

Tätigkeitsbericht
der Landesbeauftragten für den Datenschutz
und für das Recht auf Akteneinsicht
zum 31. Dezember 2013

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hat dem Landtag und der Landesregierung alle zwei Jahre einen Bericht über ihre Tätigkeit vorzulegen (§ 27 Brandenburgisches Datenschutzgesetz, § 11 Akteneinsichts- und Informationszugangsgesetz). Dieser Bericht schließt an den am 6. März 2012 vorgelegten Tätigkeitsbericht 2010/2011 an und deckt den Zeitraum vom 1. Januar 2012 bis zum 31. Dezember 2013 ab.

Der Tätigkeitsbericht kann auch aus unserem Internetangebot unter

<http://www.la.brandenburg.de>

abgerufen werden.

Impressum

Herausgeber: Die Landesbeauftragte für den Datenschutz und
für das Recht auf Akteneinsicht Brandenburg
Stahnsdorfer Damm 77
14532 Kleinmachnow

Telefon: 033203 356-0
Fax: 033203 356-49

E-Mail: Poststelle@LDA.Brandenburg.de
Internet: <http://www.lda.brandenburg.de>

Fingerprint: 0DD70C8A 65508B73 2A53EFEE AC857D66

Druck: Druckerei Arnold, Großbeeren

Inhaltsverzeichnis

Seite

Einleitung	11
-------------------------	-----------

Teil A

Brennpunkte

1	Unzulässige Steuerdatenabrufe – Mitarbeiter der Finanzämter unter Generalverdacht	15
1.1	Reguläre Prüfung der Abrufe von Steuerdaten	15
1.2	Ausdehnung des Prüfverfahrens durch das Ministerium der Finanzen	16
1.3	Datenschutzrechtliche Bewertung	17
1.4	Ergebnis	18
2	Datenschutz und Informationssicherheit bei mobilen Endgeräten	19
2.1	Mobile Endgeräte – smart, aber riskant	19
2.2	Zur Vertrauenswürdigkeit von Apps	23
2.3	BYOD – Bring Your Own Disaster?	25
3	Novellierung des Akteneinsichts- und Informationszugangsgesetzes.....	27

Teil B

Datenschutz

1	Zähes Ringen um einen wirkungsvollen Datenschutz in Europa.....	31
2	Technisch-organisatorische Entwicklungen.....	33
2.1	Trennung von Verfahren in gemeinsam genutzten IT-Infrastrukturen	33
2.2	Einsatz von IPv6 – Hinweise für Hersteller und Provider im Privatkundengeschäft	36

2.3	Datenschutzgerechtes Smart Metering – eine Orientierungshilfe	38
2.4	Neuer Standard zum Vernichten von Datenträgern	40
2.5	Einsatz von De-Mail bei öffentlichen Stellen	44
2.6	Öffentliche Speicherdienste im Internet auch für die Verwaltung?	46
3	Arbeit und Soziales	47
3.1	Kostenloses Spielzeug nur gegen Hartz-IV-Bescheid.....	47
3.2	Fehlerhafte Datenübermittlung wegen Namensgleichheit.....	48
3.3	Verarbeitung von Gesundheits- und Sozialdaten per Telearbeit?	49
4	Banken- und Inkassowesen.....	52
4.1	Fördermittel nur bei Vorlage vollständiger Kontoauszüge?.....	52
4.2	Auskunftsverweigerung von Inkasso Rechtsanwälten rechtmäßig?	53
4.3	Unzulässige Kontrollabfrage einer Bausparkasse bei der SCHUFA	54
5	Beschäftigtendatenschutz.....	55
5.1	Scheitern des Beschäftigtendatenschutzgesetzes.....	55
5.2	Rechtswidrige Personalaktenführung	56
5.3	Lohn- und Gehaltsabrechnung durch Steuerberater.....	57
5.4	Überwachung von Firmenfahrzeugen mittels GPS	58
5.5	Mit dem Fingerabdruck den Arbeitstag beginnen?	59
6	Gesundheit	62
6.1	Gesetz zur Stärkung der Patientenrechte	62
6.2	Honorarkräfte in Gesundheitsämtern.....	63
6.3	Antragsformular für Wohngruppenzuschlag	64
6.4	Das Projekt „Agnes 2“	65
6.5	Pseudonymisierung bei integrierter Versorgung	67
6.6	Ambulante Netzhaut-Glaskörperchirurgie.....	67
7	Informationstechnik in der Landesverwaltung	68
7.1	Zur Zukunft des IT-Einsatzes in der Landesverwaltung	68
7.2	IT-Sicherheitsmanagement in der Landesverwaltung	71
7.3	Novellierung der IT-Standards für die Landesverwaltung	73

7.4	Technische Kontrolle beim Brandenburgischen IT-Dienstleister	75
7.4.1	Erstellung von IT-Sicherheitskonzepten	75
7.4.2	Datenschutzbeauftragter des ZIT-BB	76
7.4.3	Verfahrensverzeichnisse	76
7.4.4	Organisations- und Dienstanweisungen	77
7.4.5	Gebäude- und Raumsicherung.....	77
7.4.6	Fileserver des ZIT-BB.....	78
7.4.7	Kommunikationsserver des ZIT-BB	78
7.4.8	Datenträgerentsorgung.....	79
7.4.9	Intranet des ZIT-BB	79
7.4.10	Sicherheit der Arbeitsplatzcomputer	79
7.4.11	Telekommunikationsanlage.....	80
8	Inneres	81
8.1	Bundsmeldegesetz.....	81
8.2	Brandenburgische Personenstandsverordnung.....	82
8.3	Einführung eines einheitlichen Einsatzleitsystems in den Regionalleitstellen Brandenburgs	84
8.4	Zensus 2011: Nach der Volkszählung ist vor der Volkszählung.....	85
9	Jugend und Familie.....	87
9.1	Heimerziehung in der DDR – Auskunft und Akteneinsicht	87
9.2	Datenübermittlung durch das Jobcenter an das Jugendamt wegen vermuteter Kindeswohlgefährdung.....	88
9.3	Veröffentlichung von Sozialdaten durch einen Kreistag.....	89
10	Justiz.....	90
10.1	Datenschutzgerechte Vorbereitung der Schöffenwahl	90
10.1.1	Nutzung des Melderegisters	90
10.1.2	Veröffentlichung der Vorschlagslisten.....	92
10.2	Einführung des bundesweiten Vollstreckungsportals.....	93
11	Kommunales.....	95
11.1	Licht und Schatten – datenschutzrechtliche Prüfungen in Kommunen.....	95
11.2	Wo drückt der Schuh? – Bürgerumfragen durch Kommunen.....	97
11.3	Dreidimensionale Erfassung des öffentlichen Straßen- raums	99

12	Polizei.....	100
12.1	Öffentlichkeitsfahndung der Polizei in sozialen Netzwerken	100
12.2	Quellen-Telekommunikationsüberwachung in Brandenburg.....	103
12.3	PolBB-App – eine mobile Anwendung der Polizei Brandenburg	106
13	Schule	107
13.1	Schulverwaltungsprogramm weBBschule.....	107
13.2	Mangelhafter Datenschutz an einem Gymnasium	109
13.3	Schülerdaten – begehrte Informationen für Krankenkassen	110
14	Telekommunikation und Medien	111
14.1	Internet Sweep Day 2013	111
14.2	Prüfung des Einsatzes von Google Analytics	113
14.3	Orientierungshilfe Soziale Netzwerke	114
14.4	Fotos von Badegästen im Internet.....	115
15	Verkehr.....	117
15.1	Gemeinsame Kraftfahrzeugzulassung.....	117
15.2	Umfrage zur Videoüberwachung im öffentlichen Personen- verkehr in Brandenburg	118
15.3	Flughafen Berlin Brandenburg.....	122
15.4	Auto-Cockpit-Kameras: Überwachung aus Kraftfahrzeugen.....	124
15.5	Videoüberwachung in Taxis	125
16	Videoüberwachung	126
16.1	Neubau des Landtagsgebäudes in Potsdam	126
16.2	Übertragung einer Videoüberwachung an alle Mitarbeiter	127
17	Wirtschaft.....	129
17.1	Kein Paket ohne Personalausweisnummer	129
17.2	Werbung durch ein Autohaus trotz Widerspruch	130
17.3	Brandenburg Business Guide.....	130
18	Tätigkeit der Sanktionsstelle	131
18.1	Unbefugte Datenabrufe aus polizeilichen Datenbanken	131
18.2	Entsorgung personenbezogener Daten im Wald und als Altpapier	132

18.3	Heimliche Videoüberwachung	133
18.4	Pflicht zur Auskunftserteilung an die Aufsichtsbehörde	133
18.5	Pflicht zur Auskunftserteilung an den Betroffenen	134
18.6	Abgaben an die Staatsanwaltschaft	134

Teil C

Akteneinsicht und Informationszugang

1	Open Data und Informationsfreiheit.....	136
1.1	Europa.....	136
1.2	Bund und Länder.....	137
1.3	Brandenburg	138
1.4	Positionen der Informationsfreiheitsbeauftragten.....	139
2	Entwicklung der Informationsfreiheit in Bund und Ländern	140
3	Grundstücksverkauf ohne Wertgutachten – Die Katze im Sack.....	143
4	Herausgabe von Planungsunterlagen als Kopien.....	145
5	Gutachten zu einer Umgehungsstraße	146
6	Die Verlegung von Wasserleitungen – ein Geheimnis?	148
7	Kommunalaufsicht im stillen Kämmerlein?	149
8	Kalkulationsunterlagen zur Berechnung von Beiträgen	151
9	Per E-Mail zur Akteneinsicht?	153

Teil D

Die Dienststelle

1	Die Dienststelle.....	156
2	Zusammenarbeit mit dem Landtag	157
3	Zusammenarbeit mit behördlichen Datenschutz- beauftragten	158

4	Zusammenarbeit mit Datenschutzbehörden	158
4.1	Datenschutzkonferenz – 2012 unter brandenburgischem Vorsitz	158
4.2	Zusammenarbeit mit weiteren Stellen.....	161
5	Zusammenarbeit mit Informationsfreiheitsbeauftragten	161
6	Öffentlichkeitsarbeit.....	163
6.1	Veranstaltungen der Landesbeauftragten.....	163
6.2	Fortbildungsangebote.....	164
6.3	Neue Publikationen der Landesbeauftragten.....	166
6.4	Neues Internetangebot.....	167

Anlagen

1	Entschlieungen der Konferenz der Datenschutzbeauf- tragten des Bundes und der Lnder	169
1.1	86. Konferenz am 1./2. Oktober 2013 in Bremen.....	169
1.1.1	Forderungen fr die neue Legislaturperiode: Die Datenschutzgrundrechte strken!.....	169
1.1.2	Handlungsbedarf zum Datenschutz im Bereich der ffent- lichen Sicherheit in der 18. Legislaturperiode des Deutschen Bundestages	170
1.1.3	Strkung des Datenschutzes im Sozial- und Gesundheitswesen	171
1.1.4	Sichere elektronische Kommunikation gewhrleisten – Ende-zu-Ende-Verschlsselung einsetzen und weiterentwickeln	173
1.2	Entschlieung zwischen der 85. und 86. Konferenz vom 5. September 2013.....	174
	Keine umfassende und anlasslose berwachung durch Nachrichtendienste! Zeit fr Konsequenzen	174
1.3	85. Konferenz am 13./14. Mrz 2013 in Bremerhaven.....	176
1.3.1	Europa muss den Datenschutz strken!	176
1.3.2	Pseudonymisierung von Krebsregisterdaten verbessern!	178
1.3.3	Soziale Netzwerke brauchen Leitplanken – Datenschutz- beauftragte legen Orientierungshilfe vor.....	179
1.3.4	Datenschutz auch in einer transatlantischen Freihandels- zone gewhrleisten!	180

1.4	EntschlieÙung zwischen der 84. und 85. Konferenz vom 25. Januar 2013	181
	Beschäftigtendatenschutz nicht abbauen, sondern stärken!	181
1.5	84. Konferenz am 7./8. November 2012 in Frankfurt (Oder)	182
1.5.1	Europäische Datenschutzreform konstruktiv und zügig voranbringen!	182
1.5.2	Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben	184
1.5.3	Übermittlung von Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und die GEZ rechtskonform gestalten	185
1.5.4	Einführung von IPv6 – Hinweise für Provider im Privatkundengeschäft und Hersteller	186
1.6	EntschlieÙungen zwischen der 83. und 84. Konferenz	188
1.6.1	EntschlieÙung vom 22. August 2012: Melderecht datenschutzkonform gestalten!	188
1.6.2	EntschlieÙung vom 27. Juni 2012: Orientierungshilfe zum datenschutzgerechten Smart Metering	189
1.6.3	EntschlieÙung vom 23. Mai 2012: Patientenrechte müssen umfassend gestärkt werden	191
1.7	83. Konferenz am 21./22. März 2012 in Potsdam	192
1.7.1	Ein hohes Datenschutzniveau für ganz Europa!	192
1.7.2	Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum – nicht ohne Datenschutz	195
1.7.3	Europäische Ermittlungsanordnung darf Grundrechtsgarantien nicht aushebeln	196
1.8	EntschlieÙung zwischen der 82. und 83. Konferenz vom 7. Februar 2012	197
	Schuldnerverzeichnis im Internet: Anzeige von Schuldnerdaten nur im Rahmen der gesetzlich legitimierten Zwecke	197
2	Beschlüsse der Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich (Düsseldorfer Kreis)	199
2.1	Beschluss vom 11./12. September 2013	199
	Datenübermittlung in Drittstaaten erfordert Prüfung in zwei Stufen	199
2.2	Beschluss vom 26./27. Februar 2013	199
	Videoüberwachung in und an Taxis	199
2.3	Beschluss vom 18./19. September 2012	201
	Near Field Communication (NFC) bei Geldkarten	201
2.4	Beschluss vom 17. Januar 2012	202
	Einwilligungs- und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft	202

3	Entschließungen der Konferenz der Informationsfreiheitsbeauftragten in Deutschland	215
3.1	27. Konferenz am 28. November 2013 in Erfurt.....	215
	Forderungen für die neue Legislaturperiode: Informationsrechte der Bürgerinnen und Bürger stärken!	215
3.2	26. Konferenz am 27. Juni 2013 in Erfurt	216
3.2.1	Open Data stärkt die Informationsfreiheit – sie ist eine Investition in die Zukunft!	216
3.2.2	Verbraucher durch mehr Transparenz im Lebensmittel- bereich schützen – Veröffentlichungspflichten für Hygieneverstöße jetzt nachbessern!.....	217
3.2.3	Transparenz bei Sicherheitsbehörden	218
3.2.4	Für einen effektiven presserechtlichen Auskunftsanspruch gegenüber allen Behörden – auch des Bundes	219
3.3	25. Konferenz am 27. November 2012 in Mainz.....	219
3.3.1	Mehr Transparenz bei Krankenhaushygienedaten	219
3.3.2	Parlamente sollen in eigener Sache für mehr Transparenz sorgen!	220
3.4	24. Konferenz am 12. Juni 2012 in Mainz.....	221
3.4.1	Informationsfreiheit auf europäischer Ebene ausbauen, nicht einschränken!	221
3.4.2	Mehr Transparenz bei der Wissenschaft – Offenlegung von Kooperationsverträgen	222
4	Abkürzungsverzeichnis	224
5	Stichwortverzeichnis.....	226

Zur besseren Lesbarkeit wird bei verallgemeinernden Substantiven lediglich das bestimmende grammatische Geschlecht verwendet. Selbstverständlich richtet sich dieser Tätigkeitsbericht an alle Leserinnen und Leser.

Einleitung

Am 6. Juni 2013 berichtete die britische Tageszeitung „The Guardian“, dass der amerikanische Geheimdienst NSA (National Security Agency) massenhaft Daten über Telefongespräche von US-Bürgern sammle. Aufgrund eines geheimen Gerichtsbeschlusses sei der Telekommunikationsanbieter Verizon verpflichtet, der NSA detaillierte Verbindungsdaten aller über sein System abgewickelten Telefonate zu übermitteln. Zu den Daten gehörten die Rufnummern der beteiligten Anschlüsse, ortsbezogene Informationen sowie Dauer und Uhrzeit der Verbindungen. Der Beschluss bezog sich auf einen begrenzten Zeitraum, dessen Ende in der Zukunft lag und umfasste alle Gespräche, die innerhalb der USA sowie zwischen den USA und dem Ausland geführt wurden. Unklar war zu diesem Zeitpunkt noch, ob der Geheimdienst mehrfach oder gar dauerhaft in dieser Weise arbeitete und ob es ähnliche Beschlüsse auch für andere Telekommunikationsanbieter gab.

Die Veröffentlichung war der Auftakt einer nicht endenden Serie von Berichten über die Tätigkeit der NSA sowie weiterer Nachrichtendienste, wie z. B. des britischen GCHQ (Government Communications Headquarters). Über viele Jahre hinweg hatten diese Dienste verschiedene technisch ausgefeilte, hoch komplexe Verfahren entwickelt und eingesetzt, um Kommunikationsvorgänge weltweit zu überwachen und auszuwerten. Bekannt wurden diese unter den Bezeichnungen PRISM, XKeyScore, Tempora u. a. Betroffen waren eine Vielzahl von Bürgern in den USA und im Ausland, Spitzenpolitiker befreundeter Staaten (wie z. B. die Bundeskanzlerin der Bundesrepublik Deutschland) sowie diplomatische Vertretungen und internationale Organisationen (wie z. B. die Vereinten Nationen oder die Europäische Union).

Quelle der Informationen war der amerikanische Whistleblower Edward Snowden, der zuvor für eine Beratungsfirma der NSA gearbeitet und in dieser Funktion auch Zugang zu internen Dokumenten hatte. Zu den Techniken, die den Berichten nach von den Nachrichtendiensten eingesetzt wurden, gehörten neben dem Sammeln und Auswerten von Verbindungsdaten der Telekommunikation u. a. auch das Ausspähen von Inhalten des E-Mail-Verkehrs und der Internetkommunikation, das Mitlesen des internen Datenverkehrs großer, weltweit agierender Internetunternehmen, das Angreifen und Umgehen von gängigen Verschlüsselungsverfahren, das Ausnutzen von Sicherheitslücken in Hard- und Softwareprodukten, das gezielte Infiltrieren und Manipulieren von Endgeräten wie PCs und Smartphones oder das Registrieren des gesamten Postverkehrs in den USA. Immer wieder wurde auch der Verdacht laut, dass Hersteller von Hard- und Software sowie große Internetunternehmen die Tätigkeiten der Geheimdienste unterstützten oder zumindest duldeten.

Wie in vielen anderen Staaten führten die Veröffentlichungen über die Überwachungs- und Ausspähaktivitäten des amerikanischen und anderer Nachrichtendienste auch in Deutschland zu ausgiebigen Diskussionen. Das Vertrauen vieler Bürger in die Privatheit und den Schutz der eigenen Kommunikation wurde mit jedem neuen Bericht weiter erschüttert. Selbst diejenigen, die das vor 30 Jahren vom Bundesverfassungsgericht aus dem allgemeinen Persönlichkeitsrecht abgeleitete Grundrecht auf informationelle Selbstbestimmung bisher nicht kannten oder besonders wertschätzten, stellen zunehmend fest, dass jede ihrer Äußerungen oder Aktivitäten Ziel der Überwachung oder Ausspähung sein kann. Sie erkennen, dass es ein Verlust an persönlicher Freiheit ist, nicht mehr vertraulich kommunizieren oder unbeobachtet agieren zu können.

Die beschriebene Entwicklung ist geeignet, eine Zeitenwende für den Datenschutz sowohl in Deutschland als auch weltweit einzuleiten. Mehr denn je stellt sich die Frage, wie grundlegende Menschenrechte im Zeitalter des Internets und der allgegenwärtigen Datenverarbeitung, bei zunehmender Miniaturisierung und gleichzeitig steigender Leistungsfähigkeit der technischen Systeme geschützt werden können. In Deutschland betrifft dies neben dem bereits genannten Grundrecht auf informationelle Selbstbestimmung auch das ebenfalls vom Bundesverfassungsgericht entwickelte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Zunächst ist es erforderlich, die nachrichtendienstlichen Überwachungs- und Ausspähaktivitäten detailliert zu untersuchen und vollständig aufzuklären. Parallel muss die bereits begonnene, breite Diskussion mit dem Ziel fortgeführt werden, Schlussfolgerungen aus politischer, rechtlicher und technischer Sicht zu ziehen. Zu klären sind dabei solche Fragen wie: Dürfen Geheimdienste mit dem Argument, terroristische Gefahren abzuwehren, weltweit Menschen anlasslos und dauerhaft überwachen? Ist es ihnen erlaubt, hierbei beliebige technische Mittel einzusetzen? Welche rechtlichen Regelungen sind zu schaffen, um die Tätigkeit der Geheimdienste zu begrenzen? Wie lässt sich die Einhaltung der Grenzen wirkungsvoll kontrollieren? Kann in Bezug auf die Tätigkeit von Geheimdiensten eine Einigung auf breiter internationaler Ebene erreicht werden? Welche technischen Möglichkeiten hat jeder Einzelne, sich gegen Überwachung und Ausspähung zu schützen? Welche Aktivitäten sind nötig, um die Entwicklung und den Einsatz geeigneter Verfahren und Produkte zur technischen Absicherung der Kommunikation zu fördern?

Die Enthüllungen von Edward Snowden zur Praxis von Geheimdiensten bei der weltweiten Überwachung und Ausspähung von Menschen haben eine Debatte angestoßen, die jeden betrifft. Letztlich geht es darum, wie viel Verlust an Freiheit die Gesellschaft bzw. der Einzelne bereit sind zu akzeptieren,

um in Sicherheit leben zu können. Wir werden uns dieser Debatte stellen müssen. An der Erarbeitung von Lösungsvorschlägen werden auch die Datenschutzbeauftragten mitwirken.

Zu diesem Tätigkeitsbericht

Die beiden zurückliegenden Berichtsjahre waren sowohl auf dem Gebiet des Datenschutzes als auch auf dem Gebiet des Akteneinsichts- und Informationszugangsrechts zwei sehr bewegte Jahre.

Im Januar 2012 legte die Europäische Kommission den lange erwarteten Entwurf einer EU-Datenschutz-Grundverordnung vor. Das zähe Ringen um das zukünftige Datenschutzrecht in Europa begann – es ist auch am Ende des zweiten Berichtsjahres noch nicht abgeschlossen. Nie zuvor hat die Wirtschaft eine so vehemente Lobbyarbeit in einem Gesetzgebungsverfahren betrieben und versucht, ihre Interessen z. B. durch die Bereitstellung vollständig ausformulierter Änderungsvorschläge durchzusetzen. Und nie zuvor war eine Stärkung des Grundrechts auf informationelle Selbstbestimmung so wichtig wie heute. Dies ergibt sich bereits aus der rasanten technischen Entwicklung, der immer stärkeren internationalen Vernetzung, der Tätigkeit weltweit agierender Unternehmen sowie aus den damit verbundenen Gefahren für jeden Einzelnen bei der Verarbeitung seiner personenbezogenen Daten. Die Verfechter eines starken Datenschutzrechts erhielten Mitte 2013 unerwartet Unterstützung. Durch die Enthüllungen des Whistleblowers Edward Snowden zu den Überwachungs- und Ausspähaktivitäten des amerikanischen und des britischen Nachrichtendienstes erkannten viele Teilnehmer an den Diskussionen zur EU-Datenschutz-Grundverordnung, dass der Entwurf nicht etwa zu weitgehende Regelungen enthält, sondern vielmehr eine weitere, konsequente Stärkung des Datenschutzrechts für die Bürger in Europa erforderlich ist. Es bleibt zu hoffen, dass sich dies im endgültigen Verordnungstext niederschlägt.

Ein weiteres, für Brandenburg sehr wichtiges Gesetzgebungsverfahren, das allerdings im Gegensatz zur EU-Datenschutz-Grundverordnung im Berichtszeitraum abgeschlossen wurde, ist die Novellierung des Akteneinsichts- und Informationszugangsgesetzes. Nachdem der Novellierungsbedarf dieses Gesetzes immer stärker zutage getreten war, hatte die Landesregierung im November 2012 einen entsprechenden Entwurf vorgelegt. Allerdings blieb die damit verbundene Chance für eine Modernisierung der Regelungen ungenutzt. Insbesondere wurden die von mir immer wieder aufgeführten Mängel und Probleme des bisherigen Gesetzes mit der Novellierung nicht gelöst. Zu meinem Bedauern ist Brandenburg nicht dem Vorreiterland Hamburg gefolgt: Dort gilt mittlerweile ein modernes Transparenzgesetz, das u. a. ein internet-basiertes Informationsregister und eine gesetzliche Verpflichtung zur Veröf-

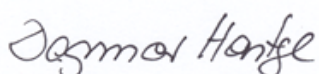
fentlichung von Daten der Verwaltung in diesem Register vorsieht. Obwohl in der Verfassung des Landes Brandenburg das Recht auf Akteneinsicht als Grundrecht verankert ist, enthält das Akteneinsichts- und Informationszugangsgesetz im Vergleich zu den anderen Informationsfreiheitsgesetzen in Deutschland weiter die umfangreichsten Ausnahmeregelungen.

Auf dem Gebiet des Datenschutzes lagen Arbeitsschwerpunkte im Berichtszeitraum in den Bereichen Beschäftigtendatenschutz, Videoüberwachung und Kommunales. Insbesondere in den beiden erstgenannten Bereichen nimmt die Anzahl von Beschwerden immer weiter zu. Kontrollen der Verarbeitung personenbezogener Daten von Beschäftigten offenbarten bei zwei öffentlichen Stellen im Land derart gravierende datenschutzrechtliche Mängel, dass ich jeweils eine Beanstandung aussprechen musste. Bezüglich der Videoüberwachung ist klar zu erkennen, dass viele Petenten eine ständige Überwachung des öffentlichen Raums durch private Videokameras nicht hinnehmen wollen. Das Recht, unbeobachtet zu sein, kollidiert hier regelmäßig mit den Sicherheitsinteressen z. B. der Grundstücks- oder Hauseigentümer, die ihr Eigentum vor Beschädigungen schützen wollen.

Im Bereich Kommunales habe ich im Berichtszeitraum unter anderem eine stichprobenartige Nachkontrolle zu meiner im Jahr 2009 durchgeführten Umfrage zum Stand von Datenschutz und IT-Sicherheit in den Kommunalverwaltungen vorgenommen. Im Ergebnis dieser und anderer Prüfungen vor Ort freue ich mich, feststellen zu können, dass viele Kommunen erhebliche Anstrengungen unternehmen, trotz personeller oder finanzieller Probleme die Anforderungen des Brandenburgischen Datenschutzgesetzes im Bereich der Informationssicherheit vollständig umzusetzen. Der eingeschlagene Weg sollte konsequent weitergegangen werden.

Mit meinem 17. Tätigkeitsbericht möchte ich Ihnen, liebe Leserinnen und Leser, einen Überblick über die aktuellen Entwicklungen, die erzielten Fortschritte sowie die noch bestehenden Probleme in den verschiedenen Bereichen des Datenschutzes sowie des Rechts auf Akteneinsicht geben. Ich wünsche Ihnen eine interessante Lektüre.

Kleinmachnow, den



Dagmar Hartge

Teil A

Brennpunkte

1 Unzulässige Steuerdatenabrufe – Mitarbeiter der Finanzämter unter Generalverdacht

Die Beschäftigten der Finanzämter müssen im Rahmen ihrer Aufgaben für die Steuerverwaltung auf personenbezogene Daten der Steuerpflichtigen zugreifen können. Über ihre Zuständigkeit hinausgehende Abrufe von Steuerdaten verstoßen allerdings gegen das Steuergeheimnis. Um zu kontrollieren, ob die Mitarbeiter sich an diese Einschränkungen halten, führte die Innenrevision des Ministeriums der Finanzen eine anlasslose, flächendeckende Überprüfung durch. Bei deren Konzeption und Umsetzung offenbarten sich gravierende datenschutzrechtliche Mängel.

1.1 Reguläre Prüfung der Abrufe von Steuerdaten

Die Möglichkeit der Finanzbeamten, im Rahmen ihrer Aufgabenwahrnehmung Steuerdaten der Bürger automatisiert abzurufen, korrespondiert mit der Pflicht seitens der Finanzbehörden, angemessene organisatorische und dem jeweiligen Stand der Technik entsprechende technische Vorkehrungen zu treffen, um das Steuergeheimnis zu wahren. Geregelt ist dies in der Steuerdaten-Abrufverordnung. Ziel ist es, zunächst alle Möglichkeiten zu nutzen, um unrechtmäßige Datenabrufe weitestgehend auszuschließen. Wesentliche Maßnahmen sind in diesem Zusammenhang die Berechtigungskonzepte, die sicherstellen sollen, dass Datenabrufe nur im Rahmen der eigenen Zuständigkeit möglich sind. Sofern durch technische Maßnahmen keine Beschränkung der Abrufbefugnis auf die zur Erledigung der jeweiligen Aufgabe erforderlichen Steuerdaten möglich ist, werden Abrufe und Abrufversuche automatisiert aufgezeichnet. Die Protokolldaten umfassen u. a. den Namen und die Benutzerkennung des Beschäftigten, den Zeitpunkt des Abrufs sowie die Steuernummer des Steuerpflichtigen bzw. die eingegebenen Suchbegriffe. Diese Aufzeichnungen dürfen nur zur Prüfung der Zulässigkeit der Abrufe verwendet werden und sind maximal zwei Jahre aufzubewahren und danach unverzüglich zu löschen. Dies muss zeitnah und in angemessenem Umfang erfolgen.

Das Ministerium der Finanzen hat in einem Erlass geregelt, dass regelmäßig Stichproben in Höhe von 5%, 10%, 15% oder 20% der aufgezeichneten Abrufe zu nehmen und von den behördlichen Datenschutzbeauftragten der Finanzämter auf ihre Rechtmäßigkeit zu überprüfen sind. Bei entsprechenden

Anhaltspunkten (z. B. Indiz für unberechtigte Abrufe aufgrund des bisherigen Verhaltens des Abrufenden) können aufgezeichnete Abrufe auch anlassbezogen geprüft werden. Eine Vollkontrolle aller aufgezeichneten Abrufe ist nicht vorgesehen.

Die Stichprobenprüfungen in den Finanzämtern haben nach Auskunft des Ministeriums der Finanzen in der Vergangenheit keine Auffälligkeiten gezeigt und damit keinen Anlass zu weiteren Überprüfungen oder für Anpassungen des Prüfverfahrens gegeben.

1.2 Ausdehnung des Prüfverfahrens durch das Ministerium der Finanzen

Dessen ungeachtet beauftragte das Ministerium der Finanzen die Innenrevision damit, die Einhaltung der Vorgaben zu den Steuerdatenabrufen in den Finanzämtern zu kontrollieren. Ziele der Prüfung waren:

- die Aufdeckung von unbefugten Zugriffen zum Schutz der Daten der Steuerpflichtigen,
- eine Sensibilisierung für den Umgang mit vertraulichen Daten in den Finanzämtern und
- die Unterstützung bei der Entscheidung über Regelungen zur Verbesserung des Datenschutzes.

Der Fokus lag daher auf Abrufen solcher Daten, bei denen zumindest Zweifel hinsichtlich einer dienstlichen Veranlassung bestanden, also bei eigenen Daten des Beschäftigten sowie bei Daten von (möglichen) Angehörigen, Nachbarn, Kollegen und Personen des öffentlichen Lebens.

Zur Erfüllung des Kontrollauftrags hat die Innenrevision alle verfügbaren Protokolldaten mit den personenbezogenen Daten der Bürger aus deren Besteuerungsverfahren (u. a. Name, Anschrift, Geburtsdatum und Steuernummer) sowie den Personaldaten der Beschäftigten der Finanzämter (u. a. Name, Geburtsdatum, Personalnummer und ggf. Adresse, Steuernummer sowie Zuständigkeit im Finanzamt) mit Hilfe der Prüfsoftware „WinIdea“ zusammengefügt und verknüpft. Der so entstandene Datensatz wurde manuell in eine Datei für jeden Bediensteten aufgesplittet. Diese jeweils mitarbeiterbezogenen Dateien wurden dann durch Eingabe entsprechender Suchkriterien überprüft (z. B. möglicher Angehöriger oder Nachbar: gleicher Nachname bzw. gleicher Wohnort/gleiche Adresse; eigene Daten bzw. Daten von Kollegen und Personen des öffentlichen Lebens: Name oder Steuernummer des Betreffenden). Auf diese Weise ermittelte die Innenrevision Verdachtsfälle für

unberechtigte Datenabrufe, die für eine weitergehende Prüfung und Auswertung mit den jeweiligen Beschäftigten an die Vorsteher der Finanzämter übergeben wurden.

Das Ministerium der Finanzen hat uns zunächst dazu mitgeteilt, dass das Vorgehen der Innenrevision eine Komplettüberprüfung darstelle und alle protokollierten Abrufe einbeziehe, um auf diese Weise ein gerechtes Verfahren und eine Gleichbehandlung aller Beschäftigten zu realisieren. Der Schutz ihrer Personaldaten sei gegenüber dem Schutz der Steuerdaten der Bürger nachrangig. Überlegungen zu abgestuften Überprüfungen (z. B. Ausweitung des Umfangs der Stichproben) oder Anpassungen des Prüfverfahrens (z. B. bzgl. des Herausfilterns von „Auffälligkeiten“) habe es nicht gegeben. Anlass seien im Land Berlin im Rahmen einer Kontrolle bekannt gewordene Fälle und die Befürchtung entsprechender Presseanfragen in Brandenburg gewesen.

1.3 Datenschutzrechtliche Bewertung

Grundsätzlich ist die Innenrevision berechtigt, zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen sowohl die Protokolle als auch die Steuer- und Personaldaten zu nutzen, allerdings nur, wenn und soweit der Zugriff auf personenbezogene Daten unverzichtbar ist. Im vorliegenden Fall war die umfassende Prüfung der Innenrevision hinsichtlich aller protokollierten Abrufe aller damit befassten Beschäftigten jedoch unverhältnismäßig und damit rechtswidrig.

Mit Blick auf die Stichprobenprüfungen bestand kein Anlass für eine Vollkontrolle durch die Innenrevision des Ministeriums. Die pauschale Berufung auf im Land Berlin angeblich zutage getretene Fälle genügte nicht. Tatsächlich wurden dort Steuerdatenabrufe nämlich nur aus einem konkreten Anlass und keineswegs flächendeckend geprüft. Dies hätte auch dem Ministerium bekannt sein müssen.

Nach dem allgemeinen datenschutzrechtlichen Grundsatz der Verhältnismäßigkeit ist jede Daten verarbeitende Stelle nur soweit zur Verarbeitung personenbezogener Daten berechtigt, wie dies zum Erreichen der verfolgten Ziele geeignet, erforderlich und angemessen ist.

Das angewandte Verfahren war nur bedingt geeignet, z. B. unzulässige Abrufe der Daten von Angehörigen oder Nachbarn gebührend herauszufiltern. So kann beispielsweise ein Verwandtschaftsverhältnis auch bei unterschiedlichen Namen vorliegen.

Zudem war eine Komplettüberprüfung nicht erforderlich. Selbst nach Darstellung des Ministeriums der Finanzen war bereits aus den Geschäftsverteilungsplänen der Finanzämter eine unzureichende (weil zu grobe) Aufteilung von Verantwortlichkeiten zwischen den Beschäftigten zu erkennen. Dies hätte gereicht, um Regelungen zur Verbesserung des Datenschutzes, insbesondere zur datenschutzgerechten Vergabe von Zugriffsberechtigungen, zu treffen. Hiermit hatte sich das Ministerium jedoch überhaupt nicht befasst. Auch für eine Sensibilisierung der Beschäftigten war die Vollkontrolle durch die Innenrevision nicht erforderlich.

Darüber hinaus ist das Vorgehen der Innenrevision nicht als angemessen zu bewerten. Die pauschale Erklärung, der Schutz von Steuerdaten genieße uneingeschränkte Priorität gegenüber dem Schutz der Mitarbeiterdaten, lässt vielmehr erkennen, dass eine detaillierte Abwägung zwischen dem Zweck der Maßnahme und den Grundrechten der Betroffenen nicht erfolgt ist.

Da im Rahmen des Prüfverfahrens personenbezogene Daten automatisiert verarbeitet wurden, hätte vor dessen Beginn ein Verzeichnissverzeichnis erstellt, ein Sicherheitskonzept entwickelt, eine Vorabkontrolle vorgenommen und eine schriftliche Freigabe erteilt werden müssen. Dies unterblieb ebenso wie die erforderliche Einbindung des behördlichen Datenschutzbeauftragten des Ministeriums der Finanzen.

Die Komplettüberprüfung der Beschäftigten der brandenburgischen Finanzämter verstieß somit gegen eine Reihe von Regelungen des Brandenburgischen Datenschutzgesetzes (BbgDSG): Sie erfolgte ohne Rechtsgrundlage (§ 4 BbgDSG), verletzte den Grundsatz der Erforderlichkeit (§ 13 BbgDSG) und das Gebot der Datensparsamkeit (§ 7 BbgDSG) und missachtete die Vorschriften zum Umgang mit automatisierten Verfahren (§§ 7, 7a, 8 und 10a BbgDSG). Die Landesbeauftragte forderte das Ministerium der Finanzen aufgrund dieser Verstöße zunächst auf, das Prüfverfahren unverzüglich auszusetzen. Nachdem die Behörde dieser Aufforderung nicht nachkam, sprach sie eine förmliche Beanstandung aus.

1.4 Ergebnis

Ungeachtet der Beanstandung durch die Landesbeauftragte hat das Ministerium der Finanzen das von ihm weiterhin als rechtmäßig bewertete Prüfverfahren beharrlich fortgesetzt und letztlich abgeschlossen.

Das Ministerium veröffentlichte erste Zwischenergebnisse der Überprüfung in einigen Finanzämtern, die eine hohe Trefferquote zeigten und damit die Komplettüberprüfung sämtlicher Finanzämter rechtfertigen und deren Verhältnismäßigkeit belegen sollten. Tatsächlich waren diese Zwischenergebnis-

se jedoch einem offensichtlich untauglichen Grobraster der Überprüfung geschuldet und ergaben lediglich erste grobe Verdachtsfälle. Im weiteren Verlauf erkannten auch die mit der weiteren Auswertung beauftragten Finanzamtsvorsteher in der überwiegenden Mehrzahl der Fälle kein für die Ahndung relevantes Fehlverhalten der Mitarbeiter. Vielmehr wurde im Ergebnis der Überprüfung überhaupt nur gegen sehr wenige Finanzbeamte disziplinarrechtlich vorgegangen.

Das Ministerium hat in keinem der geprüften Fälle das Steuergeheimnis als verletzt angesehen. Weder hat es einen Strafantrag wegen Verletzung desselben gestellt, noch hat es auch nur einen Fall an die Landesbeauftragte für den Datenschutz herangetragen, damit diese als für die Verfolgung von Ordnungswidrigkeiten zuständige Behörde den Verstoß gegen datenschutzrechtliche Regelungen hätte prüfen können.

Jeder unbefugte Steuerdatenabruf ist einer zu viel. Der Umgang mit Steuerdaten erfordert deshalb strenge Zugriffsbeschränkungen und effiziente Kontrollen, um den berechtigten Schutz sensibler personenbezogener Daten zu gewährleisten. Für die vollständige Überprüfung sämtlicher Mitarbeiter durch das Ministerium der Finanzen bestand jedoch zu keiner Zeit ein Anlass. Das Verfahren verstieß gegen das Brandenburgische Datenschutzgesetz und missachtete den Grundsatz der Verhältnismäßigkeit. Ein vermutetes Fehlverhalten Einzelner rechtfertigt weder einen Generalverdacht gegen alle Beschäftigten noch deren vollständige Überprüfung.

2 Datenschutz und Informationssicherheit bei mobilen Endgeräten

2.1 Mobile Endgeräte – smart, aber riskant

Der anhaltende gesellschaftliche Trend zur Nutzung von Smartphones oder Tablet-Computern (kurz: Tablets) setzt Behörden und Unternehmen unter Druck, ihren Führungskräften und Mitarbeitern den Einsatz entsprechender aktueller Geräte zu ermöglichen. Die dadurch entstehenden Risiken für Datenschutz und Informationssicherheit können allerdings gravierend sein, sodass es der Umsetzung umfassender Sicherheitsmaßnahmen bedarf.

Heutige Smartphones und Tablets – zusammengefasst sind dies sogenannte Smart Devices (engl. für „intelligente Geräte“) – haben die Leistungsfähigkeit von Desktop-PCs und so große Speicher, dass eine Vielzahl an Daten auf

ihnen Platz findet. Im Gegensatz zu PCs und auch zu Notebooks sind sie jedoch klein, handlich und vor allem mobil. Die Anwender tragen sie mit allen darauf befindlichen E-Mails, Kontakt- und Kalenderdaten, Fotos etc. ständig mit sich herum und nutzen die Geräte für Telefonate, SMS, E-Mail, soziale Netzwerke, Spiele usw. Sollen Smart Devices auch für geschäftliche Zwecke eingesetzt werden, bedarf es also, ähnlich wie beim Einsatz von Notebooks, umfassender Sicherheitsmaßnahmen wie z. B. der Nutzung komplexer Passwörter und einer Geräteverschlüsselung.

Allerdings wurden die aktuellen iPhones, Android-Geräte oder Windows Phones als Konsumentengeräte entwickelt und enthalten zumindest in älteren Versionen viele der für den professionellen Einsatz notwendigen Management- und Sicherheitsfunktionen nicht oder nur teilweise. Es gibt zwar das speziell für professionelle Bedarfe entwickelte Blackberry-Smartphone.¹ Die Herstellerfirma verlor zuletzt jedoch Marktanteile und konnte diese trotz diverser Anstrengungen bisher nicht zurückgewinnen. Administratoren, die vor die Aufgabe gestellt werden, Smart Devices in die IT-Infrastruktur zu integrieren, werden daher hauptsächlich mit iPhones, iPads oder Android-Geräten zu tun bekommen.

Um die notwendigen Sicherheitsmaßnahmen für den Einsatz von Smart Devices im professionellen Umfeld zu bestimmen, ist es erforderlich, zuvor die möglichen Risiken im Einzelfall zu identifizieren und zu bewerten. Die Anzahl der möglichen Sicherheitslücken und Angriffsvektoren kann erheblich sein:

- Das jeweilige Betriebssystem kann abhängig von der Version Sicherheitslücken oder unsichere Standard-Einstellungen aufweisen. Zugleich werden die Betriebssysteme je nach Gerät und Version – insbesondere bei Android-Geräten – von den Herstellern selten oder gar nicht aktualisiert, sodass Sicherheitslücken weiter bestehen bleiben. Vorinstallierte Standardapplikationen können unsicher sein, lassen sich aber zugleich nicht oder nur unvollständig deinstallieren. Um die Geräte überhaupt sinnvoll nutzen zu können, muss in der Regel ein Benutzerkonto auf dem Server der jeweiligen Entwicklerfirma (Apple, Google oder Microsoft) mit allen Nachteilen für den Schutz der dort gespeicherten personenbezogenen Daten angelegt werden.
- Zudem ist das Risiko, eine unsichere oder eine Schadsoftware auf dem Gerät zu installieren, erheblich höher als bei PCs. Die Probleme reichen hierbei von standardmäßiger Datenablage im Internet mittels sog. Cloud-Dienste und unverschlüsselten Datenübertragungen über unzuverlässige

¹ vgl. Tätigkeitsbericht 2008/2009, A 2.4

Zertifikatsprüfungen bis hin zu heimlich übertragenen Adressbüchern, dem Mitlauschen bei Telefonaten, dem heimlichen Versenden von Premium-SMS u. v. m. Allerdings ist die Installation von Software – sog. Apps - auf einem Smartphone oder Tablet so einfach zu bewerkstelligen, dass viele Benutzer schnell und unüberlegt neue Apps auf das Gerät laden. Die Wahrscheinlichkeit, dass persönliche oder geschäftliche Daten ungewollt an Unbefugte weitergegeben werden, steigt daher mit jeder neuen App auf dem Gerät.

- Ein weiteres Problem ist das sog. Rooting bzw. Jailbreaking. Dabei versuchen Nutzer, die Einschränkung der Benutzerrechte auf dem Smart Device zu überwinden, indem sie Sicherheitsmechanismen gezielt mittels spezieller Software aushebeln, welche Sicherheitslücken oder bestimmte Betriebsmodi der Geräte ausnutzt. Ziel des Rooting bzw. Jailbreaking ist die volle Kontrolle des Benutzers über alle Bereiche des Gerätes. Problematisch daran ist, dass nun auch Apps die entsprechenden Rechte und damit die Kontrolle über das System erlangen können.
- Insbesondere im professionellen Umfeld ist das Risiko der Vermischung geschäftlicher und privater Daten zu berücksichtigen. Außerdem sind Smartphones Kommunikationszentralen, können gegebenenfalls geortet werden und enthalten neben Inhaltsdaten auch eine Anzahl an Zugangsdaten, z. B. zu E-Mail-Accounts, zu Benutzerkonten von sozialen Netzwerken oder zu Firmennetzwerken, die ebenfalls dem Risiko der Ausspähung unterliegen. Zudem sind die Geräte ggf. leicht zu entwenden oder können schnell verloren gehen, sodass sämtliche Daten in falsche Hände gelangen können.

Im Verhältnis zu den Risiken sind die Möglichkeiten zur Absicherung und zur Erkennung von Anomalien relativ gering. Die Sicherheits- und Managementmechanismen sind generell in neueren Versionen der jeweiligen Betriebssysteme besser als in älteren. Ein Sicherheitskonzept muss die entsprechenden Gefährdungen berücksichtigen und die jeweils erforderlichen technischen und organisatorischen Maßnahmen ableiten. Hierfür kommen z. B. in Betracht:

- Zugriffsschutz durch sicheres Passwort mit regelmäßigem Passwortwechsel und automatisierter Datenlöschung nach einer zu hohen Anzahl an fehlerhaften Log-in-Versuchen,
- Verschlüsselung des lokalen Speichers (inkl. der externen Speicherkarte) und der Datenübertragung, verschlüsselte Kommunikation mit dem Firmennetzwerk über ein virtuelles privates Netzwerk (VPN),

- Trennung von geschäftlichen und anderen Daten durch Nutzung dafür geeigneter Betriebssysteme oder zusätzliche technische Lösungen wie verschlüsselnde Container-Applikationen oder Virtualisierungssoftware,
- Beschränkung der verwendeten Apps und Schnittstellen im Hinblick auf ihre Erforderlichkeit, insbesondere wirksames Unterbinden unkontrollierter Installation bzw. Deinstallation von Apps durch Benutzer,
- Beschränkung der Benutzerrechte sowie Verhinderung, dass Benutzer sich administrative Rechte durch sog. Rooting oder Jailbreaking auf den Geräten beschaffen,
- Fernsperrung, Fernlöschung des Gerätes bei Verlust,
- generelle Sicherheitsmaßnahmen wie z. B. regelmäßige Softwareaktualisierung, Virenschutz, regelmäßige Datensicherung (Backup).

Aus Datenschutzsicht ist zu beachten, dass mit einem Smart Device wegen der verbleibenden Restrisiken keine hochschutzbedürftigen Daten verarbeitet werden dürfen. Außerdem sollte der zuständige Datenschutzbeauftragte bei der Einführung der Geräte eine Vorabkontrolle durchführen.

Bei Einsatz von Smart Devices im professionellen Umfeld ist es sinnvoll, die Administration und Absicherung der Geräte über eine zentrale Geräteverwaltung (sog. Mobile Device Management) sicherzustellen. Dadurch können alle administrativen Aufgaben wie z. B. das Setzen einer Passwortrichtlinie, die Einschränkung der Benutzerrechte und die Festlegung von Vorgaben für Apps realisiert und in der Regel auch ein Rooting oder Jailbreaking erkannt werden. Allerdings bleiben weiterhin Probleme bestehen. So kann es sein, dass bei einem Betriebssystem-Update neue unsichere Funktionen hinzukommen, die nicht sofort durch ein Mobile Device Management administrierbar sind.

Außerdem hat eine Organisation zu bedenken, dass sie für die Durchsetzung von Beschränkungen auch Prozesse einrichten muss, die den Benutzer bei diesbezüglichen Problemen unterstützen. Hat beispielsweise ein Nutzer sein Passwort vergessen, dann muss es einen Support-Prozess geben, über den das Passwort wieder zurückgesetzt werden kann. Geht ein Smartphone verloren, dann muss klar sein, an wen sich der Nutzer wenden kann, um die Fernlöschung auszulösen.

Da das Benutzerverhalten einen großen Einfluss auf die Sicherheit des Gerätes hat, ist es erforderlich, die Nutzer bei der Planung und Umsetzung der Informationssicherheitsmaßnahmen mit einzubeziehen, sie über mögliche

Gefahren aufzuklären und Vorgaben zur sicheren Gerätenutzung zu machen. Gerade im Bereich der Smartphone-Nutzung im professionellen Umfeld sind klare, verständliche und auf allen Ebenen der Organisation geltende Regelungen unabdingbar.

Sollen Smartphones oder Tablets in Behörden oder Unternehmen eingesetzt werden, ist eine Risikoanalyse durchzuführen und ein darauf aufbauendes Sicherheitskonzept zu erstellen. Die IT-Administration muss die volle Kontrolle über die Geräte behalten und sollte dafür ein Mobile Device Management-System einsetzen. Ebenfalls bedeutsam sind organisatorische Regelungen sowie die Information und Sensibilisierung der Nutzer.

2.2 Zur Vertrauenswürdigkeit von Apps

Apps sind aus der Benutzerperspektive die zentralen Elemente der Datenverarbeitung auf Smartphones und Tablets. Sie sind typischerweise dadurch gekennzeichnet, dass sie nach außen nur eine oder wenige Funktionen ermöglichen. Für Kalender- und Adressverwaltung, E-Mails, SMS usw. benutzt man jeweils eine gesonderte App. Durch diese scheinbare Einfachheit von Apps wird aber oft verschleiert, welche Zugriffe auf Daten und Prozesse im Hintergrund – ggf. auch missbräuchlich – unbemerkt vom Nutzer geschehen.

Sollen Smartphones oder Tablets auch im Unternehmen oder in einer Behörde eingesetzt werden, ist es erforderlich zu wissen, auf welche Daten eine App zugreifen könnte. Nur so lässt sich beurteilen, inwieweit sie im geschäftlichen Bereich eingesetzt werden darf oder ob eine Installation möglicherweise verhindert werden muss.

Grundsätzlich verfügen Betriebssysteme wie iOS und Android über Sicherheitsmechanismen zum Schutz und zur Begrenzung der Rechte von Apps. Apps müssen digital signiert sein, laufen in einem vom System abgetrennten Bereich (Sandbox) und dürfen nicht auf das Dateisystem oder Ressourcen anderer Prozesse zugreifen. Die Prüfung von Apps ist stark von dem jeweiligen Vertriebsmodell der Betriebssystemhersteller abhängig. Bei iOS ist Apple die zentrale Prüfinstanz und entscheidet darüber, ob eine Anwendung auf der Vertriebsplattform – dem App Store – für die Öffentlichkeit zur Verfügung gestellt wird. Was Apple genau prüft bzw. wie weit die Prüfung reicht, ist allerdings nicht bekannt. Zumindest werden Apps, die ganz offensichtlich Schadsoftware sind, herausgefiltert. Verdeckte missbräuchliche Datenzugriffe von Applikationen sind allerdings nicht ausgeschlossen.

Bei Android werden die über den Google Play Store vertriebenen Apps nicht zentral geprüft. Stattdessen fordert eine Anwendung bei der Installation die

Einwilligung des Benutzers für Zugriffe auf Ressourcen wie Netzwerk, Ortungsdienste, Adressbuch etc. an. Allerdings ist es für die Nutzer schwer zu entscheiden, ob und in welchem Ausmaß die fragliche App jene Rechte und Ressourcen tatsächlich benötigt. Außerdem gibt es bei Android die Möglichkeit, Apps nicht nur aus dem Play Store, sondern auch aus unbekannten Quellen zu installieren. Insgesamt erhöht sich dadurch die Wahrscheinlichkeit für Schadsoftware auf dem mobilen Endgerät. Statistische Erhebungen haben dies bestätigt. Im Vergleich zu iOS und Android ist die administrative Kontrolle über Apps bei Blackberry-Geräten deutlich höher. Zugriffsberechtigungen von Apps auf z. B. Kontakt- oder Lokalisationsdaten und die Telefonfunktion können vom Administrator detailliert festgelegt und eingeschränkt werden. Die Freigabe oder auch das Verbot von Apps sind ebenfalls zentral via Funkschnittstelle des Blackberry möglich.

Ein weiteres Problem besteht darin, dass Apps nicht nur von professionellen Softwareentwicklern, sondern auch von unerfahrenen Anfängern entwickelt werden. Dementsprechend gibt es zahlreiche Anwendungen, die die qualitativen Anforderungen an die Informationssicherheit nicht erfüllen. Sehr häufig auftretende Sicherheitsrisiken sind eine fehlende oder fehlerhafte Verschlüsselung bei der Datenspeicherung oder Datenübertragung, eine fehlende oder schwache Authentifizierung und unsicheres Session Handling. Viele App-Entwickler nutzen zudem missbräuchlich aus, dass sie mittels der von ihnen entwickelten Anwendung sehr leicht Daten von den Endgeräten sammeln können, ohne dass diese für die Funktion der App zwingend erforderlich sind. Unter den gesammelten Daten befinden sich sehr häufig die Geräte-ID, Ortsdaten oder Kontaktdaten aus dem Adressbuch des Nutzers.

Wenn es um Daten oder Anwendungen im Behörden- oder Unternehmensumfeld geht, ist es daher erforderlich, Apps vor ihrem Einsatz daraufhin zu überprüfen, ob sie den Datenschutz- und Informationssicherheitsanforderungen genügen. Generell sollte zunächst anhand der AGBs der Anwendung geprüft werden, welche Rechte sich die App-Betreiber einräumen. Häufig kann man dadurch bereits viele Apps als für den geschäftlichen Einsatz ungeeignet aussortieren. Weiterhin sollte eine Laufzeitanalyse durchgeführt werden, um zu überprüfen, auf welche Daten die App zugreift, welche Daten wie gespeichert bzw. wie wohin übertragen werden. Eine weitere Form der Prüfung ist die statische Codeanalyse, die jedoch häufig nicht möglich ist, da der Quellcode der App in der Regel nicht vorliegt und die Methoden zur nachträglichen Gewinnung des Quellcodes zum einen nicht zuverlässig funktionieren und zum anderen in der Regel aus urheberrechtlichen Gründen nicht zulässig sind. Darüber hinaus ist eine Codeanalyse ein sehr aufwendiges und teures Verfahren. Leider kann aber nur sie einen verlässlichen Aufschluss darüber geben, was eine App tut bzw. tun könnte. Berücksichtigt werden muss auch, dass sich das Verhalten einer App mit jedem neuen

Update verändern kann, sodass auch diese Aktualisierungen in die Prüfung einzubeziehen sind.

Ist nicht feststellbar, inwieweit eine App tatsächlich den Sicherheitsanforderungen entspricht, sollte auf ihren Einsatz verzichtet werden. Mögliche Alternativen bestehen darin, keine personenbezogenen Daten bzw. kritischen Geschäftsdaten auf dem Smart Device zu verarbeiten oder aber Apps nur von vertrauenswürdigen Anbietern einzusetzen. Wichtig ist hierbei, dass eine entsprechende Einstufung keinesfalls auf den Nutzerbewertungen in den App-Stores basieren darf, da deren Authentizität und Vertrauenswürdigkeit in der Regel nicht überprüfbar ist.

Daten verarbeitende Stellen dürfen nur vertrauenswürdige Apps auf mobilen Endgeräten einsetzen, da die dort verarbeiteten Daten ansonsten einem zu großen Risiko bezüglich ihrer Vertraulichkeit, Integrität und Verfügbarkeit unterliegen.

2.3 BYOD – Bring Your Own Disaster?

Nutzer besitzen heute privat oft bessere Smartphones oder Tablet-PCs als sie von ihrem Arbeitgeber zur Verfügung gestellt bekommen und möchten dann auch im beruflichen Umfeld nicht darauf verzichten. Sie verwenden einfach ihr privates Gerät auch für berufliche Zwecke wie Telefonate, SMS, E-Mail usw. Oft entsteht daraus im Unternehmen bzw. in der Behörde eine bewusste Strategie. „Bring Your Own Device“, kurz BYOD, nennt sich dieser neue, aber gefährliche Trend.

Auf den ersten Blick ergibt sich für Arbeitgeber eine Reihe von Vorteilen, wenn Mitarbeiter ihre Arbeitsgeräte selbst mitbringen. Sie haben niedrigere IT- und Schulungskosten und die Motivation und Produktivität der Mitarbeiter erhöhen sich. Aber zugleich kommen erhebliche Nachteile und schwer lösbare Probleme auf Unternehmen und Behörden zu.

Generell gilt, dass Organisationen verantwortlich und haftbar für die Verarbeitung personenbezogener Daten in ihrem Bereich sind und entsprechend die volle Kontrolle über die verwendete Hard- und Software haben müssen. Dies ist bei privaten Geräten naturgemäß nicht der Fall. Die IT-Administration wird außerdem mit einer erhöhten Heterogenität der IT-Infrastruktur konfrontiert, die zu einem höheren Aufwand bei der Realisierung von technischen und organisatorischen Maßnahmen führt. Risikoanalyse und Sicherheitskonzept müssen nun auch die privaten Endgeräte umfassen; die unter 2.1 genannten Sicherheitsmaßnahmen sind umfassend umzusetzen. Der Ausschluss der Verarbeitung hochschutzbedürftiger Daten sollte dabei im besonderen Maße berücksichtigt werden.

Eine zentrale Sicherheitsmaßnahme ist die vollständige und wirksame Trennung privater und geschäftlicher Bereiche auf dem Smartphone bzw. dem Tablet. Hierbei müssen nicht nur die Daten voneinander getrennt werden, sondern auch die jeweiligen Apps. Der private Bereich darf keine Zugriffsrechte auf den geschäftlichen Bereich haben, mögliche Schadsoftware in diesem Bereich darf den geschäftlichen Bereich nicht beeinträchtigen. Der geschäftliche Bereich muss verschlüsselt sein. Der Schutz des geschäftlichen Bereiches darf vom Inhaber des Gerätes nicht durch ein mögliches Rooting bzw. Jailbreaking ausgehebelt werden können.

Außerdem muss sichergestellt werden, dass durch eine Datensicherung auf den IT-Systemen des Arbeitgebers keine privaten Daten des BYOD-Gerätes gespeichert werden. Gleichzeitig muss verhindert werden, dass dienstliche Daten ungewollt den geschützten Bereich verlassen und z. B. durch Synchronisierung auf den privaten PC des Nutzers gelangen. IT-Administratoren dürfen nicht auf die privaten Daten zugreifen. Zudem muss geklärt werden, wer eigentlich die Telekommunikationskosten übernimmt, ob eine dienstliche oder eine private SIM-Karte benutzt wird und was bei Verlust des Gerätes passiert. Problematisch kann im letzteren Falle die Notwendigkeit einer Fernlöschung sein, weil dadurch in der Regel sämtliche Daten, also auch die privaten Daten vom Gerät entfernt werden.

Um die genannten Sicherheitsmaßnahmen umzusetzen, bedarf es daher erheblicher Eingriffe und Anpassungen auf dem privaten Endgerät und einer Reihe von organisatorischen und ggf. vertraglichen Vereinbarungen über die BYOD-Nutzung im Unternehmen bzw. der Behörde. Darüber hinaus müssen weitere rechtliche Aspekte wie Urheberrechtsfragen bei Lizenznutzung auf BYOD-Geräten, Haftungsfragen, Archivierungsvorschriften etc. geprüft werden. Insgesamt betrachtet erweisen sich die Anforderungen an eine sichere BYOD-Strategie zum gegenwärtigen Zeitpunkt als so komplex und sowohl mit rechtlichen als auch technischen Unsicherheiten behaftet, dass aus unserer Sicht die Risiken nur unzureichend beherrscht werden können. Diese Sichtweise hat sich inzwischen auch bei vielen Unternehmen und teilweise im öffentlichen Bereich durchgesetzt und zu einem Verzicht bzw. einem Verbot der Nutzung von privaten Endgeräten geführt.

Die Nutzung privater mobiler Endgeräte für geschäftliche Zwecke bringt eine ganze Reihe an technischen und rechtlichen Problemen mit sich. Diese müssen anhand einer Risikoanalyse detailliert benannt und die Vorteile mit dem Aufwand zur technischen und organisatorische Absicherung abgewogen werden. Sowohl im Unternehmensumfeld als auch im öffentlichen Bereich halten wir die verbleibenden Restrisiken und Unsicherheiten einer BYOD-Strategie für so hoch, dass der Einsatz privater mobiler Endgeräte zur Verarbeitung personenbezogener Daten nicht zulässig ist.

3 Novellierung des Akteneinsichts- und Informationszugangsgesetzes

Lange hat sich Brandenburg damit zufriedengegeben, vor 16 Jahren als erstes Bundesland ein allgemeines und voraussetzungsloses Recht auf Akteneinsicht geschaffen zu haben. Zwei konkurrierende Gesetzentwürfe boten im Berichtszeitraum die Gelegenheit, den inzwischen eingetretenen Rückstand gegenüber anderen Ländern aufzuholen und das brandenburgische Informationszugangsrecht zeitgemäß zu novellieren.

In ihren zurückliegenden Tätigkeitsberichten wies die Landesbeauftragte auf den dringenden Bedarf hin, das Akteneinsichts- und Informationszugangsgesetz zu überarbeiten. Unter anderem bemängelte sie die zunehmende Rechtszersplitterung und empfahl die Zusammenführung des Gesetzes mit dem Umweltinformationsgesetz. Auch die Einführung von Veröffentlichungspflichten bzw. zeitgemäßer Open-Data-Regelungen hielt die Landesbeauftragte für erforderlich. Ein Kernpunkt der Kritik an den bislang bestehenden Regelungen war der eng gefasste Anwendungsbereich, der sich auf „klassische“ Behörden konzentrierte, aber beispielsweise Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie privatrechtlich organisierte Landesgesellschaften vom Anspruch auf Informationszugang ausnahm. Einen Widerspruch zum Transparenzzweck des Gesetzes sah die Landesbeauftragte auch in der Regelung, dieses während eines laufenden Verfahrens gar nicht anwenden zu dürfen. Ebenfalls Gegenstand ihrer Kritik war der Ausschluss der Akteneinsicht im Falle der Ausübung einer Aufsicht durch eine übergeordnete Stelle. Die zahlreichen Ausnahmetatbestände zum Schutz eines überwiegenden öffentlichen Geheimhaltungsinteresses waren in weiten Teilen zwingend, das Gesetz sah also nicht vor, einen angemessenen Ausgleich mit dem Einsichtsinteresse der Öffentlichkeit zu erzielen. Hier bedurfte es nach Auffassung der Landesbeauftragten einer Abwägungsregelung. Aufgrund des Fehlens eines ausdrücklichen Rechtsanspruchs auf Fotokopien kam es in der Praxis immer wieder zu Streitigkeiten, die durch eine entsprechende Klarstellung vermeidbar gewesen wären. Ob Unternehmensdaten herausgegeben werden konnten, hing im Wesentlichen von der Zustimmung des betroffenen Unternehmens ab. Verweigerte dieses sein Einverständnis, musste die Information auch dann geheim gehalten werden, wenn ihr Bekanntwerden nicht im Geringsten geeignet gewesen wäre, die wirtschaftlichen Interessen des Unternehmens zu beeinträchtigen. Die Landesbeauftragte forderte daher schon lange, den Schutz auf Betriebs- und Geschäftsgeheimnisse zu beschränken. Zwischenzeitlich teilte die Landesre-

gierung mit, durchaus einen Novellierungsbedarf zu erkennen, blieb jedoch zunächst untätig.²

Im August 2012 brachte die Fraktion BÜNDNIS 90/DIE GRÜNEN den Entwurf für ein Gesetz zur Neuregelung des Informationszugangs³ in den Landtag ein. Damit sollten das bisherige Akteneinsichts- und Informationszugangsgesetz, das Umweltinformationsgesetz sowie Teile des Verbraucherinformationsrechts in einem Gesetz zusammengeführt werden. Die Regelungen des Anwendungsbereichs sowie der Ausnahmetatbestände lehnten sich im Wesentlichen an jenen des europarechtlich vorgegebenen Umweltinformationsrechts an. Die von der Landesbeauftragten kritisierten Mängel des engen Anwendungsbereichs wären damit ebenso wie die fehlende Geltung des Akteneinsichts- und Informationszugangsgesetzes während des laufenden Verfahrens bzw. der Informationsanspruch im Falle der Aufsicht über eine andere Stelle beseitigt worden. Der Entwurf sah auch einen Anspruch auf Kopien, eine Beschränkung des Schutzes von Unternehmensdaten sowie eine grundsätzliche Abwägung zwischen Geheimhaltungs- und Einsichtsinteressen vor. Im Hinblick auf die Einführung von Veröffentlichungspflichten enthielt der Gesetzentwurf erste Ansätze, beispielsweise eine Bestimmung zur Publikation von Verträgen öffentlicher Stellen. Er sah zudem für die informationspflichtigen Stellen vor, eine Statistik über Zugangsanträge zu führen.

