulpflicht und die **Beantwortung/Bearbeitung** von Anfragen oder Beschwerden von Erziehungsberechtigten.

— Schließlich ergibt sich sowohl aus den Stellungnahmen des Kultusministeriums als auch der Regierungen, dass die „Unterstützung" durch die Schulämter **nicht auf den Einzelfall beschränkt** ist, **sondern dauerhaft und institutionell als Regelfall in der Praxis fest verankert** ist.

Ob und welche Aufgaben der staatlichen Schulaufsicht über private Grundschulen und Mittelschulen daneben überhaupt noch bei den Regierungen verbleiben, ist aus sämtlichen Stellungnahmen der Kultusverwaltung dagegen nicht ersichtlich.

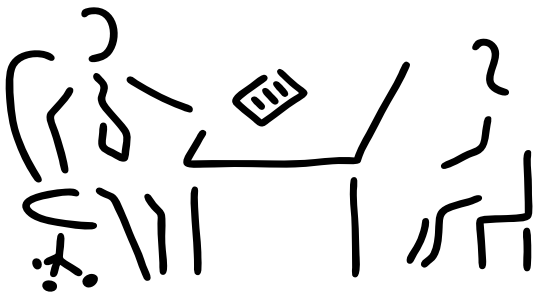
10.7.7 Fazit

Die Stellungnahmen von Kultusministerium und Regierungen haben meine bisherigen, bei meiner Kontrolltätigkeit erlangten Erkenntnisse, dass die umfassend und regelmäßig eingebundenen **Staatlichen Schulämter bayernweit faktisch wesentliche Aufgaben der staatlichen Schulaufsicht über private Grundschulen und Mittelschulen dauerhaft und in eigener Verantwortung wahrnehmen**, bestätigt.

Gewichtige Gründe sprechen dafür, dass die aus Praktikabilitätsgründen erfolgende **– strukturell verfestigte – Einbindung der Schulämter** in die staatliche Schulaufsicht über private Grundschulen und Mittelschulen **in der Art und in dem Umfang, wie derzeit bayernweit praktiziert, nicht (mehr) als bloße „Hilfstätigkeit" angesehen werden kann, die über die Vorschrift des Art. 116 Abs. 4 BayEUG abgedeckt wäre**. Der bayerische Gesetzgeber hat in Art. 114 Abs. 1 Nr. 4 Buchst. b) BayEUG die Aufgabe der Schulaufsicht bei privaten Grundschulen und Mittelschulen eindeutig und ausschließlich den Regierungen zugewiesen.

Sind die Regierungen allerdings auch künftig – schon tatsächlich – nicht in der Lage, ihrer gesetzlichen Verpflichtung zur Wahrnehmung der Schulaufsicht über private Grundschulen und Mittelschulen nachzukommen, können die aufgezeigten Bedenken aus meiner Sicht letztlich nur durch **Schaffung einer klaren gesetzlichen (Zuständigkeitsänderungs-)Regelung im Bayerischen Gesetz über das Erziehungs- und Unterrichtswesen** ausgeräumt werden. Meine diesbezügliche, dringende Empfehlung, eine entsprechende, im Übrigen formulierungstechnisch unaufwändige gesetzliche Klarstellung auf den Weg zu bringen, hat das **Staatsministerium für Bildung und Kultus, Wissenschaft und Kunst jedoch bislang leider nicht aufgegriffen**.

11 Personalwesen



11.1 Benutzung dienstlicher Telekommunikationsanlagen – Neufassung der TKBek

Ein Schwerpunkt meiner beratenden und kontrollierenden Tätigkeit im Bereich des Personaldatenschutzes liegt seit jeher darin, die **innerbehördlichen Regelungen zur Benutzung dienstlicher Telekommunikationsanlagen** bei den bayerischen öffentlichen – staatlichen wie kommunalen – Stellen **datenschutzgerecht auszugestalten**. Über meine Bemühungen zur datenschutzkonformen Fassung der entsprechenden Vorgaben im staatlichen Bereich – der Bekanntmachung des Finanzministeriums über die „Einrichtung und Benutzung dienstlicher Telekommunikationsanlagen (TK-Bek)" – hatte ich zuletzt unter Nr. 22.2 meines 23. Tätigkeitsberichts 2008 eingehend berichtet.

Auch im aktuellen Berichtszeitraum haben mich wieder zahlreiche Eingaben von öffentlichen Bediensteten und vielfältige Anfragen von Behörden zu dieser datenschutzrechtlich sensiblen Thematik erreicht. Besonders hervorheben möchte ich, dass das Staatsministerium der Finanzen, für Landesentwicklung und Heimat die massiven Preissenkungen auf dem Telekommunikationsmarkt und die zunehmende Verbreitung von Flatrates zum Anlass genommen hat, die entsprechenden, bereits aus dem Jahr 2007 stammenden staatlichen Vorgaben grundlegend zu überarbeiten und als Bekanntmachung über die **„Einrichtung und Benutzung dienstlicher Telekommunikationsanlagen (TKBek)" mit Wirkung vom 1. Januar 2015 neu zu fassen** (FMBl. 2015, S. 130). Dabei hat mich das Finanzministerium in das Normsetzungsverfahren frühzeitig eingebunden; so konnte ich hier einige datenschutzrechtliche Verbesserungen erreichen.

Im Einzelnen möchte ich folgende Punkte herausgreifen:

11.1.1 Dienstliche Telefongespräche

In Bezug auf dienstliche Telefongespräche gilt nunmehr Folgendes:

— Die Nachweise über **dienstliche Verbindungen können** – allerdings nur unter Beachtung des Verhältnismäßigkeitsprinzips – **stichprobenweise sowie in konkreten Verdachtsfällen** hinsichtlich des dienstlichen Charakters sowie der Notwendigkeit der Gespräche durch die Dienstvorgesetzten oder die von ihnen beauftragten Personen **überprüft werden** (siehe Nr. 3.1.3 Satz 1 TKBek).

— Um diese Überprüfung zu ermöglichen, sind bestimmte Daten aller in das öffentliche Telekommunikationsnetz abgehenden Verbindungen **– Beginn und Ende beziehungsweise Dauer der Verbindung nach Datum und Uhrzeit, Endeinrichtungsnummer und Zielrufnummer – durch die Telekommunikationsanlage oder durch andere Aufzeichnungen**, etwa durch einen Einzelverbindungsnachweis beim Anbieter, nach wie vor **festzuhalten** (siehe Nr. 3.1.2 Sätze 1 und 2 TKBek). Nicht mehr festgehalten werden dürfen dagegen Tarifeinheiten oder Leistungsentgelte.

— Für die zu speichernden Daten besteht eine **strikte Zweckbindung**. Die Daten dürfen nur für die genannten Kontrollzwecke verwendet werden; eine Verwendung für andere Zwecke ist nicht zulässig (siehe Nr. 3.1.3 Satz 2 TKBek).

— Die Durchführung von Kontrollen unterliegt gemäß Art. 75a Abs. 1 Nr. 1 Bayerisches Personalvertretungsgesetz der **Mitbestimmung der Personalvertretung**. Zum Schutz der Beschäftigten konnte ich erreichen, dass in Nr. 3.1.3 Satz 3 TKBek die Empfehlung aufgenommen wurde, die Durchführung von Kontrollen behördenintern im Wege einer **Dienstvereinbarung** zu regeln, wobei auch die **Beteiligung der/des behördlichen Datenschutzbeauftragten** vorgesehen werden sollte.

— Schließlich sind die gespeicherten Verkehrsdaten nach Abschluss der Prüfung, **spätestens aber nach drei Monaten zu vernichten** (siehe Nr. 3.1.2 Satz 5 TKBek). Die Aufbewahrungsdauer wurde damit deutlich verkürzt.

11.1.2 Private Telefongespräche

Aus Datenschutzsicht ist zu begrüßen, dass die **Erhebung und Verwendung von Telekommunikationsdaten bezüglich privater Telefongespräche** in der neu gefassten TKBek **deutlich beschränkt** wurde. Im Einzelnen:

— Mit Ausnahme von dienstlichen Mobiltelefonen dürfen dienstliche Telekommunikationsanlagen nunmehr von den Beschäftigten für private Zwecke – allerdings nur in dringenden Fällen und in geringfügigem Umfang – unentgeltlich benutzt werden (siehe Nrn. 3.2.1, 3.2.4 TKBek). Zum Schutz der Beschäftigten ist jetzt zwingend vorgesehen, dass die **Bediensteten private Gespräche** – etwa durch Eingabe einer PIN – als solche **kennzeichnen können** (siehe Nr. 2.6 Satz 6 TKBek). Bei als privat gekennzeichneten Verbindungen ist sodann auf den **Nachweis der Zielrufnummer zu verzichten** (siehe Nr. 3.1.2 Satz 3 TKBek).

– Die (übrigen) gespeicherten **Verkehrsdaten** sind **spätestens nach drei Monaten** – und damit schneller als bisher – zu vernichten oder **zu löschen** (siehe Nr. 3.1.2 Satz 5 TKBek).

– Die gespeicherten **Verkehrsdaten für erstattungspflichtige Privatgespräche auf dienstlichen Mobiltelefonen** (vgl. Nr. 3.2.4 TKBek) müssen nach vollständiger Abrechnung der Entgelte, **spätestens zum Ablauf der gesetzlich festgelegten Höchstspeicherdauer gelöscht** werden, soweit gegen die Abrechnung keine Einwendungen erhoben wurden (siehe Nr. 3.1.2 Satz 4 TK-Bek).

11.1.3 Datenschutzrelevante allgemeine Regelungen

Schließlich möchte ich noch besonders auf folgende datenschutzrelevante allgemeine Regelungen der TKBek hinweisen:

– **Generell unzulässig** ist nunmehr jegliche **Datenerhebung beim Telefonverkehr** von Stellen, die nicht der Aufsicht unterliegen (etwa **Personalvertretung** in Personalangelegenheiten) oder die im Rahmen einer freiwilligen Beratung (beispielsweise **Drogen-, Gesundheits-, Ehe- und Familienberatung**) tätig werden und damit einer besonderen Verschwiegenheitspflicht unterliegen (siehe Nr. 3.1.4 TKBek). Im Gegensatz zu früher sind hier auch die Leistungsentgelte nicht mehr festzuhalten.

– Die Bekanntmachung stellt in Nr. 3.1.5 Satz 1 TKBek klar, dass bei der Benutzung dienstlicher Telekommunikationsanlagen die **allgemeinen Vorschriften über den Persönlichkeits- und Datenschutz zu beachten** sind.

– Unbefugte **Aufzeichnungen von Verbindungen** sind gemäß § 201 Strafgesetzbuch **verboten**, soweit eine ausdrückliche gesetzliche Ermächtigung (§ 100a Strafprozessordnung) fehlt; darauf weist die Bekanntmachung in Nr. 3.1.5 Satz 2 TKBek ausdrücklich hin.

– Das **Aufschalten auf Gespräche von Beschäftigten** (Mithören) ist nach Nr. 3.1.5 Satz 3 TKBek **unzulässig**.

– Die **Schaffung innerbehördlicher Transparenz** ist auch aus Datenschutzsicht von besonderer Bedeutung. Ich begrüße daher, dass die **Dienststellen** in Nr. 3.2.3 TKBek **ausdrücklich dazu verpflichtet** werden, die Beschäftigten über das in der Dienststelle angewendete Erfassungsverfahren, über den Zweck der Telekommunikationsdatenerfassung und über die Behandlung der Daten zu informieren.

In Ergänzung zur Allgemeinen Geschäftsordnung für die Behörden des Freistaates Bayern **gilt die TKBek für nahezu alle staatlichen Behörden** (einschließlich der staatlichen Hochschulen), nicht hingegen für viele andere meiner Kontrollzuständigkeit unterfallende bayerische öffentliche Stellen, wie beispielsweise die Kommunalverwaltungen.

Aus Datenschutzsicht **empfehle ich jedoch allen bayerischen kommunalen und sonstigen öffentlichen Stellen**, die Neufassung der TKBek zum Anlass – und im Grundsatz auch zum Vorbild – für eine kritische Durchsicht und (soweit nötig) für

eine datenschutzgerechte Überarbeitung der internen Regelungen zur Benutzung dienstlicher Telekommunikationsanlagen zu nehmen.

11.2 Datenschutz bei elektronischen Schließanlagen

Um sich vor Verstößen gegen das Hausrecht von außen effektiv zu schützen, aber auch um die internen Zutrittsberechtigungen differenziert zu verwalten, führen nach meiner Beobachtung bayerische öffentliche – vor allem staatliche und kommunale – Stellen in den letzten Jahren zunehmend **zentrale, softwaretechnisch gesteuerte elektronische Schließanlagen** ein.

In diesem Zusammenhang wird jede(r) einzelne Beschäftigte durch Zuweisung eines **mit einer eindeutigen Identifizierungsnummer gekennzeichneten elektronischen Schlüssels** – oft in Gestalt eines Transponders – zur Öffnung von bestimmten Türschlössern berechtigt. Im **elektronischen Schließplan** wird dementsprechend festgelegt, welche Türen von welchen Schlüsseln geöffnet werden können. Darüber hinaus wird hier elektronisch gespeichert, welcher Schlüssel welcher/m Beschäftigten ausgehändigt wurde. Auf diese Weise kann insbesondere sichergestellt werden, dass Räume, in denen sensible Daten aufbewahrt werden, nur von den jeweils zuständigen Beschäftigten betreten werden können. Eine elektronische Schließanlage ermöglicht es auch, die Zutrittsberechtigungen – etwa nach dem Ausscheiden von Beschäftigten – nachträglich zu ändern. Gehen Schlüssel verloren, können sie umgehend gesperrt werden; ferner können die betroffenen Türzylinder entsprechend umprogrammiert werden, so dass sich ein etwaiger Finder nicht unberechtigt Zutritt zu den Diensträumen verschaffen kann.

Im Ergebnis gewährleistet der Einsatz einer elektronischen Schließanlange somit nicht nur eine **effektive, detaillierte Zutrittskontrolle**, sondern macht – aufgrund der softwaretechnischen Programmierung der Schlüssel und der Türzylinder – auch die gewohnte, vergleichsweise aufwändige Verwaltung und Vergabe von herkömmlichen Schlüsseln entbehrlich.

Vor diesem Hintergrund haben sich bei mir im Berichtszeitraum vermehrt sowohl öffentliche Stellen als auch Bedienstete und Personalvertretungen nach den **datenschutzrechtlichen Anforderungen an den Einsatz von elektronischen Schließanlagen** erkundigt.

Hierzu nehme ich wie folgt Stellung:

11.2.1 Erhebung und Verwendung von Beschäftigtendaten

Mittels einer elektronischen Schließanlage werden typischerweise personenbezogene Beschäftigtendaten im Sinne von Art. 4 Abs. 1 BayDSG erhoben und verwendet.

Zumindest wird im zentralen Schließplan **gespeichert, welche(r) Beschäftigte(r) welchen elektronischen Schlüssel mit welchen Zutrittsberechtigungen erhalten hat**. Möglich ist aber grundsätzlich auch, dass zentral oder in den Speichereinheiten der Schlüssel und Türzylinder **erfasst** wird, **mit welchem Schlüssel welche Tür zu welchem Zeitpunkt geöffnet wurde**. Durch eine Verknüpfung der eindeutigen Schlüssel-Identifizierungsnummer mit den zugehörigen Personendaten aus dem elektronischen Schließplan kann sodann die/der

einzelne Beschäftigte unschwer identifiziert werden; zudem kann ihr/sein **„Zutrittsverhalten" nachvollzogen** werden – und damit letztlich auch ein **Bewegungsprofil erstellt** werden.

Die Erhebung wie auch die Verarbeitung und die Nutzung solcher personenbezogenen Beschäftigtendaten stellen **Eingriffe in das grundrechtlich geschützte Recht auf informationelle Selbstbestimmung** nach Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 Grundgesetz für die Bundesrepublik Deutschland dar. Diese Eingriffe sind gemäß Art. 15 Abs. 1 BayDSG nur datenschutzrechtlich zulässig, wenn das Bayerische Datenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet (Nr. 1) oder der Betroffene eingewilligt hat (Nr. 2).

11.2.2 Einwilligung im Abhängigkeitsverhältnis

Damit eine Einwilligung eine tragfähige Rechtsgrundlage im Sinne des Art. 15 Abs. 1 Nr. 2 BayDSG darstellen kann, muss sie in erster Linie den gesetzlichen Anforderungen von Art. 15 Abs. 2 bis 4 und 7 BayDSG genügen.

Danach muss eine **datenschutzgerechte Einwilligung insbesondere freiwillig, informiert und grundsätzlich schriftlich** erteilt werden; auch müssen die Betroffenen darauf hingewiesen werden, dass sie die Einwilligung ohne Angabe von Gründen und ohne nachteilige Folgen verweigern sowie **jederzeit widerrufen** können.

Unabhängig vom Vorliegen der übrigen Rechtmäßigkeitsvoraussetzungen ist es in Anbetracht der (strukturellen) Abhängigkeit, in der die Beschäftigten zu ihrem Dienstherrn stehen, im Dienstverhältnis stets fraglich, ob eine Einwilligung **tatsächlich freiwillig, also ohne – zumindest gefühlten – (Gruppen-)Druck**, erteilt wird. Hier bestehen im Regelfall **erhebliche Bedenken**.

Der Einsatz von elektronischen Schließanlagen ist daher auf der Grundlage einer **Einwilligung** der Beschäftigten – wenn überhaupt – **nur in sehr engen Grenzen möglich**.

11.2.3 Gesetzliche Anforderungen

— Als gesetzliche Rechtsgrundlage im Sinne des Art. 15 Abs. 1 Nr. 1 BayDSG für die **Erhebung von personenbezogenen Beschäftigtendaten mittels elektronischer Schließanlagen** kommt bei bayerischen Beamtinnen und Beamten allein die Vorschrift des **Art. 102 Bayerisches Beamtengesetz** (BayBG) in Betracht. Diese Bestimmung ist als allgemein gültiges Schutzprinzip für alle öffentlichen Bediensteten nach meiner seit jeher vertretenen Auffassung auch auf die nicht-verbeamteten Beschäftigten des bayerischen öffentlichen Dienstes entsprechend anzuwenden.

  Nach Art. 102 Satz 1 BayBG darf der Dienstherr personenbezogene Daten über Beamte und Beamtinnen nur erheben, **soweit dies** (unter anderem) **zur Durchführung organisatorischer, personeller und sozialer Maßnahmen**, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, **erforderlich ist** oder eine Rechtsvorschrift dies erlaubt.

Art. 102 BayBG Erhebung personenbezogener Daten
[1]Der Dienstherr darf personenbezogene Daten über Bewerber, Bewerberinnen, Beamte und Beamtinnen sowie ehemalige Beamte und Beamtinnen nur erheben, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift dies erlaubt. [2]Fragebogen, mit denen solche personenbezogenen Daten erhoben werden, bedürfen der Genehmigung durch die oberste Dienstbehörde.

— Bei den **Daten im elektronischen Schließplan**, die eine Zuordnung der elektronischen Schlüssel zu den jeweiligen Beschäftigten erlauben, handelt es sich zwar ebenso wie bei den möglicherweise gespeicherten **„Zutrittsdaten“** nicht um die Beamtin oder den Beamten betreffende Unterlagen, die mit dem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen. Diese Daten stellen somit keine Personalaktendaten im Sinne des § 50 Satz 2 Beamtenstatusgesetz, wohl aber **personenbezogene Sachaktendaten** dar.

  Die strengen Zugangsbeschränkungen des Art. 103 BayBG für Personalakten greifen daher nicht ein. Vielmehr richtet sich die Zulässigkeit der **Verarbeitung und Nutzung** von Beschäftigtendaten mittels elektronischer Schließanlagen nach den allgemeinen Vorschriften des Bayerischen Datenschutzgesetzes; insbesondere ist hier **Art. 17 Abs. 1 BayDSG** zu beachten.

Art. 17 BayDSG Verarbeitung und Nutzung
(1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn
1. es zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist und
2. es für die Zwecke erfolgt, für die die Daten erhoben worden sind; ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.

— Nach diesen beamten- und datenschutzrechtlichen Vorschriften kommt es für die Beurteilung der datenschutzrechtlichen Zulässigkeit **entscheidend** darauf an, **ob und inwieweit** die mit dem Einsatz von elektronischen Schließanlagen verbundenen Erhebungen, Nutzungen und Verarbeitungen personenbezogener Beschäftigtendaten **zur ordnungsgemäßen Aufgabenerfüllung** der öffentlichen Stelle **– im Wesentlichen also zur sachgerechten Organisation des Betriebsablaufs und zur effektiven Wahrnehmung des Hausrechts – erforderlich** sind.

  Dieses Erforderlichkeitsprinzip liegt im Übrigen auch den vereinzelt bestehenden, vorrangigen datenschutzrechtlichen Spezialvorschriften (etwa im Schulbereich Art. 85 Abs. 1 Satz 1 BayEUG in Verbindung mit Art. 14 Abs. 1 Satz 2 Bayerisches Schulfinanzierungsgesetz in Verbindung mit § 19 Satz 1 Lehrerdienstordnung) zugrunde.

  Die Erforderlichkeit ist zu bejahen, wenn die mit dem Einsatz einer elektronischen Schließanlage einhergehenden Datenerhebungen und -verwendungen nicht nur die **Aufgabenerfüllung des Dienstherrn objektiv unterstützen und fördern**, sondern auch **zu den schutzwürdigen Interessen**

der Beschäftigten in einem angemessenen Verhältnis stehen. Insbesondere dürfen die (berechtigten) Interessen des Dienstherrn nicht auf andere, weniger in das Persönlichkeitsrecht der Beschäftigten eingreifende Weise gewahrt werden können.

— Die Führung eines **elektronischen Schließplans**, aus dem sich nicht nur ergibt, welcher elektronische Schlüssel welcher/m Beschäftigten ausgehändigt wurde, sondern auch, zu welchen Räumen jeweils der Zutritt gestattet wurde, kann in der Regel als zur Aufgabenerfüllung des Dienstherrn **erforderlich** angesehen werden. Hier bestehen zwischen einer in Papierform geführten „Schlüsselliste" und einem elektronischen Schließplan keine maßgeblichen Unterschiede.

— **Problematischer** ist es hingegen, wenn mittels der elektronischen Schließanlage – sei es zentral, sei es im Schlüssel, sei es im Türzylinder – auch die **„Zutrittsdaten"** gespeichert werden, also protokolliert wird, mit welchem Schlüssel (und damit mittelbar auch von welcher/m Beschäftigten) wann welches Türschloss geöffnet oder geschlossen wurde. Ob und inwieweit eine solche Speicherung zulässig ist, lässt sich nicht für alle Bereiche aller öffentlichen Stellen einheitlich und im Vorhinein beurteilen. Diese Bewertung hängt maßgeblich von den Umständen des Einzelfalles ab und kann daher letztlich nur vor Ort abschließend erfolgen.

Aus Datenschutzsicht ist hierbei jedoch ein **strenger Maßstab** anzulegen. **Grundsätzlich** gilt, dass eine Speicherung der Zutritte zur behördlichen Aufgabenerfüllung **nicht erforderlich** ist. Zweck einer Schließanlage ist es, eine aufgabengerechte Zutrittsverwaltung zu betreiben und eine sachgerechte Ausübung des Hausrechts zu ermöglichen. Hierzu bedarf es einer Protokollierung der Zutritte beim Einsatz einer elektronischen Schließanlage ebenso wenig wie beim Gebrauch einer herkömmlichen, mechanischen Schließanlage.

Entsprechend dieser Maßgabe hat die öffentliche Stelle die **Software der elektronischen Schließanlage zu gestalten**. Allein die Tatsache, dass auf dem Markt befindliche Anlagen Speicherungen von „Zutrittsdaten" ermöglichen oder sogar vorsehen, macht ihren Einsatz nicht erforderlich. Zutreffend hat das Bundesverfassungsgericht im Zusammenhang mit informations- und kommunikationstechnisch gestützter Datenverarbeitung allgemeingültig klargestellt: „Die Anforderungen an die technische Datenverarbeitung haben insoweit den Anforderungen des Grundrechts auf informationelle Selbstbestimmung zu genügen und nicht umgekehrt." (Bundesverfassungsgericht, Beschluss vom 13. Mai 2015 – 1 BvR 99/11).

Ist eine **Speicherung von „Zutrittsdaten" im Ausnahmefall** – etwa beim Einsatz einer elektronischen Schließanlage in besonders sicherheitsrelevanten Bereichen – einmal zulässig, so hat die öffentliche Stelle sicherzustellen, dass die Speicherung **möglichst kurz** erfolgt und ein Zugriff auf die gespeicherten Daten unmöglich ist oder zumindest auf einen vorher festgelegten Personenkreis eng begrenzt wird. Besonders wichtig ist es auch, die gespeicherten personenbezogenen Beschäftigtendaten durch **technische und organisatorische Maßnahmen vor unbefugtem Zugriff** zu schützen.

11.2.4 Datenschutzrechtliche Freigabe

Der erstmalige Einsatz einer elektronischen Schließanlage bedarf gemäß Art. 26 Abs. 1 Satz 1 BayDSG der **vorherigen schriftlichen datenschutzrechtlichen Freigabe**. Nach Art. 26 Abs. 1 Satz 3 BayDSG gilt dies auch entsprechend für spätere, wesentliche Änderungen.

Die Freigabe ist nach Art. 26 Abs. 3 Satz 2 BayDSG **von dem oder der behördlichen Datenschutzbeauftragten zu erteilen und** gemäß Art. 27 BayDSG **in das Verfahrensverzeichnis aufzunehmen**.

11.2.5 Mitbestimmung des Personalrats

Darf im Ausnahmefall einmal eine **Speicherung der beschäftigtenbezogenen „Zutrittsdaten"** erfolgen, so ist der Personalrat bei Einführung, Anwendung und erheblicher Änderung der elektronischen Schließanlage zu beteiligen. Es ist ein Fall der **zwingenden Mitbestimmung** gemäß Art. 75a Abs. 1 Nr. 1 Bayerisches Personalvertretungsgesetz (BayPVG) gegeben, da die elektronische Schließanlage dann – was nach der Rechtsprechung bereits ausreichend ist – **zur Überwachung des Verhaltens oder der Leistung der Beschäftigten an sich geeignet** ist, auch wenn sie im konkreten Fall hierzu nicht eingesetzt werden soll.

Nicht zuletzt aus Transparenzgründen empfehle ich in diesem Zusammenhang stets, eine **Dienstvereinbarung** im Sinne des Art. 73 BayPVG zwischen Dienststelle und Personalrat abzuschließen.

In dieser Dienstvereinbarung sollte **insbesondere geregelt** werden,

- zu welchen **Zwecken genau** welche – gegebenenfalls in einer Anlage zur Dienstvereinbarung konkret zu benennenden – **Daten** mittels der elektronischen Schließanlage in welchem **Umfang** erhoben, verarbeitet oder genutzt werden; dabei ist die Dauer der Speicherung auf das für den jeweiligen Zweck unbedingt erforderliche Maß zu begrenzen,

- welche Personen innerhalb der öffentlichen Stelle **Zugriff** auf die gespeicherten Daten haben, wobei – wenn möglich – eine **Protokollierung** der Zugriffe erfolgen sollte,

- wann genau die Daten zu löschen sind; dabei sind generell **kurzfristige Löschvorgaben** zu machen,

- dass die Verwendung der Daten zur **permanenten und allgemeinen Verhaltens- oder Leistungskontrolle ausgeschlossen** ist.

  Zulässig sind **allenfalls Anlasskontrollen** im Falle eines durch konkrete Tatsachen begründeten Verdachts auf einen dienst-, arbeits-, straf- oder ordnungswidrigkeitenrechtlichen Verstoß **sowie anlasslose Stichproben**. In diesen Fällen darf die Auswertung des Datenmaterials allerdings **nur unter Beteiligung der Personalvertretung und des oder der behördlichen Datenschutzbeauftragten** vorgenommen werden,

- dass die **Beschäftigten** über den Inhalt der Dienstvereinbarung **unterrichtet** werden.

11.2.6 Weiterführende Hinweise

Ergänzend möchte ich noch auf die **Ausarbeitung „Einsatz von Zutrittskontrollsystemen“** des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit aufmerksam machen. Diese befasst sich unter anderem mit der Funktionsweise und den datenschutzrechtlichen Anforderungen an Zutrittskontrollsysteme. Die Ausarbeitung ist unter https://www.tlfdi.de abrufbar.

Mit **datenschutzrechtlichen Aspekten bei der Einbruchsbekämpfung mit einer zentralen Schließanlage** hat sich das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein in seinem 27. Tätigkeitsbericht 2005 unter Nr. 4.1.3 beschäftigt. Dieser Beitrag ist unter https://www.datenschutzzentrum.de zu finden.

11.3 Und nochmals: Datenschutz beim Betrieblichen Eingliederungsmanagement

Nach § 84 Abs. 2 Satz 1 Sozialgesetzbuch Neuntes Buch – Rehabilitation und Teilhabe behinderter Menschen – (SGB IX) ist der Arbeitgeber verpflichtet, allen Beschäftigten, die innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig sind, ein **Betriebliches Eingliederungsmanagement (BEM)** anzubieten. Diese Verpflichtung besteht sowohl für private wie für öffentliche Arbeitgeber; im öffentlichen Dienst sind davon neben den Tarifbeschäftigten auch die Beamtinnen und Beamten betroffen. Das BEM umfasst **alle Aktivitäten, Maßnahmen und Leistungen**, die im Einzelfall **zur Wiedereingliederung nach längerer Arbeitsunfähigkeit** erforderlich sind. Ziele des BEM sind es, durch Einleitung rehabilitierender oder präventiver Maßnahmen vorhandene Arbeitsunfähigkeiten zu überwinden, erneuten Arbeitsunfähigkeiten vorzubeugen und den Arbeitsplatz zu sichern sowie Berufs-/Dienstunfähigkeiten zu vermeiden.

§ 84 SGB IX Prävention
(2) [1]Sind Beschäftigte innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig, klärt der Arbeitgeber mit der zuständigen Interessenvertretung im Sinne des § 93, bei schwerbehinderten Menschen außerdem mit der Schwerbehindertenvertretung, mit Zustimmung und Beteiligung der betroffenen Person die Möglichkeiten, wie die Arbeitsunfähigkeit möglichst überwunden werden und mit welchen Leistungen oder Hilfen erneuter Arbeitsunfähigkeit vorgebeugt und der Arbeitsplatz erhalten werden kann (betriebliches Eingliederungsmanagement). [2]Soweit erforderlich wird der Werks- oder Betriebsarzt hinzugezogen. [3]Die betroffene Person oder ihr gesetzlicher Vertreter ist zuvor auf die Ziele des betrieblichen Eingliederungsmanagements sowie auf Art und Umfang der hierfür erhobenen und verwendeten Daten hinzuweisen. [4]Kommen Leistungen zur Teilhabe oder begleitende Hilfen im Arbeitsleben in Betracht, werden vom Arbeitgeber die örtlichen gemeinsamen Servicestellen oder bei schwerbehinderten Beschäftigten das Integrationsamt hinzugezogen. [5]Diese wirken darauf hin, dass die erforderlichen Leistungen oder Hilfen unverzüglich beantragt und innerhalb der Frist des § 14 Abs. 2 Satz 2 erbracht werden. [6]Die zuständige Interessenvertretung im Sinne des § 93, bei schwerbehinderten Menschen außerdem die Schwerbehindertenvertretung, können die Klärung verlangen. [7]Sie wachen darüber, dass der Arbeitgeber die ihm nach dieser Vorschrift obliegenden Verpflichtungen erfüllt.

Im Zuge eines BEM werden in der Regel Personalaktendaten im Sinne der § 50 Satz 2 Beamtenstatusgesetz, Art. 102 ff. Bayerisches Beamtengesetz sowie sensible Gesundheitsdaten im Sinne des Art. 15 Abs. 7 Satz 1 BayDSG in erheblichem Umfang erhoben, verarbeitet und genutzt. Die **datenschutzrechtlichen Anforderungen**, die hierbei zu beachten sind, habe ich bereits in meinem 25. Tätigkeitsbericht 2012 unter Nr. 11.2 eingehend erläutert. Dabei habe ich den bayerischen öffentlichen – insbesondere staatlichen und kommunalen – Stellen die Verwendung des **BEM-Leitfadens** und des **BEM-Informationsblatts** des Staatsministeriums der Finanzen, für Landesentwicklung und Heimat empfohlen, die jeweils mit mir abgestimmt sind. Auch in der Folgezeit haben mich Fragen der datenschutzkonformen Gestaltung des BEM weiter intensiv beschäftigt (siehe dazu nur meinen 26. Tätigkeitsbericht 2014 unter Nr. 11.3).