Die Landesregierung brachte ihren Entwurf für ein Gesetz zur Änderung des Akteneinsichts- und Informationszugangsgesetzes⁴ Ende November 2012 in das Parlament ein. Das Problem der Rechtszersplitterung wurde durch diesen Entwurf ebenso wenig angesprochen wie die Einführung aktiver Veröffentlichungspflichten. Der Entwurf wollte den Anwendungsbereich lediglich auf die mittelbare Landesverwaltung sowie auf kommunale Anstalten erweitern. Geplant war, den zuvor weitergehenden Schutz von Unternehmensdaten auf Betriebs- und Geschäftsgeheimnisse zu beschränken. Auch wenn Letztere nicht vorliegen, sollte der Informationsanspruch unter dem Vorbehalt einer Anhörung des betroffenen Unternehmens stehen. Vorgesehen war ein Rechtsanspruch auf die Herausgabe von Fotokopien. Gleichzeitig beabsichtigte die Landesregierung, den Informationszugang an anderen Stellen einzuschränken. Ihr Gesetzentwurf nahm das beim Ministerium des Innern eingerichtete Kommunale Prüfungsamt sowie die Verfassungsschutzbehörde, die Aufsicht über Stiftungen des bürgerlichen Rechts, die öffentlich-rechtlichen Rundfunkanstalten sowie wirtschaftlich tätige, öffentlich-rechtlich organisierte Stellen pauschal vom Anwendungsbereich des Gesetzes aus. Die Ausnahme

² vgl. beispielsweise Tätigkeitsbericht 2010/2011, B 1 sowie Tätigkeitsbericht 2008/2009, B 2

³ Landtags-Drucksache 5/5787

⁴ Landtags-Drucksache 5/6428

laufender Verfahren vom Anwendungsbereich sowie die Regelung zur Ablehnung des Zugangs im Falle der Aufsicht über eine andere öffentliche Stelle wurden gegenüber der bislang bereits sehr restriktiven Regelung sogar noch erweitert. Darüber hinaus führte die Landesregierung die „Tätigkeit der Polizei“ als zusätzliches Schutzgut ein, obwohl Belange der Strafverfolgung und -vollstreckung sowie der Gefahrenabwehr und anderer Bereiche der inneren Sicherheit bereits vom Anspruch auf Akteneinsicht ausgenommen waren.

Beide Gesetzentwürfe waren am 7. März 2013 Gegenstand einer öffentlichen Anhörung im Ausschuss für Inneres des Landtags Brandenburg. In ihrer Stellungnahme⁵ empfahl die Landesbeauftragte, den Entwurf der Fraktion BÜNDNIS 90/DIE GRÜNEN der Weiterentwicklung des Informationszugangsrechts in Brandenburg zugrunde zu legen, diesen aber im Hinblick auf die vorgeschlagenen Regelungen zum Verbraucherinformationsrecht sowie zur Statistikpflicht zu straffen und die vorhanden Ansätze zu Veröffentlichungspflichten und Open Data weiterzuentwickeln. Der Entwurf der Landesregierung verharrte aus Sicht der Landesbeauftragten auf einem niedrigen Niveau des Informationszugangsrechts; den vielfachen darin vorhandenen Einschränkungen der Informationsfreiheit standen nur wenige Verbesserungen gegenüber. Die überwiegende Mehrheit der weiteren vom Ausschuss des Innern angehörten Sachverständigen sprach sich ebenfalls für eine Erweiterung der Informationsfreiheit in Brandenburg aus.

Das weitere Gesetzgebungsverfahren zeitigte mehrere Änderungsanträge sämtlicher Landtagsfraktionen. Im Ergebnis schlug der Ausschuss für Inneres Modifizierungen des Gesetzentwurfs der Landesregierung vor.⁶ So wurden beispielsweise die Lesbarkeit der Regelungen zum Anwendungsbereich verbessert, die Vorschrift zur Ausnahme der öffentlich-rechtlichen Rundfunkanstalten gestrichen und die pauschale Ausnahme der wirtschaftlich tätigen, öffentlich-rechtlich organisierten Stellen auf deren Teilnahme am Wettbewerb beschränkt. Außerdem erfolgte die Klarstellung, dass die Herausgabe von Kopien die Einsicht in die Originale der Akten nicht ausschließt. Der Landtag Brandenburg lehnte am 25. September 2013 den Gesetzentwurf der Fraktion BÜNDNIS 90/DIE GRÜNEN ab und nahm den Gesetzentwurf der Landesregierung in der vom Ausschuss für Inneres modifizierten Fassung an.⁷ Außerdem beschloss das Parlament, die Landesregierung zu bitten, die Entwick-

⁵ Landtags-Drucksache P-AI 5/41-1 (Anlage 3)

⁶ Landtags-Drucksache 5/7947

⁷ Landtags-Drucksache BePr 5/81

lung von Open Data voranzubringen.⁸ Die Änderungen des Akteneinsichts- und Informationszugangsgesetzes traten am 18. Oktober 2013 in Kraft.⁹

Die beschlossenen Gesetzesänderungen tragen den Erfordernissen eines modernen Informationsfreiheitsrechts nur unzureichend Rechnung. Die Vorteile der Novellierung vermögen die aus dem Versäumnis einer umfassenden Verbesserung entstehenden Nachteile nicht aufzuwiegen. Selbstverständlich wird die Landesbeauftragte die Umsetzung der neuen Regelungen konstruktiv begleiten und steht sowohl den Bürgern als auch den informationspflichtigen Stellen für eine Beratung zur Verfügung.

⁸ Landtags-Drucksache 5/7998-B. Siehe hierzu auch C 1.

⁹ Gesetz zur Änderung des Akteneinsichts- und Informationszugangsgesetzes und zur Aufhebung des Personalausweisgesetzes vom 15. Oktober 2013 (GVBl. I Nr. 30)

Teil B

Datenschutz

1 Zähes Ringen um einen wirkungsvollen Datenschutz in Europa

Bereits in unserem letzten Tätigkeitsbericht hatten wir über die beabsichtigte Novellierung des europäischen Datenschutzrechts berichtet.¹⁰ Der von der Europäischen Kommission am 25. Januar 2012 vorgelegte Entwurf für eine Datenschutz-Grundverordnung, die im Vergleich zur Europäischen Datenschutzrichtlinie von jedem Mitgliedstaat unmittelbar anzuwenden ist, löste erwartungsgemäß heftige Debatten aus.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßte ausdrücklich die Bemühungen der Kommission für eine Modernisierung und Harmonisierung des Datenschutzrechts in der Europäischen Union. Sie sprach sich dafür aus, den Mitgliedstaaten die Möglichkeit einzuräumen, zumindest in Bezug auf die Datenverarbeitung durch öffentliche Stellen, in einzelstaatlichem Recht über den einheitlichen Mindeststandard hinausgehen zu können. Außerdem plädierten die Datenschützer für eine Einschränkung des Letztentscheidungsrechts der Europäischen Kommission bei der Durchsetzung des Datenschutzes und für den Erhalt der Unabhängigkeit der Datenschutzaufsicht. Nach ihrer Auffassung müssen alle für den Grundrechtsschutz wesentlichen Regelungen in der Verordnung selbst bzw. durch Gesetze der Mitgliedsstaaten getroffen werden. Die Konferenz forderte zudem praxistaugliche Regelungen für einen verstärkten technisch-organisatorischen Datenschutz, die strikte Reglementierung der Profilbildung bzw. deren Verbot bei Minderjährigen sowie praktikable Regelungen für die vorgesehene zentrale Anlaufstelle („One-Stop-Shop“).¹¹

Schon kurz nach der Veröffentlichung des Kommissionsvorschlags haben der Rat der Europäischen Union und das Europäische Parlament ihre Beratungen aufgenommen. Zahlreiche Sitzungen und Abstimmungsgespräche folgten. Im Oktober 2012 fand eine Anhörung des Europäischen Parlaments mit den nationalen Parlamenten statt. Zu Beginn des Folgejahres präsentierte

¹⁰ vgl. Tätigkeitsbericht 2010/2011, A 2.3

¹¹ siehe Anlage 1.7.1: Entschließung „Ein hohes Datenschutzniveau für ganz Europa!“ vom 22. März 2012. Die Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Juni 2012 ist im Internetangebot der Landesbeauftragten veröffentlicht.

der Berichterstatter des Innenausschusses seinen Berichtsentwurf, zu welchem über 3000 Änderungsanträge eingingen.

Die Beratungen standen unter starkem Einfluss unterschiedlicher Interessenvertreter, wie z. B. aus dem Finanzsektor, von Versicherungen, Beratungsfirmen und Anwaltskanzleien, von Forschungs- und Hochschuleinrichtungen, von Nichtregierungsorganisationen und Gewerkschaften sowie von Softwareherstellern und internationalen Internetunternehmen.

Unter diesem Einfluss stand zwischenzeitlich sogar zu befürchten, dass die Datenschutz-Grundverordnung noch hinter bestehende Standards zurückfallen und sich das Europäische Parlament gegen seine eigene EntschlieÙung zum Gesamtkonzept für den Datenschutz vom Juli 2011 positionieren könnte. In dieser hatte es sich noch dafür ausgesprochen, die in der bestehenden Datenschutzrichtlinie gesetzten Grundsätze und Standards der Weiterentwicklung und Stärkung des Datenschutzrechts zugrunde zu legen. Jedoch sorgten die Enthüllungen des Whistleblowers Edward Snowden im Sommer 2013 für breite Diskussionen rund um das Thema Datenschutz und gaben den zähen Beratungen zur Datenschutz-Grundverordnung neuen Schwung.

Ende Oktober 2013 befürwortete der Innenausschuss des Europäischen Parlaments mit großer Mehrheit zahlreiche Vorschläge, die zum Teil über den Kommissionsvorschlag hinausgehen:

- An Behörden und Gerichte in Drittstaaten sollen personenbezogene Daten nur auf Grundlage europäischen Rechts oder darauf beruhender Rechtshilfeabkommen und bei voller Transparenz gegenüber den Datenschutzaufsichtsbehörden übermittelt werden dürfen. Entscheidungen seitens der Kommission zur Angemessenheit des Datenschutzniveaus in einem Drittstaat sollen auf fünf Jahre befristet werden, danach wäre die Zulässigkeit der Übermittlung erneut zu prüfen.
- Die explizite Einwilligung stellt ein wesentliches Element bei der Verarbeitung personenbezogener Daten dar. Standardisierte Symbole („Ampelprinzip“) sollen die Entscheidung für eine Zustimmung oder Ablehnung erleichtern und leicht verständlich formulierte Nutzungsbedingungen Ausführungen in unverständlichen allgemeinen Geschäftsbedingungen ersetzen. Einer Profilbildung soll grundsätzlich jeder widersprechen können. Das „Recht auf Vergessen“ wurde durch ein realistischeres „Recht auf Löschung“ ersetzt.
- Bei Verstößen soll gegenüber einem Unternehmen eine GeldbuÙe von bis zu fünf Prozent des jährlichen Umsatzes verhängt werden können.

Abhängig vom Ausmaß der Datenverarbeitung und den damit verbundenen Risiken besteht seitens der Unternehmen die Pflicht, einen betrieblichen Datenschutzbeauftragten zu bestellen.

- Am „One-Stop-Shop“-Ansatz soll festgehalten und für strittige Fragen ein noch zu gründender Europäischer Datenschutzausschuss als „Letztentscheidungsinstanz“ berufen werden. Die Ermächtigung der Kommission, zu einem späteren Zeitpunkt konkretisierende Ausführungsbestimmungen festzulegen, wurde deutlich begrenzt.

Der ausgehandelte und von einem breiten Konsens des Innenausschusses des Europäischen Parlaments getragene Kompromisstext zur Datenschutz-Grundverordnung greift viele der von der Datenschutzkonferenz angesprochenen Punkte auf.

Bevor Kommission, Rat und Parlament in die Verhandlungen zur Formulierung des endgültigen Verordnungstextes eintreten können, müssen auch die im Rat vertretenen Regierungen der Mitgliedstaaten zu einem Abschluss ihrer Beratungen kommen. Noch ist unklar, ob das Ziel, die Datenschutz-Grundverordnung noch vor den kommenden Wahlen zum Europäischen Parlament im Mai 2014 zu verabschieden, erreicht wird.

2 Technisch-organisatorische Entwicklungen

2.1 Trennung von Verfahren in gemeinsam genutzten IT-Infrastrukturen

Zur Verbesserung der Wirtschaftlichkeit des IT-Einsatzes werden bislang verteilte, dezentrale Datenverarbeitungsprozesse immer häufiger zentralisiert und konsolidiert. Die damit verbundene gemeinsame Nutzung von Hard- und Softwaresystemen für mehrere DV-Verfahren oder durch mehrere Daten verarbeitende Stellen bringt jedoch auch neue Herausforderungen für den Datenschutz und die Informationssicherheit mit sich.

Insbesondere für IT-Dienstleister ist die Zentralisierung und Konsolidierung der Datenverarbeitung von großem Interesse. Finanzielle und organisatorische Gründe führen häufig zu der Entscheidung, Hard- und Softwareressourcen nicht für jeden Kunden getrennt vorzuhalten. Stattdessen sollen mehrere Kunden die jeweiligen IT-Infrastrukturen gemeinsam nutzen. Damit jeder Kunde nur seine eigenen Daten verarbeiten kann, kommen sogenannte „mandantenfähige“ Systeme zum Einsatz. Abgesehen davon, dass es keine einheitliche Definition dieses Begriffs gibt und die konkrete technische Um-

setzung sehr vielfältig sein kann, stellt sich die Frage, ob die datenschutzrechtlichen Anforderungen durch derartige Systeme in jedem Fall eingehalten werden.

Werden in einer gemeinsamen IT-Infrastruktur personenbezogene Daten automatisiert verarbeitet, sind die Regelungen der Datenschutzgesetze zu beachten. Sowohl das Brandenburgische Datenschutzgesetz als auch das Bundesdatenschutzgesetz fordern, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten auch getrennt voneinander verarbeitet werden. Der getrennte Speicher- und Verarbeitungskontext eines Verfahrens oder einer Daten verarbeitenden Stelle wird nachfolgend als „Mandant“ bezeichnet.

Die Umsetzung des gesetzlichen Trennungsgebots führt zu einer Reihe von Anforderungen, die bei der gegenseitigen Abschottung von Verfahren in gemeinsam genutzten IT-Infrastrukturen einzuhalten sind:

- Es sind die rechtlichen Grundlagen der Verarbeitung personenbezogener Daten in der gemeinsamen IT-Infrastruktur zu prüfen. Neben dem Erfordernis einer Trennung nach unterschiedlichen Zwecken der Datenverarbeitung, nach Gruppen von Betroffenen oder nach Daten verarbeitenden Stellen kann eine solche Prüfung auch ergeben, dass aufgrund gesetzlicher Regelungen oder wegen eines besonders hohen Schutzbedarfs die Verarbeitung personenbezogener Daten in einer gemeinsamen IT-Infrastruktur ausgeschlossen ist.
- Die Trennung der Datenverarbeitung in der gemeinsamen IT-Infrastruktur bedeutet, dass jede Verarbeitung von Daten eines Mandanten in einem anderen Mandanten als Datenübermittlung (im datenschutzrechtlichen Sinne) auszugestalten ist. Für die Übermittlung bedarf es einer Rechtsgrundlage. Sie darf nur über definierte, system- oder programmtechnische Schnittstellen erfolgen und ist zu protokollieren.
- Jede Verarbeitung personenbezogener Daten in der gemeinsamen IT-Infrastruktur muss auf den jeweiligen Mandanten beschränkt bleiben. Sie darf keine Auswirkungen auf andere Mandanten haben, nicht von diesen abhängen oder auf deren Daten lesend oder schreibend zugreifen. Insbesondere dürfen Datenschutzprobleme oder Sicherheitsvorfälle in einem Mandanten nicht zu Gefährdungen in anderen Mandanten führen.
- Die Trennung der Datenverarbeitung setzt voraus, dass die Benutzerkennungen und Zugriffsrechte für jeden Mandanten separat vergeben werden. Gleiches gilt auch für Konfigurationseinstellungen. Auf diese Weise lässt sich z. B. gewährleisten, dass in unterschiedlichen Mandan-

ten jeweils spezifische Festlegungen für die Protokollierung umgesetzt werden können.

- Mandantenübergreifende Funktionen (z. B. zur Verwaltung der Mandanten selbst oder der gemeinsamen IT-Infrastruktur) sind zu beschränken. Sie dürfen grundsätzlich keine Verarbeitung personenbezogener Daten innerhalb eines Mandanten ermöglichen.

Die Trennung der Datenverarbeitung in einer gemeinsam genutzten IT-Infrastruktur kann durch verschiedene technische und organisatorische Maßnahmen erreicht werden. Diese reichen z. B. von der getrennten Speicherung der Daten in unterschiedlichen Datenbanken desselben Datenbankmanagementsystems über die Anwendung kryptographischer Mechanismen zur Abschottung oder die revisionssichere Protokollierung mandantenspezifischer und -übergreifender Aktivitäten bis hin zum Betrieb der Verfahren in unterschiedlichen virtuellen Maschinen auf derselben physischen Hardware. Die Auswahl der konkreten Maßnahmen zur Trennung der Datenspeicherung, Datenverarbeitung und Datenübermittlung muss im Rahmen des IT-Sicherheitskonzepts erfolgen. Ihre Wirksamkeit ist nachzuweisen.

Darüber hinaus sind bei der Erarbeitung des IT-Sicherheitskonzepts für die gemeinsam genutzte Infrastruktur das Maximumprinzip sowie Kumulationseffekte zu beachten: Ersteres besagt, dass der Schutzbedarf für das Gesamtsystem bestimmt wird durch die (Einzel-)Gefährdungen mit den schwerwiegendsten Auswirkungen. Letztere beschreiben die Erhöhung des Schutzbedarfs für das Gesamtsystem dadurch, dass durch Summierung mehrerer (kleinerer) Schäden ein größerer Gesamtschaden entstehen kann.

Der Problematik der Mandantentrennung widmet sich die Orientierungshilfe „Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur“, die der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet hat.¹² Zur konkreten Umsetzung für Verfahren, die in einer gemeinsamen Infrastruktur beim Zentralen IT-Dienstleister des Landes Brandenburg betrieben werden, erarbeitet das IT-Sicherheitsmanagementteam der Landesverwaltung zurzeit eine übergreifende landesweite Richtlinie.¹³

¹² siehe <http://www.lida.brandenburg.de>

¹³ siehe B 7.2

Auch wenn mehrere Daten verarbeitende Stellen eine gemeinsame IT-Infrastruktur für die automatisierte Verarbeitung personenbezogener Daten nutzen, ist das datenschutzrechtliche Trennungsgebot einzuhalten. Die neu entstehenden Risiken sowohl für die einzelnen Verfahren als auch für die zu Grunde liegende IT-Infrastruktur müssen durch geeignete technische und organisatorische Maßnahmen beherrscht werden.

2.2 Einsatz von IPv6 – Hinweise für Hersteller und Provider im Privatkundengeschäft

Der begrenzte Adressraum des Internetprotokolls in der Version 4 (IPv4) wird viele Betreiber und Anwender von Netzwerktechnik künftig dazu zwingen, das Internetprotokoll in der Version 6 (IPv6) einsetzen. Das Protokoll IPv6 bietet neue Chancen bei der datenschutzgerechten Ausgestaltung von Kommunikationsverbindungen.

Der Arbeitskreis „Technische und organisatorische Fragen des Datenschutzes“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erstellte im Berichtszeitraum eine Orientierungshilfe zum Thema „Datenschutz bei IPv6 – Hinweise für Hersteller und Provider im Privatkundengeschäft“.¹⁴ Sie ergänzt und konkretisiert die EntschlieÙung der Konferenz aus dem September 2011.¹⁵ In der Orientierungshilfe werden zusammenfassend u. a. folgende Hinweise und Empfehlungen gegeben:

- In IPv6 wird eine sichere und vertrauenswürdige Ende-zu-Ende-Kommunikation ermöglicht, ohne dass zusätzliche Verschlüsselungssoftware eingesetzt werden muss. Voraussetzung ist, dass die verwendete IPsec-Implementation starke Verschlüsselungsalgorithmen beherrscht.
- Um das Nachverfolgen des Verhaltens von Nutzern (Tracking) zu erschweren, sollen Adresspräfixe grundsätzlich dynamisch an Endkunden vergeben werden. Sollte sich ein Provider für die Vergabe eines (einzelnen) statischen Präfixes an einen Endkunden entscheiden, dann muss dieses Präfix auf Wunsch des Kunden gewechselt werden können. Hierzu muss ihm eine einfache Bedienmöglichkeit am Router oder Endgerät zur Verfügung gestellt werden. Verlangt ein Kunde ausdrücklich ein statisches Präfix, so kann auf die Wechselmöglichkeit verzichtet werden. Eine Kombination beider Modelle ist möglich.

¹⁴ siehe <http://www.lida.brandenburg.de>

¹⁵ siehe Tätigkeitsbericht 2010/2011, A 3.4

- Um den Ortsbezug von Adressen zu verringern, sollten Provider die Adressen für Einwahlknoten und sonstige Infrastrukturkomponenten zufällig aus dem gesamten ihnen zur Verfügung stehenden Adressbereich auswählen und regelmäßig wechseln.
- An Routern sollten aus Sicherheitsgründen Broadcast- und Multicast-Pakete im erforderlichen Umfang gefiltert werden.
- Privacy Extensions müssen auf Endgeräten implementiert und sollten standardmäßig eingeschaltet sein. Ist dies nicht möglich, muss eine benutzerfreundliche manuelle Wechselfrequenz für den das jeweilige Endgerät identifizierenden Teil der IPv6-Adresse (den Interface Identifier) bestehen.
- Zusätzlich sollten Betriebssystemhersteller benutzerfreundliche Konfigurationsmöglichkeiten vorsehen, mit denen Kunden die Wechselfrequenz des Interface Identifiers auf kurze Werte festlegen (z. B. alle 10 Minuten) bzw. einen Wechsel zu bestimmten Ereignissen auslösen können (z. B. beim Start des Internet Browsers oder des Rechners).
- Wünschenswert wäre darüber hinaus, dass Anwendungsprogramme gezielt eine von mehreren lokalen IPv6-Adressen nutzen und verschiedene Adressen mit unterschiedlichen Wechselfrequenzen ausstatten können. Außerdem sollten Betriebssysteme mehrere nicht zusammenhängende Präfixe verwalten können.
- Endgerätehersteller sollten ihre Produkte mit korrekt und sinnvoll vorkonfigurierten IPv6-fähigen Paketfiltern ausstatten und diese über eine leicht zu bedienende Oberfläche zugänglich machen.
- IPv6-Adressen müssen ebenso wie IPv4-Adressen als personenbezogene Daten angesehen werden. Da bei IPv6-Installationen Mechanismen zur Adressumsetzung wie Network Address Translation (NAT) oder Proxy eine geringere Rolle spielen werden, ist der Informationsgehalt der Adressen höher als bei IPv4.
- Sofern die IPv6-Adresse eines Geräts genutzt werden soll, um dessen (ungefähren) Standort zu ermitteln, gelten hierfür vergleichbare Anforderungen wie bei IPv4. Eine solche Standortermittlung ist für Provider und Diensteanbieter nur nach Anonymisierung der Adresse zulässig. Zur wirkungsvollen Anonymisierung von IPv6-Adressen sollten nach derzeitigem Kenntnisstand die unteren 88 bis 96 Bit jeder Adresse gelöscht werden.

- Der gemeinsame Betrieb von IPv6 und IPv4 auf einem Gerät (Dual-Stack-Betrieb) führt zu erhöhtem Gefahrenpotenzial und sollte möglichst vermieden werden. Dies gilt auch für die als Übergangslösung gedachten Tunnelprotokolle wie Teredo. Falls der Dual-Stack-Betrieb unbedingt erforderlich ist, muss eine sorgfältige Konfiguration und regelmäßige Aktualisierung der betroffenen Systeme sichergestellt sein.

Die Nutzung des Internetprotokolls IPv6 bietet neue Gestaltungsmöglichkeiten im Bereich des Datenschutzes und der Informationssicherheit. Die Provider im Privatkundengeschäft und die Hersteller von Netzkomponenten sind gefordert, die neuen Möglichkeiten des Protokolls IPv6 datenschutzgerecht umzusetzen.

2.3 Datenschutzgerechtes Smart Metering – eine Orientierungshilfe

Smart Meter, also intelligente Messsysteme z. B. für Strom, Gas und Wärme, waren bereits Thema unseres letzten Tätigkeitsberichts.¹⁶ Sie sollen den individuellen, tatsächlichen Energieverbrauch eines Kunden widerspiegeln, die Transparenz erhöhen und letztendlich helfen, Energie zu sparen. Bei einer hochaufgelösten Erfassung von Verbrauchswerten können jedoch auch Risiken für den Datenschutz entstehen (z. B. durch die Bildung sehr genauer Verbrauchsprofile). Die datenschutzgerechte Gestaltung der Mess- und Abrechnungsprozesse spielt deshalb eine besondere Rolle.

Die Zwecke, zu denen berechtigte Stellen personenbezogene Daten aus oder mithilfe von Messsystemen erheben, verarbeiten und nutzen dürfen, sind im Energiewirtschaftsgesetz¹⁷ (EnWG) abschließend festgelegt. Dies sind u. a. das Begründen, Ausgestalten und Ändern des Vertragsverhältnisses des Anschlussnutzers, das Messen des Energieverbrauchs, das Beliefern mit und das Einspeisen von Energie einschließlich der Abrechnung sowie die Umsetzung variabler Tarife. Näheres zur datenschutzgerechten Gestaltung der zugehörigen Prozesse ist in einer Rechtsverordnung zu regeln, die jedoch noch nicht erlassen wurde.

Die von den Datenschutzbeauftragten des Bundes und der Länder gemeinsam erstellte und im Juni 2012 veröffentlichte Orientierungshilfe¹⁸ „Datenschutzgerechtes Smart Metering“ dient als Empfehlung zur Ausgestaltung

¹⁶ siehe Tätigkeitsbericht 2010/2011, A 3.3

¹⁷ Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das durch Artikel 3 Absatz 4 des Gesetzes vom 4. Oktober 2013 (BGBl. I S. 3746) geändert worden ist

¹⁸ siehe <http://www.lda.brandenburg.de>

dieser Rechtsverordnung und gibt zahlreiche Hinweise zum datenschutzgerechten Entwurf und Betrieb der technischen Systeme. Sie zeigt, wie die zentralen Forderungen des Datenschutzes (wie Zweckbindung, Datensparsamkeit und Erforderlichkeit) beim Smart Metering berücksichtigt werden können. Dabei wird die gesamte Prozesskette vom Messen der verbrauchten Strommengen mittels Zähler über die Datenverarbeitung im Smart Meter bis zur weiteren Nutzung der Daten durch die Energielieferanten, Energieverteiler und Abrechnungsstellen betrachtet.

Jedem im Energiewirtschaftsgesetz genannten Datenverarbeitungsprozess werden in der Orientierungshilfe ein oder mehrere Anwendungsfälle (sogenannte Use Cases) zugeordnet. Jeder einzelne Anwendungsfall wird aus Datenschutzsicht analysiert und bewertet. Seine Beschreibung umfasst jeweils die beteiligten Akteure, Prozesse und Datenflüsse. Darüber hinaus werden eine Einschätzung des Schutzbedarfs bzgl. der sechs elementaren Schutzziele des Datenschutzes (Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Intervenierbarkeit, Nichtverkettbarkeit) gegeben sowie Hinweise und Empfehlungen für geeignete Maßnahmen zur Beherrschung möglicher Risiken für Datenschutz und Informationssicherheit abgeleitet.

Zusammenfassend sind beim datenschutzgerechten Smart Metering folgende Punkte zu beachten:

- Eine Verarbeitung der Smart Meter Daten darf nur erfolgen, soweit es für die im Energiewirtschaftsgesetz aufgezählten Zwecke erforderlich ist. Die strikte Zweckbindung der personenbezogenen Daten ist zu gewährleisten.
- In allen Prozessen sind so wenig personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen wie möglich. Die Intervalle zwischen den Ablesesyklen müssen so groß sein, dass aus dem Verbrauch keine Rückschlüsse auf das Verhalten der Nutzer gezogen werden können. Smart Meter Daten sollen möglichst nur anonymisiert, pseudonymisiert oder aggregiert übermittelt werden. Letztverbraucher jedoch müssen hoch aufgelöste Verbrauchsdaten lokal abrufen können. Smart Meter Daten sollen an möglichst wenige Stellen übermittelt werden. Es sind angemessene Löschfristen festzulegen, um eine Vorratsdatenspeicherung zu vermeiden.
- Zur Gewährleistung der Transparenz müssen die Kommunikations- und Verarbeitungsschritte beim Smart Metering zu jeder Zeit für den Letztverbraucher sichtbar und nachweisbar sein. Er muss Zugriffe auf Smart Meter erkennen und im Zweifel unterbinden können. Zusätzlich bedarf es

durchsetzbarer Ansprüche der Betroffenen auf Löschung, Berichtigung und Widerspruch.

- Der Letztverbraucher muss die Möglichkeit haben, einen Tarif zu wählen, bei dem möglichst wenig über seinen Lebensstil offenbart wird, ohne dass dies für seine Energieversorgung nachteilig ist.
- Es sind technische und organisatorische Maßnahmen umzusetzen, die den unzulässigen Umgang mit Daten beim Smart Metering verhindern. Messsysteme dürfen von außen nicht frei zugänglich sein. Es müssen eindeutige Profile für den berechtigten Zugang zu den Daten definiert und eingehalten werden. Anhaltspunkte hierfür bieten die Vorgaben im entsprechenden Schutzprofil und der Technischen Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik.
- Schon bei der Konzeption und Gestaltung der technischen Systeme muss die Gewährleistung des Datenschutzes berücksichtigt werden (Privacy by Design). Der Letztverbraucher muss mithilfe der Technik alle notwendigen Informationen, Optionen und Kontrollmöglichkeiten erhalten, die ihm die Kontrolle seines Energieverbrauchs und die Gestaltung seiner Privatsphäre ermöglichen, wobei der Stand der Technik nicht unterschritten werden darf. Insbesondere müssen rechtlich verbindliche Vorgaben für die Konzeption der Geräte, Verfahren und Infrastrukturen sowie für deren Betrieb geschaffen werden.

Der Einsatz intelligenter Messsysteme zur Verarbeitung personenbezogener Daten über den Verbrauch von Strom, Gas und Wärme bedarf der Beachtung gesetzlicher Vorgaben und der Anwendung datenschutzrechtlicher Grundsätze. Nur durch Einhaltung der empfohlenen Maßnahmen sind sowohl die Akzeptanz in der Bevölkerung zu erzielen als auch Datenschutz und Informationssicherheit in Smart Meter Systemen zu gewährleisten.

2.4 Neuer Standard zum Vernichten von Datenträgern

Die seit 1985 existierende Norm DIN 32757 galt lange als maßgeblicher Standard für die Vernichtung von Datenträgern. Sie bezog sich im Wesentlichen auf Papierunterlagen und war nicht mehr zeitgemäß. Mit der neuen, im Herbst 2012 veröffentlichten Norm DIN 66399 wird sowohl den aktuellen Anforderungen an die Artenvielfalt zu vernichtender Datenträger als auch dem heutigen Stand der Technik Rechnung getragen.

Die Norm DIN 66399¹⁹ enthält Vorgaben zur Vernichtung von Datenträgern unterschiedlicher Art und Schutzklassen. Ihr Ziel ist es, eine Wiederherstellung der auf den Datenträgern enthaltenen Informationen hinreichend zu erschweren oder auszuschließen. Die Norm besteht aus drei Teilen.

Im ersten Teil der Norm werden Grundlagen und Begriffe festgelegt. Hierzu gehört die Definition von drei Schutzklassen und sieben Sicherheitsstufen. Datenträger sind vor ihrer Vernichtung anhand des Schutzbedarfs der auf ihnen gespeicherten Daten einer der Schutzklassen zuzuordnen. Dabei ist Schutzklasse 1 für Datenträger mit Daten normalen Schutzbedarfs vorgesehen, Schutzklasse 2 für Datenträger mit Daten hohen Schutzbedarfs und Schutzklasse 3 für Datenträger mit Daten sehr hohen Schutzbedarfs. Hinsichtlich der Feststellung des Schutzbedarfs der Daten kann auf die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik verwiesen werden, die sich in der Praxis bewährt haben. Diesen Empfehlungen folgen auch die einheitlichen Schutzbedarfskategorien für die Landesverwaltung Brandenburg. Für die Klassifizierung von Datenträgern mit personenbezogenen Daten gelten die Hinweise zur Bestimmung des Schutzbedarfs, die wir 2010 veröffentlicht haben.²⁰

Die Sicherheitsstufen geben an, wie hoch der Aufwand für einen Angreifer ist, vernichtete Datenträger bzw. dort gespeicherte Daten wiederherzustellen und Informationen zur Kenntnis nehmen zu können. Hierbei sind die benötigte Zeit, der Aufwand und die Kosten (Material, Geräte) für Angreifer zu berücksichtigen. Die DIN 66399 unterscheidet folgende sieben Sicherheitsstufen:

¹⁹ DIN 66399: Büro- und Datentechnik – Vernichten von Datenträgern. Beuth-Verlag, 2012

²⁰ siehe Broschüre „Technische und organisatorische Aspekte des Datenschutzes“ vom November 2010, Abschnitte 3.2 und 3.3.2

Sicherheitsstufe	Erläuterung
1	für allgemeine Daten, Reproduktion mit einfachem Aufwand möglich
2	für interne Daten, Reproduktion nur mit besonderem Aufwand möglich
3	für sensible Daten, Reproduktion nur mit erheblichem Aufwand möglich
4	für besonders sensible Daten, Reproduktion nur mit außergewöhnlich hohem Aufwand möglich
5	für geheim zu haltende Daten, Reproduktion nur mit außergewöhnlich hohem Aufwand und gewerbeunüblichen Einrichtungen/Sondergeräten möglich
6	für geheim zu haltende Daten mit außergewöhnlich hohen Sicherheitsanforderungen, Reproduktion nach dem Stand der Technik unmöglich
7	für streng geheime Daten mit höchsten Sicherheitsanforderungen, Reproduktion nach dem Stand von Wissenschaft und Technik unmöglich

Weiter legt die Norm fest, dass Datenträger mit bestimmten Schutzklassen durch Verfahren mit bestimmten Sicherheitsstufen zu vernichten sind. Es gilt folgende Zuordnung:

	Sicherheitsstufen						
	1	2	3	4	5	6	7
Schutzklasse 1 – normal	x*	x*	x				
Schutzklasse 2 – hoch			x	x	x		
Schutzklasse 3 – sehr hoch				x	x	x	x

* Kombination ist nicht für personenbezogene Daten anwendbar.

Um die gesetzlichen Anforderungen zum datenschutzgerechten Löschen zu erfüllen und den zunehmenden Risiken für eine Wiederherstellung von Daten zu begegnen, empfehlen wir, Datenträger mit personenbezogenen Daten grundsätzlich mindestens nach der Sicherheitsstufe 4 zu vernichten. Für Datenträger mit personenbezogenen Daten hohen Schutzbedarfs sollte mindestens Sicherheitsstufe 5 genutzt werden.

Im zweiten Teil der DIN 66399 werden den genannten Sicherheitsstufen für sechs verschiedene Arten von Datenträgern (wie Papier, Mikrofilm, optische Datenträger wie CDs oder DVDs, magnetische Datenträger wie Disketten, elektronische Datenträger wie Flash-Speicher, Festplatten mit magnetischem Datenträger) jeweils Grenzwerte von Materialteilchengrößen zugeordnet, die bei der Vernichtung der Datenträger einzuhalten sind. So wird beispielsweise für eine Vernichtung von Papierunterlagen nach der Stufe P-3 im Wesentlichen gefordert, dass die Papierteilchen nach der Vernichtung eine Partikelgröße von maximal 320 μm^2 haben dürfen. Nach der strengeren Sicherheitsstufe P-4 ist nur eine Partikelgröße von maximal 160 μm^2 zulässig, bei der Stufe P-5 sind es maximal 30 μm^2 . Für Festplatten mit magnetischen Datenträgern verlangt eine Vernichtung nach der Stufe H-3 lediglich, dass die Festplatte mechanisch und elektronisch funktionsuntüchtig und verformt ist. Für die höhere Sicherheitsstufe H-4 muss die Festplatte zusätzlich zerkleinert sein, wobei die Partikel nicht größer als 2000 μm^2 sein dürfen, bei der Stufe H-5 beträgt die Maximalgröße 320 μm^2 .

Der dritte Teil der Norm beschreibt anhand verschiedener Varianten Anforderungen an Prozesse zur Vernichtung von Datenträgern. Insbesondere werden die erforderlichen Prozessschritte und ihre Inhalte beschrieben. Darüber hinaus werden Festlegungen für die Beauftragung externer Dienstleister mit der Vernichtung getroffen.

Daten verarbeitende Stellen sollten für die datenschutzgerechte Vernichtung von Datenträgern die Norm DIN 66399 anwenden. Hierbei sind im Vorfeld Entscheidungen zur Schutzklasse der Datenträger sowie zur Sicherheitsstufe zu treffen. Werden externe Dienstleister mit der Vernichtung beauftragt, ist die Einhaltung der Norm vertraglich sicherzustellen.

2.5 Einsatz von De-Mail bei öffentlichen Stellen

Mit dem De-Mail-Gesetz²¹ (De-Mail-G) wurde 2011 eine elektronische Kommunikationsplattform geschaffen, die im Vergleich zur herkömmlichen E-Mail einen sicheren, vertraulichen und nachweisbaren Geschäftsverkehr für jedermann im Internet sicherstellen soll. De-Mail-Dienste spielen im 2013 beschlossenen E-Government-Gesetz²² eine besondere Rolle: Das Gesetz verpflichtet Behörden des Bundes, zukünftig den elektronischen Zugang zur Verwaltung zusätzlich durch eine De-Mail-Adresse zu eröffnen. Brandenburgischen Behörden steht diese Entscheidung zwar frei. Allerdings verzeichnen wir ein zunehmendes Interesse, das sich in entsprechenden Anfragen äußert.

Möchte eine öffentliche Stelle des Landes Brandenburg einen De-Mail-Zugang für die Kommunikation mit der Verwaltung eröffnen, muss sie einerseits einen akkreditierten De-Mail-Diensteanbieter (DMDA) auswählen, der das De-Mail-Postfach bereitstellt. Die Voraussetzungen der Akkreditierung eines DMDA sind in § 18 De-Mail-G festgelegt. Danach prüft der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die Einhaltung datenschutzrechtlicher Vorschriften und erteilt dem Anbieter bei positiver Bewertung ein Datenschutzzertifikat. Die Prüfung erfolgt auf Grundlage eines Gutachtens einer anerkannten oder öffentlich bestellten oder beliehenen sachverständigen Stelle für den Datenschutz. Sie basiert auf einem im Bundesanzeiger und beim Bundesbeauftragten elektronisch veröffentlichten De-Mail-Kriterienkatalog. Weiterhin wird der DMDA u. a. daraufhin kontrolliert, ob er die technischen und organisatorischen Anforderungen für die zuverlässige und sichere Erbringung des De-Mail-Dienstes erfüllt und insoweit die Technische Richtlinie 01201 De-Mail des Bundesamtes für Sicherheit in der Informationstechnik (BSI) einhält. Ein Testat bestätigt die erfolgreiche Prüfung. Das BSI veröffentlicht eine Liste der akkreditierten De-Mail-Diensteanbieter.²³

Andererseits muss die öffentliche Stelle, die den De-Mail-Zugang eröffnen will, den Verpflichtungen nachkommen, die sich aus dem Brandenburgischen Datenschutzgesetz (BbgDSG) bei der Einführung von Verfahren zur automatisierten Verarbeitung personenbezogener Daten ergeben. Dazu zählen u. a. die Erarbeitung eines aus einer Risikoanalyse entwickelten Sicherheitskonzepts gem. § 7 Abs. 3 BbgDSG, die Umsetzung angemessener und geeigneter technischer und organisatorischer Sicherheitsmaßnahmen gem. § 10

²¹ De-Mail-Gesetz vom 28. April 2011 (BGBl. I S. 666), das durch Artikel 3 Absatz 8 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist

²² Gesetz zur Förderung der elektronischen Verwaltung vom 25. Juli 2013 (BGBl. I S. 2749)

²³ siehe <https://www.bsi.bund.de> (Themen > De-Mail > Akkreditierte DMDA)

BbgDSG sowie der Abschluss von Regelungen zur Datenverarbeitung im Auftrag gem. § 11 BbgDSG mit dem DMDA.

Insbesondere muss die Behörde gem. § 10 BbgDSG Sicherheitsmaßnahmen entsprechend dem Schutzbedarf der übertragenen De-Mail-Daten und nach dem Stand der Technik umsetzen, die geeignet sind, das mit der De-Mail-Kommunikation ggf. auftretende Risiko eines Verlustes an Vertraulichkeit zu beherrschen. Dieses Risiko der unbefugten Kenntnisnahme von De-Mail-Inhalten besteht beim DMDA, da im Verfahren keine durchgehende Ende-zu-Ende-Verschlüsselung von De-Mails vorgesehen ist: Zwar werden De-Mails zwischen den DMDAs verschlüsselt übertragen, jedoch beim DMDA entschlüsselt und liegen dort deshalb kurzzeitig im Klartext vor (u. a. zur Virenprüfung).

Aus diesem Grund ist entsprechend dem Schutzbedarf der in einer De-Mail übertragenen personenbezogenen Daten zu unterscheiden: Werden Daten mit normalem Schutzbedarf per De-Mail übertragen, hat dieses Verfahren u. a. wegen der Verschlüsselung der Datenübertragung zwischen den DMDAs, der Authentizität der Kommunikationsteilnehmer und ggf. Sende- bzw. Empfangsbestätigungen Vorteile gegenüber dem Datenversand per herkömmlicher E-Mail. Für Daten mit hohem oder sehr hohem Schutzbedarf reichen die im De-Mail-Verfahren vorgesehenen Sicherheitsmaßnahmen für die Vertraulichkeit nach unserer Auffassung jedoch nicht aus. Die Daten verarbeitende Stelle muss zusätzlich eine Ende-zu-Ende-Verschlüsselung zwischen Absender und Empfänger realisieren, um der besonderen Sensitivität der Daten ausreichend Rechnung zu tragen und eine unbefugte Kenntnisnahme auch beim DMDA auszuschließen.

Die Forderung der Datenschutzbeauftragten des Bundes und der Länder, des Bundesrats sowie von Sachverständigen in einer Anhörung im Bundestag, die Ende-zu-Ende-Verschlüsselung direkt im De-Mail-Verfahren mit vorzusehen, wurde im Gesetzgebungsverfahren nicht aufgegriffen.

Personenbezogene Daten mit hohem oder sehr hohem Schutzbedarf sind zur Wahrung der Vertraulichkeit auch bei der Nutzung des De-Mail-Verfahrens für die Kommunikation durchgängig (Ende-zu-Ende) zu verschlüsseln. Die Verantwortung für die Umsetzung trifft die jeweilige Daten verarbeitende Stelle.

2.6 Öffentliche Speicherdienste im Internet auch für die Verwaltung?

Im privaten Umfeld ist ihre Nutzung mittlerweile gang und gäbe: Speicherdienste im Internet wie z. B. Dropbox, Google Drive oder Microsoft Skydrive werden benutzt, um Dateien jederzeit und von jedem Ort aus zu bearbeiten, sie mit anderen unkompliziert auszutauschen oder eine kostengünstige Datensicherung zu realisieren. Im Berichtszeitraum wurden wir gefragt, inwieweit solche Dienste auch durch die Landes- bzw. Kommunalverwaltung verwendet werden können.

Öffentliche Stellen des Landes Brandenburg dürfen personenbezogene Daten nur dann unter Verwendung von Internetspeicherdiensten verarbeiten, wenn sie dabei Anforderungen des Brandenburgischen Datenschutzgesetzes erfüllen. Als Rechtsgrundlagen kommen entweder dessen Vorschrift zur Datenübermittlung an Dritte oder jene zur Datenverarbeitung im Auftrag in Betracht:

Für eine Datenübermittlung an Dritte fehlte es in den konkreten Fällen an der erforderlichen Rechtsgrundlage. Da es sich bei den Empfängern jeweils um Stellen außerhalb des öffentlichen Bereichs im Ausland handelte, hätten die Anforderungen von § 17 BbgDSG gegebenenfalls i. V. m. § 16 BbgDSG erfüllt sein müssen. Diese Voraussetzungen lagen nach unserer Auffassung jedoch nicht vor.

Theoretisch denkbar wäre der Abschluss eines Vertrags zwischen der öffentlichen Stelle in Brandenburg und dem ausländischen Diensteanbieter über eine Datenverarbeitung im Auftrag. Die brandenburgische Stelle bliebe dann allerdings für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich. Der Auftragnehmer müsste sich unter anderem dem Brandenburgischen Datenschutzgesetz unterwerfen, die Gewähr für die Einhaltung der erforderlichen technischen und organisatorischen Maßnahmen bieten, alle Weisungen des Auftraggebers zum Umgang mit den personenbezogenen Daten befolgen und jederzeit von ihm veranlasste Kontrollen ermöglichen. Es ist offensichtlich, dass die Verhandlungsposition brandenburgischer Behörden nicht ausreicht, um internationale Unternehmen zu derartigen Zugeständnissen zu bewegen. Auch die Datenverarbeitung im Auftrag kam somit als rechtliche Grundlage für die Verwendung von Internetspeicherdiensten nicht in Frage.

Von einer denkbaren Beschränkung der Verwendung von Internetspeicherdiensten auf nicht personenbezogene Daten ist aus unserer Sicht abzuraten. Abgesehen davon, dass durch personalisierte Zugänge zu den Speicherorten automatisch personenbezogene Daten der Beschäftigten verarbeitet würden,

kann eine öffentliche Stelle nicht in hinreichendem Maße kontrollieren, welche Daten in einem Internetspeicher abgelegt werden. Selbst wenn sie organisatorische Regelungen erlasse, um die Speicherung personenbezogener Daten zu verbieten, wären Datenschutz und Datensicherheit nicht zu gewährleisten. Wir empfehlen daher, auf die Verwendung von Internetspeicherdiensten vollständig zu verzichten.

Die Speicherung und der Austausch personenbezogener Daten auf Speicherdiensten im Internet war in den konkreten Fällen datenschutzrechtlich unzulässig. Öffentliche Stellen des Landes Brandenburg sollten auf die Nutzung solcher Angebote verzichten.

3 Arbeit und Soziales

3.1 Kostenloses Spielzeug nur gegen Hartz-IV-Bescheid

Ein gemeinnützig tätiges Unternehmen verlangte vor der kostenlosen Ausgabe von Spielzeug an Bedürftige mit Kindern die Abgabe des ALG-II-Leistungsbescheids. Dieser enthält eine Vielzahl besonders sensibler personenbezogener Daten des Leistungsempfängers. Wir wurden gebeten, diese Praxis zu überprüfen.

Unsere Nachfrage bei dem Unternehmen ergab, dass dieses teilweise die Bewilligungsbescheide kopierte. Damit verfügte es dauerhaft über verschiedene Daten zur Person des Leistungsempfängers wie z. B. das Einkommen, die Anschrift, den Geburtstag und Angaben zu weiteren Mitgliedern einer Bedarfsgemeinschaft. Zudem wurden personenbezogene Daten – unter anderem die vollständigen Geburtsdaten der Kinder der Leistungsempfänger – auf Karteikarten übertragen. Die Einsichtnahme in den Leistungsbescheid und die Anfertigung einer Kopie war nach der Auffassung des Unternehmens notwendig, um die kostenlose Ausgabe des Spielzeugs an Nichtbedürftige zu verhindern.

Das Erforderlichkeitsprinzip verlangt von der Daten erhebenden Stelle, sich auf das hierbei unerlässliche Minimum zu beschränken. Dies bedeutet, dass ausschließlich die entscheidungserheblichen Angaben zu erheben sind. Wir haben das Unternehmen darauf hingewiesen, dass personenbezogene Daten nur in dem für die Zweckerfüllung erforderlichen Umfang und auf der Grundlage einer gesetzlichen Regelung bzw. mit Einwilligung des Betroffenen erhoben und/oder gespeichert werden dürfen.

Unser Hinweis führte zu einer Änderung des Verfahrens. Kopien des ALG-II-Leistungsbescheids werden nicht mehr angefertigt. Dokumentiert werden neben dem Namen des Betroffenen und seinem Wohnort der Tag, an dem die Leistungsbewilligung abläuft sowie das Jahr und der Monat der Geburt der Kinder. Unumgänglich ist es, dass der Leistungszeitraum nachgewiesen wird. Dies kann sowohl durch Vorlage der ersten Seite des Bescheids als auch durch eine Bestätigung des Jobcenters über den Leistungsbezug erfolgen.

Zum Nachweis ihrer Bedürftigkeit genügt es, wenn die begünstigte Person ihren aktuellen Leistungsbescheid oder eine Bescheinigung über den Leistungsbezug vorlegt. Letzterem ist aus Gründen der Datensparsamkeit der Vorzug zu geben.

3.2 Fehlerhafte Datenübermittlung wegen Namensgleichheit

Immer wieder werden uns Sachverhalte bekannt, bei denen personenbezogene Daten, die dem Sozialgeheimnis unterliegen, durch öffentliche Stellen an unzuständige Dritte übermittelt wurden. Oftmals geschieht dies durch Unachtsamkeit Einzelner. Eine regelmäßige Sensibilisierung der Beschäftigten zum sorgfältigen Umgang mit Sozialdaten ist deshalb ebenso wichtig wie eine kritische Überprüfung von Verfahrensabläufen.

In einem der Fälle beantragte ein Bürger bei einem Unfallversicherungsträger Leistungen zur medizinischen Rehabilitation und ein persönliches Budget, ohne weitere Angaben zu machen. Daraufhin suchte der Letztgenannte in seinem Datenbestand nach registrierten Versicherungsfällen unter Einbeziehung der Wohnanschrift und des Nachnamens des Antragstellers. In Folge schrieb der Unfallversicherungsträger den Antragsteller an und erbat von diesem unter Angabe des Namens, Geburtsdatums und der erlittenen Verletzungen Auskunft zu den Unfällen, die sein Kind erlitten habe. Da er aber gar kein Kind hatte, war es offensichtlich, dass ihm fremde Daten übermittelt wurden.

Die falsche Zuordnung zu einer namensgleichen Person wurde durch den Unfallversicherungsträger bestätigt. Der zuständige Bearbeiter hatte es versäumt, vor der Versendung des Schreibens an den Antragsteller die Identität des Versicherten eindeutig zu klären. Nähere Angaben zur Person, wie das Geburtsdatum oder der Unfalltag, hätten zunächst abgefragt werden müssen, um eine eindeutige Zuordnung der im System gespeicherten Stammdaten sicherzustellen.

Die Übermittlung der fremden Daten an den Antragsteller war unzulässig. Bei den übermittelten Daten handelte es sich um Sozialdaten, deren Bekanntgabe an Dritte nur erlaubt ist, soweit die betroffene Person eingewilligt hat oder eine gesetzliche Befugnis vorliegt.

Der Unfallversicherungsträger entschuldigte sich für das fehlerhafte Vorgehen. Zugleich wurde intern ein Arbeitshinweis erlassen. Hiernach ist in jedem Fall vor einer Übermittlung von personenbezogenen Daten die Identität des Anfragenden zu klären. Gegebenenfalls sind zusätzliche identifizierende Merkmale, wie z. B. das Geburtsdatum, abzufragen.

Um dem Schutz des Sozialgeheimnisses gerecht zu werden, bedarf es besonderer Sorgfalt beim Umgang mit personenbezogenen Daten. Nur so können versehentliche Verwechslungen aufgrund einer Namensgleichheit vermieden werden.

3.3 Verarbeitung von Gesundheits- und Sozialdaten per Telearbeit?

Zur Flexibilisierung von Arbeitsformen und Arbeitszeiten sowie zur Verbesserung der Vereinbarkeit von Beruf und Familie plant das Landesamt für Soziales und Versorgung, seinen Beschäftigten die automatisierte Verarbeitung von Gesundheits- und Sozialdaten auch in Form von Telearbeit im häuslichen Bereich zu ermöglichen. Es ist jedoch fraglich, ob der zur Erreichung eines angemessenen Niveaus von Datenschutz und Informationssicherheit erforderliche Aufwand für die Umsetzung technischer und organisatorischer Maßnahmen vertretbar ist.

Vorgesehen ist die Telearbeit im häuslichen Bereich unter Nutzung elektronischer Kommunikationsmittel und mit Anbindung an zentrale Verfahren zur Verarbeitung von Sozial- und Gesundheitsdaten Betroffener. Zu den Prozessen, die durch Beschäftigte des Landesamtes auf diese Weise bearbeitet werden sollen, gehören u. a. die ärztliche Gutachtertätigkeit, die Bearbeitung von Einzelfällen und die Feststellung von Behinderungen nach § 69 Neuntes Buch Sozialgesetzbuch. Insgesamt ist somit von einem hohen Schutzbedarf bei der automatisierten Datenverarbeitung auszugehen.

Das Landesamt als Daten verarbeitende Stelle ist verpflichtet, die Anforderungen des Sozialgesetzbuches und des Brandenburgischen Datenschutzgesetzes (BbgDSG) für das Gesamtverfahren, d. h. unter Einbeziehung der Telearbeitsplätze im häuslichen Bereich, zu erfüllen. Zu diesen Anforderungen gehören u. a. die Erstellung eines Verfahrensverzeichnis gem. § 8 BbgDSG, die Durchführung einer Vorabkontrolle durch den behördlichen Datenschutzbeauftragten gem. § 10a BbgDSG wegen der besonderen Risi-

ken der Datenverarbeitung, die Erarbeitung eines aus einer Risikoanalyse entwickelten Sicherheitskonzeptes sowie die Umsetzung geeigneter und angemessener technischer und organisatorischer Maßnahmen zur Beherrschung der Risiken gem. § 78a Zehntes Buch Sozialgesetzbuch und dessen Anlage. Aus dem hohen Schutzbedarf ergibt sich, dass durch das Landesamt gemäß den IT-Standards des Landes Brandenburg²⁴ eine Risikoanalyse auf der Basis von IT-Grundschutz (BSI Standard 100-3) durchzuführen ist. Weiterhin sind im Vergleich zum herkömmlichen IT-Grundschutz ergänzende, weitergehende Sicherheitsmaßnahmen im Verfahren umzusetzen.

Die technischen und organisatorischen Sicherheitsmaßnahmen müssen sich auch auf die Telearbeitsplätze im häuslichen Bereich und die Kommunikationsinfrastruktur zwischen Wohnung und Dienststelle erstrecken. Diese sind besonderen Gefährdungen ausgesetzt. Die Daten verarbeitende Stelle muss durch geeignete Vorkehrungen sicherstellen, dass das Sicherheitsniveau der Büroumgebung in gleichem Maße auch am Telearbeitsplatz eingehalten wird. Kann dies nicht gewährleistet werden, darf die Telearbeit in der beabsichtigten Form nicht eingeführt werden.

Im Ergebnis unserer Beratungen mit dem Landesamt haben wir u. a. die Umsetzung folgender Maßnahmen gefordert:²⁵

- Einsatz sicherer kryptografischer Verfahren zur Ende-zu-Ende-Verschlüsselung und digitalen Signatur von Daten bei ihrer Übertragung zwischen Telearbeitsplatz und Dienststelle, Verwendung hardwarebasierter Verschlüsselungs- und Authentisierungsmechanismen,
- Nutzung einer Multifaktorauthentisierung, z. B. mittels Smartcard oder biometrischen Merkmalen und Passwort beim Zugriff auf sensitive personenbezogene Daten, Zertifizierung der Kartenlesegeräte,
- Beschränkung der auf dem Telearbeitsplatz verarbeiteten Daten auf den unbedingt erforderlichen Umfang, falls möglich ihre Anonymisierung oder Pseudonymisierung, ausschließlich verschlüsselte Speicherung personenbezogener Daten auf dem Telearbeitsplatz,
- Einsatz von Virens Scanner, Firewall und Intrusion Detection System auf dem Telearbeitsplatz, Aktivierung von Filtermechanismen, die bereits auf den untersten Schichten des ISO/OSI-Referenzmodells unberechtigte Teilnehmernummern, Adressen oder Diensteanforderungen blockieren,

²⁴ siehe B 7.3

²⁵ Diese Liste ergänzt die bereits in früheren Berichten zusammengestellten Anforderungen an Telearbeitsplätze, vgl. Tätigkeitsbericht 2008/2009, A 2.5.

- Verwendung ausschließlich dienstlicher Arbeitsplatzcomputer (APC), Nutzung des Telearbeitsplatzes nur für dienstliche Zwecke, Administration des APCs durch die Dienststelle, Verhinderung der unbefugten Nutzung externer Schnittstellen (z. B. USB-Ports), Ausschluss von Konfigurationsänderungen durch den Telearbeiter,
- sichere Aufbewahrung von dienstlichen Unterlagen und Datenträgern im häuslichen Bereich, Verhinderung des Zugriffs Unbefugter, bei Bedarf Bereitstellung von Sicherungsschränken durch die Dienststelle,
- Einbruchsschutz und Brandschutz für den häuslichen Arbeitsplatz,
- Festschreibung der erforderlichen technisch-organisatorischen Maßnahmen am Telearbeitsplatz in einer Dienstanweisung, schriftliche Verpflichtung des Beschäftigten zur Einhaltung der Maßnahmen, Schulung und Sensibilisierung des Telearbeiters zu Datenschutz und Informationssicherheit,
- schriftliche Einwilligung des Telearbeiters in Kontrollmaßnahmen im häuslichen Bereich durch den Arbeitgeber, dessen behördlichen Datenschutzbeauftragten sowie unsere Behörde.

Risiken für Datenschutz und Informationssicherheit sind auch bezüglich der verwendeten Kommunikationsinfrastruktur (Internetanbindung, Netzkomponenten) durch entsprechende Gegenmaßnahmen zu minimieren. Wir haben u. a. eine Trennung zwischen beruflichem und privatem Internetanschluss im häuslichen Bereich sowie die Absicherung der zentralen Kommunikationskomponenten wie Router oder Switches gefordert. Für Letztere empfiehlt das Bundesamt für Sicherheit in der Kommunikationstechnik als Maßnahmen z. B. die Auswahl und Beschaffung geeigneter Geräte, die sichere Konfiguration und Administration, die regelmäßige Kontrolle und Softwarepflege des Routers und die Protokollierung. Ferner haben wir das Landesamt für Soziales und Versorgung darüber informiert, dass die häufig anzutreffende Praxis der Bereitstellung und Administration des Routers durch den Telekommunikations- bzw. Internetzugangsanbieter nicht mit den hohen datenschutz- und sicherheitstechnischen Anforderungen in diesem konkreten Verfahren vereinbar ist.

Bei der automatisierten Verarbeitung hoch schutzbedürftiger personenbezogener Daten im häuslichen Umfeld ist davon auszugehen, dass eine vergleichbare Sicherheit wie bei einem Behördenarbeitsplatz nicht erreicht werden kann und damit ein hohes Restrisiko besteht. Auch vor dem Hintergrund des großen Aufwandes zur Umsetzung der erforderlichen Sicherheitsmaßnahmen sollte das Landesamt für Soziales und Versorgung genau prüfen, ob die Einführung der Telearbeit in der geplanten Form weiter verfolgt wird. Wir halten sie für nicht realisierbar und damit in letzter Konsequenz für unzulässig.

4 Banken- und Inkassowesen

4.1 Fördermittel nur bei Vorlage vollständiger Kontoauszüge?

Die Investitionsbank des Landes Brandenburg bewilligt unter anderem Fördermaßnahmen im Rahmen des europäischen Strukturfonds. Um die Nachweise über zuschussfähige Ausgaben zu prüfen, verlangte sie von den Zuwendungsempfängern, vollständige und ungeschwärzte Kontoauszüge im Original vorzulegen. Damit hätten auch personenbezogene Daten Unbeteiligter offenbart werden müssen.

Der Europäische Fonds für regionale Entwicklung (EFRE) stellt im Rahmen der europäischen Struktur- und Regionalpolitik Fördermittel bereit. Die Verwaltung dieser Mittel obliegt dem Ministerium für Wirtschaft und Europaangelegenheiten; die Investitionsbank übernimmt die Funktion der zentralen Bewilligungsbehörde.

In der Vergangenheit genügte es, wenn Zuwendungsempfänger der Investitionsbank für Prüf- und Abrechnungszwecke Rechnungslisten einreichten. Zusätzlich prüfte sie stichprobenweise die vorliegenden Rechnungsbelege. Seit dem 1. Januar 2013 forderte die Bewilligungsbehörde jedoch die Einreichung vollständiger und ungeschwärzter Kontoauszüge im Original. Gemeinden und Städte, aber auch private Einrichtungen, die Investitionsmittel aus dem Strukturfonds in Anspruch nehmen wollten, sahen sich dadurch gezwungen, nicht zuletzt personenbezogene Daten Dritter vorzulegen, die für die Prüfung der Fördermittelausreichung gänzlich irrelevant waren. Die Kontoauszüge der Kommunen gaben beispielsweise darüber Auskunft, welche Bürger zu welchem Zeitpunkt Beiträge für die Kita, Ordnungsgelder oder Steuern in welcher Höhe gezahlt hatten. Zwar bezog die Investitionsbank diese Daten nicht in die Bearbeitung ein und empfahl den Zuwendungsemp-

fängern, separate Konten nur für die Mittelverwendung zu führen. Dessen ungeachtet stellte die Verpflichtung zur Einreichung vollständiger und ungeschwärzter Kontoauszüge jedoch eine unzulässige Datenerhebung dar. Auch waren die Zuwendungsempfänger nicht berechtigt, personenbezogene Daten Dritter für diesen Zweck zu übermitteln.

Die Investitionsbank des Landes Brandenburg änderte auf Veranlassung der Landesbeauftragten zwischenzeitlich das Verfahren. Sowohl interne Arbeitsanweisungen für die Beschäftigten als auch Merkblätter für die Zuwendungsempfänger weisen nunmehr darauf hin, dass Angaben, die nicht zur Prüfung der zuschussfähigen Ausgaben erforderlich sind, geschwärzt oder anderweitig ausgesondert werden können. In diesen Fällen ist es nunmehr auch möglich, auf die Vorlage der Originale zu verzichten.

Wer Fördermittel beantragt, sollte die Buchführung so gestalten, dass separate Kontoauszüge für die nachweispflichtigen Ausgaben vorgelegt werden können. Ist dies nicht möglich, können personenbezogene Daten Dritter vor der Einreichung bei der Investitionsbank geschwärzt werden.

4.2 Auskunftsverweigerung von Inkasso Rechtsanwälten rechtmäßig?

Ein Inkasso Anwalt ist ein auf den Einzug offener Forderungen spezialisierter Rechtsanwalt. Er verwendet in seiner Tätigkeit häufig Unterlagen mit personenbezogenen Daten. Üblicherweise haben Daten verarbeitende Stellen zwar die Pflicht, Betroffene über die zu ihnen gespeicherten Daten zu informieren. Rechtsanwälte unterliegen jedoch einer anwaltlichen Schweigepflicht. In mehreren Inkasso-Fällen hatten wir zu prüfen, ob der Auskunftsanspruch oder die Schweigepflicht zum Tragen kommt.

Wenn ein Betroffener, der nicht gleichzeitig Mandant des Rechtsanwalts ist, von diesem Auskunft über die zu seiner Person gespeicherten Daten verlangt, kann sich der Rechtsanwalt auf seine Schweigepflicht berufen, soweit es sich um Informationen aus der mandatsbezogenen Tätigkeit des Anwalts handelt. Ein Verstoß gegen die anwaltliche Schweigepflicht stellt einen Straftatbestand nach § 203 Strafgesetzbuch dar. Diese Vorschrift sperrt die Anwendung des datenschutzrechtlichen Informationsanspruchs des Betroffenen nach Bundesdatenschutzgesetz. Auch besteht gegenüber der Landesbeauftragten als Aufsichtsbehörde für den Datenschutz aus demselben Grund keine Auskunftspflicht. Etwas anderes gilt nur, wenn der Mandant seinen Rechtsbeistand von der Schweigepflicht befreit hat.²⁶

²⁶ vgl. Beschluss des Kammergerichts Berlin vom 20. August 2010, 1 Ws (B) 51/07 - 2 Ss 23/07

Aus den genannten Gründen konnten wir auch den Beschwerden zu erfolgreichen Auskunftersuchen Betroffener bei den Inkasso Anwälten nicht abhelfen. Als Alternative kann ihnen nur empfohlen werden, sich unmittelbar an den Gläubiger zu wenden, der den Inkasso Anwalt beauftragt hat. Dieser kann möglicherweise selbst bestimmte Auskünfte erteilen. Der Gläubiger hat allerdings das Recht, diese zu verweigern, wenn dadurch das beabsichtigte Eintreiben von Forderungen gefährdet würde. Als Mandant kann er seinen Rechtsanwalt aber jederzeit von der Schweigepflicht entbinden.

Im Verhältnis zwischen dem Mandanten und seinem Rechtsanwalt gilt die Schweigepflicht hingegen nicht. Der Mandant kann daher seinen datenschutzrechtlichen Auskunftsanspruch gegenüber dem Anwalt geltend machen. Beschwerd er sich bei der Landesbeauftragten über den Rechtsanwalt und befreit diesen von der Schweigepflicht, kommen die Auskunftspflichten des Anwalts gegenüber der Aufsichtsbehörde für den Datenschutz zum Tragen.

Die Schweigepflicht eines Inkasso Anwalts geht den datenschutzrechtlichen Auskunftsansprüchen Betroffener vor, soweit es sich bei diesen nicht um Mandanten handelt.

4.3 Unzulässige Kontrollabfrage einer Bausparkasse bei der SCHUFA

Ein Petent beendete sein Vertragsverhältnis mit einer Bausparkasse durch vorzeitiges Zurückzahlen des ausgereichten Bauspardarlehens. Vor der Abmeldung des zugehörigen Eintrages bei der SCHUFA erfolgte dort eine Kontrollanfrage. Dabei übermittelte die Bausparkasse aber nicht nur die für eine Identitätsprüfung erforderlichen, sondern auch bonitätsrelevante Daten, wie z. B. den Scorewert mit Risikobewertungen.

Die Bausparkasse hielt es für zulässig, generell die umfassende SCHUFA-Abfrage standardmäßig zu nutzen. Die zur Abmeldung von beendeten Darlehen erfolgende Prüfung der Vertragsdaten begründete sie mit ihr aus der Praxis bekannt gewordenen Fällen fehlerhafter Abmeldungsverfahren.

Kreditinstitute dürfen zwar gem. § 28a Abs. 2 Bundesdatenschutzgesetz personenbezogene Daten u. a. über die Beendigung eines Vertragsverhältnisses betreffend ein Bankgeschäft an Auskunftsteilen übermitteln. Allerdings war im vorliegenden Fall kein Anhaltspunkt dafür gegeben, dass die Abmeldung des Darlehens bei der SCHUFA nicht ordnungsgemäß hätte erfolgen können. Die reine Kontrollabfrage war deshalb unzulässig.

Angesichts des Ziels der Abfrage, lediglich die Korrektheit der Identitätsdaten des Vertragspartners zu prüfen, ist es zudem nicht erforderlich, umfassende Informationen – z. B. auch Scorewerte – zu übermitteln. Die Daten sind auf das Minimum zu reduzieren, das für die Feststellung der Identität der bei der SCHUFA eingetragenen Person ausreicht. Außerdem darf eine solche Abfrage nur erfolgen, wenn Anhaltspunkte für Unstimmigkeiten vorliegen. Eine Regelabfrage ist, auch angesichts der in der Praxis vorkommenden geringen Fehlerzahlen, nicht erforderlich und daher unzulässig.

Im Ergebnis hat die Bausparkasse ihre Vorgehensweise geändert. Sie verzichtet im Zusammenhang mit der Abmeldung von Darlehen künftig auf Kontrollabfragen bei der SCHUFA.

Abfragen durch Kreditinstitute bei der SCHUFA sind auf das erforderliche Maß zu reduzieren. Soweit keine Anhaltspunkte für Unstimmigkeiten vorliegen, müssen Kontrollabfragen zur Prüfung der Identitätsdaten von Vertragspartnern unterbleiben.

5 Beschäftigtendatenschutz

5.1 Scheitern des Beschäftigtendatenschutzgesetzes

Der Entwurf für ein Beschäftigtendatenschutzgesetz gelangte im Berichtszeitraum zwar in die parlamentarische Beratung, eine Verabschiedung erfolgte jedoch nicht.

Nicht zuletzt die immer wiederkehrenden Vorfälle der Überwachung von Beschäftigten haben gezeigt, dass es einer klaren gesetzlichen Regelung zum Schutz ihrer personenbezogenen Daten vor und nach Begründung des Beschäftigungsverhältnisses bedarf. Bereits im Sommer 2010 hatte die Bundesregierung einen Gesetzentwurf vorgelegt, der die lückenhafte Vorschrift des § 32 Bundesdatenschutzgesetz ersetzen sollte. Hierzu unterbreiteten die Datenschutzbeauftragten des Bundes und der Länder eine Vielzahl konstruktiver Vorschläge, die aus dem unzureichenden Entwurf ein ausgewogenes Gesetz hätte werden lassen können.

Mit einem Änderungsantrag vom Januar 2013 verschlechterten die Regierungsfaktionen den Entwurf in wesentlichen Teilen sogar noch.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder kritisierte das mangelnde Datenschutzniveau der vorgesehenen gesetzlichen Regelungen. Als besonders bedenklich bewertete sie die beabsichtigte Ausweitung der offenen Videoüberwachung am Arbeitsplatz, die geplante übermäßige Überwachung von Beschäftigten in Call-Centern, die vorgesehene

Erweiterung der Datenerhebungsbefugnisse im Bewerbungsverfahren und die angestrebte Befugnis der Datenerhebung bei Dritten.²⁷

Nachdem der Änderungsantrag auch von anderer Seite heftig kritisiert wurde, entschieden die Koalitionsfraktionen, den Gesetzentwurf überhaupt nicht mehr zu beraten.

Während der Diskussion über den Gesetzentwurf wurde vereinzelt darauf verwiesen, dass es sinnvoller sei, die Verabschiedung der Datenschutz-Grundverordnung²⁸ abzuwarten. Dies erscheint jedoch nicht angebracht. Tatsächlich enthält der Verordnungsentwurf aber einen Passus, nach dem es den Mitgliedstaaten weitgehend überlassen bleiben soll, die Verarbeitung von Beschäftigten Daten selbst zu regeln.

Der bislang mangelhafte Schutz von Beschäftigten vor Überwachung, Ausforschung und widerrechtlicher Verwendung ihrer Daten im Arbeitsverhältnis kann nur durch ein spezielles Beschäftigtendatenschutzgesetz verbessert werden. Ein solches sollte in der neuen Wahlperiode so schnell wie möglich verabschiedet werden.

5.2 Rechtswidrige Personalaktenführung

Eine Beschäftigte einer großen öffentlichen Verwaltung versuchte jahrelang vergeblich, ihre Personalakte von den rechtswidrig geführten Teilen bereinigen zu lassen. Auch entsprechende Forderungen des behördlichen Datenschutzbeauftragten wurden nicht berücksichtigt. Erst nach Anrufung der Landesdatenschutzbeauftragten, deren Beanstandung und einer nochmaligen Kontrolle fand der schwere Eingriff in ihre Persönlichkeitsrechte ein Ende.

Die Verwaltung führte über die Beschäftigte eine aus drei breiten Aktenordnern bestehende Personalakte, die eine Vielzahl von rechtswidrig gespeicherten Unterlagen enthielt. Diese standen entweder nicht in einem unmittelbaren inneren Zusammenhang mit ihrem Beschäftigungsverhältnis und hätten deshalb nicht in die Personalakte aufgenommen werden dürfen. Teilweise hätte die Verwaltung Unterlagen bereits vernichten müssen, weil entweder Löschfristen abgelaufen oder die Angaben für die Aufgabenerfüllung nicht mehr erforderlich waren. Auf zahlreichen Dokumenten wurden untaugliche Schwärzungen vorgenommen, sodass in der Personalakte weitere Hinweise auf bereits entfernte Abmahnungen, arbeitsgerichtliche Streitigkeiten und

²⁷ siehe Anlage 1.4: Entschließung „Beschäftigtendatenschutz nicht abbauen, sondern stärken!“ vom 25. Januar 2013

²⁸ vgl. B 1

sogar Gesundheits- und andere Daten Dritter enthalten waren. In der Akte waren darüber hinaus durchgängig Beschwerden, Behauptungen und Bewertungen gespeichert, die ungünstig für die Beschäftigten waren und ihr nachteilig hätten werden können. Diese können zwar grundsätzlich in die Personalakte aufgenommen werden, jedoch hätte sie hierzu gehört werden müssen. Im konkreten Fall geschah dies nur äußerst selten. Der Eingriff in die Persönlichkeitsrechte der Beschäftigten war erheblich.

Nach Prüfung der Personalakte hat die Landesbeauftragte Verstöße gegen § 50 Beamtenstatusgesetz, § 94 Abs. 2 Satz 1, §§ 96, 99 Abs. 1 und § 100 Abs. 2 Landesbeamtengesetz festgestellt und die Aktenführung auf der Grundlage von § 25 Abs. 1 Brandenburgisches Datenschutzgesetz (BbgDSG) sofort beanstandet.

Die Personalverwaltung kam der Aufforderung auf Entfernung der rechtswidrig gespeicherten Unterlagen erst nach einer ein Jahr dauernden Auseinandersetzung nach. Trotz klarer Rechtslage war den Verantwortlichen insbesondere nur schwer zu vermitteln, dass auch für die Verarbeitung der Personalaktendaten von Tarifbeschäftigten gemäß § 29 Abs. 1a BbgDSG die Vorschriften des Landesbeamtengesetzes anzuwenden sind. Eine schriftliche Zusage der Verwaltung, dass die Personalakte bereinigt sei, stellte sich bei einer unangekündigten Nachkontrolle vor Ort als falsch heraus. Auch stellte die Verwaltung die Befugnisse der Landesbeauftragten in Frage, sodass sich deren Kontrolle mehr als schwierig gestaltete.

Für die Personalaktenführung von Tarifbeschäftigten gelten die Vorschriften des Landesbeamtengesetzes. Es ist rechtswidrig, willkürlich Unterlagen zur Personalakte zu nehmen und damit erheblich in Persönlichkeitsrechte von Beschäftigten einzugreifen.

5.3 Lohn- und Gehaltsabrechnung durch Steuerberater

Lohn- und Gehaltsabrechnungen für Mandanten zu erbringen, zählt zum täglichen Geschäft der Steuerberater. Zu klären war, ob es sich dabei um eine Datenverarbeitung im Auftrag handelt oder ob Steuerberater für eigene Geschäftszwecke tätig werden.

Bei einer Datenverarbeitung im Auftrag nach § 11 Bundesdatenschutzgesetz (BDSG) handelt der Auftragnehmer in Abhängigkeit von Weisungen des Auftraggebers. Letzterer hat weitreichende datenschutzrechtliche Kontrollrechte und -pflichten gegenüber dem Auftragnehmer und bleibt für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Das Tätigwerden für eigene Geschäftszwecke nach § 28 BDSG hingegen liegt bei einer sogenannten Funktionsübertragung vor: Wird einer Daten verarbeitenden Stelle

eine bestimmte Funktion übertragen, erfüllt sie diese eigenverantwortlich. Solche Aufgaben gehen über weisungsabhängige, beispielsweise technische Dienstleistungen hinaus.

Steuerberater üben, soweit sie im Rahmen des Steuerberatungsgesetzes tätig werden, keine weisungsgebundenen Aufgaben, sondern einen freien Beruf aus. Sie sind unabhängig und zu eigenverantwortlichem Handeln verpflichtet. Die Übernahme von Lohn- und Gehaltsabrechnungen für Mandanten entspricht diesem Berufsbild. Es handelt sich datenschutzrechtlich um eine Funktionsübertragung, in deren Rahmen die Steuerberater mit selbstständiger, fachlicher und intellektueller Leistung für eigene Geschäftszwecke tätig werden.

Bei der Beauftragung externer Dienstleister, die den Steuerberater unterstützen und dabei personenbezogene Daten verarbeiten, handelt es sich hingegen um eine Datenverarbeitung im Auftrag. Dies gilt z. B. bei der Einschaltung eines Rechenzentrums, bei der Wartung eines EDV-Systems oder bei der Entsorgung von Datenträgern. Der Steuerberater ist dann als Auftraggeber für die Datenverarbeitung verantwortlich und muss die Einhaltung der entsprechenden Vorschriften des Bundesdatenschutzgesetzes mit dem Dienstleister vertraglich vereinbaren.

Lohn- und Gehaltsabrechnungen erbringen Steuerberater datenschutzrechtlich gesehen für eigene Geschäftszwecke. Eine Datenverarbeitung im Auftrag erfolgt allerdings, wenn sie zur Unterstützung dieser Tätigkeiten externe Dienstleister in Anspruch nehmen.

5.4 Überwachung von Firmenfahrzeugen mittels GPS

Uns erreichen häufig Anfragen zur Zulässigkeit der Ausrüstung von Firmenfahrzeugen mit GPS-Empfängern. Dabei ist für die Arbeitnehmer von Interesse zu erfahren, ob der Arbeitgeber mit einem solchen System den Arbeitsplatz überwachen darf und ob Ortungsdaten auch bei privater Verwendung des Fahrzeugs erhoben, verarbeitet oder genutzt werden dürfen, wie etwa in Pausen oder nach Feierabend.

Es ist einem Arbeitgeber nicht von vornherein verboten, GPS bei Firmenwagen einzusetzen und die gewonnenen Daten für bestimmte Zwecke zu nutzen. Rechtsgrundlage hierfür ist § 32 Abs. 1 Satz 1 Bundesdatenschutzgesetz. Hiernach dürfen personenbezogene Daten eines Beschäftigten für die Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn sie für dessen Durchführung erforderlich sind.

Eine GPS-Ortung ist aber nur dann zulässig, wenn sie in Kenntnis der Mitarbeiter erfolgt, ein legitimer Zweck vorliegt und schutzwürdige Interessen der Beschäftigten nicht überwiegen. Dabei ist zu beachten, dass die Zweckbestimmung begrenzt und schriftlich festgehalten wird, wozu die Überwachung erfolgen soll. Legitime Zwecke können beispielsweise die Überwachung der Arbeitszeit oder der erlaubten Nutzungsart, die Unterstützung der Koordination des externen Kundendienstes, die Senkung von Verwaltungsaufwand o. Ä. sein. Dabei muss sich der Arbeitgeber – vorausgesetzt, der Einsatz von GPS ist wirklich erforderlich – strikt an den schriftlich festgelegten Zweck halten.

Unzulässig ist eine permanente Überwachung der Mitarbeiter sowohl während der Arbeitszeit als auch außerhalb, wenn etwa der Firmenwagen privat genutzt werden darf. Der Arbeitgeber hat beim Einsatz von GPS-Systemen die schutzwürdigen Interessen der Beschäftigten insofern zu beachten, als er Technik verwenden muss, die ein Ausschalten der Überwachung (z. B. bei Pausen und nach Feierabend) ermöglicht. Die Überwachung darf im Übrigen in Hinblick auf Art und Ausmaß nicht unverhältnismäßig sein.

Die Speicherdauer der durch GPS gewonnenen Daten richtet sich nach dem jeweiligen Zweck und den hierfür geltenden gesetzlichen Aufbewahrungsfristen.

Der Einsatz von GPS in Firmenfahrzeugen muss so transparent wie möglich erfolgen, d. h. die Beschäftigten sind über den Umfang und die Dauer der Datenverarbeitung vor Nutzung der Fahrzeuge zu informieren. Soweit möglich, sollten der Einsatz von GPS-Systemen sowie die innerbetrieblichen Kontrollbefugnisse in einer Betriebsvereinbarung geregelt werden.

Unter engen Voraussetzungen kann der Einsatz von GPS in Firmenwagen erlaubt sein. Eine Überwachung in Pausen oder nach Feierabend ist unzulässig.

5.5 Mit dem Fingerabdruck den Arbeitstag beginnen?

Im Berichtszeitraum erreichten uns verschiedene Anfragen von Beschäftigten, in deren Unternehmen jeweils Fingerabdrucksysteme eingeführt werden sollten. In mehreren Fällen ging es hierbei um die elektronische Erfassung der Arbeitszeiten mittels Fingerabdruck, in einem Fall um die Kontrolle des Zutritts von Beschäftigten zu Betriebsräumen. Ein Arbeitgeber wollte die Abgabe der Fingerabdrücke seiner Beschäftigten sogar erzwingen und drohte im Falle der Weigerung mit einer Abmahnung für die Betroffenen.

Fingerabdrücke gehören wie z. B. die Gesichtsgeometrie, Irismuster, Handvenenstruktur u. a. zu den körperlichen Merkmalen einer Person. Im Rahmen biometrischer Verfahren werden diese Merkmale gemessen und ausgewertet, um sie einer konkreten Person zuzuordnen.²⁹ Hierfür müssen die biometrischen Daten zuvor erfasst und digital gespeichert werden. Die Speicherung kann in Form von Rohdaten (z. B. als vollständige Bilddatei) oder als Template erfolgen. Bei Letzterem werden nur die jeweils wesentlichen, charakteristischen Merkmale extrahiert und gespeichert (z. B. bestimmte Punkte und Linien des Bildes). Biometrische Daten haben häufig einen hohen Schutzbedarf, da sie z. T. Rückschlüsse auf weitere, sensitive Informationen über die jeweilige Person zulassen (wie z. B. auf den Gesundheitszustand) und das Missbrauchspotenzial erheblich sein kann.

Da Fingerabdrücke wie alle biometrischen Daten unzweifelhaft personenbezogen sind, müssen bei ihrer Verarbeitung die jeweils geltenden datenschutzrechtlichen Regelungen eingehalten werden. Insbesondere haben Unternehmen die Festlegungen zum Beschäftigtendatenschutz im Bundesdatenschutzgesetz (BDSG) zu beachten. So dürfen gem. § 32 Abs. 1 BDSG personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses nur erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.

An die Bedingung der „Erforderlichkeit“ sind dabei hohe Anforderungen zu stellen. Insbesondere darf es kein weniger in die Persönlichkeitsrechte der Beschäftigten eingreifendes Mittel geben, das gleich gut geeignet wäre und den beabsichtigten Zweck erfüllt. Das ist aber für die Arbeitszeiterfassung in der Regel gerade nicht der Fall: Hierfür reicht es beispielsweise aus, die Zeiten aufzuschreiben (analog auf einem Papierzettel oder digital in einer Tabellenkalkulation). Zur Automatisierung der Zeiterfassung wäre auch die Nutzung einer personalisierten Chipkarte an einem entsprechenden Kartenlesegerät (ggf. mit PIN) denkbar. In beiden Fällen müssten die Beschäftigten ihre sensiblen Fingerabdruckdaten nicht an den Arbeitgeber herausgeben.

Für die Kontrolle des Zutritts kann es jedoch auch Ausnahmen geben, bei denen das Interesse des Unternehmens am Schutz von Betriebsanlagen, Geräten, Geschäftsgeheimnissen u. Ä. oder die Gewährleistung der öffentlichen Sicherheit schwerer wiegen und die Persönlichkeitsrechte der betroffenen Beschäftigten deshalb zurücktreten müssen. So können z. B. Unternehmen oder Unternehmensbereiche mit sehr hohen Sicherheitsanforderungen (wie Forschungs- und Produktentwicklungsabteilungen, Rechenzentren,

²⁹ vgl. Tätigkeitsbericht 2006/2007, A 2.2

militärische Bereiche) einer besonders strengen und überwindungssicheren Kontrolle des Zutritts von Berechtigten bedürfen. Hierfür kann im Einzelfall und bei entsprechender Abwägung der unterschiedlichen Rechte auch die Verwendung von Fingerabdruck- oder anderen biometrischen Daten der Beschäftigten zulässig sein.

Wenn die Frage der Zulässigkeit der Erhebung, Verarbeitung und Nutzung biometrischer Daten der Beschäftigten positiv beantwortet wurde, gilt es, das zugehörige automatisierte Verfahren datenschutzgerecht zu gestalten. Hierbei sind u. a. die Grundsätze der Datensparsamkeit (z. B. durch Speicherung der biometrischen Daten in Form von Templates), der strikten Zweckbindung und der Transparenz (z. B. durch detaillierte Information der Beschäftigten) einzuhalten. Wegen des hohen Schutzbedarfs biometrischer Daten müssen geeignete und angemessene technische und organisatorische Maßnahmen gem. § 9 BDSG und dessen Anlage 1 realisiert werden, um die mit der Datenverarbeitung verbundenen Risiken des Missbrauchs wirksam zu beherrschen. Regelmäßig ist bei biometrischen Verfahren auch eine Vorabkontrolle durch den betrieblichen Datenschutzbeauftragten gem. § 4d Abs. 5 BDSG durchzuführen.

Sollte in dem betreffenden Unternehmen ein Betriebsrat existieren, ist die Einführung und Anwendung einer elektronischen Zeiterfassung oder eines automatisierten Zutrittskontrollsystems nach § 87 Abs. 1 Betriebsverfassungsgesetz darüber hinaus auch mitbestimmungspflichtig.

Die Verarbeitung biometrischer Daten von Beschäftigten (wie z. B. des Fingerabdrucks) bedarf einer vorherigen detaillierten Prüfung unter Berücksichtigung des informationellen Selbstbestimmungsrechts der Beschäftigten. Wenn sie für den konkreten Zweck im Ausnahmefall erforderlich ist, sind in dem zugehörigen DV-Verfahren umfassende technische und organisatorische Maßnahmen umzusetzen, die den Missbrauch der Daten wirksam verhindern.

6 Gesundheit

6.1 Gesetz zur Stärkung der Patientenrechte

Anfang 2012 legten die zuständigen Bundesministerien einen gemeinsamen Entwurf für ein Gesetz zur Verbesserung der Rechte von Patientinnen und Patienten vor. Die bisher durch die Gerichte entwickelten Grundsätze des Arzthaftungs- und Behandlungsrechts sollten im Bürgerlichen Gesetzbuch geregelt werden. In den neuen Vorschriften finden sich unter anderem Informations- und Dokumentationspflichten für die Behandelnden sowie ein Akteneinsichtsrecht für die Betroffenen.

Die Bundesministerien der Justiz und für Gesundheit berücksichtigten eine gemeinsame Stellungnahme der Datenschutzbeauftragten zu dem vorgelegten Referentenentwurf nur unzureichend. Unter brandenburgischem Vorsitz wandte sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder daher mit einer EntschlieÙung an die Öffentlichkeit.³⁰ Sie forderte u. a., bei den Dokumentationspflichten auch Lösungsansprüche der Patienten zu bedenken und bei der Einschränkung des Akteneinsichtsrechts der Betroffenen die Einschränkungsgründe zu präzisieren bzw. deutlich zu machen, dass es dabei letztlich um eine Abwägung verschiedener Grundrechte geht. Die Konferenz empfahl insbesondere eine Harmonisierung der Rechte der Betroffenen mit den allgemeinen Datenschutzgesetzen oder Landeskrankenhausesetzen. Unsere Forderungen blieben jedoch auch im Verlauf der Gesetzgebung weitgehend unberücksichtigt. Das Patientenrechtegesetz trat am 26. Februar 2013 in Kraft.³¹

Das Gesetz zur Verbesserung der Rechte von Patientinnen und Patienten bleibt aus datenschutzrechtlicher Sicht hinter den Erwartungen zurück, die sein Name weckt.

³⁰ siehe Anlage 1.6.3: EntschlieÙung „Patientenrechte müssen umfassend gestärkt werden“ vom 23. Mai 2012

³¹ Gesetz zur Verbesserung der Rechte von Patientinnen und Patienten vom 20. Februar 2013 (BGBl. I Nr. 9)

6.2 Honorarkräfte in Gesundheitsämtern

Im Zusammenhang mit Beschwerden von Betroffenen wurden wir darauf aufmerksam, dass in den Landkreisen teilweise ehemalige Mitarbeiter des Gesundheitsamtes als Honorarkräfte beschäftigt werden. Diesbezügliche Verträge wurden häufig datenschutzrechtlichen Anforderungen nicht in vollem Umfang gerecht. In einem Fall hatte der freie Mitarbeiter sogar elektronische Zugriffsmöglichkeiten, die über seine Untersuchungsvorgänge weit hinausgingen.

Es ist zunächst in jedem Fall zu klären, wer Auftraggeber des freien Mitarbeiters ist. Bei der Aufgabenerfüllung für verschiedene Ämter (z. B. Gesundheitsamt und Jugendamt) ist eine getrennte Aufbewahrung von Unterlagen bzw. Dateien der verschiedenen Auftraggeber sicherzustellen. An die Verträge mit der Honorarkraft sind nach § 11 Abs. 5 Brandenburgisches Datenschutzgesetz bestimmte Anforderungen zu stellen, wie z. B.

- die Zweckbindung für überlassene Daten,
- die Festlegung der erforderlichen technisch-organisatorischen Maßnahmen für den Datenschutz und die Wahrung der ärztlichen Schweigepflicht oder
- der Ausschluss von Unterauftragsverhältnissen.

Die Nutzung von Räumen des Gesundheitsamtes wie z. B. Untersuchungszimmer durch die Honorarkraft darf nicht dazu führen, dass diese Kenntnis personenbezogener Daten aus anderen Fällen erlangt. Die Zugriffsmöglichkeit auf solche Patientendaten ist durch technisch-organisatorische Maßnahmen auszuschließen.

Für Kontrollen im häuslichen Bereich der Honorarkraft ohne ihre Zustimmung bestehen angesichts des Grundrechts auf Unverletzlichkeit der Wohnung keine gesetzlichen Grundlagen. Datenverarbeitungen oder auch nur die vorübergehende Aufbewahrung von Unterlagen bzw. Datenträgern an diesem Ort dürfen nur zugelassen werden, wenn eine schriftliche Einwilligung des freien Mitarbeiters in Kontrollmöglichkeiten durch den Landkreis und unsere Dienststelle vorliegt. Ansonsten sind sie auszuschließen.

Eine sichere Aufbewahrung von Patientendaten des Gesundheitsamtes oder in dessen Auftrag erstellte Unterlagen bzw. Datenträger im häuslichen Bereich der Honorarkraft bzw. unterwegs muss gewährleistet sein. Angehörige, Besucher oder sonstige Dritte dürfen keinen Zugang dazu erhalten. Unter anderem müssen Sicherungsschränke sowie für den Transport verschließba-

re Koffer zum Einsatz kommen. Auch ist festzulegen, dass datenschutzrechtlich relevante Vorfälle dem Landkreis umgehend zu melden sind.

Greifen Gesundheitsämter auf die Mitarbeit von Honorarkräften zurück, sind in den Verträgen mit diesen auch eine Reihe datenschutzrechtlicher Regelungen zu treffen. Dabei gilt es unter anderem, die nötigen technisch-organisatorischen Maßnahmen zum Schutz der von ihnen zu bearbeitenden personenbezogenen Daten zu treffen.

6.3 Antragsformular für Wohngruppenzuschlag

Seit Ende des Jahres 2012 erhielten wir verschiedene Hinweise auf ein Antragsformular der AOK Nordost zur Gewährung eines Wohngruppenzuschlags, das insbesondere wegen der Abfrage personenbezogener Daten von Mitbewohnern und Pflegenden kritisiert wurde.

§ 38a Elftes Buch Sozialgesetzbuch regelt den Anspruch auf zusätzliche Leistungen für Pflegebedürftige in ambulant betreuten Wohngruppen. Mit dem Wohngruppenzuschlag sollen die Betroffenen in die Lage versetzt werden, eine Präsenzkraft für organisatorische, verwaltende oder pflegerische Tätigkeiten zu beschäftigen. Eine Voraussetzung der Sozialversicherungsleistung ist das gemeinschaftliche Wohnen von mindestens drei Pflegebedürftigen der Pflegestufen 1 bis 3. Deshalb erfragte die AOK Namen, Pflegekasse und Pflegestufe der Mitbewohner und ließ sich diese Angaben durch deren Unterschrift bestätigen. Für den Fall, dass die Grundpflege und hauswirtschaftliche Versorgung bereits durch Privatpersonen erfolgte, wurden deren Namen, Anschriften und Telefonnummern erfragt. Auch die sog. Präsenzkraft sollte ihre Wohnanschrift offenbaren und ebenso durch Unterschrift bestätigen.

Wir halten im Normalfall eine Bestätigung des Antragstellers über das Vorhandensein von mindestens zwei geeigneten Mitbewohnern für ausreichend. Durch die Forderung nach Unterschriften der Mitbewohner auf dem Antragsformular wären möglicherweise auch Daten des Antragstellers (zumindest seine Pflegeversicherung) an diese offenbart worden. Außerdem besteht für die Mitbewohner weder Pflicht noch Befugnis, der Pflegeversicherung eines anderen Auskunft über eigene Daten zu erteilen – ein Antrag könnte damit daran scheitern, dass ein Mitbewohner seine Auskunft verweigert bzw. weil er dement ist, diese gar nicht geben kann, sodass durch die Einbeziehung seines Betreuers die Antragstellung zumindest verzögert wird.

Die Krankenkasse erklärte sich zwischenzeitlich bereit, auf die Unterschriften der Mitbewohner zu verzichten. Von der Präsenzkraft wird zwar weiterhin eine Anschrift gefordert, dies kann jedoch auch die dienstliche Adresse sein.

Auf Angaben zu privaten Pflegepersonen wird in dem überarbeiteten Formular ganz verzichtet.

Wir vertreten weiter die Auffassung, dass der Antragsteller nur mitzuteilen hat, dass zwei Mitbewohner mit der geforderten Pflegestufe vorhanden sind. Konkretere Angaben zu diesen Personen halten wir nur in besonderen Ausnahmefällen für erforderlich. Die Diskussion über die Ausgestaltung des Formulars dauert noch an.

Die datenschutzgerechte Ausgestaltung von Formularen wirft immer wieder Fragen zur Erforderlichkeit auf. Besonders problematisch sind Angaben über andere Personen als den Antragsteller, vor allem, wenn diese keine Mitwirkungspflicht trifft.

6.4 Das Projekt „Agnes 2“

Um die medizinische Versorgung und Betreuung insbesondere im ländlichen Raum zu verbessern, werden seit einigen Jahren verschiedene Modellprojekte durchgeführt. Hierzu gehört auch Agnes 2 – ein Vorhaben, bei dem Tablet-Computer mit entsprechender Software als mobile Endgeräte für die Verarbeitung von Patientendaten zum Einsatz kommen. Wir wurden von der AOK Nordost als zuständiger Stelle frühzeitig in das Projekt eingebunden.

Beim Projekt Agnes (Arztentlastende, gemeindenahe, E-healthgestützte, systemische Intervention) werden delegierbare ärztliche Leistungen zu Hause beim Patienten durch nicht-ärztliches medizinisches Fachpersonal (wie z. B. Gemeindeschwestern) erbracht. In enger Abstimmung mit dem behandelnden Arzt kümmern sich die Agnes-Fachkräfte um besonders betreuungsintensive Patienten. Sie koordinieren u. a. Arzttermine, vermitteln Pflegedienste, überwachen die häusliche Krankenpflege und sind Ansprechpartner für Angehörige. Bei Hausbesuchen werden Krankheitszustände dokumentiert und diese Informationen dann dem jeweiligen Arzt vorgelegt.

Agnes 1 kam als Pilotprojekt nur in medizinisch unterversorgten Gebieten zum Einsatz. Bei Agnes 2, welches sich derzeit in der Aufbauphase befindet, sollen die Agnes-Fachkräfte überall im Land Brandenburg tätig werden. Weiter gilt auch in Agnes 2: Die Teilnahme für den Patienten ist freiwillig. Das Muster der erforderlichen Einverständniserklärung für die Patienten wurde u. a. aufgrund unserer Hinweise und Empfehlungen datenschutzgerecht ausgestaltet.

Während bisher die Agnes-Fachkräfte schriftliche Notizen anfertigen, wenn sie im Auftrag des Arztes beim Patienten tätig sind, werden zukünftig patien-

tenbezogene Daten auf einem Tablet-Computer verarbeitet. Hierzu wurde die Technische Universität Berlin beauftragt, eine entsprechende Applikation, die Agnes 2-App, für Android-Tablets zu entwickeln. Folgende Funktionen soll die Anwendung u. a. aufweisen:

- Bereitstellung eines Kalenders, Termin- und Aufgabenverwaltung,
- Kontakt- und Patientenverwaltung,
- Druckfunktion und
- Synchronisation der Daten mit einem Arbeitsplatz-PC.

Wir haben bereits frühzeitig darauf hingewiesen, dass bei der Verarbeitung von sensiblen personenbezogenen Daten in dem Verfahren besondere technische und organisatorische Maßnahmen zu realisieren sind. In einem umfassenden Datenschutzkonzept wurden daraufhin diese Maßnahmen ausführlich beschrieben und aufgrund unserer Hinweise und Empfehlungen eine aus datenschutzrechtlicher Sicht tragbare Lösung entwickelt. Eine wichtige Forderung war die verschlüsselte Speicherung der personenbezogenen Daten auf dem Tablet. Nur so kann gewährleistet werden, dass die Daten auch bei Verlust des Gerätes nicht in fremde Hände geraten. Die implementierten Verschlüsselungsverfahren entsprechen dem aktuellen Stand der Technik.

Die auf dem Tablet gespeicherten sensiblen personenbezogenen Daten sollten anfänglich auf einem von dem Unternehmen Google betriebenen Server gesichert werden (Backup Service), eine nach Auffassung der Verantwortlichen kostengünstige und effiziente Lösung. Wir hielten diese Verfahrensweise jedoch für unzulässig: Obwohl die Daten verschlüsselt auf dem Sicherungsserver gespeichert werden sollten, wäre nicht auszuschließen, dass ausländische Sicherheitsbehörden auf sie zugreifen und sie entschlüsseln. Wir schlugen den Projektverantwortlichen daher vor, die Daten auf dem lokalen Computer der Agnes-Fachkräfte verschlüsselt zu sichern. Das Verfahren wurde dementsprechend angepasst.

Bei der Verarbeitung von sensiblen personenbezogenen Daten auf tragbaren Endgeräten (z. B. Tablet-Computern) sind technische und organisatorische Maßnahmen zu ergreifen, die einen Missbrauch dieser Daten ausschließen. Eine verschlüsselte Speicherung der Daten ist dabei unabdingbar.

6.5 Pseudonymisierung bei integrierter Versorgung

Ein brandenburgisches Unternehmen informierte uns Ende 2011 über ein integriertes Versorgungsprojekt für Patienten mit chronischen Rückenschmerzen und bat um eine datenschutzrechtliche Beurteilung.

Die Patienten sollten mit einem Pseudonym in einer gemeinsamen Datenbank der beteiligten Ärzte und Therapeuten geführt werden. Das Pseudonym enthielt unter anderem an festgelegter Stelle die Initialen und das Geburtsjahr der Betroffenen. Dem Unternehmen, das die Datenbank pflegen sollte, war der Aufbau des Pseudonyms bekannt, da es das Projekt entwickelt hatte.

Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen, um für Unbefugte die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren. Wir hatten erhebliche Zweifel an der datenschutzgerechten Bildung des Pseudonyms, weil eine Personenbeziehbarkeit für Unbefugte nicht ausgeschlossen werden konnte. Jedoch hatte das Unternehmen zum Zeitpunkt unserer Beteiligung die Weichen bereits gestellt und eine andere technische Lösung war nicht mehr möglich.

Wir hielten es deshalb für erforderlich, den Patienten in der Einwilligungserklärung zur Datenverarbeitung nicht nur mitzuteilen, dass die behandelnden Ärzte und Therapeuten ihre Daten untereinander austauschen. Wegen der ungeeigneten Pseudonyme hätten die Patientendaten im Zweifel auch von Dritten den Betroffenen zugeordnet werden können. Die Ärzte bzw. Therapeuten waren darüber hinaus von ihrer Schweigepflicht nach § 203 Abs. 1 Strafgesetzbuch zu entbinden.

Die Pseudonymisierung ist ein hilfreiches Mittel, wenn es darum geht, dass Befugte auch nachträglich Angaben sicher einer Person zuordnen können. In der Praxis stellen wir jedoch häufig fest, dass es sich die Verwender von Pseudonymen zu einfach machen, sodass die Bestimmung des konkreten Betroffenen für Unbefugte nicht wesentlich erschwert ist.

6.6 Ambulante Netzhaut-Glaskörperchirurgie

Im Berichtszeitraum befassten wir uns mit einem integrierten Versorgungsvertrag zwischen der Innungskrankenkasse Brandenburg und Berlin sowie der Augenärztegenossenschaft Brandenburg e. G. für ausgewählte operationsbedürftige Augenerkrankungen.

Die Augenärztegenossenschaft ist sowohl für die Abrechnung mit den teilnehmenden Augenärzten als auch für eine Qualitätssicherung der Leistungen

zuständig. Abrufe aus einer gemeinsamen Dokumentation der behandelnden Leistungserbringer sollten neben diesen auch den Vertragspartnern, also der Krankenkasse und der Genossenschaft möglich sein.

Nach § 140a Abs. 2 Satz 5 Fünftes Buch Sozialgesetzbuch darf der betroffene Krankenversicherte nur den Leistungserbringern Abrufe der Behandlungsdaten und Befunde aus der gemeinsamen Patientendokumentation erlauben. Infolge unserer Intervention verzichten die Krankenkasse und die Genossenschaft auf die Berechtigung zu eigenen Abrufen.

Auch wurden aufgrund unserer Empfehlungen die Hinweise zur Einwilligungserklärung vervollständigt. Weiter bemühten sich die Vertragspartner um eine bessere Pseudonymisierung bzw. Anonymisierung der Patientendaten. Es darf der Genossenschaft z. B. nicht möglich sein, bei Daten, die sie für die Qualitätssicherung erhält, den Patientenbezug wiederherzustellen.

Der Gesetzgeber ermöglicht es den Krankenkassen und Leistungserbringern, mithilfe integrierter Versorgungsprojekte neue Wege zu gehen. Auch dabei sind jedoch Grundsätze des Datenschutzes zu wahren.

7 Informationstechnik in der Landesverwaltung

7.1 Zur Zukunft des IT-Einsatzes in der Landesverwaltung

Bereits in unserem letzten Tätigkeitsbericht³² hatten wir angemahnt, dass sich die Landesregierung dringend der erforderlichen Fortschreibung der IT-Strategie der Landesverwaltung widmen muss. Wir hatten kritisiert, dass fehlende strategische Planungen und Entscheidungen mittel- und langfristig auch zu einer Senkung des Niveaus an Informationssicherheit und Datenschutz beim IT-Einsatz führen können. Was hat sich in den vergangenen zwei Jahren in diesem Punkt getan?

In ihrer Stellungnahme³³ zu unserer Kritik verwies die Landesregierung in drei knappen Zeilen lediglich darauf, dass die Fortschreibung der IT-Strategie sich nicht losgelöst vom Aufbau des Brandenburgischen IT-Dienstleisters (ZIT-BB) betrachten lasse. Die festgestellten Verzögerungen seien in deutlichem Umfang durch die unerwarteten Schwierigkeiten beim seit 2008 laufenden Aufbau des ZIT-BB entstanden. Keine Aussage traf die Landesregierung

³² siehe Tätigkeitsbericht 2010/2011, A 10.1

³³ siehe Landtags-Drucksache 5/5636 vom 9. Juli 2012

jedoch dazu, ob und wann bzw. auf welche Weise die IT-Strategie fortgeschrieben werden soll.

Wir hatten daraufhin wiederholt angeregt, das Thema im Beratungs- und Entscheidungsgremium der IT-Beauftragten der Ressorts, dem RIO-Ausschuss, zu behandeln. Hierzu kam es jedoch erst im Frühjahr bzw. Herbst 2013, als der Ausschuss in zwei Klausursitzungen damit begann, sich mit den zukünftigen Zielen und Entwicklungslinien für den IT-Einsatz in der Landesverwaltung intensiver auseinanderzusetzen.

In den dortigen Diskussionen spielten die Perspektiven für den Brandenburgischen IT-Dienstleister eine wesentliche Rolle. Als Schwerpunkte wurden u. a. die Konsolidierung der historisch gewachsenen, sehr heterogenen IT-Infrastruktur sowie die konsequente Standardisierung und Optimierung von Prozessen bei der Erbringung von Dienstleistungen identifiziert. Allerdings reicht eine Konzentration auf die Weiterentwicklung des ZIT-BB nicht aus. Eine tragfähige Zukunftsstrategie für den IT-Einsatz in der Landesverwaltung muss darüber hinaus nach unserer Ansicht auch weitere Aussagen enthalten und detailliert mit Maßnahmen untersetzen, z. B.

- zu Planungen für die Einführung bzw. Weiterentwicklung von ressortübergreifenden und Querschnittsverfahren der Datenverarbeitung,
- zu zentralen Vorhaben im Rahmen des E-Government,
- zur Weiterentwicklung des operativen und strategischen Informationssicherheitsmanagements in der Landesverwaltung,
- zur breiteren Anwendung von aktuellen Sicherheitsmechanismen wie Ende-zu-Ende-Verschlüsselung, digitalen Signaturen, Multifaktorauthentisierung oder Single SignOn,
- zur Einbindung mobiler Endgeräte und zum sicheren mobilen Arbeiten,
- zum Umgang mit aktuellen technischen Entwicklungen wie IPv6, Cloud Computing, serviceorientierten Architekturen, De-Mail oder Dienstleistungsportalen für Bürger oder Beschäftigte,
- zur Ebenen übergreifenden IT-Zusammenarbeit mit dem Bund bzw. Kommunen u. a. m.

Bereits diese Aufzählung zeigt die engen Bezüge der Inhalte der IT-Strategie zu Aspekten des Datenschutzes und der Informationssicherheit.

Die Festlegung der wesentlichen Entwicklungsziele des IT-Einsatzes in der Landesverwaltung und der Wege zur Erreichung dieser Ziele innerhalb der IT-Strategie muss durch die Landesregierung selbst erfolgen. In der Vergangenheit war es häufig der Brandenburgische IT-Dienstleister, der im Rahmen von Projekten oder durch kundenspezifische Einzeldienstleistungen die Entwicklungslinien bestimmte. Dies spiegelt sich auch an verschiedenen Stellen der IT-Standards des Landes³⁴ wider, in denen nur abstrakt auf das „entsprechende Produkt“ des ZIT-BB verwiesen, dieses jedoch nicht konkret benannt (und damit standardisiert) wird. Hinzu kommt, dass gerade bei kurzfristig von Kunden nachgefragten und vom Dienstleister erbrachten Leistungen immer wieder zu beobachten war, dass Grundfragen des Datenschutzes und der Informationssicherheit nicht hinreichend beachtet wurden. Hierzu zählen beispielsweise die rechtzeitige und vollständige Umsetzung von IT-Sicherheitsmaßnahmen vor der Produktivsetzung, die datenschutzgerechte Gestaltung des Verfahrens selbst oder die Erfüllung formaler datenschutzrechtlicher Anforderungen wie die Freigabe des Verfahrens, der Abschluss eines Vertrages zur Datenverarbeitung im Auftrag oder die Vorabkontrolle durch den behördlichen Datenschutzbeauftragten.

Nach unserer Ansicht ist es auch erforderlich, bereits zu Beginn der Umsetzung der Strategie die notwendigen zeitlichen, personellen und finanziellen Ressourcen zu planen und deren Bereitstellung langfristig zu sichern. Hierbei muss die weitere Entwicklung des Brandenburgischen IT-Dienstleisters und der von ihm betriebenen IT-Infrastruktur besonders berücksichtigt werden. In der Vergangenheit waren diesbezüglich innerhalb der Landesverwaltung mehrfach Mängel festzustellen, die zu einer Verzögerung von Projekten oder zu deren Abbruch führten. Beispielhaft zu nennen sind hier ein im Berichtszeitraum erarbeiteter Maßnahmenplan zur Beseitigung der wichtigsten technischen und organisatorischen Defizite beim ZIT-BB, dessen Umsetzung wegen fehlender Ressourcen seit über einem Jahr ruht, oder die nach wie vor unklare Perspektive zur langfristigen Unterbringung des Rechenzentrums selbst.

Die Gewährleistung eines ordnungsgemäßen IT-Betriebs in der Landesverwaltung umfasst auch die Sicherstellung von Datenschutz und Informationssicherheit. Im Rahmen der Fortschreibung der IT-Strategie muss sich die Landesregierung den Herausforderungen der modernen Informationsgesellschaft stellen und in die Zukunft gerichtete Schlussfolgerungen für den IT-Betrieb der Verwaltung ziehen. Die Formulierung der Ziele und Entwicklungslinien ist durch eine Bereitstellung der für die Umsetzung erforderlichen Ressourcen – insbesondere für den Brandenburgischen IT-Dienstleister – zu flankieren.

³⁴ siehe B 7.3

7.2 IT-Sicherheitsmanagement in der Landesverwaltung

Das IT-Sicherheitsmanagementteam ist das zentrale Koordinierungsgremium zu Fragen der Informationssicherheit in der Landesverwaltung. Ihm gehören die IT-Sicherheitsbeauftragten der Ressorts an, die Leitung obliegt dem IT-Sicherheitsmanager des Landes. Unsere Behörde wirkt in dem Gremium seit seiner Gründung beratend mit.

Obwohl das IT-Sicherheitsmanagementteam bereits seit 2008 besteht, gab es bislang keine Geschäftsordnung für seine Arbeit. Diese wurde im Berichtszeitraum jedoch erforderlich, um Abstimmungs- und Entscheidungsprozesse zu formalisieren und die Verbindlichkeit zu erhöhen. Die Geschäftsordnung wurde unter Berücksichtigung der Festlegungen in der E-Government- und IT-Organisationsrichtlinie sowie der IT-Sicherheitsleitlinie für die Landesverwaltung verabschiedet.

In den vergangenen beiden Jahren führte das IT-Sicherheitsmanagementteam seine Arbeit kontinuierlich fort.³⁵ So wurden z. B. Fragen der Informationssicherheit in landesweiten DV-Projekten erörtert, Sicherheitsvorfälle analysiert und entsprechende Konsequenzen gezogen sowie der weitere Aufbau des zentralen Sicherheitsinformationssystems für die Landesverwaltung beim Brandenburgischen IT-Dienstleister (ZIT-BB) begleitet. Im Mittelpunkt der Aktivitäten stand jedoch die Erarbeitung und Verabschiedung landesweit einheitlicher technischer und organisatorischer Richtlinien für die Informationssicherheit. Der intensive Diskussionsprozess fand dabei in Arbeitsgruppen unter Federführung des ZIT-BB statt. Im Ergebnis liegen Richtlinien u. a. für folgende Bereiche vor:

- Schutz vor Viren und anderer Schadsoftware: Die Richtlinie beschreibt, wie im Informationsverbund der Landesverwaltung der Virenschutz gewährleistet wird. Hierzu erfolgt eine Klassifizierung der IT-Systeme, deren Einstufung in Gefährdungsklassen und die Definition mehrerer Schutzzonen. Für jede Schutzzone werden geeignete Maßnahmen des Virenschutzes vorgesehen.
- Absicherung von Netzübergängen: Zur Abschottung des Kernnetzes der Landesverwaltung von Fremdnetzen sind Firewalls einzusetzen. Die Richtlinie enthält u. a. eine Klassifikation der Fremdnetze hinsichtlich ihrer Vertrauenswürdigkeit und Konsequenzen für die Architektur und die erforderlichen Sicherheitswirkungen der jeweils einzusetzenden Firewalls.

³⁵ siehe Tätigkeitsbericht 2010/2011, A 10.2

- Regelungen zu Passwörtern: Neben grundlegenden Festlegungen zu Passwörtern (wie Länge, Zeichenvorrat, Häufigkeit der Änderung) für IT-Systeme in der Landesverwaltung enthält die Richtlinie Aussagen zur Hinterlegung von Passwörtern für bestimmte Rollenträger und Notfälle sowie zu Verfahren für die Rücksetzung von Passwörtern, falls Nutzer diese vergessen haben.
- Fernwartung von Benutzerarbeitsplätzen: Im Zuge der Übertragung von Aufgaben auf den Brandenburgischen IT-Dienstleister hat dieser auch die Betreuung von Arbeitsplatz-PCs der Benutzer in den Ressorts übernommen. In der Richtlinie wird u. a. geregelt, welche Anforderungen an die Fernwartung der PCs durch den Dienstleister zu erfüllen sind, welche Rechte und Pflichten Wartungspersonal sowie Benutzer haben und wie Wartungsvorgänge protokolliert werden.

Aktuell befasst sich das IT-Sicherheitsmanagementteam u. a. mit der Erarbeitung einer Richtlinie zur Mandantentrennung von Verfahren, die beim Brandenburgischen IT-Dienstleister für die Landesverwaltung betrieben werden, und setzt dabei auch die entsprechende Orientierungshilfe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder um.³⁶

Zusätzlich wurde eine Arbeitsgruppe für Grundsatzfragen eingerichtet, die sich frühzeitig mit ausgewählten Zukunftsthemen der Informationssicherheit in der Landesverwaltung befassen soll. Zu den ersten Schwerpunkten dieser Arbeitsgruppe gehören z. B. die Einführung von IPv6³⁷ sowie des sicheren Namensdienstes DNSsec im Landesverwaltungsnetz oder die sicherheitstechnischen Auswirkungen des Trends, private mobile Endgeräte auch für dienstliche Zwecke verwenden zu wollen.³⁸

Die Abstimmung und Vorbereitung von Entscheidungsgrundlagen in Arbeitsgruppen des IT-Sicherheitsmanagementteams hat sich bewährt. Bereits beschlossene Richtlinien müssen nun zügig durch die Ressorts und den Brandenburgischen IT-Dienstleister umgesetzt werden. Weitere landesweit einheitliche Richtlinien sind unter Berücksichtigung der Themen, die in der Arbeitsgruppe für Grundsatzfragen identifiziert wurden, zu erarbeiten.

³⁶ siehe B 2.1

³⁷ siehe Tätigkeitsbericht 2010/2011, A 3.4

³⁸ siehe A 2

7.3 Novellierung der IT-Standards für die Landesverwaltung

Gemäß der IT-Standardisierungsrichtlinie des Landes Brandenburg sind die geltenden IT-Standards jährlich zu überprüfen und fortzuschreiben. Nach ihrer ersten Veröffentlichung im Jahr 2004 wurden die Standards 2008, 2010 und 2012 aktualisiert. Welche Neuigkeiten bringt die letzte Novellierung?

Mit den IT-Standards werden ressortübergreifend grundlegende Techniken (Protokolle, Schnittstellen, Datenformate und Methoden) sowie konkrete Implementationen (Produkte und Verfahren) für den Einsatz der Informationstechnik in der Landesverwaltung festgelegt. Ziele sind neben der Erhöhung der Wirtschaftlichkeit und der Sicherheit von Verfahren auch die Vereinheitlichung und Gewährleistung der Kompatibilität beim IT-Betrieb. Die IT-Standards sind als Anlage 2 Bestandteil der IT-Standardisierungsrichtlinie des Landes.

Bei ihrer Aktualisierung im Jahr 2012³⁹ stand neben der inhaltlichen Weiterentwicklung auch eine strukturelle Anpassung der IT-Standards im Vordergrund. Insbesondere waren die Arbeiten zur IT-Standardisierung auf Bundesebene zu beachten, die unter dem Namen SAGA (Standards und Architekturen für E-Government-Anwendungen) zusammengefasst werden. Die aktuelle Version SAGA 5 zeichnet sich durch ihren modularen Charakter, die größere Flexibilität bei der Fortschreibung, eine höhere Verbindlichkeit sowie die Möglichkeit domänen- oder fachspezifischer Spezialisierungen aus. Letzteres führte zu der neuen Bezeichnung „SAGA de.bb 5.0.0“ für die aktuellen IT-Standards der Landesverwaltung Brandenburg.

Aus Sicht des Datenschutzes und der Informationssicherheit ist es als positiv zu bewerten, dass eine Reihe von Festlegungen für die Landesverwaltung als verbindlich in den IT-Standards verankert wurden. Hierzu gehören:

- Bei der Gewährleistung der Informationssicherheit muss der IT-Grundschutz auf Basis der Empfehlungen in den Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und den BSI-Grundschutzkatalogen in der jeweils aktuellen Fassung gewährleistet werden.

³⁹ Richtlinie über die Anwendung der IT-Strategie und von IT-Standards in der Landesverwaltung Brandenburg vom 15. Juni 2004, zuletzt geändert durch die Bekanntmachung vom 12. Dezember 2012 (ABl. 09/13 S. 505)

- Für das Erstellen von Sicherheitskonzepten müssen die methodischen Vorgaben des BSI in den BSI-Standards 100-1 bis 100-4 beachtet werden.
- Die Feststellung des Schutzbedarfs muss auf Grundlage festgelegter, landesweit einheitlicher Schutzbedarfskategorien erfolgen.⁴⁰
- Zur Abschottung des Kernnetzes der Landesverwaltung von anderen Netzen müssen Firewalls eingesetzt werden, deren Sicherheitswirkung in Abhängigkeit von der Vertrauenswürdigkeit der Fremdnetze steigt.⁴¹ Eine separate Firewall ist jeweils erforderlich zur Abschottung von Sicherheitsdomänen, in denen Daten mit hohem oder sehr hohem Schutzbedarf verarbeitet werden.
- Bei der Datenübermittlung in Weitverkehrsnetzen (z. B. dem Landesverwaltungsnetz) müssen Daten normalen Schutzbedarfs bezüglich der Vertraulichkeit mit einer Netzverschlüsselung (d. h. zwischen Ausgangspunkt des lokalen Quellnetzes und Eingangspunkt des lokalen Zielnetzes) gesichert werden. Bei Daten mit hohem oder sehr hohem Schutzbedarf sollte eine Ende-zu-Ende-Verschlüsselung vorgesehen werden.

SAGA de.bb ist bei Beschaffung, Erstellung und Weiterentwicklung von IT-Systemen der Landesverwaltung anzuwenden. Die Vorgaben der Standards gelten für alle neuen IT-Systeme direkt und in vollem Umfang. Für bestehende IT-Systeme gelten sie nur für Erweiterungen des Funktionsumfanges, welche ggf. zu kapseln sind. Unabhängig davon sollte jedoch für das gesamte bestehende IT-System geprüft werden, ob die Umsetzung der aktuellen Vorgaben von SAGA de.bb möglich und vorteilhaft ist.

Die Verankerung von Mindestanforderungen für die Informationssicherheit in den IT-Standards des Landes Brandenburg ist grundsätzlich zu begrüßen. Im Rahmen der regelmäßigen Fortschreibung der Dokumente sind die Inhalte an die technische Entwicklung sowie an geänderte Gefährdungslagen anzupassen.

⁴⁰ siehe Tätigkeitsbericht 2010/11, A 10.2

⁴¹ siehe B 7.2

7.4 Technische Kontrolle beim Brandenburgischen IT-Dienstleister

Im Berichtszeitraum führten wir eine von den einzelnen Fachverfahren unabhängige, mehrtägige Kontrolle der Informationstechnik beim Brandenburgischen IT-Dienstleister (ZIT-BB) durch. Diese zeigte Mängel bei der Umsetzung technisch-organisatorischer Maßnahmen auf.

Der ZIT-BB ist zentraler IT-Dienstleister für die unmittelbare Landesverwaltung. Er betreibt u. a. das Landesrechenzentrum und das Landesverwaltungsnetz (LVN). Die Kontrolle beschränkte sich auf die interne Informationstechnik und Datenverarbeitung. In den nachfolgenden Betrachtungen sind die wesentlichen Ergebnisse zusammengefasst.

7.4.1 Erstellung von IT-Sicherheitskonzepten

Vor dem erstmaligen Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, ist von der Daten verarbeitenden Stelle zu untersuchen, ob von diesen Verfahren spezifische Risiken für die Rechte und Freiheiten der Betroffenen ausgehen können. Die Freigabe eines automatisierten Verfahrens darf gem. § 7 Abs. 3 Brandenburgisches Datenschutzgesetz (BbgDSG) nur erteilt werden, wenn ein aus einer Risikoanalyse entwickeltes IT-Sicherheitskonzept ergeben hat, dass diese Risiken durch technisch-organisatorische Maßnahmen nach § 10 Abs. 1 und 2 BbgDSG beherrscht werden können. Entsprechend der technischen Entwicklung ist die Ermittlung der zu treffenden technischen und organisatorischen Maßnahmen in angemessenen Abständen zu wiederholen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt in seinen Standards 100-2 und 100-3 die Vorgehensweise bei der Erstellung von IT-Sicherheitskonzepten und gibt in den IT-Grundschiebkatalogen Empfehlungen zu geeigneten Sicherheitsmaßnahmen. In der IT-Sicherheitsleitlinie und den IT-Standards des Landes⁴² wurde die Anwendung dieser Dokumente für die Landesverwaltung als verbindlich erklärt.

Die uns vom ZIT-BB vorgelegten IT-Sicherheitskonzepte befanden sich zum Teil noch in Bearbeitung. Die Analyse der Dokumente ergab gute Ansätze bei der Etablierung eines umfassenden IT-Sicherheitsprozesses. Die Empfehlungen des BSI zur Vorgehensweise wurden beachtet. Die abgeleiteten Sicherheitsmaßnahmen müssen nun konsequent und vollständig umgesetzt werden.

⁴² siehe B 7.3

Auf Grund der Komplexität der zu betrachtenden IT-Verbünde und Verfahren müssen aus unserer Sicht dem IT-Sicherheitsbeauftragten des ZIT-BB und den an der Umsetzung der jeweiligen Sicherheitsmaßnahmen beteiligten Mitarbeitern zur Erfüllung ihrer Aufgaben mehr Ressourcen zur Verfügung gestellt werden. Die befragten Beschäftigten brachten mehrfach zum Ausdruck, dass aufgrund der Überleitung von IT-Aufgaben aus den Ressorts der Landesverwaltung zum ZIT-BB, der Heterogenität der genutzten IT-Infrastruktur sowie der parallel stattfindenden Konsolidierungsbemühungen beim Dienstleister der größte Anteil ihrer Arbeitszeit allein für die reine Aufrechterhaltung des IT-Betriebes aufgebracht werden muss.

7.4.2 Datenschutzbeauftragter des ZIT-BB

Der behördliche Datenschutzbeauftragte hat gem. § 7a Abs. 5 BbgDSG die Aufgabe, die Daten verarbeitende Stelle bei der Ausführung der Datenschutzvorschriften zu unterstützen und die Realisierung von technischen und organisatorischen Maßnahmen zu überprüfen. Er hat weiterhin die Aufgabe, die Vorabkontrolle nach § 10a BbgDSG vorzunehmen. Eine Vorabkontrolle ist für solche Verfahren zur automatisierten Verarbeitung personenbezogener Daten durchzuführen, von denen besondere Risiken für die Rechte und Freiheiten der Betroffenen ausgehen können.

Die Prüfung der Rechtmäßigkeit einer Datenverarbeitung und die Kontrolle der zu realisierenden technischen und organisatorischen Maßnahmen kann der behördliche Datenschutzbeauftragte nur dann durchführen, wenn er fachlich dazu in der Lage ist und ihm genügend Zeit zur Wahrnehmung seiner Funktion zur Verfügung steht. Aufgrund der vielfältigen Aufgaben, die der Datenschutzbeauftragte des ZIT-BB bewältigen muss, forderten wir die Befreiung von anderen Fachaufgaben. Der ZIT-BB hat zwischenzeitlich eine neue behördliche Datenschutzbeauftragte benannt und ihr mehr Ressourcen zur Erfüllung ihrer Aufgaben zur Verfügung gestellt.

7.4.3 Verfahrensverzeichnisse

Für Verfahren, mit denen personenbezogene Daten automatisiert verarbeitet werden, ist gem. § 8 BbgDSG ein Verfahrensverzeichnis zu erstellen. In dem Verzeichnis sind wesentliche Informationen über das Verfahren und seine datenschutzrechtlichen bzw. -technischen Eigenschaften zusammenzustellen. Diese Informationen umfassen z. B. die Zweckbestimmung und Rechtsgrundlage des Verfahrens, die betroffenen Personengruppen, die verarbeiteten Daten bzw. Datenkategorien, geplante Datenübermittlungen sowie eine Zusammenfassung der technischen und organisatorischen Sicherheitsmaßnahmen.

In Vorbereitung unserer Prüfung wurde uns vom ZIT-BB eine Übersicht über die erstellten Verfahrensverzeichnisse übersandt. Während der Prüfung wurden die Verfahrensverzeichnisse auf Vollständigkeit und Aktualität überprüft. Der größte Teil der uns vorgelegten Verfahrensverzeichnisse entsprach den gesetzlichen Anforderungen.

7.4.4 Organisations- und Dienstanweisungen

Gem. § 10 BbgDSG sind neben technischen auch organisatorische Maßnahmen festzulegen und umzusetzen, um den Datenschutz zu gewährleisten. Ein Großteil der uns vorgelegten Organisations- und Dienstanweisungen war veraltet und stark überarbeitungsbedürftig. So wurde beispielsweise in der „Dienstanweisung für den Einsatz von Informationstechnik im Landesamt für Datenverarbeitung und Statistik Brandenburg“ vom 29. Juni 2000 noch eine Mindestpasswortlänge von 6 Zeichen gefordert. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) fordert schon seit Jahren eine Passwortlänge von mindestens 8 Zeichen. Wir forderten den ZIT-BB auf, die Organisations- und Dienstanweisungen zeitnah zu überarbeiten und dem aktuellen Stand der Technik anzupassen.

7.4.5 Gebäude- und Raumsicherung

Zu den Serverräumen erhalten nur berechtigte Mitarbeiter Zutritt. Die installierten Brand- und Einbruchmeldeanlagen sind zum Pförtnerdienst des ZIT-BB, der rund um die Uhr besetzt ist, aufgeschaltet. Im Falle eines Alarms wird der Leiter vom Dienst des ZIT-BB informiert, der dann weitere Entscheidungen trifft.

In zwei Serverräumen entsprachen die Stromversorgung sowie die zur Kühlung der Technik benötigte Klimaanlage nicht dem Stand der Technik. Berichtet wurde, dass in heißen Sommermonaten die Klimaanlage auf dem Dach des Gebäudes manuell mit Wasser gekühlt werden muss, um einen Ausfall des Klimasystems zu verhindern. Wir sahen hier dringenden Handlungsbedarf: Gem. § 10 Abs. 2 Nr. 3 BbgDSG sind technische und organisatorische Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Sicherstellung der Verfügbarkeit).

Weiterhin existierte für die Serverräume kein Notfallkonzept. Ein Ausfallrechenzentrum ist bis heute nicht vorhanden. Bei einer Havarie in den Räumen wären nicht nur die Server des ZIT-BB selbst betroffen, sondern auch diejenigen der diversen Querschnitts- und Fachverfahren des Landes. Beim Ausfall dieser Technik wären weite Teile der Landesverwaltung nur noch eingeschränkt arbeitsfähig.

Erschwerend kommt hinzu, dass der Mietvertrag für den Standort des ZIT-BB ausläuft. Zur Gewährleistung der Planungssicherheit des ZIT-BB muss der schon seit Jahren geplante Neubau eines modernen Rechenzentrums forciert werden.

7.4.6 Fileserver des ZIT-BB

Auf dem Fileserver des ZIT-BB befinden sich u. a. die Home-Verzeichnisse der Nutzer, die Dezernatsverzeichnisse und die Verzeichnisse von Projektgruppen. Die Passwortrestriktionen für die Benutzer entsprachen unseren Forderungen. Die minimale Passwortlänge der administrativen Zugänge und Dienstkonten sollte jedoch mindestens 14 Zeichen betragen.

Die Vergabe von Zugriffsrechten sollte revisionssicher protokolliert werden. Zum Zeitpunkt der Kontrolle war es nur mit einem unverhältnismäßig hohen Aufwand möglich, die konkreten Rechte eines Benutzers zu ermitteln und zu dokumentieren. Das Serverbetriebssystem Windows 2008 stellt hierzu nur sehr rudimentäre Funktionen zur Verfügung. Darüber hinaus empfehlen wir dringend, zusätzliche Rechtemanagementsoftware zu beschaffen, mit der die Berechtigungen administriert und dokumentiert werden können. Weiterhin forderten wir die Erstellung und Umsetzung eines Virenschutzkonzepts für die Fileserver.

7.4.7 Kommunikationsserver des ZIT-BB

Auf dem zentralen Kommunikationsserver werden neben den E-Mail-Postfächern der Beschäftigten des ZIT-BB selbst auch Postfächer von Mitarbeitern anderer Daten verarbeitenden Stellen (u. a. verschiedener Ministerien) ohne wirksame Trennung gespeichert. Diese gemeinsame Speicherung von Postfächern auf einem Server halten wir für unzulässig. Die Datenverarbeitung muss gem. § 7 Abs. 1 Satz 3 BbgDSG so organisiert sein, dass bei der Verarbeitung die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist. Im Rahmen der Konsolidierung der E-Mail-Systeme in der Landesverwaltung sind deshalb die Postfächer der verschiedenen Daten verarbeitenden Stellen schnellstmöglich auf separaten physischen oder virtuellen Servern abzulegen.

Weiterhin bemängelten wir, dass Softwaretests derzeit im Produktivsystem durchgeführt werden. Dadurch können Störungen nicht ausgeschlossen werden. Zur Sicherstellung der Verfügbarkeit forderten wir die Installation von Testsystemen.

7.4.8 Datenträgerentsorgung

Auszusondernde Datenträger (u. a. Festplatten, CDs, DVDs) wurden zum Zeitpunkt der Kontrolle zentral in einem Raum in verschlossenen Behältern gelagert und bei Bedarf von einer Entsorgungsfirma datenschutzgerecht entsorgt. Der Raum war verschlossen und nur durch Berechtigte zu betreten.

Der ZIT-BB hat mit der betreffenden Entsorgungsfirma einen Datenträgervernichtungsvertrag abgeschlossen. In diesem Vertrag werden zwar die technischen und organisatorischen Maßnahmen im Rahmen der Entsorgung beschrieben. Da nicht ausgeschlossen werden kann, dass sich auch sensitive personenbezogene Daten auf den Datenträgern befinden, forderten wir die vertragliche Festschreibung einer gem. der geltenden DIN-Norm (zurzeit DIN 66399) geeigneten Sicherheitsstufe⁴³ für die Vernichtung. Der ZIT-BB hat das Dokument zwischenzeitlich entsprechend angepasst.

7.4.9 Intranet des ZIT-BB

Auf das hausinterne Intranet des ZIT-BB konnten zum Zeitpunkt der Kontrolle grundsätzlich alle am Landesverwaltungsnetz angeschlossenen Einrichtungen zugreifen. Dieser Sachverhalt war den meisten befragten Mitarbeitern nicht bekannt. Im Intranet wurde eine Vielzahl von internen Dokumenten (u. a. Dienstanweisungen, Informationen des Personalrates, Gebäudegrundrisse) zum Abruf bereitgehalten.