Eine spezifische, besonders praxisrelevante Problematik bei der konkreten Umsetzung des BEM betrifft die **Reichweite des Informationsanspruchs der örtlichen Personalvertretung**. Diese hat nämlich nach § 84 Abs. 2 Satz 7 SGB IX darüber zu wachen, dass der Arbeitgeber seine Verpflichtungen zur Anbietung und – bei Annahme des Angebots – auch zur ordnungsgemäßen Durchführung eines BEM erfüllt. Nach Art. 69 Abs. 2 Sätze 1 und 2 Bayerisches Personalvertretungsgesetz (BayPVG) ist der Personalrat zur Durchführung seiner Aufgaben – und damit auch zur Wahrnehmung seiner Überwachungsaufgabe nach § 84 Abs. 2 Satz 7 SGB IX – rechtzeitig und umfassend zu unterrichten; die Dienststelle hat ihm die hierfür erforderlichen Unterlagen zur Verfügung zu stellen.

Art. 69 BayPVG
(2) [1]Der Personalrat ist zur Durchführung seiner Aufgaben rechtzeitig und umfassend zu unterrichten. [2]Ihm sind die hierfür erforderlichen Unterlagen zur Verfügung zu stellen. …[6]Personalakten dürfen nur mit schriftlicher Zustimmung des Beschäftigten und nur von einem von ihm bestimmten Mitglied des Personalrats eingesehen werden.

In diesem Zusammenhang ist in Rechtsprechung und Praxis **umstritten** gewesen, **ob die Dienststelle die Personalvertretung über Beschäftigte**, die die Voraussetzungen für ein BEM erfüllen, auch **ohne deren Zustimmung namentlich informieren darf**.

Im Einklang mit der bisherigen Rechtsprechung des Bayerischen Verwaltungsgerichtshofs (siehe insbesondere den Beschluss vom 12. Juni 2012 – 17 P 11.1140) habe ich diese Frage bereits in Nr. 11.2.1 meines 25. Tätigkeitsberichts 2012 und erneut in Nr. 11.3.1 meines 26. Tätigkeitsberichts 2014 verneint. Im Hinblick auf das Grundrecht auf informationelle Selbstbestimmung nach Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 Grundgesetz für die Bundesrepublik Deutschland dürfen danach personenbezogene Gesundheitsdaten von Beschäftigten nur dann an die Personalvertretung weitergegeben werden, wenn hierfür schriftliche Einwilligungen der Betroffenen vorliegen, die sich ausdrücklich auf Daten über die Gesundheit beziehen (vgl. Art. 15 Abs. 1 Nr. 2, Abs. 2 bis 4, Abs. 7 Satz 1 Nr. 2 BayDSG). Personenbezogene Gesundheitsdaten enthält aber auch die namentliche Mitteilung, welche Beschäftigten innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig waren.

Mit Beschluss vom 15. März 2016 (17 P 14.2689) hat der **Bayerische Verwaltungsgerichtshof** allerdings seine **bisherige Rechtsprechung** zu dieser Problematik ausdrücklich **aufgegeben** und sich der Auffassung des Bundesverwaltungsgerichts (siehe Beschluss vom 4. September 2012 – 6 P 5.11) im Grundsatz

angeschlossen. Danach hat der **Dienststellenleiter einem vom Personalrat bestimmten Mitglied regelmäßig die Namen der Beschäftigten**, denen ein BEM anzubieten ist, **unabhängig von deren Zustimmung mitzuteilen**. Dies ist nach Ansicht des Verwaltungsgerichtshofs erforderlich, damit der Personalrat seinen Überwachungsauftrag nach § 84 Abs. 2 Satz 7 SGB IX ordnungsgemäß wahrnehmen kann. Gegebenenfalls wird das vom Personalrat bestimmte Mitglied zusätzlich über den Erstkontakt beziehungsweise über das Angebot eines BEM gegenüber den betroffenen Beschäftigten, etwa durch Überlassung eines Abdrucks der entsprechenden Anschreiben, informiert. Die Mitteilung anonymisierter Daten sieht der Verwaltungsgerichtshof dagegen nicht mehr als ausreichend an.

Vor diesem Hintergrund sind für die namentliche Information der Personalvertretung nunmehr folgende Eckpunkte zu beachten:

— Die **Namensliste der vom BEM betroffenen Beschäftigten** darf neben der Angabe der Organisationseinheiten nur die Mitteilung enthalten, dass die dort aufgeführten Beschäftigten im maßgeblichen Jahreszeitraum länger als sechs Wochen arbeitsunfähig waren; **Angaben zu Art und Dauer der Erkrankung** sind demgegenüber **nicht zulässig**.

— Die **namentliche Information der Personalvertretung** hat „regelmäßig“ zu erfolgen. Das Bundesverwaltungsgericht geht hier von einem flexiblen Zeitrahmen aus und hält insoweit eine Mitteilung **„in regelmäßigen Abständen, mindestens halbjährlich“** für ausreichend.

  Werden die jeweiligen Krankheitsdaten – wie in dem vom Verwaltungsgerichtshof zuletzt entschiedenen Fall – in der Dienststelle ohnehin monatlich ausgewertet, sodass für die Erstellung und Weitergabe der Namensliste keine zusätzliche Datenerfassung notwendig ist, kann auch eine monatliche Information der Personalvertretung in Betracht kommen.

— Die Dienststelle darf die **Namensliste** – ebenso wie die **Abdrucke der Anschreiben an die betroffenen Beschäftigten** – zudem **nur einem vom Personalrat bestimmten Mitglied** zur Verfügung stellen.

  Dieses Personalratsmitglied darf die ihm **auf diese Weise bekannt gewordenen personenbezogenen Informationen –** dem Rechtsgedanken des Art. 10 Abs. 1 Satz 2 Nr. 1 BayPVG in Verbindung mit Art. 69 Abs. 2 Satz 6 BayPVG entsprechend – **den übrigen Personalratsmitgliedern nicht offenbaren**.

— Der Personalrat darf die zur Verfügung gestellten Daten **nur** nutzen, um seinem **gesetzlichen Überwachungsauftrag nach § 84 Abs. 2 Satz 7 SGB IX** nachzukommen; eine **Nutzung zu anderen Zwecken** ist **unzulässig**.

— Wegen der Vertraulichkeit und der Sensibilität der betreffenden Daten hat der Personalrat sein **Augenmerk besonders auf die Auswahl des betreffenden Personalratsmitglieds** zu legen.

— Das vom Personalrat bestimmte Mitglied darf die ihm zur Verfügung gestellten Unterlagen **nur so lange aufbewahren, wie** dies **zur Aufgabenerfüllung im Rahmen des § 84 Abs. 2 Satz 7 SGB IX erforderlich** ist.

Eine Aufbewahrung ist daher regelmäßig dann nicht mehr erforderlich, wenn die Verpflichtungen des Arbeitgebers zur Anbietung und gegebenenfalls zur ordnungsgemäßen Durchführung des BEM überprüft wurden (zur Speicherung von Beschäftigtendaten beim Personalrat allgemein siehe meinen 25. Tätigkeitsbericht 2012 unter Nr. 11.7).

Nicht Gegenstand der genannten jüngsten Entscheidung des Bayerischen Verwaltungsgerichtshofs war die **namentliche Information der Schwerbehindertenvertretung**. Zu dieser Thematik verweise ich auf meine – weiterhin geltenden – Ausführungen unter Nr. 11.3.2 meines 26. Tätigkeitsberichts 2014.

Das Staatsministerium der Finanzen, für Landesentwicklung und Heimat hat den **BEM-Leitfaden** und das **BEM-Informationsblatt** an die geänderte Rechtsprechung des Bayerischen Verwaltungsgerichtshofs **angepasst**. Die Unterlagen wurden **mit mir abgestimmt** und sind im Bayerischen Behördennetz unter www.stmf.bybn.de abrufbar. Ich empfehle allen bayerischen öffentlichen – insbesondere staatlichen und kommunalen – Stellen, diese Unterlagen bei der Durchführung eines BEM zugrunde zu legen.

11.4 Ausstattung von Dienstfahrzeugen mit Ortungssystemen

In den letzten Jahren ist nicht nur in der Privatwirtschaft, sondern auch bei bayerischen öffentlichen Stellen – vor allem im Bereich der Kommunen – eine stetig zunehmende **Ausrüstung von Dienstfahrzeugen mit GPS-Ortungssystemen** zu beobachten. Die Ausstattung der Dienstfahrzeuge mit derartigen Ortungssystemen dient in erster Linie dem Zweck, die Fahrzeugeinsätze – insbesondere durch die Verringerung der Fahrzeiten zum nächsten Einsatzort – zu optimieren. In der Praxis werden nach meinen Erkenntnissen vor allem kommunale Bauhoffahrzeuge **zur optimalen Organisation des Betriebsablaufs** – etwa bei der Planung und Steuerung der Straßenreinigungs-/-pflegearbeiten oder des Winterdienstes – mit Ortungssystemen ausgerüstet.

So ist im Berichtszeitraum die Anzahl der Eingaben und Anfragen erneut wieder angestiegen, in denen sich sowohl betroffene Beschäftigte als auch öffentliche – staatliche wie kommunale – Stellen nach der Zulässigkeit einer Ausstattung von Dienstfahrzeugen mit Ortungssystemen – und insbesondere nach den bestehenden **datenschutzrechtlichen Grenzen** – bei mir erkundigen.

11.4.1 Erhebung personenbezogener Daten mittels Ortungssystemen

Mit Hilfe satellitengestützter Ortungssysteme ist eine Positionsbestimmung des Fahrzeugs, in aller Regel über Global Positioning System (GPS), möglich. Es kann jederzeit der geographische Standort des Fahrzeugs – und damit im Regelfall auch der **Aufenthaltsort** der/des **Beschäftigten** – exakt bestimmt werden. In der Folge können schließlich die Fahrzeit und die Fahrtroute der/des Beschäftigten (**Bewegungsmuster**) genau nachvollzogen werden. Erfasst werden – je nach System – zudem etwa auch Fahrtunterbrechungen nach Ort und Zeit, Geschwindigkeiten oder Verbrauchswerte; so können zusätzlich Rückschlüsse auf das **Fahrverhalten** gezogen werden.

Die auf diese Weise gewonnenen Informationen zum Aufenthaltsort der/des einzelnen Beschäftigten, zur von dieser/diesem gewählten und gefahrenen Route

und zu ihrem/seinem Fahrverhalten sind allesamt Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter natürlicher Personen und damit **personenbezogene Daten** im Sinne des Art. 4 Abs. 1 BayDSG.

Die Erhebung wie auch die Verarbeitung und Nutzung solcher personenbezogener Daten ist von Gesetzes wegen nicht ohne weiteres zulässig. Nach Art. 15 Abs. 1 BayDSG ist dies vielmehr nur dann der Fall, wenn das Bayerische Datenschutzgesetz oder eine andere Rechtsvorschrift die Erhebung, Verarbeitung oder Nutzung erlaubt oder anordnet oder die/der Betroffene eingewilligt hat; es bedarf also einer **Rechtsgrundlage**.

11.4.2 Einwilligung im Abhängigkeitsverhältnis

Damit eine Einwilligung eine tragfähige Rechtsgrundlage im Sinne des Art. 15 Abs. 1 Nr. 2 BayDSG darstellen kann, muss sie in erster Linie den gesetzlichen Anforderungen von Art. 15 Abs. 2 bis 4 und 7 BayDSG genügen. Danach muss eine **– datenschutzgerechte – Einwilligung insbesondere freiwillig**, informiert und grundsätzlich schriftlich erteilt werden; auch müssen die Betroffenen darauf hingewiesen werden, dass die Einwilligung ohne Angabe von Gründen und ohne nachteilige Folgen verweigert sowie jederzeit widerrufen werden kann.

In Anbetracht der strukturellen Abhängigkeit, in der ein(e) Beschäftigte(r) zu ihrem/seinem Dienstherrn steht, ist es im Dienstverhältnis – schon unabhängig vom Vorliegen der übrigen Rechtmäßigkeitsvoraussetzungen – stets problematisch, ob eine Einwilligung tatsächlich freiwillig, also ohne – zumindest gefühlten – (Gruppen-)Druck, erteilt wird. Hier bestehen **im Regelfall erhebliche Bedenken**.

Der Einsatz der gegenständlichen Ortungssysteme in Dienstfahrzeugen ist daher auf der Grundlage einer Einwilligung der Beschäftigten – wenn überhaupt – **nur in sehr engen Grenzen möglich**.

11.4.3 Datenschutzanforderungen an den Einsatz von Ortungssystemen

Als gesetzliche Rechtsgrundlage im Sinne des Art. 15 Abs. 1 Nr. 1 BayDSG für die **Erhebung von personenbezogenen Daten mittels Ortungssystemen** kommt bei bayerischen Beamtinnen und Beamten in erster Linie die – als allgemein gültiges Schutzprinzip für alle öffentlichen Bediensteten ebenso wie die übrigen Bestimmungen des bayerischen Personalaktenrechts im Grundsatz auch auf die nicht-verbeamteten Beschäftigten des bayerischen öffentlichen Dienstes entsprechend anzuwendende – Vorschrift des Art. 102 Bayerisches Beamtengesetz (BayBG) in Betracht. Nach Art. 102 BayBG darf der Dienstherr personenbezogene Daten über Beamte und Beamtinnen nur erheben, **soweit dies** (unter anderem) **zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist.**

Art. 102 BayBG Erhebung personenbezogener Daten
[1]Der Dienstherr darf personenbezogene Daten über Bewerber, Bewerberinnen, Beamte und Beamtinnen sowie ehemalige Beamte und Beamtinnen nur erheben, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des

Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift dies erlaubt. [2]Fragebogen, mit denen solche personenbezogenen Daten erhoben werden, bedürfen der Genehmigung durch die oberste Dienstbehörde.

Da es sich bei Ortungsdaten allerdings nicht um die Beamtin oder den Beamten betreffende Unterlagen handelt, die mit dem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen, stellen diese Daten keine Personalaktendaten im Sinne des § 50 Satz 2 Beamtenstatusgesetz, sondern vielmehr bloße **Sachaktendaten** dar.

Die **Verarbeitung und Nutzung der Ortungsdaten** richtet sich damit nach den allgemeinen Vorschriften des Bayerischen Datenschutzgesetzes; insbesondere ist hier die Vorschrift des Art. 17 BayDSG zu beachten.

Nach den genannten beamten- und datenschutzrechtlichen Vorschriften kommt es für die Beurteilung der **datenschutzrechtlichen Zulässigkeit** somit **entscheidend** darauf an, **ob und inwieweit** die mit dem Einsatz von Ortungssystemen verbundenen Datenerhebungen, -nutzungen und -verarbeitungen zur ordnungsgemäßen Aufgabenerfüllung der einsetzenden öffentlichen Stelle – im Wesentlichen also **zur Optimierung des Betriebsablaufs wie des Personaleinsatzes – erforderlich** sind. Dies ist nur dann der Fall, wenn die mit dem Einsatz der Ortungssysteme tatsächlich verbundenen Datenumgänge nicht nur die Aufgabenerfüllung des Dienstherrn objektiv unterstützen, fördern und beschleunigen, sondern auch zu den schutzwürdigen Interessen der Beschäftigten in einem angemessenen Verhältnis stehen. Insbesondere dürfen die – berechtigten – Informationsinteressen des Dienstherrn nicht auf andere, weniger in das Persönlichkeitsrecht der Beschäftigten eingreifende Weise gewahrt werden können.

Ob und inwieweit der Einsatz von Ortungssystemen nach Art und Umfang diesen Anforderungen in der Praxis genügen kann, lässt sich nicht für alle öffentlichen Stellen einheitlich und im Vorhinein beurteilen. Vielmehr hängt dies **maßgeblich** von den **Umständen des Einzelfalls** ab und kann daher letztlich meist **nur vor Ort abschließend beurteilt** werden. Aus Datenschutzsicht ist hier jedenfalls stets ein **strenger Maßstab** anzulegen.

Unabhängig davon gebe ich **folgende allgemeine Hinweise**:

— **Kein permanenter Kontrolldruck**

  Festzuhalten ist, dass eine **Dauerüberwachung unzulässig** ist. Unzulässig ist insoweit schon die Erhebung der Daten, nicht erst deren Nutzung und Verarbeitung.

  Nicht zulässig ist insbesondere eine **Überwachung auf Vorrat**, etwa für den Fall, dass das Dienstfahrzeug gestohlen wird.

  Insgesamt dürfen die Beschäftigten **keinem permanenten Kontrolldruck** ausgesetzt werden.

— **Keine Ortung bei Privatnutzung**

  Ist den Beschäftigten die **Nutzung des Dienstfahrzeugs zu privaten Zwecken** gestattet, so müssen sie währenddessen das **Ortungssystem deak-**

tivieren können. Denn die Dokumentation einer solchen – zulässigen – Privatnutzung ist zur Optimierung des Betriebsablaufs augenscheinlich nicht erforderlich.

Der (Weiter-)Betrieb des Ortungssystems während einer erlaubten Privatnutzung des Dienstfahrzeugs ist auf der Grundlage einer **Einwilligung der Beschäftigten nur in sehr engen Grenzen** möglich (siehe oben Nr. 11.4.2).

– **Verwendung von Ortungsdaten zur Dienstaufsicht**

Nicht von vornherein und in jedem Falle unzulässig ist eine **Verwendung von Ortungsdaten zu Zwecken der Dienstaufsicht**. So ist gemäß Art. 17 Abs. 3 Satz 1 Fall 1 BayDSG – im Rahmen der Verhältnismäßigkeit – eine Datenverarbeitung oder -nutzung für andere Zwecke möglich, wenn sie der Wahrnehmung von Aufsichts- oder Kontrollbefugnissen dient.

Aus Datenschutzsicht sollte aber von dieser Möglichkeit – auch zur Vermeidung eines unzulässigen permanenten Kontrolldrucks – **nur zurückhaltend** Gebrauch gemacht werden. Letztlich erscheint eine Verwendung von Ortungsdaten zur Dienstaufsicht nur im Falle eines hinreichenden, **tatsachengestützten Verdachts auf eine dienst- oder arbeitsrechtliche Pflichtverletzung** oder bei einem durch konkrete Tatsachen begründeten Verdacht auf eine **Straftat oder Ordnungswidrigkeit** denkbar.

– **Diebstahl des Dienstfahrzeugs**

Wenig problematisch ist es, wenn eine GPS-Ortung **erst aktiviert** wird, **wenn** ein Dienstfahrzeug **gestohlen wurde**.

In diesem Fall liegt schon keine Erhebung personenbezogener Daten einer/eines Beschäftigten vor; die daher dann einschlägige Rechtsgrundlage in Art. 16 BayDSG ist in ihren Voraussetzungen erfüllt. Die Datenverarbeitung und -nutzung ist sodann gemäß Art. 17 BayDSG gerechtfertigt.

11.4.4 Datenschutzrechtliche Freigabe

Die Ausrüstung dienstlicher Fahrzeuge mit Ortungssystemen bedarf, soweit dadurch personenbezogene Daten gewonnen werden, gemäß Art. 26 BayDSG der **vorherigen schriftlichen datenschutzrechtlichen Freigabe** durch die einsetzende öffentliche Stelle.

Die Freigabe ist nach Art. 26 Abs. 3 Satz 2 BayDSG von der oder dem behördlichen Datenschutzbeauftragten zu erteilen und gemäß Art. 27 BayDSG **in das Verfahrensverzeichnis aufzunehmen**.

11.4.5 Mitbestimmung des Personalrats

Zudem ist der Personalrat vor der Ausstattung dienstlicher Fahrzeuge mit Ortungssystemen zu beteiligen. Es ist ein Fall der **zwingenden Mitbestimmung** gemäß Art. 75a Abs. 1 Nr. 1 Bayerisches Personalvertretungsgesetz (BayPVG)

gegeben, da die Systeme an sich – was nach der Rechtsprechung bereits ausreichend ist – zur Überwachung des Verhaltens oder der Leistung der Beschäftigten stets geeignet sind, auch wenn sie im konkreten Fall hierzu nicht eingesetzt werden sollen.

Nicht zuletzt aus Transparenzgründen ist in diesem Zusammenhang dringend zu empfehlen, eine **Dienstvereinbarung** im Sinne des Art. 73 BayPVG abzuschließen.

In dieser Dienstvereinbarung sollte **insbesondere geregelt** werden,

- zu welchen **Zwecken** genau welche – gegebenenfalls in einer Anlage zur Dienstvereinbarung konkret zu benennenden – Daten mittels des Ortungssystems in welchem **Umfang** erhoben, verarbeitet oder genutzt werden; dabei ist die Dauer der Speicherung auf das für den jeweiligen Zweck unbedingt erforderliche Maß zu begrenzen,

- welche Personen **Zugriff** auf die gespeicherten Daten haben, wobei – wenn möglich – eine Protokollierung der Zugriffe erfolgen sollte,

- wann die Daten genau gelöscht werden; dabei sind generell kurzfristige **Löschvorgaben** zu machen,

- dass die Verwendung der Daten zur permanenten und allgemeinen Verhaltens- oder Leistungskontrolle ausgeschlossen ist.

  Zulässig sind allenfalls **Anlasskontrollen** im Falle eines durch konkrete Tatsachen begründeten Verdachts auf einen dienst-, arbeits-, straf- oder ordnungswidrigkeitenrechtlichen Verstoß sowie anlasslose **Stichproben**; in diesen Fällen darf die Auswertung des Datenmaterials allerdings nur unter Beteiligung der Personalvertretung und des behördlichen Datenschutzbeauftragten vorgenommen werden,

- dass während einer erlaubten Nutzung des Dienstfahrzeugs zu **privaten Zwecken** das Ortungssystem abschaltbar ist und

- dass die Beschäftigten über diese Vorgaben **unterrichtet** werden.

11.4.6 Weiterführende Hinweise

Ergänzend mache ich noch auf die **umfangreiche Ausarbeitung „Einsatz von Ortungssystemen und Beschäftigtendatenschutz“** der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen aufmerksam. Dieses Papier bezieht sich zwar in erster Linie auf den Einsatz von Ortungssystemen in der Privatwirtschaft; doch enthält es auch für öffentliche Stellen zahlreiche Anhaltspunkte zum datenschutzgerechten Umgang mit Ortungssystemen. Die Ausarbeitung ist auf der Homepage der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen https://www.ldi.nrw.de abrufbar.

11.5 Einstellung von Bedienstetenfotos ins behördeneigene Intranet

Im Berichtszeitraum hat sich eine große bayerische Kommune mit folgender Problemstellung an mich gewandt:

Schon nicht alle der etwa 500 kommunalen Mitarbeiterinnen und Mitarbeiter würden sich untereinander kennen. Insbesondere für neue Bedienstete sei das Kennenlernen aber besonders schwierig. Daher sei es sinnvoll, **ins behördeneigene Intranet Fotos von allen Mitarbeiterinnen und Mitarbeitern einzustellen**. Fraglich sei aber, ob eine Einstellung der Mitarbeiterfotos ins Intranet auch ohne Einwilligung der Betroffenen rechtlich zulässig sei.

Aus datenschutzrechtlicher Sicht nehme ich zu dieser – nach meinen Erfahrungen bayernweit im staatlichen wie im kommunalen Bereich anzutreffenden – Problematik wie folgt Stellung:

– Datenschutzrechtlich handelt es sich bei **Fotoaufnahmen** um **personenbezogene Daten** im Sinne des Art. 4 Abs. 1 BayDSG.

– Ebenso wie die Anfertigung stellt auch die Verwendung von Fotoaufnahmen einen **besonders schwerwiegenden Eingriff in das „Recht am eigenen Bild“** dar, das als Ausprägung des Allgemeinen Persönlichkeitsrechts nicht nur in §§ 22 ff. Kunsturheberrechtsgesetz einfachgesetzlich, sondern auch als Grundrecht in Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 Grundgesetz für die Bundesrepublik Deutschland verfassungsrechtlich besonders geschützt ist.

– **Grundrechtseingriffe** liegen dabei **auch** dann vor, wenn die Fotos nur für behördeninterne Zwecke angefertigt und verwendet werden, also etwa – wie hier – **zur Einstellung ins behördeneigene Intranet erstellt** werden sollen.

– Ohne datenschutzgerechte Einwilligung der Betroffenen sind die mit der Anfertigung und Verwendung von Fotoaufnahmen verbundenen Grundrechtseingriffe allerdings nur dann gerechtfertigt, wenn eine Rechtsvorschrift sie erlaubt oder anordnet (siehe Art. 15 Abs. 1 Nr. 1 BayDSG).

  Eine solche **Rechtsvorschrift** im Sinne des Art. 15 Abs. 1 Nr. 1 BayDSG besteht in diesem Zusammenhang **in Bayern allerdings nicht**.

– Vor diesem Hintergrund ist die Anfertigung ebenso wie die Veröffentlichung von Mitarbeiterfotos im Intranet einer bayerischen öffentlichen Stelle **nur mit datenschutzgerechter Einwilligung der Betroffenen** im Sinne des Art. 15 Abs. 1 Nr. 2 BayDSG rechtlich zulässig.

  Nach den vom bayerischen Gesetzgeber aufgestellten Vorgaben des Art. 15 Abs. 2 bis 4 und 7 BayDSG muss die Einwilligung insbesondere freiwillig, informiert und **grundsätzlich schriftlich** erteilt werden. An der **Freiwilligkeit** fehlt es beispielsweise, wenn die Betroffenen einem starken Gruppendruck ausgesetzt sind. Im Rahmen der **vollständigen Aufklärung** müssen die Betroffenen vor allem darüber informiert werden, zu welchem konkreten Zweck die Fotos gemacht werden, in welcher Form und wie lange die Fotos gespeichert werden, wer darauf Zugriff hat, an wen sie unter

Umständen weitergegeben werden und welche Gefahren für die Persönlichkeitsrechte mit der Einstellung in das Intranet möglicherweise verbunden sind. Die Betroffenen müssen somit eine konkrete Vorstellung über Ziel, Inhalt, Ablauf und Umfang der Datenerhebung und -verwendung erhalten können. Auch müssen die Betroffenen darauf hingewiesen werden, dass sie die Einwilligung ohne Angabe von Gründen und **ohne nachteilige Folgen verweigern sowie jederzeit widerrufen** können.

Diese Rechtsauffassung habe ich bereits in meinem 21. Tätigkeitsbericht 2004 unter Nr. 16.3.2 vertreten. Auch schon früher habe ich mich zu der gegenständlichen Thematik in diesem Sinne geäußert (siehe meinen 20. Tätigkeitsbericht 2002 unter Nr. 13.1.4). Die **Bedrohungen und Gefahren**, denen jeder **Betrieb eines Intranets** ausgesetzt ist, habe ich beispielsweise unter Nr. 2 meiner „Orientierungshilfe Datensicherheit beim Betrieb eines Intranets am Beispiel eines Landkreis-Behördennetzes“ (abrufbar von meiner Homepage https://www.datenschutz-bayern.de) im Einzelnen beschrieben. Auch und gerade im Zeitalter der allgegenwärtigen digitalen Fotografie halte ich diese **strengen rechtlichen Vorgaben für eine Einstellung von Bedienstetenfotos ins Intranet** einer bayerischen öffentlichen – staatlichen wie kommunalen – Stelle **zum Schutz der Persönlichkeitsrechte der Mitarbeiterinnen und Mitarbeiter** weiterhin für angemessen.

Mit meiner Auffassung übereinstimmend weist nicht zuletzt auch das **Standardwerk zum Bayerischen Datenschutzgesetz** darauf hin, dass behördeninternen – gedruckten wie elektronischen – **Personalnachrichten nur mit Zustimmung der Betroffenen Fotos beigefügt** werden dürfen (Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Kommentar und Handbuch für Datenschutzverantwortliche, Teil C Handbuch für Datenschutzverantwortliche, Abschnitt XII. Datenschutz in der Gemeinde, Nr. 9 Personalnachrichten in gemeindeinternen Mitteilungen, Seite 60.14, München, Stand: 2016).

Die von den bayerischen öffentlichen Stellen zu beachtende Rechtslage ist im Übrigen **mit den rechtlichen Vorgaben für die bayerischen privatwirtschaftlichen Unternehmen vergleichbar**. So hat das für die bayerischen nicht-öffentlichen Stellen zuständige Landesamt für Datenschutzaufsicht in seinem 3. Tätigkeitsbericht 2008 unter Nr. 10.3 „Mitarbeiterfotos im Intranet“ ausdrücklich festgestellt, dass die Veröffentlichung von Fotos von Beschäftigten privatwirtschaftlicher Unternehmen im betrieblichen Intranet ebenfalls **nur mit Einwilligung der Betroffenen bei ausdrücklichem Hinweis auf die Freiwilligkeit rechtlich zulässig** ist. Der genannte Tätigkeitsbericht steht auf der Homepage des Landesamts für Datenschutzaufsicht https://www.lda.bayern.de zum Abruf bereit.

11.6 Entgegennahme von Dienst- und Arbeitsunfähigkeitsbescheinigungen

Im Berichtszeitraum haben mir zahlreiche Eingaben und Anfragen gezeigt, dass bei bayerischen öffentlichen – staatlichen wie kommunalen – Stellen immer wieder Unsicherheit darüber besteht, **wer innerbehördlich für die Annahme der Dienst- und Arbeitsunfähigkeitsbescheinigungen** von bayerischen Beamtinnen und Beamten sowie von nicht-verbeamteten Beschäftigten des bayerischen öffentlichen Dienstes **zuständig ist**.

Nach Art. 95 Abs. 1 Satz 2 Bayerisches Beamtengesetz (BayBG) ist eine Dienstunfähigkeit wegen Krankheit auf Verlangen nachzuweisen; dauert die Dienstunfähigkeit länger als drei Kalendertage, so ist gemäß § 21 Abs. 2 Satz 1 Verordnung

über den Urlaub der bayerischen Beamten und Richter (UrlV) spätestens am vierten Kalendertag, auf Verlangen auch früher, ein ärztliches Zeugnis vorzulegen. Vergleichbares gilt nach § 5 Gesetz über die Zahlung des Arbeitsentgelts an Feiertagen und im Krankheitsfall (EFZG) für den Nachweis einer Arbeitsunfähigkeit bei Tarifbeschäftigten des bayerischen öffentlichen Dienstes.

Art. 95 BayBG Fernbleiben vom Dienst
(1) [1]Beamte und Beamtinnen dürfen dem Dienst nicht ohne Genehmigung ihrer Dienstvorgesetzten fernbleiben. [2]Dienstunfähigkeit wegen Krankheit ist auf Verlangen nachzuweisen. [3]Wollen Beamte und Beamtinnen während einer Krankheit ihren Wohnort verlassen, so haben sie dies vorher ihren Dienstvorgesetzten anzuzeigen und ihren Aufenthaltsort anzugeben.

§ 21 UrlV Nachweis vorübergehender Dienstunfähigkeit
(1) [1]Eines Urlaubs bedarf es nicht bei Dienstunfähigkeit wegen Krankheit. [2]Die Erkrankung und deren voraussichtliche Dauer sind dem Dienstvorgesetzten spätestens am folgenden Arbeitstag anzuzeigen. [3]In gleicher Weise ist die Beendigung der Krankheit anzuzeigen.
(2) [1]Dauert die Dienstunfähigkeit länger als drei Kalendertage, so ist spätestens am vierten Kalendertag, auf Verlangen des Dienstvorgesetzten auch früher, ein ärztliches Zeugnis vorzulegen. [2]Auf Anordnung des Dienstvorgesetzten ist ein amtsärztliches Zeugnis beizubringen.

§ 5 EFZG Anzeige- und Nachweispflichten
(1) Der Arbeitnehmer ist verpflichtet, dem Arbeitgeber die Arbeitsunfähigkeit und deren voraussichtliche Dauer unverzüglich mitzuteilen. Dauert die Arbeitsunfähigkeit länger als drei Kalendertage, hat der Arbeitnehmer eine ärztliche Bescheinigung über das Bestehen der Arbeitsunfähigkeit sowie deren voraussichtliche Dauer spätestens an dem darauffolgenden Arbeitstag vorzulegen. Der Arbeitgeber ist berechtigt, die Vorlage der ärztlichen Bescheinigung früher zu verlangen. Dauert die Arbeitsunfähigkeit länger als in der Bescheinigung angegeben, ist der Arbeitnehmer verpflichtet, eine neue ärztliche Bescheinigung vorzulegen. Ist der Arbeitnehmer Mitglied einer gesetzlichen Krankenkasse, muß die ärztliche Bescheinigung einen Vermerk des behandelnden Arztes darüber enthalten, daß der Krankenkasse unverzüglich eine Bescheinigung über die Arbeitsunfähigkeit mit Angaben über den Befund und die voraussichtliche Dauer der Arbeitsunfähigkeit übersandt wird.