In der Dienstvereinbarung über die Einführung eines WebOrganigramms (WebOrg) wird in § 2 Abs. 1 u. a. ausgeführt, dass die in WebOrg eingegebenen Daten ausschließlich im Hausnetz des ZIT-BB zugänglich sind. Die vorgefundene Verfahrensweise stellte einen Verstoß gegen diese Dienstvereinbarung dar. Wir forderten den ZIT-BB auf, den Zugriff auf das Verfahren WebOrg umgehend auf die Mitarbeiter des ZIT-BB zu beschränken. Die Maßnahme wurde vom ZIT-BB zeitnah umgesetzt.

7.4.10 Sicherheit der Arbeitsplatzcomputer

Während der Kontrolle wurde ein Arbeitsplatzcomputer (APC) des Personaldezernates geprüft. Der APC war mit einem Virens Scanner ausgestattet, der auch automatisch aktualisiert wurde. Erforderliche Sicherheitsupdates wurden automatisch eingespielt, um Sicherheitslücken des Betriebssystems schnellstmöglich zu schließen. Die Passwortvergabe entsprach den derzeitigen Anforderungen: Der Nutzer musste ein mindestens 8-stelliges Passwort verwenden, welches nach spätestens 90 Tagen zu ändern war.

⁴³ siehe B 2.4

Wir empfehlen, aufgrund der Vielzahl von Passwörtern, die sich Nutzer im ZIT-BB für diverse Fachanwendungen merken müssen, zur Erhöhung der Sicherheit zukünftig eine Single-Sign-On-Anmeldung auf Chipkartenbasis zu realisieren.

Die externen Schnittstellen der APCs waren zum Zeitpunkt der Kontrolle im ZIT-BB nicht gesperrt. Die Nutzer konnten damit z. B. USB-Geräte oder CD/DVD-Laufwerke frei verwenden. Diese Verfahrensweise stellt ein erhebliches Sicherheitsrisiko dar. Es kann nicht ausgeschlossen werden, dass Daten unberechtigt kopiert werden. Um eine missbräuchliche Nutzung auszuschließen, forderten wir, die externen Schnittstellen der APCs zentral zu administrieren und nur im erforderlichen Maße freizugeben.

Im Personaldezernat werden sensitive personenbezogene Daten (Personal-daten) verarbeitet und zurzeit unverschlüsselt zentral auf dem Fileserver gespeichert. Auf diese Weise ist es möglich, dass die jeweiligen Daten auch durch andere Mitarbeiter (wie z. B. Administratoren) unberechtigt eingesehen oder manipuliert werden. Durch den Einsatz kryptographischer Verfahren (z. B. symmetrische und asymmetrische Verschlüsselung, digitale Signatur) ließe sich dieser Missbrauch verhindern. Derartige Verfahren sind heute Stand der Technik und können mit vertretbarem Aufwand eingesetzt werden. Mindestens folgende Verzeichnisse sollten nach unserer Ansicht auf dem Fileserver verschlüsselt werden:

- Verzeichnis, in dem Personaldaten gespeichert werden,
- Verzeichnis, in dem Haushaltsdaten gespeichert sind,
- Verzeichnis des behördlichen Datenschutzbeauftragten,
- Verzeichnis des Personalrates,
- Verzeichnis der Gleichstellungsbeauftragten.

Der ZIT-BB hat uns in seiner Stellungnahme zum Prüfbericht mitgeteilt, dass die erforderlichen Maßnahmen im Rahmen des geplanten Konsolidierungsprojektes mit betrachtet werden.

7.4.11 Telekommunikationsanlage

Im ZIT-BB kommt für die Telekommunikation flächendeckend Voice over IP (VoIP) zum Einsatz. Die Daten und Signalisierungsströme wurden zum Zeitpunkt der Kontrolle verschlüsselt. Es ist aus Sicht des Datenschutzes und der Informationssicherheit zwingend erforderlich, diese Verfahrensweise auch bei

der zurzeit in der Ausschreibung befindlichen neuen VoIP-Anlage beizubehalten.

Der ZIT-BB sollte die Erstellung des IT-Sicherheitskonzeptes unter Berücksichtigung der BSI-Standards 100-2 und 100-3 zügig abschließen. Die daraus resultierenden Maßnahmen müssen konsequent, vollständig und zeitnah umgesetzt werden.

8 Inneres

8.1 Bundesmeldegesetz

Das Meldewesen ist seit der Föderalismusreform im Jahr 2006 nicht mehr Länderangelegenheit, sondern unterliegt der Gesetzgebungskompetenz des Bundes. Der Deutsche Bundestag hat ein Bundesmeldegesetz⁴⁴ beschlossen, welches am 1. Mai 2015 in Kraft tritt und von den Ländern unmittelbar anzuwenden ist.

Zwar sah der Regierungsentwurf zu den Melderegisterrückkünften in einigen Fällen bereits datenschutzfreundliche Regelungen vor (Einwilligung zu Zwecken der Werbung und des Adresshandels), jedoch blieben wesentliche Forderungen der Datenschutzbeauftragten unberücksichtigt. Beispielsweise wurden weder die Hotelmeldepflicht abgeschafft noch auf die Mitwirkung des Wohnungsgebers bei der Anmeldung verzichtet.

Selbst die datenschutzfreundlichen Regelungen des Regierungsentwurfs hatten nicht lange Bestand: Am 28. Juni 2012 beschloss der Deutsche Bundestag ein Gesetz, das nunmehr nur noch eine Widerspruchslösung bei Melderegisterrückkünften zu Werbe- oder Adresshandelszwecken vorsah.

Die Datenschutzbeauftragten des Bundes und der Länder forderten den Bundesrat auf, das Gesetz in der vom Bundestag beschlossenen Form abzulehnen.⁴⁵ Auf Antrag Brandenburgs sowie neun weiterer Länder beschloss der Bundesrat, den Vermittlungsausschuss anzurufen. Der Antrag hatte u. a. zum Inhalt, dass für die Melderegisterrückkünfte zu Zwecken des Adresshandels und der Werbung wieder die Einwilligung der Betroffenen vorliegen muss. Im Ergebnis der Tätigkeit des Vermittlungsausschusses wurde ein

⁴⁴ Artikel 1 des Gesetzes zur Fortentwicklung des Meldewesens vom 3. Mai 2013 (BGBl I S. 1084)

⁴⁵ siehe Anlage 1.6.1: Entschließung „Melderecht datenschutzkonform gestalten!“ vom 22. August 2012

Meldegesetz verabschiedet, das im Wesentlichen die von der Bundesregierung formulierten Regelungen wieder aufgegriffen hat. Weitergehende Vorschläge der Datenschutzbeauftragten fanden keine Berücksichtigung.

Das Bundesmeldegesetz wird das Landesmeldegesetz zum großen Teil ablösen. Im Gesetzgebungsverfahren konnte erreicht werden, dass es für einfache Melderegisterauskünfte zu Zwecken der Werbung und des Adresshandels einer Einwilligung der Betroffenen bedarf.

8.2 Brandenburgische Personenstandsverordnung

Die Brandenburgische Personenstandsverordnung⁴⁶ ermöglicht den Standesämtern erstmalig, das neu bei der Stadt Cottbus eingerichtete zentrale Personenstandsregister zu nutzen. Die Landesbeauftragte hat sowohl das Verordnungsgebungsverfahren als auch die Einrichtung des Registers datenschutzrechtlich begleitet.

Das Land Brandenburg hat von der ihm im Personenstandsgesetz⁴⁷ eingeräumten Möglichkeit Gebrauch gemacht, ein zentrales Personenstandsregister einzurichten und im Abschnitt 2 der neuen Brandenburgischen Personenstandsverordnung entsprechende Regelungen getroffen. Diese erörterten wir vor dem Erlass der Verordnung mit dem Ministerium des Innern des Landes Brandenburg, dem Brandenburgischen IT-Dienstleister, dem Städte- und Gemeindebund, dem Landkreistag sowie dem Landesfachverband der Standesbeamtinnen und Standesbeamten zusammen mit Detailfragen zur datenschutzgerechten Gestaltung.

Nahezu alle Standesämter des Landes betreiben ihre Fachverfahren und die elektronischen Personenstandsregister bereits als Datenverarbeitung im Auftrag gemäß § 11 Brandenburgisches Datenschutzgesetz (BbgDSG) beim Kommunalen Rechenzentrum Cottbus. Auf den dort vorliegenden Datenbeständen wurde durch das Rechenzentrum das zentrale elektronische Personenstandsregister eingerichtet, welches als Abrufverfahren allen angeschlossenen Standesämtern den gegenseitigen Zugriff auf alle Registerdatensätze erlaubt.

Zu beachten ist, dass die Verantwortung für die Korrektheit und Pflege der einzelnen Datensätze stets bei den jeweiligen Standesämtern verbleibt. Deshalb muss beim zentralen Betrieb der Standesamtsfachverfahren im

⁴⁶ Artikel 1 der Verordnung zur Anpassung landesrechtlicher Vorschriften an das Personenstandsrecht vom 22. August 2013 (GVBl. II Nr. 62)

⁴⁷ Personenstandsgesetz vom 19. Februar 2007 (BGBl. I S. 122), das durch Artikel 3 des Gesetzes vom 28. August 2013 (BGBl. I S. 3458) geändert worden ist

Kommunales Rechenzentrum Cottbus eine strikte mandantenbezogene Trennung⁴⁸ eingehalten werden.

In Bezug auf das zentrale elektronische Personenstandsregister wurde auch die Frage der datenschutzrechtlichen Verantwortlichkeit diskutiert. Die Stadt Cottbus kann die Verantwortung nur für die in ihrem Einflussbereich liegenden zentralen Verfahrenskomponenten übernehmen. Für diese Komponenten erstellt sie das Sicherheitskonzept und erteilt die datenschutzrechtliche Freigabe gem. § 7 Abs. 3 BbgDSG. Ihr behördlicher Datenschutzbeauftragter führt das Verfahrensverzeichnis gem. § 8 BbgDSG.

Davon unberührt bleibt die datenschutzrechtliche Verantwortung der Standesämter für die in ihrem Einflussbereich liegenden dezentralen Verfahrenskomponenten. Hierfür müssen sie ohnehin gemäß den Vorschriften des Brandenburgischen Datenschutzgesetzes das Sicherheitskonzept erstellen, die Freigabe erteilen und ein Verfahrensverzeichnis führen. Bei der Bestimmung der erforderlichen technischen und organisatorischen Maßnahmen werden sie durch Vorgaben unterstützt, die das Kommunale Rechenzentrum Cottbus zur Sicherstellung eines Mindestniveaus an Datenschutz und Informationssicherheit im Verfahren erarbeitet hat. Darüber hinaus erhalten die Standesämter jeweils eine Kopie des Verfahrensverzeichnisses des zentralen elektronischen Personenstandsregisters von der Stadt Cottbus, um dem Transparenzgedanken gerecht zu werden, der mit der Möglichkeit der unentgeltlichen Einsichtnahme in das Verfahrensverzeichnis gem. § 8 Abs. 4 BbgDSG verfolgt wird.

Die Erstellung von Sicherheitskonzepten sowie die Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen bei den Standesämtern wurden von uns stichprobenartig geprüft. Es konnte festgestellt werden, dass die Städte und Gemeinden bemüht sind, den ihnen gestellten Anforderungen gerecht zu werden. Sie sind sich bewusst, dass sie trotz der zentralen Datenerhaltung im Kommunalen Rechenzentrum der Stadt Cottbus selbst die Verantwortung für die Verarbeitung der personenbezogenen Daten im Fachverfahren tragen.

Das zentrale elektronische Personenstandsregister ermöglicht allen angeschlossenen Standesämtern erstmalig einen gegenseitigen Zugriff auf die Registerdatensätze. Unsere Hinweise und Empfehlungen wurden sowohl bei der Erarbeitung der Rechtsverordnung als auch bei der Gestaltung des konkreten Verfahrens berücksichtigt.

⁴⁸ siehe B 2.1

8.3 Einführung eines einheitlichen Einsatzleitsystems in den Regionalleitstellen Brandenburgs

Die kreisfreien Städte Brandenburg an der Havel, Cottbus, Frankfurt (Oder) und Potsdam sowie der Landkreis Barnim betreiben jeweils eine Regionalleitstelle für den Brandschutz, den Rettungsdienst und den Katastrophenschutz. Um im Fall der Überlastung oder des Ausfalls einer Regionalleitstelle eine Unterstützung oder Vertretung durch eine andere Leitstelle zu ermöglichen, startete im Berichtszeitraum ein Projekt zur Einführung eines einheitlichen Standardisierten Kommunalen Einsatzleitsystems in Brandenburg (SKEiBB).

Die fünf Regionalleitstellen des Landes Brandenburg nehmen Hilfeersuchen über den Notruf 112 entgegen. Sie veranlassen und koordinieren Einsatzmaßnahmen im Brandschutz, bei Gefahren in Not- und Unglücksfällen sowie bei Großschadensereignissen und Katastrophen.

Zur Sicherstellung eines durchgängigen Brand- und Katastrophenschutzes ist eine dauerhafte Erreichbarkeit und Einsatzfähigkeit der Regionalleitstellen geboten. Es sind deshalb Vorkehrungen erforderlich, durch die der zeitweise Ausfall einer Regionalleitstelle kompensiert und deren Aufgaben temporär durch eine andere Regionalleitstelle übernommen werden können. Vor diesem Hintergrund zielt das Projekt SKEiBB darauf ab, die Grundlagen für einen redundant ausgelegten Leitstellenverbund zu schaffen, indem ein einheitliches Einsatzleitsystem mit Möglichkeiten des Datenaustausches sowie ein Stammdatenportal für Informationen über zur Verfügung stehende Rettungsmittel eingeführt werden sollen.

Die Verarbeitung personenbezogener Daten durch die Regionalleitstellen im Brand- oder Katastrophenfall bzw. bei besonderen Hilfeleistungen in Not- oder Unglücksfällen unterliegt datenschutzrechtlichen Bestimmungen. So regelt § 17 Brandenburgisches Brand- und Katastrophenschutzgesetz u. a. den Umfang und die Arten der zu verarbeitenden Daten, ihre Zweckbindung sowie Löschfristen. Darüber hinaus sind die Bestimmungen des Brandenburgischen Datenschutzgesetzes (BbgDSG) anzuwenden, insbesondere in Bezug auf die Gewährleistung technischer und organisatorischer Maßnahmen (§ 10 BbgDSG), die Freigabe des Verfahrens (§ 7 Abs. 3 BbgDSG), das Verfahrensverzeichnis (§ 8 BbgDSG) und die Vorabkontrolle durch den behördlichen Datenschutzbeauftragten (§ 10a BbgDSG).

Für den Zeitraum des Ausfalls einer Regionalleitstelle sind ggf. personenbezogene Daten (z. B. der Geschädigten oder Hilfesuchenden) an die vertretende Leitstelle zu übermitteln und Einsatzaufgaben durch diese wahrzunehmen. Nach der Wiederaufnahme des Betriebs sind die jeweiligen Einsatzda-

ten der ausgefallenen Leitstelle zu übertragen. Die Datenübermittlungen sind gem. § 14 Abs. 1 BbgDSG zulässig, da sie für die Erfüllung der gesetzlichen Aufgaben der Leitstellen erforderlich sind. Eine strenge Zweckbindung der Daten ist zu gewährleisten.

Das im Einsatzleitsystem integrierte Stammdatenportal soll Berechtigten eine schnelle und einfache Auskunft über die im Verantwortungsbereich der Regionalleitstellen zur Verfügung stehenden Rettungsmittel und Ansprechpartner ermöglichen. Es wird durch die Regionalleitstelle Lausitz (Cottbus) als Datenverarbeitung im Auftrag gem. § 11 BbgDSG zentral für alle Leitstellen betrieben. Entsprechende vertragliche Regelungen liegen vor.

Die Landesbeauftragte wurde frühzeitig durch die Regionalleitstellen in dem Projekt beteiligt. Datenschutzrechtliche Anforderungen konnten so bereits bei der Erstellung der Vergabeunterlagen und bei der Umsetzung des Konzepts des Standardisierten Einsatzleitsystems sowie des Stammdatenportals eingebracht werden. Dabei konzentrierten sich unsere Aktivitäten insbesondere auf die Regelungen zur Weitergabe von personenbezogenen Daten im Leitstellenverbund sowie auf die Erarbeitung des IT-Sicherheitskonzeptes durch die Regionalleitstellen.

Das Standardisierte Kommunale Einsatzleitsystem in Brandenburg ist die technische Grundlage für einen redundanten Leitstellenverbund und damit für eine durchgängige Sicherung des Brand- und Katastrophenschutzes im Land. Die datenschutzrechtlichen Anforderungen wurden im Projekt von Beginn an berücksichtigt und in die Planung und Umsetzung des Verfahrens einbezogen.

8.4 Zensus 2011: Nach der Volkszählung ist vor der Volkszählung

Im Berichtszeitraum wurden die Datenerhebungen des Zensus 2011 abgeschlossen und erste Ergebnisse veröffentlicht. Die Arbeitsgruppe der Leitungen der Erhebungsstellen in Berlin und Brandenburg beendete ihre Tätigkeit. Gleiches gilt auch für das entsprechende Gremium zur Koordinierung der Tätigkeit der Datenschutzbehörden von Bund und Ländern im Zensus-Projekt. In beiden Gruppen wirkte unsere Behörde aktiv mit.

Die letzte Beratung mit den Leitungen der Erhebungsstellen in Berlin und Brandenburg zum Zensus 2011 fand im Mai 2012 in einer Berliner Außenstelle des Amtes für Statistik Berlin-Brandenburg statt. Dabei wurden die abschließenden Aufgaben bis zur Auflösung der Erhebungsstellen besprochen sowie die gute Zusammenarbeit zwischen dem Ministerium des Innern des

Landes Brandenburg, dem Statistikamt, dem Städte- und Gemeindebund sowie unserer Behörde bei der Vorbereitung und Durchführung des Projekts gewürdigt.

Im Juni 2012 begann die Vernichtung der Erhebungsunterlagen aus Brandenburg und Berlin. Eine Kontrolle durch unsere Behörde ergab keine Beanstandungen. Die Erhebungsbögen wurden unter Aufsicht von Mitarbeitern des Amtes für Statistik vor Ort durch eine Spezialfirma datenschutzgerecht vernichtet. Die speziell für den Zensus 2011 eingerichtete Berliner Außenstelle Alt-Moabit wurde schließlich im Dezember 2012 planmäßig aufgelöst.

Am 31. Mai 2013 war es dann soweit: Die amtlichen Einwohnerzahlen wurden bekannt gegeben. Darüber hinaus sind auch aktuelle Daten zur demografischen Struktur der Bevölkerung nach Alter, Geschlecht, Familienstand und Staatsangehörigkeit verfügbar. Statistische Angaben zum Erwerbsstatus, zum Schul- und Berufsabschluss, zum Migrationshintergrund und zur Religion komplettieren die Resultate. Die Zahlen können im Internet über die Zensusdatenbank⁴⁹ abgerufen werden. Im Zusammenspiel mit den Ergebnissen der Gebäude- und Wohnungszählung, die ebenfalls Teil des Zensus war, werden ab Frühjahr 2014 zusätzlich statistische Angaben über die Wohnsituation der Haushalte verfügbar sein. Für Brandenburg liegen damit erstmalig seit 1981 aktuelle statistische Zahlen bezogen auf die einzelnen Städte und Gemeinden vor.

Die Ad-hoc-Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder zum Zensus 2011 tagte zum letzten Mal im Dezember 2012. Als Ergebnis ihrer Tätigkeit wurden einige wesentliche Eckpunkte zusammengefasst, die aus datenschutzrechtlicher Sicht beim Zensus 2011 nicht angemessen Berücksichtigung fanden. Sie betreffen neben der Ausgestaltung der gesetzlichen Grundlagen des Zensus-Projektes auch einzelne organisatorische Probleme bei dessen konkreter Durchführung.

Nach den Vorgaben der Europäischen Union wird die nächste Volkszählung in Deutschland im Jahr 2021 durchgeführt. Die hierfür notwendigen Vorbereitungen beginnen in Kürze und werden von der Landesbeauftragten wieder kritisch begleitet.

⁴⁹ siehe <https://ergebnisse.zensus2011.de>

9 Jugend und Familie

9.1 Heimerziehung in der DDR – Auskunft und Akteneinsicht

Vor dem Hintergrund der Aufarbeitung, der Geltendmachung von Entschädigungsansprüchen und möglicher Leistungen aus dem Fonds „Heimerziehung in der DDR“ haben sich immer wieder Betroffene mit Fragen zu ihren Auskunfts- und Akteneinsichtsrechten an uns gewandt.

Für Betroffene ist es nicht immer einfach, ihre Rechte insbesondere bei der richtigen Stelle wahrzunehmen. Solange sich die Akten noch bei den Jugendämtern (oder ggf. einem Zwischenarchiv) befinden, haben Betroffene nach dem Zehnten Buch Sozialgesetzbuch einen Anspruch auf Akteneinsicht nach pflichtgemäßem Ermessen sowie auf Auskunft über die zur Person gespeicherten Sozialdaten, deren Herkunft und Empfänger sowie den Zweck der Speicherung. Nachdem Akten als Archivgut übernommen oder dem öffentlichen Archiv zur Nutzung überlassen werden, richtet sich das Einsichts- und Auskunftsrecht nach dem Brandenburgischen Archivgesetz.

Die Aufbewahrung der Unterlagen und Gewährung von Auskunft und Einsicht für Betroffene wird zurzeit unterschiedlich gehandhabt. Dies ist für alle Beteiligten höchst unbefriedigend. Zur Vereinheitlichung des Verfahrens haben wir uns daher dafür ausgesprochen, dass seitens der Archive erklärt wird, dass die betreffenden Unterlagen archivwürdig und in den zuständigen Archiven aufzubewahren sind. Ihre Vernichtung mit negativen Auswirkungen für die Nachweismöglichkeiten zulasten der Opfer wird so verhindert.

Als Hilfestellung bei entsprechenden Anfragen und Anträgen haben wir unter Beteiligung der Landesbeauftragten zur Aufarbeitung der Folgen der kommunistischen Diktatur, des Ministeriums für Bildung, Jugend und Sport und des Ministeriums für Wissenschaft, Forschung und Kultur einige datenschutzrechtliche Hinweise erarbeitet und diese an die Jugendämter des Landes Brandenburg, die Kreis- und Stadtarchive, das Landesjugendamt und das Landeshauptarchiv übersandt und in unserem Internetangebot⁵⁰ veröffentlicht.

Ehemalige Heimkinder der DDR haben ein Recht auf Auskunft aus ihrer bzw. Einsicht in ihre damaligen Akten. Aufgrund verschiedener Aufbewahrungsorte sind unterschiedliche Rechtsvorschriften zu prüfen. Datenschutzrechtliche Hinweise wurden hierfür erarbeitet.

⁵⁰ siehe <http://www.lda.brandenburg.de> (Datenschutz > Themen > Recht > Arbeit und Soziales)

9.2 Datenübermittlung durch das Jobcenter an das Jugendamt wegen vermuteter Kindeswohlgefährdung

Dürfen Mitarbeiter des Jobcenters an das Jugendamt herantreten und dieses auf eine mögliche Kindeswohlgefährdung hinweisen?

Es liegt in der Verantwortung der Eltern, für das Wohl des Kindes zu sorgen. Der Staat hat diesbezüglich eine „Wächterfunktion“ und überträgt mit § 8a Achtes Buch Sozialgesetzbuch den Schutzauftrag auf die Jugendämter. Diesen obliegt es, bei „gewichtigen Anhaltspunkten“ für eine Gefährdung des Kindeswohls Maßnahmen zur Abwendung der Gefahr zu ergreifen, d. h. den Eltern Hilfe anzubieten bzw. das Familiengericht einzuschalten.

Wie verhält es sich aber, wenn ein Mitarbeiter eines Jobcenters eine Gefährdung für das Kindeswohl bemerkt? Eine solche ist beispielsweise gegeben, wenn durch Vernachlässigung, Misshandlung, Missbrauch oder Konflikte eine erhebliche Beeinträchtigung der körperlichen, geistigen oder seelischen Entwicklung des Kindes oder Jugendlichen sehr wahrscheinlich ist oder bereits vorliegt. Darf ein Mitarbeiter eines Jobcenters an das Jugendamt herantreten, obwohl mit einer Übermittlung von Informationen über das Kind zugleich offenbar würde, dass die Betroffenen Leistungen zur Grundsicherung für Arbeitsuchende beziehen?

Gegenüber den Jobcentern haben wir die Auffassung vertreten, dass eine solche Datenübermittlung vom Jobcenter an das Jugendamt auf § 69 Abs.1 Nr. 1 Zehntes Buch Sozialgesetzbuch (SGB X) gestützt werden kann. Die Übermittlung ist zulässig, wenn ohne sie die Kindeswohlgefährdung nicht abgewendet werden kann.

Vor jeder Übermittlung muss immer im Einzelfall geprüft werden, ob und gegebenenfalls in welchem Ausmaß eine Gefährdung des Kindeswohls vorliegen könnte. Hierfür müssen konkrete Anhaltspunkte gegeben sein. Auch deren Herkunft ist bei der Beurteilung zu berücksichtigen, beispielsweise ob es sich um eine anonyme Anzeige, Äußerungen der Betroffenen selbst oder Erkenntnisse von Mitarbeitern des Jobcenters handelt.

Da diese Einschätzung im Einzelfall sehr schwierig sein kann, empfehlen wir den Jobcentern, Kontakt mit dem Jugendamt aufzunehmen und den Fall zunächst ohne Nennung der Namen der Betroffenen oder einen sonstigen Hinweis, der Rückschluss auf die Personen zulässt, zu besprechen. Die Fachkräfte im Jugendamt verfügen über die besonderen Erfahrungen in der Beurteilung einer solchen Gefährdungslage.

Darüber hinaus sollte nicht jeder Sachbearbeiter allein eine solche Beurteilung vornehmen. Die Aufgabe der Prüfung derartiger Verdachtsfälle sollte bei einer Leitungsperson „gebündelt“ werden. Diese entscheidet dann auch über die Datenübermittlung, wobei die Angaben auf das erforderliche Maß zu reduzieren sind. Geprüft werden sollte auch, ob die jeweilige Fallkonstellation die Einholung der Einwilligung zur Datenübermittlung bei den Betroffenen zulässt. Stets sind die Datenübermittlungen an das Jugendamt zu dokumentieren und die Betroffenen nach § 67a Abs. 3 Satz 2 SGB X darüber zu informieren.

Die Jobcenter dürfen bei konkreten Anhaltspunkten für eine Gefährdung des Kindeswohls Daten an das Jugendamt übermitteln.

9.3 Veröffentlichung von Sozialdaten durch einen Kreistag

Ein Petent beschwerte sich beim zuständigen Kreistag in allgemeiner Form über die Handhabung staatlicher Hilfe und Unterstützung bei der Erziehung von Kindern und Jugendlichen. Die entsprechende Beschlussvorlage für den Kreisausschuss umfasste eine eigens hierfür angefertigte Stellungnahme des Jugendamtes. Darin offenbarte die Behörde Details zu einem individuellen Antrag des Beschwerdeführers auf entsprechende Sozialleistungen. Da die Ausschusssitzung öffentlich war, wurde auch die Beschlussvorlage publik.

Sein Vorgehen begründete der Landkreis mit dem Bestreben, die Ausschussmitglieder umfassend zu informieren, ihnen das Thema anschaulicher zu machen und ihnen die Entscheidung zu erleichtern. Dabei verkannte er sowohl die Anforderungen des Sozialgeheimnisses und die datenschutzrechtlichen Grundsätze der Erforderlichkeit als auch die Vorschriften der Brandenburgischen Kommunalverfassung (BbgKVerf) zur Öffentlichkeit von Sitzungen des Kreistages.

Die Stellungnahme des Jugendamtes zu dem individuellen Antrag eines Erziehungsberechtigten auf Unterstützung enthielt zwangsläufig Sozialdaten des Betroffenen bzw. seines Kindes und unterfiel damit dem Sozialgeheimnis nach § 35 Erstes Buch Sozialgesetzbuch. Die Übermittlung und Veröffentlichung solcher Daten bedarf einer Rechtsgrundlage, an welcher es im vorliegenden Fall fehlte. Aber auch soweit es sich nicht um Sozialdaten handelte, waren die Übermittlung und Veröffentlichung personenbezogener Daten des Erziehungsberechtigten unzulässig. Zur Beantwortung der im Wesentlichen allgemein gehaltenen Beschwerde bedurfte es der Kenntnis von Informationen über den konkreten Antrag des Petenten in keiner Weise. Personenbezogene Daten hätte die Behörde aus der Beschlussvorlage daher entfernen oder schwärzen müssen. Die Beratung und Beschlussfassung des Kreistags

wäre problemlos ohne diese Angaben möglich gewesen, da es auf sie nicht ankam.

Gegen eine anonymisierte Beschlussvorlage für die Kreistagsabgeordneten bestehen aus datenschutzrechtlicher Sicht keine Einwände. Dies gilt auch für die nach den Vorschriften der Brandenburgischen Kommunalverfassung grundsätzlich öffentlich erfolgende Erörterung der Beschwerde. Sollte die Kenntnis personenbezogener Daten für die Ausschussmitglieder bzw. Kreistagsabgeordneten im Einzelfall erforderlich sein, ist die Öffentlichkeit jedoch nach § 36 Abs. 2 Satz 2 BbgKVerf auszuschließen, wenn berechtigte Interessen Einzelner dies erfordern. Soweit Sozialdaten Gegenstand der vorgesehenen Erörterung sein sollen, ist davon auszugehen, dass das Schutzinteresse der Betroffenen im Rahmen einer solchen Abwägung in den meisten Fällen überwiegt und die Öffentlichkeit auszuschließen ist.

Beschlussvorlagen für kommunale Vertretungen dürfen Sozialdaten von Bürgern nur enthalten, wenn dies für die Beratung und Beschlussfassung unvermeidlich ist. In solchen Fällen ist die Öffentlichkeit von den Sitzungen auszuschließen. Allgemein gehaltene Anfragen oder Beschwerden bedürfen generell keiner personenbezogenen Aufbereitung. Über sie kann in allgemeiner Form beraten und beschlossen werden.

10 Justiz

10.1 Datenschutzgerechte Vorbereitung der Schöffenwahl

Alle fünf Jahre werden Schöffen und Jugendschöffen sowie Ersatzpersonen für die Amtsgerichte und Strafkammern der Landgerichte gewählt. Die Vorbereitung der Wahl obliegt den Gemeinden bzw. Jugendhilfeausschüssen, die einheitliche Vorschlagslisten mit mindestens doppelt so vielen Personen wie benötigt aufstellen müssen. Wir hatten die Frage zu beantworten, ob zur Vorauswahl geeigneter Kandidaten ein Rückgriff auf das Melderegister genommen werden und inwieweit eine Veröffentlichung der Vorschlagslisten erfolgen darf.

10.1.1 Nutzung des Melderegisters

Die Schöffenwahl stellt die Gemeinden teilweise vor erhebliche Probleme, weil einerseits die Anforderungskriterien an die ehrenamtlichen Richter hoch sind und die Auswahl einschränken und andererseits möglichst nur Personen eingesetzt werden sollen, die freiwillig bereit sind, diese verantwortungsvolle Aufgabe zu übernehmen. Immer häufiger gibt es jedoch zu wenig freiwillige

Bewerber, sodass die zuständigen Stellen sich gezwungen sehen, gezielt Personen anzusprechen.

Mithilfe der in den Melderegistern eingetragenen Daten können Personen, die bestimmte Grundvoraussetzungen für die Schöffenwahl erfüllen, wie z. B. Mindest- und Höchstalter, deutsche Staatsangehörigkeit oder Ansässigkeit in der Gemeinde ermittelt werden. Aus den formal in Frage kommenden Einwohnern können Personen angesprochen und befragt werden, ob sie sich für die Vorschlagslisten zur Schöffenwahl nominieren lassen. Danach lässt sich anhand weiterer Kriterien gezielt überprüfen, ob sie geeignet sind. Aus Sicht der zuständigen gemeindlichen Stellen erleichtert die Vorauswahl über das Melderegister die ihnen gestellte Aufgabe insbesondere dann, wenn anderweitige aktive Bemühungen, z. B. über Verbände, Kirchen, Parteien und Gewerkschaften oder Informationsveranstaltungen, erfolglos bleiben.

Nach datenschutzrechtlicher Regelungssystematik bedarf es bei einem Datenaustausch stets einer Befugnisnorm für die Daten übermittelnde Stelle auf der einen und einer weiteren Erlaubnis für die zulässige Datenerhebung des Empfängers auf der anderen Seite. Weder das Gerichtsverfassungsgesetz, das Jugendgerichtsgesetz noch die von den zuständigen Ministern herausgegebene Allgemeinverfügung zur Vorbereitung der Wahl und Berufung ehrenamtlicher Richter enthält jedoch Hinweise auf die Rechtmäßigkeit eines Zugriffs auf das Melderegister durch die Gemeinden. § 28 Abs. 1 des Brandenburgischen Meldegesetzes (BbgMeldG) erlaubt der Meldebehörde, bestimmte aufgelistete Daten an andere Behörden zu übermitteln, vorausgesetzt, die Daten sind zur Erfüllung der Aufgaben der Empfängerbehörde erforderlich. Diese Datenübermittlungsbefugnis der Meldebehörden korrespondiert jedoch nicht mit einer Datenerhebungsbefugnis. Wir haben zunächst die Auffassung vertreten, dass der Rückgriff auf die Meldedaten unzulässig ist, da allein die Aufgabenzuweisung an die Gemeinden, Vorschlagslisten zu erstellen, nicht ausreicht, um Meldedaten anzufordern. Wir zweifelten im Übrigen auch an der Erforderlichkeit der Datenverarbeitung.

Nach intensivem Austausch mit dem Ministerium des Inneren änderten wir unsere Position. Aufgrund einer Besonderheit im Meldegesetz kann auf eine spezifische Rechtsgrundlage für die Nutzung der Meldedaten durch die zuständigen Stellen in den Gemeinden verzichtet werden. § 28 Abs. 4 BbgMeldG erlaubt, die bereits von der Gemeinde erhobenen Meldedaten der Einwohner innerhalb der Behörden und Stellen einer Gemeinde oder kreisfreien Stadt weiterzugeben, sofern dies zu deren Aufgabenerfüllung erforderlich ist. Dass gespeicherte Meldedaten für eine gemeindeinterne Nutzung außerhalb der Meldebehörde vorgesehen sind, spiegelt sich auch in der Aufgabenbeschreibung für Meldebehörden, die eine Mitwirkung bei der Durchführung von Aufgaben anderer Behörden vorsieht (§ 2 Abs. 1 Satz 2

BbgMeldG), wider. Der Datentransfer ist nach datenschutzrechtlicher Terminologie daher nicht als Datenübermittlung, also als Bekanntgabe an Dritte zu beurteilen, sondern als bloße interne Datenweitergabe. Es bedarf keiner korrespondierenden Erhebungsnorm der gemeindlichen Stelle. Die Intention des Gesetzgebers, eine Sonderregelung zu schaffen, die darauf abzielt, Meldedaten für öffentliche rechtmäßige Zwecke leichter nutzbar zu machen, muss auch bezüglich des Erforderlichkeitsmaßstabs berücksichtigt werden. Wir halten es deshalb für vertretbar, die Nutzung der Meldedaten bereits dann als erforderlich anzusehen, wenn bestimmte Faktoren nahelegen, dass die Aufgabe ohne Kenntnis der Daten nicht in angemessener Zeit zu erfüllen wäre. Bei der Aufstellung von Vorschlagslisten für die Schöffenwahl ist insoweit zu berücksichtigen, dass die formellen Anforderungen, gesetzliche Ausschlussgründe und die erforderliche persönliche Eignung der Bewerber den Kreis der potenziellen Kandidaten besonders stark einschränken. Im Vergleich zur Auswahl von freiwilligen Funktionsträgern für andere öffentliche Aufgaben – wie z. B. Wahlhelfer – ist zu beachten, dass fehlende Freiwillige aber nicht durch Zwangsverpflichtung öffentlicher Bediensteter ersetzt werden können. Wir tragen eine Datenerhebung aus dem Melderegister zwecks Vorauswahl von Bewerbern für die Schöffenwahl datenschutzrechtlich künftig mit. Voraussetzung ist, dass die Gemeinde vorher anderweitige Auswahlmethoden ausgiebig jedoch ohne ausreichenden Erfolg genutzt hat.

10.1.2 Veröffentlichung der Vorschlagslisten

Im Zusammenhang mit der Schöffenwahl beschäftigte uns noch eine andere Frage. Aufgrund einer Eingabe erfuhren wir, dass ältere Vorschlagslisten für vergangene Schöffen- und Jugendschöffenwahlen im Amtsblatt einer Stadt veröffentlicht waren. Vorschlagslisten enthalten die Namen der Kandidaten, Geburtsort, -datum, Anschrift, Beruf und vorhandenen Erfahrungen in diesem Bereich. Da die Amtsblätter auch auf der Webseite der Stadt eingestellt waren, konnten Daten einer ehemaligen Schöffin recherchiert werden, die dadurch ihr Recht auf informationelle Selbstbestimmung verletzt sah.

Das Gerichtsverfassungsgesetz schreibt in § 36 Abs. 3 hinsichtlich des Verfahrens lediglich vor, dass die Vorschlagslisten in der Gemeinde eine Woche lang zu jedermanns Einsicht „aufzulegen“ sind. Der Zeitpunkt der Auflegung muss vorher öffentlich bekannt gemacht werden. Die Auflegung oder Auslegung dient dem Zweck, anderen Einwohnern zu ermöglichen, Einwendungen gegen die Bewerber geltend zu machen. Darüber hinaus ist jedoch eine Veröffentlichung der Vorschlagslisten nicht vorgesehen. Wir haben die betreffende Stadt und darüber hinaus alle Landkreise und kreisfreien Städte davon unterrichtet, dass die uns bekannt gewordene Praxis der Veröffentlichung in Amtsblättern gegen das informationelle Selbstbestimmungsrecht der Betroffenen verstößt. Die Veröffentlichung in Printmedien bzw. über online

gestellte Amtsblätter stellt eine Datenübermittlung an Dritte dar, für die es keine Rechtsgrundlage gibt. Der Gesetzgeber hat lediglich für einen eng begrenzten Zeitraum eine öffentliche Kenntnisnahme der Vorschlagslisten vorgesehen. Wir haben die betroffenen Kommunen daher aufgefordert, künftig nur Ort, Zeitpunkt und Dauer der Auslegung in Amtsblättern oder in anderer geeigneter Form zu veröffentlichen. Auf Webseiten bereits eingestellte Vorschlagslisten früherer Wahlverfahren sind aus digitalisierten Veröffentlichungsorganen zu entfernen oder die enthaltenden personenbezogenen Daten unkenntlich zu machen.

Gemeinden stellen für die Schöffenwahl Vorschlagslisten zusammen. Kann die erforderliche Anzahl freiwilliger Bewerber nicht durch Aufrufe und Werbemaßnahmen sichergestellt werden, dürfen die zuständigen Stellen – sofern andere Mittel erfolglos ausgeschöpft wurden – Daten von potenziell geeigneten Einwohnern nach bestimmten Auswahlkriterien von den Meldebehörden abrufen. Die so aufgestellten Vorschlagslisten dürfen nur innerhalb einer gesetzlichen Auslegungsfrist der Öffentlichkeit bekannt gegeben, jedoch nicht in Amtsblättern oder sonstigen Veröffentlichungen, insbesondere nicht im Internet dauerhaft veröffentlicht werden.

10.2 Einführung des bundesweiten Vollstreckungsportals

Die Schaffung eines internetgestützten, bundesweiten Vollstreckungsportals ermöglicht es, Informationen aus Schuldner- und Vermögensverzeichnissen online abzurufen. Wird dem Datenschutz dabei ausreichend Rechnung getragen?

Zum 1. Januar 2013 ist das Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung⁵¹ in Kraft getreten. Ziel der Neuregelungen war es, insbesondere die Möglichkeiten der Informationsgewinnung für Gläubiger in der Zwangsvollstreckung wegen Geldforderungen zu verbessern. Zugleich sollte der Verwaltungsaufwand, der dadurch entstand, dass Vermögens- und Schuldnerverzeichnisse in Papierform bei einzelnen Vollstreckungsgerichten geführt wurden, durch den Einsatz moderner Informationstechnologien verringert werden. Zu diesem Zweck wurde u. a. ein von allen Ländern gemeinsam betriebenes Internetportal⁵² erstellt. Dieses dient als zentrales Informations- und Kommunikationssystem, über das Daten aus Schuldner- und Vermögensverzeichnissen der Länder abrufbar sind. Technischer Betreiber des Portals ist der Landesbetrieb Information und Technik des Landes Nordrhein-Westfalen, der die Daten zwecks Einsichtnahme bzw. Abdruckversand

⁵¹ Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung vom 29. Juli 2009 (BGBl. I S. 2258) zuletzt geändert durch Artikel 18 des Gesetzes vom 23. Mai 2011 (BGBl. I S. 898)

⁵² siehe <https://www.vollstreckungsportal.de>

bereitstellt und Abrufe protokolliert. Das Land Nordrhein-Westfalen ist auch zuständig für die Erhebung und Vollstreckung der für Abdrucke aus dem Schuldnerverzeichnis erhobenen Gebühren. Entsprechende Befugnisse wurden mittels Staatsvertrag zwischen den Ländern festgelegt und vom Land Brandenburg durch ein Zustimmungsgesetz⁵³ in Landesrecht transformiert. In jedem Bundesland wurde ein zentrales Vollstreckungsgericht bestimmt, das das Schuldnerverzeichnis führt. In Brandenburg übernimmt diese Aufgabe das Amtsgericht Nauen.

Schuldnerverzeichnisse enthalten die Daten von zahlungsunfähigen oder -unwilligen Schuldnern. Diese konnten auch bisher von Privatpersonen bei Vorliegen bestimmter Voraussetzungen eingesehen werden. Da über das Vollstreckungsportal automatisierte Abrufe über das Internet erfolgen können, bedurfte es neuer Regelungen, die datenschutzrechtliche Aspekte zum Schutz der Schuldner berücksichtigen. Einzelheiten zur Führung des Schuldnerverzeichnisses, Registrierung von Nutzungsberechtigten und Abfragedatenübermittlung wurden durch eine bundesgesetzliche Verordnung über die Führung des Schuldnerverzeichnisses⁵⁴ festgelegt. Durch frühzeitige Stellungnahmen der Datenschutzbeauftragten des Bundes und der Länder zum Verordnungsentwurf konnten einige mit dem neuen Verfahren verbundene datenschutzrechtliche Probleme beseitigt werden.

Nur registrierte Nutzer können über das Vollstreckungsportal Einsicht in das Schuldnerverzeichnis nehmen, wobei die Berechtigung zur Einsichtnahme bei jeder Anmeldung geprüft wird. Wird für die Registrierung das elektronische Verfahren genutzt, kann hierbei die eID-Funktion des neuen Personalausweises verwendet werden. Die ursprüngliche Absicht, Kreditkartendaten zu diesem Zweck zuzulassen, wurde nicht weiterverfolgt.

Die Einsichtnahme wurde vom Gesetzgeber nur zu bestimmten aufgelisteten Zwecken gestattet. Allerdings wird eine Entscheidung über die Einsichtnahme automatisiert ohne Einzelfallprüfung getroffen. Es wurde zunächst als ausreichend angesehen, wenn identifizierte Nutzungsberechtigte einen die Abfrage legitimierenden Zweck aus einer vorgegebenen Liste auswählten. Um eine nachträgliche Prüfung der Zulässigkeit zu gewährleisten, muss aber nunmehr der Abfragegrund in einem Freitextfeld konkretisiert werden. Die Protokolldaten der Abrufvorgänge werden sechs Monate gespeichert. Ob diese Zeit

⁵³ Gesetz zu dem Staatsvertrag über die Übertragung von Aufgaben nach §§ 802k Absatz 1 Satz 2, 882h Absatz 1 Satz 2 und 3 der Zivilprozessordnung und § 6 Absatz 1 Schuldnerverzeichnisführungsverordnung und § 7 Absatz 1 Satz 1 der Vermögensverzeichnisverordnung zur Errichtung und zum Betrieb eines gemeinsamen Vollstreckungsportals der Länder vom 4. April 2013 (GVBl. I Nr. 12)

⁵⁴ Schuldnerverzeichnisführungsverordnung vom 26. Juli 2012 (BGBl. I S. 1654), die durch Artikel 4 des Gesetzes vom 15. Juli 2013 (BGBl. I S. 2379) geändert worden ist

ausreicht, um effektive nachträgliche Kontrollen der Datenzugriffe zu gewährleisten, bleibt abzuwarten.

Schließlich wurden auch die Suchfunktionalitäten bei Abfragen von Privatpersonen im Schuldnerverzeichnis beschränkt. Die Eingabe von mindestens zwei Suchkriterien (wie Name der Schuldner und Sitz des zuständigen zentralen Vollstreckungsgerichts) sollte ausreichend sein, damit eine Ergebnisübersicht mit Daten aller in Frage kommenden Personen angezeigt wird. Bei Personen mit geläufigen Namen hätte ein hohes Risiko bestanden, dass unzulässige Informationen zu unbeteiligten Betroffenen an die Abrufenden übermittelt werden. Zudem hätte die Gefahr von Personenverwechslungen bestanden, wenn keine weiteren identifizierenden Merkmale wie z. B. Geburtsdatum die gesuchte Person konkretisieren. Die Suchanfrage wurde dahingehend abgeändert, dass keine Trefferlisten angezeigt werden. Neben Vor- und Nachnamen sowie Wohnsitz oder Vollstreckungsgericht müssen – wenn mehrere Datensätze dazu vorhanden sind – weitere Merkmale eingegeben werden, damit ein eindeutiger Treffer übermittelt wird.

Über das bundesweite Vollstreckungsportal können registrierte Nutzungsberechtigte – auch Privatpersonen – für bestimmte Zwecke online Einsicht in das Schuldnerverzeichnis nehmen. Das Verfahren wurde so ausgestaltet, dass sowohl dem Informationsinteresse von Gläubigern als auch den Datenschutzbelangen der betroffenen Schuldner Rechnung getragen wird.

11 Kommunales

11.1 Licht und Schatten – datenschutzrechtliche Prüfungen in Kommunen

Die Landesbeauftragte hatte im Jahr 2009 eine Umfrage zum Thema Datenschutz und Informationssicherheit in den Kommunalverwaltungen des Landes Brandenburg durchgeführt.⁵⁵ Im Berichtszeitraum haben wir diese Umfrage erneut aufgegriffen und in mehreren Kommunen datenschutzrechtliche Kontrollen durchgeführt.

Ziel der Kommunalumfrage von 2009 war es, den Ist-Zustand bei der Umsetzung von Datenschutz und Informationssicherheit in den Verwaltungen zu erheben, den Unterstützungsbedarf in diesen Bereichen zu bestimmen und Empfehlungen sowie mögliche Unterstützungsleistungen abzuleiten. Außer-

⁵⁵ siehe Tätigkeitsbericht 2008/2009, A 1.1

dem sollten die Verwaltungen für das Thema Datenschutz sensibilisiert und die Verantwortlichen auf Defizite hingewiesen werden.

Die durchgeführten anlassunabhängigen Kontrollen haben insgesamt einen Fortschritt bei der Berücksichtigung des Datenschutzes gezeigt. Insbesondere die Bemühungen in den Kommunalverwaltungen bei der Erstellung von Sicherheitskonzepten – in der Regel nach den Empfehlungen in den Standards und IT-Grundschutzkatalogen des Bundesamtes für Sicherheit in der Informationstechnik – sind zu begrüßen. Es zeigt sich aber auch, dass der erforderliche Aufwand an Ressourcen sowohl in personeller als auch in finanzieller Hinsicht manche Verwaltung vor große Herausforderungen stellt.

Positiv zu bewerten ist, dass gerade bei der Einführung neuer Verfahren zur Verarbeitung personenbezogener Daten die Anforderungen des Brandenburgischen Datenschutzgesetzes nun meist konsequenter beachtet werden, insbesondere in Bezug auf die Umsetzung technischer und organisatorischer Maßnahmen, die Freigabe und, falls erforderlich, die Vorabkontrolle. Deren nachträgliche Umsetzung für bereits eingeführte, seit Jahren benutzte Verfahren neben dem normalen Tagesgeschäft überfordert jedoch viele Verwaltungen. Wir empfehlen in diesen Fällen ein schrittweises Vorgehen: So sind beispielsweise wesentliche Verfahrensänderungen wie System- oder Softwareumstellungen geeignete Anlässe, die erforderlichen Dokumente nachzuarbeiten, Konzepte zu vervollständigen oder noch offene technische und organisatorische Maßnahmen umzusetzen.

Auch das Bestreben vieler Verwaltungen, Mitarbeiter für Belange des Datenschutzes und der Informationssicherheit zu sensibilisieren, sehen wir positiv. Häufig werden Schulungen durch die behördlichen Datenschutzbeauftragten oder durch externe Dienstleister angeboten oder entsprechendes Informationsmaterial im Intranet der Verwaltung bereitgestellt. Weiterhin beobachten wir, dass Kommunalverwaltungen sich mittlerweile besser vernetzen sowie Wissen und Erfahrungen zu datenschutzrechtlichen Fragen austauschen.

Bei unseren Kontrollen trafen wir jedoch auch auf einzelne Verwaltungen, in denen datenschutzrechtliche Regelungen nur unzureichend Beachtung finden oder gar unbekannt sind. In einer Gemeinde wurde weder ein behördlicher Datenschutzbeauftragter benannt noch gab es eine Dokumentation zum Datenschutz oder zur Informationssicherheit. Dienstanweisungen existierten zwar auf dem Papier, wurden aber bei der täglichen Arbeit nicht umgesetzt und ihre Einhaltung auch nicht kontrolliert. Wir wiesen die Leitung der Verwaltung auf den Handlungsbedarf hin, konnten jedoch zunächst kein Interesse an der Einhaltung datenschutzrechtlicher Regelungen feststellen. Erst mit unserer nachdrücklichen Aufforderung zur Beachtung der gesetzlichen Regelungen änderte sich die Situation.

Die Kommunalverwaltungen in Brandenburg unternehmen – von wenigen Ausnahmen abgesehen – große Anstrengungen, die Vorgaben und Anforderungen des Datenschutzes und der Informationssicherheit einzuhalten. Fortschritte gegenüber dem Stand des Jahres 2009 sind erkennbar. Es gilt nun, die positiven Entwicklungen zu verstetigen und noch bestehende Lücken zu schließen.

11.2 Wo drückt der Schuh? – Bürgerumfragen durch Kommunen

Eine Kommune beabsichtigte, ein aktuelles und repräsentatives Bild der Zufriedenheit ihrer Einwohner mit den Lebens-, Arbeits-, Versorgungs-, Freizeit- und Wohnbedingungen sowie mit den Dienstleistungen der Verwaltung zu gewinnen. Sie entwarf hierzu einen mehrseitigen Fragebogen und bat einen ausgewählten Teil der Bürger um dessen Beantwortung. Die statistische Auswertung der Antworten sollte bei der Planung der weiteren Stadtentwicklung sowie bei der Tätigkeit der Verwaltung Berücksichtigung finden.

Rechtsgrundlage der Umfrage war eine entsprechende Satzung. Die Durchführung und Auswertung übernahm die kommunale Statistikstelle vor Ort, die gemäß Brandenburgischem Statistikgesetz (BbgStatG) von anderen Stellen des Verwaltungsvollzugs räumlich, organisatorisch und personell getrennt ist. Nach einem mathematischen Zufallsverfahren wurden durch die zuständige Meldebehörde 4 % aller Einwohner im Alter zwischen 16 und 80 Jahren mit Hauptwohnsitz in der entsprechenden Kommune als Stichprobe ausgewählt und die Adressdaten an die Statistikstelle übermittelt. Diese Datenverarbeitung war gem. § 28 Brandenburgisches Meldegesetz sowie § 11 Abs. 4 BbgStatG zulässig.

In dem zum Fragebogen gehörenden Anschreiben wies die Verwaltung auf die Freiwilligkeit der Teilnahme hin. Gleichwohl beabsichtigte sie, Maßnahmen zur Erhöhung des Rücklaufs der Fragebögen durchzuführen: Einerseits sollten alle Einwohner, die den Fragebogen ausfüllten und zurücksandten, ein kleines Präsent als Dank erhalten. Andererseits war geplant, Erinnerungsschreiben an diejenigen Teilnehmer zu verschicken, die bis zu einem bestimmten Zeitpunkt noch nicht geantwortet hatten. Hierzu war es für die Statistikstelle erforderlich zu wissen, ob der Adressat eines Fragebogens geantwortet hatte oder nicht. Die Herstellung eines Zusammenhangs zu den konkreten Antworten des Betroffenen war jedoch nicht erforderlich.

Zur Identifikation derjenigen Bürger, die an der Umfrage teilnahmen, enthielt jeder Fragebogen einen eindeutigen Strichcode, der bei der automatisierten,

maschinellen Auswertung (durch Scannen der Bögen und Text- bzw. Mustererkennung) mit ausgelesen wurde. Falls jemand den Fragebogen im Internet ausfüllen wollte, musste er hierzu ein eindeutiges Zugangskennwort angeben, das neben dem Strichcode vermerkt war. Bis auf diese Ausnahmen waren die Fragebögen so gestaltet, dass aus den Antworten kein Rückschluss auf die ausfüllende Person möglich war.

§ 14 Abs. 1 BbgStatG verlangt (genauso wie die in diesem Fall anzuwendende kommunale Satzung) eine frühestmögliche Trennung und die gesonderte Aufbewahrung der für die statistische Auswertung bestimmten Erhebungsmerkmale von den nur zur technischen Durchführung der Erhebung notwendigen Hilfsmerkmalen. Die für die Durchführung und Auswertung der Umfrage zuständige Statistikstelle konfigurierte die verwendete Software deshalb so, dass eine physische Trennung der Adressdaten der Umfrageteilnehmer und der Information, ob sie bereits geantwortet hatten (als Hilfsmerkmale), von den jeweils konkreten Antworten (als Erhebungsmerkmalen) erfolgte. Eine Zusammenführung beider Datenbestände und damit die Herstellung des Personenbezugs einzelner Antworten wurden durch technisch-organisatorische Maßnahmen ausgeschlossen. Wir regten ergänzend an, jede diesbezügliche Konfigurationsänderung an der Software zu protokollieren.

Außerdem wiesen wir die Verwaltung auf die Erfüllung der formalen Anforderungen des Brandenburgischen Datenschutzgesetzes bei der Einführung von automatisierten Verfahren hin (wie der Freigabe des Verfahrens, der Erstellung eines Sicherheitskonzepts und der Erarbeitung des Verfahrensverzeichnis). Unter den genannten Voraussetzungen sowie mit der Maßgabe, die strenge Zweckbindung der Adressdaten und ihre frühestmögliche Löschung zu gewährleisten, stimmten wir dem beabsichtigten Verfahren zu.

Die statistische Auswertung von Bürgerumfragen ist so zu gestalten, dass die Herstellung des Personenbezugs von Antworten zu einzelnen Umfrageteilnehmern ausgeschlossen ist. Hilfsmerkmale, die allein der technischen Durchführung der statistischen Erhebung dienen, sind zum frühestmöglichen Zeitpunkt zu löschen.

11.3 Dreidimensionale Erfassung des öffentlichen Straßenraums

Die digitale, dreidimensionale Erfassung des öffentlichen Straßenraums ermöglicht der Verwaltung beispielsweise die Bewertung des Straßenzustands, die Georeferenzierung von Straßen und Verkehrsschildern oder auch Vermessungsarbeiten. Bei der Erhebung der Umgebungsdaten ist aber auch das informationelle Selbstbestimmungsrecht der Bürger zu beachten.

Mehrere Kommunen zeigten Interesse an einer Befahrung der in ihrem Verantwortungsbereich liegenden Straßen durch spezielle Kamerafahrzeuge, um mit den aufgezeichneten Video- und Geodaten eine Straßenzustandsbewertung durchzuführen. Die Auswertung sollte als Grundlage für zukünftige Entscheidungen zum Straßenausbau und zur Straßensanierung dienen. Weitere Einsatzzwecke wurden nicht ausgeschlossen und sollten ggf. erst zu einem späteren Zeitpunkt festgelegt werden.

Eine Kommune setzte uns im Vorfeld einer Straßenbefahrung über ihr Vorhaben in Kenntnis. Unserer rechtlichen Bewertung des Verfahrens und den daraus abgeleiteten Hinweisen und Empfehlungen folgte sie jedoch nicht. Einer Pressemitteilung, die die geplante Befahrung ankündigte, war der Verzicht auf die Einhaltung datenschutzrechtlicher Erfordernisse zu entnehmen. Insbesondere sollten auch Passanten und Kfz-Kennzeichen erfasst und gespeichert werden.

Aufgrund eines hohen Medieninteresses und der Intervention der Landesbeauftragten, wurde die Befahrung von der Kommune zunächst abgesagt und auf das Frühjahr 2014 verschoben. Bis dahin sagten die Verantwortlichen zu, mit Unterstützung unserer Behörde für eine datenschutzgerechte Ausgestaltung des Verfahrens zu sorgen.

In einem weiteren Fall wandte sich eine Kommune erst an uns, als die Straßenbefahrung bereits beendet war. Da hierbei auch nicht erforderliche personenbezogene Daten erhoben und gespeichert wurden, forderten wir deren Löschung bzw. Anonymisierung. Dazu teilte uns die Gemeinde mit, dass dies aus finanziellen Gründen nicht möglich sei.

Ein selbst herbeigeführter rechtswidriger Zustand kann nicht mit der Begründung, es fehlten die Haushaltsmittel für seine Beseitigung, gerechtfertigt werden. Die Forderung zur Anonymisierung der Daten halten wir daher nach wie vor aufrecht. Alternativ sind die Aufzeichnungen zu löschen.

Grundsätzlich können eine Straßenbefahrung und die Verarbeitung von Daten der öffentlichen Umgebung zur Erfüllung der gesetzlichen Aufgaben von Kommunen zulässig sein. Die Erhebung personenbezogener Daten hierbei ist jedoch gem. § 12 Abs. 1 Brandenburgische Datenschutzgesetz (BbgDSG) nur in dem Umfang gestattet, wie er für die Aufgabenerfüllung erforderlich ist. Für Zwecke der Analyse und Bewertung des Straßenzustandes ist die Erfassung zufälliger Passanten oder Kennzeichen von Fahrzeugen nicht von der genannten Rechtsgrundlage gedeckt. Ihre Speicherung nach Beendigung der Straßenbefahrung ist unzulässig – sie sind gem. § 19 Abs. 2 BbgDSG zu löschen. Um die Aufzeichnungen nutzen zu können, kommt nur die Entfernung des Personenbezugs in Betracht.

Gem. § 12 Abs. 2 BbgDSG sind personenbezogene Daten grundsätzlich bei dem Betroffenen mit seiner Kenntnis zu erheben. Im konkreten Fall ist es nach unserer Auffassung ausreichend, auf dem Wege einer ortsüblichen Bekanntmachung über die Straßenbefahrung und mögliche Bildaufnahmen zu informieren. Hierbei ist auch über den Verwendungszweck aufzuklären und die Anonymisierung nicht erforderlicher personenbezogener Daten zuzusichern.

Die dreidimensionale Erfassung des öffentlichen Straßenraumes ist ein legitimes Mittel zur Erfüllung von Verwaltungsaufgaben wie die Analyse und Bewertung der Straßeninfrastruktur. Zur Berücksichtigung der datenschutzrechtlichen Anforderungen sind insbesondere die Zweckbindung, die Transparenz und das Löschen bzw. die Anonymisierung nicht erforderlicher personenbezogener Daten durch die Verwaltung zu gewährleisten.

12 Polizei

12.1 Öffentlichkeitsfahndung der Polizei in sozialen Netzwerken

In einigen Bundesländern erstellte die Polizei bei Facebook eine eigene Internetpräsenz und startete Pilotprojekte zur Öffentlichkeitsfahndung über das Netzwerk. Dabei argumentieren die Sicherheitsbehörden, dass sie insbesondere die jüngere Generation über klassische Medien nicht mehr erreichen könnten und erhofften sich über das Online-Netzwerk Hinweise zu ihren Ermittlungen.

Soziale Netzwerke im Internet (wie z. B. Facebook, Wer-kennt-wen, MySpace, Xing) erfreuen sich großer Popularität und werden mittlerweile von Millionen Menschen genutzt. Nicht nur Einzelpersonen legen sich Profilseiten

zu, auch Interessengruppen, private und öffentliche Institutionen (Vereine, Schulen, Unternehmen, Rundfunkanstalten, Kommunen und Ministerien) erstellen neben ihren offiziellen Webseiten zusätzlich Facebook-Auftritte (sog. „Fanpages“). Dieses Netzwerk hat in Deutschland mit Abstand die meisten angemeldeten Nutzer. Nach einer Untersuchung des Bundesverbandes Informationswirtschaft über „Soziale Netzwerke“ aus dem Jahr 2011 verwendeten 45 Prozent der Internetnutzer das Netzwerk Facebook. Sie hinterlassen dort vielfältige Informationen, die auch für polizeiliche Ermittlungs- und Fahndungszwecke interessant sind. Es ist daher nicht verwunderlich, dass sich die Polizei dieser Plattform auch für ihre Aufgaben bedienen will.

Grundlage für die Öffentlichkeitsfahndung ist § 131 Abs. 3 Strafprozessordnung. Die Regelung erlaubt bei einer Straftat von erheblicher Bedeutung in bestimmten Fällen die Öffentlichkeitsfahndung, wenn andere Formen der Aufenthaltsermittlung erheblich weniger Erfolg versprechen. Sie schließt grundsätzlich auch die Nutzung öffentlich zugänglicher elektronischer Medien mit ein. Einzelheiten dazu sind in einer Verwaltungsvorschrift⁵⁶ für die Ermittlungsbehörden niedergelegt. Danach ist bei Fahndungsmaßnahmen in der Öffentlichkeit stets nach dem Grundsatz der Verhältnismäßigkeit im Einzelfall zwischen dem öffentlichen Interesse an der Strafverfolgung und den schutzwürdigen Interessen des Beschuldigten oder anderer Betroffener abzuwägen. Da Daten bei der Internetnutzung weltweit und ggf. dauerhaft abrufbar sind, ergibt sich ein besonderes Gefährdungspotenzial. Ziffer 3.2 der o. g. Richtlinie erläutert zur Nutzung des Internets u. a., dass es zweckmäßig sei, die staatlichen Fahndungsaufrufe auf speziellen Seiten – etwa der Polizei – zu bündeln. Private Internetanbieter sollten grundsätzlich nicht eingeschaltet werden.

Dieses restriktive Konzept ist zu begrüßen und muss insbesondere bezüglich der Nutzung sozialer Netzwerke beachtet werden. Die Veröffentlichung von Fahndungsausschreibungen im Internet bedeutet für die Betroffenen bereits einen gravierenden Eingriff in ihr Persönlichkeitsrecht. Aus unserer Sicht ergeben sich bei Fahndungsaufrufen über soziale Netzwerke weitere erhebliche datenschutzrechtliche Probleme. Netzwerke amerikanischer Betreiber (wie etwa Facebook) sind faktisch einer Datenschutzkontrolle nach deutschen Maßstäben entzogen. Bei Facebook werden darüber hinaus bei jedem Aufruf der Seite personenbezogene Daten über die Nutzer von dem Betreiber erhoben. Facebook wie auch andere Netzbetreiber nutzen spezielle Dienste, um z. B. mithilfe von Cookies das Nutzungsverhalten zu analysieren

⁵⁶ Richtlinie über die Inanspruchnahme von Publikationsorganen zur Fahndung nach Personen bei der Strafverfolgung – Anlage B zu den Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) – Allgemeine Verfügung des Ministers der Justiz vom 25. November 1991 (JMBl. S. 90), zuletzt geändert durch Allgemeine Verfügung des Ministers der Justiz vom 6. März 2012 (JMBl. S. 18) (4208-III.1)

und Statistiken zu erstellen. Die sog. Reichweitenanalyse ist Diensteanbietern zwar grundsätzlich rechtlich erlaubt, allerdings nur, wenn eine wirksame Einwilligung der Betroffenen eingeholt oder ihnen bei pseudonymisierter Verarbeitung ein Widerspruchsrecht eingeräumt wird. Beides ist bisher bei Facebook nicht der Fall.

Fahndungsdaten, die von der Polizei auf einer Fanpage veröffentlicht sind, werden von dem Betreiber gespeichert und können, da sich Facebook die uneingeschränkte Nutzung jeglicher eingestellter Inhalte vorbehält, beliebig verwendet werden. Eine spätere Löschung der auf Facebook-Server hochgeladenen Fahndungsdaten wäre von den zuständigen Behörden faktisch nicht zu kontrollieren. Auch wenn auf einer Fanpage nur Verweise zu Fahndungsinformationen auf polizeiliche Webseiten gesetzt werden, erfasst Facebook Inhaltsdaten der verknüpften Seiten sowie Nutzungsdaten für die Reichweitenanalyse. Diese Erfassung kann zum Teil durch die Nutzung sog. Inlineframes (I-frames) verhindert werden. Dabei werden die Fahndungsdaten ausschließlich auf dem polizeieigenen Server gespeichert, von dort geladen und für die Nutzenden der Fanpage mittels definierter Rahmen am Bildschirm sichtbar gemacht. Allerdings können auch I-frames einer auf deren Anzeige beschränkten Reichweitenanalyse durch Facebook unterliegen.