Zuständig für die Entgegennahme der Dienstunfähigkeitsbescheinigung **sind die Dienstvorgesetzten**; dies ergibt sich bereits unmittelbar aus Art. 95 BayBG sowie aus § 21 UrlV. Dienstvorgesetzte sind dabei nach Art. 3 Satz 1 BayBG diejenigen, die für beamtenrechtliche Entscheidungen über die persönlichen Angelegenheiten der ihnen nachgeordneten Beamten und Beamtinnen zuständig sind. Abzugrenzen sind die Dienstvorgesetzten von den (Fach-)Vorgesetzten. (Fach-)Vorgesetzte sind gemäß Art. 3 Satz 2 BayBG diejenigen, die Beamten und Beamtinnen für ihre dienstliche Tätigkeit Anordnungen (Weisungen) erteilen können. Fachvorgesetzte sind damit grundsätzlich nicht zur Entgegennahme von Dienstunfähigkeitsbescheinigungen berufen. Für die Entgegennahme der Arbeitsunfähigkeitsbescheinigungen von Tarifbeschäftigten des bayerischen öffentlichen Dienstes gilt im Wesentlichen Vergleichbares.

Jedoch dürfen Dienstvorgesetzte diese **Zuständigkeit delegieren**, gegebenenfalls **auch an die jeweiligen (Fach-)Vorgesetzten**. Ein praktisches Bedürfnis für die damit bezweckte schnellstmögliche Information der (Fach-)Vorgesetzten ist

oftmals nicht von der Hand zu weisen: Schließlich müssen die (Fach-)Vorgesetzten im Falle der Dienst- oder Arbeitsunfähigkeit eines Mitarbeiters oder einer Mitarbeiterin unverzüglich die notwendigen Vertretungsregelungen treffen.

Dass Dienstvorgesetzte ihre Aufgaben nicht nur persönlich, sondern auch durch – nach internen Regelungen damit betraute – Beschäftigte ihrer Behörde wahrnehmen können, entspricht allgemeiner Verwaltungspraxis, die auch das Bundesverwaltungsgericht gebilligt hat (siehe Beschluss vom 21. August 1995 – 2 B 83/95). Im vorliegenden Zusammenhang ist allerdings zu beachten, dass Dienst- und Arbeitsunfähigkeitsbescheinigungen besonders sensible (Gesundheits-)Daten enthalten (vgl. auch Art. 15 Abs. 7 BayDSG). Aus Datenschutzsicht ist daher zu verlangen, dass die Aufgabe der Entgegennahme der Dienst- und Arbeitsunfähigkeitsbescheinigungen **nur an jeweils konkret benannte Personen delegiert** wird – und nicht etwa alle beliebigen Beschäftigten einer fachlichen Organisationseinheit zur Entgegennahme berechtigt werden.

Dienst- und Arbeitsunfähigkeitsbescheinigungen dürfen im Regelfall zwar **keine Aussagen über die Art und Ursache der Dienst- oder Arbeitsunfähigkeit** enthalten. Dennoch stellen sie **Personalaktendaten** im Sinne des § 50 Satz 2 Gesetz zur Regelung des Statusrechts der Beamtinnen und Beamten in den Ländern dar, da es sich um die Beamtin oder den Beamten betreffende Unterlagen handelt, die mit dem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen. Für den Zugang zu Personalaktendaten gilt die **„doppelte Zugangsbeschränkung“** des Art. 103 BayBG: Danach dürfen Zugang zur Personalakte – zum einen – nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und – zum anderen – nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist. Als allgemein gültige Schutzprinzipien für alle öffentlichen Bediensteten sind die detaillierten Regelungen des Personalaktenrechts der bayerischen Beamtinnen und Beamten dabei nach meiner seit jeher vertretenen Auffassung im Grundsatz auch auf die nicht-verbeamteten Beschäftigten des bayerischen öffentlichen Dienstes entsprechend anzuwenden.

Art. 103 BayBG Zugang zur Personalakte
Zugang zur Personalakte dürfen nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist; dies gilt auch für den Zugang im automatisierten Abrufverfahren.

Wird also die Aufgabe der Entgegennahme der Dienst- und Arbeitsunfähigkeitsbescheinigungen innerbehördlich von der/dem Dienstvorgesetzten an eine oder mehrere Personen außerhalb der Personalstelle delegiert, so müssen diese die Dienst- und Arbeitsunfähigkeitsbescheinigungen **– nach Ergreifung der für die fachliche Organisationseinheit jeweils notwendigen Sofortmaßnahmen –** zur weiteren Behandlung, insbesondere zur Aufbewahrung, **umgehend an die Personalstelle weiterleiten**. Nur so kann dem Sinn und Zweck des Art. 103 BayBG Rechnung getragen werden, den Kreis der mit Personalaktendaten befassten Personen auf das – auch in zeitlicher Hinsicht – unbedingt erforderliche Maß zu beschränken.

11.7 Zeitliche Grenzen der Aufbewahrung von Arzneimittelverordnungen bei den Beihilfestellen

Im Zuge der vom Deutschen Bundestag Ende 2010 beschlossenen Neuordnung des Arzneimittelmarktes ist am 1. Januar 2011 das „Gesetz über Rabatte für Arzneimittel“ (im Folgenden: AMRabG) in Kraft getreten. Dieses Gesetz verpflichtet die pharmazeutischen Unternehmer, die den gesetzlichen Krankenkassen gewährten **Rabatte auf bestimmte verschreibungspflichtige Arzneimittel** unter anderem auch den bayerischen – insbesondere staatlichen und kommunalen – **Trägern der beamtenrechtlichen Beihilfe einzuräumen**. Zur Überprüfung der von den Beihilfeträgern eingeforderten Rabatte sieht § 3 AMRabG vor, dass in begründeten Fällen sowie in Stichproben ein von den pharmazeutischen Unternehmern beauftragter Treuhänder die dafür erforderlichen personenbezogenen Daten aus den einschlägigen Arzneimittelverordnungen erhalten darf.

§ 3 AMRabG Prüfung durch Treuhänder
[1]Die pharmazeutischen Unternehmer können in begründeten Fällen sowie in Stichproben die Abrechnung der Abschläge durch einen Treuhänder überprüfen lassen. [2]Hierfür dürfen an den Treuhänder die für den Prüfungszweck erforderlichen personenbezogenen Daten übermittelt werden. [3]Zum Nachweis dürfen auch Reproduktionen von digitalisierten Verordnungsblättern vorgelegt werden. [4]Der Treuhänder darf die ihm übermittelten Daten nur zum Zwecke der Überprüfung der Abrechnung der Abschläge verarbeiten und nutzen. [5]Weitere Einzelheiten der Prüfung können in der Vereinbarung nach § 2 Satz 4 geregelt werden.

11.7.1 Verfahren der Arzneimittelrabattierung

Die Arzneimittelrabatte werden nicht schon direkt bei Erwerb der Arzneimittel durch die bayerischen Beamtinnen und Beamten in der Apotheke abgezogen. Vielmehr müssen die Beamtinnen und Beamten auch die Verordnungen über Arzneimittel im Sinne des § 1 AMRabG erst – wie gewohnt – bei der zuständigen Beihilfestelle einreichen. Nach Gewährung der entsprechenden Beihilfen fordern sodann die Beihilfeträger die Arzneimittelrabatte über eine „zentrale Stelle“ im Sinne des § 2 Satz 1 AMRabG bei den pharmazeutischen Unternehmern ein.

In datenschutzrechtlicher Hinsicht hat dieses komplexe Verfahren der nachträglichen Rabattgewährung zur Folge, dass es sich bei den **personenbezogenen Daten aus den Arzneimittelverordnungen** ab der Geltendmachung der Arzneimittelaufwendungen bei den bayerischen Beihilfestellen um **Personalaktendaten der jeweiligen Beamtinnen und Beamten** handelt, die den **besonderen Schutzvorschriften** der § 50 Beamtenstatusgesetz, Art. 102 ff. Bayerisches Beamtengesetz (BayBG) unterliegen.

Damit der von den pharmazeutischen Unternehmern eingerichtete Treuhänder die Rechtmäßigkeit der Rabatteinforderung überprüfen kann, dürfen die Beihilfestellen die dafür erforderlichen personenbezogenen Daten aus den Arzneimittelverordnungen im Sinne des § 1 AMRabG **– ausschließlich zum Zweck der Prüfung gemäß § 3 AMRabG – auf Anforderung an den Treuhänder übermitteln**; Rechtsgrundlage für diese Übermittlung von Personalaktendaten ist die Vorschrift des Art. 105 Satz 5 BayBG.

In der Regel erfolgt die **Prüfung** durch den Treuhänder **allerdings erst geraume Zeit nach der Einforderung und Gewährung der Rabatte**. Daher dürfen die entsprechenden Arzneimittelverordnungen nicht sofort an die Beihilfeberechtigten zurückgegeben werden, sondern müssen zunächst bei den Beihilfestellen verbleiben. Dort dürfen sie erst vernichtet werden, wenn sie für die Prüfung nicht mehr benötigt werden. Die gesetzlichen Vorgaben zum Umgang der Beihilfestellen mit den Arzneimittelverordnungen im Sinne des § 1 AMRabG enthält die personalaktenrechtliche Vorschrift des Art. 110 Abs. 2 Satz 3 BayBG.

Insgesamt verweise ich in diesem Zusammenhang auf meinen Beitrag im 25. Tätigkeitsbericht 2012 unter Nr. 11.1.2, in dem ich mich mit der datenschutzkonformen Geltendmachung von Arzneimittelrabatten bereits eingehend auseinandergesetzt habe.

Art. 110 BayBG Aussonderung von Personalakten
(2) [1]Unterlagen über Beihilfen, Heilfürsorge, Heilverfahren, Unterstützungen, Erholungsurlaub, Erkrankungen sowie Umzugs- und Reisekosten sind fünf Jahre nach Ablauf des Jahres, in dem die Bearbeitung des einzelnen Vorgangs abgeschlossen wurde, aufzubewahren. [2]Unterlagen, aus denen die Art der Erkrankung ersichtlich ist, sind unverzüglich zurückzugeben oder zu vernichten, wenn sie für den Zweck, zu dem sie vorgelegt worden sind, nicht mehr benötigt werden. [3]Arzneimittelverordnungen im Sinn des § 1 des Gesetzes über Rabatte für Arzneimittel sind zur Geltendmachung von Rabatten nach diesem Gesetz nicht zurückzugeben; die Vernichtung dieser Arzneimittelverordnungen erfolgt auf der Grundlage der nach § 3 Satz 5 des Gesetzes über Rabatte für Arzneimittel zu treffenden Vereinbarungen unverzüglich, sobald sie für die dort geregelten Zwecke nicht mehr benötigt werden.

11.7.2 Problematik der Aufbewahrung von Arzneimittelverordnungen

Seit dem Inkrafttreten des Gesetzes über Rabatte für Arzneimittel zum 1. Januar 2011 sind mittlerweile mehrere Jahre vergangen. In Anbetracht der strengen Vorgaben des bayerischen Personalaktenrechts stellte sich daher im Berichtszeitraum immer dringlicher die **Frage, wie lange nun genau die bayerischen Beihilfestellen die Arzneimittelverordnungen** im Sinne des § 1 AMRabG der beilhilfeberechtigten bayerischen Beamtinnen und Beamten **für eine (mögliche) Überprüfung der Rabatteinforderung durch den Treuhänder aufbewahren müssen und auch dürfen**.

Denn die gegenständlichen Arzneimittelverordnungen enthalten nicht nur besonders sensible Gesundheitsdaten im Sinne des Art. 15 Abs. 7 BayDSG, sondern stellen auch Unterlagen dar, aus denen – zumindest mittelbar – die Art der Erkrankung ersichtlich ist. Damit wären sie an sich gemäß der Vorschrift des Art. 110 Abs. 2 Satz 2 BayBG nach der Erstattung unverzüglich zurückzugeben oder zu vernichten. Allerdings wird dieser **Grundsatz der unverzüglichen Rückgabe oder Vernichtung** im Hinblick auf die Arzneimittelverordnungen im Sinne des § 1 AMRabG durch Art. 110 Abs. 2 Satz 3 BayBG in zweierlei Hinsicht **modifiziert**: Zum einen wird die Rückgabe an den Beihilfeberechtigten gänzlich ausgeschlossen (Halbsatz 1), zum anderen greift die Pflicht zur unverzüglichen Vernichtung erst nach Ablauf der – in den nach § 3 Satz 5 AMRabG in Verbindung mit § 2 Satz 4 AMRabG zu treffenden Vereinbarungen festgelegten – Überprüfungsfrist (Halbsatz 2).

Nicht explizit geregelt ist aber, welche Aufbewahrungsfrist gilt, wenn auch in den nach § 3 Satz 5 AMRabG in Verbindung mit § 2 Satz 4 AMRabG zwischen den Trägern der Kosten in Krankheits-, Pflege- und Geburtsfällen nach beamtenrechtlichen Vorschriften und dem Verband der privaten Krankenversicherung einerseits sowie den für die Wahrnehmung der wirtschaftlichen Interessen gebildeten Spitzenorganisationen der pharmazeutischen Unternehmer andererseits zu treffenden Vereinbarungen gar keine Überprüfungsfrist festgelegt wird.

11.7.3 Keine ausdrückliche Festlegung einer Überprüfungshöchstfrist

Bereits frühzeitig habe ich daher das innerhalb der Staatsregierung für das öffentliche Dienstrecht federführend zuständige Staatsministerium der Finanzen, für Landesentwicklung und Heimat auf die Problematik der fehlenden – vertraglichen oder gesetzlichen – Festlegung einer Überprüfungsfrist aufmerksam gemacht.

Dabei habe ich das Finanzministerium im Interesse der bayerischen Beihilfeberechtigten gebeten, alle ihm zur Verfügung stehenden Maßnahmen zu einer datenschutzgerechten Klärung der Rechtslage – also zu einer ausdrücklichen Festlegung einer angemessenen, möglichst kurzen Überprüfungshöchstfrist – zu ergreifen. Da die aufgezeigte Problematik bundesweit besteht, habe ich dem Finanzministerium vorgeschlagen, die auf Ebene der für Beihilfefragen zuständigen obersten Dienstbehörden in Bund und Ländern bestehenden Koordinierungsgremien baldmöglich mit dieser Problematik zu befassen. Aus datenschutzrechtlicher Sicht sollte das Finanzministerium dabei in erster Linie auf eine ausdrückliche Festlegung einer Überprüfungshöchstfrist in den Vereinbarungen nach § 3 Satz 5 AMRabG in Verbindung mit § 2 Satz 4 AMRabG hinwirken. Wenn eine solche einvernehmliche Festlegung allerdings nicht erreichbar sein sollte, sollte nach meiner Auffassung eine ausdrückliche Festlegung einer angemessenen, möglichst kurzen Überprüfungsfrist in § 3 AMRabG selbst erfolgen. Hierzu könnte aus meiner Sicht etwa eine entsprechende Gesetzesinitiative im Bundesrat eingebracht werden.

Nach weitgehendem Abschluss der langwierigen Meinungsbildung in den für Beihilfefragen zuständigen Gremien des Bundes und der Länder hat mir das Staatsministerium der Finanzen, für Landesentwicklung und Heimat im Ergebnis Folgendes mitgeteilt:

— Ein Abschluss der entsprechend der Vorstellung des Bundesgesetzgebers gemäß § 3 Satz 5 AMRabG in Verbindung mit § 2 Satz 4 AMRabG zu treffenden Vereinbarungen – und damit auch eine einvernehmliche Festlegung einer Überprüfungshöchstfrist – zwischen den Trägern der Kosten in Krankheits-, Pflege- und Geburtsfällen nach beamtenrechtlichen Vorschriften und dem Verband der privaten Krankenversicherung einerseits sowie den für die Wahrnehmung der wirtschaftlichen Interessen gebildeten Spitzenorganisationen der pharmazeutischen Unternehmer andererseits sei bislang noch nicht zustande gekommen.

— Nach Auffassung der pharmazeutischen Unternehmer könnten die Überprüfungen der Rabatte vielmehr jederzeit, sogar noch nach mehreren Jahren, vorgenommen werden und die Rabatte somit für einen unbegrenzten Zeitraum zurückgefordert werden.

In diesem Falle müssten dann allerdings auch die bayerischen Beihilfestellen die **gegenständlichen Arzneimittelverordnungen als Nachweise für eine rechtmäßige Rabatteinforderung zeitlich unbegrenzt aufbewahren**. Bei einer Vernichtung der für eine rechtmäßige Rabatteinforderung notwendigen Nachweise würden die bayerischen Beihilfeträger ansonsten hohe Rabattrückzahlungen riskieren.

— Darüber hinaus **zögen verschiedene pharmazeutische Unternehmer die Verfassungsmäßigkeit des Gesetzes über Rabatte für Arzneimittel insgesamt in Zweifel** und verweigerten daher entsprechende Rabattzahlungen. Mittlerweile seien sogar mehrere Verfahren bei obersten Gerichten anhängig; eine Überprüfung durch das Bundesverfassungsgericht sei zudem nicht auszuschließen.

  Vor diesem Hintergrund würden auf Bundesebene **Änderungen des Gesetzes über Rabatte für Arzneimittel derzeit nicht in Betracht gezogen**.

11.7.4 Aber: Zeitliche Grenzen der Überprüfung und der Aufbewahrung

Da somit eine einvernehmliche Vereinbarung ebenso wenig wie eine gesetzliche Festlegung einer bestimmten Überprüfungshöchstfrist absehbar ist, stellt sich die **Frage, wie lange die bayerischen – insbesondere staatlichen und kommunalen – Beihilfestellen die Arzneimittelverordnungen im Sinne des § 1 AMRabG auf der Grundlage der gegenwärtigen Rechtslage aufbewahren dürfen**. Die Beantwortung dieser Frage hängt entscheidend davon ab, wie lange die bayerischen Beihilfeträger mit Rabattüberprüfungen und gegebenenfalls Rückforderungsansprüchen der pharmazeutischen Unternehmer zu rechnen haben.

Nach meiner Auffassung unterliegt die Geltendmachung möglicher Rabattrückzahlungsansprüche durch die pharmazeutischen Unternehmer und damit auch die Aufbewahrung der gegenständlichen Arzneimittelverordnungen durch die bayerischen Beihilfestellen **zeitlichen Grenzen**. Im Einzelnen:

— Sofern die Ansprüche der pharmazeutischen Unternehmer auf Rückforderung von Arzneimittelrabatten als **öffentlich-rechtliche Ansprüche** einzuordnen sind, ist die Vorschrift des Art. 71 Abs. 1 Gesetz zur Ausführung des Bürgerlichen Gesetzbuchs und anderer Gesetze (AGBGB) einschlägig.

  Nach Art. 71 Abs. 1 Satz 1 Nr. 2, Satz 2 Halbsatz 1 AGBGB **erlöschen** die auf eine Geldzahlung gerichteten öffentlich-rechtlichen Ansprüche gegen den Freistaat Bayern, eine bayerische Gemeinde oder einen bayerischen Gemeindeverband **drei Jahre** nach Schluss des Jahres, in dem der Berechtigte von den den Anspruch begründenden Umständen und der Person des Verpflichteten Kenntnis erlangt oder ohne grobe Fahrlässigkeit erlangen müsste, jedoch nicht vor dem Schluss des Jahres, in dem der Anspruch entstanden ist. Somit spricht vieles dafür, dass die Rabattrückforderungsansprüche drei Jahre nach Schluss des Jahres, in dem die Rabatte gegenüber den pharmazeutischen Unternehmern geltend gemacht wurden, erlöschen.

  In jedem Falle erlöschen die Ansprüche der pharmazeutischen Unternehmer auf Rückforderung von Arzneimittelrabatten jedoch ohne Rücksicht auf die Kenntnis der anspruchsbegründenden Umstände und der Person

des Verpflichteten nach Art. 71 Abs. 1 Satz 4 AGBGB **spätestens in zehn Jahren** von ihrer Entstehung an.

Art. 71 AGBGB Erlöschen
(1) [1]Die auf eine Geldzahlung gerichteten öffentlich-rechtlichen Ansprüche
1. des Freistaates Bayern, einer bayerischen Gemeinde oder eines bayerischen Gemeindeverbands,
2. gegen den Freistaat Bayern, eine bayerische Gemeinde oder einen bayerischen Gemeindeverband
erlöschen, soweit nicht anderes bestimmt ist, in drei Jahren. [2]Die Frist beginnt mit dem Schluss des Jahres, in dem der Berechtigte von den den Anspruch begründenden Umständen und der Person des Verpflichteten Kenntnis erlangt oder ohne grobe Fahrlässigkeit erlangen müsste, jedoch nicht vor dem Schluss des Jahres, in dem der Anspruch entstanden ist. [3]Soweit der Freistaat Bayern, eine bayerische Gemeinde oder ein bayerischer Gemeindeverband berechtigt ist, ist die Kenntnis der zuständigen Behörde erforderlich. [4]Ohne Rücksicht auf die Kenntnis erlischt der Anspruch in 10 Jahren von seiner Entstehung an.

— Nichts anderes gilt, wenn die Ansprüche der pharmazeutischen Unternehmer auf Rückforderung von Arzneimittelrabatten nicht als öffentlich-rechtliche, sondern als **zivilrechtliche Ansprüche** einzuordnen sind. Denn zivilrechtliche Ansprüche unterliegen nach §§ 194 ff. Bürgerliches Gesetzbuch (BGB) der Verjährung.

Der Beginn der regelmäßigen **Verjährungsfrist von drei Jahren** (§ 195 BGB) hängt unter anderem von der Kenntnis oder dem Kennenmüssen von Anspruch und Schuldner ab (siehe § 199 Abs. 1 BGB). Da der Bundesgesetzgeber die Funktion des Treuhänders einzig und allein zu dem Zweck in § 3 AMRabG gesetzlich eingerichtet hat, die Rechtmäßigkeit der Rabatteinforderung zu überprüfen, spricht vieles dafür, dass im vorliegenden Zusammenhang bereits die Fallkonstellation des § 199 Abs. 1 Nr. 2 Fall 2 BGB einschlägig ist und die dreijährige Verjährungsfrist mit dem Schluss des jeweiligen Jahres der Rabattgewährung beginnt. Der Treuhänder handelt grob fahrlässig, wenn er nicht in der Lage ist, seiner einzigen – unmittelbar vom Bundesgesetzgeber gestellten – Aufgabe innerhalb von drei Jahren nach Schluss des Jahres der Rabattgewährung wirkungsvoll nachzukommen.

Jedenfalls sind aber in § 199 Abs. 2 bis 4 BGB kenntnisunabhängige **Verjährungshöchstfristen** vorgesehen. So verjähren nach § 199 Abs. 4 BGB andere Ansprüche als Schadensersatzansprüche und erbrechtliche Ansprüche – und damit auch die gegenständlichen Rückforderungsansprüche – ohne Rücksicht auf die Kenntnis oder grob fahrlässige Unkenntnis **in zehn Jahren** von ihrer Entstehung an.

§ 199 BGB Beginn der regelmäßigen Verjährungsfrist und Verjährungshöchstfristen
(1) Die regelmäßige Verjährungsfrist beginnt, soweit nicht ein anderer Verjährungsbeginn bestimmt ist, mit dem Schluss des Jahres, in dem
1. der Anspruch entstanden ist und
2. der Gläubiger von den den Anspruch begründenden Umständen und der Person des Schuldners Kenntnis erlangt oder ohne grobe Fahrlässigkeit erlangen müsste.

(2) Schadensersatzansprüche, die auf der Verletzung des Lebens, des Körpers, der Gesundheit oder der Freiheit beruhen, verjähren ohne Rücksicht auf ihre Entstehung und die Kenntnis oder grob fahrlässige Unkenntnis in 30 Jahren von der Begehung der Handlung, der Pflichtverletzung oder dem sonstigen, den Schaden auslösenden Ereignis an.
(3) [1]Sonstige Schadensersatzansprüche verjähren
1. ohne Rücksicht auf die Kenntnis oder grob fahrlässige Unkenntnis in zehn Jahren von ihrer Entstehung an und
2. ohne Rücksicht auf ihre Entstehung und die Kenntnis oder grob fahrlässige Unkenntnis in 30 Jahren von der Begehung der Handlung, der Pflichtverletzung oder dem sonstigen, den Schaden auslösenden Ereignis an.
[2]Maßgeblich ist die früher endende Frist.
(3a) Ansprüche, die auf einem Erbfall beruhen oder deren Geltendmachung die Kenntnis einer Verfügung von Todes wegen voraussetzt, verjähren ohne Rücksicht auf die Kenntnis oder grob fahrlässige Unkenntnis in 30 Jahren von der Entstehung des Anspruchs an.
(4) Andere Ansprüche als die nach den Absätzen 2 bis 3a verjähren ohne Rücksicht auf die Kenntnis oder grob fahrlässige Unkenntnis in zehn Jahren von ihrer Entstehung an.
(5) Geht der Anspruch auf ein Unterlassen, so tritt an die Stelle der Entstehung die Zuwiderhandlung.

Meine Rechtsauffassung habe ich dem Staatsministerium der Finanzen, für Landesentwicklung und Heimat im Einzelnen dargelegt. Die Rückforderung von Rabatten durch die pharmazeutischen Unternehmer unterliegt bereits nach der geltenden Rechtslage zeitlichen Grenzen. Für eine zeitlich unbegrenzte Aufbewahrung der Arzneimittelverordnungen im Sinne des § 1 AMRabG bei den bayerischen Beihilfestellen zur Abwehr möglicher Rückforderungsansprüche besteht daher von vornherein kein Raum. Da die Ansprüche der pharmazeutischen Unternehmer spätestens nach zehn Jahren erlöschen oder verjähren, ist auch die **Aufbewahrung der einschlägigen Arzneimittelverordnungen bei den bayerischen – insbesondere staatlichen und kommunalen – Beihilfestellen höchstens für die Dauer von zehn Jahren zulässig**.

In diesem Zusammenhang habe ich das Finanzministerium zudem darum gebeten, die **pharmazeutischen Unternehmer baldmöglich in geeigneter Weise darauf aufmerksam zu machen**, dass die Geltendmachung von Rückforderungsansprüchen gegenüber bayerischen Beihilfeträgern zeitlich nicht unbegrenzt möglich ist, sondern bereits nach der gegenwärtigen Rechtslage zeitlichen Grenzen unterliegt.

Erfreulicherweise hat sich das **Staatsministerium der Finanzen, für Landesentwicklung und Heimat meiner Rechtsauffassung angeschlossen**. Die bayerischen Beihilfestellen haben somit die ersten seit dem Inkrafttreten des Gesetzes über Rabatte für Arzneimittel aufbewahrten Verordnungen über Arzneimittel im Sinne des § 1 AMRabG aus dem Jahr 2011 sukzessive ab dem 1. Januar 2021 zu vernichten.

11.8 Einsicht in Personalakten durch Gemeinderats-„Referent“

Art. 45 Abs. 1 der Gemeindeordnung für den Freistaat Bayern (GO) sieht vor, dass der Gemeinderat sich eine Geschäftsordnung zu geben hat. Nach dem Vorschlag des § 3 Abs. 3 der vom Bayerischen Gemeindetag herausgegebenen „Muster-

Geschäftsordnung für den Gemeinderat-Marktgemeinderat-Stadtrat“ (Stand: März 2014 – im Folgenden: MGOGR) kann hier der Gemeinderat unter anderem die Regelung treffen, zur Vorbereitung seiner Entscheidungen durch besonderen Beschluss einzelnen seiner Mitglieder bestimmte Aufgabengebiete (Referate) zur Bearbeitung zuzuteilen und sie insoweit mit der Überwachung der gemeindlichen Verwaltungstätigkeit zu betrauen (Art. 46 Abs. 1 Satz 2, Art. 30 Abs. 3 GO).

Sinn und Zweck dieser vom Bayerischen Gemeindetag empfohlenen Einrichtung von **Gemeinderats-„Referenten“** ist es, die Arbeit im Gemeinderat durch **Spezialisierung einzelner Gemeinderatsmitglieder auf bestimmte Fachgebiete** zu erleichtern. Diesen Gemeinderats-„Referenten“ soll dementsprechend nach dem Vorschlag des § 3 Abs. 5 MGOGR ein gegenüber dem ersten Bürgermeister geltend zu machendes **Recht auf Akteneinsicht innerhalb ihres Aufgabenbereichs** zustehen, **sofern Gründe der Geheimhaltungsverpflichtung nicht entgegenstehen**.

§ 3 MGOGR Rechtsstellung der ehrenamtlichen Gemeinderatsmitglieder, Befugnisse
(3) Der Gemeinderat kann zur Vorbereitung seiner Entscheidungen durch besonderen Beschluss einzelnen seiner Mitglieder bestimmte Aufgabengebiete (Referate) zur Bearbeitung zuteilen und sie insoweit mit der Überwachung der gemeindlichen Verwaltungstätigkeit betrauen (Art. 46 Abs. 1 Satz 2, Art. 30 Abs. 3 GO).
(5) [1]Gemeinderatsmitglieder, die eine Tätigkeit nach Absatz 3 oder 4 ausüben, haben ein Recht auf Akteneinsicht innerhalb ihres Aufgabenbereichs. [2]Zur Vorbereitung von Tagesordnungspunkten der nächsten Sitzung erhält jedes Gemeinderatsmitglied nach vorheriger Terminvereinbarung das Recht zur Einsicht in die entscheidungserheblichen Unterlagen, sofern Gründe der Geheimhaltungsverpflichtung nicht entgegenstehen.[3]Im Übrigen haben Gemeinderatsmitglieder ein Recht auf Akteneinsicht, wenn sie vom Gemeinderat durch Beschluss mit der Einsichtnahme beauftragt werden. [4]Das Verlangen zur Akteneinsicht ist gegenüber dem ersten Bürgermeister geltend zu machen.

In diesem Zusammenhang wandte sich im Berichtszeitraum eine bayerische Gemeinde an mich und schilderte mir folgenden Sachverhalt:

Der Gemeinderat habe ein **Gemeinderatsmitglied zum „Personalreferenten“** bestellt. Dieser „Personalreferent“ begehre nun allgemeine und umfassende Einsicht in sämtliche Personalakten aller Gemeindebediensteten, und zwar – so die Darstellung der Gemeindeverwaltung – „ohne konkreten Bezug zu irgendeiner Aufgabenstellung“. Eine solche allgemeine Personalakteneinsicht habe das gemeindliche Personalamt dem „Personalreferenten“ bisher verweigert. Zum einen könne der „Personalreferent“ höchstens über die Befugnisse des Gemeinderats verfügen, die in Personalangelegenheiten jedoch auf bestimmte Maßnahmen bei Bediensteten in höheren Besoldungs-/Entgeltgruppen beschränkt seien. Zum anderen sei Voraussetzung für eine Gewährung von Personalakteneinsicht, dass sich der „Personalreferent“ mit einer konkreten Fragestellung an das Personalamt wende, die nicht schon in allgemeiner, nicht-personenbezogener Form beantwortet werden könne.

Da der „Personalreferent“ des Gemeinderats allerdings an seiner Forderung festhielt, bat mich die Gemeinde um Rechtsauskunft.

Meine datenschutzrechtliche Prüfung des vorgelegten Sachverhalts hat ergeben, dass ein **anlassloses und voraussetzungsloses Personalakteneinsichtsrecht des Gemeinderats-„Referenten" nach der Rechtsordnung nicht besteht**. Vielmehr konnte ich die Rechtsauffassung des gemeindlichen Personalamts, die dem Personalaktengeheimnis und damit dem Grundrecht der Gemeindebediensteten auf informationelle Selbstbestimmung nach Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 Grundgesetz für die Bundesrepublik Deutschland (GG) wirkungsvoll Rechnung trägt, im Ergebnis bestätigen.

Im Einzelnen:

— Bei der begehrten Akteneinsicht handelt es sich um eine Weitergabe personenbezogener Daten im Sinne des Art. 4 Abs. 1 BayDSG durch das gemeindliche Personalamt an ein zum „Personalreferenten" bestelltes Gemeinderatsmitglied und damit um eine **Datenweitergabe von der Gemeindeverwaltung an den Gemeinderat**.

— Die Weitergabe personenbezogener Daten von der Gemeindeverwaltung an den Gemeinderat stellt eine **Datennutzung** gemäß Art. 4 Abs. 7 BayDSG dar. Diese Datennutzung ist ohne datenschutzgerechte Einwilligung der betroffenen Gemeindebediensteten nur zulässig, wenn hierfür eine **gesetzliche Grundlage** besteht (Art. 15 Abs. 1 BayDSG).

— Soweit es sich um **Personalaktendaten** im Sinne des § 50 Satz 2 Beamtenstatusgesetz (BeamtStG) handelt, beurteilt sich die Zulässigkeit der Weitergabe speziell nach § 50 Satz 4 BeamtStG in Verbindung mit Art. 102 ff. Bayerisches Beamtengesetz (BayBG).

  Diese beamtenrechtlichen Regelungen sind als allgemein gültige Schutzvorschriften für alle öffentlichen Bediensteten im Grundsatz auch auf die nicht-verbeamteten Beschäftigten des bayerischen öffentlichen Dienstes entsprechend anzuwenden.

§ 50 BeamtStG Personalakte
[1]Für jede Beamtin und jeden Beamten ist eine Personalakte zu führen. [2]Zur Personalakte gehören alle Unterlagen, die die Beamtin oder den Beamten betreffen, soweit sie mit dem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten). [3]Die Personalakte ist vertraulich zu behandeln. [4]Personalaktendaten dürfen nur für Zwecke der Personalverwaltung oder Personalwirtschaft verwendet werden, es sei denn, die Beamtin oder der Beamte willigt in die anderweitige Verwendung ein. [5]Für Ausnahmefälle kann landesrechtlich eine von Satz 4 abweichende Verwendung vorgesehen werden.

— Nach der **doppelten Zugangsbeschränkung** des Art. 103 BayBG darf Zugang zu Personalaktendaten nur haben, wer mit der Bearbeitung von Personalangelegenheiten beauftragt ist, und dies auch nur dann, soweit dies für Zwecke der Personalverwaltung oder der Personalwirtschaft erforderlich ist.

Art. 103 BayBG Zugang zur Personalakte
Zugang zur Personalakte dürfen nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt

sind, und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist; dies gilt auch für den Zugang im automatisierten Abrufverfahren.

– Die Befugnisse des **Gemeinderats** in Personalangelegenheiten sind im Wesentlichen in Art. 43 Abs. 1 GO aufgezählt. Die Zuständigkeit des Gemeinderats erstreckt sich danach nur auf die **wesentlichen statusrelevanten Maßnahmen** – wie etwa Ernennungen und Beförderungen, Einstellungen und Höhergruppierungen – **bei Gemeindebediensteten ab bestimmten Besoldungs-/Entgeltgruppen**. Darüber hinaus hat der Gemeinderat nach Art. 30 Abs. 3 GO die **allgemeine Aufgabe, die gesamte Gemeindeverwaltung zu überwachen**.

  Mehr als die ihm nach der Gemeindeordnung selbst zustehenden Befugnisse kann der Gemeinderat auf seinen „Personalreferenten" nicht übertragen.

Art. 43 GO Anstellung und Arbeitsbedingungen
(1) [1]Der Gemeinderat ist zuständig,
1. die Beamten der Gemeinde ab Besoldungsgruppe A 9 zu ernennen, zu befördern, abzuordnen oder zu versetzen, an eine Einrichtung zuzuweisen, in den Ruhestand zu versetzen und zu entlassen,
2. die Arbeitnehmer der Gemeinde ab Entgeltgruppe 9 des Tarifvertrags für den öffentlichen Dienst oder ab einem entsprechenden Entgelt einzustellen, höherzugruppieren, abzuordnen oder zu versetzen, einem Dritten zuzuweisen, mittels Personalgestellung zu beschäftigen und zu entlassen.
[2]Befugnisse nach Satz 1 kann der Gemeinderat einem beschließenden Ausschuss (Art. 32 Abs. 2 bis 5) übertragen. [3]In kreisfreien Gemeinden kann der Gemeinderat die Befugnisse nach Satz 1 für Beamte bis zur Besoldungsgruppe A 14 und für Arbeitnehmer bis zur Entgeltgruppe 14 des Tarifvertrags für den öffentlichen Dienst oder mit einem entsprechenden Entgelt dem Oberbürgermeister übertragen; Art. 39 Abs. 2 findet Anwendung. [4]Ein solcher Beschluss bedarf der Mehrheit der stimmberechtigten Mitglieder des Gemeinderats; falls der Beschluss nicht mit dieser Mehrheit wieder aufgehoben wird, gilt er bis zum Ende der Wahlzeit des Gemeinderats.
(2) [1]Für Beamte der Gemeinde bis zur Besoldungsgruppe A 8 und für Arbeitnehmer der Gemeinde bis zur Entgeltgruppe 8 des Tarifvertrags für den öffentlichen Dienst oder bis zu einem entsprechenden Entgelt obliegen die in Abs. 1 genannten personalrechtlichen Befugnisse dem ersten Bürgermeister. [2]Art. 39 Abs. 2 findet Anwendung.
(3) Dienstvorgesetzter der Gemeindebeamten ist der erste Bürgermeister.
(4) Die Arbeitsbedingungen und das Entgelt der Arbeitnehmer müssen angemessen sein.

– Die personalrechtlichen Befugnisse für die Gemeindebediensteten der übrigen Besoldungs-/Entgeltgruppen obliegen dagegen dem **ersten Bürgermeister** (Art. 43 Abs. 2 GO).

  Dieser führt nach Art. 37 Abs. 4 GO überdies die **Dienstaufsicht** über die Beamten und Arbeitnehmer der Gemeinde. Die Dienstaufsicht des ersten Bürgermeisters umfasst unter anderem das Recht, den Dienstbetrieb und den Geschäftsablauf zu überwachen. Der erste Bürgermeister ist zudem nach Art. 43 Abs. 3 GO **Dienstvorgesetzter** der Gemeindebeamten.

Unter den Voraussetzungen des Art. 39 Abs. 2 GO kann der erste Bürgermeister allerdings einzelne seiner Befugnisse im Rahmen der Geschäftsverteilung den weiteren Bürgermeistern, aber auch einem Gemeinderatsmitglied oder einem Gemeindebediensteten übertragen.

Vor dem Hintergrund dieser klaren gesetzlichen Aufgaben- und Zuständigkeitsverteilung zwischen Gemeinderat einerseits und Gemeindeverwaltung andererseits vermag ich nicht zu erkennen, inwiefern ein **allgemeines und voraussetzungsloses Einsichtsrecht eines vom Gemeinderat bestellten „Personalreferenten" in die Personalakten der Gemeindebediensteten** im Hinblick auf die personalrechtlichen Kompetenzen des Gemeinderats nach Art. 43 Abs. 1 und Art. 30 Abs. 3 GO erforderlich sein könnte. Für eine regelmäßige und pauschale, ohne konkreten Anlass erfolgende Einsichtnahme des „Personalreferenten" des Gemeinderats in Personalakten der Gemeindebediensteten sehe ich daher **keine Rechtfertigung**.

Ein Zugangsrecht zu Personalakten kann einem Gemeinderats-„Referenten" somit **nur unter den engen Voraussetzungen des Art. 103 BayBG in Verbindung mit Art. 43 Abs. 1 GO, Art. 30 Abs. 3 GO und Art. 46 Abs. 1 Satz 2 GO im konkreten Einzelfall** zustehen. Hier kommt es allerdings stets entscheidend darauf an, dass die Weitergabe von Personaldaten durch die Gemeindeverwaltung **zur Erfüllung der konkreten Aufgabenstellung des Gemeinderats erforderlich** ist. Dies ist jedoch schon dann nicht der Fall, wenn die vom „Personalreferenten" aufgeworfene Fragestellung von der Gemeindeverwaltung bereits in allgemeiner, nicht-personenbezogener Form beantwortet werden kann. Jedenfalls hat das gemeindliche Personalamt die Erforderlichkeit jeder Weitergabe von Personaldaten an den Gemeinderat mit Blick auf das verfassungsrechtlich in Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 GG gewährleistete informationelle Selbstbestimmungsrecht der Gemeindebediensteten sorgfältig zu prüfen.

Zu der übergreifenden Problematik der Nutzung von Personaldaten durch den Gemeinderat möchte ich abschließend noch auf meinen ausführlichen Beitrag in meinem 21. Tätigkeitsbericht 2004 unter Nr. 16.2 aufmerksam machen.

11.9 Dienstliche Beurteilung von behördlichen Datenschutzbeauftragten

Ausweislich der Bestimmungen der Art. 54 ff. Gesetz über die Leistungslaufbahn und die Fachlaufbahnen der bayerischen Beamten und Beamtinnen (Leistungslaufbahngesetz – LlbG) **sind die bayerischen Beamtinnen und Beamten in bestimmten Fällen und Zeitabständen dienstlich zu beurteilen**. Insbesondere sind nach Art. 56 Abs. 1 LlbG fachliche Leistung, Eignung und Befähigung der bayerischen Beamtinnen und Beamten im Grundsatz mindestens alle drei Jahre dienstlich zu beurteilen (periodische Beurteilung).

Art. 56 LlbG Periodische Beurteilung
(1) [1]Fachliche Leistung, Eignung und Befähigung sind mindestens alle drei Jahre dienstlich zu beurteilen (periodische Beurteilung). [2]Dies gilt nicht für Beamte und Beamtinnen auf Widerruf im Vorbereitungsdienst und während der Probezeit nach § 4 Abs. 3 Buchst. a BeamtStG. [3]Satz 1 gilt auch für Beamte und Beamtinnen, die nach Art. 15 Abs. 4 Satz 1 Nr. 3 zur Ausübung einer Tätigkeit bei Fraktionen, kommunalen Vertretungskörperschaften oder kommunalen Spitzenverbänden beurlaubt wurden.

Inhaltlich ist der periodischen Beurteilung zunächst gemäß Art. 58 Abs. 1 LlbG eine **Beschreibung der Aufgaben**, die im Beurteilungszeitraum wahrgenommen wurden, voranzustellen. Sodann hat die Beurteilung nach Art. 58 Abs. 2 Satz 1 LlbG die **fachliche Leistung** in Bezug auf die Funktion und im Vergleich zu den anderen Beamten und Beamtinnen derselben Besoldungsgruppe der Fachlaufbahn und, soweit gebildet, desselben fachlichen Schwerpunkts **objektiv darzustellen** und außerdem von **Eignung und Befähigung** ein **zutreffendes Bild** zu geben.

Die dienstliche Beurteilung kann unter anderem nach Art. 16 Abs. 1 Satz 3 LlbG **Grundlage für die** Entscheidung des Dienstherrn über die **Übertragung höherwertiger Dienstposten** sowie gemäß Art. 17 Abs. 7 LlbG in Verbindung mit Art. 16 Abs. 1 Satz 3 LlbG Grundlage für die Entscheidung des Dienstherrn über **Beförderungen** sein. Sie ist nach § 50 Satz 2 Beamtenstatusgesetz in die **Personalakte** aufzunehmen.

Bei der Tätigkeit als Mitglied des Personalrats oder der Schwerbehindertenvertretung handelt es sich allerdings nicht um eine dienstliche, sondern um eine außerdienstliche ehrenamtliche – und damit vom Dienstherrn nicht zu beurteilende – Tätigkeit. Nur auf Antrag wird die Tätigkeit als Gleichstellungsbeauftragte(r) gemäß Art. 16 Abs. 3 Satz 2 Bayerisches Gleichstellungsgesetz (BayGlG) in die Beurteilung einbezogen. Dagegen ist die **Tätigkeit als behördliche(r) Datenschutzbeauftragte(r)** im Sinne des Art. 25 Abs. 3 BayDSG – unabhängig von einem Antrag – **als dienstliche Tätigkeit einzuordnen und somit in die** nach Art. 58 Abs. 1 LlbG der Beurteilung voranzustellende **Aufgabenbeschreibung aufzunehmen**.

Allerdings stellt sich die Frage, welche **Auswirkungen** die gesetzlich in Art. 25 Abs. 3 Satz 2 BayDSG garantierte **Unabhängigkeit des oder der behördlichen Datenschutzbeauftragten** sowie das in Art. 25 Abs. 3 Satz 4 BayDSG ausdrücklich angeordnete **Benachteiligungsverbot** auf den wertenden Inhalt der Beurteilung im Sinne des Art. 58 Abs. 2 LlbG haben.

Art. 25 BayDSG Sicherstellung des Datenschutzes, behördliche Datenschutzbeauftragte
(3) [1]Die behördlichen Datenschutzbeauftragten sind in dieser Eigenschaft der Leitung der öffentlichen Stelle oder deren ständigen Vertretung unmittelbar zu unterstellen; bei obersten Dienstbehörden können sie auch dem Ministerialdirektor (Amtschef), in Gemeinden einem berufsmäßigen Gemeinderatsmitglied unterstellt werden. [2]Sie sind in ihrer Eigenschaft als behördliche Datenschutzbeauftragte weisungsfrei. [3]Sie können sich in Zweifelsfällen unmittelbar an den Landesbeauftragten für den Datenschutz wenden. [4]Sie dürfen wegen der Erfüllung ihrer Aufgaben nicht benachteiligt werden. [5]Sie sind im erforderlichen Umfang von der Erfüllung sonstiger dienstlicher Aufgaben freizustellen. [6]Die Beschäftigten öffentlicher Stellen können sich in Angelegenheiten des Datenschutzes an ihre behördlichen Datenschutzbeauftragten wenden.

Allgemeine Richtlinien für die dienstliche Beurteilung der Beamtinnen und Beamten des **Freistaates Bayern** enthält Abschnitt 3 der Verwaltungsvorschriften zum Beamtenrecht (VV-BeamtR). Das für das öffentliche Dienstrecht innerhalb der Staatsregierung federführend zuständige Staatsministerium der Finanzen, für Landesentwicklung und Heimat hat dabei in **Abschnitt 3 Nr. 4 VV-BeamtR Benachteiligungsverbot** unter anderem festgelegt, dass sich Teilzeitbeschäftigung oder Beurlaubung ebenso wie die Tätigkeit als Mitglied des Personalrats oder der

Schwerbehindertenvertretung sowie die Tätigkeit als Gleichstellungsbeauftragte oder Gleichstellungsbeauftragter beziehungsweise Ansprechpartnerin oder Ansprechpartner im Sinne des Art. 15 Abs. 1 und 2 BayGlG nicht nachteilig auf die Beurteilung auswirken dürfen.

Abschnitt 3 Nr. 4 VV-BeamtR Benachteiligungsverbot
[1]Teilzeitbeschäftigung oder Beurlaubung dürfen sich nicht nachteilig auf die Beurteilung auswirken (Art. 14 Abs. 1 Satz 2, Abs. 2 des Bayerischen Gesetzes zur Gleichstellung von Frauen und Männern, Bayerisches Gleichstellungsgesetz – BayGlG – vom 24. Mai 1996, GVBl S. 186, BayRS 2039-1-A, zuletzt geändert durch Gesetz vom 23. Mai 2006, GVBl S. 292). [2]Dies gilt auch für die Tätigkeit als Mitglied des Personalrats oder der Schwerbehindertenvertretung sowie als Gleichstellungsbeauftragte oder Gleichstellungsbeauftragter bzw. Ansprechpartnerin oder Ansprechpartner (im Sinn des Art. 15 Abs. 1 und 2 BayGlG). [3]Insbesondere ist bei einer Teilzeitbeschäftigung oder teilweisen Freistellung die geleistete Arbeitsmenge im Verhältnis zur anteiligen Arbeitszeit zu bewerten.

Die Tätigkeit des oder der behördlichen Datenschutzbeauftragten ist in dieser Bestimmung zwar nicht ausdrücklich erwähnt. Aufgrund des Charakters dieser Regelung als **Schutzvorschrift** meine ich allerdings, dass das in Abschnitt 3 Nr. 4 VV-BeamtR speziell für dienstliche Beurteilungen angeordnete Benachteiligungsverbot – mit Blick auf die gesetzlich in Art. 25 Abs. 3 Satz 2 BayDSG garantierte Unabhängigkeit und das gesetzlich in Art. 25 Abs. 3 Satz 4 BayDSG gewährleistete Benachteiligungsverbot – **auch auf behördliche Datenschutzbeauftragte anzuwenden** ist.

Eine ordnungsgemäße, für die Behördenleitung aber möglicherweise unbequeme Aufgabenwahrnehmung des oder der **behördlichen Datenschutzbeauftragten** – die sich durchaus auch einmal in deutlicher sachlicher Kritik oder anhaltendem fachlichen Widerstand äußern kann – darf somit **in keinem Fall** Grund sein oder auch nur Anlass geben, behördliche Datenschutzbeauftragte in der dienstlichen Beurteilung **schlechter zu stellen** als Bedienstete, die bei gleicher fachlicher Leistung, Eignung und Befähigung diese – unabhängige und weisungsfreie – Funktion nicht wahrnehmen.

In Abschnitt 18 VV-BeamtR wird den **Gemeinden** und den sonstigen der Aufsicht des Freistaates Bayern unterstehenden **Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts** empfohlen, entsprechend dieser Bekanntmachung zu verfahren. Auch bei Beamtinnen und Beamten dieser Dienstherren ist daher **im Rahmen der dienstlichen Beurteilung eine Benachteiligung aufgrund der Tätigkeit als behördliche Datenschutzbeauftragte** in entsprechender Anwendung des Abschnitts 3 Nr. 4 VV-BeamtR **auszuschließen**.

11.10 Zugriff des Personalrats auf elektronische Zeiterfassungsdaten

In meiner täglichen Kontroll- und Beratungspraxis muss ich immer wieder feststellen, dass in den bayerischen öffentlichen – insbesondere staatlichen und kommunalen – Stellen bei der Beantwortung der Frage, ob überhaupt und, wenn ja, in welchem Umfang und in welcher Form der **Personalrat Zugriff auf die elektronischen Zeiterfassungsdaten der Bediensteten** haben darf, Unsicherheiten und Unklarheiten bestehen.

Bereits in der Vergangenheit **habe ich entsprechende pauschale Informationsbegehren des Personalrats** mit Blick auf das verfassungsrechtlich in Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 Grundgesetz für die Bundesrepublik Deutschland (GG) gewährleistete Grundrecht der Bediensteten auf informationelle Selbstbestimmung **kritisch gesehen**. Insbesondere verweise ich hierzu auf meine Ausführungen zum Datenschutz bei Zeiterfassungsdaten in meinem 22. Tätigkeitsbericht 2006 unter Nr. 19.3, in dem ich mich im Abschnitt „Einsichtnahme durch den Personalrat" schon mit der aufgeworfenen Fragestellung auseinandergesetzt habe. An diesen Ausführungen halte ich weiterhin fest. Erfreulicherweise hat das **Bundesverwaltungsgericht** meine seit jeher kritische Haltung nunmehr in seiner Entscheidung vom 19. März 2014 (6 P 1.13) **bestätigt**.

Im Einzelnen nehme ich zur Problematik des Zugriffs der Personalvertretung auf die elektronischen Zeiterfassungsdaten der Beschäftigten wie folgt Stellung:

11.10.1 Informationsanspruch des Personalrats allgemein

— Zunächst ist festzuhalten, dass der Personalrat im Verhältnis zur Dienststelle – datenschutzrechtlich gesehen – nicht die Position eines Dritten im Sinne des Art. 4 Abs. 10 Satz 1 BayDSG einnimmt. Vielmehr ist der **Personalrat** als **unselbstständiger Teil der Dienststelle** – datenschutzrechtlich also der „speichernden Stelle" (vgl. Art. 4 Abs. 9 BayDSG) – zu betrachten.

— Bei einer **Weitergabe personenbezogener (Personal-)Daten** (siehe Art. 4 Abs. 1 BayDSG) von der Dienststelle an den Personalrat – wie sie etwa bei einem Zugriff des Personalrats auf die elektronischen Zeiterfassungsdaten der Bediensteten vorliegt – handelt es sich daher um eine **Datennutzung** im Sinne des Art. 4 Abs. 7 BayDSG.

— Ohne Einwilligung der betroffenen Bediensteten ist eine solche Nutzung nur zulässig, wenn hierfür eine **gesetzliche Rechtsgrundlage** besteht (Art. 15 Abs. 1 BayDSG). Als spezialgesetzliche, die allgemeinen Erlaubnistatbestände des Bayerischen Datenschutzgesetzes gemäß Art. 2 Abs. 7 BayDSG verdrängende Rechtsgrundlage kommt im vorliegenden Zusammenhang allein die Vorschrift des **Art. 69 Abs. 2 Sätze 1 und 2 Bayerisches Personalvertretungsgesetz (BayPVG)** in Betracht.

Art. 69 BayPVG
(1) Der Personalrat hat folgende allgemeine Aufgaben:
a) Maßnahmen, die der Dienststelle und ihren Angehörigen dienen, zu beantragen,
b) dafür zu sorgen, daß die zugunsten der Beschäftigten geltenden Gesetze, Verordnungen, Tarifverträge, Dienstvereinbarungen und Verwaltungsanordnungen durchgeführt werden,
c) Anregungen und Beschwerden von Beschäftigten entgegenzunehmen und, falls sie berechtigt erscheinen, durch Verhandlung mit dem Leiter der Dienststelle auf ihre Erledigung hinzuwirken,
d) die Eingliederung Schwerbehinderter und sonstiger schutzbedürftiger, insbesondere älterer Personen in die Dienststelle zu fördern und für eine ihren Fähigkeiten und Kenntnissen entsprechende Beschäftigung zu sorgen; die Schwerbehindertenvertretung ist vor einer Entscheidung zu hören,
e) Maßnahmen zur beruflichen Förderung Schwerbehinderter zu beantragen; die Schwerbehindertenvertretung ist vor einer Entscheidung zu hören,

f) die Eingliederung ausländischer Beschäftigter in die Dienststelle und das Verständnis zwischen ihnen und den deutschen Beschäftigten zu fördern,
g) mit der Jugend- und Auszubildendenvertretung zur Förderung der Belange der Beschäftigten im Sinn von Art. 58 Abs. 1 eng zusammenzuarbeiten,
h) bei Einstellung, Beschäftigung, Aus-, Fort- und Weiterbildung und beim beruflichen Fortkommen auf die Gleichbehandlung von Frauen und Männern zu achten und entsprechende Maßnahmen zu beantragen.

(2) [1]Der Personalrat ist zur Durchführung seiner Aufgaben rechtzeitig und umfassend zu unterrichten. [2]Ihm sind die hierfür erforderlichen Unterlagen zur Verfügung zu stellen. [3]Bei einer Einstellung, Beförderung und Übertragung der Dienstaufgaben eines anderen Amtes mit höherem Endgrundgehalt oder höherer Amtszulage für eine Dauer von mehr als sechs Monaten kann der Personalrat auch die zur Erfüllung seiner Aufgaben erforderliche Vorlage von Bewerbungsunterlagen verlangen. [4]Von dienstlichen Beurteilungen ist nur die abschließende Bewertung bekanntzugeben. [5]Sofern für eine Auswahlentscheidung eine Binnendifferenzierung nach Art. 16 Abs. 2, Art. 17 Abs. 7 LlbG vorzunehmen ist, sind auch die Bewertungen der wesentlichen Beurteilungskriterien mitzuteilen. [6]Personalakten dürfen nur mit schriftlicher Zustimmung des Beschäftigten und nur von einem von ihm bestimmten Mitglied des Personalrats eingesehen werden.

— Nach Art. 69 Abs. 2 Satz 1 BayPVG ist der **Personalrat zur Durchführung seiner Aufgaben rechtzeitig und umfassend zu unterrichten**. Ihm sind gemäß Art. 69 Abs. 2 Satz 2 BayPVG **die hierfür erforderlichen Unterlagen zur Verfügung zu stellen**.

Ein Anspruch der Personalvertretung auf umfassende und rechtzeitige Information besteht damit nur insoweit, als sie Auskünfte und Unterlagen von der Dienststelle benötigt, um die ihr obliegenden Aufgaben wirkungsvoll erfüllen und ihre Beteiligungsrechte rechtzeitig und uneingeschränkt wahrnehmen zu können.

Bei Inanspruchnahme ihres Informationsrechts hat die Personalvertretung daher der Dienststelle darzulegen, aus welchem bestimmten Anlass sie die Vorlage welcher Auskünfte und Unterlagen verlangt und aus welchen Gründen sie diese Informationen zur Erfüllung ihrer Aufgaben für erforderlich hält (zu den Informations- und Einsichtsrechten der Personalvertretung siehe mein 20. Tätigkeitsbericht 2002 unter Nr. 13.4). **Die Personalvertretung ist jedoch kein Kontrollorgan der Verwaltung**, das die Aufgabenerfüllung und den inneren Betrieb der Dienststelle allgemein zu überwachen hat.

Der **Informationsanspruch des Personalrats** gemäß Art. 69 Abs. 2 Satz 1 BayPVG ist somit ebenso wie der darauf bezogene Vorlageanspruch nach Art. 69 Abs. 2 Satz 2 BayPVG **aufgabengebunden und** in seiner Reichweite **durch das Erforderlichkeitsprinzip begrenzt**.

11.10.2 Informationsanspruch des Personalrats hinsichtlich elektronischer Zeiterfassungsdaten

— In der vorliegenden Fallkonstellation bezieht sich die **Überwachungsaufgabe der Personalvertretung** – insbesondere bei einem bestimmten Anlass – auf die **Einhaltung der arbeitszeitrechtlichen Bestimmungen bei der elektronischen Zeiterfassung**.

So hat der Personalrat nach Art. 69 Abs. 1 Buchst. b) BayPVG dafür zu sorgen, dass die zugunsten der Beschäftigten geltenden Gesetze, Verordnungen, Tarifverträge, Dienstvereinbarungen und Verwaltungsanordnungen durchgeführt werden. Arbeitszeitrechtliche Bestimmungen sind stets – zumindest auch – normative Regelungen zugunsten der Beschäftigten, die der Sicherheit und dem Gesundheitsschutz dienen.

Zu den für die bayerischen öffentlichen – insbesondere staatlichen und kommunalen – Stellen bedeutsamen arbeitszeitrechtlichen Bestimmungen zählen etwa die gesetzlichen Regelungen der Art. 87 ff. BayBG und des Arbeitszeitgesetzes (ArbZG), die Verordnung über die Arbeitszeit für den bayerischen öffentlichen Dienst (AzV), der Abschnitt 11 der Verwaltungsvorschriften zum Beamtenrecht (VV-BeamtR) sowie die tarifrechtlichen Regelungen der §§ 6 ff. Tarifvertrag für den öffentlichen Dienst (TVöD) beziehungsweise der §§ 6 ff Tarifvertrag für den öffentlichen Dienst der Länder (TV-L). Da bei der Einführung, Anwendung und erheblichen Änderung elektronischer Zeiterfassungssysteme der Personalrat nach Art. 75a Abs. 1 Nr. 1 in Verbindung mit Art. 70 BayPVG mitzubestimmen hat, kommt in der Praxis zudem **Dienstvereinbarungen zur elektronischen Zeiterfassung** (siehe Art. 73 BayPVG) eine erhebliche Bedeutung zu.

– Kann sich der Personalrat hiernach auf eine konkrete Überwachungsaufgabe berufen, bestimmen sich die **Art und der Umfang seines Zugriffsrechts auf elektronische Zeiterfassungsdaten nach dem Maßstab der Erforderlichkeit**.

– Um den Personalrat in die Lage zu versetzen, im Hinblick auf die Einhaltung der arbeitszeitrechtlichen Bestimmungen bei der elektronischen Zeiterfassung etwaige Rechtsverstöße erkennen zu können, ist es nach Art. 69 Abs. 2 Sätze 1 und 2 BayPVG allerdings nicht erforderlich, dem Personalrat ein **generelles und ständiges (lesendes) Zugriffsrecht auf die (elektronischen) Zeiterfassungsdaten aller Bediensteten** einzuräumen.

  Ein solches pauschales Auskunftsverlangen ist **vom Informationsrecht des Personalrats nicht gedeckt**. Es trägt überdies dem verfassungsrechtlich in Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 GG gewährleisteten informationellen Selbstbestimmungsrecht der Bediensteten nicht ausreichend Rechnung.

– Vielmehr ist es in diesen Fällen nach Art. 69 Abs. 2 Sätze 1 und 2 BayPVG **auf einer ersten Stufe ausreichend, dem Personalrat anonymisierte Zeiterfassungsdaten zukommen zu lassen**.

  Denn bereits anonymisierten Arbeitszeitlisten lässt sich entnehmen, ob die arbeitszeitrechtlichen Regelungen – insbesondere über die Einhaltung der Tageshöchstarbeitszeit, der Ruhepausen, der Ruhezeiten und der Wochenarbeitszeit – eingehalten wurden.

– Nur soweit die Überprüfung der Arbeitszeitlisten Unstimmigkeiten zu erkennen gibt, hat der Personalrat **auf einer zweiten Stufe Anspruch auf nähere Erläuterungen**, die – wenn im konkreten Fall anders eine Klärung nicht möglich ist – auch zur Aufdeckung der Identität des betroffenen Bediensteten führen können.

Die **Erforderlichkeit jeder Weitergabe von Personaldaten** an den Personalrat hat die Dienststelle mit Blick auf das verfassungsrechtlich in Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 GG gewährleistete informationelle Selbstbestimmungsrecht der Bediensteten **allerdings stets sorgfältig zu prüfen**.

Soweit die Erfüllung der Aufgaben des Personalrats nur durch eine **Unterrichtung in personenbezogener Form** möglich ist, bestimmt sich auch die **Form der Auskunftserteilung nach dem Maßstab der Erforderlichkeit**.

Daran gemessen hat die Information des Personalrats durch die Dienststelle gemäß Art. 69 Abs. 2 Satz 1 BayPVG – abhängig von Umfang und Komplexität der gewünschten Informationen – mündlich oder schriftlich zu erfolgen. Die Pflicht der Dienststelle zur Vorlage von Unterlagen nach Art. 69 Abs. 2 Satz 2 BayPVG reicht dementsprechend von der bloßen Einsichtsgewährung bis zur zeitweisen oder auch dauerhaften Überlassung. Nach dem Erforderlichkeitsprinzip bestimmt sich ferner, ob Auskünfte nur einmalig, in größeren Abständen oder gar fortlaufend zu erteilen sind.

– Im Ergebnis führt dieses **zweistufige Verfahren** zu einem interessengerechten **Ausgleich zwischen der Überwachungsaufgabe des Personalrats einerseits und dem Grundrecht der Beschäftigten auf informationelle Selbstbestimmung andererseits**. Damit trägt es auch dem gesetzlich in Art. 69 Abs. 2 Sätze 1 und 2 BayPVG vorgegebenen Erforderlichkeitsgrundsatz wirkungsvoll Rechnung.

Erfreulicherweise hat das **Bundesverwaltungsgericht** meine Auffassung in seinem **Beschluss vom 19. März 2014** (6 P 1.13) **zur Reichweite des Auskunftsanspruchs der Personalvertretung in Bezug auf elektronische Zeiterfassungsdaten bestätigt**. Der amtliche Leitsatz dieser Entscheidung lautet wörtlich:

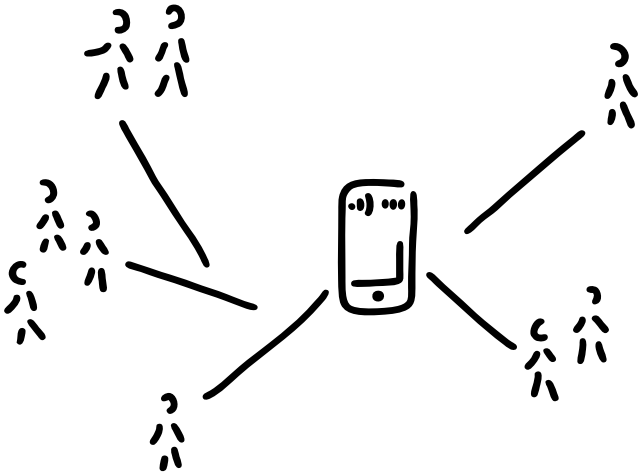
„Der Personalrat kann nicht verlangen, dass ihm die in der elektronischen Arbeitszeiterfassung gespeicherten Daten unter Namensnennung der Beschäftigten zur Verfügung gestellt werden; seine Überwachungsaufgabe kann er bereits effektiv wahrnehmen, wenn er zunächst nur die anonymisierten Arbeitszeitlisten der Dienststelle erhält."