Grundsätzlich empfehlen wir brandenburgischen öffentlichen Stellen, keine Profilseiten oder Fanpages bei sozialen Netzwerken wie Facebook einzurichten. Sofern die Polizei das Internet und insbesondere soziale Netzwerke nutzt, ist sie verpflichtet, bei ihrer Tätigkeit ein hohes Datenschutzniveau zu beachten. Deshalb sollte bei der Auswahl eines Betreibers eines sozialen Netzwerks darauf geachtet werden, dass die Einhaltung deutschen Rechts gewährleistet wird. Für Öffentlichkeitsfahndungen sind stets vorrangig eigene Internetseiten der Polizei zu nutzen.

Für die Polizei des Landes Brandenburg betreibt das Ministerium des Innern ein Online-Angebot in Form der „Internetwache“. Für Pflege und Inhalt des Internetangebots zeichnet der Zentraldienst der Polizei verantwortlich. Auf den Seiten werden u. a. aktuelle Personenfahndungen auch mit Bild und Sachfahndungen eingestellt. Nach unseren Erkenntnissen veröffentlicht die Polizei in Brandenburg bislang keine Fahndungsaufrufe in sozialen Netzwerken.

Bei der Öffentlichkeitsfahndung muss die Wahrnehmung datenschutzrechtlicher Verantwortung durch die Polizei oder Staatsanwaltschaft gewährleistet sein. Die direkt auf einer Facebook-Fanpage eingestellte oder verlinkte Öffentlichkeitsfahndung widerspricht datenschutzrechtlichen Vorgaben.

12.2 Quellen-Telekommunikationsüberwachung in Brandenburg

Im Herbst 2011 beschäftigte sich die Öffentlichkeit wochenlang mit der Überwachung von Telefongesprächen, die über das Internet geführt werden (Voice over IP), durch deutsche Sicherheitsbehörden. Der Chaos Computer Club hatte eine ihm zugespielte Software zur Überwachung von Telekommunikationsverbindungen analysiert, die von Ermittlern eingesetzt worden war. Kurz danach wurde in den Medien bekannt, dass auch brandenburgische Strafverfolgungsbehörden ein Spähprogramm nutzten. Wir nahmen dies zum Anlass, die eingeleiteten Maßnahmen bei den Staatsanwaltschaften in Brandenburg zu überprüfen.

Da die mittels Internettelefonie geführten Gespräche regelmäßig vor dem Versand der Sprachdaten auf dem Nutzer-Kommunikationsgerät verschlüsselt werden, muss für eine Überwachung auf eines der beteiligten Endgeräte zugegriffen werden, bevor das Gespräch ver- oder nachdem es auf der Empfängerseite entschlüsselt wurde. Ein „Spähprogramm“ auch „Trojaner“ genannt, mit dem ein Endgerät (in der Regel ein PC) infiltriert wird, dient dem Zweck, die Ausleitung, Aufzeichnung und Auswertung der unverschlüsselten Sprachdaten zu gewährleisten. Weil das Abhören direkt an der Quelle – dem Zielrechner – geschieht, spricht man im Gegensatz zur herkömmlichen netzbasierten Telefonüberwachung von einer „Quellen-Telekommunikationsüberwachung“ (Quellen-TKÜ).

Der Chaos Computer Club stellte bei der Analyse der Software fest, dass der von Ermittlungsbehörden eingesetzte sog. „Bundestrojaner“ so konstruiert war, dass er nicht nur Internet-Telefonate ausleiten konnte, sondern auch eine Fernsteuerfunktion zum Nachladen beliebiger weiterer Software auf den Computer bot und das Anfertigen von Bildschirmfotos (Screenshots), beispielsweise von Inhalten des Webbrowsers oder E-Mail-Programms, ermöglichte.

Bei unserer Kontrolle ging es zunächst darum, abzuklären, ob, wie häufig und in welcher Form eine Spähsoftware gegen Beschuldigte zum Einsatz gekommen ist. Hierzu baten wir das Ministerium des Inneren und das Ministerium der Justiz um Auskünfte. In Brandenburg wurden im Zeitraum von 2010 – 2011 vier Maßnahmen zur Quellen-Telekommunikationsüberwachung im Rahmen von strafrechtlichen Ermittlungsverfahren angeordnet. Davon wurde nur in einem Fall eine Spähsoftware erfolgreich aktiviert und somit Daten ausgeleitet und ausgewertet. Dieser Fall betraf ein Ermittlungsverfahren der Schwerpunktabteilung für Wirtschaftskriminalität bei der Staatsanwaltschaft Potsdam. Das Amtsgericht Potsdam ordnete auf Antrag der Staatsanwaltschaft gemäß §§ 100a, 100b Abs. 1 Satz 1 Strafprozessordnung ausschließ-

lich die Überwachung der via Skype geführten Telekommunikation des Hauptbeschuldigten an. Da die Ermittlungsbehörden in Brandenburg nach Auskunft des Innenministeriums nicht über die für Quellen-TKÜ-Maßnahmen erforderliche Software verfügten, wurde die technische Umsetzung durch das Zollkriminalamt bzw. das Zollfahndungsamt Berlin-Brandenburg realisiert. Die Software, die im Auftrag des Zollkriminalamtes von einer privaten Firma entwickelt worden war, spielte das Zollfahndungsamt auf den Computer des Betroffenen auf, während das Auslesen und die Auswertung der Dateien durch Ermittlungsbeamte des Zollfahndungsamtes erfolgte. Die verschriftlichten Gespräche wurden der zuständigen Staatsanwaltschaft zur Verfügung gestellt. Laut einer Antwort der Landesregierung auf eine Kleine Anfrage mehrerer Abgeordneter⁵⁷ wurde die Maßnahme im Zuge der Amtshilfe für die Staatsanwaltschaft durchgeführt.

Im Februar 2012 führten wir einen Kontrollbesuch bei der Staatsanwaltschaft Potsdam durch. Dabei hatten wir Gelegenheit mit Vertretern der ermittelnden Staatsanwaltschaft und des Zollfahndungsamtes zu sprechen und Unterlagen einzusehen. Nach ihren Angaben verfügte die Staatsanwaltschaft selbst nicht über Kenntnisse bezüglich der Funktionalitäten der Software, sondern vertraute diesbezüglich auf Auskünfte des Zollfahndungsamtes. Das Justizministerium teilte uns mit, dass die vom Chaos Computer Club getestete Software nicht für die brandenburgischen Maßnahmen verwendet wurde. Vielmehr sei die genutzte Software auf die Beschlüsse der brandenburgischen Gerichte zugeschnitten worden und nicht in der Lage gewesen, über die Überwachung der Internet-Telefonie hinaus weitere Funktionen auf den Zielcomputern zu überwachen. Bei der stichprobenartigen Durchsicht der uns zur Verfügung gestellten Akten zum Ermittlungsverfahren haben wir zumindest keine Anhaltspunkte für weitergehende Datenzugriffe oder Bildschirmfotos gefunden.

Schwerpunkte der weiteren Prüfung waren die rechtlichen Voraussetzungen der Anordnung und die Kontrolle, ob ausgewertete Gesprächsinhalte den Kernbereich privater Lebensgestaltung verletzt hatten.

Die Überwachung der Telekommunikation ist durch ein Gericht anzuordnen, sofern nicht ausnahmsweise wegen Gefahr in Verzug die Anordnung auch durch die Staatsanwaltschaft ergehen kann. Der richterliche Beschluss des Amtsgerichts Potsdam unterfällt – im Gegensatz zur staatsanwaltlichen Beantragung der Maßnahme – wegen der richterlichen Unabhängigkeit nicht unserer Prüfungskompetenz. Die hier relevante staatsanwaltliche Verfügung stützte die beantragte Überwachung der Internettelefonie einschließlich der dafür erforderlichen Begleitmaßnahmen auf §§ 100a, 100b Strafprozessord-

⁵⁷ Antwort der Landesregierung vom 23. November 2011 auf die Kleine Anfrage 1637, Drucksache 5/4154: Einsatz von Überwachungssoftware (Trojanern) im Land Brandenburg

nung (StPO), die als Rechtsgrundlage für die herkömmliche netzbasierte Telekommunikationsüberwachung dient. Eine dafür erforderliche Katalogstraftat lag wegen des Verdachts des gewerbs- und bandenmäßigen Schmuggels und Verstoßes gegen das Arzneimittelgesetz laut Verfügung der Staatsanwaltschaft vor. Die Staatsanwaltschaft wies zudem darauf hin, dass nur Maßnahmen zur Überwachung der Telekommunikation über das Internet zulässig sind, nicht jedoch weitergehende Datenerhebungen wie die Durchsuchung des Computers oder das Kopieren oder Übertragen sonstiger Daten. Beantragt wurde ein Programm, das entsprechende Funktionsweisen sicherstellt.

Diese Beschränkungen entsprechen grundsätzlich verfassungsrechtlichen Vorgaben, die das Bundesverfassungsgericht aufgestellt hat. In seinem Urteil zur „Online-Durchsuchung“⁵⁸ – einer Maßnahme, die über die in Brandenburg beantragte Überwachung hinausgeht – stellte das Gericht fest, dass das Grundrecht auf Wahrung des Telekommunikationsgeheimnisses nach Art. 10 Abs. 1 Grundgesetz nur dann alleiniger grundrechtlicher Maßstab für die Beurteilung einer Quellen-Telekommunikationsüberwachung ist, wenn ausschließlich Daten aus einem laufenden Kommunikationsvorgang erfasst werden. Wird ein komplexes informationstechnisches System – wie ein Personal Computer – zur Telekommunikationsüberwachung infiltriert, besteht jedoch die Gefahr, dass, auch wenn dies nicht beabsichtigt ist, noch andere auf dem Computer abgelegte Dateiinhalte und persönlichkeitsrelevante Informationen erhoben werden. Die dadurch bewirkten spezifischen Gefährdungen für die Persönlichkeit des Betroffenen müssen anhand des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme beurteilt werden. Das Gericht stellte im Hinblick auf eine Ermächtigung zur Quellen-Telekommunikationsüberwachung durch Behörden fest, dass eine Beschränkung auf Daten aus einem laufenden Telekommunikationsvorgang durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein muss.

In der Strafprozessordnung gibt es keine Regelung, die diesen Anforderungen genügt. Die erforderlichen Einschränkungen werden erst durch die Staatsanwaltschaft beantragt bzw. im Rahmen eines Gerichtsbeschlusses festgelegt. Wegen der besonderen grundrechtsrelevanten Risiken, die beim Abhören verschlüsselter Internetkommunikation durch das Infiltrieren eines informationstechnischen Systems entstehen, müssen aus unserer Sicht die rechtlichen Vorgaben und Schutzvorkehrungen in der gesetzlichen Befugnisnorm formuliert werden. Wir halten grundsätzlich die §§ 100a, 100b StPO nicht für eine hinreichende Rechtsgrundlage für eine Quellen-Telekommunikationsüberwachung.

⁵⁸ Urteil des Bundesverfassungsgerichts vom 27. Februar 2008, 1 BvR 370/07

Bei der hier infrage stehenden Überwachung von Telekommunikation werden regelmäßig auch für das Strafverfahren nicht relevante Gesprächsinhalte erfasst. Handelt es sich dabei um Inhalte, die dem Kernbereich privater Lebensgestaltung angehören, wie z. B. seelsorgerische Äußerungen gegenüber Geistlichen oder Gespräche über das Intimleben, sind diese nicht verwertbar und unverzüglich zu löschen. Bei der stichprobenartigen Durchsicht der verschriftlichten Gespräche stießen wir auf aufgezeichnete Gesprächspassagen des Betroffenen, die aus unserer Sicht eine Verletzung des Kernbereichs darstellen. Wir haben gegenüber der Staatsanwaltschaft die Löschung dieser Passagen gefordert. Die betroffenen Beschuldigten waren nach Auskunft der Staatsanwaltschaft gemäß den gesetzlichen Vorgaben nachträglich über die Maßnahme informiert worden.

Greifen Sicherheitsbehörden bei Überwachungsmaßnahmen für Internettelefonie auf Endgeräte zu, müssen sich die erhobenen Daten auf die laufende Telekommunikation beschränken. Um entsprechende Beschränkungen sicherzustellen, ist eine neue gesetzliche Regelung erforderlich. Die Maßnahme kann aus unserer Sicht nicht auf §§ 100a, 100b Strafprozessordnung gestützt werden. Im Berichtszeitraum hat es eine Quellen-Telekommunikationsüberwachung in Brandenburg gegeben, die auf die Rechtsgrundlage für herkömmliche Telefonüberwachungen gestützt wurde. Einschränkende Vorgaben erfolgten ausschließlich durch die Staatsanwaltschaft bzw. im Gerichtsbeschluss. Bei der Prüfung der Überwachungsmaßnahme konnten wir keine Anhaltspunkte für Datenerhebungen außerhalb der laufenden Telekommunikation feststellen. Für das aufgezeichnete Material muss sichergestellt werden, dass Passagen, die den Kernbereich der privaten Lebensgestaltung betreffen, erkannt und gelöscht werden können.

12.3 PolBB-App – eine mobile Anwendung der Polizei Brandenburg

Die Polizei des Landes Brandenburg stellt eine Applikation für mobile Endgeräte (App) zur Verfügung, mit der Bürger aktuelle Informationen abfragen und Notrufe standortgenau absetzen können. Bei der Entwicklung wurden wir frühzeitig eingebunden.

Das Ziel der mobilen Applikation PolBB-App besteht darin, den Nutzern aktuelle Informationen zeitgemäß auf mobilen Endgeräten zur Verfügung zu stellen. Die App bietet u. a. die Möglichkeit, aktuelle Verkehrsmeldungen, Angaben zu Waldbrandwarnstufen und Pegelständen der Gewässer oder den schnellsten Weg zur nächsten Polizeidienststelle abzurufen. Auch kann der Nutzer sich den aktuellen Standort und die Geokoordinaten anzeigen lassen.

Verirrt sich beispielsweise ein Pilzsucher im Wald, so hat er die Möglichkeit, einen Notruf inklusive Standortdaten an die Polizei abzusetzen.

Die Polizei hat die Applikation in Zusammenarbeit mit der Fachhochschule Potsdam entwickelt und zunächst für Geräte mit dem Betriebssystem iOS konzipiert. Versionen für mobile Endgeräte mit Android- oder anderen Betriebssystemen sollen folgen.

Die Nutzung der PolBB-App ist freiwillig. Der Inhaber des jeweiligen mobilen Endgerätes muss sich bei der Installation entscheiden, ob der Ortungsdienst aktiviert und von der App verwendet werden soll oder nicht. Diese Entscheidung kann er im Nachhinein jederzeit ändern. Darüber hinaus werden für statistische Zwecke Angaben zur Art der abgerufenen Informationen an einen Server der Polizei übertragen, dies jedoch ohne Personenbezug.

Bieten öffentliche Stellen mobile Applikationen an, sind die Prinzipien der Datenvermeidung und der Datensparsamkeit einzuhalten. Es sind nur die für den beabsichtigten Zweck der Anwendung unbedingt erforderlichen personenbezogenen Daten zu verarbeiten. Auch bei einer freiwilligen Nutzung der jeweiligen App muss die verantwortliche Stelle Anwender über die Art und den Umfang der verarbeiteten Daten umfassend aufklären.

13 Schule

13.1 Schulverwaltungsprogramm weBBschule

Im Oktober 2012 stellte uns das Ministerium für Bildung, Jugend und Sport das Projekt zur Einführung des Schulverwaltungsprogramms weBBschule vor. Geplant ist, das Programm als einheitliche Schulverwaltungssoftware in ganz Brandenburg einzusetzen.

Die Software weBBschule soll die allgemeinbildenden Schulen im Land Brandenburg bei der Erledigung der regelmäßig anfallenden administrativen Aufgaben im Schulalltag unterstützen. Schwerpunkt ist dabei die Eingabe und Pflege von personenbezogenen Daten (Schüler, Eltern, Lehrer), die Planung von Klassen, Kursen und Unterrichtsplänen sowie das Erstellen von Dokumenten (z. B. Zeugnissen, Schulbescheinigungen, Klassenlisten). Die Software richtet sich vor allem an Schulleiter und Schulsachbearbeiter, die für die Verwaltung dieser Daten primär verantwortlich sind.

WeBBschule ist als modulares, webbasiertes Softwaresystem konzipiert. Der Betrieb soll zentral durch das Kompetenzzentrum für IT-Fachverfahren beim

Staatlichen Schulamt Wünsdorf erfolgen, das seinerseits den Brandenburgischen IT-Dienstleister (ZIT-BB) mit der Erbringung der erforderlichen Rechenzentrumsdienstleistungen beauftragt. Vonseiten unserer Behörde werden sowohl die Bereitstellung einer einheitlichen Schulverwaltungssoftware als auch der vorgesehene zentrale Betrieb grundsätzlich begrüßt. Schulträger bzw. Schulen können auf diese Weise bei der Beschaffung und Wartung der Programme entlastet, der Konfigurations- und Administrationsaufwand verringert und die Datensicherheit erhöht werden. Außerdem lässt sich der Datenaustausch zu anderen Fachverfahren (wie z. B. der Schulstatistik) vereinfachen.

Aus Beschwerden, Prüfungen vor Ort sowie Gesprächen mit Schulträgern und dem Ministerium ist uns bekannt, dass Schulleitungen häufig Probleme haben, einen datenschutzgerechten und sicheren Betrieb von Hard- und Software zu gewährleisten sowie dort die erforderlichen technischen und organisatorischen Maßnahmen vollständig umzusetzen.⁵⁹ Ein Schritt zur Verbesserung der Situation kann die nun vorgesehene Zentralisierung des Betriebs des Schulverwaltungsprogramms beim Brandenburgischen IT-Dienstleister sein. Die gem. § 7 Abs. 3 Brandenburgisches Datenschutzgesetz (BbgDSG) aus einer Risikoanalyse abgeleiteten und im IT-Sicherheitskonzept dokumentierten Sicherheitsmaßnahmen sind bezüglich der zentralen Systemkomponenten nur einmal und für alle Schulen gemeinsam umzusetzen (z. B. Gebäude- und Raumsicherung im Rechenzentrum, Konfiguration und Betrieb von Datenbank- und Applikationsservern, Softwareaktualisierungen, Virenschutz, Betrieb von Firewalls, Datensicherung). In den Schulen selbst sind nur noch die verbleibenden technischen und organisatorischen Maßnahmen (z. B. zur Absicherung der Arbeitsplatz-PCs, Vergabe von Rollen und Zugriffsrechten, Belehrung des Schulpersonals) zu realisieren. Diese können im Rahmen einer einfach zu handhabenden und zentral bereitgestellten Checkliste zusammengefasst werden.

Detaillierte Verfahrensunterlagen zum Projekt weBBschule wurden uns im Frühjahr 2013 durch das Bildungsministerium zur Verfügung gestellt. Hierzu gehörten das IT-Sicherheitskonzept für die zentralen Verfahrenskomponenten, die o. g. Checkliste mit in den Schulen umzusetzenden technischen und organisatorischen Maßnahmen, das Muster eines Verfahrensverzeichnisses gem. § 8 BbgDSG sowie ein Vertrag zur Datenverarbeitung im Auftrag gem. § 11 BbgDSG zwischen dem Ministerium als oberster Schulaufsichtsbehörde und dem Kompetenzzentrum für IT-Fachverfahren (mit einem Unterauftrag für den ZIT-BB). Insbesondere das IT-Sicherheitskonzept für die zentralen Komponenten wurde dabei noch nicht allen datenschutzrechtlichen Anforderungen gerecht, da einige wesentliche technische und organisatorische Maß-

⁵⁹ siehe B 13.2

nahmen nicht bzw. nicht vollständig umgesetzt waren. Weiterhin haben wir die Projektverantwortlichen darauf hingewiesen, dass auch bei einer Zentralisierung der Datenverarbeitung eine Trennung der Verarbeitung gem. § 7 Abs. 1 BbgDSG nach Schulen – eine sogenannte Mandantentrennung⁶⁰ – zu gewährleisten ist. Nur so können aus unserer Sicht Vertraulichkeit und Integrität der zentral verarbeiteten personenbezogenen Daten sichergestellt werden.

Die Schulen haben zu beachten, dass sie weiterhin Daten verarbeitende Stellen und somit verantwortlich für die Verarbeitung der personenbezogenen Daten der Schüler, Eltern und Lehrer sind. Insofern haben sie für ihren Verantwortungsbereich die erforderlichen technischen und organisatorischen Maßnahmen gem. Checkliste umzusetzen, die Freigabe des Verfahrens zu erklären und ein Verfahrensverzeichnis gem. § 8 BbgDSG vorzuhalten. Durch die Bereitstellung eines Musters des Verfahrensverzeichnisses verringert sich der Verwaltungsaufwand hierbei. Dem Kompetenzzentrum für IT-Fachverfahren haben wir empfohlen, Schulen erst dann die Zugangsdaten zum zentralen Programmsystem zu übermitteln, wenn vor Ort alle datenschutzrechtlichen Anforderungen erfüllt sind und die Freigabe durch die Schule erklärt wurde.

Die Einführung eines einheitlichen Schulverwaltungsprogramms für alle Schulen Brandenburgs und der zentrale Betrieb dieses Verfahrens können grundsätzlich zu einer Verbesserung des Datenschutzes und der Informationssicherheit bei der Verarbeitung personenbezogener Daten von Schülern, Lehrern und Eltern führen. Hierfür ist es jedoch erforderlich, dass die technischen und organisatorischen Maßnahmen für die zentralen und dezentralen Verfahrenskomponenten umgesetzt, eine Mandantentrennung im Verfahren realisiert und jede Schule ihrer Verantwortung als Daten verarbeitende Stelle gerecht wird.

13.2 Mangelhafter Datenschutz an einem Gymnasium

Im Berichtszeitraum wurden wir auf offensichtliche Mängel bei der Umsetzung der datenschutzrechtlichen Vorschriften an einem Gymnasium hingewiesen. Unsere Prüfung bestätigte diese.

Wir stellten fest, dass im Hinblick auf die Sicherheit der elektronischen Datenverarbeitung erhebliche Defizite bestanden. So war z. B. der Serverraum nicht ausreichend gegen unberechtigte Zutritte, Einbruch und Brand gesichert sowie Server auch für Unbefugte zugänglich. Datensicherungen wurden nicht gesondert aufbewahrt. Mängel traten auch bezüglich der Berechtigungen

⁶⁰ siehe B 2.1

zum Zugriff auf personenbezogene Daten auf. Weiter waren Unterlagen wie Verträge zur Datenverarbeitung im Auftrag, Verzeichnisse und Sicherheitskonzepte nicht vorhanden. Akten mit personenbezogenen Daten lagerten teilweise in unverschlossenen Schränken. Ein behördlicher Datenschutzbeauftragter war nicht bestellt.

Nach unseren Erfahrungen sind dies Probleme, die an einer Reihe brandenburgischer Schulen auftreten. Die Schule ist verantwortliche Daten verarbeitende Stelle und damit für die Einhaltung der datenschutzrechtlichen Anforderungen des Brandenburgischen Schulgesetzes und der Datenschutzverordnung Schulwesen zuständig. Zum großen Teil kann sie selbst für Abhilfe bei entsprechenden Mängeln sorgen. Dazu ist es jedoch notwendig, das Personal entsprechend zu schulen und auch personelle sowie zeitliche Kapazitäten für die Durchsetzung des Datenschutzes zu schaffen.

Einige gravierende Probleme, insbesondere im technisch-organisatorischen Datenschutz können die Schulen allerdings nicht allein lösen. Hier sind einerseits die Schulträger in der Pflicht, die notwendige materielle Ausstattung zur Verfügung zu stellen. Dies umfasst z. B. bauliche Voraussetzungen, die einen effektiven Datenschutz ermöglichen sowie die Ausstattung mit Hard- und Software. Andererseits müssen auch vonseiten der obersten Schulbehörde Hilfestellungen z. B. in Form standardisierter Verträge und Formulare erfolgen. Viele Datenschutzprobleme treten in der gleichen Form an mehreren Schulen auf, sodass zentrale Vorgaben und Handreichungen das Datenschutzniveau an brandenburgischen Schulen flächendeckend erhöhen könnten. Wir stehen hierzu mit dem Bildungsministerium im Kontakt.

Datenschutzrechtliche Probleme sind an brandenburgischen Schulen nicht die Ausnahme. Um dies zu ändern, bedarf es eines koordinierten Vorgehens aller Beteiligten. Das Personal in den Schulen muss entsprechend sensibilisiert und fortgebildet werden. Darüber hinaus sind die materiellen Voraussetzungen zu schaffen, die einen effektiven Datenschutz ermöglichen.

13.3 Schülerdaten – begehrte Informationen für Krankenkassen.

Im Rahmen sog. Informationsveranstaltungen versuchen Unternehmen, personenbezogene Daten von Schülern zu erheben, um sich zukünftige Kunden zu sichern. Datenschutzrechtliche Vorschriften werden dabei zum Teil umgangen.

Im Berichtszeitraum informierte uns ein Petent, dass Mitarbeiter einer Krankenversicherung in einer sog. Informationsveranstaltung Schüler der 9. Klasse eines Gymnasiums aufforderten, persönliche Daten wie Anschrift,

E-Mailadresse, den gegenwärtigen Versicherungsschutz sowie die Telefonnummer anzugeben. Da eine gesetzliche Grundlage für diese Datenerhebung nicht existiert, hätte eine wirksame Einwilligung zur Datenverarbeitung eingeholt werden müssen. Schüler einer 9. Klasse sind regelmäßig nicht volljährig und damit nicht geschäftsfähig. Die Eltern der Schüler hätten deshalb in die Datenverarbeitung einwilligen müssen. Dies ist nicht erfolgt. Somit war die Datenerhebung durch die Mitarbeiter der Krankenkasse rechtswidrig.

Zwar hatte die Schule in diesem Fall nicht selbst gegen datenschutzrechtliche Bestimmungen verstoßen. Durch die Genehmigung der sog. Informationsveranstaltung wurde jedoch die Möglichkeit zu der rechtswidrigen Datenverarbeitung geschaffen. Die Schulen haben dafür Sorge zu tragen, dass bei Veranstaltungen Dritter im schulischen Bereich das Recht der Schüler auf informationelle Selbstbestimmung vollumfänglich gewahrt wird.

Schulen, die Veranstaltungen von Dritten im Rahmen des Schulbetriebes zulassen, sind in der Pflicht, die Schüler vor Eingriffen in deren Grundrechte zu schützen.

14 Telekommunikation und Medien

14.1 Internet Sweep Day 2013

Im Berichtszeitraum haben 19 Aufsichtsbehörden aus unterschiedlichen Ländern erstmals eine weltweit abgestimmte Datenschutzprüfung vorgenommen. Sie gingen der Frage nach, ob Unternehmen auf ihren Internetseiten und in ihren Applikationen für mobile Endgeräte die datenschutzrechtliche Grundanforderung der Transparenz einhalten. Unsere Behörde nahm an dieser Prüfung teil.

Das „Global Privacy Enforcement Network“ (GPEN)⁶¹ ist ein internationales Netzwerk zur grenzübergreifenden Förderung der Kooperation zwischen Datenschutzbehörden. Ein wesentliches Arbeitsgebiet des Netzwerks besteht in der Abstimmung von Prüfgegenständen und Prüftätigkeiten sowie in konzertierten Aktionen zur Kontrolle ausgewählter datenschutzrechtlicher Aspekte.

Im Jahr 2013 einigten sich die teilnehmenden Aufsichtsbehörden, die Sweep Working Group, für ihre abgestimmte Kontrolle auf das Thema „Privacy Practice Transparency“, also die Einhaltung der datenschutzrechtlichen Grundan-

⁶¹ siehe <https://www.privacyenforcement.net>

forderung der Transparenz. Durch die Gewährleistung der Transparenz sollen Betroffene die Verarbeitung ihrer personenbezogenen Daten nachvollziehen können. Daten verarbeitende Stellen müssen hierzu auf ihren Websites und in Applikationen für mobile Endgeräte (Apps) Informationen zum Umgang mit den personenbezogenen Daten verfügbar machen. Die Informationen müssen verständlich und leicht auffindbar sein. Für die abgestimmte Prüfung und zur Vergleichbarkeit der Ergebnisse vereinbarten die Aufsichtsbehörden deshalb folgende Indikatoren:

- Verfügbarkeit: Gibt es auf der jeweiligen Website oder in der jeweiligen App eine Datenschutzerklärung oder vergleichbare Informationen zum Datenschutz?
- Auffindbarkeit: Wie schwer ist es, diese Informationen zu finden?
- Erreichbarkeit: Sind Kontaktinformationen z. B. für Fragen zum Datenschutz oder für datenschutzrechtliche Beschwerden ohne Weiteres verfügbar?
- Verständlichkeit: Wie verständlich sind die Datenschutzerklärung oder die vergleichbaren Informationen, insbesondere im Hinblick auf die Zielgruppe?
- Relevanz: Wie gut behandeln die Datenschutzerklärung oder die vergleichbaren Informationen allgemeine datenschutzrechtliche Fragen?

Die Prüfung selbst wurde in der 19. Kalenderwoche 2013 durchgeführt. Jede teilnehmende Aufsichtsbehörde wählte in ihrem Zuständigkeitsbereich eine Reihe von Unternehmen aus und kontrollierte deren Websites bzw. Apps hinsichtlich der genannten Indikatoren. Weltweit wurden insgesamt mehr als 2.200 Internetseiten und Apps untersucht. Die Auswertung der Ergebnisse zeigte, dass 23 % der Anbieter gar keine Informationen zur Verarbeitung personenbezogener Daten ihrer Nutzer bereitstellen. Bei über die Hälfte der untersuchten Angebote wurden ein oder mehrere Mängel festgestellt, im Falle mobiler Applikationen betrug die Mängelrate sogar über 90 %.

Für das Land Brandenburg haben wir am 17. Mai 2013 ausschließlich Websites in Bezug auf die Einhaltung der vereinbarten Transparenzkriterien geprüft. Betreiber und damit Daten verarbeitende Stellen waren vorrangig lokale Energieversorger und Stadtwerke. Die Auswertung ergab, dass fast alle Angebote (90 %) zwar über eine Datenschutzerklärung verfügen. Diese ist jedoch häufig inhaltlich zu überarbeiten, um Verständlichkeit und Relevanz der Informationen zu erhöhen.

Der erste weltweite Internet Sweep Day 2013 deckte z. T. erhebliche Mängel bei der Einhaltung der datenschutzrechtlichen Grundanforderung der Transparenz auf Websites und in Applikationen für mobile Endgeräte auf. Wir werden auch in Zukunft an derartigen, international abgestimmten Prüfkaktivitäten von Datenschutzaufsichtsbehörden teilnehmen.

14.2 Prüfung des Einsatzes von Google Analytics

Betreiber von Webseiten interessieren sich häufig für die Reichweite und Nutzungsstatistiken ihrer Angebote. Sie verwenden hierzu gern entsprechende Analysewerkzeuge (sogenannte Tracking Tools) wie z. B. Google Analytics. Während der datenschutzkonforme Einsatz von Google Analytics durch nicht öffentliche Stellen unter bestimmten Bedingungen möglich ist, müssen öffentliche Stellen hierauf nach wie vor verzichten.

Bereits in unserem letzten Tätigkeitsbericht⁶² hatten wir die wesentlichen Bedingungen zusammengefasst, die nicht öffentliche Stellen wie Unternehmen erfüllen müssen, wenn sie Google Analytics auf ihren Webseiten datenschutzgerecht einsetzen wollen. Hierzu gehören der Abschluss eines schriftlichen Vertrags mit dem Unternehmen Google über die Datenverarbeitung im Auftrag gem. § 11 Bundesdatenschutzgesetz (BDSG), die Verwendung einer Funktion zur Anonymisierung der IP-Adresse des Webseitenbesuchers durch Google im Quelltext der Webseite sowie die Aufklärung der Webseitenbesucher über die Erfassung ihrer Daten mit Google Analytics und über Möglichkeiten zur Verhinderung dieser Erfassung (Opt-Out durch Installation von Webbrowser Plugins). Ggf. mit früheren Versionen von Google Analytics unzulässig erhobene Altdaten sind zu löschen. Zusätzlich ist der Webseitenbetreiber verpflichtet, auch für alternative Webbrowser, insbesondere für Browser von Smartphones, eine Widerspruchslösung zu implementieren. Dazu muss er den Quellcode seiner Webseiten so modifizieren, dass mittels eines Schalters die Datenerfassung der Webseitenbesucher programmgesteuert unterbunden wird. Eine exemplarische Lösung hierfür wird von Google publiziert.⁶³

Öffentlichen Stellen im Land Brandenburg ist es zurzeit nicht möglich, einen datenschutzgerechten Betrieb von Google Analytics zu gewährleisten. Hintergrund ist u. a., dass kein Vertrag mit dem Unternehmen Google zur Datenverarbeitung im Auftrag gem. § 11 Brandenburgisches Datenschutzgesetz geschlossen werden kann, da Google eine Anpassung des mit den Aufsichtsbehörden abgestimmten Mustervertrags zur Datenverarbeitung im

⁶² vgl. Tätigkeitsbericht 2010/2011, A 3.2

⁶³ siehe <https://developers.google.com/analytics/devguides/collection/gajs/?hl=de#disable>

Auftrag im nicht öffentlichen Bereich nach § 11 BDSG an landesspezifische Besonderheiten bisher konsequent ablehnt.

Wir haben im Berichtszeitraum die Webseiten von 275 öffentlichen Stellen des Landes Brandenburg (u. a. von Ministerien, Landesämtern, Finanzämtern, Kreisverwaltungen, Ämtern und Gemeinden) automatisiert auf die Verwendung von Google Analytics untersucht. Ergebnis war, dass 37 Stellen (13 %) rechtswidrig den Tracking Code von Google Analytics in ihren Webseiten verwendeten. Gemeinden analysierten dabei die Besucher ihrer Webseiten besonders häufig (19 %) unerlaubterweise.

Eine stichprobenhafte Prüfung von Webseiten privatrechtlich organisierter Institutionen, hier von brandenburgischen Krankenhäusern und Kliniken, ergab, dass insgesamt 25 % der Einrichtungen Google Analytics einsetzen. Bei der Mehrzahl der geprüften Webseiten (15 %) scheint ein datenschutzkonformer Betrieb gegeben zu sein, da eine Anonymisierung der IP-Adressen der Webseitenbesucher vorgenommen wird. Eine abschließende Aussage kann jedoch erst nach einer weitergehenden Abfrage erfolgen, insbesondere zur Existenz eines Vertrags nach § 11 BDSG. Die übrigen 10 % der Einrichtungen nutzen Google Analytics offensichtlich nicht datenschutzkonform, da die IP-Adressen der Webseitenbesucher nicht anonymisiert werden.

Im Land Brandenburg nutzen eine Reihe öffentlicher Stellen sowie einige privatrechtlich organisierte Krankenhäuser und Kliniken Google Analytics rechtswidrig. Wir werden verstärkt darauf hinwirken, dass diese Stellen die Bedingungen für einen datenschutzkonformen Einsatz von Google Analytics einhalten oder Alternativen zur Reichweitenanalyse datenschutzgerecht verwenden.

14.3 Orientierungshilfe Soziale Netzwerke

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine Orientierungshilfe⁶⁴ für Betreiber sozialer Netzwerke herausgegeben. Sie richtet sich darüber hinaus an Stellen, die mithilfe solcher Netzwerke eigene Aufgaben erfüllen oder Geschäftszwecke verfolgen.

Zu Beginn des Jahres 2013 wurde bekannt, dass die wichtigsten Betreiber sozialer Netzwerke, wie Facebook, Google, LinkedIn und Xing nicht bereit waren, den Entwurf einer geplanten Selbstverpflichtung zum Schutz der Privatsphäre der Nutzer zu unterzeichnen. Damit war das vom Bundesinnenministerium initiierte Projekt endgültig gescheitert.

⁶⁴ siehe <http://www.lida.brandenburg.de>

Vor diesem Hintergrund ist es Ziel der Orientierungshilfe, neben der Konkretisierung der gesetzlichen Mindeststandards auch Best-Practice-Ansätze aufzuzeigen, soweit der gesetzliche Normierungsrahmen Lücken hinsichtlich eines ausreichenden Schutzes des Rechts auf informationelle Selbstbestimmung und des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aufweist. Die Darstellung zielt auf die datenschutzrechtliche Bewertung der verschiedenen „Schichten“ sozialer Netzwerke. Diese Schichten setzen sich aus den Inhaltsdaten, Bestandsdaten und Nutzungsdaten zusammen.

Auf eine Trennung zwischen der Darstellung technischer und rechtlicher Anforderungen wird in der Orientierungshilfe bewusst verzichtet. Vielmehr wurden als Leitlinie die Schutzziele der Datensicherheit und des Datenschutzes, Vertraulichkeit, Integrität, Verfügbarkeit, Intervenierbarkeit, Transparenz und Nichtverkettbarkeit (Zweckbindung) herangezogen.

Außerhalb des Fokus liegen die privaten Nutzer sozialer Netzwerke. Die Orientierungshilfe ist insofern keine Anleitung für den datenschutzgerechten Gebrauch solcher Netzwerke. Hinweise und Anleitungen für Nutzer derartiger Dienste werden von verschiedenen Datenschutzbehörden und anderen Einrichtungen zur Verfügung gestellt.

Angesichts der zunehmenden Bedeutung sozialer Netzwerke weist die Datenschutzkonferenz deren Betreiber auf ihre Verpflichtung hin, die Einhaltung datenschutzrechtlicher Anforderungen sicherzustellen. Auch Unternehmen und öffentliche Stellen, die soziale Netzwerke nutzen, müssen diesen Anforderungen Rechnung tragen.

14.4 Fotos von Badegästen im Internet

Die Thermen und Badelandschaften im Land Brandenburg werben verstärkt im Internet um Kundschaft. Um sich interessant zu präsentieren, nehmen sie es, wie zwei Fälle aus dem Berichtszeitraum zeigen, mit dem Recht am eigenen Bild der Badegäste nicht immer ganz genau.

Ein Petent informierte uns darüber, dass in einer Therme regelmäßig sog. Saunaevents stattfinden. Bei diesen Veranstaltungen fertigten Mitarbeiter Fotoaufnahmen, die dann im Foyer der Therme und zum Teil in deren Internetangebot veröffentlicht wurden. Eine Einwilligung der Abgebildeten wurde nicht eingeholt. Auch erfolgte beim Erwerb der Eintrittskarte kein Hinweis auf die vorgesehenen Aufnahmen. Die Abbildungen zeigten zum Teil völlig unbedeckte Menschen, deren Mimik oder Körperhaltung signalisierte, dass ihnen die Aufnahmen unangenehm waren. Es konnte deshalb nicht von einer Einwilligung aller Abgebildeten durch schlüssiges Verhalten ausgegangen wer-

den. Einzige Möglichkeit der ungewollten Abbildung zu entgehen, war es, trotz bezahltem Eintritt die Veranstaltung zu verlassen.

Das Abbilden von nackten Menschen ist regelmäßig ein schwerer Eingriff in das Persönlichkeitsrecht der Betroffenen. Hier wird immer die sog. Intimsphäre verletzt, solange keine ausdrückliche Einwilligung in die Anfertigung und ggf. die Veröffentlichung der Fotos erfolgt ist. Auf unsere Intervention hin wurden die betreffenden Fotos aus dem Internetangebot entfernt. Weiter erließ die Leitung der Therme eine Dienstanweisung, die jeden Mitarbeiter verpflichtet, von allen Teilnehmern der Saunaevents eine Einwilligung einzuholen. Ist dies nicht möglich, unterbleiben die Fotoaufnahmen.

Durch eine uns vorliegende Beschwerde eines Besuchers eines weiteren Thermalbades erfuhren wir, dass im Eingangsbereich des Bades die Möglichkeit bestand, sich durch einen Automaten vor einer bunten Leinwand fotografieren zu lassen. Diese Fotos wurden dann sofort und ohne Nachfrage auf der Facebook-Fanpage des Bades veröffentlicht. Da die Anlage für jeden frei zugänglich und unbewacht war, hatten sich insbesondere auch Kinder dort selbst fotografiert.

Erläuterungen an dem Gerät informierten den Nutzer zwar darüber, dass die dort aufgenommen Bilder über die Facebook-Fanpage des Bades im Internet verbreitet werden. Durch die Betätigung der Schaltfläche setzte der Besucher nach Kenntnisnahme der Erläuterung den Aufnahme- und damit auch Verbreitungsvorgang selbstständig und freiwillig in Gang. Dies ist grundsätzlich als Einwilligung im Sinne von § 22 Kunsturhebergesetz anzusehen. Uneingeschränkt gelten kann dies aber nur für geschäftsfähige (volljährige) Personen. Kindern und Jugendlichen unter 18 Jahren oder aus anderen Gründen nicht geschäftsfähigen Personen ist es rechtlich nicht möglich, wirksam in die Verbreitung ihrer Fotos einzuwilligen. Es bedarf hier zwingend der Einwilligung der gesetzlichen Vertreter. Da die Leitung des Bades nicht gewährleisten konnte, dass die notwendigen Einwilligungen in jedem Fall vorliegen, wurden das Abbildungsgerät demontiert und die bereits im Internet veröffentlichten Fotos entfernt.

Die Anfertigung und Veröffentlichung von Fotografien bedarf auch für Werbezwecke grundsätzlich der Einwilligung der darauf abgebildeten Personen. Kinder und Jugendliche unter 18 Jahren können selbst keine wirksame Einwilligung erteilen.

15 Verkehr

15.1 Gemeinsame Kraftfahrzeugzulassung

Eine kreisfreie Stadt und der sie umgebende Landkreis haben in einem Kooperationsprojekt vereinbart, Aufgaben der Kraftfahrzeugzulassung auch für die jeweils andere Behörde wahrzunehmen. Seit Anfang 2013 können die Einwohner dadurch ihr Auto auch im jeweils anderen Zuständigkeitsbereich zulassen bzw. ummelden. Zu Fragen der datenschutzgerechten Verarbeitung der durch die erweiterte Zuständigkeit betroffenen Bürgerdaten haben wir das Projekt beraten.

Die Verarbeitung der Zulassungsdaten erfolgt stets über das Zentrale Fahrzeugregister des Kraftfahrt-Bundesamtes. Es gibt keine direkten Zugriffe auf lokale Datenbanken des jeweiligen Kooperationspartners. Die Berechtigungen zum Zugriff auf die notwendigen Zulassungsdaten sind auf das für die Erfüllung der Aufgabe erforderliche Maß begrenzt. Liegen den Zulassungsanträgen wichtige Unterlagen bei, werden diese eingescannt und verschlüsselt über einen für die beteiligten Zulassungsstellen zugänglichen Server ausgetauscht. Für die automatische Datenlöschung auf dem Austauschserver existieren enge Fristen. Ein Verfahrensverzeichnis und eine verfahrensspezifische Risikoanalyse wurden erstellt. Zudem gibt es klare organisatorische Richtlinien für die Nutzer, wie Anträge im Rahmen der erweiterten Zuständigkeit zu bearbeiten sind und wie insbesondere der Datentransfer über den Austauschserver durchzuführen ist.

Um sicherzustellen, dass bei Verfahren, in denen personenbezogene Daten automatisiert verarbeitet werden, auch alle erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen zum Schutz der Daten ergriffen werden, muss gem. § 7 Abs. 3 Brandenburgisches Datenschutzgesetz neben einer Risikoanalyse auch ein Sicherheitskonzept erstellt werden. Das vorgelegte Konzept für den Datenaustauschserver ließ erkennen, dass alle Datenübertragungswege mittels SSL verschlüsselt werden, eine differenzierte Rechteverwaltung der Benutzer umgesetzt und ein angemessener Schutz des zugrunde liegenden Webservers implementiert ist. Wir haben angeregt, zusätzlich einen IP-Filter einzurichten, sodass nur von Rechnern mit einer IP-Adresse aus den zugelassenen IP-Adressbereichen auf die Weboberfläche zugegriffen werden kann. Des Weiteren fehlte im Sicherheitskonzept noch die Bearbeitung einiger Bausteine der IT-Grundschutz-Kataloge des Bundesamtes für Sicherheit in der Informationstechnik, die jedoch kurzfristig nachzuholen ist. Eine Umsetzung der erforderlichen Maßnahmen wurde von den Verantwortlichen zugesagt.

Sollen Verwaltungszuständigkeiten im Rahmen von Projekten zur Steigerung der Bürgerfreundlichkeit erweitert werden, sind immer auch die datenschutzrechtlichen Anforderungen zu beachten. Die beteiligten Kfz-Zulassungsstellen haben diese Anforderungen von Anfang an berücksichtigt. Verbesserungen der Informationssicherheit können im Rahmen regelmäßiger Änderungsprozesse erzielt werden.

15.2 Umfrage zur Videoüberwachung im öffentlichen Personennahverkehr in Brandenburg

Der öffentliche Personennahverkehr (ÖPNV) in Brandenburg wird von einer Vielzahl regionaler Verkehrsunternehmen betrieben. Wir wollten einen Überblick darüber gewinnen, inwieweit hierbei Videoüberwachung eingesetzt wird und haben einen Fragebogen an die betreffenden Unternehmen mit Sitz im Land Brandenburg versandt. Die Auswertung der Umfrage ergab einen erheblichen Anteil an videoüberwachenden Unternehmen. Der Schwerpunkt der Überwachung liegt im Schienenverkehr.

Wenn private Unternehmen öffentlich zugängliche Räume mit Videokameras beobachten, ist dies gem. § 6b Bundesdatenschutzgesetz (BDSG) nur zulässig, soweit es zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Im öffentlichen Personennahverkehr darf die Videoüberwachung nur zum Schutz vor Gewalt gegen Personen und Beförderungseinrichtungen oder zur technischen Fahrgastsicherheit erfolgen. Es darf keinen Automatismus beim Einsatz von Videokameras geben – vielmehr ist in jedem Einzelfall zu prüfen, ob eine Videoüberwachung für den beabsichtigten Zweck tatsächlich erforderlich ist, die schutzwürdigen Interessen der beobachteten Personen nicht überwiegen und auch kein milderer Mittel zur Verfügung steht, das zur Zweckerreichung eingesetzt werden kann. Der verfolgte Zweck muss zuvor schriftlich festgelegt werden. Eine Verarbeitung zu anderen als den festgelegten Zwecken darf gem. § 6b Abs. 3 Satz 2 BDSG nur erfolgen, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist. Die Einrichtung einer Videoüberwachung erfordert gem. § 4d Abs. 5 BDSG eine Vorabkontrolle des betrieblichen Datenschutzbeauftragten des Unternehmens.

Im Rahmen unserer Umfrage wurden 39 Unternehmen befragt, die über insgesamt 1632 Busse und 137 Bahnen für den Einsatz im öffentlichen Personennahverkehr verfügen. Nicht zu den befragten Unternehmen gehörten die DB Regio AG mit dem Regionalbahnverkehr der Deutschen Bahn und die S-Bahn Berlin GmbH, da beide ihren Sitz nicht im Land Brandenburg haben.

Von den 39 befragten Unternehmen führen 18 Unternehmen (46 %) Videoüberwachungsmaßnahmen in insgesamt 441 Bussen (27 %) und 103 Bahnen (75 %) durch.

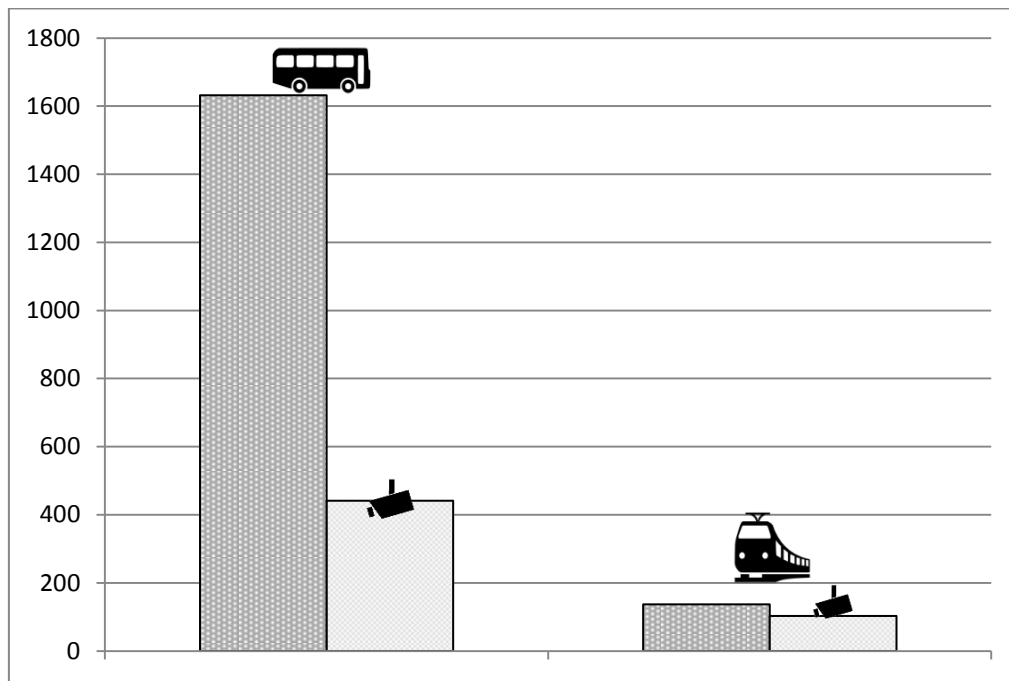


Abb. 15.1: Anteil videoüberwachter Busse und Bahnen

Unter dem Begriff „Videoüberwachung“ haben wir bei unserer Umfrage jeglichen Einsatz von Videokameras mit oder ohne Aufzeichnung (sog. Live-Monitoring) verstanden. In Brandenburg findet Videoüberwachung im öffentlichen Personennahverkehr ausnahmslos mit Bildaufzeichnung statt. Die reine Beobachtung ohne Aufzeichnung wird nicht eingesetzt.

Fast ausschließlich finden die Videomaßnahmen dabei als Innenraumüberwachung von Bussen und Bahnen statt. Eine Überwachung von Haltestellen, Bahnsteigen oder Fahrkartenautomaten kommt nicht vor. Allerdings sind zehn Straßenbahnen an der Außenhülle mit Videokameras an Stelle von Rückspiegeln ausgestattet, um für den Fahrer die Nachtsicht zu verbessern, die Blendwirkung zu reduzieren und die Möglichkeit zur Auswertung von Unfällen zu nutzen. Durch diese Rückspiegelkameras wird ein Teil des Ein-/Ausstiegsbereichs mit erfasst. Soweit es sich hierbei um öffentliches Straßenland handelt, werden die Videoaufnahmen nach 10 Minuten gelöscht.

Als Zweck der Videoüberwachung gaben alle 18 überwachenden Unternehmen die Beweisführung bei Sachbeschädigung an. 17 Unternehmen nannten als Zweck den Beweis bei Gewalt gegen Fahrgäste. Der Zweck „Beweis bei Gewalt gegen Beschäftigte“ ist für 15 Unternehmen ein Grund für den Einsatz von Videoüberwachung. 6 Unternehmen gaben an, die Videoüberwachung zur technischen Fahrgastsicherheit einzusetzen.

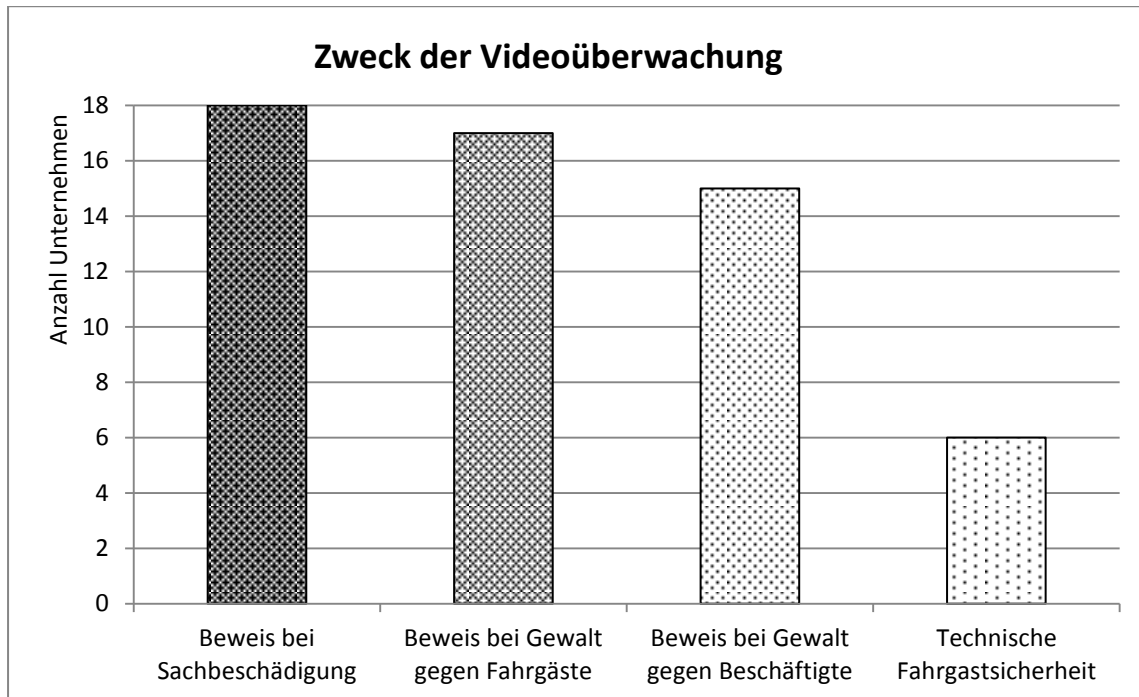


Abb. 15.2: Angaben zum Zweck der Videoüberwachung

Die Speicherdauer der Videoaufnahmen bewegt sich zwischen 24 und 96 Stunden, falls kein besonderes Vorkommnis auftritt. Der größte Anteil, auf die Anzahl der Fahrzeuge gerechnet, liegt bei 48 oder 72 Stunden: In 76 % aller Fahrzeuge wird mit dieser Speicherdauer überwacht. Das untere und das obere Ende (24 bzw. 96 Stunden) umfasst je 4 % der Fahrzeuge. In 7 % der Fahrzeuge dauert die Speicherung ohne Vorkommnis 36 Stunden an. Im übrigen Anteil variiert die Speicherdauer in Abhängigkeit von der vorhandenen Technik zwischen einem und vier Tagen (24 bis 96 Stunden).

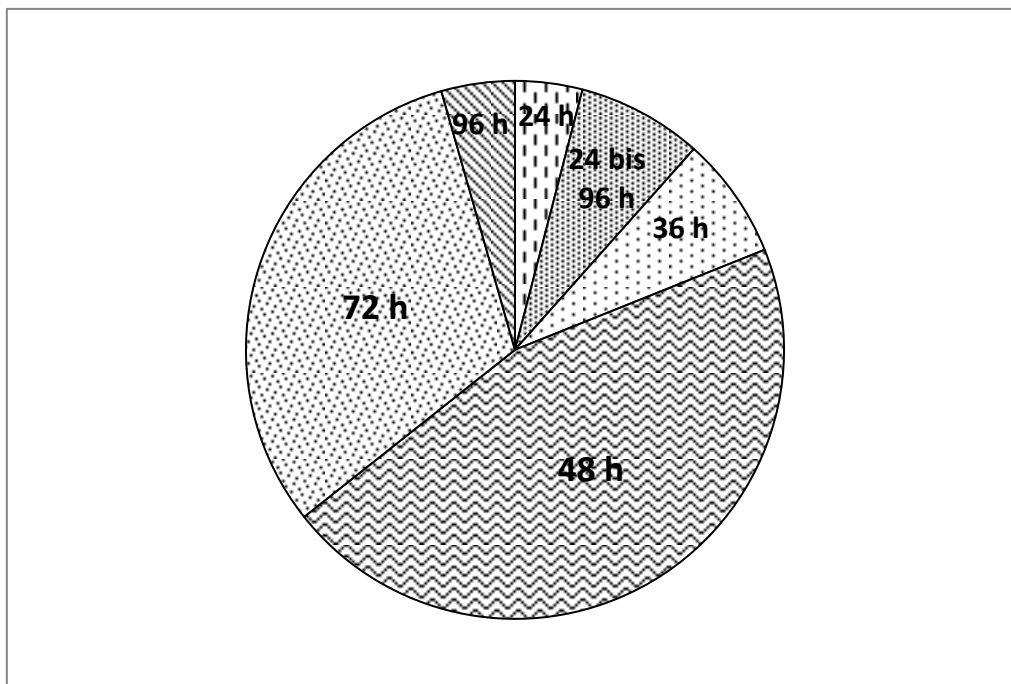


Abb. 15.3: Speicherdauer der Videoaufnahmen bezogen auf die Fahrzeuganzahl

Die Speicherdauer wurde von vielen Unternehmen mit innerbetrieblichen Abläufen begründet, die eine Feststellung von Vorkommnissen und eine entsprechende Sicherung der Videodaten auch über ein Wochenende oder über Feiertage hinweg ermöglichen sollen. Allerdings haben einige Unternehmen die Speicherdauer mit angeblichen technischen Vorgaben oder überhaupt nicht begründet. Dies ist aus datenschutzrechtlicher Sicht nicht akzeptabel, da die Löschung der Bilddaten unverzüglich zu erfolgen hat, wenn kein Vorkommnis festgestellt wurde. Es muss daher im Einzelfall nachvollziehbar die kürzest mögliche Frist festgelegt und entsprechend begründet werden. Technische Vorgaben dürfen hierbei nicht ausschlaggebend sein.

Generell halten wir eine Speicherdauer von 48 Stunden für vertretbar. Um das Wochenende bzw. Feiertage zu überbrücken, kann es im Einzelfall erforderlich sein, bis zu 72 Stunden zu speichern, um für den Fall eines Vorkommnisses noch auf Videobeweise zugreifen zu können. Eine längere Speicherdauer ist unseres Erachtens nur in Ausnahmefällen datenschutzrechtlich begründbar.

Fast alle Unternehmen gaben an, die erhobenen Bilddaten in einem speziell verschlossenen, nur besonders Berechtigten zugänglichen Aufzeichnungsgerät (Blackbox) zu speichern. Allerdings verfügen viele Unternehmen nicht über ausreichende organisatorische Regelungen zum Umgang mit den Aufzeichnungen. Um den datenschutzrechtlichen Anforderungen bei der Videoüberwachung von öffentlichen Verkehrsmitteln gerecht zu werden, sollte es schriftliche Festlegungen geben, welche Ereignisse als Vorkommnis im Sinne

der Beweisführung durch Videoüberwachung zu werten sind, welche Personen Zugang zu den Aufzeichnungen haben, wie Bilder zu Beweiszwecken zu sichern sind und wie die Datenweitergabe an Polizei bzw. Staatsanwaltschaft zu erfolgen hat. Sind Beschäftigte mit einbezogen, sollte auch eine Betriebsvereinbarung abgeschlossen werden.

16 der 18 überwachenden Unternehmen antworteten, dass in ihrem Verantwortungsbereich bereits Vorkommnisse auftraten, bei denen sie auf die Videoaufzeichnungen zurückgriffen. Beispielhaft wurden u. a. Sachbeschädigungen, Vandalismus, Gewalt gegen Fahrgäste oder Beschäftigte, aber auch Beschwerden wegen überfüllter Busse genannt. Insbesondere Letzteres ist allerdings kein datenschutzrechtlich zulässiger Grund zum Zugriff auf die Videodaten und stellt eine unzulässige Zweckänderung dar. An diesem Beispiel zeigt sich auch, wie wichtig umfassende und konkrete Regelungen zu den Videoüberwachungsmaßnahmen sind, damit der Zugriff auf die Videoaufnahmen tatsächlich auf den Schutz von Personen und Einrichtungen beschränkt bleibt.

Alle überwachenden Unternehmen machen die Videoüberwachung durch Hinweispiktogramme kenntlich. Manche Unternehmen brachten die Hinweise allerdings entweder nur im Innenraum der Fahrzeuge oder nur im äußeren Einstiegsbereich an. Eine ausreichende Information für die Fahrgäste muss jedoch beides umfassen, damit Kunden sowohl vor dem Einstieg in das Fahrzeug als auch beim Aufenthalt im Fahrzeug auf die stattfindende Videoüberwachung hingewiesen werden. Eine ausreichende Kenntlichmachung muss darüber hinaus auch immer die Bezeichnung der verantwortlichen Stelle mit Angabe der Anschrift umfassen, damit sich Betroffene zur Wahrnehmung ihrer Auskunftsrechte gegebenenfalls dorthin wenden können.

Unsere Umfrage hat ergeben, dass fast die Hälfte der brandenburgischen Verkehrsunternehmen Videoüberwachungsmaßnahmen in öffentlichen Verkehrsmitteln durchführen. Dabei ist der Schienenverkehr deutlich stärker betroffen als der Busverkehr. Verbesserungen sind bei einigen Unternehmen noch in Bezug auf Speicherfristen, organisatorische Regelungen und die Kenntlichmachung der Überwachung erforderlich. Außerdem ist immer die strenge Zweckbindung der Videoaufnahmen zu beachten.

15.3 Flughafen Berlin Brandenburg

Der Bau des Flughafens Berlin Brandenburg verursacht seit Jahren immer wieder Schlagzeilen. Neben vielen anderen Fragen ist auch die Einhaltung der datenschutzrechtlichen Belange durch die Flughafenbetreiber zu berücksichtigen. Im Berichtszeitraum haben wir mit den Verantwortlichen dazu erste Gespräche geführt.

Wichtigstes Thema der datenschutzrechtlichen Beratungen war das geplante Videoüberwachungssystem. Am zukünftigen Flughafen ist eine Vielzahl von Videokameras vorgesehen, die aus Gründen der Sicherheit und des reibungslosen Betriebsablaufes installiert werden sollen. Die Bilddaten aus den Videokameras werden an spezielle Arbeitsplätze übertragen und dort beobachtet und ausgewertet. Dazu berechtigt sind die Bundespolizei, die Deutsche Flugsicherung und der Bereich Flughafensicherheit der Flughafen Berlin Brandenburg GmbH. Die Speicherfrist für den von der Flughafengesellschaft überwachten Bereich beträgt 48 Stunden, für die Bundespolizei standardmäßig zehn Tage, bei besonderen Vorkommnissen 30 Tage. Die Deutsche Flugsicherung darf die Videoüberwachung nur zum Live-Monitoring im Rahmen der Betriebsführung verwenden, aber nicht auf gespeicherte Daten zugreifen.

Für die Zugriffsrechte auf das Videomanagementsystem, die Live-Bilder und die gespeicherten Daten gibt es ein abgestuftes Rollen- und Berechtigungskonzept, sodass nur berechtigte Personen in dem für sie erforderlichen Umfang Einsicht nehmen können. Auch die Zoombarkeit der Kameras ist auf das jeweils erforderliche Maß begrenzt.

Das Videomanagementsystem enthält eine automatisierte Bildanalysemöglichkeit, die sich auf zwei Muster beschränkt: Zum einen kann die Bewegungsrichtung von Personen in Fluchtszenarien (z. B. bei Katastrophen) erkannt werden, um Rettungsteams mit Informationen zu möglicherweise verirrtten Personen versorgen zu können. Zum anderen werden Gegenstände, die das Muster eines verlassenen Koffers haben, erkannt.

Grundsätzlich hat die Flughafengesellschaft die wesentlichen Anforderungen bei der Planung des Videoüberwachungssystems beachtet. Die Dokumentation zum Videomanagementsystem muss noch aus datenschutzrechtlicher Sicht bewertet werden. Wie sich die Umsetzung gestalten wird, bleibt abzuwarten. Hierzu muss die Flughafen Berlin Brandenburg GmbH noch verbindlich regeln, wer Entscheidungen dazu treffen kann, ob und wie eine konkrete Videokamera den datenschutzrechtlichen Anforderungen genügt.

Weitere Schwerpunkte unserer Beratungs- und Kontrolltätigkeit werden die Personaldatenverarbeitung, die Verarbeitung von Daten Beschäftigter aus Drittunternehmen, die Verarbeitung biometrischer Daten bei Zugangskontrollsystemen für Beschäftigte und die IT-Sicherheit in Rechenzentren sein.

Die Flughafengesellschaft muss auch in sicherheitssensiblen Bereichen des zukünftigen Flughafens die datenschutzrechtlichen Belange der Betroffenen berücksichtigen. Die bisherigen Gespräche zeigen, dass die Verantwortlichen diese Aufgabe ernst nehmen. Wir werden auch weiterhin die Umsetzung der datenschutzrelevanten Verfahren begleiten.

15.4 Auto-Cockpit-Kameras: Überwachung aus Kraftfahrzeugen

Um im Schadensfall über Beweise zu verfügen, beabsichtigen Unternehmen und Privatpersonen teilweise, ihre Fahrzeuge mit nach außen gerichteten Kameras auszustatten. Diese sollen das Verkehrsgeschehen im Umfeld ständig aufzeichnen und so den Hergang eines eventuellen Unfalls dokumentieren.

Die Zulässigkeit von Videoaufnahmen wird nur dann nicht durch die Vorgaben des Bundesdatenschutzgesetzes (BDSG) eingeschränkt, wenn die Datenverarbeitung ausschließlich für persönliche oder familiäre Zwecke – wie beispielsweise bei Familienaufnahmen aus dem Urlaub – erfolgt. Die Absicht der Beweissicherung für einen Schadensfall unterfällt nicht diesem rein privaten Gebrauch. Somit sind die gesetzlichen Voraussetzungen des § 6b BDSG zu beachten. Privatpersonen und Unternehmen ist es danach nur erlaubt, Videoüberwachung im öffentlich zugänglichen Raum zu betreiben, wenn dies zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass die schutzwürdigen Interessen der Betroffenen überwiegen.

Der Einsatzzweck zur Beweissicherung für einen Schadensfall dient nicht der Wahrnehmung des Hausrechts. Dieses Recht endet in der Regel an einer festen Grundstücks- oder Eigentumsgrenze, d. h. im konkreten Fall beschränkt es sich auf das Fahrzeug selbst. Öffentliche Verkehrsflächen (Straßen, Wege, Parkplätze) sind davon nicht umfasst.