Schließlich hat das Bundesverwaltungsgericht seine Entscheidung mit folgenden Worten abgeschlossen:

„Die unmittelbar grundrechtsgebundene Dienststelle darf dem Personalrat keine Auskünfte erteilen, wenn damit zugleich das Persönlichkeitsrecht der Beschäftigten verletzt wird."

Auch dieser – allgemein das datenschutzrechtliche Verhältnis zwischen Dienststelle und Personalrat kennzeichnenden – Aussage des Bundesverwaltungsgerichts ist aus meiner Sicht uneingeschränkt zuzustimmen.

12 E-Government, Telemedienrecht, Soziale Medien



12.1 E-Government-Regelungen

Angesichts der fortschreitenden Digitalisierung unseres Alltags steht E-Government seit geraumer Zeit auf der politischen Agenda. Die bisherigen Vorschriften habe ich im 26. Tätigkeitsbericht 2014 unter Nr. 12.1 beleuchtet, insbesondere das im letzten Berichtszeitraum auf Bundesebene erlassene **Gesetz zur Förderung der elektronischen Verwaltung** (**E-Government-Gesetz – EGovG**). Nach Maßgabe von § 1 Abs. 2 EGovG waren Vorschriften dieses Gesetzes auch von bayerischen öffentlichen Stellen anzuwenden. Für die bayerische Verwaltung spielt das E-Government-Gesetz des Bundes jedoch seit dem 30. Dezember 2015 nur noch in eng begrenzten Bereichen eine Rolle.

Denn am 30. Dezember 2015 ist das **Gesetz über die elektronische Verwaltung in Bayern (Bayerisches E-Government-Gesetz – BayEGovG)** in wesentlichen Teilen in Kraft getreten und seither grundsätzlich für bayerische öffentliche Stellen maßgeblich. Das E-Government-Gesetz des Bundes ist hingegen gemäß Art. 1 Abs. 3 BayEGovG von bayerischen öffentlichen Stellen nur noch beim Vollzug von Bundesrecht im Auftrag des Bundes anzuwenden (siehe die Beispiele in der Begründung des Gesetzentwurfs, Landtags-Drucksache 17/7537 vom 14. Juli 2015, Seite 27). Im Bereich der Bundesauftragsverwaltung hat der Freistaat Bayern keine Regelungskompetenz.

Das Bayerische E-Government-Gesetz und der Ausbau des E-Government sollen die Leistungsfähigkeit und Effizienz der Verwaltung erhöhen und wesentlich zu Verwaltungsmodernisierung und Bürokratieabbau beitragen. Für Bürgerinnen,

Bürger und Unternehmen kann durch digitale Verwaltungsangebote und elektronische Kommunikation der Zugriff auf öffentliche Dienste und Verfahren erleichtert werden.

Ich bin in den Entstehungsprozess des Bayerischen E-Government-Gesetzes frühzeitig eingebunden worden. Meine datenschutzrechtlichen Positionen sind an mehreren Stellen in den Gesetzestext eingeflossen. Darüber hinaus haben sich einige Klarstellungen, die auf mein Drängen zumindest in die Gesetzesbegründung aufgenommen wurden, bereits als wertvoll erwiesen. Beispielsweise wollten einzelne Behörden aus der Regelung, dass Behörden jeweils ein geeignetes **Verschlüsselungsverfahren** bereit zu stellen haben (Art. 3 Abs. 1 Satz 3 BayEGovG), einen – unrichtigen – Gegenschluss ziehen: Da diese Regelung erst zum 1. Januar 2020 in Kraft tritt, müssten also – so diese Behörden – vor 2020 gerade keine Verschlüsselungsverfahren verwendet werden. In Erwartung solcher Argumente habe ich mich erfolgreich für die Aussage in der Gesetzesbegründung eingesetzt, dass bereits geltende Verschlüsselungsverpflichtungen, etwa nach Maßgabe von Art. 7 BayDSG, unberührt bleiben (und damit fortbestehen). Mittels unter anderem dieser Formulierung in der Gesetzesbegründung konnten Rechtsunsicherheiten und langwierige Auseinandersetzungen mit Behörden vermieden werden. Die Regelung des Art. 3 Abs. 1 Satz 3 BayEGovG ist grundsätzlich zu begrüßen, auch wenn sie leider erst 2020 in Kraft tritt. Denn sie entfaltet mit der ausdrücklichen Normierung einer Verschlüsselungsverpflichtung Signalwirkung, beseitigt Rechtsunsicherheiten und geht in ihrem Anwendungsbereich über bisherige Verschlüsselungspflichten hinaus.

Leider wurden aber meine Forderungen teilweise nicht umgesetzt. So wurden die Grundsätze der Datenvermeidung und Datensparsamkeit (siehe 26. Tätigkeitsbericht 2014 unter Nr. 12.1 am Ende) nicht ausdrücklich im Gesetz verankert. Dies hat nunmehr allerdings der europäische Gesetzgeber mit Wirkung zum 25. Mai 2018 in Art. 5 Abs. 1 Buchst. c) Datenschutz-Grundverordnung getan („**Datenminimierung**“).

Ein weiterer Kritikpunkt betraf teils zu allgemeine Formulierungen im Bayerischen E-Government-Gesetz. Insbesondere Zuständigkeiten und Aufgaben im Zusammenhang mit einem Service- oder Bürgerkonto beziehungsweise mit zentralen Diensten hätten konkreter geregelt werden müssen. Über die Registrierung bei einem zentralen Servicekonto kann etwa Bürgerinnen und Bürgern die Möglichkeit eröffnet werden, die dortige Anmeldung zur Identifizierung gegenüber anderen Behörden zu nutzen, beispielsweise bei der Inanspruchnahme öffentlicher Dienstleistungen. Solche zentralen Servicekonten sind über Webseiten wie das BayernPortal (siehe Nr. 12.2) zugänglich.

Die Staatsregierung hat meine Kritik inzwischen insoweit aufgegriffen, als sie die Verordnungsermächtigung nach Art. 9 Abs. 4 BayEGovG zu Konkretisierungen genutzt hat. In § 3 der **Bayerischen Verordnung zur Schaffung barrierefreier Informationstechnik (BayBITV)** findet sich nunmehr eine konkretere Regelung zur Identitätsfeststellung durch das Staatsministerium der Finanzen, für Landesentwicklung und Heimat bei der Bereitstellung zentraler Dienste wie einem Servicekonto. Die Daten, die hier unter strenger Zweckbindung erhoben werden dürfen, sind nunmehr konkret aufgezählt.

Auch meine Kolleginnen und Kollegen in Bund und Ländern sehen die Notwendigkeit einer klaren Rechtsgrundlage für behördenübergreifende Servicekonten:

Entschließung der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 06./07. April 2016 in Schwerin

Datenschutz bei Servicekonten

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

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

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

- *Auch künftig muss es möglich sein, ohne Servicekonto Verwaltungsdienstleistungen in Anspruch zu nehmen.*

- *Die einmalige Inanspruchnahme von Verwaltungsdienstleistungen muss auch ohne dauerhafte Speicherung identifizierender Daten möglich sein. Für diese Zwecke sollten temporäre Servicekonten eingerichtet werden.*

- *Bürgerinnen und Bürgern muss die Möglichkeit eingeräumt werden, sowohl einzelne im permanenten Servicekonto dauerhaft gespeicherte, personenbezogenen Daten als auch das Konto selbst löschen zu lassen.*

- *Soweit Daten aus dem Servicekonto übermittelt werden, müssen diese Übermittlungen durch die Bürger im Servicekonto selbst nachvollzogen werden können.*

- *Für die Erhebung personenbezogener Daten in behördenübergreifenden Servicekonten ist eine Rechtsgrundlage erforderlich, da sie als Aufgabe verwaltungsorganisationsrechtlich einer Stelle zugewiesen werden muss. Der Staat darf personenbezogene Daten zur Erfüllung seiner gesetzlichen Aufgaben grundsätzlich nur auf der Basis einer klaren Rechtsgrundlage verarbeiten. Da zudem die Bedeutung dieser Servicekonten zunehmen wird und*

absehbar ist, dass den Betroffenen durch die Nutzung dieser Konten erhebliche Vorteile im Sinne von "Digital by Default" eingeräumt werden sollen, reicht die Einwilligung als Rechtsgrundlage für die Datenerhebung nicht aus.

— *Vorbehaltlich weiterer verfassungsrechtlicher Prüfungen ist für die Länder übergreifende Nutzung von Servicekonten eine Rechtsgrundlage erforderlich. Durch die dauerhafte Speicherung identifizierender Daten werden bundesweit nutzbare Servicekonten zu einer digitalen Meldestelle bzw. zu einer zweiten, zentralen Identifizierungsstelle neben den Meldebehörden aufgewertet. Die Rechtsgrundlage muss eindeutige Vorgaben zum Datenumfang, zu Zweckbindungsregelungen, zur Löschung und zur Transparenz der Datenverarbeitung enthalten. Daten der Betroffenen sind alleine zum Betrieb des Serviceportals und zur Erledigung der Verfahren der Nutzer zu verarbeiten. Eine Nutzung dritter Stellen zu anderen Zwecken ist gesetzlich ausdrücklich auszuschließen.*

— *Bevor Unternehmen verpflichtet werden sollen, die eID-Funktion für Verwaltungsangelegenheiten zu nutzen, ist zu prüfen, ob und unter welchen Voraussetzungen der Einsatz privater digitaler Identifikationsnachweise zu nichtprivaten Zwecken bzw. zur Erfüllung arbeitsvertraglicher Pflichten zulässig ist und inwieweit Arbeitnehmerinnen und Arbeitnehmer hierzu verpflichtet werden können.*

— *Angesichts des Abhängigkeitsverhältnisses der Arbeitnehmerinnen und Arbeitnehmer im Beschäftigungsverhältnis kann die Nutzung von Servicekonten auf der Basis der privaten eID-Funktion keinesfalls auf der Einwilligungsbasis erfolgen. Auch hierfür ist eine Rechtsgrundlage erforderlich, die die Datenverarbeitung in Servicekonten vollständig erfasst. Bei der Identifizierung eines bevollmächtigten Beschäftigten dürfen nur die für diese Identifizierung erforderlichen Daten erfasst werden.*

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

12.2 Plattformen und Verfahren

Angesichts sich fortlaufend verändernder Rahmenbedingungen habe ich im Berichtszeitraum staatliche und kommunale Stellen zu verschiedenen E-Government-Projekten beraten.

Dies betrifft etwa den Einsatz von **De-Mail** (siehe 26. Tätigkeitsbericht 2014 unter Nr. 2.2.5). Der IT-Beauftragte der Bayerischen Staatsregierung hatte mir im Dezember 2015 einen Zwischenbericht übermittelt, in dem die Erkenntnisse der Pilotphasen zusammengefasst waren. Danach wurden im Rahmen der zwischenzeitlich zweijährigen Pilotphase zahlreiche Staats- und Kommunalbehörden aus unterschiedlichen Verwaltungsebenen in die Lösungsfindung einbezogen. Dabei wurden Einsatzfähigkeit, Praktikabilität und verschiedene Ausgestaltungen der Umsetzbarkeit überprüft.

Auf der Basis dieses Zwischenberichts des IT-Beauftragten der Bayerischen Staatsregierung habe ich diesen zu den weiter zu beachtenden datenschutzrechtlichen Anforderungen beraten, insbesondere im Hinblick auf eine auch im Raum stehende zentrale Gateway-Lösung. Bei dieser Variante werden eingehende De-Mails über ein zentrales Gateway an die angeschlossenen Behörden verteilt. Die zwischenzeitlichen Rechtsänderungen insbesondere durch das Bayerische E-Government-Gesetz (siehe Nr. 12.1) waren dabei zu berücksichtigen. Kommende Planungen und eine Umsetzung werde ich weiter begleiten.

Zum **Bürgerservice-Portal** (siehe 26. Tätigkeitsbericht 2014 unter Nr. 12.2) waren ebenfalls fortlaufende Beratungen erforderlich. Das Bürgerservice-Portal ist ein Projekt der Anstalt für Kommunale Datenverarbeitung in Bayern. Bausteine sind das Bürgerkonto, eine E-Payment- und eine Postkorb-Funktion. Portallösungen werden regelmäßig initiiert, um für Bürger, Unternehmen und Verwaltung einheitliche und effektive Verfahren beziehungsweise digitale Leistungen anzubieten. Einzelne Bausteine wie einerseits der Betrieb des Bürgerkontos und andererseits der Betrieb einer Postkorb- sowie einer E-Payment-Funktion wurden rechtlich unterschiedlichen Stellen zugeordnet. Daraus ergibt sich ein komplexes Netzwerk anzuwendender Vorschriften und rechtlicher Verantwortlichkeiten, teilweise ergänzt durch Auftragsdatenverarbeitungen. In der Regel sind also von verschiedenen Stellen mehrere Rechtsbereiche zu beachten, etwa das Telemediengesetz und das Bayerische Datenschutzgesetz sowie spezialgesetzliche Datenschutzregelungen wie solche des Sozialgesetzbuchs. Nach Inkrafttreten des Bayerischen E-Government-Gesetzes sowie der Änderungen der Bayerischen Verordnung zur Schaffung barrierefreier Informationstechnik (siehe Nr. 12.1) sind auch diese Vorschriften zu beachten. Hierzu habe ich die Anstalt für Kommunale Datenverarbeitung sowie weitere anfragende Stellen, die derartige Portallösungen nutzen wollten, auf die rechtlichen und technisch-organisatorischen Anforderungen hingewiesen.

Beispielhaft möchte ich herausgreifen, dass Nutzerinnen und Nutzer solcher Portallösungen über die verantwortliche Stelle und darüber, welche Daten zu welchem Zweck erhoben und verarbeitet werden, informiert werden müssen. Dies gilt umso mehr, wenn einzelne Datenverarbeitungen auch auf Einwilligungen von Betroffenen gestützt werden sollen. Soweit für einzelne Bausteine und die dabei verarbeiteten personenbezogenen Daten verschiedene Stellen verantwortlich sind, müssen dies und die zugehörigen Informationen jeweils ausreichend klar ersichtlich sein. Denn mit dem nächsten Klick im Rahmen von Portalwebseiten beziehungsweise Webseiten einer Behörde, die solche Portallösungen nutzt, „betritt“ die betroffene Person (mit ihren Daten) ansonsten möglicherweise eine andere Behörde, ohne dies zu bemerken. Hier hat die Anstalt für Kommunale Datenverarbeitung nach intensivem Gedankenaustausch im Rahmen des Bürgerkontos erhebliche Verbesserungen vorgenommen, etwa im Hinblick auf das Auffinden des zugehörigen Impressums und der zugehörigen Datenschutzerklärung.

Seit 18. November 2015 ist das **BayernPortal** online. Unter www.freistaat.bayern wird seither die zentrale Informationsplattform der öffentlichen Verwaltung in Bayern für Bürgerinnen und Bürger, Unternehmen und Verwaltungen betrieben. Hierüber sind Online-Dienstleistungen, Fachdatenbanken, Formulare und Merkblätter sowie Ansprechpartner bei Behörden zu finden. Dabei werden Angebote von Staat und Kommunen „unter einem Dach" gebündelt. Mittels des Bayernportals kann man sich aber nicht nur informieren, sondern über diese Plattform können auch weitere Funktionen wie eine digitale Authentifizierung, ein digitaler Postkorb oder digitales Bezahlen zugänglich sein.

Auch beim Betrieb dieser Plattform und der hierüber zugänglichen Dienstleistungen sind verschiedene Gesetze und Verantwortlichkeiten zu berücksichtigen. Erfahrungen bei anderen Plattformen konnten in meine Beratung einfließen. Derartige Plattformen und die zugänglichen Dienste sind allerdings keine statischen Einrichtungen, sondern unterliegen sich verändernden tatsächlichen, technischen und rechtlichen Anforderungen, die von den jeweils verantwortlichen Stellen immer wieder neu erkannt und nachjustiert werden müssen. Auch hierauf werde ich weiterhin achten.

Im Zusammenhang mit **Service- oder Bürgerkonten** weise ich auch an dieser Stelle auf die Entschließung der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 6./7. April 2016 in Schwerin „Datenschutz bei Servicekonten" (siehe Nr. 12.1) hin.

12.3 Verfolgung des Nutzerverhaltens im Internet

Unter welchen Voraussetzungen das Verhalten von Nutzerinnen und Nutzern im Internet verfolgt werden darf, ist im Telemediengesetz geregelt. Leider setzt dieses Gesetz die europarechtlichen Vorgaben nicht umfassend in deutsches Recht um. Dies war der Anlass für die

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 05.02.2015

Verfolgung des Nutzerverhaltens im Internet

Cookies und verschiedene andere Technologien ermöglichen die Verfolgung des Nutzerverhaltens im Internet. Sie werden immer häufiger zur Bildung von anbieterübergreifenden Nutzungsprofilen verwendet, um Nutzern dann z.B. auf sie zugeschnittene Werbung anzuzeigen. Die Datenschutzrichtlinie für elektronische Kommunikation (E-Privacy Richtlinie, Art. 5 Abs. 3, RL 2002/58/EG) gestattet die Speicherung von Informationen oder den Zugriff auf Informationen, die bereits im Endgerät eines Nutzers gespeichert sind, jedoch nur, wenn der Nutzer dazu seine Einwilligung gegeben hat. Außerdem müssen die Diensteanbieter die Nutzer vor der Speicherung von Informationen mittels Cookies, Web Storage oder ähnlichen Instrumenten klar und umfassend über deren Zweck informieren. Dies gilt auch für den Zugriff auf Browser- oder Geräteinformationen zur Erstellung von sog. Device Fingerprints. Der europäische Gesetzgeber misst dem Einsatz dieser Technologien zu Recht ein hohes Gefährdungspotential für die Persönlichkeitsrechte der Nutzer bei.

Das Telemediengesetz (TMG) setzt diese europarechtlichen Vorgaben allerdings nur unvollständig in deutsches Recht um. Darauf haben die Datenschutzbeauftragten von Bund und Ländern die Bundesregierung bereits wiederholt hingewiesen. Dies hat bisher jedoch nicht zu einer Änderung des TMG geführt. Die Bundesregierung hält vielmehr die derzeit geltenden Vorgaben des Telemediengesetzes für ausreichend. Diese Auffassung ist unzutreffend. So ist die europarechtlich geforderte Einwilligung bereits in den Zugriff auf in den Endgeräten der Nutzer gespeicherte Informationen (Cookies) im deutschen Recht nicht enthalten.

Die fortgesetzte Untätigkeit der Bundesregierung und des Gesetzgebers hat zur Folge, dass gegenwärtig die Betroffenen ihre Ansprüche zur Wahrung der Privatsphäre aus Art. 5 Abs. 3 der E-Privacy-Richtlinie gegenüber Anbietern in Deutschland, bei denen das TMG zur Anwendung kommt, nur unzureichend wahrnehmen können. Damit wird den Bürgerinnen und Bürgern faktisch ein europarechtlich vorgesehenes, wesentliches Instrument zur Wahrung ihrer Privatsphäre bei der Nutzung des Internets vorenthalten. Die Datenschutzbeauftragten des Bundes und der Länder halten diesen Zustand für nicht hinnehmbar. Sie fordern die Bundesregierung auf, die E-Privacy-Richtlinie nun ohne weitere Verzögerungen vollständig in das nationale Recht zu überführen. Gerade die Weiterentwicklung von neuen Technologien zur Sammlung und Analyse des Nutzerverhaltens im Internet macht moderne und effiziente Regelungen zum Schutz der Privatsphäre der Nutzer unabdingbar.

Eine Initiative der Bundesregierung zu einer entsprechenden Änderung des Telemediengesetzes erfolgte leider bislang nicht.

Aber auch hier wirft der neue europäische Datenschutz-Rechtsrahmen seine Schatten voraus. In Erwägungsgrund 173 zur Datenschutz-Grundverordnung wird zu der – in der Entschließung genannten – Richtlinie 2002/58/EG Folgendes ausgeführt: Die Richtlinie sollte einer Überprüfung unterzogen werden, um insbesondere die Kohärenz mit der Datenschutz-Grundverordnung zu gewährleisten.

Die Europäische Kommission hat bereits eine öffentliche Konsultation in Bezug auf die Evaluierung und Überprüfung der Richtlinie 2002/58/EG durchgeführt. Die Artikel 29-Datenschutzgruppe hat am 19. Juli 2016 ausführlich Stellung genommen und Empfehlungen für Änderungen gegeben. Es steht also zu hoffen, dass nach der zu erwartenden Überarbeitung dieses Rechtsbereichs der Schutz personenbezogener Daten noch effektiver gewährleistet wird.

In der unabhängigen Artikel 29-Datenschutzgruppe stimmen sich die Datenschutzaufsichtsbehörden aller Mitgliedstaaten der Europäischen Union untereinander ab und beraten die Europäische Kommission. Diese Arbeitsgruppe beruht auf Artikel 29 der Europäischen Datenschutzrichtlinie (95/46/EG) und ist daher nach diesem Artikel benannt.

12.4 Soziale Medien, insbesondere Soziale Netzwerke

Soziale Medien und deren Nutzung durch weite Teile der Bevölkerung sind inzwischen Alltag. Die Nutzung Sozialer Medien durch bayerische öffentliche Stellen, die anderen Anforderungen unterliegt, habe ich bereits in meinem 25. Tätigkeitsbericht 2012 unter Nr. 1.3 aufgegriffen. Zu den Schwerpunkten „Fanpages bayerischer Behörden“, „Facebook als dienstlicher Kommunikationskanal“ und „Social

Plugins auf Webseiten bayerischer Behörden“ habe ich in meinem 26. Tätigkeitsbericht 2014 unter Nr. 12.4 ausführlich berichtet. Auch wenn mittlerweile weitere Rechtsprechung ergangen ist, so hat sie zentrale Fragen zum Betrieb einer Fanpage noch nicht abschließend geklärt.

Von besonderem Interesse ist eine noch ausstehende Entscheidung des Europäischen Gerichtshofs. Das Bundesverwaltungsgericht hat ein bei ihm anhängiges Revisionsverfahren zum Betrieb einer Fanpage ausgesetzt und dem Europäischen Gerichtshof Fragen zur Vorabentscheidung vorgelegt (Beschluss vom 25. Februar 2016 – 1 C 28.14): Etwa, ob einen Fanpagebetreiber eine datenschutzrechtliche Verantwortlichkeit für die Auswahl des Betreibers seiner Internetrepräsentanz und dessen datenschutzkonformen Umgangs mit personenbezogenen Daten trifft. Ausgangspunkt für den Rechtsstreit war eine Anordnung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, eine Fanpage zu deaktivieren. Es besteht die Hoffnung, dass im Rahmen dieser Verfahren zentrale Fragen nunmehr höchstrichterlich geklärt werden.

Auch im aktuellen Berichtszeitraum habe ich bei Beratungen und Prüfungen meine bisherigen Bewertungen zugrunde gelegt. Maßstab für die Nutzung Sozialer Medien durch bayerische Behörden bleibt dabei, ob dies nach den datenschutzrechtlichen Vorschriften zulässig ist. Gesichtspunkte wie „Bürgernähe“ oder „Image“ können diesen Maßstab nicht ersetzen. Der Beratungsbedarf hat sich hier auf hohem Niveau stabilisiert.

13 Spezielle datenschutzrechtliche Themen

13.1 Recht auf Auskunft

Mit dem Gesetz über die elektronische Verwaltung in Bayern wurde ein allgemeines **Recht auf Auskunft** eingeführt. Dieses Recht ist in Art. 36 BayDSG geregelt. Die Norm ist zum 30. Dezember 2015 in Kraft getreten. Zwar konnte bereits bisher auf Grundlage von § 9 Abs. 1 Satz 1 Allgemeine Geschäftsordnung für die Behörden des Freistaates Bayern (AGO) Auskunft gewährt werden. Nun hat erstmals der Gesetzgeber einen echten allgemeinen, von Verfahrenspositionen unabhängigen Auskunftsanspruch geschaffen. Der Auskunftsanspruch soll die Einbindung der Bürgerinnen und Bürger in Vorgänge der öffentlichen Verwaltung stärken (siehe Landtags-Drucksache 17/7537, S. 48).

Art. 36 BayDSG Recht auf Auskunft
(1) [1]Jeder hat das Recht auf Auskunft über den Inhalt von Dateien und Akten öffentlicher Stellen, soweit ein berechtigtes, nicht auf eine entgeltliche Weiterverwendung gerichtetes Interesse glaubhaft dargelegt wird und

1. *bei personenbezogenen Daten eine Übermittlung an nicht-öffentliche Stellen zulässig ist und*
2. *Belange der öffentlichen Sicherheit und Ordnung nicht beeinträchtigt werden.*

[2]Die Auskunft kann verweigert werden, soweit

1. *Kontroll- und Aufsichtsaufgaben oder sonstige öffentliche oder private Interessen entgegenstehen,*
2. *sich das Auskunftsbegehren auf den Verlauf oder auf vertrauliche Inhalte laufender oder abgeschlossener behördeninterner Beratungen oder auf Inhalte aus nicht abgeschlossenen Unterlagen oder auf noch nicht aufbereitete Daten bezieht oder*

3. ein unverhältnismäßiger Aufwand entsteht.

(2) Abs. 1 findet keine Anwendung auf Auskunftsbegehren, die Gegenstand einer Regelung in anderen Rechtsvorschriften sind.

(3) Ausgenommen von der Auskunft nach Abs. 1 sind

1. Verschlusssachen,

2. einem Berufs- oder besonderen Amtsgeheimnis unterliegende Datei- und Akteninhalte sowie

3. zum persönlichen Lebensbereich gehörende Geheimnisse oder Betriebs- und Geschäftsgeheimnisse, sofern der Betroffene nicht eingewilligt hat.

(4) [1]Öffentliche Stellen im Sinn des Abs. 1 sind nicht

1. der Landtag, der Oberste Rechnungshof und die Staatlichen Rechnungsprüfungsämter, der Bayerische Kommunale Prüfungsverband, der Landesbeauftragte für den Datenschutz und das Landesamt für Datenschutzaufsicht,

2. die obersten Landesbehörden in Angelegenheiten der Staatsleitung und der Rechtsetzung,

3. die Gerichte, Strafverfolgungs- und Strafvollstreckungsbehörden, Gerichtsvollzieher, Notare und die Landesanwaltschaft Bayern als Organe der Rechtspflege sowie die Justizvollzugsbehörden, die Disziplinarbehörden und die für Angelegenheiten der Berufsaufsicht zuständigen berufsständischen Kammern und Körperschaften des öffentlichen Rechts,

4. die Polizei und das Landesamt für Verfassungsschutz einschließlich der für ihre Aufsicht zuständigen Stellen,

5. Finanzbehörden in Verfahren nach der Abgabenordnung,

6. Universitätskliniken, Forschungseinrichtungen, Hochschulen, Schulen sowie sonstige öffentliche Stellen im Bereich von Forschung und Lehre, Leistungsbeurteilungen und Prüfungen,

7. die Landeskartellbehörde und die Regulierungskammer des Freistaates Bayern sowie die Industrie- und Handelskammern und die Handwerkskammern,

8. die kommunalen Spitzenverbände.

[2]Datei- und Aktenbestandteile der in Satz 1 genannten oder für Angelegenheiten im Sinn von Art. 2 Abs. 4 zuständigen Stellen sind von der Auskunft nach Abs. 1 auch dann ausgenommen, wenn sie sich in Dateien oder Akten anderer öffentlicher Stellen befinden.

(5) Für die Auskunft werden Kosten nach Maßgabe des Kostengesetzes erhoben.

Zu Art. 36 BayDSG habe ich sowohl Bürgerinnen und Bürger als auch bayerische öffentliche Stellen bei konkreten Vorgängen und allgemeinen Anfragen beraten. Dabei habe ich auch dann auf diese Regelung hingewiesen, wenn sich die Beteiligten selbst nicht auf Art. 36 BayDSG bezogen hatten. Beispielsweise haben sich Auskunftssuchende wiederholt auf das Informationsfreiheitsgesetz (IFG) berufen. Dieses Gesetz regelt einen Anspruch auf Zugang zu amtlichen Informationen jedoch nur gegenüber den Behörden des Bundes, nicht hingegen gegenüber Behörden des Freistaates Bayern oder den Kommunen. Bei Auskunftsbegehren sollten Behörden also nicht ausschließlich eine im Antrag angegebene Vorschrift in den Blick nehmen, sondern auch das erkennbar Gewollte und die möglicherweise in diesem Zusammenhang sonst noch bestehenden Regelungen.

Darüber hinaus habe ich eine **erste Handreichung** erarbeitet, die auf meiner Homepage https://www.datenschutz-bayern.de abrufbar ist. Diese Handreichung ist nachfolgend auszugsweise wiedergegeben.

Wie Sie das allgemeine Auskunftsrecht geltend machen:

1. Müssen Sie Ihren Auskunftsantrag begründen?

*Zur Begründung Ihres Auskunftsanspruchs müssen Sie ein „berechtigtes, nicht auf eine entgeltliche Weiterverwendung gerichtetes Interesse" glaubhaft darlegen. Ein **berechtigtes Interesse** kann im Grundsatz „jedes von der Rechtsordnung gebilligte Interesse" sein, das über reine Neugierde hinausgeht. Berechtigte Interessen können rechtlich, wirtschaftlich oder ideell begründet werden. Das berechtigte Interesse ist also weit zu verstehen.*

Beispiel:
Ein kleiner Sportverein bemüht sich um finanzielle Förderung. Ein Mitglied des Vereins will von seiner Gemeindeverwaltung wissen, ob und welche bislang nicht veröffentlichten Kriterien es für die Förderung von Vereinen gibt. Ein berechtigtes Interesse liegt vor.

*Sie müssen Ihr berechtigtes Interesse **glaubhaft darlegen**; gemeint ist, dass Sie Ihr Auskunftsinteresse nachvollziehbar schildern müssen. Hieran darf die Verwaltung keine überzogenen Anforderungen stellen, insbesondere müssen Sie Ihr berechtigtes Interesse nicht beweisen.*

*Der allgemeine Auskunftsanspruch soll allerdings keine kommerzielle Verwertung, insbesondere keinen Handel mit den Verwaltungsdaten ermöglichen. Deshalb darf das Interesse nicht auf die **entgeltliche Weiterverwendung** gerichtet sein.*

2. Ist die Auskunft kostenpflichtig?

Für die Auskunftserteilung sieht Art. 36 Abs. 5 BayDSG die Erhebung von Kosten nach dem Kostengesetz vor. Insbesondere bei umfangreicheren Auskunftsbegehren und der Bitte um Zusendung von Kopien kann es empfehlenswert sein, sich vorher bei der Verwaltung über den möglichen Umfang der Kosten zu erkundigen.

Auskünfte einfacher Art sind nicht kostenpflichtig (Art. 3 Abs. 1 Satz 1 Nr. 3 Kostengesetz).

3. Welche Informationen können Sie mithilfe des allgemeinen Auskunftsrechts erhalten?

Im Grundsatz können Sie Inhalte von Dateien und von Akten bayerischer öffentlicher Stellen erfragen. Steht Ihnen ein Auskunftsanspruch zu, entscheidet die öffentliche Stelle sodann nach pflichtgemäßem Ermessen darüber, in welcher Form der Auskunftsanspruch erfüllt wird, ob durch Gewährung von Akteneinsicht, mündliche Auskunftserteilung, Überlassung von Kopien o.ä.

Beispiel:
Eine Gemeindeverwaltung, die ihre Förderkriterien für Vereine in einem Vermerk zusammengefasst hat, wird in ihrer Antwort diesen Vermerk häufig nicht umschreiben, sondern schlichtweg ausdrucken und dem Antragsteller oder der Antragstellerin zusenden.

*Bayerische öffentliche Stellen sind **fast alle Behörden** des Freistaates Bayern, der Bezirke, Landkreise, Gemeinden und der sonstigen der Aufsicht des Freistaates Bayern unterstehenden juristischen Personen des öffentlichen Rechts. Dazu können auch bestimmte Unternehmen zählen, die öffentliche Aufgaben wahrnehmen (Art. 2 Abs. 2 BayDSG).*

***Für einige Stellen bzw. Bereiche klammert Art. 36 Abs. 3 und Abs. 4 allerdings von vornherein das allgemeine Auskunftsrecht ausdrücklich aus**. Teilweise hängt das damit zusammen, dass diese Stellen ohnehin weitreichende Informationspflichten erfüllen (z.B. Bayerischer Landtag, Bayerischer Oberster Rechnungshof), teilweise will der Gesetzgeber die Effektivität und Funktionsfähigkeit bestimmter Verwaltungszweige schützen (z.B. Polizei, Finanzbehörden, Gerichte), teilweise verwenden diese Stellen in besonders großem Umfang vertrauliche Daten, die nicht beauskunftet werden dürfen (Landesamt für Verfassungsschutz, Bayerischer Landesbeauftragter für den Datenschutz).*

4. Beeinträchtigt das Auskunftsrecht nicht den Datenschutz oder sonstige Geheimnisse?

*Das Auskunftsrecht besteht nur, wenn die allgemeinen **datenschutzrechtlichen Voraussetzungen** für eine Datenübermittlung erfüllt sind. Soweit hiervon konkret bestimmbare Personen in schutzwürdigen Interessen betroffen sind, darf die Verwaltung die begehrte Auskunft also nicht erteilen.*

*Zudem darf die Auskunft **Belange der öffentlichen Sicherheit und Ordnung** nicht beeinträchtigen.*

*In Art. 36 Abs. 1 Satz 2 BayDSG ist auch vorgesehen, dass die Verwaltung eine beantragte Auskunft verweigern kann, **soweit** bestimmte **weitere öffentliche und private Schutzinteressen** das individuelle Auskunftsinteresse überwiegen. Dabei muss die Verwaltung die Interessen an der Auskunftserteilung und an der Auskunftsverweigerung unter Berücksichtigung aller wesentlichen Umstände des Einzelfalls abwägen. Überwiegt das Auskunftsinteresse etwaige Auskunftsverweigerungsgründe, muss die Verwaltung den Auskunftsanspruch erfüllen. Das Wort „soweit" verdeutlicht, dass die Verwaltung unter Umständen Auskünfte auch nur teilweise verweigern kann und dann zumindest Teilauskünfte erteilen muss.*

5. In welchem Verhältnis steht das allgemeine Auskunftsrecht zu anderen Informationszugangsrechten?

Der allgemeine Auskunftsanspruch ist gegenüber anderen, speziellen Informationszugangsregelungen nachrangig.

Beispiele:
Die Gesetzesbegründung nennt dazu beispielsweise das Auskunftsrecht der Presse, das Umweltinformationsrecht, die Regelungen der Auskunftsrechte von Mandatsträgerinnen und -trägern sowie die besonderen Auskunftsrechte von Verfahrensbeteiligten eines Verwaltungsverfahrens.

„Nachrangig" heißt: Ist ein besonderes Informationszugangsrecht anwendbar, findet das allgemeine Auskunftsrecht keine Anwendung.

6. *Sind mit dem allgemeinen Recht auf Auskunft jetzt alle gemeindlichen Informationsfreiheitssatzungen außer Kraft getreten?*

Nein. Im Grundsatz beeinträchtigt das neue Recht auf Auskunft die Geltung gemeindlicher Informationsfreiheitssatzungen nicht.

7. *Welche Neuerungen ergeben sich für Gemeinden, die bereits eine Informationsfreiheitssatzung erlassen haben?*

Das Recht auf Auskunft in Art. 36 BayDSG kann weiter reichen als das in einer gemeindlichen Informationsfreiheitssatzung verankerte Zugangsrecht, aber auch hinter einem solchen Recht zurückbleiben. Die Gemeinde sollte deshalb prüfen, in welchem Verhältnis die beiden Zugangsrechte zueinander stehen. Dann kann sie den Auskunft suchenden Bürger sachgerecht beraten, mit welchem Anspruch er sein Auskunftsanliegen am besten verfolgen kann.

Das gesetzliche Zugangsrecht erfasst anders als das satzungsmäßige auch Akten und Dateien, die bei Erfüllung von Aufgaben im übertragenen Wirkungskreis der Gemeinde entstehen.

8. *Können einem Bürger Auskunftsansprüche aus der gemeindlichen Informationsfreiheitssatzung und aus Art. 36 BayDSG nebeneinander zustehen oder schließt einer dieser Ansprüche den jeweils anderen aus?*

Auskunftsansprüche aus einer gemeindlichen Informationsfreiheitssatzung und aus Art. 36 BayDSG können sowohl allein als auch nebeneinander bestehen. Oftmals werden sie ähnliche Wirkungen entfalten.

Steht dem Bürger nach Art. 36 BayDSG ein Auskunftsanspruch zu, nach der gemeindlichen Informationsfreiheitssatzung jedoch nicht, muss die Gemeinde den gesetzlichen Anspruch erfüllen. Sie kann nicht durch Satzungsrecht den gesetzlichen Auskunftsanspruch „aushebeln".

Gemeindliche Informationsfreiheitssatzungen können für den eigenen Wirkungskreis der Gemeinden Auskunftsansprüche regeln, die weiter reichen als Art. 36 BayDSG.

Dabei müssen die gemeindlichen Informationsfreiheitssatzungen aber die gesetzlichen Vorgaben beachten, die schon bisher für die Einräumung solcher Ansprüche maßgeblich waren. Transparenz gibt es nach bayerischem Landesrecht nur „Hand in Hand" mit dem Daten- und Geheimnisschutz, nicht zu dessen Lasten. Art. 36 BayDSG gibt den Gemeinden zwar grundsätzlich kein verbindliches Regelungsmodell vor. Gemeindliche Informationsfreiheitssatzungen werden gleichwohl nicht in einem „rechtsfreien Raum" erlassen. Sie dürfen insbesondere keine Datenflüsse gestatten, die den Anforderungen des Art. 19 BayDSG nicht entsprechen. Die Bedeutung dieser Vorgabe des bayerischen Datenschutzrechts auch für Auskunftsansprüche hat der Gesetzgeber in Art. 36 Abs. 1 Satz 1 Nr. 1 BayDSG ausdrücklich bekräftigt. Zudem verweist Art. 36 Abs. 3 BayDSG darauf, dass bei der Regelung von Informationszugangsrechten bestimmte Geheimnisse nicht zur Disposition stehen. Diese Geheimnisse hat auch der kommunale Satzungsgeber zu respektieren.

Gemeindliche Informationsfreiheitssatzungen können allerdings Fragen regeln, die der Gesetzgeber nicht beantwortet hat. So kann die Gemeinde etwa verfahrensrechtliche Vorgaben festlegen, welche die Effektivität des Rechts auf Auskunft erhöhen.

Beispiele:
Die Gemeinde kann einen festen Ansprechpartner bestimmen oder Bearbeitungsfristen vorgeben.

9. Steht die allgemeine beamtenrechtliche Verschwiegenheitspflicht einer Auskunftserteilung entgegen?

*Nein. Die **allgemeine beamtenrechtliche Verschwiegenheitspflicht** ist in § 37 Abs. 1 Satz 1 Beamtenstatusgesetz geregelt. Dort heißt es: „Beamtinnen und Beamte haben über die ihnen bei oder bei Gelegenheit ihrer amtlichen Tätigkeit bekannt gewordenen dienstlichen Angelegenheiten Verschwiegenheit zu bewahren." Nach § 37 Abs. 2 Satz 1 Nr. 1 Beamtenstatusgesetz gilt dies allerdings nicht, soweit Mitteilungen im dienstlichen Verkehr geboten sind. Dies ist der Fall, wenn ein Bürger sein Recht auf Auskunft nach Art. 36 BayDSG gegenüber einer öffentlichen Stelle geltend macht und ein dort tätiger Beamter einen bestehenden Auskunftsanspruch erfüllt. Der Beamte muss dafür zuständig sein und darf diejenigen Tatsachen mitteilen, deren Kenntnis der Bürger kraft seines Rechts auf Auskunft verlangen kann.*

***Besondere Verschwiegenheitspflichten** werden einer Auskunft dagegen regelmäßig entgegenstehen. Art. 36 Abs. 3 Nr. 2 BayDSG bestimmt, dass „einem […] besonderen Amtsgeheimnis unterliegende Datei- und Akteninhalte" dem Recht auf Auskunft nicht unterliegen. Besondere Verschwiegenheitspflichten ergeben sich etwa aus dem Steuergeheimnis, aus dem Sozialgeheimnis sowie im Zusammenhang mit der Vertraulichkeit von Personaldaten."*

13.2 Safe Harbor – EU-US Privacy Shield

Die Übermittlung personenbezogener Daten an Empfänger außerhalb der Europäischen Union gehört nicht zum klassischen Aufgabenbereich einer bayerischen öffentlichen Stelle. In Zeiten der Digitalisierung und Globalisierung können solche Datenübermittlungen durch bayerische Behörden dennoch im Raum stehen, beispielsweise wenn sie Dienstleister (Datenverarbeiter) mit Sitz in den USA nutzen wollen.

Die Europäische Kommission hat nach Art. 25 Abs. 6 der Europäischen Datenschutzrichtlinie (RL 95/46/EG) die Befugnis zur Feststellung, dass ein Drittland hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau im Sinne des Art. 25 Abs. 2 dieser Richtlinie gewährleistet. Ob ein angemessenes Datenschutzniveau vorliegt, hat Auswirkungen auf die Zulässigkeit von Datenübermittlungen.

Insbesondere in der Folge der Safe Harbor-Entscheidung des Europäischen Gerichtshofs vom 6. Oktober 2015 (C-362/14) ergab sich hier erheblicher Beratungsbedarf. Daher habe ich am 7. Oktober 2015 eine Pressemitteilung und in der Folge entsprechend den Entwicklungen aktualisierte Informationen auf meiner

Homepage https://www.datenschutz-bayern.de veröffentlicht. Daneben habe ich konkrete Anfragen von Bürgerinnen und Bürgern sowie von Behörden hierzu beantwortet.

Der Europäische Gerichtshof hat mit seinem Urteil vom 6. Oktober 2015 die Entscheidung der Europäischen Kommission (2000/520/EG) für ungültig erklärt, dass in den USA im Rahmen der Safe Harbor-Regelungen ein angemessenes Datenschutzniveau gewährleistet ist.

Es ist also seither nicht mehr möglich, sich im Zusammenhang mit Datenübermittlungen in die USA auf Safe Harbor zu berufen.

Dabei ist zu beachten, dass Ausgangspunkt einer Zulässigkeitsprüfung nicht die Safe Harbor-Regelungen als solche waren, sondern das für die jeweilige Behörde geltende Datenschutzgesetz. Für bayerische öffentliche Stellen ist dies – soweit keine vorrangigen Regelungen wie etwa im Sozialgesetzbuch anzuwenden sind – das Bayerische Datenschutzgesetz. Dort finden sich neben den Regelungen zur Auftragsdatenverarbeitung auch Vorschriften zu Datenübermittlungen an Stellen außerhalb der Mitgliedstaaten der Europäischen Union beziehungsweise des Europäischen Wirtschaftsraums. Insbesondere in Art. 21 Abs. 2 BayDSG sind Datenübermittlungen (auch) in die USA geregelt.

Im Rahmen der jeweils anzuwendenden Vorschrift spielten dann bei einem Tatbestandsmerkmal „angemessenes Datenschutzniveau“ die Safe Harbor-Regelungen eine Rolle.

Nach Aufhebung der Entscheidung der Europäischen Kommission zu Safe Harbor war dies eben nicht mehr der Fall. Bayerische öffentliche Stellen, die sich bislang hierauf bezogen hatten, mussten schon deswegen entsprechende Datenübermittlungen überprüfen.

Nach weiteren Verhandlungen haben sich die Europäische Kommission und die US-Regierung auf (neue) Rahmenbedingungen geeinigt, die gewährleisten sollen, dass beim Empfänger in den USA ein angemessenes Datenschutzniveau besteht. Die Europäische Kommission sah sich veranlasst, am 12. Juli 2016 festzustellen, dass ein angemessenes Datenschutzniveau unter den Rahmenbedingungen des EU-US Privacy Shield besteht (vgl. Durchführungsbeschluss (2016) 1250, veröffentlicht im Amtsblatt EU vom 1. August 2016, L 207/1). Der Privacy Shield ist unter veränderten Bedingungen sozusagen der Nachfolger von Safe Harbor. Diese Angemessenheitsentscheidung gilt jedoch nicht grundlegend im Hinblick auf alle Empfänger in den USA, sondern nur im Hinblick auf Unternehmen, die sich den Privacy Shield-Regelungen unterwerfen und entsprechend vom US-Handelsministerium registriert sind.

Der neue Rechtsakt ist bereits heftig kritisiert worden. Kritiker meinen, die Feststellungen des Europäischen Gerichtshofs seien nicht vollständig umgesetzt worden. Problematisch sei unter anderem, dass die Zusicherungen der US-Regierung nicht gesetzlich abgesichert seien.

Die Artikel 29-Datenschutzgruppe hat zwar Verbesserungen gegenüber Safe Harbor und gegenüber dem vorhergehenden Entwurf des Privacy Shield anerkannt, jedoch ebenfalls eine Reihe von Bedenken geäußert. Diese Gruppe verlangt insbesondere eine Garantie von den US-Behörden, keine ungerichtete Massenüberwachung vorzunehmen. Zudem bleibe abzuwarten, ob der Datenzugriff

durch US-Behörden wie zugesichert in einem engen Rahmen bleibt. Die Artikel 29-Datenschutzgruppe hat angekündigt, das Abkommen erst im Jahr 2017 nach Vorliegen erster Vollzugserfahrungen abschließend zu bewerten.

In der unabhängigen Artikel 29-Datenschutzgruppe stimmen sich die Datenschutzaufsichtsbehörden aller Mitgliedstaaten der Europäischen Union untereinander ab und beraten die Europäische Kommission. Diese Arbeitsgruppe beruht auf Art. 29 RL 95/46/EG und ist daher nach diesem Artikel benannt.

Der Privacy Shield ändert – wie zuvor Safe Harbor – nichts daran, dass eine bayerische öffentliche Stelle anhand der für sie geltenden Datenschutzbestimmungen eine eigene Prüfung durchführen muss, ob die beabsichtigte Datenverarbeitung zulässig ist.

Durch die Entscheidung der Europäischen Kommission bin ich bei entsprechenden Eingaben nicht an der Prüfung gehindert, ob das Recht und die Praxis in den USA beziehungsweise beim Empfänger ein angemessenes Datenschutzniveau gewährleisten. Zwar können die Datenschutzaufsichtsbehörden die Entscheidung der Europäischen Kommission nicht aufheben. Gemäß dem Europäischen Gerichtshof ist es allerdings Sache des nationalen Gesetzgebers, Rechtsbehelfe für die Datenschutzaufsichtsbehörden vorzusehen, damit diese die Angelegenheit vor Gericht bringen können und damit die Möglichkeit des Gerichts besteht, den Europäischen Gerichtshof um Vorabentscheidung über die Gültigkeit der Kommissionsentscheidung zu ersuchen.

Daher erging auch folgende

Umlaufentschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 20.04.2016

Klagerecht für Datenschutzbehörden – EU-Kommissionsentscheidungen müssen gerichtlich überprüfbar sein

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

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

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

Das Bundesministerium des Innern hat hierzu mit Schreiben vom 11. Juli 2016 mitgeteilt, dass es bereits intensiv an der Anpassung des nationalen Datenschutzrechts an die Datenschutz-Grundverordnung arbeite. Der Gesetzentwurf werde auch Rechtsbehelfe der Aufsichtsbehörden enthalten und dabei die einschlägige Rechtsprechung des Europäischen Gerichtshofs berücksichtigen (siehe Unterrichtung durch die Bundesregierung zu Bundesrats-Drucksache 171/16 vom 15. Juli 2016).

13.3 Cloud Computing

Zum Cloud Computing habe ich mich schon in meinem 24. Tätigkeitsbericht 2010 unter Nr. 2.1.5, in meinem 25. Tätigkeitsbericht 2012 unter Nrn. 1.2 und 2.3.3 und in meinem 26. Tätigkeitsbericht 2014 unter Nr. 13.1 kritisch geäußert.

Im aktuellen Berichtszeitraum habe ich mich intensiv mit den Themen Datenverarbeitung im Auftrag durch nichtöffentliche Dienstleister, mit Outsourcing und mit Cloud-Diensten befasst. Bei deren Bewertung ist unter anderem zu berücksichtigen, ob der Dienstleister seine Leistung im Inland, im europäischen Ausland oder aber in einem Staat außerhalb der Europäischen Union beziehungsweise des Europäischen Wirtschaftsraums (und damit in einem sogenannten Drittland) erbringt. Von besonderem Interesse waren dabei Verträge mit Dienstleistern aus Drittländern, namentlich den USA. Dabei war auch von Bedeutung, nicht allgemeine Werbeaussagen von Anbietern zugrunde zu legen, sondern die tatsächlichen Verträge beziehungsweise Vereinbarungen genau zu lesen und zu hinterfragen.

Auch bayerische öffentliche Stellen wollten Dienstleistungsverträge mit nicht deutschen Unternehmen abschließen oder haben dies bereits getan. Die Unternehmen erbringen beziehungsweise erbrachten dabei ihre vertraglichen Leistungen sowohl im Inland als auch im europäischen Ausland (beispielsweise Irland, Niederlande) aber auch gegebenenfalls in einem Staat außerhalb von Europa (beispielsweise USA).

Auch mit dem nun geltenden EU-US Privacy Shield (siehe Nr. 13.2) kann nicht von einer abschließenden Lösung der Herausforderungen gesprochen werden. Denn zum einen betrifft der Privacy Shield nur bestimmte Fallkonstellationen beziehungsweise Teile davon. Zum anderen steht zu erwarten, dass auch gegen den Privacy Shield vor dem Europäischen Gerichtshof geklagt wird. Der Ausgang eines solchen Verfahrens ist offen.

Ich wiederhole daher meine schon bislang ausgesprochene Empfehlung an bayerische öffentliche Stellen, von der Nutzung von Public-Cloud-Diensten mit (auch nur eventuellen) Datenverarbeitungen in den USA abzusehen und möglichst nach nationalen oder zumindest europäischen Lösungen zu suchen.

Für die zweite Jahreshälfte 2016 wurde die sogenannte „Microsoft Cloud Deutschland“ angekündigt. Dabei soll ein Datentreuhändermodell mit einem deutschen Unternehmen angewandt werden, bei dem unter anderem die Datenverarbeitung und -speicherung ausschließlich in zwei, in Deutschland gelegenen Rechenzentren des Treuhänders erfolgen soll. Ein direkter Datenzugriff soll damit dem Dienstleister, also dem vertragsmäßigen Anbieter der Leistung, nämlich Microsoft, unmöglich sein. Inwieweit dies einen möglichen Lösungsansatz für Teile der Herausforderungen darstellt bleibt näheren Untersuchungen vorbehalten.

13.4 Datenübermittlungen durch die Industrie- und Handelskammern

Die Industrie- und Handelskammern haben nach § 1 Industrie- und Handelskammergesetz (IHKG) die Aufgabe, das Gesamtinteresse der ihnen zugehörigen Gewerbetreibenden ihres Bezirkes wahrzunehmen, für die Förderung der gewerblichen Wirtschaft zu wirken und dabei die wirtschaftlichen Interessen einzelner Gewerbezweige oder Betriebe abwägend und ausgleichend zu berücksichtigen.

Zur Erfüllung dieser Aufgaben hat der Gesetzgeber den Kammern in § 9 IHKG bestimmte Möglichkeiten eingeräumt, Daten an andere Industrie- und Handelskammern, aber auch an nichtöffentliche Stellen – also an Dritte oder die Öffentlichkeit – zu übermitteln. Diese rechtlichen Regelungen sind Pflichtmitgliedern vielfach unbekannt, so dass die Rechtmäßigkeit von Datenübermittlungen immer wieder hinterfragt wird.

Ich möchte daher auf folgende Gesetzeslage hinweisen:

13.4.1 Datenübermittlung an andere Industrie- und Handelskammern

Nach § 9 Abs. 3a IHKG dürfen die Industrie- und Handelskammern Name, Firma, Anschrift und Wirtschaftszweig ihrer Kammerzugehörigen sowie die übrigen in § 9 Abs. 1 IHKG genannten Daten (das sind die sonstigen in der Gewerbeanzeige genannten Daten, vgl. § 14 Abs. 1, Abs. 14 Gewerbeordnung (GewO) in Verbindung mit § 3 Abs. 1 Nr. 1 Gewerbeanzeigeverordnung) an andere Industrie- und Handelskammern auf Ersuchen oder durch Abruf im automatisierten Verfahren übermitteln, soweit dies für die Erfüllung der ihnen nach diesem Gesetz übertragenen Aufgaben erforderlich ist. Eine Übermittlung „durch Abruf im automatisierten Verfahren“ bedeutet hierbei, dass ein Bereithalten der genannten Daten in einer Datenbank, auf die andere Industrie- und Handelskammern Zugriff haben, erlaubt ist.

13.4.2 Datenübermittlung an nichtöffentliche Stellen

Nach § 9 Abs. 4 Satz 1 IHKG dürfen die Industrie- und Handelskammern Name, Firma, Anschrift und Wirtschaftszweig – sogenannte **Grunddaten** – von Kammerzugehörigen zur Förderung von Geschäftsabschlüssen und zu anderen dem Wirtschaftsverkehr dienenden Zwecken **an nichtöffentliche Stellen übermitteln**.

Die übrigen in § 9 Abs. 1 IHKG genannten Daten – also die Daten, die darüber hinaus in einer Gewerbeanzeige nach § 14 Abs. 1, Abs. 14 GewO enthalten sind – dürfen an nichtöffentliche Stellen nur übermittelt werden, sofern das Kammermitglied **nicht widersprochen** hat.

Eine solche **Übermittlung** an nichtöffentliche Stellen umfasst auch eine **Veröffentlichung im Internet** (siehe etwa die **Firmendatenbank www.firmen-in-bayern.de** der Industrie- und Handelskammern in Bayern). Denn eine Übermittlung ist das Bekanntgeben gespeicherter personenbezogener Daten an Dritte unter anderem in der Weise, dass Daten von der speichernden Stelle – der Industrie- und Handelskammer – **zum Abruf** bereit gehalten werden, also etwa im Internet durch eine allgemein zugängliche Datenbank jedermann zugänglich gemacht werden. Das Industrie- und Handelskammergesetz beschreibt auch die Zwecke, zu denen eine derartige Veröffentlichung erfolgen darf: Sie darf nur zur Förderung von Geschäftsabschlüssen oder anderen dem Wirtschaftsverkehr dienenden Zwecken erfolgen. Deshalb müssen die Kammern, wenn sie im Internet eine entsprechende Datenbank anbieten, deren Benutzerinnen und Benutzer auf die Einhaltung dieser Zwecke verpflichten (etwa durch entsprechende Allgemeine Geschäftsbedingungen).

Während also eine Veröffentlichung von **Grunddaten** auch gegen den Willen der Pflichtmitglieder rechtlich möglich ist, hat der Gesetzgeber ihnen bei den darüber hinaus reichenden Daten ein Widerspruchsrecht eingeräumt. Da keine (vorherige) Einwilligung vorgesehen ist, ist eine Datenübermittlung solange zulässig, bis das Kammermitglied dieser widerspricht. Der Widerspruch ist jederzeit und ohne Begründung möglich.

Damit die Betroffenen auch Kenntnis vom Widerspruchsrecht erhalten, muss nach § 9 Abs. 4 Satz 3 IHKG auf die Widerspruchsmöglichkeit vor der ersten Übermittlung durch die Industrie- und Handelskammer **schriftlich hingewiesen** werden. Beispielsweise weist daher die Industrie- und Handelskammer für München und Oberbayern in ihrem Begrüßungsschreiben bei neuen Gewerbetreibenden, die nach den Vorgaben des § 2 IHKG Pflichtmitglied sind, auf das Widerspruchsrecht ausdrücklich – und nach meiner Einschaltung durch einen Beschwerdeführer seit dem Frühjahr 2015 in verständlicherer Form – hin.

Das Gesetz schreibt allerdings nicht vor, welche Frist zur Ausübung des Widerspruchsrechts vor (!) einer Datenübermittlung der betroffenen Person eingeräumt werden muss. Ich halte eine Frist von mindestens vier Wochen nach Zugang der Belehrung über das Widerspruchsrecht für angemessen. In diesem Zeitraum kann sich jede betroffene Person darüber klar werden, ob sie eine Datenübermittlung an nichtöffentliche Stellen hinsichtlich ihres Betriebs möchte oder nicht.

§ 9 IHKG Datenschutz
(1) [1]Zur Erfüllung der ihnen nach diesem Gesetz übertragenen Aufgaben dürfen die Industrie- und Handelskammern die Daten nach § 14 Absatz 8 Satz 1 Nummer 1 und Satz 2 der Gewerbeordnung sowie der Rechtsverordnung nach § 14 Absatz 14 der Gewerbeordnung bei den Kammerzugehörigen erheben, soweit diese Daten ihnen nicht von der zuständigen Behörde übermittelt worden sind. …
(3a) Die Industrie- und Handelskammern dürfen Name, Firma, Anschrift und Wirtschaftszweig ihrer Kammerzugehörigen sowie die übrigen in Absatz 1 genannten Daten an andere Industrie- und Handelskammern auf Ersuchen oder durch Abruf im automatisierten Verfahren übermitteln, soweit dies für die Erfüllung der ihnen nach diesem Gesetz übertragenen Aufgaben erforderlich ist.
(4) [1]Die Industrie- und Handelskammern dürfen Name, Firma, Anschrift und Wirtschaftszweig von Kammerzugehörigen zur Förderung von Geschäftsabschlüssen und zu anderen dem Wirtschaftsverkehr dienenden Zwecken an nichtöffentliche Stellen übermitteln. [2]Die übrigen in Absatz 1 genannten Daten dürfen nur zu den

in Satz 1 genannten Zwecken an nichtöffentliche Stellen übermittelt werden, sofern der Kammerzugehörige nicht widersprochen hat. [3]Auf die Möglichkeit, der Übermittlung der Daten an nichtöffentliche Stellen zu widersprechen, sind die Kammerzugehörigen vor der ersten Übermittlung schriftlich hinzuweisen. …

13.5 Erhebung von Kundendaten des Antragstellers in einem Genehmigungsverfahren nach § 10 Bundesimmissionsschutzgesetz

In einem Verwaltungsverfahren muss die Behörde den entscheidungserheblichen Sachverhalt aufklären. Manchmal empfinden Bürgerinnen und Bürger die „Neugier" der Behörde als zu aufdringlich, gerade, wenn es um besonders sensible Daten geht.

So wandte sich in einem Fall ein Bürger an mich, der ein Gewerbe im Bereich der Abfallwirtschaft betreibt. Der Bürger plante eine Verlagerung seines Betriebs. Für den neuen Standort war eine immissionsschutzrechtliche Anlagengenehmigung einzuholen. Das zuständige Landratsamt stellte in Aussicht, im Zuge des Genehmigungsverfahrens Angaben zur Herkunft der in dem Betrieb behandelten Abfälle anzufordern. Der Bürger wollte seine Kundendaten nicht offenlegen, da es sich um Geschäftsgeheimnisse handle. Er verzichtete deshalb zunächst darauf, einen Genehmigungsantrag zu stellen.

Ich habe dem Bürger aus datenschutzrechtlicher Sicht einige Hinweise gegeben:

Soweit sich die Genehmigung für den neuen Standort nach § 6 Abs. 1 Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche Vorgänge (BImSchG) richtet, ist für das Verfahren § 10 BImSchG zu beachten. Dort heißt es:

§ 10 BImSchG Genehmigungsverfahren
(2) Soweit Unterlagen Geschäfts- oder Betriebsgeheimnisse enthalten, sind die Unterlagen zu kennzeichnen und getrennt vorzulegen. Ihr Inhalt muss, soweit es ohne Preisgabe des Geheimnisses geschehen kann, so ausführlich dargestellt sein, dass es Dritten möglich ist, zu beurteilen, ob und in welchem Umfang sie von den Auswirkungen der Anlage betroffen werden können.

Anstelle von Unterlagen mit Geschäfts- oder Betriebsgeheimnissen wird im Rahmen der Öffentlichkeitsbeteiligung eine Inhaltsangabe ausgelegt (§ 10 Abs. 3 Satz 2 BImSchG, § 10 Abs. 3 Satz 1 Neunte Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes – 9. BImSchV). Beansprucht der Antragsteller für Kundendaten aus Sicht der Genehmigungsbehörde zu Unrecht den Schutz durch ein Geschäfts- oder Betriebsgeheimnis und will die Behörde die Angaben deshalb in die Auslegung einbeziehen, muss sie den Antragsteller vorher anhören (§ 10 Abs. 3 Satz 2 9. BImSchV). Eine auf diese Anhörung getroffene Entscheidung, die Unterlagen auszulegen, ist gerichtlich überprüfbar.

Unabhängig vom Schutz der Kundendaten durch ein Geschäfts- oder Betriebsgeheimnis stellt sich die Frage, ob und inwieweit diese Angaben für die Entscheidung über einen Genehmigungsantrag erforderlich wären. Diese Frage kann die Genehmigungsbehörde beantworten, sobald ein Antrag vorliegt, anhand dessen insbesondere die genaue Anlagenart, das zur Genehmigung erforderliche Verfahren sowie der darin maßgebliche Prüfungsumfang bestimmt werden können. Welche Unterlagen im Genehmigungsverfahren benötigt werden, lässt sich dann aus den

einzelnen zum Prüfungsmaßstab gehörenden Vorschriften ableiten. Ein üblicher Verfahrensschritt für die Diskussion dieser Frage ist ein alsbald nach Antragstellung durchgeführter Scoping-Termin.

Das Gesetz stellt sicher, dass Betriebs- und Geschäftsgeheimnisse bei den Genehmigungsbehörden in guten Händen sind. Die Genehmigungsbehörden haben nach Art. 30 Bayerisches Verwaltungsverfahrensgesetz über solche Geheimnisse Verschwiegenheit zu wahren. Die Verpflichtung ist nach Maßgabe von § 353b Abs. 1 Satz 1 Strafgesetzbuch strafbewehrt.

13.6 Übergabe von Ausweisdokumenten an Dritte zum Zwecke der Kfz-Zulassung

Im Berichtszeitraum wurde die Frage an mich herangetragen, ob bei der Fahrzeugzulassung durch Dritte (etwa Autohäuser) diese die Aushändigung des Personalausweises von der zukünftigen Halterin oder vom zukünftigen Halter verlangen dürfen, um die Zulassung bei der Kfz-Zulassungsbehörde stellvertretend vornehmen zu können.

Zweifel an der Rechtmäßigkeit eines solchen Verfahrens werden wegen § 1 Abs. 1 Satz 3 Personalausweisgesetz (PAuswG) geäußert:

§ 1 PAuswG Ausweispflicht; Ausweisrecht
(1)… [3]Vom Ausweisinhaber darf nicht verlangt werden, den Personalausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben. [4]Dies gilt nicht für zur Identitätsfeststellung berechtigte Behörden sowie in den Fällen der Einziehung und Sicherstellung.

Diese Zweifel teile ich allerdings nicht. Denn durch diese Vorschrift sollte eine freiwillige Hingabe des Personalausweises an Dritte durch den Ausweisinhaber **nicht** verboten werden (vgl. Möller, in: Hornung/Möller, Passgesetz – Personalausweisgesetz, 2011, § 1 Rn. 8).

Die Freiwilligkeit ist so lange zu bejahen, wie Betroffene ihr Ziel auch erreichen können, ohne den Gewahrsam am Ausweis aufgeben zu müssen. Das fachlich zuständige Staatsministerium des Innern, für Bau und Verkehr ist unter Bezugnahme auf aktuelle Vorgaben des Bundesministeriums des Innern – zutreffend – der Ansicht, dass die Zulassung von Fahrzeugen durch Dritte (Autohändler) nicht alternativlos ist, sondern eine Dienstleistung darstellt, die vom Ausweisinhaber (Fahrzeughalter) auch selbst erledigt werden könnte. Sie wird also vom Ausweisinhaber **freiwillig** in Anspruch genommen. Insofern stellt die Übergabe des Ausweises an den Autohändler eine freiwillige Herausgabe dar. Ein Verstoß gegen das Personalausweisgesetz besteht daher nicht.

Ist die Fahrzeughalterin oder der Fahrzeughalter bei der Antragstellung zur Fahrzeugzulassung in der Kfz-Zulassungsbehörde persönlich anwesend, kann die Behörde die Vorlage des Ausweises zum Zwecke des Nachweises der Richtigkeit der Halterdaten (vgl. § 33 Abs. 1 Nr. 2 Buchst. a) Straßenverkehrsgesetz in Verbindung mit § 6 Abs. 1 Satz 2 Fahrzeug-Zulassungsverordnung) verlangen.