Selbst wenn der Einsatz der sog. Auto-Cockpit-Kameras erforderlich wäre, um den angestrebten Dokumentationszweck zu erreichen, ist regelmäßig davon auszugehen, dass die schutzwürdigen Interessen der Betroffenen überwiegen. Bei der in der Regel sehr weitwinkligen Optik der genannten Kameras werden erhebliche Teile des Straßenlands vor und neben dem Fahrzeug einschließlich etwaiger Gehwege erfasst. Auf diese Weise geraten Passanten, wenngleich unbeabsichtigt und zufällig, in den Blick der Kameras. Auch die Kennzeichen anderer Fahrzeuge, die als personenbezogene Daten einzustufen sind, werden dabei aufgenommen. Das Recht des Einzelnen, sich in der Öffentlichkeit frei und ungezwungen zu bewegen, ohne befürchten

zu müssen, überwacht zu werden, wird so erheblich eingeschränkt. Hinzu kommt, dass die Kameras für die Betroffenen üblicherweise nicht zu erkennen sind, es sich somit um eine verdeckte Videoüberwachung handelt.

Für den Betrieb von Auto-Cockpit-Kameras, die das Verkehrsgeschehen auf öffentlich zugänglichen Straßen und Plätzen aufnehmen und dabei immer auch personenbezogene Daten erfassen, gibt es keine Rechtsgrundlage. Er ist daher unzulässig. Die Überwachung des öffentlichen Raums darf in der Regel nur durch die Polizei – und auch dann nur unter engen Voraussetzungen – erfolgen.

15.5 Videoüberwachung in Taxis

Immer wieder werden Taxifahrer Opfer von Raubüberfällen oder anderen Gewaltverbrechen. Die Täter haben dabei leichtes Spiel, da sie das Ziel der Fahrt und somit den Ort der Tat selbst bestimmen und mit ihrem Opfer allein sind. Darf der Innenraum von Taxis per Video überwacht werden, um solche Vorfälle zu verhindern oder die Strafverfolgung zu erleichtern?

Gemäß § 6b Bundesdatenschutzgesetz ist eine Beobachtung und Aufzeichnung mittels Videokameras nur zulässig, soweit dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Um Leben, Gesundheit und Freiheit der Taxifahrer zu schützen, kann der Einsatz von Videokameras in Betracht kommen. Allerdings müssen die Persönlichkeitsrechte der Fahrgäste, der angestellten Taxifahrer sowie anderer Verkehrsteilnehmer gewahrt bleiben.

Zunächst sind alternative Schutzmaßnahmen zu ergreifen, die weniger stark in die Persönlichkeitsrechte der Fahrgäste eingreifen, also beispielsweise die Möglichkeit, im konkreten Fall der Bedrohung einen Notruf abzusetzen. Auch darf die Videokamera nicht permanent betrieben werden; vielfach genügt es, einzelne Standbilder zu fertigen. Im Fall einer zulässigen Aufzeichnung sind die Bilder im Regelfall innerhalb von 24 Stunden, spätestens aber nach 48 Stunden zu löschen. Vor dem Einstieg sind die Fahrgäste zudem durch eine sichtbare Kennzeichnung auf den Umstand der Videoüberwachung hinzuweisen. Ein Zugriff auf die Bildaufzeichnungen durch Unbefugte ist auszuschließen. Außerdem muss die Überwachung auf den Fahrzeuginnenraum beschränkt bleiben.⁶⁵

⁶⁵ siehe B 15.4

Die Aufsichtsbehörden für den Datenschutz in der Privatwirtschaft haben zu diesem Thema einen Beschluss gefasst, um bundesweit zu einer einheitlichen Rechtsanwendung zu gelangen.⁶⁶

Um die körperliche Unversehrtheit oder das Eigentum der Taxifahrer zu schützen, kann der Einsatz von Videokameras in Betracht kommen. Im Interesse der Persönlichkeitsrechte von Fahrgästen muss die Kameraüberwachung jedoch auf das erforderliche Mindestmaß beschränkt werden.

16 Videoüberwachung

16.1 Neubau des Landtagsgebäudes in Potsdam

Nach dem Vorbild des ehemaligen Potsdamer Stadtschlusses wurde in den vergangenen Jahren in der Landeshauptstadt ein neues Landtagsgebäude errichtet. Damit befindet sich im unmittelbaren Innenstadtbereich ein Objekt mit hohem Sicherheitsbedarf. Eine Videoüberwachungsanlage, welche Bestandteil eines übergreifenden Sicherheitskonzeptes ist, dient neben anderen Maßnahmen mit dazu, die Sicherheit des Landtages zu gewährleisten.

Das Landtagsgebäude in Potsdams historischer Mitte soll zukünftig für die Öffentlichkeit grundsätzlich zugänglich sein. Es muss aber gleichzeitig auch den Sicherheitsanforderungen an ein Parlamentsgebäude und einen Parlamentsbetrieb genügen. Darüber hinaus besteht das Risiko von Fremdeinwirkungen, insbesondere von politisch motivierten Sachbeschädigungen. Um die weitgehende Zugänglichkeit mit dem erforderlichen Maß an Sicherheit zu verbinden und eine unmittelbare, flexible Reaktion auf sich verändernde Gefahrensituationen zu ermöglichen, erstellte die Landtagsverwaltung in Kooperation mit der Polizei sowie dem Bauträger eine umfassende Risikoanalyse und ein daraus abgeleitetes Sicherheitskonzept.

Eine wesentliche Komponente dieses Sicherheitskonzeptes ist die Videoüberwachungsanlage. Videokameras sind an der Außenhülle des Gebäudes umlaufend sowie an besonders sicherheitsrelevanten Stellen installiert. Die Landtagsverwaltung darf gemäß § 33c Brandenburgisches Datenschutzgesetz in Verbindung mit der Datenschutzordnung des Landtages Brandenburg öffentlich zugängliche Räume mit optisch-elektronischen Einrichtungen überwachen, soweit dies zur Erfüllung ihrer Aufgaben, zur Wahrnehmung des Hausrechts, zum Schutz des Eigentums oder Besitzes oder zur Kontrolle von

⁶⁶ siehe Anlage 2.2: Beschluss „Videoüberwachung in und an Taxis“ vom 26./27. Februar 2013

Zugangsberechtigungen erforderlich ist und keine Anhaltspunkte bestehen, dass überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen. Die hierfür notwendigen Abwägungsprozesse wurden unter Beteiligung und in Absprache mit unserer Behörde definiert und detailliert dokumentiert.

Gleiches gilt auch für die technischen und organisatorischen Maßnahmen. So wurden z. B. die durch Videoüberwachung erfassten Bereiche eng begrenzt, die maximale Speicherdauer der Videoaufnahmen auf das erforderliche Maß beschränkt und Regelungen zum Schutz der verwendeten IT-Infrastruktur sowie zum Zugriff auf gespeicherte Aufnahmen und zur Protokollierung der Zugriffe getroffen. Das im Ergebnis vorliegende Konzept berücksichtigt sowohl die schutzwürdigen Interessen der Besucher und Passanten als auch die berechtigten Sicherheitsinteressen des Landtages. Aus unserer Sicht ist damit ein datenschutzgerechter Betrieb der Anlage möglich.

Das übergreifende Sicherheitskonzept für den Neubau des Landtagsgebäudes in der Potsdamer Stadtmitte enthält auch Maßnahmen zur Videoüberwachung öffentlich zugänglicher Bereiche. Durch eine datenschutzgerechte Gestaltung dieser Überwachung werden sowohl die schutzwürdigen Interessen der Besucher und Passanten als auch die berechtigten Sicherheitsinteressen des Landtages berücksichtigt.

16.2 Übertragung einer Videoüberwachung an alle Mitarbeiter

Eine Gemeindeverwaltung informierte uns, dass von einem Firmengelände der angrenzende Gehweg und die dahinter liegende Straße videoüberwacht würden. Fußgänger und Autofahrer seien davon betroffen. Im weiteren Verfahren offenbarten sich überraschende Einzelheiten.

Wir forderten zunächst das Unternehmen zur schriftlichen Stellungnahme auf. Es bedurfte mehrerer Mahnungen und der Ankündigung eines Ordnungswidrigkeitenverfahrens wegen fehlender Auskunftserteilung, bis die Antwort des Geschäftsführers einging. Dieser teilte mit, dass auf dem relativ kleinen Gelände von ca. 1500 qm insgesamt 12 Kameras angebracht sind, die nicht nur Straße und Gehweg, sondern auch Verkaufsraum und Produktionsstätten überwachen. Als Zweck nannte er u. a. die Verbrechensbekämpfung sowie die Zeitersparnis beim Auffinden seiner Mitarbeiter auf dem Gelände. Außerdem hätten alle Beschäftigten Zugriff auf die übertragenen Aufnahmen. Diese Stellungnahme nahmen wir zum Anlass, eine Vor-Ort-Kontrolle durchzuführen.

Die auf den Gehweg und die Straße gerichtete Außenkamera war zum Zeitpunkt unserer Kontrolle bereits deinstalliert worden. Im Gespräch mit dem

Geschäftsführer bestätigte dieser, dass jeder Mitarbeiter von seinem Arbeitsplatz aus Einsicht in die Live-Bilder der im Verkaufsraum und in den Produktionsstätten angebrachten Kameras hatte. Alle Beschäftigten seien vor der Inbetriebnahme der Videoüberwachung informiert worden und tolerierten diese Maßnahme. Der Geschäftsführer teilte uns auf Nachfrage mit, dass er die Aufnahmen von zu Hause und auch von seinem Mobiltelefon ansehen könnte. Die hierfür notwendige Übertragung der Bilddaten über das Internet erfolgte unverschlüsselt. Außerdem wurde die Anlage durch ein externes Unternehmen – jedoch ohne Beachtung der Vorgaben des § 11 Bundesdatenschutzgesetz (BDSG) – gewartet.

Die angestrebte Zeitersparnis beim Auffinden der Mitarbeiter auf dem Gelände rechtfertigt keine Videoüberwachung der Belegschaft. Deshalb waren die Kameras in den Produktionsstätten abzubauen. Zum Schutz bzw. zur Aufklärung von Einbrüchen ist die Videoüberwachung des Verkaufsraums und des Eingangsbereichs zulässig. Wir empfahlen, diese auf die Zeiten nach Geschäftsschluss zu beschränken und forderten die Begrenzung der Speicherfrist der Aufnahmen auf 48 Stunden. Des Weiteren baten wir darum, uns die umgesetzten technischen und organisatorischen Maßnahmen zu benennen und zu erläutern sowie einen Vertrag zur Wartung der Anlage zu erarbeiten, der den Vorgaben von § 11 BDSG entspricht.

Der Geschäftsführer folgte unseren Empfehlungen und Forderungen wiederum erst nach mehrmaliger Aufforderung. Die Videoanlage wurde als Insellösung konfiguriert, sodass keine Netzwerk- oder Fernzugriffe mehr möglich sind. Das Rollenkonzept wurde dahingehend geändert, dass nur ein reduzierter Personenkreis passwortgeschützten Zugriff auf die Anlage und das Bildmaterial hat. Relevante Ereignisse wie Zugriffe auf Aufzeichnungen und Änderungen der Konfiguration werden protokolliert. Auch wurde uns bestätigt, dass ein Wartungsvertrag gemäß § 11 BDSG mit dem beauftragten Unternehmen vorliegt.

Die Videoüberwachung eines Firmengeländes mit dem Ziel, Straftaten aufzudecken oder zu verhindern, kann unter bestimmten Voraussetzungen zulässig sein. Wir empfehlen, sie auf die Zeiten nach Geschäftsschluss zu beschränken. Produktionsstätten mit Videotechnik zu überwachen, um Mitarbeiter schneller aufzufinden, ist in jedem Fall unzulässig.

17 Wirtschaft

17.1 Kein Paket ohne Personalausweisnummer

Wird ein beim Empfänger nicht zustellbares Paket in einem Paketshop zur Abholung hinterlegt, erfolgt die Herausgabe nur gegen Vorlage des Personalausweises. Ein Petent beschwerte sich, dass die Nummer seines Ausweises sogar notiert wurde.

Für die Tätigkeit von Postzustelldiensten gilt u. a. die Postdienste-Datenschutzverordnung. Diese regelt in § 8 den Umgang mit Ausweisdaten, wonach die Art des Ausweises, die ausstellende Behörde sowie die Nummer des Ausweises und das Ausstellungsdatum zum späteren Beweis der ordnungsgemäßen Ausführung des Postdienstes gespeichert werden können, wenn ein besonderes Beweissicherungsinteresse besteht.

Ein solches Interesse wird insbesondere im Falle der Abholung einer Postsendung von einem sog. Zustellpunkt angenommen. Diese kommt immer dann in Betracht, wenn der Adressat eines Pakets zum Zeitpunkt der Lieferung nicht angetroffen wird. Dann erfolgt eine entsprechende Benachrichtigung verbunden mit dem Hinweis, binnen welcher Frist und an welchem Ort die Sendung zur Abholung bereit liegt.

Da sich im Falle der Abholung eine Identifikation des Empfängers nicht schon durch die räumlichen Umstände (Öffnen der Wohnungstür) erschließt, bestehen höhere Anforderungen an die Beweisbarkeit einer ordnungsgemäßen Abgabe (Zustellung) einer Paketsendung. Nähme man an, eine Person mit einem gefälschten Personalausweis würde ein Paket abholen, so könnte anhand der falschen Personalausweisnummer zumindest nachgewiesen werden, dass der richtige Adressat das Paket nicht erhalten hat, seine Haftung (etwa die Zahlung einer Warensendung) würde dann nicht eintreten.

Um diese Beweissicherung zu gewährleisten, genügt die Vorlage des Personalausweises nicht. Vielmehr darf für einen solchen Zweck die Ausweisnummer notiert werden. Die Anfertigung einer Kopie des Ausweises ist dagegen nicht erforderlich und aus diesem Grunde unzulässig.

Bei der Abholung eines Pakets an einem sog. Zustellpunkt, reicht es nicht aus, sich lediglich durch die Vorlage eines Personalausweises zu legitimieren. Vielmehr müssen die Betroffenen hinnehmen, dass die Ausweisnummer vor Ort aufgenommen und gespeichert wird. Die Anfertigung einer Kopie des Ausweises dagegen ist unzulässig.

17.2 Werbung durch ein Autohaus trotz Widerspruch

Gegenüber einem Autohaus hatte ein Petent der Verwendung seiner Anschrift für Werbezwecke widersprochen. Zwar bestätigte ihm das Unternehmen, von künftigen Werbeschreiben abzusehen. Dennoch erhielt er drei Jahre später erneut Angebote zum Kauf von Fahrzeugen.

Das Unternehmen gab der Landesbeauftragten gegenüber an, den Widerspruch des Petenten erhalten und in seiner Datenbank eine Buchungs-, Kontakt- und Auftragssperre eingetragen zu haben. Da das Autohaus jedoch Fabrikate unterschiedlicher Hersteller vertreibt und die Kundendaten für diese jeweils von seinem hauseigenen System getrennt verwaltet, hätte die Sperre in allen Datenbanken vorgenommen werden müssen. Dies war jedoch nicht der Fall, weil ein Herstellersystem zum Zeitpunkt des Widerspruchs nicht verfügbar gewesen ist. Das Versäumnis, die Sperre der Adressdaten auch dort zu berücksichtigen bzw. nachzutragen, führte schließlich zu der unerwünschten Zusendung von Werbung an den Petenten.

Der Geschäftsführer des Autohauses sicherte zu, den Widerspruch des Petenten auch im Hinblick auf diese Datenbank zu berücksichtigen. Anlässlich dieser Beschwerde überprüfte das Unternehmen die Prozesse der Datenverarbeitung, ohne weitere Versäumnisse festzustellen. Es erklärte, künftig in jedem Einzelfall zu prüfen, dass Widersprüche gegen die Verwendung von Adressdaten zu Werbezwecken in allen Datenbanken eingetragen werden.

Führt ein Unternehmen mehrere Datenbanken, in denen Kundendaten verarbeitet werden, hat es eine gewünschte Sperre von Adressdaten zu Werbezwecken in jedem einzelnen System zu berücksichtigen.

17.3 Brandenburg Business Guide

Das Ministerium für Wirtschaft und Europaangelegenheiten fragte an, ob die Landesbeauftragte die Projektverantwortlichen bei der Klärung datenschutzrechtlicher Fragen im Zusammenhang mit dem Aufbau des Internetportals zum Standortmarketing unterstützen könne.

Der Brandenburg Business Guide ist ein vom Wirtschaftsministerium initiiertes multimediales und geodatenbasiertes Webportal.⁶⁷ Seine wesentlichen Ziele bestehen darin, Brandenburg als attraktiven Wirtschaftsstandort zu präsentieren, für die Ansiedlung neuer Unternehmen im Land zu werben und den Bestand vorhandener Unternehmen zu entwickeln. Im Portal werden

⁶⁷ siehe <http://www.brandenburg-business-guide.de>

Informationen zu sogenannten harten und weichen Standortfaktoren verknüpft und ortsbezogen visualisiert. Bei den harten Faktoren handelt es sich z. B. um Verkehrsinfrastruktur, Finanzierungsanreize, Steuerhebesätze und Gewerbeflächen. Zu den weichen Faktoren gehören z. B. Bildungseinrichtungen, Freizeitmöglichkeiten und Kulturangebote.

Positiv hervorzuheben ist, dass das Ministerium unsere Behörde frühzeitig in die Planung und den Aufbau des Portals mit einbezogen hat. In mehreren konstruktiven Gesprächen konnten Fragen zu datenschutzrechtlichen Themen umfassend besprochen und geklärt werden. Dabei ging es u. a. darum, ob die Namen und ggf. weitere Informationen zu Inhabern von Einzelunternehmen, die bereits im öffentlichen Handelsregister eingetragen sind, im Portal dargestellt werden dürfen. Der Nutzung dieser Angaben steht aus datenschutzrechtlicher Sicht nichts entgegen. Auch bei Fragen der Reichweitenmessung⁶⁸ des Angebotes sowie der Erfüllung formaler Anforderungen (Sicherheitskonzept, Freigabeerklärung, Verfahrensverzeichnis) konnte eine datenschutzgerechte Gestaltung erreicht werden.

Die Freischaltung des Portals erfolgte kurz vor dem Ende des Berichtszeitraums. Betreiber ist die ZukunftsAgentur Brandenburg GmbH. Eine Vereinbarung zur Auftragsdatenverarbeitung liegt vor.

Der Brandenburg Business Guide trägt in der gegenwärtigen Gestaltung datenschutzrechtlichen Anforderungen Rechnung.

18 Tätigkeit der Sanktionsstelle

Im Berichtszeitraum haben wir 19 Ordnungswidrigkeitenverfahren geführt, die in zwei Fällen mit einer Verwarnung, im Übrigen mit der Festsetzung eines Bußgeldes endeten. Die Summe der verhängten Bußgelder betrug 10.300 Euro. Darüber hinaus hat die Landesbeauftragte von ihrem Recht Gebrauch gemacht, Strafantrag zu stellen.

18.1 Unbefugte Datenabrufe aus polizeilichen Datenbanken

Einen Schwerpunkt bildeten Fälle, in denen Polizeibedienstete ohne dienstlichen Anlass, personenbezogene Daten, die nicht offenkundig waren und dem Datengeheimnis unterlagen, aus polizeilichen Datenbanken abriefen und zum Teil an Dritte bekanntgaben.

⁶⁸ siehe B 14.2

Personenbezogene Daten, die in polizeilichen Datenbanken gespeichert sind, dienen ausschließlich der Polizei zu deren Aufgabenerfüllung. Für jeden Datenabruf muss eine konkrete dienstliche Notwendigkeit gegeben sein. Private Gründe, etwa ob die neue Freundin des Sohnes vorbestraft ist oder ob ein Ermittlungsverfahren gegen die Tochter eingeleitet wurde, rechtfertigen einen Abruf nicht.

In den durchgeführten Bußgeldverfahren wurde von den Betroffenen mehrfach die Auffassung vertreten, dass ein Datenabruf tatbestandsmäßig nur vorliegen kann, wenn bezüglich der abgefragten Person auch ein Datensatz im polizeilichen Auskunftssystem existiert. Dem ist jedoch nicht so. Vielmehr ist auch bei einem „Nulltreffer“, also wenn keine Einträge vorhanden sind, der Tatbestand des Abrufens erfüllt. Darauf, ob und welche Datensätze dem Abrufenden angezeigt wurden, kommt es nicht an. Vielmehr lassen sich auch aus dem „Nulltreffer“ Rückschlüsse auf die gesuchte Person ziehen; beispielsweise, dass gegen sie kein Ermittlungsverfahren eingeleitet wurde.

Aber nicht nur die Abfrage anderer Personen stellt einen Verstoß gegen datenschutzrechtliche Vorschriften dar. Dies gilt auch für Zugriffe eines Polizeibediensteten auf die eigenen im System der Polizei gespeicherten Daten. Wie jeder andere Bürger muss auch er einen Antrag auf Auskunft über die zu seiner Person gespeicherten Daten gegenüber der zuständigen Polizeidienststelle stellen. Dem Begehren kann nur unter den engen gesetzlichen Voraussetzungen des § 71 Brandenburgisches Polizeigesetz entsprochen werden, wenn etwa eine Gefährdung der Aufgabenerfüllung der Polizei nicht zu besorgen ist. Hierüber kann der Polizeibedienstete nicht selbst entscheiden. Insoweit wird deutlich, dass eine sog. Selbstabfrage unzulässig ist und den Tatbestand einer Ordnungswidrigkeit erfüllt. Dies gilt gleichfalls für Fälle, in denen die Person, die im System abgefragt wird, in die Abfrage eingewilligt hat. Meist ist es der gute Freund oder Bekannte, der den Polizeibediensteten drängt, mal schnell nachzuschauen, ob über ihn etwas gespeichert wurde. In diesen Fällen sollte der Auskunftbegehrende stets an die zuständige Polizeidienststelle verwiesen werden, denn ohne dienstlichen Anlass, etwa aus reiner Freundschaft, verletzt der Polizeibedienstete mit dem Abruf datenschutzrechtliche Vorschriften.

18.2 Entsorgung personenbezogener Daten im Wald und als Altpapier

Eine Personalvermittlungsfirma, die ihr Büro auflöste, entsorgte die Bewerbungsunterlagen ihrer Kunden in einem Wald. Zwar konnte nicht geklärt werden, wer die Bewerbungsanschreiben mit Lebenslauf, Zeugnissen und Fotos dort ablagerte. In jedem Fall trifft den Inhaber des Unternehmens die Pflicht, diese Dokumente, die eine Vielzahl personenbezogener Daten enthal-

ten, an die Bewerber zurückzusenden oder datenschutzkonform zu vernichten. Dies war hier nicht geschehen.

In einem weiteren Fall handelte die Inhaberin einer Apotheke ordnungswidrig, weil Abholscheine, die Namen, Anschriften und Medikamente ihrer Kunden enthielten, in eine öffentlich zugängliche Papiertonne geworfen wurden. Anwohner fanden diese Unterlagen und erhielten somit als unbefugte Dritte Kenntnis von Gesundheitsdaten anderer Bürger.

18.3 Heimliche Videoüberwachung

Vertrauen ist gut, Kontrolle ist besser. Nach diesem Motto verfuhr die Inhaberin eines Friseurgeschäfts und überwachte heimlich ihre Angestellten mittels mehrerer Videokameras, die in kleinen Weckern versteckt waren. Die im Aufenthaltsraum und im Salon aufgestellten Kameras erfassten die ahnungslosen Angestellten. Auch Kunden gerieten in das Blickfeld.

Die Videoüberwachung öffentlich zugänglicher Räume ist Unternehmen nur unter den engen Voraussetzungen des § 6b Bundesdatenschutzgesetz (BDSG) gestattet. Insbesondere muss sie für den beabsichtigten Zweck erforderlich sein, was nach unseren Feststellungen zu verneinen war. Auch die Überwachung des Aufenthaltsraumes war unzulässig, denn konkrete Anhaltspunkte einer von Mitarbeitern begangenen Straftat, wie sie § 32 BDSG verlangt, lagen nicht vor.

18.4 Pflicht zur Auskunftserteilung an die Aufsichtsbehörde

Grundsätzlich müssen Daten verarbeitende Stellen der Landesbeauftragten gemäß § 38 Abs. 3 Satz 1 BDSG die für die Erfüllung ihrer gesetzlichen Aufgaben erforderlichen Auskünfte erteilen. Dies gilt auch bei schriftlichen Anfragen. Nur wenn sich der Auskunftspflichtige durch die Beantwortung der Fragen der Gefahr strafrechtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde, ist er von dieser Pflicht befreit. Er muss sich jedoch ausdrücklich auf dieses Auskunftsverweigerungsrecht berufen. Hierauf und auf die gesetzliche Auskunftspflicht weisen wir die verantwortlichen Stellen bereits bei der ersten Kontaktaufnahme hin. Auch in Fällen, in denen die Anwendbarkeit des Bundesdatenschutzgesetzes von der zu überprüfenden Stelle bestritten wird, kann diese Behauptung von der Aufsichtsbehörde erst dann auf ihren Wahrheitsgehalt überprüft werden, wenn Auskunft erteilt wurde. Dennoch werden Anfragen unserer Dienststelle trotz wiederholter Nachfragen gar nicht oder nur unvollständig beantwortet.

Die Nichterteilung sowie die nicht richtige, nicht vollständige und nicht rechtzeitige Erteilung der Auskunft stellen eine Ordnungswidrigkeit dar. Im Berichtszeitraum führten wir mehrere Verfahren wegen eines derartigen Formalverstößes durch.

18.5 Pflicht zur Auskunftserteilung an den Betroffenen

Nach § 34 BDSG hat der Betroffene ein Recht darauf, Auskunft darüber zu erhalten, welche personenbezogenen Daten über ihn gespeichert sind. Zum Umfang der Auskunft gehört auch, zu welchem Zweck die Daten erhoben wurden, woher diese stammen und an welche Stellen diese übermittelt wurden. Daten verarbeitende Stellen, die Wahrscheinlichkeitswerte (Scorewerte) nutzen, wie z. B. Banken oder Auskunftsteien, müssen zudem über die verwendeten Scorewerte auf Antrag informieren.

In einem uns zur Kenntnis gelangten Fall gab ein Unternehmen auf die Frage eines Bürgers, welche Daten es über ihn gespeichert habe, erst nach mehreren Monaten Auskunft. Zwar bestimmt § 34 BDSG keine konkrete Frist, jedoch ergibt sich aus dem Schutzzweck der Vorschrift, dass die Auskunft unverzüglich zu erfolgen hat. Eine längere Frist ist nur unter besonderen Umständen gerechtfertigt. Diese lagen in dem von uns zu prüfenden Fall jedoch nicht vor.

Zudem erfordert die umfassende Auskunftspflicht auch, die Antragsteller darüber zu informieren, wenn über sie keine Daten gespeichert sind. Auch die Negativauskunft ist eine gebotene Form der Auskunftserteilung. Die Auskunft muss nachvollziehbar und in allgemein verständlicher Form erteilt werden. Eine eindeutige, unmissverständliche Mitteilung an den Anfragenden, beispielsweise in der Form: „Wir haben keine Daten zu Ihrer Person vorliegen.“ wäre erforderlich, aber auch ausreichend gewesen.

18.6 Abgaben an die Staatsanwaltschaft

Stellt die Landesdatenschutzbeauftragte Verstöße gegen datenschutzrechtliche Normen fest, die den Verdacht einer Straftat nahelegen, so hat sie das Recht, einen Strafantrag zu stellen. Erst dieser ermöglicht eine Verfolgung der Tat.

In einem Fall wurde Strafantrag gestellt, weil ein IT-Systembetreuer eines Sozialamtes eine Vielzahl von Daten von Sozialleistungsempfängern an seine private E-Mail-Adresse gesendet hatte, um diese für eigene Zwecke zu nutzen und seinen Arbeitgeber zu schädigen. Der Betroffene wurde zu einer Geldstrafe verurteilt.

In einem anderen Fall informierte uns ein Petent über die Verletzung der beruflichen Schweigepflicht. Eine Apothekerin gab unbefugt Gesundheitsdaten weiter, indem Rezepte zu Testkäufen bei einer konkurrierenden Apotheke verwendet wurden. Nach Abgabe dieses Vorganges an die Staatsanwaltschaft wurde Anklage erhoben. Über den Ausgang des Strafverfahrens liegen noch keine Informationen vor.

In Fällen, in denen gravierende Verstöße gegen datenschutzrechtliche Normen festgestellt werden, sind diese mit den vom Gesetzgeber vorgesehenen Mitteln zu verfolgen und gegebenenfalls zu ahnden.

I:\ap\p1\intern\Parlamentsmaterialien\Drucksachen\8866.docx

Teil C

Akteneinsicht und Informationszugang

1 Open Data und Informationsfreiheit

Die bereits im letzten Tätigkeitsbericht dargestellte Entwicklung⁶⁹ hin zu einer Ergänzung der Informationsfreiheit durch Veröffentlichungspflichten, Informationsregister und Open-Data-Projekten hat sich im Berichtszeitraum fortgesetzt. Das betrifft sowohl die Realisierung entsprechender Vorhaben als auch die Gesetzgebung.

1.1 Europa

Bereits zum Ende des Jahres 2011 stellte die Europäische Kommission eine Strategie für offene Daten in Europa vor. Im Ergebnis eines Gesetzgebungsverfahrens wurde die bestehende Weiterverwendungsrichtlinie fortentwickelt. Im Juli 2013 traten die entsprechenden Änderungen in Kraft.⁷⁰ Ziel der geänderten Richtlinie ist es, die Erstellung unionsweiter Produkte und Dienstleistungen der Informationswirtschaft anhand von Dokumenten des öffentlichen Sektors zu erleichtern und eine effektive grenzüberschreitende Nutzung derselben zu gleichen und fairen Bedingungen sowohl durch Privatunternehmen als auch durch die Bürger sicherzustellen. Durch die Änderungsrichtlinie wird ein grundsätzliches Recht auf Weiterverwendung jener Inhalte etabliert, die unter den Bedingungen der nationalen Informationsfreiheitsgesetze zugänglich sind. Den Mitgliedstaaten obliegt somit die Aufgabe, diese Informationen zur Weiterverwendung freizugeben und praktische Vorkehrungen zu treffen, um die Suche nach den zur Weiterverwendung verfügbaren Dokumenten zu erleichtern. Dazu gehören – möglichst online und in maschinenlesbarem Format – zum Beispiel Bestandslisten der wichtigsten Dokumente mit zugehörigen Metadaten sowie damit verknüpfte Internet-Portale. Die Befugnis zur Erhebung von Gebühren beschränkt sich nunmehr im Wesentlichen auf die individuellen Kosten für Vervielfältigung, Bereitstellung und Verbreitung der jeweils zur Weiterverwendung beantragten Daten. Kultureinrichtungen wie Bibliotheken, Museen und Archive fallen erstmals – wenngleich mit umfassenden Einschränkungen – unter den Anwendungsbereich der Richtlinie. Bis zum 18. Juli 2015 sind die nationalen Vorschriften – in

⁶⁹ siehe Tätigkeitsbericht 2010/2011, B 1.4

⁷⁰ Richtlinie 2013/37/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 zur Änderung der Richtlinie 2003/98/EG über die Weiterverwendung von Informationen des öffentlichen Sektors (ABl. Nr. L 175 S. 1)

Deutschland also das Informationsweiterverwendungsgesetz – an die geänderte Richtlinie anzupassen; drei Jahre später ist eine Überprüfung der Anwendung der Richtlinie durch die Kommission vorgesehen.

Zum Ende des Jahres 2012 errichtete die Europäische Kommission eine Betaversion des Offenen Datenportals der Europäischen Union⁷¹. Es bietet zunächst einen zentralen Zugang zu Dokumenten der Institutionen und Einrichtungen der Union und dient darüber hinaus als erster Schritt hin zu einer unionsweiten Plattform, die den Zugang zu Datenportalen sämtlicher Mitgliedstaaten ermöglichen soll.

Durch eine öffentliche Konsultation erkundete die Europäische Kommission zum Ende des Jahres 2013 Möglichkeiten, Informationen des öffentlichen Sektors für die Weiterverwendung zu erschließen.⁷² Ihr Ziel ist es, Leitlinien auszuarbeiten und praktischen Rat zu erhalten, um die Weiterverwendung von Wetterdaten, Verkehrsdaten, Daten aus öffentlich finanzierter Forschung, Statistiken, digitalisierten Büchern und anderen Arten von Informationen des öffentlichen Sektors zu fördern.

1.2 Bund und Länder

Auch in der Bundesrepublik Deutschland sind im Berichtszeitraum verschiedene Aktivitäten zu Open Data zu verzeichnen. Vor dem Hintergrund des Regierungsprogramms „Vernetzte und transparente Verwaltung“ und der Strategie des IT-Planungsrats (eines Steuerungsgremiums für die Anwendung der Informations- und Kommunikationstechnik in der öffentlichen Verwaltung) wurde im August 2012 eine im Auftrag des Bundesministeriums des Innern erstellte Studie zu Open Government in Deutschland veröffentlicht.⁷³ Sie legt die Grundlagen sowie die rechtlichen, organisatorischen und technischen Aspekte von Open Government Data dar. Die Studie gibt insbesondere Empfehlungen für die technische Ausgestaltung eines ebenenübergreifenden Online-Portals, für Geldleistungs- und Lizenzmodelle sowie mögliche Betreibermodelle. Ein solches Portal wurde mit GovData,⁷⁴ dem „Datenportal für Deutschland“, im Februar 2013 als Betaversion freigeschaltet. Das Projekt soll ab dem Jahr 2015 als Bund-Länder-Plattform in den Regelbetrieb gehen und einen einheitlichen, zentralen Zugang zu Verwaltungsdaten aus Bund,

⁷¹ siehe <http://open-data.europa.eu/de/>

⁷² Konsultation: Wie können mehr öffentliche Daten frei verfügbar gemacht werden? (European Commission – IP/13/798, 30/08/2013)

⁷³ Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS, Partnerschaften Deutschland, Lorenz-von-Stein-Institut für Verwaltungswissenschaften der Christian-Albrecht-Universität zu Kiel: Open Government Data Deutschland. Eine Studie zu Open Government in Deutschland im Auftrag des Bundesministeriums des Innern vom Juli 2012.

⁷⁴ siehe <https://www.govdata.de>

Ländern und Kommunen bieten. Parallel hierzu trat im August 2013 das E-Government-Gesetz⁷⁵ in Kraft, das mit seiner Regelung zur Bereitstellung von maschinenlesbaren Datenbeständen durch die Verwaltung die technische Entwicklung von Open Data flankiert.

Der erfolgreiche Betrieb der beschriebenen Bund-Länder-Plattform hängt nicht zuletzt vom Vorhandensein entsprechender Länderangebote ab, die es in diesem Rahmen zu vernetzen gilt. Den kräftigsten Impuls sowohl im Hinblick auf Gesetzgebung als auch auf Projektrealisierung setzte das im Oktober 2012 in Kraft getretene Hamburgische Transparenzgesetz. Mit einer zweijährigen Umsetzungsfrist sieht es weitgehende Veröffentlichungspflichten vor. Das hierfür einzurichtende Informationsregister wird nicht nur in öffentlichen Sitzungen gefasste Beschlüsse, Haushalts- und Aktenpläne, Globalrichtlinien und Verwaltungsvorschriften, sondern auch Geodaten, das Baukataster, Bauleit- und Landschaftspläne, die wesentlichen Regelungen erteilter Baugenehmigungen, Informationen über Subventions- und Zuwendungsvergaben sowie die Verträge der Daseinsvorsorge beinhalten. Dieses Beispiel diente als Vorbild für zahlreiche Entwürfe von Transparenzgesetzen, die ähnliche Open-Data-Regelungen vorsahen.⁷⁶ Die Freie Hansestadt Bremen verfügte bereits über ein gesetzlich normiertes Informationsregister, in Thüringen ist ein solches zwar im Informationsfreiheitsgesetz vorgesehen, befindet sich aber noch im Aufbau. Einige Länder betreiben ohne gesetzliche Verpflichtung Portale im Internet (beispielsweise Baden-Württemberg, Bayern, Berlin, Rheinland-Pfalz) oder entwickeln entsprechende Konzepte und Strategien (beispielsweise Niedersachsen, Nordrhein-Westfalen, Sachsen-Anhalt). Auch verschiedene deutsche Städte bieten inzwischen Open-Data-Plattformen im Internet an.

Darüber hinaus existieren bereits zahlreiche Plattformen, die von nicht öffentlichen Stellen betrieben werden und Daten des öffentlichen Sektors in aufbereiteter Form anbieten. An ihnen zeigt sich besonders der partizipative Ansatz von Open Data bzw. Open Government, geht es doch darum, die Informationen als Rohstoff der Demokratie nutzbar zu machen.

1.3 Brandenburg

Ein konkreter Beitrag des Landes Brandenburg stand zum Ende des Berichtszeitraums noch aus. Der Gesetzgeber konnte sich nicht, wie von der Landesbeauftragten empfohlen, dazu entschließen, die im September 2013 erfolgte Novellierung des Akteneinsichts- und Informationszugangsgesetzes⁷⁷

⁷⁵ Gesetz zur Förderung der elektronischen Verwaltung vom 25. Juli 2013 (BGBl. I S. 2749)

⁷⁶ siehe C 2

⁷⁷ siehe A 3

zu nutzen, um Open Data gesetzlich zu verankern. Der Landtag verabschiedete lediglich einen Beschluss, mit dem die Landesregierung gebeten wird, die Beteiligung des Landes Brandenburg an der Bund-Länder-Plattform GovData zu forcieren, Vorbereitungen für die Veröffentlichung von Daten des Landes im bestehenden Landesportal zu treffen und den Aspekt Open Data bei der Weiterentwicklung der E-Government-Strategie des Landes zu berücksichtigen. Bis zum 30. April 2014 soll dem Innenausschuss des Landtags ein Bericht über die getroffenen Maßnahmen vorgelegt werden. Eine Open-Data-Strategie der Landesregierung lag zum Ende des Berichtszeitraums noch immer nicht vor; in der Beantwortung parlamentarischer Anfragen zeigte sich die Landesregierung bislang eher abwartend.⁷⁸

Das Fehlen einer brandenburgischen Open-Data-Strategie ist umso erstaunlicher, als durchaus bereits entsprechende Ansätze vorhanden sind, die allerdings nicht so heißen. So sind beispielsweise die Behörden durch die europäische INSPIRE-Richtlinie bzw. das Brandenburgische Geodateninfrastrukturgesetz verpflichtet, raumbezogene Daten in großem Umfang öffentlich bereitzustellen. Der Aufbau der hierfür erforderlichen Geodateninfrastruktur hat auch in Brandenburg längst begonnen. Auch für die Bereitstellung von Umweltinformationen, die durch das ebenfalls auf einer europäischen Richtlinie basierende Brandenburgische Umweltinformationsgesetz gesetzlich vorgeschrieben ist, wurde eine Infrastruktur geschaffen. Zudem betreiben die Landesregierung mit dem Brandenburgischen Vorschriftenystem (BRAVORS) und der Landtag Brandenburg mit dem Parlamentsdokumentationssystem gut funktionierende Plattformen. Ähnliches gilt für zahlreiche Ratsinformationssysteme brandenburgischer Kommunen. Diese und weitere Instrumente und Inhalte sollten bei der Erstellung einer Open-Data-Strategie unbedingt berücksichtigt werden, um Doppelarbeit zu vermeiden.

1.4 Positionen der Informationsfreiheitsbeauftragten

Die Landesbeauftragte sieht sich zudem durch einen internationalen Erfahrungsaustausch in ihrer Forderung bestätigt, Open Data auch in Brandenburg als Chance zu begreifen und gesetzlich zu regeln. Während eines von ihr im Mai 2013 veranstalteten Internationalen Symposiums⁷⁹ zu diesem Thema boten Experten aus verschiedenen europäischen Ländern Einblicke in ausgewählte Open-Data-Projekte. So hat die Bereitstellung von Daten aus dem Beschaffungswesen, zu Staatsausgaben und aus dem Bereich der Justiz die Slowakei in punkto Transparenz grundlegend verändert. Die Pflicht zur Veröf-

⁷⁸ Siehe hierzu auch folgende Antworten der Landesregierung auf Kleine Anfragen: Landtags-Drucksachen 5/5721 (Anwendung des Brandenburgischen Akteneinsichts- und Informationszugangsgesetzes), 5/6820 (Open Data in Brandenburg), 5/7075 (Brandenburger Beteiligung an GovData?), 5/7165 (Open Data / Offene Daten in Brandenburg)

⁷⁹ siehe auch D 6.1

fentlichung von Verträgen zwischen dem Staat und privaten Unternehmen gehört dort längst zum Alltag. Dass Open Data keineswegs eine Einbahnstraße ist, zeigte ein Vortrag aus Kroatien. Im Rahmen öffentlicher Konsultationen werden in dem jüngsten Mitgliedstaat der Europäischen Union Informationen als Grundlage für den Dialog mit der Zivilgesellschaft betrachtet. Ihre proaktive Veröffentlichung dient der Stärkung der Mitgestaltungsmöglichkeiten für Bürger auf den verschiedensten Politikfeldern. Aber auch Regierung und Verwaltung selbst, so zeigte ein Beitrag aus Österreich, können sich die positiven Effekte von Open Data unmittelbar zunutze machen. Durch Aufbereitung und Verknüpfung von Daten gelangen sie schließlich an steuerungsrelevante Informationen, die ihnen sonst verschlossen blieben.

In ihrem Positionspapier „Informationsfreiheit und Open Data“ vom Juni 2013 spricht sich die Konferenz der Informationsfreiheitsbeauftragten in Deutschland für die Stärkung von Open Data aus und formuliert wesentliche Anforderungen an eine moderne Transparenzgesetzgebung.⁸⁰ Ein wichtiges Anliegen ist ihr, dass Open Data in den Informationsfreiheits- und Transparenzgesetzen geregelt wird. Diese müssen um geeignete Instrumente zur Veröffentlichung von Informationen ergänzt werden, ohne allerdings den Anspruch auf Informationszugang im herkömmlichen Antragsverfahren aufzugeben. Mit dem Positionspapier unterstützen die Informationsfreiheitsbeauftragten die begonnenen Open-Data-Projekte und empfehlen eine enge Verzahnung von Informationsfreiheit und Open Data. Die Chance, die Novellierung des Akteneinsichts- und Informationszugangsgesetzes zu nutzen, um eine solche Verzahnung in Brandenburg vorzunehmen, ist zwar ungenutzt verstrichen. Der Gesetzgeber hat aber jederzeit die Möglichkeit, die Initiative wieder aufzunehmen.

2 Entwicklung der Informationsfreiheit in Bund und Ländern

Die Entstehung und das In-Kraft-Treten des Hamburgischen Transparenzgesetzes⁸¹ vom 19. Juni 2012 haben die Fortentwicklung des Informationsfreiheitsrechts sowohl auf Bundesebene als auch in den Ländern während des gesamten Berichtszeitraums wesentlich geprägt. Sein Hauptanliegen ist die Schaffung eines internetbasierten Registers, über welches ein umfangreicher Informationsbestand der öffentlichen Stellen zugänglich sein wird. Das Ge-

⁸⁰ siehe Anlage 3.2.1: Entschließung „Open Data stärkt die Informationsfreiheit – sie ist eine Investition in die Zukunft!“ vom 27. Juni 2013

⁸¹ Hamburgisches Transparenzgesetz vom 19. Juni 2012 (Hamburgisches Gesetz- und Verordnungsblatt, Teil I, Nr. 29 vom 6. Juli 2012, Seite 271)

gesetz listet bestimmte Arten von Dokumenten auf, die dort aktiv zu veröffentlichen sind – und geht damit über die im Bremischen Informationsfreiheitsgesetz vorgesehene „Soll-Vorschrift“ zur Veröffentlichung in einem elektronischen Informationsregister weit hinaus. Außerdem enthält das Hamburgische Transparenzgesetz einen individuellen Anspruch auf Veröffentlichung bestimmter Informationen. Zur Schaffung der technischen Voraussetzungen hierfür sieht das Gesetz eine Übergangsfrist von zwei Jahren vor. In der Praxis wird das Register als Open-Data-Plattform der Freien und Hansestadt Hamburg dienen.⁸² Gleichzeitig wird der herkömmliche Anspruch auf Informationszugang gestärkt; dies geschieht unter anderem durch eine Reduzierung der Ausnahmeregelungen sowie durch die Ausweitung des Anwendungsbereichs des Gesetzes auf privatrechtlich organisierte Stellen, die öffentliche Aufgaben wahrnehmen.

Zahlreiche Transparenzinitiativen sowie konkrete Gesetzentwürfe in den übrigen Parlamenten orientierten sich an diesen weitgehenden Vorgaben des Hamburgischen Transparenzgesetzes. Der Deutsche Bundestag lehnte den Entwurf für ein Informationsfreiheits- und Transparenzgesetz im Juni 2013 ab. Dieser sah unter anderem vor, die bislang getrennten Informationsansprüche aus dem Informationsfreiheits-, Umweltinformations- sowie Verbraucherinformationsgesetz in einer Rechtsgrundlage zusammenzuführen sowie eine Verpflichtung zur aktiven Veröffentlichung bestimmter Informationen einzuführen. Dem Gesetzentwurf vorausgegangen war die Veröffentlichung einer vom Innenausschuss des Deutschen Bundestages in Auftrag gegebenen Evaluation des Informationsfreiheitsgesetzes vom Mai 2012. Die umfangreiche Studie⁸³ kommt unter anderem zum Ergebnis, dass es noch zahlreiche Möglichkeiten gibt, das Gesetz zu verbessern. Eine Zusammenführung der unterschiedlichen Rechtsgrundlagen für den Informationszugang hält das Gutachten für möglich. Es empfiehlt die Überarbeitung der Ausschlussgründe, die Einführung allgemeiner Abwägungsklauseln, die Erweiterung der Kompetenzen des Bundesbeauftragten für die Informationsfreiheit auch auf andere bundesrechtliche Vorschriften über die Informationsfreiheit sowie die Einrichtung eines behördlichen Informationsfreiheitsbeauftragten. Die Umsetzung dieser und vieler weiterer Empfehlungen der Studie kam in der 17. Legislaturperiode nicht zustande.

Im September 2012 trat das geänderte Verbraucherinformationsgesetz in Kraft, dessen Novellierung bereits im letzten Berichtszeitraum begonnen

⁸² Mehr zum Thema Open Data siehe C 1.

⁸³ Institut für Gesetzesfolgenabschätzung und Evaluation des Deutschen Forschungsinstituts für öffentliche Verwaltung Speyer: Evaluation des Gesetzes zur Regelung des Zugangs zu Informationen des Bundes – Informationsfreiheitsgesetz des Bundes (IFG) im Auftrag des Innenausschusses des Deutschen Bundestages vom 22. Mai 2012. Bundestags-Drucksachen 17(4)522 A bzw. 17(4)522 B.

wurde.⁸⁴ Damit verbunden war die Änderung der Veröffentlichungspflichten des Lebensmittel- und Futtermittelgesetzbuches (§ 40 Abs. 1a), das die Behörden nunmehr zur Veröffentlichung von Rechtsverstößen durch Grenzwertüberschreitungen unter Nennung der verantwortlichen Unternehmen verpflichtet. Die Art und Weise der Veröffentlichung wird nicht näher geregelt. In einigen Bundesländern informierten die Behörden fortan auf eigens hierfür eingerichteten Internetportalen über Verstöße gegen Hygienestandards. Die Verwaltungsgerichte stoppten die Praxis der Internetveröffentlichungen, da das Lebensmittel- und Futtermittelgesetzbuch unter anderem deshalb unverhältnismäßig in die Rechte der betroffenen Unternehmen eingreife, weil die Vorschrift schon bei geringen Verstößen eine Veröffentlichung zulasse und keine Grenzen für die Dauer der Veröffentlichung vorsehe. Bereits im Gesetzgebungsverfahren hatte die Konferenz der Informationsfreiheitsbeauftragten darauf hingewiesen, dass die Vorschrift zu undifferenziert sei. Eine Neuregelung erfolgte während der 17. Legislaturperiode des Deutschen Bundestags nicht mehr.

In fast allen Ländern, die über ein Informationsfreiheitsgesetz verfügen, wurden im Berichtszeitraum Initiativen zur Modernisierung des allgemeinen Informationszugangsanspruchs diskutiert oder entschieden die Parlamente über konkrete Gesetzentwürfe. Die am weitestgehenden Änderungen hat das Land Schleswig-Holstein vorgenommen. Dort führte der Landtag das Informationsfreiheitsgesetz und das Umweltinformationsgesetz zu einem neuen Informationszugangsgesetz zusammen.⁸⁵ Ziel dieses Vorhabens war es unter anderem, die Verfahren zur Akteneinsicht zu vereinfachen und Abgrenzungsprobleme zwischen den zuvor getrennten Rechtsgrundlagen zu vermeiden. Im Freistaat Thüringen trat ein neues Informationsfreiheitsgesetz in Kraft, das – im Gegensatz zu dem seit 2007 geltenden Thüringer Informationsfreiheitsgesetz, welches im Wesentlichen auf die Regelungen des Bundesgesetzes verwies – die Einrichtung eines Landesbeauftragten für die Informationsfreiheit vorsieht. Außerdem enthält das neue Gesetz die Verpflichtung, ein Informationsregister im Internet zu schaffen.⁸⁶ Das Land Rheinland-Pfalz, in dem eine vorangegangene Gesetzesänderung bereits einen Informationsfreiheitsbeauftragten etablierte, soll nach Ankündigung der Landesregierung bald über ein Transparenzgesetz verfügen, welches das Informationsfreiheitsgesetz mit dem Umweltinformationsgesetz zusammenführt und Open-Data-Regelungen enthält. In Sachsen-Anhalt steht das Ergebnis einer gesetzlich vorgeschriebenen Evaluierung des Informationszu-

⁸⁴ siehe Tätigkeitsbericht 2010/2011, B 1.3

⁸⁵ Informationszugangsgesetz für das Land Schleswig-Holstein vom 19. Januar 2012 (Gesetz- und Verordnungsblatt für Schleswig-Holstein, Ausgabe Nr. 2 vom 26. Januar 2012, Seite 89)

⁸⁶ Thüringer Informationsfreiheitsgesetz vom 14. Dezember 2012 (Gesetz- und Verordnungsblatt für den Freistaat Thüringen, Nr. 13 vom 21. Dezember 2012, Seite 464)

gangsgesetzes noch aus. Dort wird unter anderem die Möglichkeit zur Senkung der Kosten für den Informationszugang sowie zur Zusammenführung der verschiedenen Informationszugangsgesetze auf Landesebene geprüft. Das Hamburgische Vorbild eines Transparenzgesetzes fand in unterschiedlicher Weise Eingang in die parlamentarischen Debatten weiterer Länder, beispielsweise in Berlin, Mecklenburg-Vorpommern, Nordrhein-Westfalen oder im Saarland.

Aber auch in jenen Ländern, deren Gesetzgeber bislang keine Notwendigkeit für ein Informationsfreiheitsgesetz sahen, ist Bewegung in die Diskussion gekommen. Nach der bislang folgenlosen Ankündigung der baden-württembergischen Landesregierung, unter Beachtung des Grundsatzes von Open Data ein Informationsfreiheitsgesetz schaffen zu wollen, lehnte der Landtag inzwischen den entsprechenden Gesetzentwurf einer Oppositionsfraktion ab. Ein Entwurf der Landesregierung steht aber weiterhin aus. In Hessen fand vor der Konstituierung des neuen Landtags zwar noch eine Anhörung zu dem Entwurf einer Oppositionsfraktion für ein Hessisches Transparenzgesetz statt; eine Entscheidung erfolgte jedoch nicht mehr. Nachdem der Koalitionsvertrag der Regierungspartner in Niedersachsen eine umfassende Open-Data-Strategie mit einem modernen Informationsfreiheits- und Transparenzgesetz in Aussicht stellte, beriet der Landtag zum Ende des Berichtszeitraums über den Entwurf einer Oppositionsfraktion für ein Niedersächsisches Informationsfreiheitsgesetz. Abgelehnt haben der Sächsische Landtag den Entwurf für ein Verwaltungstransparenzgesetz sowie der Bayerische Landtag den für ein Transparenz- und Informationsfreiheitsgesetz. Der bereits im vorigen Berichtszeitraum festzustellende Trend vor allem bayerischer, aber auch hessischer, niedersächsischer und sächsischer Gemeinden, Städte und Landkreise, eigene Informationsfreiheitsgesetze als Ausgleich für die fehlende landesgesetzliche Regelung zu schaffen, hält unvermindert an.

3 Grundstücksverkauf ohne Wertgutachten – Die Katze im Sack

Um ein städtisches Grundstück zu verkaufen, forderte eine Stadt auf ihrer Website potenzielle Käufer auf, Angebote abzugeben. Sie stellte ein kurzes Exposé zur Verfügung und teilte mit, weitere Informationen könnten bei Bedarf angefordert werden. Ein Kaufinteressent nahm dieses Angebot an und beantragte die Herausgabe des Verkehrswertgutachtens. Die Stadtverwaltung ließ dann jedoch keinerlei Informationsbereitschaft mehr erkennen.

Der Antragsteller formulierte sein Begehren, Zugang zu dem von der Stadt in Auftrag gegebenen Verkehrswertgutachten zu erhalten, zunächst per E-Mail. Die Ablehnung erfolgte ebenfalls per E-Mail und ohne Begründung. Dagegen legte der Kaufinteressent – wiederum per E-Mail – Widerspruch ein. Die Behörde erläuterte, es handle sich um ein laufendes Verfahren, teilte aber gleichzeitig mit, das Gutachten sei gar nicht Bestandteil der Ausschreibungsunterlagen. Die Einsichtnahme durch den Antragsteller würde zudem einen unzulässigen Wettbewerbsvorteil gegenüber anderen Interessenten darstellen und das Gutachten unterfalle dem Urheberrechtsschutz. Auch diese Mitteilung erfolgte per E-Mail und ohne Rechtsbehelfsbelehrung.

Die Landesbeauftragte wies die Stadtverwaltung auf die Erforderlichkeit hin, die Vorschriften des hier allein einschlägigen Akteneinsichts- und Informationszugangsgesetzes zu beachten und insbesondere eine Ablehnung ausschließlich und in nachvollziehbarer Weise auf die gesetzlich normierten Ausnahmetatbestände zu beschränken. Weshalb der Wettbewerb zwischen den Bietern dadurch beeinträchtigt werden soll, dass potenzielle Bieter mithilfe eines Wertgutachtens erfahren, worauf sie ihr Gebot überhaupt abgeben, erschien ihr nicht nachvollziehbar. Daraufhin erging ein schriftlicher Ablehnungsbescheid mit Rechtsmittelbelehrung, in dem die Stadtverwaltung zusätzlich noch auf den Schutz des Willensbildungsprozesses sowie von Betriebs- und Geschäftsgeheimnissen verwies. Wir hielten die Ablehnung des Antrags mit dieser Begründung für unzulässig und empfahlen die Rücknahme der Entscheidung.

Nur wenige Tage nach dem schriftlichen Ablehnungsbescheid und ohne Gelegenheit gehabt zu haben, darauf zu reagieren, erhielt der Antragsteller einen schriftlichen Widerspruchsbescheid. Mit diesem wies die Stadt den anfangs eingelegten Widerspruch des Petenten zurück. Diesen hatte sie zuvor im Glauben gelassen, der Widerspruch würde wegen der Missachtung des Schriftformerfordernisses gar nicht mehr berücksichtigt. Die Stadt vertrat die Auffassung, der formale Mangel würde dadurch ausgeglichen, dass sie selbst inzwischen einen rechtswirksamen Bescheid erlassen und ihren eigenen Formfehler damit geheilt habe. Den Sinn eines Widerspruchsverfahrens – nämlich dem Widerspruchsführer die Gelegenheit zu geben, Argumente vorzubringen und daraufhin die Rechtmäßigkeit der eigenen Entscheidung zu überprüfen – führte die Stadt damit vollkommen ad absurdum. Schließlich kannte der Antragsteller die Ablehnungsgründe noch gar nicht, als er per E-Mail widersprach. Er hatte jetzt nur noch die Möglichkeit, den Gerichtsweg zu beschreiten. Somit war absehbar, dass ein Informationszugang bis zur Abgabefrist für die Kaufangebote nicht würde erfolgen können. Die Landesbeauftragte legte der Stadt gegenüber erneut die Rechtslage dar und bekräftigte ihre Forderung, die Angelegenheit zu überprüfen. Den Widerspruchsbescheid hielt sie für nichtig und empfahl, dies von Amts wegen festzustellen.

Der Antragsteller formulierte einen neuen, dieses Mal schriftlichen Widerspruch, der nach Ablauf der Angebotsfrist bei der Stadtverwaltung einging. Diese reagierte innerhalb nur eines Tages: Die Sachlage habe sich geändert, der faire Wettbewerb der Bieter stehe einer Akteneinsicht nach Ablauf der Frist zur Angebotsabgabe nicht mehr entgegen. Alle übrigen Ablehnungsgründe spielten plötzlich keine Rolle mehr. Die Akteneinsicht wurde in der Folge gewährt, die dadurch gewonnenen Informationen hatten ihren Wert für den Antragsteller jedoch weitgehend verloren. Es spricht viel dafür, dass das zögerliche, widersprüchliche und rechtlich unhaltbare Vorgehen der Stadtverwaltung nicht zufällig war.

Der Verkauf von Grundstücken durch die öffentliche Hand sollte so transparent wie möglich erfolgen. Wertgutachten über diese Grundstücke sind daher möglichst frühzeitig offenzulegen. Für potenzielle Käufer stellen sie eine wichtige Entscheidungsgrundlage für die Abgabe ihres Kaufangebots dar.

4 Herausgabe von Planungsunterlagen als Kopien

Steht das Urheberrecht der Herausgabe von Planungsunterlagen entgegen? Diese Frage stellen sich Verwaltungen vor allem, wenn Antragsteller die Übersendung der Informationen in elektronischer Form wünschen.

Planungsfragen sind stets von großem Interesse sowohl für die örtliche Gemeinschaft als auch beispielsweise für einzelne Anlieger. Da Planungsverfahren in der Regel ohnehin unter Beteiligung der Öffentlichkeit stattfinden, ist ein Geheimhaltungsbedarf der entsprechenden Unterlagen nur selten gegeben. Wer einen Antrag auf Zugang zu Planungsunterlagen stellt, möchte aber zumeist nicht einfach nur in die Akten schauen, sondern über die Unterlagen verfügen, um beispielsweise in einer Bürgerinitiative oder mit sachverständigen Freunden oder Bekannten darüber zu beraten und die Ergebnisse in den politischen Prozess einzubringen. Die Förderung einer solchen Mitgestaltung ist schließlich ausdrückliches Ziel des Akteneinsichts- und Informationszugangsgesetzes. Die Herausgabe der Unterlagen in elektronischer Form ist sowohl für Antragsteller als auch für Verwaltungen häufig am besten geeignet, diesem Anspruch gerecht zu werden. Ist ein solches Vorgehen aber mit dem Urheberrecht vereinbar, wenn es um Pläne geht, deren Erstellung eine Behörde bei privaten Planungsbüros in Auftrag gibt?

Zunächst stellt sich in solchen Fällen die Frage, ob die Unterlagen überhaupt dem Schutz des Urheberrechts unterfallen. Geschützt sind danach nämlich nur Werke, die eine persönliche schöpferische Leistung darstellen. Einfache Planungsvorhaben, die mehr oder weniger vorgegebenen Standards folgen

oder keine eigenen Besonderheiten aufweisen, die auf die erforderliche Schöpfungstiefe schließen lassen, sind vom Urheberrecht nicht erfasst.

Soweit das Urheberrecht Anwendung auf die Dokumente findet, ist der Zweck des Urheberrechtsgesetzes zu berücksichtigen. Es schützt Werke nicht vor ihrem Bekanntwerden, sondern vor einer unerlaubten (in der Regel wirtschaftlichen) Verwendung ohne Beteiligung des Urhebers. Der Herausgabe von Fotokopien – auch in elektronischer Form – steht das Urheberrecht daher nicht grundsätzlich entgegen. Im Rahmen des Auftragsverhältnisses räumt das Planungsbüro der Verwaltung ein Nutzungsrecht ein, das die Verwendung für die behördlichen Aufgaben einschließt. Die Gewährung von Informationszugang gehört zu den gesetzlichen Aufgaben der Behörde, die der Erledigung der fachlichen (planerischen) Aufgaben nicht nachstehen. Dies betrifft den Informationszugang sowohl nach dem Akteneinsichts- und Informationszugangsgesetz als auch nach dem Umweltinformationsgesetz. Der Herausgabe von Planungsunterlagen in elektronischer Form steht also im Regelfall nichts entgegen.

Um dieses Ergebnis von vornherein klarzustellen, kann es sinnvoll sein, die Möglichkeit der Weitergabe von Kopien bzw. Dateien im Vertrag mit dem Planungsbüro ausdrücklich vorzusehen. Die Behörde ist im Übrigen nicht für die Einhaltung des Urheberrechts durch den Antragsteller verantwortlich, kann diesen jedoch darauf hinweisen, dass die herausgegebenen Dokumente dem Urheberrecht unterliegen.

Das Urheberrecht räumt der Behörde die Nutzung von Planungsunterlagen ihres Auftragnehmers für behördliche Zwecke ein. Die Herausgabe der Dokumente als Fotokopie oder in elektronischer Form im Rahmen der Gewährung von Informationszugang ist von diesem Zweck umfasst.

5 Gutachten zu einer Umgehungsstraße

Wo genau eine neue Umgehungsstraße verlaufen soll, ist in den betroffenen Gemeinden stets Gegenstand strittiger Diskussionen. Obwohl die Verwaltung in einem Fall sogar ein Rechtsgutachten in Auftrag gegeben hatte, um die Auswirkungen alternativer Streckenführungen einzuschätzen, verweigerte sie dessen Herausgabe und verwies stattdessen auf die Bürgerbeteiligung in dem noch durchzuführenden Planfeststellungsverfahren.

Das Akteneinsichts- und Informationszugangsgesetz bestimmt, dass während des laufenden Verfahrens die Einsichtnahme nur nach Maßgabe des anzu-

wendenden Verfahrensrechts gewährt wird. Da das Verfahren zur Linienbestimmung kein solches Einsichtsrecht enthalte, argumentierte die Verwaltung, bestehe auch kein Anspruch auf Herausgabe des Gutachtens. Außerdem sei der Prozess der Willensbildung zu schützen. Nachdem die Linienführung bestätigt und amtlich verkündet worden war, erneuerte der Antragsteller sein Begehren, erhielt jedoch von der Behörde keine Antwort.

Wir gingen davon aus, dass zumindest nach der Bestätigung der Linienführung nicht mehr von einem laufenden Verfahren auszugehen und der Anwendungsbereich somit eröffnet war. Darüber hinaus bezweifelten wir, dass es sich zuvor überhaupt um ein Verfahren im Sinne des Akteneinsichts- und Informationszugangsgesetzes gehandelt hatte. Das Gesetz bezweckt mit seiner Ausnahme der Einsicht in laufenden Verfahren im Wesentlichen den Schutz von Verwaltungsverfahren mit einer Außenwirkung, nicht aber des Zustandekommens planerischer Feststellungen. Die Behörde selbst beschied dem Antragsteller zudem, dass ein Verfahren zur Linienbestimmung nicht näher gesetzlich geregelt sei. Der Verweis auf das anzuwendende Verfahrensrecht ging somit aus unserer Sicht ins Leere. Soweit kein Verfahrensrecht besteht, kann die Anwendung des Akteneinsichts- und Informationszugangsgesetzes auch nicht mit Verweis auf ein solches ausgeschlossen werden.

Auch hielten wir den Hinweis auf einen schützenswerten Willensbildungsprozess nicht für zutreffend. Ein Rechtsgutachten stellt eine neutrale Grundlage für eine fachliche Bewertung dar und ist die Basis für eine behördliche Willensbildung und Entscheidung. Es bildet die Entscheidungsfindung aber keineswegs ab, sondern liegt ihr lediglich zugrunde. Selbst wenn der entsprechende Ausnahmetatbestand zum Tragen gekommen wäre, hätte die Behörde eine Abwägung zwischen dem Einsichts- und dem Geheimhaltungsinteresse vornehmen müssen. Dabei wäre das offensichtliche Interesse der lokalen Öffentlichkeit an den Informationen angemessen zu berücksichtigen gewesen. Eine solche Interessenabwägung fand jedoch nicht statt.

Angesichts der in jedem Fall zu erwartenden Auswirkungen von Straßenplanungen für die Umwelt vertraten wir zudem die Auffassung, dass zumindest teilweise das Umweltinformationsgesetz zum Tragen kommt. Soweit von einem Antrag auf Akteneinsicht Umweltinformationen betroffen sind, ist es vorrangig vor dem Akteneinsichts- und Informationszugangsgesetz anzuwenden, auf dessen Ausnahmetatbestände dann nicht mehr zurückgegriffen werden kann.

Nachdem wir mit diesen Hinweisen an die Behörde herangetreten waren, erhielt der Antragsteller den begehrten Zugang zu dem Gutachten.

Gutachten über die Linienführung einer Umgehungsstraße können nicht unter Verweis auf die schützenswerte Willensbildung der Behörden abgelehnt werden. Sie stellen eine neutrale Entscheidungsgrundlage dar, die möglichst frühzeitig offenzulegen ist.

6 Die Verlegung von Wasserleitungen – ein Geheimnis?

Im Zusammenhang mit der Verlegung von Leitungen für Schmutz- und Trinkwasser interessierten sich Bürger der betroffenen Ortschaft für Unterlagen zu dieser Erschließungsmaßnahme. In seinem Bemühen, den Informationszugang abzuwehren, war der Zweckverband einfallsreich.

Der Antrag war hinreichend bestimmt, sodass keine Zweifel bestanden, auf welche Akten er sich richtete. Zwar bestritt der Verband dies nicht, forderte die Antragsteller aber zunächst auf, ihr Interesse an der Akteneinsicht darzulegen. Außerdem sollten sie erklären, weshalb sie sich die Informationen nicht bei einer anderen Stelle beschaffen können. Schließlich lehnte der Zweckverband den Antrag mit der Begründung ab, der Anspruch aus dem Akteneinsichts- und Informationszugangsgesetz beschränke sich auf Verfahrensbeteiligte oder „anderweitig Betroffene“, um die es sich bei den Antragstellern nicht handle. Nachdem wir mit umfangreichen rechtlichen Hinweisen an den Verband herangetreten waren, hielt dieser an der Verweigerung des Informationszugangs fest. In seinem Ablehnungsbescheid teilte er mit, sich „den Standpunkt erarbeitet“ zu haben, das Akteneinsichts- und Informationszugangsgesetz sei als Ergänzung des Verwaltungsverfahrensgesetzes zu sehen.

Der Informationsanspruch des Akteneinsichts- und Informationszugangsgesetzes gilt für jedermann und kann ohne Voraussetzungen geltend gemacht werden. Ein Antragsteller ist in der Regel nicht verpflichtet, darzulegen, aus welchen Gründen er den Informationszugang begehrt. Seine Verpflichtung, den Antrag hinreichend zu bestimmen, bedeutet lediglich, ihn soweit zu konkretisieren, dass die Behörde erkennen kann, welche Unterlagen für ihn von Interesse sind. Zudem muss der Antragsteller keine bestimmte Rechtsposition – wie z. B. die formale Beteiligung an einem Verwaltungsverfahren – vorweisen. Im Gegenteil ist das Gesetz im laufenden Verwaltungsverfahren sogar ausdrücklich nicht anwendbar. Der vom Zweckverband „erarbeitete Standpunkt“ ließ sich mit diesen bereits mehrfach gerichtlich bestätigten Grundsätzen des Gesetzes in keiner Weise vereinbaren. Der Anspruch bezieht sich zudem auf Unterlagen, die bei einer informationspflichtigen Stelle vorhanden sind und gilt unabhängig von der Frage, welche andere Stelle möglicherweise ebenfalls über Informationen verfügt oder gegebenenfalls das

Verfahren führt oder geführt hat. Ein zusätzlicher Hinweis auf andere Stellen, die als Adressat eines Antrags in Frage kommen, kann für den Antragsteller durchaus hilfreich sein; die Ablehnung des Antrags mit dieser Begründung ist jedoch unzulässig.

Nachdem wir den Zweckverband erneut auf die Rechtslage hingewiesen hatten, half er dem gleichzeitig eingelegten Widerspruch ab und gewährte Zugang zu den begehrten Informationen.

Das Akteneinsichts- und Informationszugangsgesetz gilt für jedermann und ohne Voraussetzungen. Wer auf dieser Grundlage Informationen begehrt, darf in der Regel nicht nach den Gründen für das Einsichtsinteresse gefragt werden.

7 Kommunalaufsicht im stillen Kämmerlein?

Wenn eine Kommunalaufsichtsbehörde die Rechtmäßigkeit einer gemeindlichen Satzung prüft, ist davon auszugehen, dass eine solche Kontrolle nicht ohne Anlass erfolgt. Regelmäßig scheitern Antragsteller aber mit ihren Begehren, sich über den genauen Inhalt und das Ergebnis kommunalrechtlicher Prüfungen zu informieren.

Werden beispielsweise Eigentümer für die Reinigung oder Schneeräumung der öffentlichen Straßen vor ihren Grundstücken finanziell in Anspruch genommen, so erfolgt dies auf der Grundlage einer Satzung. Die Einsichtsrechte aus dem Verwaltungsverfahren zur Kostenerhebung gelten nur für die formal Beteiligten und beschränken sich auf den unmittelbaren Vorgang der Kostenerhebung. Sie erstrecken sich somit nicht auf das Zustandekommen des entsprechenden Ortsrechts, das der Berechnung zugrunde liegt. Erhält die Kommunalaufsichtsbehörde einen relevanten Hinweis darauf, dass die Satzung möglicherweise fehlerhaft ist, leitet sie ein entsprechendes Prüfungsverfahren ein, das formal ebenfalls nicht im Zusammenhang mit dem Verfahren zur Kostenerhebung steht.

In einem konkreten Fall erfuhr ein Antragsteller von der Tatsache, dass die Kommunalaufsicht des Landkreises eine Straßenreinigungssatzung geprüft hatte, und beantragte Einsicht in den Kontrollvorgang. Die Behörde verweigerte den Informationszugang unter Verweis auf den entsprechenden Ausnahmetatbestand des Akteneinsichts- und Informationszugangsgesetzes. Danach ist ein Antrag abzulehnen, wenn ansonsten Inhalte von Akten offenbart würden, die der Aufsicht über eine andere Stelle dienen. Eine Aussonderung schutzbedürftiger Informationen sowie die Offenlegung der übrigen Akte

kämen nicht in Frage, da sich sämtliche Aktenteile auf die Aufsichtstätigkeit bezögen.

Im Ergebnis bestätigte die Landesbeauftragte die Rechtsauffassung des Landkreises. Der beschriebene Ausnahmetatbestand war durch die Aufsichtsmaßnahme der Kommunalaufsicht gegenüber der Gemeinde zweifelsfrei erfüllt. Auch erschien es plausibel, dass der Vorgang ausschließlich Unterlagen enthielt, die im Zusammenhang mit der Aufsichtstätigkeit standen. Das Gesetz sieht an dieser Stelle keine Abwägungsmöglichkeit vor, d. h. wenn die Ausnahme vorliegt, muss die Behörde den Antrag auf Informationszugang ablehnen. Sie hat keine Möglichkeit, einen Ausgleich zwischen ihrem Geheimhaltungsinteresse und dem Einsichtsinteresse des Antragstellers herzustellen.

Der Landkreis berief sich in seinem Ablehnungsbescheid zusätzlich auf ein Urteil des Verwaltungsgerichts Potsdam,⁸⁷ welches feststellte, das öffentliche Interesse an der Zurückhaltung der Aufsichtsakten werde nicht schon aufgrund des Abschlusses einzelner Aufsichtsmaßnahmen hinfällig, beschränke sich also nicht auf laufende Aufsichtsvorgänge. In einem früheren Urteil kam dasselbe Verwaltungsgericht unter Bezugnahme auf die Gegenwartsform des Verbs in der Formulierung „der Aufsicht über eine andere Stelle dienen“ hingegen zur Feststellung, dass der Schutzbedarf nach Abschluss der Aufsichtsmaßnahme entfalle.⁸⁸ Der Gesetzgeber hat sich im Rahmen der Novellierung des Akteneinsichts- und Informationszugangsgesetzes inzwischen für eine restriktive Klarstellung entschieden. Künftig sind alle Akten geschützt, „die der Aufsicht über eine andere Stelle dienen oder gedient haben.“

Akten, die der Aufsicht über eine andere Stelle dienen, dürfen nicht offengelegt werden. Das betrifft nicht nur die Aufgaben der Kommunalaufsicht, sondern auch andere fach- und dienstrechtliche Aufsichtstätigkeiten. Der Gesetzgeber hat inzwischen klargestellt, dass auch abgeschlossene Aufsichtsvorgänge unter diesen Ausnahmetatbestand fallen.

⁸⁷ Verwaltungsgericht Potsdam, Urteil vom 8. Juni 2011, 9 K 116/08.

⁸⁸ Verwaltungsgericht Potsdam, Urteil vom 27. April 2010, 3 K 1595/05.

8 Kalkulationsunterlagen zur Berechnung von Beiträgen

Werden Kosten für die Erschließung eines Grundstücks erhoben, kommen auf die Eigentümer oft hohe Summen zu. Wer wollte in dieser Situation nicht nachrechnen, ob die Beiträge in der geforderten Höhe berechtigt sind? Beantragen die Eigentümer Akteneinsicht, muss die Verwaltung genau prüfen, welche Rechtsgrundlage für den Informationszugang anzuwenden ist.

Nicht selten werden bereits die Entscheidungen für die Baumaßnahmen von Anwohnern wegen der ihnen drohenden Kosten abgelehnt. Der Ausbau einer Straße, der Anschluss eines Wohngebiets an die Wasserversorgung oder auch die umstrittene Heranziehung so genannter „Altanschließer“ für die lange zurückliegende Errichtung einer Kanalisation – in vielen Fällen kommen auf die Betroffenen Kostenforderungen in Höhe mehrerer tausend Euro zu.

Der Adressat eines Beitragsbescheids beantragte bei seiner Stadtverwaltung vor diesem Hintergrund unter anderem den Informationszugang zu Unterlagen, die als Grundlage für die Beitragssatzung herangezogen wurden, zu einem Rechtsgutachten über die Finanzierung der Abwasserentsorgungsanlage sowie zu Fördermitteln, die für die Erstellung der Anlage verwendet wurden. Die Behörde gewährte lediglich Akteneinsicht in den Vorgang zur Beitragserhebung sowie in die Beitragskalkulation. Sie stützte dieses Vorgehen auf die Ausübung ihres pflichtgemäßen Ermessens. Die Anfertigung von Kopien wurde von ihr ausdrücklich, aber ohne nähere Begründung, nicht für erforderlich erachtet. Mit dem Argument, es liefen mehrere verwaltungsgerichtliche Verfahren zur Überprüfung der Rechtmäßigkeit der Satzung, verweigerte die Stadtverwaltung – unter Berufung auf die Ausnahme laufender Verfahren vom Anwendungsbereich des Akteneinsichts- und Informationszugangsgesetzes – den Informationszugang zu den Grundlagen der Beitragssatzung. Das Begehren im Hinblick auf das Rechtsgutachten und die Unterlagen zu den Fördermitteln ignorierte sie.

Die Landesbeauftragte wies die Stadtverwaltung darauf hin, dass die verwaltungsgerichtliche Überprüfung der Rechtmäßigkeit der Beitragssatzung es nicht rechtfertigt, die Einsicht in den längst abgeschlossenen Vorgang der Satzungsgebung abzulehnen und empfahl die Herausgabe von Fotokopien. Nachfragen der Landesbeauftragten zu den übrigen noch offenen Aspekten beantwortete die Stadt erst unzureichend, später auch nach mehrfacher Erinnerung gar nicht. Diesen Verstoß gegen die Verpflichtung, die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht bei der Erfüllung ihrer Aufgaben zu unterstützen, beanstandete diese förmlich. Im Nachgang zu dieser Beanstandung sowie vor dem Hintergrund der Klageer-

hebung durch den Antragsteller, erhielt dieser zunächst die erbetenen Kopien sowie später auch die Fördermittelbescheide und das Rechtsgutachten.

In diesem und weiteren Fällen, mit denen sich die Landesbeauftragte im Berichtszeitraum zu befassen hatte, wurde deutlich, dass es zunächst wesentlich darauf ankommt, beide Verfahren – also das laufende Verfahren zur Beitragserhebung gegenüber Einzelnen und die grundsätzlich vorgelagerte Satzungsgebung – bei der Prüfung von Anträgen auf Akteneinsicht voneinander getrennt zu betrachten. Dabei ist zu berücksichtigen, dass sich die Rechtslage im Berichtszeitraum teilweise geändert hat:

Bislang stand die Gewährung der Einsicht in die unmittelbaren Verfahrensunterlagen unter dem Vorbehalt der Ausübung des pflichtgemäßen Ermessens. Die üblichen Einsichtsrechte aus dem Verwaltungsverfahrensgesetz standen den Kostenschuldnern nicht zu, weil in diesen Verfahren kommunalabgabenrechtliche Vorschriften angewandt wurden. Aufgrund einer Änderung des Kommunalabgabengesetzes stehen den Beteiligten künftig in kommunalabgabenrechtlichen Verfahren dieselben Akteneinsichtsrechte zu wie den Beteiligten in herkömmlichen Verwaltungsverfahren.⁸⁹ Dieser Einsichtsanspruch umfasst – unter den im Verwaltungsverfahrensgesetz genannten Voraussetzungen – im Wesentlichen den Vorgang zur Berechnung des von der Satzung vorgesehenen Beitrags für das jeweilige Grundstück. Die Berechnung ist jedoch ohne Kenntnis der vollständigen Beitragskalkulation bezogen auf die Gesamtheit der Grundstücke nicht nachvollziehbar, sodass auch diese Unterlagen noch vom Einsichtsrecht der Verfahrensbeteiligten umfasst sind.

Oft ist die Berechnung des individuellen Beitragssatzes aus den Vorgaben der Satzung jedoch relativ einfach und ihre Richtigkeit wird auch gar nicht bestritten. Bezweifelt wird aber teilweise, dass der im jeweiligen Ortsrecht enthaltene Beitragssatz korrekt ermittelt wurde. Diese Zweifel richten sich somit auf das Verfahren zum Zustandekommen der Satzung. Mit dem in solchen Fällen stets zurückliegenden In-Kraft-Treten der Satzung ist dieser Vorgang abgeschlossen. Den Kostenschuldnern steht hier kein Einsichtsanspruch aus dem Verwaltungsverfahrensgesetz zu. Dieses gilt nur für Beteiligte im Rahmen laufender Verwaltungsverfahren. Der Anspruch ist vielmehr auf der Grundlage des Akteneinsichts- und Informationszugangsgesetzes zu prüfen. Dieses gilt somit für Kostenschuldner wie für unbeteiligte Antragsteller gleichermaßen. Soweit keine schutzbedürftigen öffentlichen oder privaten Interessen der Akteneinsicht entgegenstehen, ist die Akteneinsicht zu gewähren. Seit der Novellierung des Gesetzes besteht nunmehr auch ein ausdrücklicher Anspruch auf die Herausgabe von Fotokopien.

⁸⁹ Artikel 4 Nr. 3 des Gesetzes zur Änderung verwaltungsvollstreckungs- und abgabenrechtlicher Vorschriften vom 16. Mai 2013 (GVBI I Nr. 18 S. 18)

Das Akteneinsichts- und Informationszugangsgesetz vermag jedoch nur im Nachhinein für Transparenz zu sorgen. Zweckverbände, Gemeinden, Städte und Landkreise sollten daher bereits den Prozess zur Entscheidung, Straßen auszubauen oder Versorgungsanlagen zu errichten, sowie die konkrete Planung dieser Maßnahmen möglichst offen gestalten.

Werden die Kosten für den Ausbau von Straßen auf die Anwohner umgelegt, haben diese als Verfahrensbeteiligte grundsätzlich einen Anspruch auf Einsicht in die Akte zur Beitragserhebung sowie in die Gesamtkalkulation. Der Zugang zu Unterlagen, die dem Zustandekommen der Beitragssatzung zugrunde liegen, richtet sich nach dem Akteneinsichts- und Informationszugangsgesetz.

9 Per E-Mail zur Akteneinsicht?

Das Akteneinsichts- und Informationszugangsgesetz berechtigt zur Antragstellung per E-Mail. Eine Verschlüsselung der E-Mail oder Authentifizierung des Antragstellers ist dafür nicht erforderlich. Behörden erkundigen sich deshalb, ob sie den elektronischen Weg überhaupt für die weitere Korrespondenz nutzen dürfen.

Ein Antrag ist schriftlich oder elektronisch an die Akten führende Behörde zu richten. Dieser Wortlaut des Akteneinsichts- und Informationszugangsgesetzes wurde vom Gesetzgeber bereits im Jahr 2003 mit dem Ziel beschlossen, die Hürden für die Antragstellung möglichst niedrig anzusetzen. Seither können Anträge per E-Mail eingereicht werden. Dies erfolgt in der Praxis auch weitgehend ohne Probleme und mindert den Aufwand des Schriftverkehrs für alle Beteiligten. Die meisten Informationen der Verwaltungen werden inzwischen ohnehin in elektronischer Form geführt. Richtet sich ein Antrag auf eine solche Datei, deren Inhalt keinerlei gesetzlich geregelten Schutzbedarf aufweist, kann der Versand unbürokratisch per Mausklick erfolgen. Schließlich könnte die Behörde solche Informationen auch für jedermann abrufbar auf ihre Internetseiten stellen.

Bei jeder Entscheidung über die Akteneinsicht handelt es sich um einen Verwaltungsakt, der, vor allem, wenn Informationen ganz oder teilweise zurückgehalten oder Kosten erhoben werden müssen, in Form eines Bescheides getroffen wird. Während der Antragsteller frei wählen kann, ob er schriftlich oder per E-Mail an die Behörde herantritt, ist diese in den genannten Fällen an das Schriftformerfordernis gebunden. Der Begriff „schriftlich“ umfasst dabei neben der herkömmlichen Papiervariante auch die qualifiziert elektronisch signierte E-Mail. Wenn der letztgenannte Weg bei der Kommuni-

kation mit dem Antragsteller nicht zur Verfügung steht, kann der Bescheid nur per Post verschickt werden. Hierzu benötigt die Behörde die zustellfähige Anschrift des Antragstellers. Sobald also feststeht, dass ein Ablehnungs- oder Kostenbescheid ergehen soll, ist es erforderlich, den Antragsteller entsprechend zu informieren, nach der postalischen Anschrift zu fragen und die weitere Korrespondenz dann auf dem Postweg zu führen. Auch können Fälle vorkommen, in denen die Beteiligtenfähigkeit der Antragsteller zu prüfen ist, was ebenfalls nähere Angaben zur Person erfordert. Das schließt jedoch keineswegs aus, die beantragten Informationen in elektronischer Form zu übermitteln, falls der Antragsteller dies wünscht.

Für Anträge auf Informationszugang, die über das Internetportal „Frag den Staat“⁹⁰ eingereicht werden, gilt dasselbe wie für die Beantragung per unverschlüsselter E-Mail. Die Plattform veröffentlicht Anfragen und Antworten nach den Informationsfreiheitsgesetzen und beabsichtigt, die Antragstellung zu erleichtern. Das Projekt wird von der Open Knowledge Foundation Deutschland e. V. getragen und von zahlreichen zivilgesellschaftlichen Organisationen unterstützt. Die Veröffentlichung der Korrespondenz zwischen Antragstellern und Behörden soll den staatlichen Umgang mit der Informationsfreiheit transparent machen und die auf diesem Wege übermittelten Informationen für jedermann abrufbar bereitstellen.

Seit August 2012 ermöglicht es die Plattform, Anfragen auf der Grundlage des Akteneinsichts- und Informationszugangsgesetzes, des Umweltinformationsgesetzes und des Verbraucherinformationsgesetzes auch an öffentliche Stellen aus Brandenburg zu richten. Davon wird zunehmend Gebrauch gemacht. Die angefragte Stelle erhält eine E-Mail mit einem vorformulierten Rahmentext, der vom Antragsteller vor allem um die Angabe der gewünschten Information ergänzt wird. Diese Anfrage wird gleichzeitig auf der Internetplattform veröffentlicht. Bei der Absenderadresse handelt es sich um eine computergenerierte Mailadresse. Zu beantworten ist diese Anfrage in derselben Weise wie jede andere E-Mail. Der Unterschied besteht lediglich darin, dass die Antwort der informationspflichtigen Stelle an die Plattform geleitet und dort veröffentlicht wird. Dies gilt auch für die gegebenenfalls noch folgende Korrespondenz. Enthält die Antwort der Behörde Anhänge, so bedarf deren Veröffentlichung der Zustimmung des Antragstellers. Er kennzeichnet den Status der Anfrage beispielsweise als erfolgreich beantwortet, abgelehnt oder verspätet oder gibt an, dass die beantragte Information nicht vorhanden ist. Zudem besteht für den Antragsteller die Möglichkeit, die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht über die Plattform anzurufen. Durch entsprechende Piktogramme sind der Status bzw. das Ergebnis der Anfrage auf einen Blick zu erkennen. Der Antragsteller hat auch

⁹⁰ siehe <https://fragdenstaat.de>

die Möglichkeit, Anfragen nicht öffentlich zu stellen und erst zu einem späteren Zeitpunkt öffentlich zu machen. Deshalb ist nicht jede Anfrage, die bei einer Behörde eingeht, von Anfang an auf der Website zu sehen.

Sollte im Verlauf der Bearbeitung des Antrags aus den genannten rechtlichen Gründen die Korrespondenz auf dem Postweg erfolgen, steht es dem Antragsteller frei, den Schriftverkehr sowie die ihm zugänglich gemachten Unterlagen auf der Plattform zu veröffentlichen. Über die Veröffentlichung seines Namens auf „Frag den Staat“ entscheidet der Antragsteller selbst; die Namen der zuständigen Beschäftigten der informationspflichtigen Stellen werden in der Regel nicht geschwärzt (s. a. § 5 Abs. 3 AIG).

Die Verwendung unverschlüsselter elektronischer Kommunikation erleichtert zwar die Antragstellung, allerdings empfiehlt die Landesbeauftragte den Antragstellern, davon grundsätzlich nur Gebrauch zu machen, wenn es auf die Vertraulichkeit der Inhalte nicht ankommt. Insbesondere die unverschlüsselte Übermittlung personenbezogener Daten in einer E-Mail ist mit erheblichen datenschutzrechtlichen Risiken verbunden.

Akteneinsicht kann auf einfachem Wege per E-Mail beantragt werden. Wird dieser Antrag jedoch ganz oder teilweise abgelehnt oder muss die Behörde Kosten erheben, benötigt sie bei postalischer Kommunikation die zustellfähige Anschrift des Antragstellers. Soll der Bescheid elektronisch versandt werden, ist er qualifiziert zu signieren. Dies gilt auch für Anfragen, die über die Internetplattform „Frag den Staat“ gestellt werden.

Teil D

Die Dienststelle

1 Die Dienststelle

Im Jahr 2010 entschied der brandenburgische Gesetzgeber, die Datenschutzaufsicht über den öffentlichen und den nicht öffentlichen Bereich in meiner Dienststelle zusammenzulegen und die Zuständigkeit für die Verfolgung von Ordnungswidrigkeiten hierhin zu verlagern. Diese Entscheidung war mit einem Zuwachs an Aufgaben verbunden, der jedoch nur teilweise durch die Bereitstellung entsprechender personeller Ressourcen ausgeglichen wurde. Im Berichtszeitraum sind die Herausforderungen für meine Behörde weiter gestiegen. Dies ist z. B. an der stetig wachsenden Zahl der Anfragen und Beschwerden sowohl im Bereich des Datenschutzes als auch bei der Akteneinsicht und dem Informationszugang ablesbar. Zudem haben sich in den vergangenen beiden Jahren die Zahl und der Umfang der Beratungsgesprächen sowohl auf rechtlichem als auch auf technischem Gebiet kontinuierlich erhöht. Und auch die Verfolgung und Ahndung von Verstößen gegen datenschutzrechtliche Vorschriften, die Durchführung von Ordnungswidrigkeitenverfahren sowie die Verhängung von Bußgeldern verursachen einen zunehmenden Aufwand.

Das Parlament hat diesem Umstand Rechnung getragen und für den Doppelhaushalt 2013/2014 eine zusätzliche Referentenstelle für meine Dienststelle bewilligt. Diese konnte nach erfolgter Ausschreibung mit einer qualifizierten Informatikerin aus meinem Haus besetzt werden. Die dadurch freigewordene Stelle wurde ebenfalls ausgeschrieben. Aus der Vielzahl von Bewerbungen wählte ich eine Diplomverwaltungswirtin aus, die nun den juristischen Bereich verstärkt. Auf Grund der hohen Arbeitsbelastung war es darüber hinaus erforderlich, im Berichtszeitraum zusätzlich einen juristischen Mitarbeiter und eine juristische Mitarbeiterin befristet zu beschäftigen. Einer dauerhaften Anstellung stand entgegen, dass im Haushaltsplan keine Stelle vorgesehen war.

Um Arbeitsabläufe effizienter zu gestalten, habe ich die Organisationsstruktur meiner Dienststelle verändert. Seit August 2013 ist sie in drei Bereiche gegliedert: Technik, Recht, Verwaltung. Darüber hinaus verfügen die Bereiche Recht und Verwaltung nunmehr über Unterstrukturen in Form von Gruppen.

Wie bereits auch meine Vorgänger im Amt bemühe ich mich nach wie vor um einen Sitz der Dienststelle in der Landeshauptstadt Potsdam. Damit verspre-

che ich mir wesentlich mehr Bürgernähe und Präsenz, die nicht zuletzt durch eine bessere Erreichbarkeit der Dienststelle gegeben wäre. Wichtig ist mir zudem eine größere Nähe zu den Daten verarbeitenden Stellen, die von meiner Behörde beraten und kontrolliert werden. Es bleibt abzuwarten, ob im Zuge der vielen Standortveränderungen der Landesverwaltung in Potsdam auch eine Möglichkeit für einen Umzug meiner Dienststelle gefunden wird.

2 Zusammenarbeit mit dem Landtag

Die Zusammenarbeit mit dem Landtag war in den letzten beiden Jahren wieder eng und von Vertrauen geprägt.

Als Landesbeauftragte wurde ich zu unterschiedlichen Datenschutzfragen in Gesetzgebungsverfahren sowohl vom Innen-, Haupt-, Rechts- und Europa-ausschuss angehört. Darüber hinaus hatte ich die Möglichkeit, als Sachverständige beispielsweise zu den Gesetzentwürfen eines Informationszugangsneuregelungsgesetzes der Fraktion Bündnis 90/Die Grünen und dem Entwurf der Landesregierung zu einer Novellierung des Akteneinsichts- und Informationszugangsgesetzes vorzutragen. Im Innenausschuss berichtete ich regelmäßig über die Ergebnisse der Konferenz der Datenschutzbeauftragten des Bundes und der Länder.

Im September und November 2012 befasste sich der Innenausschuss mit meinem 16. Tätigkeitsbericht. Er verabschiedete eine Beschlussempfehlung, um die Landesregierung aufzufordern, dem Landtag die bereits angekündigte Neufassung des Akteneinsichts- und Informationszugangsgesetzes bis Ende des Jahres 2012 zuzuleiten. Die Beschlussempfehlung enthielt zudem eine Aufforderung an die Landesregierung, beim weiteren Aufbau des Brandenburgischen IT-Dienstleisters die erforderlichen Voraussetzungen sicherzustellen, damit Sicherheitslücken im IT-Sicherheitsmanagement der Landesverwaltung frühzeitig erkannt und interministeriell geschlossen werden. Der Landtag ist der Beschlussempfehlung des Innenausschusses in seiner Sitzung am 13. Dezember 2012 gefolgt.⁹¹

Der im Dezember 2012 vom Parlament beschlossene Doppelhaushalt für die Jahre 2013 und 2014 hat einer Beschlussvorlage des zuständigen Ausschusses Rechnung getragen und meiner Dienststelle einen Personalzuwachs im Rahmen einer zusätzlichen Stelle der Entgeltgruppe 14 gewährt.

⁹¹ siehe Beschluss des Landtages Brandenburg vom 13. Dezember 2012, Landtags-Drucksache 5/6453-B

3 Zusammenarbeit mit behördlichen Datenschutzbeauftragten

Einmal jährlich laden wir die behördlichen Datenschutzbeauftragten der Landkreise, kreisfreien Städte und größeren kreisangehörigen Gemeinden zu einer jeweils ganztägigen Beratung in unsere Dienststelle ein, um gemeinsam Fragen und Probleme der Anwendung des Datenschutz- bzw. des Akteneinsichtsrechts in den Kommunalverwaltungen zu erörtern. Darüber hinaus dienen die Treffen regelmäßig dem Austausch der Beteiligten zu den Aufgabenfeldern der behördlichen Datenschutzbeauftragten sowie zur Umsetzung ihrer Empfehlungen in den jeweiligen Behörden.

Die Themen werden jeweils von den Teilnehmern selbst angemeldet. Sie stammen in der Regel aus ihrer täglichen Praxis der behördlichen Datenschutzbeauftragten und sind von allgemeinem Interesse. Oft resultieren sie auch aus aktuellen Projekten zur Einführung von neuen oder Änderung bestehender DV-Verfahren in den Verwaltungen. Die Diskussionen während der Veranstaltung ermöglichen es z. B. Lösungsansätze vorzustellen, Rechtsauffassungen auszutauschen und Stellungnahmen abzustimmen oder bewährte Vorgehensweisen weiterzuempfehlen. Für die Landesbeauftragte verringert sich der Aufwand im Vergleich zu Einzelberatungen erheblich.

Im Berichtszeitraum fanden die Treffen jeweils im August 2012 bzw. 2013 statt. Schwerpunkte waren u. a. datenschutzgerechte Personalaktenführung, Datenverarbeitung durch Jobcenter, Datenschutzaufgaben der Schulträger, Datenübermittlungen zwischen Gesundheitsämtern, Datenschutz in kommunalen Gremien, Auswirkungen des E-Government-Gesetzes, Umgang mit Geodaten sowie Abgrenzung von Rechtsgrundlagen für die Akteneinsicht und den Informationszugang.

4 Zusammenarbeit mit Datenschutzbehörden

4.1 Datenschutzkonferenz – 2012 unter brandenburgischem Vorsitz

Im Rahmen halbjährlicher Konferenzen stimmen die Datenschutzbeauftragten des Bundes und der Länder ihre Haltung in Fragen aus Technik, Wirtschaft oder Recht ab. Sie veröffentlichen diese Positionen in Form von Entschlüssen. Im Jahr 2012 übernahm die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht – nach 17 Jahren nunmehr zum zweiten Mal – den jährlich wechselnden Vorsitz der Konferenz.

Die Übernahme des Konferenzvorsitzes fiel zeitlich mit dem derzeit wohl wichtigsten Datenschutzvorhaben – der Novellierung des Datenschutzrechts in der Europäischen Union – zusammen. Im Januar 2012 stellte die Europäische Kommission ihren Entwurf einer Datenschutz-Grundverordnung sowie einer Richtlinie für den polizeilichen und justiziellen Bereich vor. Durch die Verordnung soll der Datenschutz modernisiert und harmonisiert werden; mit der Richtlinie beabsichtigt die Kommission, die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung neu zu regeln. Da sich auch die Datenschutzbestimmungen des Bundes und der Länder nach europäischen Vorgaben richten, konzentrierte sich die Konferenz im Jahr 2012 darauf, ihre Position in die Diskussion um diese Vorgaben einzubringen.

Als Konferenzvorsitzende koordinierte die Landesbeauftragte die Positionierung der Datenschutzbeauftragten des Bundes und der Länder zu den Vorhaben der Europäischen Kommission. Die zuständige Kommissarin für Justiz, Grundrechte und Bürgerschaft sowie Vizepräsidentin der Kommission, Viviane Reding, folgte ihrer Einladung zur Frühjahrskonferenz der Datenschutzbeauftragten am 21. und 22. März 2012 in Potsdam, um die Entwürfe gemeinsam zu erörtern. In einer ersten EntschlieÙung unterstützte die Datenschutzkonferenz das Vorhaben der Europäischen Kommission. Im weiteren Verlauf führte die Konferenzvorsitzende zahlreiche Gespräche in den zuständigen Gremien der Europäischen Union und vertrat dort eine ausführliche, im Juni 2012 veröffentlichte Stellungnahme der Konferenz zu den vorgelegten Entwürfen.⁹² Die Frühjahrskonferenz befasste sich darüber hinaus mit öffentlich geförderten Forschungsprojekten zur Entdeckung abweichenden Verhaltens im öffentlichen Raum sowie mit der Europäischen Ermittlungsanordnung. Später veröffentlichten die Datenschutzbeauftragten EntschlieÙungen zur Stärkung von Patientenrechten und zur datenschutzgerechten Gestaltung des Melderechts sowie eine Orientierungshilfe zum Smart Metering.

Auch auf der von der Landesbeauftragten ausgerichteten Herbstkonferenz am 7. und 8. November 2012 in Frankfurt (Oder) war die Novellierung des Datenschutzes in Europa der wichtigste Tagesordnungspunkt. Die Konferenz bekräftigte mit einer erneuten EntschlieÙung ihren Einsatz für eine wirksame Datenschutz-Grundverordnung und wandte sich gegen inzwischen erhobene Bestrebungen, Ausnahmen vom Datenschutz zu schaffen. Darüber hinaus fasste die Konferenz EntschlieÙungen zur Reform der Sicherheitsbehörden sowie zur Übermittlung von Meldedaten an öffentlich-rechtliche Religionsge-

⁹² Zum Inhalt der Stellungnahme und weiteren Einzelheiten des Entwurfs der Datenschutz-Grundverordnung siehe B 1.

meinschaften und die GEZ. Außerdem veröffentlichte sie Hinweise für Provider und Hersteller zur Einführung von IPv6.

Den Abschluss des brandenburgischen Konferenzvorsitzes stellte die am 28. Januar 2013 von der Landesbeauftragten im Auftrag der Datenschutzbeauftragten des Bundes und der Länder ausgerichtete öffentliche Veranstaltung in Berlin anlässlich des 7. Europäischen Datenschutztages⁹³ dar.

Unter Vorsitz der bremischen Landesbeauftragten für Datenschutz und Informationsfreiheit, Dr. Imke Sommer, befasste sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Jahr 2013 erneut mit der Novellierung des europäischen Datenschutzrechts. Hintergrund waren Diskussionen im Europäischen Parlament und im Rat, die eine Absenkung des Datenschutzniveaus befürchten ließen. Außerdem veröffentlichte die Konferenz im Frühjahr 2013 Entschlüsse zum Beschäftigtendatenschutz, zur Pseudonymisierung von Krebsregisterdaten und zum Datenschutz in einer transatlantischen Freihandelszone. Sie legte zudem eine Orientierungshilfe für Betreiber sozialer Netzwerke sowie Unternehmen und öffentliche Stellen, die diese nutzen, vor. Die zweite Hälfte des bremischen Konferenzvorsitzes fiel zusammen mit den Enthüllungen über die Ausspähungen durch verschiedene Nachrichtendienste. Im September 2013 wandten sich die Datenschutzbeauftragten gegen diese umfassende und anlasslose Überwachung und forderten zügige Konsequenzen. Auf ihrer Herbstkonferenz veröffentlichten sie Positionen zur sicheren elektronischen Kommunikation und zur Stärkung des Datenschutzes im Sozial- und Gesundheitswesen. Sie formulierten datenschutzrechtliche Forderungen für die neue Legislaturperiode des Deutschen Bundestages und wiesen auf den Handlungsbedarf zum Datenschutz im Bereich der öffentlichen Sicherheit hin.

Der Düsseldorfer Kreis koordiniert als Gremium der Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Arbeit der Aufsichtsbehörden im nicht öffentlichen Bereich. Den Vorsitz hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen. Die Beschlüsse des Düsseldorfer Kreises bezwecken eine möglichst einheitliche Anwendung der bundesrechtlichen Datenschutzvorschriften durch private Stellen. Sie sollen Rechtssicherheit für die Wirtschaft schaffen. Im Berichtszeitraum setzte sich das Gremium für eine transparentere Gestaltung der Einwilligungs- und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft ein und wies auf die Erforderlichkeit eines datenschutzgerechten Einsatzes der NFC-Funktion (Near Field Communication) von Geldkarten hin. Außerdem fassten die Aufsichtsbehörden Beschlüsse zur Videoüberwachung

⁹³ siehe D 6.1

in und an Taxis sowie zur Datenübermittlung in Staaten außerhalb des Europäischen Wirtschaftsraums.

Die Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie die Beschlüsse des Düsseldorfer Kreises sind als Anlage zu diesem Tätigkeitsbericht veröffentlicht.

4.2 Zusammenarbeit mit weiteren Stellen

Nach einer längeren Pause fand im Mai des Jahres 2013 wieder ein Kooperationsgespräch mit dem Ministerium des Innern statt. Die Landesbeauftragte hatte die Datenschutzaufsicht im Juni 2010 vom Ministerium übernommen. Es bestand also Anlass, zwischenzeitlich gewonnene Erfahrungen auszutauschen und aktuelle Entwicklungen – nicht zuletzt vor dem Hintergrund der laufenden Novellierung des europäischen Datenschutzrechts – zu erörtern. Die Landesbeauftragte und das Ministerium vereinbarten, solche Gespräche wieder regelmäßig zu führen.

Im Berichtszeitraum wurden zudem die Kooperationstreffen mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit fortgesetzt. Die räumliche Nähe sowie zahlreiche gemeinsame Einrichtungen der Länder Berlin und Brandenburg bringen auch für den Datenschutz und den Informationszugang umfangreiche Verflechtungen mit sich, die einer gegenseitigen Abstimmung bedürfen.

Im April des Jahres 2013 nahm die Landesbeauftragte als Gast an der Tagung der Datenschutzbeauftragten aus den Gliedkirchen der Evangelischen Kirche in Deutschland teil, um von ihrer Arbeit zu berichten. An einem Austausch der Rechtsauffassungen und Praxiserfahrungen besteht ein großes gemeinsames Interesse – nicht zuletzt deshalb, weil insbesondere Datenschutzfragen aus dem Gesundheitswesen für alle Beteiligten gleichermaßen relevant sind. Krankenhäuser haben schließlich unabhängig davon, ob sie in öffentlicher, privater oder kirchlicher Trägerschaft geführt werden, sehr ähnliche Anliegen.

5 Zusammenarbeit mit Informationsfreiheitsbeauftragten

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland tagt in der Regel zweimal jährlich und befasst sich mit den aktuellen Fragen der Informationsfreiheit. Im Berichtszeitraum trat sie insgesamt viermal zusammen.

Im Jahr 2012 führte der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, Edgar Wagner, den Vorsitz. In dieser Zeit forderte die Konferenz in einer EntschlieÙung, die Informationsfreiheit auf europäischer Ebene auszubauen. Anlass hierfür waren Bestrebungen der Mitgliedstaaten, das Zugangsrecht zu Akten der Institutionen der Europäischen Union deutlich einzuschränken. Außerdem sprachen sich die Beauftragten für mehr Transparenz bei der Wissenschaft aus. Insbesondere sollten Kooperationsverträge zwischen Wissenschaft und Unternehmen grundsätzlich offengelegt werden, um einer verborgenen Einflussnahme auf die Forschung zu begegnen. In einer weiteren EntschlieÙung ermutigte die Konferenz die Parlamente von Bund und Ländern, in eigener Sache Vorreiter in Sachen Transparenz zu werden. Die Gesetzgeber forderte sie zudem auf, für mehr Transparenz bei Krankenhaushygienedaten zu sorgen.

Unter dem Vorsitz des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit, Dr. Lutz Hasse, verabschiedete die Konferenz der Informationsfreiheitsbeauftragten im Jahr 2013 ein unter wesentlicher Mitwirkung der brandenburgischen Landesbeauftragten entstandenes Positionspapier zu Open Data. Die Konferenz hält eine Weiterentwicklung der bestehenden Informationsfreiheitsrechte um möglichst umfassende Veröffentlichungspflichten für unerlässlich. Mit dem Positionspapier unterstützt sie die begonnenen Open-Data-Projekte und empfiehlt den Gesetzgebern eine enge Verzahnung von Informationsfreiheit und Open Data. Vor dem Hintergrund verwaltungsgerichtlicher Entscheidungen, die eine Veröffentlichung von Hygieneverstößen im Internet für unzulässig erklärten, forderten die Informationsfreiheitsbeauftragten den Bundesgesetzgeber mit einer EntschlieÙung auf, die lebensmittelrechtlichen Vorschriften über die Information der Öffentlichkeit zu überarbeiten und eine rechtskonforme Gesamtkonzeption zu schaffen. In einer weiteren EntschlieÙung plädierten sie für einen effektiven presserechtlichen Auskunftsanspruch auch gegenüber Bundesbehörden. Anlass hierfür war ein Urteil des Bundesverwaltungsgerichts, nach welchem die Pressegesetze der Länder keine Verpflichtung von Bundesbehörden begründen.

Im Zusammenhang mit den Enthüllungen der umfassenden und anlasslosen Überwachungsmaßnahmen des amerikanischen und britischen Geheimdienstes verlangten die Informationsfreiheitsbeauftragten mehr Transparenz auf nationaler und internationaler Ebene auch von Nachrichtendiensten und Sicherheitsbehörden. Anlässlich des Beginns der 18. Legislaturperiode des Deutschen Bundestags forderte die Konferenz alle Beteiligten in Bund und in den Ländern auf, sich für die Stärkung der Transparenz auf nationaler, europäischer und internationaler Ebene einzusetzen. Sie plädierte unter anderem für ein Verfassungsrecht auf Informationsfreiheit, eine Zusammenführung der unterschiedlichen Anspruchsgrundlagen in einem einheitlichen Gesetz, die

Beschränkung von Ausnahmeregelungen, eine unabhängige Überprüfung der Klassifizierung von Verschlusssachen sowie die Anerkennung eines Menschenrechts auf Informationszugang im Rahmen der Vereinten Nationen.

6 Öffentlichkeitsarbeit

6.1 Veranstaltungen der Landesbeauftragten

Auf Initiative des Europarates wird in jedem Jahr am 28. Januar der Europäische Datenschutztag begangen. Die Datenschutzbeauftragten des Bundes und der Länder richten aus diesem Anlass stets eine zentrale Veranstaltung in Berlin aus. In ihrem Mittelpunkt standen im Jahr 2012 Vorträge und Diskussionen zur Vorratsdatenspeicherung. Vor dem Hintergrund der Anforderungen des Bundesverfassungsgerichts einerseits sowie der europarechtlichen Vorgaben andererseits wurde erörtert, ob eine gesetzliche Neuregelung zur Vorratsdatenspeicherung überhaupt datenschutzgerecht erfolgen kann. Im Folgejahr oblag der Landesbeauftragten als Vorsitzender der Datenschutzkonferenz 2012 die Organisation der zentralen Veranstaltung zum Europäischen Datenschutztag. Wieder stand ein aktuelles Thema auf der Tagesordnung: „Eine Datenschutz-Grundverordnung für Europa – internationale Perspektiven“. Mehrere hundert Interessierte aus Unternehmen, Verbänden und Verwaltungen erhielten durch Referate und eine Podiumsdiskussion einen Einblick in die Entwicklung dieses wohl wichtigsten Datenschutzvorhabens der laufenden Dekade.

Auf dem Brandenburg-Tag am 1. und 2. September 2012 in Lübbenau/Spreewald (Lubnjow/Blota) standen die Landesbeauftragte und ihre Mitarbeiter an einem rege besuchten Informationsstand Rede und Antwort. Vor dem Hintergrund der seinerzeit aktuellen Diskussion um das Bundesmeldegesetz betrafen viele Fragen den Datenschutz im Meldewesen. Auch Auskünfte zum Adresshandel und zur Verwendung personenbezogener Daten zu Werbezwecken waren stark nachgefragt. Großen Zuspruch fand ein Preisrätsel, mit dem die Landesbeauftragte anlässlich des 20jährigen Jubiläums der Verfassung des Landes Brandenburg auf die Grundrechte auf Datenschutz und Akteneinsicht aufmerksam machte. Ein Praxistext führte den Gästen am Stand zum wiederholten Male vor Augen, wie einfach es ist, schlechte Windows-Passwörter zu „knacken“. Außerdem wies die Landesbeauftragte mit einer Demonstration auf die Risiken des Einsatzes von RFID-Chips hin.

Am 27. Mai 2013 veranstaltete die Landesbeauftragte das achte Internationale Symposium in Potsdam. Unter der Leitfrage „Open Data – Ergänzung oder

Einschränkung der Informationsfreiheit?“ wurden die aktuellen europarechtlichen Entwicklungen auf diesem Gebiet vorgestellt. Die Teilnehmer versuchten, das Verhältnis zwischen Informationsfreiheit, Open Data und der Weiterverwendung von Informationen des öffentlichen Sektors zu klären. Experten aus Mittel- und Osteuropa boten Einblicke in ihre Erfahrungen. An ausgewählten Beispielen zeigten sie auf, welche Interessen und Erwartungen Staat, Zivilgesellschaft und Wirtschaft einbringen und diskutierten unterschiedliche Open-Data-Ansätze. Vor dem Hintergrund der Einführung von Open Data in der Bundesrepublik Deutschland und der Debatte um die Novellierung des Informationsfreiheitsrechts in Brandenburg bot die Veranstaltung zahlreiche Anregungen für die Praxis. Das Internationale Symposium wurde gemeinsam mit der Alcatel-Lucent Stiftung für Kommunikationsforschung und der Deutschen Gesellschaft für Recht und Informatik organisiert. Die Beiträge der Referenten sind in einer Dokumentation veröffentlicht. Diese ist in gedruckter Form erhältlich, aber auch – ebenso wie die Audio-Mitschnitte der Vorträge – auf der Website der Landesbeauftragten veröffentlicht.

Eine Delegation der Provinzregierung von Guangxi (Volksrepublik China) war im September 2012 bei der Landesbeauftragten zu Gast, um sich über die Praxis der Informationsfreiheit in Brandenburg zu informieren. Zunächst standen die Grundzüge der Akteneinsicht und die Besonderheit des Artikels 21 der Verfassung des Landes Brandenburg im Fokus der Veranstaltung. Die fünfzehn Mitglieder der Delegation interessierten sich aber auch für die Schwierigkeiten bei der Umsetzung des Akteneinsichts- und Informationszugangsgesetzes und für die Möglichkeiten zur Schaffung einer transparenten Verwaltung durch Open Data. Guangxi ist ein autonomes Gebiet im Süden Chinas mit etwa 50 Millionen Einwohnern. Die Volksrepublik sieht sich vor der Aufgabe, die zunehmenden Probleme der Korruption staatlicher Einrichtungen zielgerichtet anzugehen.

6.2 Fortbildungsangebote

Der Bedarf an Fortbildung in den Bereichen Datenschutz und IT-Sicherheit sowie Akteneinsicht und Informationsfreiheit ist nach wie vor sehr hoch. Immer wieder stellen wir im Rahmen von Beratungen oder bei Kontrollen vor Ort fest, dass Verantwortliche in Verwaltungen oder Unternehmen die gesetzlichen Vorschriften nur unzureichend kennen oder bei ihrer Auslegung und Anwendung unsicher sind. Darüber hinaus werden wir – insbesondere durch Beschwerden von Bürgern, Beschäftigten oder Kunden – häufig auf Mängel hingewiesen, deren Ursache eine fehlende oder nur ungenügende Sensibilisierung der Beschäftigten für Belange des Datenschutzes bzw. der Informationsfreiheit sind.

Oft erreichen uns Anfragen, in Fortbildungsveranstaltungen oder bei Vorträgen neben den rechtlichen und technischen Grundlagen des Datenschutzes und der Informationsfreiheit auch aktuelle Entwicklungen auf diesen Gebieten zu diskutieren. So werden wir z. B. um Schulungen zu speziellen Themen wie der Nutzung sozialer Netze, Datenschutz beim Cloud Computing oder Open Data gebeten. Auf technischem Gebiet haben gerade die Enthüllungen über die Praktiken ausländischer Nachrichtendienste zur Überwachung der Kommunikation zu einer erhöhten Nachfrage nach Unterrichtungen zum Selbstschutz geführt. Wegen unserer begrenzten personellen und zeitlichen Ressourcen gelang es nicht immer, allen Wünschen gerecht zu werden.

Vor diesem Hintergrund führten Mitarbeiter unserer Dienststelle wie auch in den voran gegangenen Jahren im Berichtszeitraum zahlreiche Fortbildungen in der Landes- und Kommunalverwaltung durch. Darüber hinaus hielten sie Vorträge auf diversen Veranstaltungen. Zu den behandelten Themen gehörten u. a.

- im Bereich „Datenschutzrecht“: Allgemeine Grundlagen des Datenschutzes und der Datensicherheit (jeweils mehrfach für unterschiedliche Zielgruppen), Datenschutz in der Justiz für Richter und Staatsanwälte (gemeinsame Veranstaltung mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit), Fragen des Datenschutzes und der ärztlichen Schweigepflicht für Mitarbeiter in Krankenhäusern, Datenschutz und Persönlichkeitsrechte im Internet, Urheberrecht, Facebook: Privatsphäre und Selbstdarstellung im Netz, Suchmaschinen als Datenaggregator,
- im Bereich „Technischer Datenschutz und Informationssicherheit“: Grundlagen bzw. Weiterführende Aspekte des technischen und organisatorischen Datenschutzes, Kriminalität im Internet, Technische Risiken, Angriffsszenarien und Sicherheitsmaßnahmen im Internet, Datenschutzgerechtes Cloud Computing, Mobile Endgeräte und Bring Your Own Device,
- im Bereich „Akteneinsicht und Informationsfreiheit“: Akteneinsicht und Informationsfreiheit im Bauamt, im Umweltamt und im Amt für Landwirtschaft.

Darüber hinaus stellten wir im Rahmen von Lehrveranstaltungen an der Fachhochschule Brandenburg die Tätigkeit unserer Behörde für Studenten der Studiengänge Betriebswirtschaftslehre (Bachelor), Wirtschaftsinformatik (Bachelor) sowie Security Management (Master) vor.

Einer der Veranstalter, mit denen wir bei der Fortbildung von Mitarbeitern der Landesverwaltung eng zusammenarbeiten, ist der Brandenburgische IT-

Dienstleister. Im Rahmen einer Schulung zum technischen und organisatorischen Datenschutz im Jahr 2013 wurde von den Teilnehmern der Wunsch geäußert, zusätzliche und vertiefende Informationen zu ausgewählten Fragen zu erhalten. Die Diskussion dieses Anliegens mit dem Dienstleister führte zu einer inhaltlichen Neukonzeption unserer Fortbildungsveranstaltungen zum technischen und organisatorischen Datenschutz und zu dem Angebot für ein entsprechendes Aufbauseminar. Dieses wird 2014 erstmalig stattfinden. Wir hoffen auf viele Teilnehmer und interessante Diskussionen.

6.3 Neue Publikationen der Landesbeauftragten

Die Landesbeauftragte hat ihre Broschüre mit dem Text des Brandenburgischen Datenschutzgesetzes (Stand 2010) wegen der stetigen hohen Nachfrage in unveränderter Form nachdrucken lassen. Komplett zu überarbeiten war der Band zum Verbraucherinformationsrecht, der nunmehr in zweiter Auflage vorliegt. Alle darin aufgeführten Regelungen waren im Berichtszeitraum wesentlich geändert worden. Ähnliches gilt für das Akteneinsichts- und Informationszugangsgesetz, welches im September 2013 novelliert wurde. Der aktuelle Gesetzestext wurde noch zum Ende des Berichtszeitraums in siebenter Auflage als Broschüre herausgegeben.

Im November 2012 wurden die überarbeiteten Anwendungshinweise der Landesbeauftragten zum Akteneinsichts- und Informationszugangsgesetz veröffentlicht. Gerade von Städten, Gemeinden, Ämtern und Landkreisen wird diese Broschüre sehr häufig angefordert. Die Hinweise konnten in der Kürze der zur Verfügung stehenden Zeit jedoch noch nicht an das novellierte Gesetz angepasst werden. Es handelt sich nicht um einen Kommentar zum Gesetz, sondern um eine Zusammenstellung der in der Praxis von der Landesbeauftragten vertretenen Rechtsauffassung zu den einzelnen Regelungen des Akteneinsichts- und Informationszugangsgesetzes. Die Fortschreibung der Broschüre wird unter Berücksichtigung der Gesetzesänderungen auch weiterhin erfolgen.

Im Nachgang zum Internationalen Symposium „Open Data – Ergänzung oder Einschränkung der Informationsfreiheit?“ am 27. Mai 2013 gab die Landesbeauftragte eine Dokumentation der Tagungsbeiträge heraus. Sie ist als achter Band in der Reihe „Potsdamer Materialien zu Akteneinsicht und Informationszugang“ erschienen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, deren Mitglied die brandenburgische Landesbeauftragte ist, hat im Berichtszeitraum verschiedene Orientierungshilfen herausgegeben, um die praktische Umsetzung des Datenschutzes zu erleichtern.

Die Orientierungshilfe „Smart Metering“ enthält Empfehlungen zur datenschutzgerechten Konzeption von technischen Systemen für das Smart Metering. Ihr Kernstück ist die Beschreibung und datenschutzrechtliche Bewertung konkreter Anwendungsfälle. Mit ihrer Orientierungshilfe „Datenschutz bei IPv6 – Hinweise für Hersteller und Provider im Privatkundengeschäft“ informiert die Konferenz über die Anforderungen zur Anpassung der Netzwerke an die neue Version des Internet-Protokolls. Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur sind Inhalt der Orientierungshilfe „Mandantenfähigkeit“.

Angesichts der nur unzureichend funktionierenden Selbstregulierung der Netzbetreiber haben die Datenschutzbeauftragten die Orientierungshilfe „Soziale Netzwerke“ erarbeitet. Sie soll die Betreiber sozialer Netzwerke sowie öffentliche und private Stellen bei der datenschutzgerechten Gestaltung und Nutzung der Angebote unterstützen.

Die Handreichung „Datenschutzrechtliche Leitlinien mit Mindestanforderungen für die Ausgestaltung und den Betrieb von Arztbewertungsportalen im Internet“ fasst die aus Sicht der Datenschutzaufsicht zu beachtenden Mindestvoraussetzungen für eine datenschutzgerechte Errichtung und den Betrieb derartiger Bewertungsportale zusammen.

Der Düsseldorfer Kreis als Gremium der Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich hat Anwendungshinweise zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten für werbliche Zwecke erarbeitet. Diese Hinweise sowie sämtliche Orientierungshilfen stehen auf der Website der Landesbeauftragten zum Herunterladen zur Verfügung.

6.4 Neues Internetangebot

Das bestehende Internetangebot der Landesbeauftragten wurde im Sommer des Jahres 2012 aufgeräumt, übersichtlicher strukturiert und mit neuer Farbe versehen:

www.lida.brandenburg.de

Im Mittelpunkt der Neugestaltung stand der für den Nutzer unsichtbare Einsatz eines vom Brandenburgischen IT-Dienstleister zur Verfügung gestellten Content Management Systems. Dieses reduziert den Aufwand der Erstellung, Bearbeitung und Veröffentlichung von Inhalten erheblich. Beispielsweise entfällt das Erfordernis, einzelne Webseiten durch spezielle Textauszeichnungen zu formatieren. Wesentliche Einstellungen müssen nun nicht mehr in

jedem einzelnen Dokument, sondern können übergreifend für das gesamte Internetangebot vorgenommen werden. Weitere Gründe für die Überarbeitung waren Kosten- und Zeitersparnisse bei Administration und Konfiguration sowie eine Vereinheitlichung der Struktur von Inhalten auf der Bearbeitungs- und Darstellungsebene.

Die Tätigkeitsberichte und Presseinformationen der Landesbeauftragten werden ebenso wie Informationsmaterial und Gesetzestexte mit wenigen Klicks erreicht. Wer sich intensiver informieren möchte, findet unter den Rubriken „Datenschutz“ und „Akteneinsicht“ weitergehende Informationen über die Grundlagen und Zuständigkeiten, die rechtlichen und technischen Aspekte des jeweiligen Aufgabengebiets sowie die Entschlüsse der Konferenzen der Datenschutzbeauftragten bzw. Informationsfreiheitsbeauftragten. Neu ist der sog. Ariadnefaden, der den Benutzer darüber informiert, an welcher Stelle innerhalb des verzweigten Internetangebots er sich gerade befindet und somit eine schnellere Navigation ermöglicht. Selbstverständlich steht auch eine Suchfunktion zur Verfügung.

Seit dem Herbst des Jahres 2013 ist im Internetangebot der Landesbeauftragten darüber hinaus eine Zusammenstellung wichtiger Gerichtsentscheidungen zur Informationsfreiheit verfügbar. Die öffentlich und kostenfrei zugängliche Rechtsprechungsdatenbank ist ein gemeinsames Projekt der Landesbeauftragten und der Deutschen Gesellschaft für Informationsfreiheit e. V. Sie soll den Bürgerinnen und Bürgern dabei helfen, ihr Recht auf Informationszugang effektiv wahrzunehmen. Der Überblick über die inzwischen sehr umfangreiche Rechtsprechung zur Informationsfreiheit soll außerdem Verwaltungen und Gerichte bei ihrer täglichen Arbeit unterstützen. Das noch im Aufbau befindliche Projekt umfasst inzwischen etwa 500 Gerichtsentscheidungen und wird ständig ergänzt.

Anregungen zum neuen Internetangebot sowie Hinweise auf noch nicht berücksichtigte Gerichtsentscheidungen zur Informationsfreiheit sind jederzeit willkommen.

Anlagen

1 EntschlieÙungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

1.1 86. Konferenz am 1./2. Oktober 2013 in Bremen

1.1.1 Forderungen für die neue Legislaturperiode: Die Datenschutzgrundrechte stärken!

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

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

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

- Im besonders eingriffsintensiven Bereich der öffentlichen Sicherheit müssen wirksame Schranken für Grundrechtseingriffe dem Grundsatz der Verhältnismäßigkeit, dem informationellen Trennungsprinzip und dem Schutz des Kernbereichs privater Lebensgestaltung Rechnung tragen. Wichtig ist eine umfassende Kontrolle der Sicherheitsbehörden. Die Bundesregierung muss sich auch auf europäischer und internationaler Ebene für den wirksamen Schutz der Grundrechte einsetzen. Dies gilt insbesondere für die Verhinderung von umfassender und anlassloser Überwachung durch Nachrichtendienste.¹

¹ Siehe dazu die EntschlieÙungen „Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen“ und „Handlungsbedarf zum Datenschutz im Bereich der öffentlichen Sicherheit in der 18. Legislaturperiode des Deutschen Bundestags“.

- Angesichts der mit dem zunehmenden Wettbewerb im Sozial- und Gesundheitswesen verbundenen Risiken für die informationelle Selbstbestimmung müssen die Schutzrechte für die Privat- und Intimsphäre von Patientinnen, Patienten und Versicherten gestärkt werden.²
- Die Vertraulichkeit und Integrität elektronischer Kommunikation sind zu fördern. Der öffentliche Bereich muss hier mit gutem Beispiel vorangehen und die Ende-zu-Ende-Verschlüsselung z. B. mit Hilfe von OSCI-Transport flächendeckend einsetzen.³

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

1.1.2 Handlungsbedarf zum Datenschutz im Bereich der Öffentlichen Sicherheit in der 18. Legislaturperiode des Deutschen Bundestages

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

Die internationalen Überwachungsaktivitäten von Nachrichtendiensten machen dies deutlich. Die Bundesrepublik Deutschland ist verpflichtet, sich dagegen zu wenden und auf europäischer und internationaler Ebene dafür einzusetzen, dass es keine umfassende Überwachung gibt. Hierzu hat die Konferenz bereits die EntschlieÙung „Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen“ verabschiedet. Die Konferenz erwartet von der Bundesregierung außerdem, dass sie

² Siehe dazu die heutige EntschlieÙung „Stärkung des Datenschutzes im Sozial- und Gesundheitswesen“.

³ Siehe dazu die heutige EntschlieÙung „Sichere elektronische Kommunikation gewährleisten – Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln“.

sich für die Aufhebung der EU-Richtlinie zur anlasslosen Vorratsdatenspeicherung von Telekommunikationsdaten einsetzt.

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

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

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

1.1.3 Stärkung des Datenschutzes im Sozial- und Gesundheitswesen

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

Vor dem Hintergrund des sich verschärfenden Wettbewerbs der Beteiligten im Sozial- und Gesundheitswesen geraten die Rechte der Patientinnen und Patienten und Versicherten immer stärker unter Druck. Dies zeigt sich zum Beispiel darin, dass eine Reihe von Krankenkassen und andere Sozialleis-

tungsträger im Rahmen der Informationsbeschaffung die Empfänger von gesetzlichen Leistungen (zum Beispiel Krankengeld) über ihren Gesundheitszustand über das erforderliche Maß hinaus befragen und dabei gesetzlich vorgesehene Verfahren wie zum Beispiel die Einschaltung des Medizinischen Dienstes der Krankenversicherung umgehen.

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

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

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

- Bei der Nutzung neuer technischer Möglichkeiten muss das Recht auf informationelle Selbstbestimmung als unverzichtbares Grundrecht von vornherein berücksichtigt werden (privacy by design). Die Entwicklung datenschutzfreundlicher Technologien, zum Beispiel von Anonymisierungs-, Pseudonymisierungs- und Verschlüsselungsverfahren, sollte gefördert und deren Einsatz nach dem aktuellen Stand der Technik gesetzlich abgesichert werden.
- Die Telematikinfrastruktur ist umgehend und funktionsfähig so zu realisieren, dass die medizinische Kommunikation zwischen den Beteiligten im Gesundheitsbereich vertraulich und zuverlässig realisiert wird und die Patientinnen und Patienten praktisch in die Lage versetzt werden, ihr Recht auf informationelle Selbstbestimmung wahrzunehmen.
- Für die zunehmende Einschaltung technischer Dienstleister durch Leistungserbringer, insbesondere niedergelassene Ärztinnen und Ärzte, müssen angemessene datenschutzgerechte gesetzliche Regelungen verabschiedet werden.

1.1.4 Sichere elektronische Kommunikation gewährleisten – Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln

Die elektronische Datenübermittlung zwischen den Bürgern beziehungsweise der Wirtschaft und der öffentlichen Verwaltung im Zusammenhang mit E-Government-Verfahren erfordert insbesondere auch mit Blick auf die umfassenden und anlasslosen Überwachungsmaßnahmen ausländischer Geheimdienste technische und organisatorische Maßnahmen, um den Anforderungen an Datenschutz und Datensicherheit gerecht zu werden. Zur Sicherung der Vertraulichkeit, Integrität, Authentizität, Zweckbindung und Transparenz bei der Datenübertragung sind kryptographische Verfahren erforderlich. Diese Verfahren können sowohl die Verbindungen zwischen den Endpunkten der Übertragung (Ende-zu-Ende-Verschlüsselung) als auch die Verbindungen zwischen den an der Übertragung beteiligten Netzknoten (Verbindungsverschlüsselung) sichern.

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

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

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

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

Sendungen kann mittels Quittungen bestätigt werden. Schließlich ist das Anbringen elektronischer Signaturen nach dem Signaturgesetz möglich.

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

1.2 Entschließung zwischen der 85. und 86. Konferenz vom 5. September 2013

Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen

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

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

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

Die staatliche Pflicht zum Schutz der Grundrechte erfordert es, sich nicht mit der gegenwärtigen Situation abzufinden. Die Regierungen und Parlamente des Bundes und der Länder sind dazu aufgerufen, das ihnen im Rahmen ihrer Zuständigkeiten Mögliche zu tun, um die Einhaltung des deutschen und des europäischen Rechts zu gewährleisten. Das Bundesverfassungsgericht hat festgestellt, dass es „zur verfassungsrechtlichen Identität der Bundesre-

publik Deutschland gehört, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss“, „dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf“. Es müssen daher alle Maßnahmen getroffen werden, die den Schutz der informationellen Selbstbestimmung der in Deutschland lebenden Menschen und ihr Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme für die Zukunft sicherstellen.

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

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

- Nationales, europäisches und internationales Recht so weiterzuentwickeln und umzusetzen, dass es einen umfassenden Schutz der Privatsphäre, der informationellen Selbstbestimmung, des Fernmeldegeheimnisses und des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme garantiert.
- Sofern verfassungswidrige nachrichtendienstliche Kooperationen erfolgen, müssen diese abgestellt und unterbunden werden.
- Die Kontrolle der Nachrichtendienste muss durch eine Erweiterung der Befugnisse sowie eine gesetzlich festgelegte verbesserte Ausstattung der parlamentarischen Kontrollgremien intensiviert werden. Bestehende Kontrolllücken müssen unverzüglich geschlossen werden. In diesem Zusammenhang ist zu prüfen, ob die Datenschutzbeauftragten verstärkt in die Kontrolle der Nachrichtendienste eingebunden werden können.
- Es sind Initiativen zu ergreifen, die die informationelle Selbstbestimmung und das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme sicherstellen.

Dazu gehört,

- zu prüfen, ob das Routing von Telekommunikationsverbindungen in Zukunft möglichst nur über Netze innerhalb der EU erfolgen kann.
- sichere und anonyme Nutzungsmöglichkeiten von Telekommunikationsangeboten aller Art auszubauen und zu fördern. Dabei ist sicherzustellen, dass den Betroffenen keine Nachteile entstehen, wenn sie

die ihnen zustehenden Rechte der Verschlüsselung und Nutzung von Anonymisierungsdiensten ausüben.

- die Voraussetzungen für eine objektive Prüfung von Hard- und Software durch unabhängige Zertifizierungsstellen zu schaffen.
- Völkerrechtliche Abkommen wie das Datenschutz-Rahmenabkommen und das Freihandelsabkommen zwischen der EU und den USA dürfen nur abgeschlossen werden, wenn die europäischen Datenschutzgrundrechte ausreichend geschützt werden. Das bedeutet auch, dass jeder Mensch das Recht hat, bei vermutetem Datenmissbrauch den Rechtsweg zu beschreiten. Das Fluggastdatenabkommen und das Überwachungsprogramm des Zahlungsverkehrs müssen auf den Prüfstand gestellt werden.
- Auch innerhalb der Europäischen Union ist sicherzustellen, dass die nachrichtendienstliche Überwachung durch einzelne Mitgliedstaaten nur unter Beachtung grundrechtlicher Mindeststandards erfolgt, die dem Schutzniveau des Art. 8 der Charta der Grundrechte der Europäischen Union entsprechen.