13.7 Speicherung von durch die Polizei übermittelten Daten durch die Fahrerlaubnisbehörde

Hat die Polizei Informationen über Tatsachen, die auf nicht nur vorübergehende Mängel hinsichtlich der Eignung oder auf Mängel hinsichtlich der Befähigung einer Person zum Führen von Kraftfahrzeugen schließen lassen, so darf sie diese Informationen nach § 2 Abs. 12 Satz 1 Straßenverkehrsgesetz (StVG) den Fahrerlaubnisbehörden grundsätzlich übermitteln. Die Fahrerlaubnisbehörde soll auf diese Weise in die Lage versetzt werden zu prüfen, ob die Einleitung von Überprüfungsmaßnahmen angezeigt ist. Mitgeteilt werden dürfen dabei nur solche Tatsachen, die zur Überprüfung der Eignung oder Befähigung erforderlich sind (siehe auch Nr. 3.8.2).

Im Rahmen meiner Kontrolltätigkeit habe ich erfahren, dass sich bei Fahrerlaubnisbehörden die Praxis entwickelt hat, die von der Polizei übermittelnden Informationen auch dann längerfristig zu speichern, wenn entweder die mitgeteilten Informationen für ein Verfahren zur Klärung von Eignungs- und Befähigungszweifeln nach den §§ 11, 13 Fahrerlaubnisverordnung (FeV) nicht ausgereicht haben oder die betroffene Person überhaupt keine Fahrerlaubnis hat.

Durch die längerfristige Speicherung möchten die Fahrerlaubnisbehörden sicherstellen, dass die übermittelten Informationen noch zur Verfügung stehen, wenn die Betroffenen später einmal eine Fahrerlaubnis beantragen oder die Polizei erneut Auffälligkeiten mitteilen sollte, die sodann – gegebenenfalls im Zusammenhang mit den zunächst nicht ausreichenden Informationen – die Einleitung eines entsprechenden Überprüfungsverfahrens rechtfertigen könnten.

Eine solche langfristige Speicherung ist mit dem Gesetz nicht vereinbar. Nach § 2 Abs. 12 Satz 2 StVG sind die Unterlagen „unverzüglich zu vernichten, soweit die mitgeteilte Information für die Beurteilung der Eignung oder Befähigung nicht erforderlich sind“. Die Vorschrift lässt ersichtlich keine Speicherung auf Vorrat zu, sondern ist an individuelle Erforderlichkeitsüberlegungen im konkreten Fall gebunden. Auch wenn es sich bei der Verkehrssicherheit um ein wichtiges und hohes Gut handelt, kann die Aufgabe der Fahrerlaubnisbehörden eine Speicherung teils sehr sensibler (etwa Gesundheits-)Daten über Bürgerinnen und Bürger nicht rechtfertigen.

Ich habe mich daher an das fachlich zuständige Innenministerium gewandt, das meine Feststellungen zum Anlass genommen hat, ein die Rechtslage bereits zutreffend würdigendes Rundschreiben aus dem Jahr 2001 zu aktualisieren und den Fahrerlaubnisbehörden erneut zur Kenntnis zu geben. Hiernach gelten für die gemäß § 2 Abs. 12 Satz 2 StVG notwendigen individuellen Erforderlichkeitsüberlegungen insbesondere folgende Maßstäbe:

— Wird gegen die Inhaberin oder den Inhaber einer Fahrerlaubnis angesichts der übermittelten Informationen kein Überprüfungsverfahren eingeleitet, so sind die Unterlagen im Grundsatz unverzüglich zu löschen.

— Besitzt die betroffene Person keine Fahrerlaubnis oder hat sie aktuell keine Erlaubnis beantragt, so sind die Daten ebenfalls grundsätzlich zu löschen.

  Eine Speicherung ist jedoch zulässig, wenn und solange mit einer Antragstellung nach den Umständen des Einzelfalls mit hoher Wahrscheinlichkeit und in absehbarer Zeit zu rechnen ist. Dies ist etwa dann der Fall, wenn der

betroffenen Person die Fahrerlaubnis entzogen wurde und die Sperrfrist noch nicht abgelaufen ist oder sie das Mindestalter für die Erteilung der Fahrerlaubnis noch nicht erreicht hat. Bei Betroffenen, die noch nicht das 16. Lebensjahr vollendet haben, ist eine Speicherung nur in besonders begründeten Einzelfällen zulässig. Spätestens ab Vollendung des 25. Lebensjahres sind die Unterlagen zu vernichten, wenn bis zu diesem Zeitpunkt kein Antrag auf Erlaubnis gestellt wurde.

— Für die Speicherung von Informationen, die den Behörden unaufgefordert von anderen öffentlichen Stellen oder Dritten mitgeteilt werden, gelten die Ausführungen grundsätzlich entsprechend.

14 Datenschutzkommission

Der Datenschutzkommission beim Bayerischen Landtag gehörten in den vergangenen zwei Jahren folgende Mitglieder und stellvertretende Mitglieder an:

Für den Landtag:

Mitglieder:

Eberhard Rotter, CSU
Max Gibis, CSU
Walter Nussel, CSU
Florian Ritter, SPD
Eva Gottstein, Freie Wähler
Verena Osgyan, BÜNDNIS 90/DIE GRÜNEN

Stellvertretende Mitglieder:

Tobias Reiß, CSU
Thorsten Schwab, CSU
Michael Brückner, CSU
Alexandra Hiersemann, SPD
Bernhard Pohl, Freie Wähler
Ulrike Gote, BÜNDNIS 90/DIE GRÜNEN

Auf Vorschlag der Staatsregierung:

Mitglied:

Friederike Sturm,
Ministerialrätin im Staatsministerium der Finanzen, für Landesentwicklung und Heimat bis zum 31. Januar 2016
Präsidentin der Staatlichen Lotterieverwaltung
ab dem 1. Februar 2016 bis zum 27. September 2016

Dr. Stephan Bobe, Ministerialrat im Staatsministerium der Finanzen, für Landesentwicklung und Heimat ab dem 28. September 2016

Stellvertretendes Mitglied:

Michael Will, Ministerialrat im Staatsministerium des Innern, für Bau und Verkehr

Auf Vorschlag der kommunalen Spitzenverbände in Bayern:

Mitglied:

Rudolf Schleyer, Mitglied des Vorstands der AKDB

Stellvertretendes Mitglied:

Gudrun Aschenbrenner, Abteilungsleiterin der AKDB

Auf Vorschlag des Staatsministeriums für Arbeit und Soziales, Familie und Integration aus dem Bereich der gesetzlichen Sozialversicherungsträger:

Mitglied:

Werner Krempl, Erster Direktor und Vorsitzender der Geschäftsführung der Deutschen Rentenversicherung Nordbayern

Stellvertretendes Mitglied:

Dr. Helmut Platzer, Vorstandsvorsitzender der AOK Bayern

Auf Vorschlag des Verbands Freier Berufe in Bayern e.V.:

Mitglied:

Dr. Till Schemmann, Notar

Stellvertretendes Mitglied:

Dr. Janusz Rat, Vorsitzender der Kassenzahnärztlichen Vereinigung Bayerns

Herr Eberhard Rotter, MdL, führt den Vorsitz in der Datenschutzkommission; stellvertretender Vorsitzender ist Herr Florian Ritter, MdL.

Die Datenschutzkommission beim Bayerischen Landtag tagte im vergangenen Berichtszeitraum fünf Mal. Dabei befasste sie sich unter anderem mit folgenden Themen:

- Vorberatung des 27. Tätigkeitsberichts 2016,
- Berichte über Beanstandungen,
- Berichte von Datenschutzkonferenzen,
- Vorratsdatenspeicherung,
- Videoüberwachung,
- Pläne der Europäischen Kommission zur Reform des europäischen Datenschutzrechts, insbesondere Berichte und Beratungen zur Datenschutz-Grundverordnung sowie zur Richtlinie über den Datenschutz der Strafjustiz.

15 Abbildungen

Zeichnungen:

Ferdinand Wedler
E-Mail: info@lineamentum.de
www.lineamentum.de

Anlage 1:
Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19.03.2015

Datenschutz nach „Charlie Hebdo“
Rechtsstaat und Grundrechte beweisen sich gerade in Zeiten terroristischer Bedrohung!

Terrorismus und internationale Kriminalität erfordern effektive Abwehrmaßnahmen auch in freiheitlichen Verfassungsstaaten. Für etwaige Defizite kann der Datenschutz nicht verantwortlich gemacht werden. Eine Zielrichtung terroristischer Angriffe ist es, Furcht und Hass in der Gesellschaft zu verbreiten und demokratische Freiheitsrechte zu beseitigen. Die Verteidigung und Bewahrung der verfassungsmäßigen Freiheitsrechte sind zentrale Grundbedingungen zur Abwehr der vom Terrorismus ausgehenden Gefahren.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt ihren nach den Terror-Anschlägen vom 11. September 2001 formulierten Appell, dass alle neu erwogenen Maßnahmen sich daran messen lassen müssen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus wirklich zielführend und erforderlich sind und ob sie den Verfassungsgrundsatz der Verhältnismäßigkeit einhalten. Weder die Vorratsdatenspeicherung noch die pauschale Übermittlung von Flugpassagierdaten erfüllen diese Voraussetzungen. Einseitiges Streben nach einer umfassenden Sicherheit darf nicht den bisherigen gesellschaftlichen Konsens über die wertsetzende Bedeutung bürgerlicher Freiheits- und Persönlichkeitsrechte überlagern. Es darf in unserem Land zu keiner Verschiebung zugunsten staatlicher Überwachung und zu Lasten freier und unbeobachteter Aktion, Bewegung und Kommunikation der Bürgerinnen und Bürger kommen. Der Datenschutz ist nicht ein Hindernis für Abwehrmaßnahmen, sondern selbst ein identitätsstiftendes Merkmal des Verfassungsstaates oder – mit den Worten des Bundesverfassungsgerichts – „elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens“. Ließe man jeden Eingriff in die informationelle Selbstbestimmung zu, hätten die Terroristen eines ihrer Ziele erreicht.

Anlage 2:
Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19.03.2015

Datenschutzgrundverordnung darf keine Mogelpackung werden!

Der Rat der Europäischen Innen- und Justizminister hat sich am 12. und 13. März 2015 erneut mit der Reform des Europäischen Datenschutzrechts befasst und dabei über drei weitere Kapitel der geplanten Datenschutz-Grundverordnung (DSGVO) grundsätzlich geeinigt. Hierzu gehören u. a. die zentralen Vorschriften über die Datenschutzgrundsätze und die Zulässigkeit der Verarbeitung personenbezogener Daten.

Die Datenschutzbeauftragten des Bundes und der Länder warnen eindringlich vor einer Aushöhlung des Datenschutzes in Europa durch eine Abkehr von den tragenden grundrechtlich vorgegebenen Datenschutzgrundsätzen. Die vom Rat nunmehr vorgeschlagene Fassung des Kapitels II der DSGVO hebelt zentrale Datenschutzgrundsätze aus:

— Der Rat verabschiedet sich mit seiner Einigung vom Grundsatz der Datensparsamkeit. Damit wird ein tragender Grundsatz des Rechts auf informationelle Selbstbestimmung aufgegeben, der die Datenverarbeitung auf das unbedingt notwendige Maß reduziert und einen Anreiz für datenschutzfreundliche Technologien darstellt.

— Nach den Vorstellungen des Rates sollen einerseits personenbezogene Daten ohne jede weitere Rechtsgrundlage zu anderen Zwecken als dem ursprünglichen Erhebungszweck verarbeitet werden dürfen, wenn der neue Zweck mit dem ursprünglichen Zweck noch vereinbar ist. Zweckänderungen sollen andererseits schon dann erlaubt sein, wenn der Datenverarbeiter hieran ein überwiegendes berechtigtes Interesse hat. Durch das Zusammenspiel dieser beiden Möglichkeiten und die ausdrücklich gewünschte Privilegierung der Datenverarbeitung zu Direktmarketingzwecken werden Zweckänderungen in einem derart weiten Umfang zulässig, dass das für den Datenschutz elementare Prinzip der Zweckbindung preisgegeben wird. Dies würde die Entscheidungsfreiheit und die Transparenz für den Einzelnen in problematischer Weise einschränken.

— Ferner wird in den Vorschlägen des Rates das Instrument der Einwilligung entwertet. In der Vergangenheit hat sich gezeigt, dass das bloße Unterlassen des Erhebens von Widersprüchen gegenüber der Datenverarbeitung (opt-out) eben nicht mit einer expliziten Willensbekundung (opt-in) gleichzusetzen ist. Der Vorschlag des Rates, „ausdrücklich“ zu streichen und durch den minder klaren Begriff „eindeutig“ zu ersetzen, ermöglicht es gerade den global agierenden Diensteanbietern, durch Verwendung pauschaler Datenschutzbestimmungen weitreichende Datenverarbeitungsbefugnisse ohne eine ausdrückliche Einwilligung des Nutzers für sich zu reklamieren. Mit diesem Vorschlag wird das informationelle Selbstbestimmungsrecht der Nutzer wesentlich geschwächt.

— Schließlich will der Rat die Verarbeitung personenbezogener Daten zu Forschungszwecken derart weitgehend privilegieren, dass ein angemessener Ausgleich mit dem Recht auf informationelle Selbstbestimmung der Betroffenen kaum noch möglich ist.

Mit diesen Vorschlägen fällt der Rat nicht nur hinter die Entwürfe der Europäischen Kommission und des Europäischen Parlaments zurück. Er ebnet dadurch den Weg zu einer Verschlechterung des derzeitigen Datenschutzniveaus, obwohl die Verbesserung des Datenschutzes eines der erklärten politischen Ziele der Reform ist.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher an Bund und Länder, den Rat, das Europäische Parlament und die Europäische Kommission, sich in den im zweiten Halbjahr 2015 anstehenden Trilogverhandlungen für eine Verbesserung des Datenschutzniveaus einzusetzen und eine Aushöhlung zentraler Datenschutzgrundsätze zu verhindern.

Anlage 3:
Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19.03.2015

IT-Sicherheitsgesetz nicht ohne Datenschutz!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht Informationssicherheit als eine Grundvoraussetzung an, um die Grundrechte auf informationelle Selbstbestimmung sowie auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme und das Telekommunikationsgeheimnis zu wahren.

Der von der Bundesregierung eingebrachte Gesetzentwurf für ein IT-Sicherheitsgesetz (BT-Drs. 18/4096 v. 25.02.2015) soll dazu beitragen, die Sicherheit informationstechnischer Systeme bei kritischen Infrastrukturen zu verbessern. Der Ausbau des Bundesamts für die Sicherheit in der Informationstechnik (BSI) zu einer nationalen Zentrale für Informationssicherheit, die Festlegung von Sicherheitsstandards, die Pflicht zur Sicherheitsvorsorge in Unternehmen sowie die Melde- und Benachrichtigungspflichten bei sicherheitsrelevanten Vorfällen sollen dabei wichtige Bausteine einer nationalen Strategie für mehr Informationssicherheit sein.

Datenschutz und Informationssicherheit haben weitreichende Schnittmengen, nehmen in einzelnen Bereichen jedoch unterschiedliche Gewichtungen vor. Bei einer Gesamtabwägung darf es nicht zu einer Unterordnung oder gar Missachtung der grundrechtlich verankerten Bestimmungen des Datenschutzrechts kommen. Auch um das Vertrauen der Bevölkerung in die Gesetzgebung zur IT-Sicherheit zu stärken, muss ein beiden Seiten gerecht werdender Abwägungs- und Abstimmungsprozess deutlich zum Ausdruck kommen. Dies gilt sowohl bei der Festlegung von Sicherheitsstandards, als auch bei der Beurteilung von Einzelfällen.

Wenn Maßnahmen zur Erhöhung der Informationssicherheit ergriffen werden, geht damit in vielen Fällen auch eine Verarbeitung personenbezogener Daten einher. Die damit verbundenen Eingriffe in das Recht auf informationelle Selbstbestimmung sowie in das Telekommunikationsgeheimnis müssen gesetzlich auf das unabdingbar Erforderliche beschränkt werden. Es muss im Gesetz klar geregelt sein, welche personenbezogenen Daten im Rahmen der IT-Sicherheitsmaßnahmen von wem für welche Zwecke erhoben, verarbeitet und gespeichert werden dürfen. Diesen Anforderungen genügt der vorliegende Entwurf nicht. So fehlen Regelungen, die verpflichteten Unternehmen Klarheit über die Notwendigkeit und Zulässigkeit bestimmter Angriffspräventions- und erkennungssysteme geben. Regeln zur Zweckbindung erhobener Daten sind nur für das BSI vorgesehen. Vorgaben zur Datensparsamkeit etwa durch Anonymisierung, Pseudonymisierung, frühzeitiges Löschen und Abschotten sind bei den vorgesehenen Maßnahmen zur Verbesserung der Informationssicherheit bisher nicht geplant.

Die Informationssicherheit darf nicht allein den Behörden im Direktionsbereich des Bundesministeriums des Innern überlassen bleiben, die bei einer Abwägung zwischen Informationssicherheit einerseits und klassischer Gefahrenabwehr und Strafverfolgung andererseits Interessenkonflikten ausgesetzt sein könnten. Die Beteiligung unabhängiger Datenschutzbehörden ist daher gefordert.

Neben der Zuständigkeit des BSI für die Informationssicherheit muss im Gesetzentwurf auch die Zuständigkeit der Datenschutzaufsichtsbehörden für Fragen der Geeignetheit und Angemessenheit der vom Datenschutzrecht geforderten technisch-organisatorischen Maßnahmen mit in den Blick genommen werden. Insofern sind die Datenschutzaufsichtsbehörden auch an der Festlegung von Informationssicherheitsstandards beteiligt und müssen daher in die Meldewege eingebunden und bei der Beratung der Beteiligten im Sinne des o.g. Abwägungsprozesses zwischen Informationssicherheits- und Datenschutzmaßnahmen beteiligt werden. Zudem kann mit der Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle an das BSI eine datenschutzrechtliche Meldeplicht von Datenpannen verbunden sein, woraus auch eine rechtliche Einbindung der Datenschutzaufsichtsbehörden in die Meldewege resultiert. Dies setzt unabhängige und leistungsfähige Datenschutzaufsichtsbehörden und deren entsprechende Ausstattung voraus.

Die Bestrebungen nach mehr IT-Sicherheit dürfen sich nicht allein auf die Verabschiedung eines IT-Sicherheitsgesetzes beschränken. Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme enthält einen objektiven Auftrag an den Staat, für vertrauenswürdige und sichere IT-Infrastrukturen zu sorgen. Dabei kommt der Weiterentwicklung und Implementierung von Verfahren eine zentrale Funktion zu, die gleichzeitig eine starke Verschlüsselung und eine effektive Erkennung von Sicherheitsvorfällen ermöglichen.

Anlage 4:
Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19.03.2015

Mindestlohngesetz und Datenschutz

Die Umsetzung des Mindestlohngesetzes wirft eine Reihe von datenschutzrechtlichen Problemen auf, die einer Klärung bedürfen.

Unter anderem haftet ein Unternehmen dafür, wenn ein Subunternehmer – und ggf. auch dessen Subunternehmer – den Beschäftigten nicht den Mindestlohn zahlt; außerdem kann ein hohes Bußgeld verhängt werden, wenn der Auftraggeber weiß oder fahrlässig nicht weiß, dass Auftragnehmer den Mindestlohn nicht zahlen. Da das Mindestlohngesetz nicht bestimmt, wie die Überprüfung durch den Auftraggeber konkret zu erfolgen hat, sichern sich – wie Industrie- und Handelskammern berichten – zahlreiche Unternehmen vertraglich durch umfangreiche Vorlagepflichten und Einsichtsrechte in Bezug auf personenbezogene Beschäftigtendaten beim Subunternehmer (z. B. Lohnlisten, Verdienstbescheinigungen usw.) ab. Dies ist in Anbetracht der schutzwürdigen Interessen der Beschäftigten weder datenschutzrechtlich gerechtfertigt noch im Hinblick auf die soziale Zielrichtung des Mindestlohngesetzes erforderlich.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, bei der in Aussicht genommenen Überprüfung des Mindestlohngesetzes stärker auf die Belange des Datenschutzes zu achten. Auch im Interesse einer unbürokratischen Lösung sollte der Gesetzgeber klarstellen, dass eine schriftliche Erklärung des Auftragnehmers ausreicht, um die Voraussetzungen des Mindestlohngesetzes einzuhalten. Dies kann eventuell durch Vertragsstrafenregelungen, Übernahme des Haftungsrisikos durch Bankbürgschaf-

ten sowie vertragliche Zustimmungsvorbehalte für den Fall der Beauftragung weiterer Subunternehmer durch den Auftragnehmer abgesichert werden. Aus Datenschutzsicht sind allenfalls stichprobenartige Kontrollen von geschwärzten Verdienstbescheinigungen hinnehmbar. Bei einer Novellierung des Gesetzes, sollte der Gesetzgeber darüber hinaus klarstellen, dass Zugriffe des Auftraggebers auf personenbezogene Beschäftigtendaten des Auftragnehmers unzulässig sind.

Anlage 5:
Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19.03.2015

Safe Harbor bietet keinen ausreichenden Schutz für den Datentransfer in die USA

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Safe Harbor-Entscheidung der Europäischen Kommission aus dem Jahr 2000 keinen ausreichenden Schutz für das Grundrecht auf Datenschutz bei der Übermittlung personenbezogener Daten in die USA entfaltet.

Im Jahr 2010 haben die deutschen Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich bereits ausgeführt, dass die Erklärung über eine Selbst-Zertifizierung, wie sie die Safe Harbor-Grundsätze vorsehen, für Datenübermittlungen in die USA nicht ausreicht. Sie wiesen darauf hin, dass sich übermittelnde Unternehmen von den Datenempfängern nachweisen lassen müssen, dass die Safe Harbor-Grundsätze auch eingehalten werden. Mit den Enthüllungen von Edward Snowden wurde offengelegt, dass US-Sicherheitsbehörden systematisch und massenhaft auf in die USA übermittelte personenbezogene Daten zugreifen, und damit die Safe Harbor-Grundsätze mit großer Wahrscheinlichkeit gravierend verletzt werden.

Die Konferenz weist darauf hin, dass bei Übermittlungen in einen Staat, in dem europäisches Datenschutzrecht nicht direkt anwendbar ist, zumindest folgende Garantien für den Datenschutz gegeben sein müssen: Die Zweckbindung der Daten ist grundsätzlich sicherzustellen. Staatliche Zugriffsmöglichkeiten müssen auf ein angemessenes und grundrechtskonformes Maß begrenzt bleiben. Den Betroffenen ist ein effektiver Anspruch auf Auskunft und auf Berichtigung bzw. Löschung falscher bzw. unzulässig gespeicherter Daten zu gewähren. Bei Verstößen bedarf es eines effektiven Rechtsschutzes. Formelle und sprachliche Barrieren dürfen nicht dazu führen, dass die Betroffenen ihre Rechte nicht wahrnehmen können.

Anlage 6:
Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18./19.03.2015

Verschlüsselung ohne Einschränkungen ermöglichen

Zur Stärkung des Brief-, Post- und Fernmeldegeheimnisses und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie im Interesse der ungestörten Kommunikation in Wirtschaft und Verwaltung sind neben entsprechenden gesetzlichen Regelungen und deren Um-

setzung wirksame technische Vorkehrungen erforderlich, um elektronisch übermittelte und gespeicherte Daten vor Zugriffen Unberechtigter zu schützen. Schutzbedürftig sind neben der Kommunikation von Privatpersonen auch die geschäftliche Kommunikation von Wirtschaftsunternehmen, die Kommunikation von Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen (z. B. Ärzte, Anwälte, Psychologen, Steuerberater), und die Kommunikation mit und innerhalb der öffentlichen Verwaltung.

Mit modernen kryptographischen Verfahren zur Verschlüsselung von Daten stehen datenschutzfreundliche Technologien zur Verfügung, die prinzipiell von jedermann genutzt werden können. Einer umfassenden und leicht nutzbaren Verschlüsselung stehen jedoch noch technische und organisatorische Hürden entgegen. Dies führt dazu, dass diese Schutzmaßnahmen bisher viel zu selten genutzt werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher,

— eine einfach bedienbare Verschlüsselungs-Infrastruktur und insbesondere eine sichere Ende-zu-Ende-Verschlüsselung ohne Eingriffsmöglichkeiten Dritter bereitzustellen,

— die Entwicklung sicherer, transparenter und einfach bedienbarer kryptographischer Verfahren ohne Hintertüren auf allen, insbesondere auch mobilen Plattformen zu fördern,

— die Wirtschaft bei der Wahrung der Vertraulichkeit und Integrität ihrer geschäftlichen Kommunikation zu unterstützen und

— kryptographische Technologien in E Government-Verfahren standardmäßig zu implementieren

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert einen aktiven Einsatz der Politik bei der Gestaltung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Die Bundesregierung hat in ihren eigenen Zielstellungen aus der Digitalen Agenda 2014-2017 deutlich gemacht, wie wichtig eine zuverlässige und sichere Verschlüsselung ist. Die Pläne der De-Mail-Anbieter für eine Ende-zu-Ende-Verschlüsselung ab April 2015 sind zwar ein erster Schritt in die richtige Richtung. Dennoch wird im Zusammenhang mit der Bekämpfung des internationalen Terrorismus in letzter Zeit erneut über eine Schwächung von Verschlüsselungstechnologien diskutiert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt Forderungen ab, den Einsatz kryptographischer Verfahren durch staatliche Regulierungen zu unterbinden oder zumindest einzuschränken. Solche Regulierungen könnten leicht umgangen werden, wären kaum kontrollierbar, würden Grundrechte einschränken, den Schutz von Berufs- und Geschäftsgeheimnissen gefährden und Schwachstellen schaffen, die auch von Kriminellen ausgenutzt werden können. Im Ergebnis wäre dann der erhoffte Nutzen bei der Bekämpfung des internationalen Terrorismus äußerst fraglich.

Anlage 7:
Entschließung der 90. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 30.09./01.10.2015

Cloud-unterstützte Betriebssysteme bergen Datenschutzrisiken

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

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

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

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

Den Benutzern der neuen Betriebssysteme empfehlen die Datenschutzbeauftragten von Bund und Ländern, sich möglichst schon vor dem Kauf detailliert über die Funktionsweise zu informieren und alle Möglichkeiten der datenschutzfreundlichen Einstellungen der Betriebssysteme zu nutzen. Insbesondere die Verantwortlichen im behördlichen und kommerziellen Umfeld sind angehalten vor der Entscheidung für einen Einsatz zu prüfen, ob für ihr Umfeld zugeschnittene Be-

triebssystemversionen verfügbar sind und ob sie bei der Nutzung der neuen Betriebssysteme ihrer datenschutzrechtlichen Verantwortung als Daten verarbeitende Stelle gerecht werden können.

Anlage 8:
Entschließung der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder am 06./07.04.2016

Wahrung der Freiheits- und Persönlichkeitsrechte bei der Bekämpfung des internationalen Terrorismus

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

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

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

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

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

*)

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

Anlage 9:
Entschließung Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 25.05.2016

EU-Datenschutz-Grundverordnung erfordert zusätzliche Ressourcen für Datenschutzbehörden!

(Enthaltung: Bayern)

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

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

— Bearbeitung von Beschwerden und Beratung Betroffener sowie datenschutzrechtliche Beratung und Kontrolle von Unternehmen nunmehr unter Beachtung des erweiterten räumlichen Anwendungsbereichs der Verordnung (Marktortprinzip),

— verpflichtende Beratung von Behörden und Unternehmen bei der Datenschutz-Folgenabschätzung, insbesondere im Rahmen der vorherigen Konsultation der Aufsichtsbehörde, sowie Beratung bei der Umsetzung neuer Anforderungen wie Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen (Privacy By Design, Privacy By Default),

— Aufbau und Anwendung eines Kooperationsverfahrens zwischen Datenschutzbehörden in Europa bei grenzüberschreitenden Datenverarbeitungen (One-Stop-Shop), Verpflichtung zur gegenseitigen Amtshilfe und umfassender Austausch von Informationen zwischen federführenden und betroffenen Aufsichtsbehörden jeweils mit kurzen Bearbeitungsfristen,

— Etablierung eines Kohärenzverfahrens zwischen den Datenschutzbehörden in Europa zur Gewährleistung der europaweit einheitlichen Anwendung der Verordnung, Mitwirkung im Europäischen Datenschutzausschuss,

— europaweit einheitliche Auslegung der Grundverordnung in Bezug auf fehlende Regelungen (z. B. zur Videoüberwachung oder zum Scoring) und neue Anforderungen (z. B. Recht auf transparente Information oder Recht auf Datenübertragbarkeit),

- Erarbeitung von Stellungnahmen und Billigung von branchenspezifischen Verhaltensregeln zur ordnungsgemäßen Anwendung der Verordnung, Erarbeitung von Zertifizierungskriterien, ggf. Durchführung von Zertifizierungen, Erarbeitung von Kriterien für die Akkreditierung von Zertifizierungsstellen, ggf. Durchführung der Akkreditierung,

- Bearbeitung von gerichtlichen Rechtsbehelfen Betroffener gegen Entscheidungen von Aufsichtsbehörden,

- Ausübung neuer bzw. erweiterter Befugnisse der Datenschutzbehörden zur Erteilung von Anordnungen gegenüber den Verantwortlichen nunmehr auch im öffentlichen Bereich sowie Berücksichtigung zusätzlicher Tatbestände für Ordnungswidrigkeiten und eines erweiterten Bußgeldrahmens.

Die Europäische Datenschutz-Grundverordnung verpflichtet die Mitgliedstaaten, die Aufsichtsbehörden zur Gewährleistung ihrer Unabhängigkeit mit den erforderlichen personellen, finanziellen und technischen Ressourcen auszustatten (Art. 52 Abs. 4 DSGVO). Aus Sicht der Datenschutzkonferenz ist es für die Bewältigung der neuen Aufgaben zwingend erforderlich, für die Datenschutzbehörden in Deutschland erweiterte personelle und finanzielle Ressourcen vorzusehen. Dies gilt bereits für die jetzt laufende Vorbereitungsphase, in der die Weichen für eine funktionierende Umsetzung der Datenschutz-Grundverordnung gestellt werden. Die Konferenz appelliert deshalb an die Gesetzgeber in Bund und Ländern, rechtzeitig die haushaltsrechtlichen Vorkehrungen für eine jeweils angemessene, erweiterte Ausstattung der Datenschutzbehörden zu treffen. Nur so lassen sich die zusätzlichen Aufgaben der Datenschutz-Grundverordnung von den Datenschutzbehörden in Deutschland effektiv wahrnehmen.

Anlage 10:
Entschließung der 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 09.11.2016

„Videoüberwachungsverbesserungsgesetz“ zurückziehen!

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

Gleichwohl lässt es die einschlägige Bestimmung des § 6b BDSG bereits gegenwärtig zu, die Sicherheitsbelange von Personen, die sich in öffentlich zugänglichen Bereichen aufhalten, bei der Abwägung zwischen den Rechten Betroffener und den Betreiberinteressen zu berücksichtigen. Im Rahmen der Hausrechtsausübung können auch heute Kameras installiert werden, um Personen von Straftaten an den Objekten abzuhalten. Darüber hinaus kann Videotechnik zur Beweissicherung eingesetzt werden und nach § 6 Abs. 3 Satz 2 BDSG können Videobilder an Polizei-, Ordnungs- und Strafverfolgungs- und Ordnungsbehörden weitergegeben werden, wenn dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist. Die Begründung des BMI suggeriert, die Datenschutzaufsichtsbehörden verhinderten angesichts der angespannten Sicherheitslage die Durchführung von Videoüberwachung. Dies trifft nicht zu. Tatsächlich werden gerade im Bereich der großen Einkaufszentren, aber auch an Bahnhöfen und in Fahrzeugen des Personennahverkehrs bereits heute zahlreiche Kameras mit ausdrücklicher Billigung der Aufsichtsbehörden betrieben.

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

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

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

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

Abkürzungsverzeichnis

a.a.O.	am angegebenen Ort
a.F.	alte Fassung
Abs.	Absatz
AEAO	Anwendungserlass zur Abgabenordnung
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AGBGB	Gesetz zur Ausführung des Bürgerlichen Gesetzbuchs und anderer Gesetze
AGO	Allgemeine Geschäftsordnung für die Behörden des Freistaats Bayern
AKDB	Anstalt für Kommunale Datenverarbeitung in Bayern
AMRabG	Gesetz über Rabatte für Arzneimittel
Anm.	Anmerkung
AO	Abgabenordnung
App	Application, Anwendungsprogramm auf Smartphone
ArbZG	Arbeitszeitgesetz
Archivierungsvereinbarung	Archivierungsvereinbarung im Hinblick auf die Aussonderung von Schülerunterlagen
Art.	Artikel
AsylG	Asylgesetz
ATDG	Antiterrordateigesetz
Az.	Aktenzeichen
AzV	Verordnung über die Arbeitszeit für den bayerischen öffentlichen Dienst
BAMF	Bundesamt für Migration und Flüchtlinge
BayAGBMG	Bayerisches Gesetz zur Ausführung des Bundesmeldegesetzes
BayArchivG	Bayerisches Archivgesetz
BayBG	Bayerisches Beamtengesetz
BayBIS	Bayerisches Behördeninformationssystem
BayBITV	Bayerische Verordnung zur Schaffung barrierefreier Informationstechnik
BayBO	Bayerische Bauordnung
BayDSG	Bayerisches Datenschutzgesetz
BayEGovG	Bayerisches E-Government-Gesetz
BayEUG	Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen
BayGlG	Bayerisches Gleichstellungsgesetz
BayKRegG-E	Entwurf eines Bayerischen Krebsregistergesetzes
BayKrG	Bayerisches Krankenhausgesetz
BayPVG	Bayerisches Personalvertretungsgesetz
BayRS	Bayerische Rechtssammlung
BaySchO	Schulordnung für schulartübergreifende Regelungen an Schulen in Bayern
BayStVollzG	Bayerisches Strafvollzugsgesetz
BayVGH	Bayerischer Verwaltungsgerichtshof
BayVSG	Bayerisches Verfassungsschutzgesetz
BayVwVfG	Bayerisches Verwaltungsverfahrensgesetz
Bcc	Blind Carbon Copy

BDSG	Bundesdatenschutzgesetz
BeamtStG	Beamtenstatusgesetz
BEM	Betriebliches Eingliederungsmanagement
BfDI	Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BfV	Bundesamt für Verfassungsschutz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BImSchG	Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche Vorgänge
BIMSchV	Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtsgesetz
BMG	Bundesmeldegesetz
BND	Bundesnachrichtendienst
BNotO	Bundesnotarordnung
BOÄ	Berufsordnung für die Ärzte Bayerns
BR-Drs.	Bundesrats-Drucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestagsdrucksache
Buchst.	Buchstabe
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts (zitiert nach Band und Seite)
bzw.	beziehungsweise
ca.	circa
Cc	Carbon Copy
CPT	European Comitee for the Prevention of Torture an Inhuman or Degrading Treatment or Punishment
CSU	Christlich-Soziale Union in Bayern
d.h.	das heißt
DolmG	Gesetz über die öffentliche Bestellung und allgemeine Beeidigung von Dolmetschern und Übersetzern (Dolmetschergesetz)
DolmGABek	Bekanntmachung des Bayerischen Staatsministeriums der Justiz und für Verbraucherschutz zur Ausführung des Dolmetschergesetzes (Dolmetschergesetzausführungsbekanntmachung vom 11. März 2010)
Doppelbuchst.	Doppelbuchstabe
DRiG	Deutsches Richtergesetz
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG – Datenschutz-Grundverordnung
Durchführungshinweise	Durchführungshinweise zum Umgang mit Schülerunterlagen
DVBayDSG-KM	Verordnung zur Durchführung des Art. 28 Abs. 2 des Bayerischen Datenschutzgesetzes

e.V.	eingetragener Verein
EASy	Ermittlungs- und Analyseunterstützendes EDV-System
ED-Daten	Erkennungsdienstliche Daten
ED-DI	Erkennungsdienst Digital
EDV	Elektronische Datenverarbeitung
EFZG	Entgeltfortzahlungsgesetz
EG	Europäische Gemeinschaft
EGovG	E-Government-Gesetz
E-Government	Elektronische Verwaltung
eID	eletronic Identity
E-Learning	elektronisch unterstütztes Lernen
ELSTER	Elektronische Steuererklärung
E-Mail	Elektronische Post
EStG	Einkommensteuergesetz
EStR	Einkommenssteuer-Richtlinien
EU	Europäische Union
EuGH	Europäischer Gerichtshof
FDR	Falldatei Rauschgift
FeV	Fahrerlaubnis-Verordnung
ff.	fortfolgende
FMBl.	Amtsblatt des Bayerischen Staatsministeriums der Finanzen, für Landesentwicklung und Heimat
FQA	Fachstellen für Pflege und Behinderteneinrichtungen – Qualitätsentwicklung und Aufsicht
GBA	Generalbundesanwalt
GDVG	Gesundheitsdienst- und Verbraucherschutzgesetz
GESiK	Gesundheits- und Entwicklungsscreening im Kindergartenalter
GETZ	Gemeinsames Extremismus- und Terrorismusabwehrzentrum
GewO	Gewerbeordnung
GEZ	Gebühreneinzugszentrale
GG	Grundgesetz
GKV	Entwurf eines Gesetzes zur Stärkung der Versorgung in der gesetzlichen Krankenversicherung
GmbH	Gesellschaft mit beschränkter Haftung
GO	Gemeindeordnung für den Freistaat Bayern
GPS	Global Positioning System
GTAZ	Gemeinsames Terrorismusabwehrzentrum
GVBl.	Bayerisches Gesetz- und Verordnungsblatt
GVG	Gerichtsverfassungsgesetz
HIV	Humane Immundefizienz-Virus
https	Hyper Text Transfer Protocol Secure
i.V.m.	in Verbindung mit
IFG	Informationsfreiheitsgesetz
IfSG	Infektionsschutzgesetz
IGVP	Integrationsverfahren der Bayerischen Polizei
IHKG	Industrie- und Handelskammergesetz
IMS	Rundschreiben des Staatsministeriums des Innern, für Bau und Verkehr
INPOL	Informationssystem der Polizei (bundesweit)
IP	Internetprotokoll

ISDN	Integrated Services Digital Network
IT	Informationstechnik
JAVollzO	Jugendarrestvollzugsordnung
JGG	Jugendgerichtsgesetz
JVA	Justizvollzugsanstalt
KAG	Kommunalabgabengesetz
KAN	Kriminalaktennachweis
Kfz	Kraftfahrzeug
KWMBl.	Amtsblatt des Bayerischen Staatsministeriums für Bildung und Kultus, Wissenschaft und Kunst
LfV	Landesamt für Verfassungsschutz
LGL	Bayerisches Landesamt für Gesundheit und Lebensmittelsicherheit
LKA	Landeskriminalamt
LlbG	Leistungslaufbahngesetz
MAD	Militärischer Abschirmdienst
MDK	Medizinischer Dienst der Krankenversicherung in Bayern
MdL	Mitglied des Landtages
MeldDV	Meldedatenverordnung
MeldeG	Meldegesetz
MGOGR	Mustergeschäftsordnung für den Gemeinderat-Marktgemeinderat-Stadtrat
MiStra	Anordnung über Mitteilungen in Strafsachen
n.F.	neue Fassung
NADA	Nationale Doping Agentur Deutschland
NADIS	Nachrichtendienstliches Informationssystem
NAKO	Nationale Kohorte
Nr.	Nummer
NSA	National Security Agency
NSU	Nationalsozialistischer Untergrund
o.ä.	oder ähnliches
o.g.	oben genannt
PAG	Polizeiaufgabengesetz
PAuswG	Personalausweisgesetz
PC	Personalcomputer
PfleWoqG	Pflege- und Wohnqualitätsgesetzes
PFS	Perfect Forward Secrecy
PIAV	Polizeilicher Informations- und Analyseverbund
PIN	Personell Identification Number
QR	Quick Response
RiJAVollzO	Richtlinie zur Jugendarrestvollzugsordnung
RiStBV	Richtlinien für das Straf- und Bußgeldverfahren
RL	Richtline
RLDSJ	JI-Richtlinie (Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI)
Rn.	Randnummer

S/MIME	Secure/Mulitpurpose Internet Mail Extensions
SGB I	Sozialgesetzbuch Erstes Buch – Allgemeiner Teil
SGB II	Sozialgesetzbuch Zweites Bauch – Grundsicherung für Arbeitssuchende
SGB V	Sozialgesetzbuch Fünftes Buch – Gesetzliche Krankenversicherung
SGB VIII	Sozialgesetzbuch Achtes Buch – Kinder- und Jugendhilfe
SGB IX	Sozialgesetzbuch Neuntes Buch – Rehabilitation und Teilhabe behinderter Menschen
SGB X	Sozialgesetzbuch Zehntes Buch – Sozialverwaltungsverfahren und Sozialdatenschutz
SMS	Short Message Service
sog.	sogenannt
SPD	Sozialdemokratische Partei Deutschlands
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
TK	Telekommunikation
TKBek	Bekanntmachung über die Errichtung und Benutzung dienstlicher Telekommunikationsanlagen
TLS	Transportlayer Security
TMF	Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V.
TMG	Telemediengesetz
TMSI	Temporary Mobile Subscriber Identity
TV-L	Tarifvertrag für den öffentlichen Dienst der Länder
TVöD	Tarifvertrag für den öffentlichen Dienst
u.a.	unter anderem/und andere(s)
UrlV	Verordnung über den Urlaub der bayerischen Beamten und Richter
USB	Universal Serial Bus
UPD	Unabhängige Patientenberatung Deutschland
User-ID	User Identifier – Benutzerkennung
UStDV	Umsatzsteuer-Durchführungsverordnung
UStG	Umsatzsteuergesetz
usw.	und so weiter
vgl.	vergleiche
VV-BeamtR	Verwaltungsvorschriften zum Beamtenrecht
VwZG	Verwaltungszustellungsgesetz
www	World Wide Web
z.B.	zum Beispiel
ZBFS	Zentrum Bayern Familie und Soziales
ZKA	Zollkriminalamt

Stichwortverzeichnis

Abschottungsgebot
Statistikstelle ... 34
Akteneinsicht ... 168, 270
Personalakte ... 251
Schülerunterlagen ... 194
Allgemeines Auskunftsrecht ... 26, 270
Amtsermittlung
Umfang ... 281
Amtshilfe ... 161
Anlagengenehmigung
Anfordern sensibler Daten ... 281
Anmeldebestätigung ... 162
Meldebehörde ... 162
Anmeldung
Kindertageseinrichtung ... 175
Anschlussrehabilitation ... 152
Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) ... 29, 265
Melderegisterauskunft ... 124
Anti-Doping-Gesetz ... 85
Antragstellung
Sozialleistung ... 164
Anzeigeerstatter
Auskunftserteilung ... 121
App ... 41
Datenschutzerklärung ... 41
Datenschutzrechtliche Freigabe ... 41
Eingebundene Dienste Dritter ... 41
Freigabepflicht ... 41
Impressum ... 41
Prüfung ... 39
Verschlüsselung der Übertragung ... 41
Zugriffsrecht ... 41
Arbeitsunfähigkeitsbescheinigung
Entgegennahme ... 243
Arbeitsvertrag ... 162
Archiv
Anbietung ... 175
Digitalisierung von Personenstandsdaten ... 104
Archivierung
Audioaufzeichnungen von Stadtratssitzungen ... 118
Archivierungsvereinbarung
Schülerunterlagen ... 194
Arzneimittelrabatt
Bei der beamtenrechtlichen Beihilfe ... 246
Arzneimittelverordnung
Aufbewahrung bei den Beihilfestellen ... 246
Asylbewerber ... 130, 132, 136
Flüchtling ... 130, 134

Asylbewerberleistungsgesetz
Datenübermittlung 136
Asylgesetz 136
Asylsozialberatung 134
Asylsuchende 130, 132, 134
Aufbewahrung
Schülerunterlagen 194
Sozialdaten 174
Aufenthaltsgesetz 136
Aufnahmeeinrichtung 133
Gemeinschaftsunterkunft 130
Auftragsdatenverarbeitung
Externer Dienstleister 144
Krankenhaus 40
Sozialbehörde 172
Auftragsdatenverarbeitung plus
Patientengeheimnis 174
Auskunft 146
Behandlungsunterlagen 146
Auskunftsanspruch 170, 270
Kostenfreiheit 146
Auskunftsantrag 73
Bearbeitungsdauer 71
Auskunftssperre 124
Ausländer 133, 134
Aussonderung
Schülerunterlagen 194
Ausstellung Datenschutz 27
Baugenehmigungsverfahren
Nachbar 123
Bauherrendaten
Bekanntgabe in öffentlicher Gemeinderatssitzung 116
Baukosten
Baugenehmigungsverfahren 123
Bayerische Landesstelle für den Schulsport 217
Bayerische Schulordnung
Schülerunterlagen 194
Bayerischer Rundfunk
Übermittlung von Meldedaten 126
Bayerisches Behördeninformationssystem (BayBIS) 153
Bayerisches Verfassungsschutzgesetz (BayVSG) 73
BayernPortal 168, 265
BCC-E-Mail 32
Beamte
Entgegennahme von Dienstunfähigkeitsbescheinigungen 243
Beanstandung 48, 153, 156
Bedienstetenfoto
Intranet 242
Personalnachrichten 242
Begutachtender Arzt 160
Behandlungsunterlagen 149
Auskunft 146

Behördlicher Datenschutzbeauftragter ... 155
Beurteilung ... 255
Zweckvereinbarung ... 109
Beihilfe
Arzneimittelrabatte ... 246
Beihilfestelle
Aufbewahrung von Arzneimittelverordnung ... 246
Beitragsermittlung ... 154
Beitragsservice von ARD, ZDF und des Deutschlandradios
Übermittlung von Meldedaten ... 126
Bekanntgabe
Steuerbescheid ... 182
Bekanntmachung
Einstellung in das Internet ... 118
Benachrichtigungspflicht ... 73
Benachteiligungsverbot
Beurteilung behördlicher Datenschutzbeauftragter ... 255
Beratungsstelle
Dienstliche Telekommunikationsanlage ... 226
Berechtigungskonzept
Krankenhaus ... 38
Berufsgeheimnisträger
Verkehrsdatenerfassung ... 73
Beschränkte Steuerpflicht
Schweiz ... 182
Besondere Arten personenbezogener Daten ... 158
Besondere Versorgung
Integrierte Versorgung ... 153
Betreuer ... 156
Betriebliches Eingliederungsmanagement(BEM) ... 234
Beurteilung
Behördlicher Datenschutzbeauftragter ... 255
Briefüberwachung ... 98
Broschüre ... 27
Bundesamt für Migration und Flüchtlinge ... 136
Bundesmantelvertrag Ärzte ... 152
Bundesmeldegesetz
Anmeldebestätigung ... 161
Melderegisterauskunft ... 124
Übermittlung von Meldedaten ... 126
Bürgerbegehren
Nutzung der Unterschriften ... 113
Unterschriftenliste ... 113
Zweckbindung ... 113
Bürgerkonto ... 265
Bürgerservice-Portal ... 265
Cloud Computing ... 278
Cookie ... 267
Datenminimierung ... 17, 262
Datenschutzbeauftragter
Benachteiligungsverbot bei dienstlicher Beurteilung ... 255
Beurteilung ... 255
Finanzamt ... 177
Gemeinsamer behördlicher ... 109

Datenschutz-Grundverordnung(DSGVO) 14
Datenübermittlung
Asylbewerber 136
Industrie- und Handelskammern 279
Meldebehörde 126
De-Mail 265
Detektiv
Sozialbehörde 164
Dienstaufsicht
Ortungssystem in Dienstfahrzeug 237
Dienstfahrzeug
GPS 237
Ortungssystem 237
Dienstleister siehe Auftragsdatenverarbeitung 145
Dienstliche Beurteilung
Behördlicher Datenschutzbeauftragter 255
Benachteiligungsverbot 255
Dienstunfähigkeitsbescheinigung
Entgegennahme 243
Dienstverhältnis höherer Art 172
Digitales Lernen Bayern 202
Digitalisierung
Personenstandsdaten 104
Dokumentation 155
Dokumentenmanagementsystem 76
Dolmetscher
Aufnahmeeinrichtung für Asylsuchende 132
Drive-by-exploits 30
Durchsuchungsmaßnahme 79
E-Government 26
Gesetz 262
Ehrenamtliche
Helferkreis 134
Jugendhilfe 176
eID 262
Eingaben
Schwärzung personenbezogener Daten 119
Einkommenssituation 163
Einkommensteuer
Photovoltaikanlage 189
Einkommensteuerbescheid 154
Einsichtnahme
Schülerunterlagen 194
Einwilligung 156
Asylbewerber 136
Bedienstetenfoto im Intranet 242
Krankenhaus 147
Mitarbeiterfoto im Intranet 242
Ortungssystem in Dienstfahrzeug 237
Schule 202, 211, 217
Einwilligungserklärung 151, 153, 154, 161
Asylbewerber 136
pauschal 137

E-Learning
Schule ... 202
Elektronische Schließanlage ... 229
Elektronische Steuererklärung ... 189
Elektronische Zeiterfassung
Zugriff durch Personalrat ... 257
elektronisches Urkundenarchiv ... 84
ELSTER
Photovoltaikanlage ... 189
E-Mail
Auftragsdatenverarbeitung ... 44
Blind-Copy-Funktion ... 32
Sozialbehörde ... 167
Spam-Filter ... 44
STARTTLS ... 44
Entlassmanagement ... 152
Entsorgungskonzept
Krankenhaus ... 40
E-Postbrief ... 33
Erkennungsdienst Digital (ED-DI) ... 63
Erkennungsdienstliche Maßnahme ... 54, 63, 67
Europäischer Datenschutzausschuss ... 18
EU-US Privacy Shield ... 19, 275
Facebook ... 21, 268
Fachstellen für Pflege und Behinderteneinrichtungen – Qualitätsentwicklung und Aufsicht (FQAs) ... 157
Fahrerlaubnis
Zweifel an Eignung und Befähigung ... 283
Fahrerlaubnisbehörde ... 69
Datenübermittlung durch die Polizei ... 283
Speicherung von Daten ... 283
Falldatei Rauschgift (FDR) ... 65
Familienfeier
Finanzamt ... 186
Fanpage ... 268
Fax ... 167
Finanzamt
Datenschutzbeauftragter ... 177
Familienfeier ... 186
Gaststättenrechnung ... 186
Geschäftsessen ... 186
Restaurantrechnung ... 186
Zugriffskontrolle ... 177
Flüchtling ... 130, 133, 136
Asylbewerber ... 130
Formular ... 157, 163, 164
Forschung ... 153
forumSTAR-Straf ... 94
Foto
Intranet ... 242
Freigabe
datenschutzrechtlich ... 29
Elektronische Schließanlage ... 229
Kommune ... 29

Ortungssystem in Dienstfahrzeug ... 237
staatliches Verfahren ... 29
Freiheitsentziehungsbuch ... 54
Führungszeugnis
erweitertes ... 176
Funktionsübertragung
Sozialbehörde ... 174
Funkzellenabfrage ... 90
Gas- und Stromliefervertrag ... 163
Gaststättenrechnung
Finanzamt ... 186
Gemeinde
Sitzungsvorlage (eingescannt) im WWW ... 114
Gemeinderat
Einrichtung einer Mediathek von Sitzungsaufzeichnungen ... 116
Einsicht in Personalakten ... 251
E-Mail-Adresse ... 36
Personalreferent ... 251
Gemeinsamer behördlicher Datenschutzbeauftragter ... 109
Gemeinsames Extremismus- und Terrorismusabwehrzentrum (GETZ) ... 78
Gemeinsames Terrorismus Abwehrzentrum (GTAZ) ... 70, 78
Gemeinschaftsunterkunft ... 133
Geschäftsessen
Finanzamt ... 186
Geschwindigkeitsanzeigetafel ... 112
Gesetz über Rabatte für Arzneimittel
Beamtenrechtliche Beihilfe ... 246
Gesetzliche Krankenversicherung ... 151
Gesprächsaufzeichnung
TKBek ... 226
Gesundheitsakte
Gefangene ... 86
Gesundheitsamt ... 142
Impfberatung ... 141
Schuleingangsuntersuchung ... 141
Gesundheitsdaten
Weitergabe an Polizei ... 142
Gesundheitsdatenzentrum ... 147
Gesundheitsuntersuchung ... 133
Gewahrsam
Krankenhaus ... 145
Gewinnspiel
Krankenkasse ... 153
GPS
Dienstfahrzeug ... 237
Grundrecht auf Vertraulichkeit von Abstammungsinformationen
Digitalisierung von Personenstandsregistern ... 104
Hausrecht
Elektronische Schließanlage ... 229
Helferkreis
Asylbewerber ... 134
Hinweise ... 159
Hochschule
Immatrikulation ... 47

Homepage
Landesstelle für den Schulsport ... 217
Hundehaltung ... 120
Hybridbrief ... 33
Immatrikulationsbescheinigung
online ... 47
Immissionsschutzrechtliche Anlagengenehmigung
Erhebung von Kundendaten ... 281
Impfberatung ... 141
Impfnachweis ... 141
Industrie- und Handelskammern
Datenübermittlung ... 279
Infektionsschutzgesetz ... 142
Information ... 161
Informationelle Selbstbestimmung ... 52, 84, 85, 108, 137, 164, 168, 170, 196, 203, 229, 230
Digitalisierung von Personenstandsregistern ... 104
Informationelles Trennungsgebot ... 79
Informationelles Trennungsprinzip ... 73
Informationsanspruch
Personalrat ... 257
Informationsfreiheit
Recht auf Auskunft ... 270
Informationsfreiheitsgesetz ... 270
Informationsfreiheitssatzung
Verhältnis zu Recht auf Auskunft ... 270
Informationsmaterial ... 27
Informationsstand ... 27
Informationssystem Polizei (INPOL) ... 59
Integrationsverfahren der Bayerischen Polizei (IGVP) ... 59
Kurzsachverhalt ... 63
Internet
Recherche ... 164
Tracking ... 267
Intranet
Bedienstetenfoto ... 242
Mitarbeiterfoto ... 242
Jahresbericht
Schulische Videoaufnahmen ... 206
Jobcenter ... 89
Jugendarrestanstalt ... 96
Kameraattrappe ... 101
Kernbereichsschutz ... 73
Kfz-Haftpflichtversicherungsvertrag ... 163
Kinder ... 143
Kindertageseinrichtung
Kindergarten ... 175
Klassenfoto ... 211
Kommunale Zusammenarbeit
Gemeinsamer behördlicher Datenschutzbeauftragter ... 109
Kommune
datenschutzrechtliche Freigabe ... 29
Kontounterlagen ... 158
Kopie ... 162

Kosten
Akteneinsicht 169
Krankengeldfallmanagement
schriftliche Information 149
Krankenhaus 152
Auftragsdatenverarbeitung 40
Berechtigungskonzept 38
Entsorgungskonzept 40
Outsourcing 40
Protokollierung 38
Videoüberwachung 36
Krankenkasse 149, 151, 152, 153
Freiwillig versichertes Mitglied 154
Krebsregister 137
Kreistag
E-Mail-Adresse 36
Kriminalaktennachweis (KAN) 59
Erstkonsument 65
Restverdacht 64
Kundendaten
Erhebung im immissionsschutzrechtlichen Genehmigungsverfahren 281
Landesjustizkasse 89
Landesstelle für den Schulsport 217
Lern- und Entwicklungsdefiziten 143
Lernplattform
Schule 202
Lichtbildaufnahme 100
Liste
Asylbewerber 134
Löschmoratorium 77
Managementgesellschaft 153
mebis – Landesmedienzentrum Bayern 202
mebis-Lernplattform 202
Mediathek
Archivierung von aufgezeichneter Sitzung im Gemeinderat 116
Medienbildung
Schule 202
Medizinische Daten
Erhebung 159
Medizinischer Dienst der Krankenversicherung (MDK) 149, 151
Meldebehörde
Datenübermittlung 126
Meldedatenverordnung 54, 124, 143
Melderecht
Bundesmeldegesetz 124
Melderegisterauskunft 124
Melderegisterauskunft 124, 154
Auskunftssperre 124
Rundfunkgebühr 124
Microsoft Cloud Deutschland 278
Mietvertrag 162
Minderjährige 73, 153

Mitarbeiterfoto
Intranet ... 242
Personalnachrichten ... 242
Mitglieder ... 153
Mithören
TKBek ... 226
Mitwirkungspflicht ... 158
Mobilfunkdaten
anonymisiert ... 35
Verkehrsflussanalyse ... 35
Nachbar
Baugenehmigungsverfahren ... 123
nachrichtendienstliche Mittel ... 73
Nationale Kohorte (NAKO) ... 46
Gesundheitsstudie ... 46
Non-Responder-Fragebogen ... 46
Normenvertrag ... 152
Notariatsunterlage ... 84
Objektdatenbank ... 58
Observation ... 165
Öffentliche Zustellung
Steuerbescheid ... 182
Optisch-Elektronische Klingelanlage ... 155
Organisierte Kriminalität ... 73
Orientierungshilfe ... 49
Originalunterschrift
Sitzungsvorlage (eingescannt) im WWW ... 114
Örtliche Personalvertretung ... 155
Ortungssystem
Dienstfahrzeug ... 237
Outsourcing
Krankenhaus ... 40, 144
Sozialbehörde ... 171
Parkverstoß ... 100
Passwortgeschützte Lernplattform
Schule ... 202
Patientendaten
medizinische ... 145
Patientengeheimnis
Auftragsdatenverarbeitung plus ... 174
Personalakte
Betriebliches Eingliederungsmanagement ... 234
Einsicht durch Gemeinderat ... 251
Personalausweis ... 162
Kopie ... 68, 71
Personalnachrichten
Bedienstetenfoto ... 242
Mitarbeiterfoto ... 242
Personalrat
Dienstliche Telekommunikationsanlage ... 226
Elektronische Schließanlage ... 229
Informationsanspruch ... 257
Ortungssystem in Dienstfahrzeug ... 237
Videoüberwachung ... 131

Zugriff auf Zeiterfassungsdaten ... 257
Personalreferent
Gemeinderat ... 251
Personalvertretung
Betriebliches Eingliederungsmanagement ... 234
Personenpool
Bayerische Landesstelle für den Schulsport ... 217
Personenstandsdaten
Digitalisierung ... 104
Photovoltaikanlage
Einkommensteuer ... 189
ELSTER ... 189
Steuererklärung ... 189
Umsatzsteuer ... 189
Polizei
Erhebung von Gesundheitsdaten ... 142
Polizeiaufgabengesetz ... 50
Polizeiliche Beobachtung ... 56
Polizeilicher Informations- und Analyseverbund (PIAV) ... 61, 63, 65
Polizeilicher Restverdacht ... 59
Precobs ... 52
Pressearbeit ... 27
Privacy Shield ... 19, 275, 278
Privatgespräch
TKBek ... 226
Privatschule
Schulaufsicht ... 220
Protokollauswertung ... 38
Protokollierung
Krankenhaus ... 38
Prüfung ... 39
Radikalenerlass ... 87
Ransomware ... 30
Recht am eigenen Bild
Videoaufnahmen im Schulunterricht ... 206
Recht auf Auskunft ... 270
Recht auf informationelle Selbstbestimmung
Digitalisierung von Personenstandsregistern ... 104
Recht auf Vertraulichkeit von Abstammungsinformationen
Digitalisierung von Personenstandsregistern ... 104
Regelanfrage beim Landesamt für Verfassungsschutz ... 87
Regensburger Modell
Führungszeugnis ... 176
Regierung
Schulaufsicht ... 220
Reisezeitmessung ... 35
Restaurantrechnung
Finanzamt ... 186
Richter ... 87
Richtlinie für den Datenschutz der Strafjustiz (RLDSJ) ... 16, 50, 59, 71
Rundfunkbeitrag/-gebühr
Auskunftssperre ... 124
Melderegisterauskunft ... 124
Safe Harbor ... 275

Scheidungsurteil ... 163
Schließanlage ... 229
Schulamt
    Schulaufsicht ... 220
Schulaufsicht
    Private Grundschulen und Mittelschulen ... 220
Schule
    Archivierungsvereinbarung ... 194
    Bayerische Landesstelle für den Schulsport ... 217
    Einwilligung ... 202, 211, 217
    E-Learning ... 202
    Impfberatung ... 141
    Klassenfoto ... 211
    Kommerzielle Werbung ... 211
    mebis-Lernplattform ... 202
    Medienbildung ... 202
    Passwortgeschützte Lernplattform ... 202
    Sponsoring ... 211
    Videoaufnahmen im Schulunterricht ... 206
    Videoüberwachung ... 213
    Weitergabe von Schülerdaten zu Werbezwecken ... 211
Schuleingangsuntersuchung ... 141, 143
Schülerakte ... 194
Schülerfoto ... 211
Schülerunterlagen ... 194
Schülerunterlagenverordnung ... 194
Schulhomepage
    Videoaufnahmen ... 206
Schulsportwettbewerb ... 217
Schwärzung ... 154, 159, 162
Schweiz
    Beschränkte Steuerpflicht ... 182
Schwerbehindertenvertretung
    Betriebliches Eingliederungsmanagement ... 234
Servicekonto ... 262, 265
Sitzungsvorlage (eingescannt) im WWW ... 114
Smart Meter
Social Plugin ... 268
    App ... 41
Sozialbehörde ... 158, 159
    Outsourcing ... 171
Sozialbetreuer
    Asylbewerber ... 135
Soziales Medium ... 268
Soziales Netzwerk ... 164, 268
    Polizeiliche Ermittlung ... 70
Sozialhilfe ... 164
Sozialleistungsmissbrauch ... 113, 165
Spendenbrief
    Krankenhaus ... 147
Sponsoring
    Schule ... 211
Stadtrat
    E-Mail-Adresse ... 36

Statistikstelle
Abschottungsgebot ... 34
Steuerbescheid
Bekanntgabe ... 182
Öffentliche Zustellung ... 182
Steuerdaten
Zugriffskontrolle ... 177
Steuererklärung
elektronische ... 189
Photovoltaikanlage ... 189
Steuergeheimnis ... 177
Steuerung ... 153
Steuerverwaltung
Datenschutzbeauftragte ... 177
Stichprobenkonzept ... 38
Tarifbeschäftigte
Entgegennahme von Arbeitsunfähigkeitsbescheinigungen ... 243
Telefax ... 99
Telekommunikationsanlage
Benutzung ... 226
Textform ... 156
TKBek ... 226
Übertragbare Krankheit ... 133
Umsatzsteuer
Photovoltaikanlage ... 189
Umschlagverfahren ... 151
Unbedenklichkeitsbescheinigung
Führungszeugnis ... 176
Universitätsklinikum
Einwilligung ... 147
Untersuchungsgrundsatz ... 161
Verdeckte Ermittler ... 165
Verdeckter Mitarbeiter ... 73
Verfassungsschutz ... 22, 73
Verkehrsdaten
Beratungsstelle ... 226
Dienstliche Telekommunikationsanlage ... 226
Personalrat ... 226
Verkehrsflussanalyse
Mobilfunkdaten ... 35
Verordnung zur Schaffung barrierefreier Informationstechnik ... 262
Verschlossener Umschlag ... 160
Verschlüsselung ... 262
Verschwiegenheitspflicht
Dienstliche Telekommunikationsanlage ... 226
Vertrauensleute (V-Leute) ... 73
Vertraulichkeit von Abstammungsinformationen
Digitalisierung von Personenstandsregistern ... 104
Videoaufnahme
Schulunterricht ... 206
Videodolmetscher
Telefondolmetscher ... 132

Videoüberwachung 54, 130, 155
Asylsuchende 130
G7-Gipfel 54
Gemeinde 101
Justizvollzugsanstalt 97
Kameraattrappe 101
Krankenhaus 36
Objektdatenbank 58
Rechtsgrundlage 101
Schule 213
Vorfallsdokumentation 101
Zugriff auf Kameras der Verkehrsbetriebe 58
Vordrucke 152
Vordruckvereinbarung 152
Vorratsdatenspeicherung 73, 83
Wählerverzeichnis 95
Wasserzähler
intelligenter 107
Wearables und Gesundheits-App 128
Werbung
Schule 211
Widerspruch 161
Wohngeld 163
Zeiterfassungsdaten
Zugriff durch Personalrat 257
Zeugendaten 69
Zugriffskontrolle
Finanzamt 177
Zuverlässigkeitsüberprüfung 54
Zweckvereinbarung
Behördlicher Datenschutzbeauftragter 109