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

1.3 85. Konferenz am 13./14. März 2013 in Bremerhaven

1.3.1 Europa muss den Datenschutz stärken!

Das Europäische Parlament und der Rat der Europäischen Union bereiten derzeit ihre Änderungsvorschläge für den von der Europäischen Kommission vor einem Jahr vorgelegten Entwurf einer Datenschutz-Grundverordnung für Europa vor. Aktuelle Diskussionen und Äußerungen aus dem Europäischen Parlament und dem Rat lassen die Absenkung des derzeitigen Datenschutzniveaus der Europäischen Datenschutzrichtlinie von 1995 befürchten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erinnert alle Beteiligten des Gesetzgebungsverfahrens daran, dass das Europäische Parlament in seiner Entschließung vom 6. Juli 2011 zum damaligen Gesamtkonzept für Datenschutz in der Europäischen Union (2011/2025(INI)) sich unter Hinweis auf die Charta der Grundrechte der Europäischen Union und insbesondere auf Artikel 7 und 8 der Charta einhellig dafür ausgespro-

chen hat, die Grundsätze und Standards der Richtlinie 95/46/EG zu einem modernen Datenschutzrecht weiterzuentwickeln, zu erweitern und zu stärken. Das Europäische Parlament hat eine volle Harmonisierung des Datenschutzrechts auf höchstem Niveau gefordert.

Die Datenschutzbeauftragten von Bund und Ländern setzen sich dafür ein, dass die wesentlichen Grundpfeiler des Datenschutzes erhalten und ausgebaut werden. Sie wenden sich entschieden gegen Bestrebungen, den Datenschutz zu schwächen. Insbesondere fordern sie:

- Jedes personenbeziehbare Datum muss geschützt werden: Das europäische Datenschutzrecht muss unterschiedslos alle Daten erfassen, die einer natürlichen Person zugeordnet werden können. Dies schließt auch pseudonyme Daten oder Identifizierungsmerkmale wie beispielsweise IP-Adressen ein.
- Es darf keine grundrechtsfreien Räume geben: Die generelle Herausnahme von bestimmten Datenkategorien und Berufs- und Unternehmensgruppen ist daher abzulehnen.
- Einwilligungen müssen ausdrücklich erteilt werden: Einwilligungen in die Verarbeitung personenbezogener Daten dürfen nur dann rechtswirksam sein, wenn sie auf einer eindeutigen, freiwilligen und informierten Willensbekundung der Betroffenen beruhen. Auch deshalb muss eine gesetzliche Pflicht geschaffen werden, die Kompetenz zum Selbstschutz zu fördern.
- Datenverarbeiter dürfen ihre Ziele nicht eigenmächtig verändern: Die Zweckbindung als zentraler Baustein zur Gewährleistung der Transparenz und Vorhersehbarkeit der Datenverarbeitung muss ohne Abstriche erhalten bleiben.
- Profilbildung muss beschränkt werden: Für die Zusammenführung und Auswertung vieler Daten über eine Person müssen enge Grenzen gelten.
- Stärkung der Eigenverantwortung der Datenverarbeiter durch betriebliche Datenschutzbeauftragte: Betriebliche Datenschutzbeauftragte sollten europaweit eingeführt, obligatorisch bestellt und in ihrer Stellung gestärkt werden. Sie sind ein wesentlicher Bestandteil der Gesamtstruktur einer effektiven Datenschutzkontrolle.
- Datenverarbeiter dürfen sich ihre Aufsichtsbehörde nicht aussuchen können: Es ist auszuschließen, dass sich Datenverarbeiter ihre Aufsichtsbehörde durch die Festlegung ihrer Hauptniederlassung aussuchen. Ne-

ben der federführenden Aufsichtsbehörde des Hauptsitzlandes müssen auch die anderen jeweils örtlich zuständigen Kontrollbehörden inhaltlich beteiligt werden.

- Völlige Unabhängigkeit der Aufsichtsbehörden auch gegenüber der Kommission: Die Datenschutz-Aufsichtsbehörden müssen unabhängig und verbindlich über die Einhaltung des Datenschutzes entscheiden. Ein Letztentscheidungsrecht der Kommission verletzt die Unabhängigkeit der Aufsichtsbehörden und des künftigen Europäischen Datenschutzausschusses.
- Grundrechtsschutz braucht effektive Kontrollen: Um die datenschutzrechtliche Kontrolle in Europa zu stärken, müssen die Aufsichtsbehörden mit wirksamen und flexiblen Durchsetzungsbefugnissen ausgestattet werden. Die Sanktionen müssen effektiv und geeignet sein, damit die Verantwortlichen und Datenverarbeiter die Datenschutzvorschriften nachhaltig beachten. Ohne spürbare Bußgelddrohungen bleibt die Datenschutzkontrolle gegen Unternehmen zahnlos.
- Hoher Datenschutzstandard für ganz Europa: Soweit etwa im Hinblick auf die Sensitivität der Daten oder sonstige Umstände ein über die Datenschutz-Grundverordnung hinausgehender Schutz durch nationale Gesetzgebung erforderlich ist, muss dies möglich bleiben. Jedenfalls hinsichtlich der Datenverarbeitung durch die öffentliche Verwaltung müssen die Mitgliedstaaten auch zukünftig strengere Regelungen und damit ein höheres Datenschutzniveau in ihrem nationalen Recht vorsehen können.

1.3.2 Pseudonymisierung von Krebsregisterdaten verbessern!

In allen Ländern werden Daten über individuelle Fälle von Krebserkrankungen in Krebsregistern gespeichert, um sie der epidemiologischen Forschung zur Verfügung zu stellen. Zum Schutz der Betroffenen werden die Daten in allen Ländern (außer Hamburg) mit Kontrollnummern nach § 4 Bundeskrebsregisterdatengesetz (BKRG) pseudonymisiert gespeichert. Als Pseudonyme werden so genannte Kontrollnummern verwendet. Kontrollnummern werden darüber hinaus von allen Ländern zum Abgleich der Daten der epidemiologischen Krebsregister untereinander und mit dem Zentrum für Krebsregisterdaten nach § 4 BKRG verwendet.

Die Datenschutzbeauftragten von Bund und Ländern sind der Auffassung, dass das vor ca. 20 Jahren entwickelte Verfahren zur Bildung der Kontrollnummer den erforderlichen Schutz dieser höchst sensiblen Daten nicht mehr in ausreichendem Maße gewährleisten kann. Dies ist auf die folgenden Entwicklungen zurückzuführen:

- Das Anwachsen der für eine Depseudonymisierung verfügbaren Rechenkapazität hat die Schutzwirkung der bei den Krebsregistern genutzten kryptographischen Hashfunktion aufgehoben, die derzeit als erste Komponente bei der Kontrollnummernbildung verwendet wird.
- Die Wechselwirkungen zwischen mehreren Verfahren im Umfeld der epidemiologischen Krebsregistrierung verursachen Risiken im Zuge der erforderlichen Entschlüsselungen und der gemeinsamen Verwendung von geheimen Schlüsseln, die bisher nicht berücksichtigt wurden.

Diese Entwicklungen machen es erforderlich, die Regeln zur Bildung der Kontrollnummern zu überarbeiten. Hierbei ist das Umfeld aller Verfahren in Betracht zu ziehen, in dem Kontrollnummern zum Einsatz kommen beziehungsweise absehbar kommen sollen. Hierzu hat der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Datenschutzkonferenz einen entsprechenden Anforderungskatalog formuliert (siehe Anlage zu dieser EntschlieÙung).

Die Datenschutzkonferenz fordert die zuständigen Fachaufsichtsbehörden der Länder auf, für eine koordinierte Umstellung des Verfahrens bei den ihrer Aufsicht unterstehenden Stellen zu sorgen, die Kontrollnummern bilden oder verwenden. Sie empfiehlt den Ländern, für den Datenaustausch klinischer Krebsregister mit den Auswertungsstellen der klinischen Krebsregistrierung auf Landesebene nach dem Krebsfrüherkennungs- und -registergesetz ein Pseudonymisierungsverfahren anzuwenden, das im Wesentlichen den gleichen Anforderungen genügt.

Die entsprechenden Vorgaben für den Datenabgleich nach § 4 BKRG sollten durch das Bundesministerium für Gesundheit in einer Verordnung nach § 4 Absatz 3 BKRG festgelegt werden.

1.3.3 Soziale Netzwerke brauchen Leitplanken – Datenschutzbeauftragte legen Orientierungshilfe vor

Angesichts der zunehmenden Bedeutung sozialer Netzwerke erinnert die Datenschutzkonferenz deren Betreiber an ihre Verpflichtung, die Einhaltung datenschutzrechtlicher Anforderungen sicherzustellen. Auch Unternehmen und öffentliche Stellen, die soziale Netzwerke nutzen, müssen diesen Anforderungen Rechnung tragen. Die Erfahrung der Aufsichtsbehörden zeigt, dass der Schutz der Privatsphäre von den Betreibern sozialer Netzwerke nicht immer hinreichend beachtet wird.

Häufig vertrauen die Nutzenden den Betreibern dieser Dienste sehr persönliche Informationen an. Auch die Vielfalt der Informationen, die innerhalb eines

Netzwerkes aktiv eingestellt oder über die Nutzerinnen und Nutzer erhoben werden, ermöglicht einen tiefen Einblick in deren persönliche Lebensgestaltung.

Es zeichnet sich ab, dass die angekündigte Selbstregulierung für soziale Netzwerke – insbesondere auf Grund der mangelnden Bereitschaft einiger großer Netzwerk-Betreiber – den erforderlichen Datenschutzstandard nicht gewährleisten kann. Deshalb haben die Datenschutzbeauftragten des Bundes und der Länder die Orientierungshilfe „Soziale Netzwerke“ erarbeitet. Sie soll die Betreiber sozialer Netzwerke und die die Netzwerke nutzenden öffentlichen und privaten Stellen bei der datenschutzgerechten Gestaltung und Nutzung der Angebote unterstützen. Die Konferenz weist darauf hin, dass der vorhandene Rechtsrahmen zur Gewährleistung eines angemessenen Datenschutzes bei sozialen Netzwerken weiterentwickelt werden muss, insbesondere in Bezug auf konkrete und präzise Vorgaben zu datenschutzfreundlichen Voreinstellungen, zum Minderjährigenschutz, zur Löschungsverpflichtung bei Dritten und zum Verhältnis von Meinungsfreiheit und Persönlichkeitsrecht. Ferner wird die Verantwortlichkeit für den Umgang mit Nutzungsdaten in Bezug auf Social Plug-Ins, Fanpages sowie für den Einsatz von Cookies von vielen Unternehmen und Behörden in Abrede gestellt. Der europäische und nationale Gesetzgeber bleiben aufgefordert, für die notwendige Klarheit zu sorgen und damit einen ausreichenden Datenschutzstandard zu sichern. Darauf weist die Konferenz der Datenschutzbeauftragten erneut nachdrücklich hin.

1.3.4 Datenschutz auch in einer transatlantischen Freihandelszone gewährleisten!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist auf die Notwendigkeit hin, bei den angekündigten Verhandlungen zwischen der Europäischen Union und der Regierung der Vereinigten Staaten über eine transatlantische Freihandelszone auch die unterschiedlichen datenschutzrechtlichen Rahmenbedingungen zu thematisieren. Dabei muss sichergestellt werden, dass das durch die Europäische Grundrechtecharta verbrieft Grundrecht auf Datenschutz und die daraus abgeleiteten Standards gewahrt bleiben.

Von der Kommission erwartet die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass sie bei den Verhandlungen das Ziel einer grundrechtsorientierten Wertegemeinschaft nicht aus dem Auge verliert. Keineswegs dürfen durch die angestrebte transatlantische Wirtschaftsunion europäische Grundrechtsgewährleistungen abgeschwächt werden. Auch wäre es nicht hinzunehmen, wenn sich die Verhandlungen negativ auf den

durch die Europäische Kommission angestoßenen Reformprozess des EU-Datenschutzrechts auswirken würden.

Die Konferenz sieht in der vom US-Präsidenten vorgeschlagenen Freihandelszone die Chance, international eine Erhöhung des Datenschutzniveaus zu bewirken. Sie begrüßt daher die vom US-Präsidenten angekündigte Initiative für verbindliche Vorgaben zum Datenschutz in der Wirtschaft. Sie erinnert daran, dass nach den Vorgaben der Welthandelsorganisation der Datenschutz kein Handelshindernis darstellt.

1.4 EntschlieÙung zwischen der 84. und 85. Konferenz vom 25. Januar 2013

Beschäftigtendatenschutz nicht abbauen, sondern stärken!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erinnert an ihre EntschlieÙung vom 16./17. März 2011 und ihre Forderung nach speziellen Regelungen zum Beschäftigtendatenschutz. Bei einer Gesamtbetrachtung ist die Konferenz enttäuscht von dem jetzt veröffentlichten Änderungsentwurf der Koalitionsfraktionen.

Bereits der ursprünglich von der Bundesregierung vorgelegte Entwurf enthielt aus Datenschutzsicht erhebliche Mängel. Der nun vorgelegte Änderungsentwurf nimmt zwar einzelne Forderungen – etwa zum Konzerndatenschutz – auf und stärkt das informationelle Selbstbestimmungsrecht auch gegenüber Tarifverträgen und Betriebsvereinbarungen. Das Datenschutzniveau für die Beschäftigten soll jedoch in einigen wesentlichen Bereichen sogar noch weiter abgesenkt werden.

Besonders bedenklich sind die folgenden Regelungsvorschläge:

- Die Möglichkeiten der offenen Videoüberwachung am Arbeitsplatz sollen noch über das bisher Geplante hinaus ausgeweitet werden. Überdies ist die Beschreibung der zuzulassenden Überwachungszwecke unverständlich und würde deshalb nicht zur Rechtssicherheit beitragen.
- Beschäftigte in Call-Centern sollen noch stärker überwacht werden können, als dies der Regierungsentwurf ohnehin schon vorsah. Die Beschäftigten müssen sich nunmehr auf eine jederzeit mögliche, unbemerkte Überwachung einstellen. Hierdurch kann ein unzumutbarer Überwachungsdruck entstehen.
- Die Datenerhebungsbefugnisse im Bewerbungsverfahren sollen erweitert werden. Der noch im Regierungsentwurf vorgesehene Ausschluss von

Arbeitgeberrecherchen über Bewerberinnen und Bewerber in sozialen Netzwerken außerhalb spezieller Bewerbungsportale wurde gestrichen. Damit wird der Grundsatz der Direkterhebung bei den Betroffenen weiter unterlaufen.

- Dem Arbeitgeber soll es gestattet sein, auch nicht allgemein zugängliche Beschäftigtendaten bei Dritten zu erheben, wenn die Beschäftigten eingewilligt haben. Die tatsächliche Freiwilligkeit einer solchen Einwilligung ist fraglich.
- Die im Regierungsentwurf enthaltene Vorgabe, Eignungstests grundsätzlich nach wissenschaftlich anerkannten Methoden durchzuführen, soll wieder entfallen.

Die Konferenz appelliert an den Bundestag, bei seinen Beratungen zum Gesetz den Forderungen der Datenschutzbeauftragten Rechnung zu tragen.

1.5 84. Konferenz am 7./8. November 2012 in Frankfurt (Oder)

1.5.1 Europäische Datenschutzreform konstruktiv und zügig voranbringen!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht der Europäischen Kommission, den Datenschutz in Europa auf hohem Niveau zu harmonisieren. Sie hat dies bereits in ihrer Entschließung vom 21./22. März 2012 verdeutlicht. In zwei umfassenden Stellungnahmen vom 11. Juni 2012 haben die Datenschutzbeauftragten des Bundes und der Länder eine Vielzahl einzelner Aspekte der Datenschutzreform bewertet und Empfehlungen für den weiteren Rechtssetzungsprozess gegeben.

Angesichts der aktuellen Diskussionen in Deutschland und im Rat der Europäischen Union sowie entsprechender Äußerungen aus der Bundesregierung im Rahmen des Reformprozesses betont die Konferenz folgende Punkte:

- Im Hinblick auf geforderte Ausnahmen für die Wirtschaft ist es für die Datenschutzbeauftragten des Bundes und der Länder unabdingbar, in der Datenschutz-Grundverordnung an der bisherigen Systematik des Datenschutzrechts festzuhalten. Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn dies durch eine gesetzliche Grundlage oder die Einwilligung des Betroffenen legitimiert ist. Die hier für die Wirtschaft geforderten Ausnahmen lehnt die Konferenz ab. Wollte man in Zukunft nur noch eine besonders risikobehaftete Datenverarbeitung im Einzelfall re-

geln und die so genannte alltägliche Datenverarbeitung weitgehend unregelt lassen, würde dies zu einer massiven Einschränkung des Datenschutzes führen und die Rechte der Betroffenen deutlich beschneiden.

Jede Verarbeitung scheinbar „belangloser“ Daten kann für den Einzelnen schwerwiegende Folgen haben, wie das Bundesverfassungsgericht bereits 1983 ausdrücklich klargestellt hat. Diese Aussage gilt heute mehr denn je. Deshalb lehnt es die Konferenz ab, angeblich „belanglose“ Daten von einer Regelung auszunehmen.

Soweit die Datenschutz-Grundverordnung eine Datenverarbeitung erlaubt, enthält der Reformvorschlag der Kommission bereits jetzt Ansätze für am Risiko der Datenverarbeitung ausgerichtete Differenzierungen. Diese sollten dort, wo ein risikobezogener Ansatz angemessen ist, weiter ausgebaut werden.

- Die Konferenz spricht sich nachdrücklich dafür aus, das bewährte Konzept eines grundsätzlich einheitlichen Datenschutzrechts sowohl für den öffentlichen als auch für den nicht-öffentlichen Bereich beizubehalten und insbesondere für die Datenverarbeitung im öffentlichen Bereich die Möglichkeit eines höheren Schutzniveaus durch einzelstaatliches Recht zu belassen.
- Sie hält es für sinnvoll, für den Beschäftigtendatenschutz in der Datenschutz-Grundverordnung selbst qualifizierte Mindestanforderungen festzulegen und klarzustellen, dass die Mitgliedstaaten über diese zugunsten des Datenschutzes hinausgehen, sie aber nicht unterschreiten dürfen.
- Mit Blick auf die **Richtlinie im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen** bekräftigt die Konferenz nochmals die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch in diesem Bereich und damit die Wichtigkeit der Verabschiedung einer entsprechenden Regelung.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, sich im Sinne dieser Positionen im Rat der Europäischen Union für die Belange eines harmonisierten Datenschutzrechts auf einem hohen Niveau einzusetzen.

1.5.2 Reform der Sicherheitsbehörden: Der Datenschutz darf nicht auf der Strecke bleiben

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist Versuche zurück, vermeintlich „überzogene“ Datenschutzerfordernisse für das Versagen der Sicherheitsbehörden bei der Aufdeckung und Verfolgung rechtsextremistischer Terroristen verantwortlich zu machen und neue Datenverarbeitungsbefugnisse zu begründen.

Sie fordert die Bundesregierung und die Landesregierungen auf, vor einer Reform der Struktur und Arbeitsweise der Polizei- und Verfassungsschutzbehörden zunächst die Befugnisse, den Zuschnitt und die Zusammenarbeit der Verfassungsschutzbehörden vor dem Hintergrund der aufgetretenen Probleme zu evaluieren. Nur auf dieser Grundlage kann eine Diskussion über Reformen seriös geführt und ein Mehrwert für Grundrechtsschutz und Sicherheit erreicht werden.

In datenschutzrechtlicher Hinsicht geklärt werden muss insbesondere, ob die bestehenden Vorschriften in der Vergangenheit richtig angewandt, Arbeitsschwerpunkte richtig gesetzt und Ressourcen zielgerichtet verwendet worden sind. In diesem Zusammenhang ist auch zu untersuchen, ob die gesetzlichen Vorgaben den verfassungsrechtlichen Anforderungen genügen, also verhältnismäßig, hinreichend klar und bestimmt sind. Nur wenn Ursachen und Fehlentwicklungen bekannt sind, können Regierungen und Gesetzgeber die richtigen Schlüsse ziehen. Gründlichkeit geht dabei vor Schnelligkeit.

Schon jetzt haben die Sicherheitsbehörden weitreichende Befugnisse zum Informationsaustausch. Die Sicherheitsgesetze verpflichten Polizei, Nachrichtendienste und andere Behörden bereits heute zu umfassenden Datenübermittlungen. Neue Gesetze können alte Vollzugsdefizite nicht beseitigen.

Bei einer Reform der Sicherheitsbehörden sind der Grundrechtsschutz der Bürgerinnen und Bürger, das Trennungsgebot, die informationelle Gewaltenteilung im Bundesstaat und eine effiziente rechtsstaatliche Kontrolle der Nachrichtendienste zu gewährleisten. Eine effiziente Kontrolle schützt die Betroffenen und verhindert, dass Prozesse sich verselbständigen, Gesetze übersehen und Ressourcen zu Lasten der Sicherheit falsch eingesetzt werden. Nur so kann das Vertrauen in die Arbeit der Sicherheitsbehörden bewahrt und gegebenenfalls wieder hergestellt werden.

Datenschutz und Sicherheit sind kein Widerspruch. Sie müssen zusammenwirken im Interesse der Bürgerinnen und Bürger.

1.5.3 Übermittlung von Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und die GEZ rechtskonform gestalten

Die Meldebehörden sind verpflichtet, regelmäßig Meldedaten an öffentlich-rechtliche Religionsgemeinschaften und an die Gebühreneinzugszentrale (GEZ) zu übermitteln. Die zu übermittelnden Daten beinhalten u. a. Angaben über die Religionszugehörigkeit, aber auch Meldedaten, für die eine Auskunfts- und Übermittlungssperre (beispielsweise wegen Gefahr für Leib und Leben oder einer Inkognito-Adoption) im Meldedatensatz eingetragen ist. Sie sind daher besonders schutzbedürftig.

Die datenschutzrechtliche Verantwortung für den rechtmäßigen Umgang mit Meldedaten tragen allein die Meldebehörden. Eine Übermittlung in elektronischer Form ist nur dann zulässig, wenn die Identitäten von Absender und Empfänger zweifelsfrei feststehen und wenn die Daten vor dem Transport verschlüsselt werden. Diese Anforderungen werden jedoch häufig missachtet.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, für die elektronische Übertragung von Meldedaten elektronische Signaturen und geeignete Verschlüsselungsverfahren mit öffentlichen Schlüsseln zu verwenden, die der jeweils aktuellen Richtlinie des Bundesamtes für die Sicherheit in der Informationstechnik entnommen sind. Durch Zertifizierung oder Beglaubigung der eingesetzten Schlüssel lassen sich auch bei der Nutzung öffentlicher Netze Absender und Empfänger eindeutig und zuverlässig identifizieren.

Mit dem Online Services Computer Interface (OSCI) steht eine bewährte Infrastruktur für E-Government-Anwendungen zur Verfügung. Die Meldeämter setzen das Verfahren entsprechend der Bundesmeldedatenübermittlungsverordnung u. a. für den Datenabgleich zwischen Meldebehörden verschiedener Länder ein. Wird ein auch nach heutigem Kenntnisstand sicheres Verschlüsselungsverfahren eingesetzt, ist die OSCI-Infrastruktur geeignet, die Sicherheit der Meldedatenübertragung auch an GEZ und öffentlich-rechtliche Religionsgemeinschaften zu gewährleisten. Wie jedes kryptographische Verfahren ist auch das Verfahren OSCI-Transport regelmäßig einer Revision zu unterziehen und weiter zu entwickeln.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt dem Bundesministerium des Innern, die Verwendung von OSCI-Transport für die Übermittlungen an GEZ und die öffentlich-rechtlichen Religionsgemeinschaften vorzuschreiben und fordert die Kommunen und die Innenressorts der Länder auf, unverzüglich die gesetzlichen Vorgaben bei Datenübermittlungen an die GEZ und öffentlich-rechtliche Religionsgemeinschaften umzusetzen.

1.5.4 Einführung von IPv6 – Hinweise für Provider im Privatkundengeschäft und Hersteller

Viele Provider werden demnächst in ihren Netzwerken die neue Version 6 des Internet-Protokolls (IPv6) einführen. Größere Unternehmen und Verwaltungen werden ihre Netze meist schrittweise an das neue Protokoll anpassen. Privatkunden werden von dieser Umstellung zuerst betroffen sein.

Für einen datenschutzgerechten Einsatz von IPv6 empfehlen die Datenschutzbeauftragten insbesondere:

- Um das zielgerichtete Verfolgen von Nutzeraktivitäten (Tracking) zu vermeiden, müssen Adresspräfixe grundsätzlich dynamisch an Endkunden vergeben werden. Auch eine Vergabe mehrerer statischer und dynamischer Adresspräfixe kann datenschutzfreundlich sein, wenn Betriebssystem und Anwendungen den Nutzer dabei unterstützen, Adressen gezielt nach der erforderlichen Lebensdauer auszuwählen.
- Entscheidet sich ein Provider für die Vergabe statischer Präfixe an Endkunden, müssen diese Präfixe auf Wunsch des Kunden gewechselt werden können. Hierzu müssen dem Kunden einfache Bedienmöglichkeiten am Router oder am Endgerät zur Verfügung gestellt werden.
- Privacy Extensions müssen auf Endgeräten implementiert und sollten standardmäßig eingeschaltet sein. Ist dies nicht möglich, muss eine benutzerfreundliche manuelle Wechselemöglichkeit für den Interface Identifier bestehen.
- Zusätzlich sollten die Betriebssystem-Hersteller benutzerfreundliche Konfigurationsmöglichkeiten bereitstellen, mit denen Kunden die Wechselfrequenz des Interface Identifiers auf kurze Werte festlegen können bzw. einen Wechsel zu bestimmten Ereignissen anstoßen lassen können, z. B. beim Start des Browsers oder beim Start oder Aufwachen des Rechners.
- Interface Identifier und Präfix sollten synchron gewechselt werden.
- Um den Ortsbezug von Adressen zu verringern, sollten Provider die Adressen für Einwahl-Knoten und sonstige Infrastrukturkomponenten zufällig aus dem ganzen ihnen zur Verfügung stehenden Pool auswählen und regelmäßig innerhalb des Pools wechseln.
- Damit eine sichere und vertrauenswürdige Ende-zu-Ende-Kommunikation mit IPv6 unter Nutzung des Sicherheitsprotokolls IPsec möglich ist, müs-

sen Hersteller von Betriebssystemen starke Verschlüsselungsalgorithmen im TCP/IP-Protokollstack implementieren.

- Die Endgerätehersteller sollten ihre Produkte mit korrekt und sinnvoll vorkonfigurierten IPv6-fähigen Paketfiltern ausstatten und diese über eine leicht zu bedienende Oberfläche zugänglich machen. Bei der Aktivierung der IPv6-Unterstützung im Router sollte die Aktivierung des Paketfilters automatisch stattfinden, dem Nutzer aber zumindest empfohlen werden.
- Hersteller von nicht IPv6-fähigen Firewalls (Firmware und Systemsoftware) sollten entsprechende Updates anbieten. Hersteller von IPv6-fähigen Firewalls sollten den Reifegrad ihrer Produkte regelmäßig prüfen und soweit erforderlich verbessern.
- IPv6-Adressen sind ebenso wie IPv4-Adressen personenbezogene Daten. Sofern eine Speicherung der Adressen über das Ende der Erbringung des Dienstes hinaus unzulässig ist, dürfen Provider und Diensteanbieter IPv6-Adressen allenfalls nach einer Anonymisierung speichern und verarbeiten. Ebenso ist die Ermittlung des ungefähren Standorts eines Endgerätes anhand der IPv6-Adresse für Provider und Diensteanbieter nur nach Anonymisierung der Adresse zulässig. Zur wirkungsvollen Anonymisierung der IPv6-Adressen sollten nach derzeitigem Kenntnisstand mindestens die unteren 88 Bit jeder Adresse gelöscht werden, d. h. der gesamte Interface Identifier sowie 24 Bit des Präfix.
- Der gemeinsame Betrieb von IPv6 und IPv4 auf einem Gerät (Dual-Stack-Betrieb) führt zu erhöhtem Gefahrenpotenzial und sollte daher vermieden werden. Dies gilt auch für die als Übergangslösung gedachten Tunnelprotokolle.
- Bestimmte Arten von Anonymisierungsdiensten sind dazu geeignet, die IP-Adressen von Nutzern wirksam zu verbergen. Auch Peer-to-Peer-Anwendungen können zu einem robusten und datenschutzfreundlichen, weil nicht an einzelnen Punkten stör- und überwachbaren Internet beitragen. Netzbetreiber können die Forschung auf diesem Gebiet unterstützen und selbst Anonymisierungsdienste anbieten. Die Verwendung von Anonymisierungsdiensten und Peer-to-Peer-Anwendungen darf durch Netzbetreiber nicht blockiert werden.

Mit der Orientierungshilfe „Datenschutz bei IPv6 – Hinweise für Hersteller und Provider im Privatkundengeschäft“ präzisieren die Datenschutzbeauftragten des Bundes und der Länder ihre Hinweise vom September 2011.

1.6 Entschlieungen zwischen der 83. und 84. Konferenz

1.6.1 Entschlieung vom 22. August 2012: Melderecht datenschutzkonform gestalten!

Das vom Deutschen Bundestag am 28. Juni 2012 beschlossene neue Melde-
recht weist erhebliche datenschutzrechtliche Defizite auf. Schon die im Re-
gierungsentwurf enthaltenen Datenschutzbestimmungen blieben zum Teil
hinter dem bereits geltenden Recht zurck. Darber hinaus wurde der Regie-
rungsentwurf durch das Ergebnis der Ausschussberatungen des Bundesta-
ges noch einmal deutlich verschlechtert.

Bei den Meldedaten handelt es sich um Pflichtangaben, die die Brgerinnen
und Brger gegenber dem Staat machen mssen. Dies verpflichtet zu be-
sonderer Sorgfalt bei der Verwendung, insbesondere wenn die Daten an
Dritte weitergegeben werden sollen.

Die Datenschutzbeauftragten des Bundes und der Lnder fordern daher den
Bundesrat auf, dem Gesetzentwurf nicht zuzustimmen, damit im Vermitt-
lungsverfahren die erforderlichen datenschutzgerechten Verbesserungen
erfolgen knnen. Dabei geht es nicht nur darum, die im Deutschen Bundes-
tag vorgenommenen Verschlechterungen des Gesetzentwurfs der Bundesre-
gierung rckgngig zu machen, vielmehr muss das Melderecht insgesamt
datenschutzkonform ausgestaltet werden. Hierfr mssen auch die Punkte
aufgegriffen werden, die von den Datenschutzbeauftragten im Gesetzge-
bungsverfahren gefordert worden sind, aber unbercksichtigt blieben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Lnder hlt
insbesondere in den folgenden Punkten Korrekturen und Ergnzungen fr
erforderlich:

- Einfache Melderegisterausknfte fr Zwecke der Werbung und des
Adresshandels bedrfen ausnahmslos der Einwilligung des Meldepflichti-
gen. Dies gilt auch fr die Aktualisierung solcher Daten, ber die die an-
fragenden Stellen bereits verfgen und die Weitergabe der Daten an Ad-
ressbuchverlage.
- Melderegisterausknfte in besonderen Fllen, wie Ausknfte an Parteien
zu Wahlwerbungszwecken und an Presse oder Rundfunk ber Alters- und
Ehejubilen sollten im Interesse der Betroffenen ebenfalls nur mit Einwilli-
gung der Meldepflichtigen zulssig sein.
- Der Meldepflichtige muss sonstigen einfachen Melderegisterausknfte
widersprechen knnen. Die bermittlung hat bei Vorliegen eines Wider-

spruchs zu unterbleiben, sofern der Anfragende kein rechtliches Interesse geltend machen kann.

- Die Zweckbindung der bei Melderegisterauskünften übermittelten Daten ist zu verstärken. Die im Gesetzentwurf nur für Zwecke der Werbung und des Adresshandels vorgesehene Zweckbindung muss auch auf die Verwendung für sonstige gewerbliche Zwecke erstreckt werden.
- Angesichts der Sensibilität der Daten, die im Rahmen einer erweiterten Melderegisterauskunft mitgeteilt werden, und der relativ niedrigen Voraussetzungen, die an die Glaubhaftmachung des berechtigten Interesses gestellt werden, sollte anstelle des berechtigten Interesses ein rechtliches Interesse an der Kenntnis der einzelnen Daten vom potentiellen Datenempfänger glaubhaft gemacht werden müssen.
- Die Erteilung einfacher Melderegisterauskünfte im Wege des Abrufs über das Internet oder des sonstigen automatisierten Datenabrufs sollte wie bisher nur zulässig sein, wenn die betroffene Person ihr nicht widerspricht.
- Die Hotelmeldepflicht sollte entfallen, weil es sich dabei um eine sachlich nicht zu rechtfertigende Vorratsdatenspeicherung handelt. Hotelgäste dürfen nicht schlechthin als Gefahrenquellen oder (potentielle) Straftäter angesehen und damit in ihrem Persönlichkeitsrecht verletzt werden.
- Die erst vor wenigen Jahren abgeschaffte Mitwirkungspflicht des Wohnungsgebers bei der Anmeldung des Mieters darf nicht wieder eingeführt werden. Die Verpflichtung des Meldepflichtigen, den Vermieter zu beteiligen, basiert auf einer Misstrauensvermutung gegenüber der Person des Meldepflichtigen. Der Gesetzgeber hat die damalige Abschaffung der Vermietermeldepflicht unter anderem damit begründet, dass die Erfahrungen der meldebehördlichen Praxis zeigen, dass die Zahl der Scheinmeldungen zu vernachlässigen ist. Es liegen keine Anhaltspunkte dafür vor, dass sich dies zwischenzeitlich geändert hat. Ferner steht der Aufwand hierfür – wie auch bei der Hotelmeldepflicht – außer Verhältnis zum Nutzen.

1.6.2 Entschließung vom 27. Juni 2012: Orientierungshilfe zum datenschutzgerechten Smart Metering

Intelligente Energienetze und -zähler sind ein zentraler Baustein zur Sicherstellung einer nachhaltigen Energieversorgung im Sinne einer ressourcenschonenden, umweltfreundlichen und effizienten Produktion, Verteilung und Nutzung von Energie. Die Konferenz der Datenschutzbeauftragten des Bun-

des und der Länder hat eine Orientierungshilfe beschlossen, die Empfehlungen zur datenschutzgerechten Konzeption von technischen Systemen für das Smart Metering enthält. Kernstück der Orientierungshilfe ist die Beschreibung und datenschutzrechtliche Bewertung sog. Use Cases, d. h. Anwendungsfälle, für die einzelnen Datenverarbeitungsprozesse beim Smart Metering unter Berücksichtigung des jeweiligen Schutzbedarfs der Daten.

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

- Eine Verarbeitung der Smart Meter Daten darf nur erfolgen, soweit es für die im Energiewirtschaftsgesetz aufgezählten Zwecke erforderlich ist.
- Die Ablesintervalle müssen so groß sein, dass aus dem Verbrauch keine Rückschlüsse auf das Verhalten der Nutzer gezogen werden können.
- Smart Meter Daten sollen möglichst nur anonymisiert, pseudonymisiert oder aggregiert übermittelt werden.
- Es muss möglich sein, hoch aufgelöste Daten lokal beim Letztverbraucher abzurufen, ohne dass dieser auf eine externe Verarbeitung der Daten angewiesen ist.
- Die Daten sollen an möglichst wenige Stellen übermittelt werden.
- Es sind angemessene Löschfristen für die Daten festzulegen, um eine Vorratsdatenspeicherung zu vermeiden.
- Die Kommunikations- und Verarbeitungsschritte von Smart Metering müssen zu jeder Zeit für den Letztverbraucher sichtbar und nachweisbar sein. Er muss Zugriffe auf den Smart Meter erkennen und dies im Zweifel unterbinden können.
- Zusätzlich bedarf es durchsetzbarer Ansprüche der Betroffenen auf Löschung, Berichtigung und Widerspruch.
- Der Letztverbraucher muss die Möglichkeit haben, einen Tarif zu wählen, bei dem möglichst wenig über seinen Lebensstil offenbart wird, ohne dass dies für seine Energieversorgung nachteilig ist.
- Smart Meter dürfen von außen nicht frei zugänglich sein. Es müssen eindeutige Profile für den berechtigten Zugang zu den Daten definiert werden. Anhaltspunkte hierfür bieten die Vorgaben im Schutzprofil und in der Technischen Richtlinie des BSI.

- Schon bei der Konzeption und Gestaltung der technischen Systeme muss die Gewährleistung des Datenschutzes berücksichtigt werden (Privacy by Design). Der Letztverbraucher muss mithilfe der Technik alle notwendigen Informationen, Optionen und Kontrollmöglichkeiten erhalten, die ihm die Kontrolle seines Energieverbrauchs und die Gestaltung seiner Privatsphäre ermöglichen, wobei der Stand der Technik nicht unterschritten werden darf. Insbesondere müssen rechtlich verbindliche Vorgaben für die Konzeption der Geräte, Verfahren und Infrastrukturen sowie für deren Einsatz geschaffen werden.

1.6.3 EntschlieÙung vom 23. Mai 2012: Patientenrechte müssen umfassend gestärkt werden

Datenschutzkonferenz fordert die Bundesregierung zur Überarbeitung des vorgelegten Gesetzentwurfs auf!

Mit dem im Januar 2012 der Öffentlichkeit vorgestellten und nun dem Bundeskabinett zugeleiteten Entwurf eines Gesetzes zur Verbesserung der Rechte von Patientinnen und Patienten (Patientenrechtegesetz) sollen insbesondere die bislang von den Gerichten entwickelten Grundsätze des Arzthaftungs- und Behandlungsrechts zusammengeführt und transparent für alle an einer Behandlung Beteiligten geregelt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder teilt das Anliegen der Bundesregierung, die Rechte von Patientinnen und Patienten zu stärken.

Die Datenschutzkonferenz hält allerdings die vorgelegten Regelungen in dem Entwurf eines Patientenrechtegesetzes für nicht ausreichend. Sie fordert die Bundesregierung nachdrücklich auf, den Gesetzentwurf zu überarbeiten und dabei die folgenden Aspekte zu berücksichtigen:

- Die vertraglichen Offenbarungsobliegenheiten der Patientinnen und Patienten gegenüber den Behandelnden dürfen nicht ausgeweitet werden. Die Patientinnen und Patienten dürfen nicht zur Offenlegung von Angaben über ihre körperliche Verfassung verpflichtet werden, die keinen Behandlungsbezug haben.
- Die Patientinnen und Patienten müssen in jedem Fall und nicht erst auf Nachfrage über erlittene Behandlungsfehler informiert werden.
- Der Gesetzentwurf sollte im Zusammenhang mit der Behandlungsdokumentation um verlässliche Vorgaben zur Absicherung des Auskunfts-

rechts der Patientinnen und Patienten sowie zur Archivierung und Löschung ergänzt werden.

- Der Zugang der Patientinnen und Patienten zu der sie betreffenden Behandlungsdokumentation darf nur in besonderen Ausnahmefällen eingeschränkt werden. Die in dem Entwurf vorgesehenen Beschränkungen sind zu weitgehend und unpräzise. Zudem sollte klargestellt werden, dass auch berechnigte eigene Interessen der Angehörigen einen Auskunftsanspruch begründen können.
- Der Gesetzentwurf ist um Regelungen zur Einbeziehung Dritter im Rahmen eines Behandlungsvertrages (Auftragsdatenverarbeitung) zu ergänzen.
- Regelungsbedürftig ist ferner der Umgang mit der Behandlungsdokumentation beispielsweise im Falle eines vorübergehenden Ausfalls, des Todes oder der Insolvenz des Behandelnden. Im Bereich der Heilberufe fehlt es – anders als z. B. bei den Rechtsanwälten – an einem bundesweit einheitlichen Rechtsrahmen.

1.7 83. Konferenz am 21./22. März 2012 in Potsdam

1.7.1 Ein hohes Datenschutzniveau für ganz Europa!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt die Absicht der Europäischen Kommission, den Datenschutz in der Europäischen Union zu modernisieren und zu harmonisieren.

Der Entwurf einer **Datenschutz-Grundverordnung** enthält Regelungen, die zu einer Weiterentwicklung des europäischen Datenschutzrechts führen können. Dazu gehören vor allem

- das Prinzip Datenschutz durch Technik,
- der Gedanke datenschutzfreundlicher Voreinstellungen,
- der Grundsatz der Datenübertragbarkeit,
- das Recht auf Vergessen,
- die verbesserte Transparenz durch Informationspflichten der verantwortlichen Stellen und
- die verschärften Sanktionen bei Datenschutzverstößen.

Hervorzuheben ist zudem die Geltung des europäischen Rechts für Anbieter aus Drittstaaten, deren Dienste sich auch an europäische Bürgerinnen und Bürger richten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für wesentlich, dass bei der Harmonisierung des Datenschutzrechts ein möglichst hohes Niveau für alle Mitgliedsstaaten vorgeschrieben wird. Die Konferenz hatte bereits im Konsultationsverfahren die Auffassung vertreten, dass diesem Ziel angesichts der gewachsenen Traditionen und Rechtsstandards in den Mitgliedsstaaten und der eingeschränkten begrenzten Rechtssetzungskompetenz der EU in Bezug auf innerstaatliche Datenverarbeitungsvorgänge im öffentlichen Bereich am wirksamsten durch eine Richtlinie Rechnung getragen werden kann. Wenn jetzt stattdessen der Entwurf einer unmittelbar geltenden Verordnung vorgelegt wird, muss diese im Sinne eines europäischen Mindestdatenschutz-niveaus den Mitgliedsstaaten zumindest in Bezug auf die Datenverarbeitung der öffentlichen Verwaltung die Möglichkeit eröffnen, durch einzelstaatliches Recht weitergehende Regelungen zu treffen, die entsprechend der jeweiligen Rechtstradition die Grundrechte der Bürgerinnen und Bürger absichern und Raum für eine innovative Rechtsfortbildung schaffen. Nur so können beispielsweise in Deutschland die in der Rechtsprechung des Bundesverfassungsgerichts entwickelten Datenschutzgrundsätze bewahrt und weiterentwickelt werden.

Die Konferenz erkennt an, dass die Institution der betrieblichen Datenschutzbeauftragten erstmals verbindlich in Europa eingeführt werden soll. Die Erfahrungen in Deutschland mit den betrieblichen Datenschutzbeauftragten als unabhängige Kontroll- und Beratungsstellen in Unternehmen sind ausgesprochen positiv. Die Konferenz bedauert deshalb, dass die Kommission grundsätzlich nur Unternehmen mit mindestens 250 Beschäftigten zur Bestellung von Datenschutzbeauftragten verpflichten will. Dieses Vorhaben bedroht eine gewachsene und erfolgreiche Kultur des betrieblichen Datenschutzes in Deutschland.

Über die bereits in dem Verordnungsentwurf vorgeschlagenen Modernisierungen hinaus hält die Konferenz weitere Schritte für erforderlich, die sie etwa in ihrem Eckpunktepapier für ein modernes Datenschutzrecht vom 18. März 2010 vorgeschlagen hat:

- eine strikte Reglementierung der Profilbildung, insbesondere deren Verbot bei Minderjährigen,
- ein effektiver Schutz von Minderjährigen, insbesondere in Bezug auf das Einwilligungserfordernis eine Anhebung der Altersgrenze,

- die Förderung des Selbst Datenschutzes,
- pauschalisierte Schadensersatzansprüche bei Datenschutzverstößen,
- einfache, flexible und praxistaugliche Regelungen zum technisch-organisatorischen Datenschutz, welche vor allem die Grundsätze der Vertraulichkeit, der Integrität, der Verfügbarkeit, der Nichtverkettbarkeit, der Transparenz und der Intervenierbarkeit anerkennen und ausgestalten,
- das Recht, digital angebotene Dienste anonym oder unter Pseudonym nutzen zu können und
- die grundsätzliche Pflicht zur Löschung der angefallenen Nutzerdaten nach dem Ende des Nutzungsvorganges.

Die Regelungen zur Risikoanalyse, Vorabkontrolle und zur Zertifizierung bedürfen der weiteren Präzisierung in der Verordnung selbst.

Für besonders problematisch hält die Konferenz die vorgesehenen zahlreichen Ermächtigungen der Europäischen Kommission für delegierte Rechtsakte, die dringend auf das unbedingt erforderliche Maß zu reduzieren sind. Alle für den Grundrechtsschutz wesentlichen Regelungen müssen in der Verordnung selbst bzw. durch Gesetze der Mitgliedsstaaten getroffen werden.

Die Konferenz weist darüber hinaus darauf hin, dass das im Entwurf der Datenschutz-Grundverordnung vorgesehene Kohärenzverfahren, welches die Aufsichtsbehörden in ein komplexes Konsultationsverfahren einbindet, die Unabhängigkeit der Datenschutzaufsicht beeinträchtigen und zu einer Bürokratisierung des Datenschutzes führen würde. Es muss deshalb vereinfacht und praktikabler gestaltet werden.

Die durch Artikel 8 der EU-Grundrechte-Charta und Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union gewährleistete Unabhängigkeit der Datenschutzaufsichtsbehörden gilt auch gegenüber der Europäischen Kommission. Die vorgesehenen Befugnisse der Kommission in Bezug auf konkrete Maßnahmen der Aufsichtsbehörden bei der Umsetzung der Verordnung wären damit nicht vereinbar.

Wiederholt hat die Konferenz auf die Bedeutung eines hohen und gleichwertigen Datenschutzniveaus auch im **Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen** in Europa hingewiesen. Sie bedauert, dass der für diesen Bereich vorgelegte Richtlinienentwurf in vielen Einzelfragen hinter dem Entwurf für eine Datenschutz-Grundverordnung und hinter

dem deutschen Datenschutzniveau zurückbleibt, etwa im Hinblick auf die Prinzipien der Datenverarbeitung (wie den Grundsatz der Erforderlichkeit) und auf die Rechte der Betroffenen (insbesondere zum Schutz des Kernbereiches der privaten Lebensgestaltung). Auch in diesem Bereich sollte die Richtlinie unter angemessener Berücksichtigung der mitgliedsstaatlichen Verfassungstraditionen ein EU-weit möglichst hohes Mindestniveau festschreiben.

Die Konferenz erklärt, dass sie den Gang des Gesetzgebungsverfahrens konstruktiv und kritisch begleiten wird.

1.7.2 Öffentlich geförderte Forschungsprojekte zur Entdeckung abweichenden Verhaltens im öffentlichen Raum – nicht ohne Datenschutz

Mit erheblichen öffentlichen Mitteln werden derzeit zahlreiche Forschungsprojekte finanziert, die darauf abzielen, mit Hilfe modernster Technik – insbesondere der Videoüberwachung und dem Instrument der Mustererkennung – menschliche Verhaltensweisen zu analysieren. Dadurch sollen in öffentlich zugänglichen Bereichen mit hohem Sicherheitsbedarf „potentielle Gefährder“ frühzeitig entdeckt werden. Zu derartigen Forschungsvorhaben zählen beispielsweise das Projekt „INDECT“ (Intelligentes Informationssystem zur Überwachung, Suche und Detektion für die Sicherheit der Bürger in urbaner Umgebung), das von der Europäischen Union gefördert wird, oder in Deutschland Projekte wie ADIS (Automatisierte Detektion interventionsbedürftiger Situationen durch Klassifizierung visueller Muster), CamInSens (Verteilte, vernetzte Kamerasysteme zur in situ-Erkennung personeninduzierter Gefahrensituationen) oder die Gesichtserkennung in Fußballstadien.

Bei der Mustererkennung soll auf Basis von Video- oder anderen Aufzeichnungen, die mit Daten aus anderen Informationsquellen kombiniert werden, das Verhalten aller erfassten Personen computerunterstützt ausgewertet werden. Menschen, deren Verhalten als ungewöhnlich eingestuft wird, können so in Verdacht geraten, zukünftig eine Straftat zu begehen. Gerade bei der Mustererkennung von menschlichem Verhalten besteht daher die große Gefahr, dass die präventive Analyse einen Anpassungsdruck erzeugt, der die Persönlichkeitsrechte der betroffenen Bürgerinnen und Bürger verletzen würde.

Insoweit ist generell die Frage aufzuwerfen, inwieweit die grundrechtliche Zulässigkeit des Einsatzes der zu erforschenden Überwachungstechnik hinreichend untersucht wird. Bei Projekten, bei denen öffentliche Stellen des Bundes und der Länder beteiligt sind, sollten jeweils die zuständigen Daten-

schutzbehörden frühzeitig über das Projektvorhaben informiert und ihnen Gelegenheit zur Stellungnahme eingeräumt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an alle öffentlichen Stellen von Bund und Ländern, aber auch an die der Europäischen Union, die solche Projekte in Auftrag geben oder Fördermittel hierfür zur Verfügung stellen, bereits bei der Ausschreibung oder Prüfung der Förderfähigkeit derartiger Vorhaben rechtliche und technisch-organisatorische Fragen des Datenschutzes in ihre Entscheidung mit einzubeziehen. Nur so kann verhindert werden, dass Vorhaben öffentlich gefördert werden, die gegen Datenschutzvorschriften verstoßen.

1.7.3 Europäische Ermittlungsanordnung darf Grundrechtsgarantien nicht aushebeln

Zurzeit wird auf europäischer Ebene der Entwurf einer Richtlinie über die Europäische Ermittlungsanordnung in Strafsachen beraten. Diese hat massive Auswirkungen auf den Grundrechtsschutz der Bürgerinnen und Bürger in den EU-Mitgliedstaaten. Sie kann dazu führen, dass der verfahrensrechtliche Schutzstandard bei strafprozessualen Maßnahmen europaweit auf niedrigstes Niveau abgesenkt wird. So kann sie etwa zur Folge haben, dass ein Mitgliedstaat für einen anderen Daten oder Beweismittel erhebt und diesem übermittelt, obwohl die Erhebung nach eigenem Recht nicht zulässig wäre.

Der Richtlinienentwurf verfolgt vorrangig das Ziel einer weitgehenden gegenseitigen Anerkennung von Eingriffsentscheidungen der Strafverfolgungsbehörden, ohne dass einheitliche Verfahrensgarantien geschaffen werden. Dies wirft Probleme auf, wenn der Anordnungsstaat niedrigere Schutzstandards aufweist als der Vollstreckungsstaat. Die Möglichkeiten der Mitgliedstaaten, eine entsprechende Anordnung eines anderen Mitgliedstaates zurückzuweisen, sind nicht immer ausreichend. Eingriffsschwellen, Zweckbindungs- und Verfahrensregelungen müssen gewährleisten, dass die Persönlichkeitsrechte der Betroffenen gewahrt werden.

Eine effektive grenzüberschreitende Strafverfolgung im vereinten Europa darf nicht zu Lasten des Grundrechtsschutzes der Betroffenen gehen. Die Anforderungen der EU-Grundrechte-Charta sind konsequent einzuhalten. Die Europäische Ermittlungsanordnung muss in ein schlüssiges Gesamtkonzept zur Datenerhebung und -verwendung im Bereich der inneren Sicherheit und der Strafverfolgung eingebettet werden, das die Grundrechte der Bürgerinnen und Bürger gewährleistet.

1.8 Entschließung zwischen der 82. und 83. Konferenz vom 7. Februar 2012

Schuldnerverzeichnis im Internet: Anzeige von Schuldnerdaten nur im Rahmen der gesetzlich legitimierten Zwecke

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert das Bundesministerium der Justiz auf, für einen besseren Datenschutz bei der geplanten Internetabfrage aus dem Schuldnerverzeichnis Sorge zu tragen. Es sollen möglichst nur diejenigen Personen angezeigt werden, auf die sich der Abfragezweck bezieht.

Wer eine Wohnung vermieten oder einen Ratenkredit einräumen will, möchte wissen, ob sein zukünftiger Schuldner Zahlungsschwierigkeiten hat. Er hat unter bestimmten Voraussetzungen ein legitimes Interesse an der Einsicht in das von den zentralen Vollstreckungsgerichten geführte Schuldnerverzeichnis. So können sich mögliche Geschäftspartner darüber informieren, ob ihr Gegenüber in wirtschaftliche Not geraten ist.

Mit dem Gesetz zur Reform der Sachaufklärung in der Zwangsvollstreckung aus dem Jahr 2009 will der Gesetzgeber die Stellung des Gläubigers stärken. Das Gesetz sieht unter anderem vor, dass der Inhalt des Schuldnerverzeichnisses ab dem 1. Januar 2013 über eine zentrale und länderübergreifende Abfrage im Internet eingesehen werden kann. Die Ausgestaltung der damit wesentlich erleichterten Einsicht wird derzeit vom Bundesministerium der Justiz durch eine Rechtsverordnung im Einzelnen vorbereitet.

Die gesetzliche Regelung erlaubt Privatpersonen die Einsicht in das Schuldnerverzeichnis nur für bestimmte Zwecke, die bei einer Anfrage darzulegen sind, zum Beispiel, um wirtschaftliche Nachteile abzuwenden, die daraus entstehen können, dass Schuldner ihren Zahlungsverpflichtungen nicht nachkommen. Dennoch ist es derzeit vorgesehen, dass bereits nach Eingabe eines Nachnamens und des zuständigen Vollstreckungsgerichts eine Ergebnisliste mit allen Personen angezeigt wird, auf die diese beiden Kriterien zutreffen. Da Vollstreckungsgerichte jeweils zentral für ein Bundesland eingerichtet sind, erhielte die anfragende Person bei einer Vielzahl von zu erwartenden Namensgleichheiten auch Einsicht zu Angaben über Schuldner, deren Kenntnis sie zum angestrebten Zweck nicht benötigt.

Es ist zu befürchten, dass beispielsweise Vermieter Mietinteressenten nicht berücksichtigen, weil im Schuldnerverzeichnis namensgleiche Personen stehen und es ihnen zu mühsam oder zu schwierig erscheint, anhand weiterer Angaben zu prüfen, ob es sich beim Mietinteressenten tatsächlich um eine der eingetragenen Personen handelt. Auch aus der Sicht der Gläubiger

ist die Anzeige von derart umfangreichen Ergebnislisten wenig hilfreich, denn um den auf die Anfrage bezogenen Datensatz aus der Liste auswählen zu können, müssen ohnehin weitere Daten wie zum Beispiel der Vorname bekannt sein. Da es für Geschäftspartner erforderlich ist, mehr als nur den Nachnamen und den Sitz des zuständigen Vollstreckungsgerichts voneinander zu kennen, ist es auch nicht unangemessen, eine Einsicht von vornherein von weiteren Angaben abhängig zu machen.

2 Beschlüsse der Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich (Düsseldorfer Kreis)

2.1 Beschluss vom 11./12. September 2013

Datenübermittlung in Drittstaaten erfordert Prüfung in zwei Stufen

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

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

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

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

2.2 Beschluss vom 26./27. Februar 2013

Videoüberwachung in und an Taxis

Leben, Gesundheit und Freiheit der Taxifahrer sind hohe Rechtsgüter, die es nachhaltig zu schützen gilt. Zu diesem Zweck kann auch der Einsatz von Videokameras in Betracht kommen. Allerdings müssen die Persönlichkeitsrechte der Fahrgäste, der angestellten Taxifahrer sowie anderer Verkehrsteilnehmer gewahrt bleiben. Der Einsatz von Videokameras muss daher unter Würdigung der berechtigten Sicherheitsinteressen und schutzwürdigen Belange aller Betroffenen auf das erforderliche Mindestmaß beschränkt bleiben.

Die Zulässigkeit einer Videoüberwachung durch Taxi-Unternehmen bestimmt sich nach § 6b Bundesdatenschutzgesetz (BDSG). Gemäß § 6b Abs. 1 Nr. 3, Abs. 3 BDSG ist eine Beobachtung und Aufzeichnung mittels Videokameras nur zulässig, soweit dies zur Wahrnehmung berechtigter Interessen für konk-

ret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

1. Innenkameras

Das betroffene Taxi-Unternehmen muss als verantwortliche Stelle vorrangig alternative und weniger einschneidende Schutzmaßnahmen berücksichtigen, bevor eine Videoüberwachung erwogen werden kann. In Betracht zu ziehen sind beispielsweise die Möglichkeit der anlassbezogenen Auslösung eines „stillen Alarms“ oder eines GPS-gestützten Notrufsignals.

Taxifahrern kann die Möglichkeit eröffnet werden, die Videoaufzeichnung selbsttätig (z. B. über einen Schalter) zu aktivieren, wenn nach ihrer eigenen Einschätzung eine bedrohliche Situation gegeben ist und es mithin einen Anlass für die Aufzeichnung gibt.

Eine anlasslose Videoüberwachung, die ohne Einflussnahmemöglichkeit des Fahrers generell und automatisch einsetzt und bei der sowohl die Fahrgäste als auch das gesamte Geschehen im Fahrgastbereich permanent aufgezeichnet werden, ist weder erforderlich noch verhältnismäßig. Unter Berücksichtigung sowohl der Sicherheitsinteressen des Fahrpersonals als auch der Persönlichkeitsrechte der betroffenen Fahrgäste ist die Videoaufzeichnung vielmehr in der Regel auf das Anfertigen einzelner Standbilder der Fahrgäste beim Einsteigen zu beschränken.

Soweit Bilder zulässigerweise aufgezeichnet wurden, sind diese gemäß § 6b Abs. 5 BDSG unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. Gab es kein Schadensereignis, sind die Bildaufnahmen der Innenkameras im Regelfall innerhalb von 24 Stunden, spätestens aber nach 48 Stunden zu löschen.

Dem Transparenzgebot des § 6b Abs. 2 BDSG folgend müssen durch deutlich sichtbare Beschilderungen an den Fahrgasttüren potentielle Fahrgäste vor dem Einsteigen auf den Umstand der Videoüberwachung und die hierfür verantwortliche Stelle hingewiesen werden.

Schließlich haben die Taxi-Unternehmen durch geeignete technische und organisatorische Maßnahmen zu gewährleisten, dass nur berechtigten Personen ein Zugriff auf die Bildaufzeichnungen möglich und ein unbefugtes Auslesen der Daten ausgeschlossen ist.

2. Außenkameras

Die Voraussetzungen des § 6b Abs. 1, Abs. 3 BDSG sind bei Außenkameras, mit denen der öffentliche Verkehrsraum – etwa zwecks vorsorglicher Beweis

sichernder Dokumentation für den Fall eines Schadensereignisses – einer Überwachung unterzogen werden soll, nicht erfüllt. Unerheblich ist dabei, ob die Kameras mobil sind und eventuell nur die nähere Umgebung des Taxis erfassen. Mit derartigen Kameras sollen gezielt personenbezogene Daten (Bilder, auf denen Personen, Kfz-Kennzeichen, Aufschriften auf Fahrzeugen etc. erkennbar sind) erhoben werden, um später anhand der Aufnahmen beispielsweise Verantwortlichkeiten von Verkehrsteilnehmern und Haftungsfragen klären zu können. Das Recht auf informationelle Selbstbestimmung umfasst jedoch die Möglichkeit, sich in der Öffentlichkeit frei und ungezwungen zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden. Eine Rechtsgrundlage für diese Datenerhebung gibt es nicht. Eine andere Beurteilung ergibt sich auch nicht, wenn § 28 BDSG zugrunde gelegt wird.

Die Ausstattung von Taxis mit „Unfallkameras“, wie sie von Versicherungsunternehmen vorgeschlagen wird, ist daher unzulässig. Die Taxiunternehmen müssen sich darüber im Klaren sein, dass nicht das Versicherungsunternehmen, sondern sie selbst in der datenschutzrechtlichen Verantwortlichkeit stehen.

2.3 Beschluss vom 18./19. September 2012

Near Field Communication (NFC) bei Geldkarten

Es ist datenschutzrechtlich problematisch, wenn beim Einsatz von Near Field Communication (NFC) bei Geldkarten eine eindeutige Kartenummer, Geldbeträge und Transaktionshistorien unverschlüsselt von unberechtigten Dritten auslesbar sind. Die Geldkartenanbieter haben gemäß § 9 BDSG im Rahmen der Verhältnismäßigkeit mit angemessenen technisch-organisatorischen Maßnahmen dafür zu sorgen, dass Dritten kein unberechtigtes Auslesen von Daten möglich wird.

Datenschutzrechtlich erstrebenswert ist die Einräumung einer Wahlmöglichkeit für die Betroffenen, ob sie eine Geldkarte mit NFC-Funktionalität einsetzen wollen. Insoweit nehmen die Aufsichtsbehörden die Ankündigung der Deutschen Kreditwirtschaft zur Kenntnis, das Kartenbetriebssystem so bald wie möglich so zu ändern, dass die Betroffenen die NFC-Funktionalität ein- und ausschalten können. Die Gefahr des (unbemerkten) unberechtigten Auslesens der Transaktionsdaten durch Dritte kann auch dadurch verringert werden, dass insofern nur das kontaktbehaftete Auslesen der Daten zugelassen wird.

Zudem sind die Vorgaben des § 6c BDSG zu beachten. Die Betroffenen müssen ausreichend informiert werden, insbesondere über die Funktionswei-

se des Mediums, die per NFC auslesbaren Daten, die Schutzmöglichkeiten für die Daten und ihre Rechte als Betroffene nach den §§ 34 und 35 BDSG.

2.4 Beschluss vom 17. Januar 2012

Einwilligungs- und Schweigepflichtentbindungserklärung in der Versicherungswirtschaft

Der Düsseldorfer Kreis hat sich dafür eingesetzt, die Einwilligungs- und Schweigepflichtentbindungserklärungen in der Versicherungswirtschaft transparenter zu gestalten. Gemeinsam mit dem Gesamtverband der deutschen Versicherungswirtschaft e. V. haben die Datenschutzaufsichtsbehörden eine Mustererklärung erarbeitet. Die Versicherungsunternehmen sind aufgefordert, die bisherigen Einwilligungstexte zeitnah durch neue zu ersetzen, die der Mustererklärung entsprechen. Der Text lautet wie folgt:

Einwilligung in die Erhebung und Verwendung von Gesundheitsdaten und Schweigepflichtentbindungserklärung

(Der Text der Einwilligungs-/Schweigepflichtentbindungserklärung wurde 2011 mit den Datenschutzaufsichtsbehörden inhaltlich abgestimmt.)

Die Regelungen des Versicherungsvertragsgesetzes, des Bundesdatenschutzgesetzes sowie anderer Datenschutzvorschriften enthalten keine ausreichenden Rechtsgrundlagen für die Erhebung, Verarbeitung und Nutzung von Gesundheitsdaten durch Versicherungen. Um Ihre Gesundheitsdaten für diesen Antrag und den Vertrag erheben und verwenden zu dürfen, benötigt die Versicherung XY¹ daher Ihre datenschutzrechtliche(n) Einwilligung(en). Darüber hinaus benötigt die Versicherung XY Ihre Schweigepflichtentbindungen, um Ihre Gesundheitsdaten bei schweigepflichtigen Stellen, wie z. B. Ärzten, erheben zu dürfen. Als Unternehmen der Lebensversicherung (Krankenversicherung)² benötigt die Versicherung XY Ihre Schweigepflichtentbindung ferner, um Ihre Gesundheitsdaten oder weitere nach § 203 Strafgesetzbuch geschützte Daten, wie z. B. die Tatsache, dass ein Vertrag mit Ihnen besteht, an andere Stellen, z. B. ...³ weiterleiten zu dürfen.

¹ Hier und im Folgenden kann anstelle von „die Versicherung XY“ der Name des verwendenden Unternehmens oder nach einmaliger Nennung (etwa „wir, die Versicherung XY“) jeweils „wir“ eingefügt werden.

² Hier kann die konkrete Sparte genannt werden.

³ Das Beispiel soll verdeutlichen, dass Versicherer diese Daten nicht willkürlich an x-beliebige Stellen weitergeben. Daher können hier einige für die verwendende Versicherung typische Beispiele genannt werden, die die Breite der Weitergabemöglichkeiten erkennen lassen, wie z. B. Assistancegesellschaften, HIS-Betreiber oder IT-Dienstleister.

Die folgenden Einwilligungs- und Schweigepflichtentbindungserklärungen⁴ sind für die Antragsprüfung sowie die Begründung, Durchführung oder Beendigung Ihres Versicherungsvertrages in der Versicherung XY unentbehrlich. Sollten Sie diese nicht abgeben, wird der Abschluss des Vertrages in der Regel nicht möglich sein.⁵

Die Erklärungen betreffen den Umgang mit Ihren Gesundheitsdaten und sonstiger nach § 203 StGB geschützter Daten

- durch die Versicherung XY [Versicherungsgesellschaft, mit der der Versicherungsvertrag abgeschlossen wird] selbst (unter 1.),
- im Zusammenhang mit der Abfrage bei Dritten (unter 2.),
- bei der Weitergabe an Stellen außerhalb der Versicherung XY (unter 3.) und
- wenn der Vertrag nicht zustande kommt (unter 4.).

Die Erklärungen gelten für die von Ihnen gesetzlich vertretenen Personen wie Ihre Kinder, soweit diese die Tragweite dieser Einwilligung nicht erkennen und daher keine eigenen Erklärungen abgeben können.⁶

1. Erhebung, Speicherung und Nutzung der von Ihnen mitgeteilten Gesundheitsdaten durch die Versicherung XY

Ich willige ein, dass die Versicherung XY die von mir in diesem Antrag und künftig mitgeteilten Gesundheitsdaten erhebt, speichert und nutzt, soweit dies zur Antragsprüfung sowie zur Begründung, Durchführung oder Beendigung dieses Versicherungsvertrages erforderlich ist.

⁴ Die Klausel ist zunächst nur für Kranken-, Lebens- und Berufsunfähigkeitsversicherungen zu verwenden, weil in diesen Sparten von Vertragsbeginn an Gesundheitsdaten erhoben und verwendet werden. In anderen Sparten ist der Text entsprechend anzupassen und ggf. nur auszugsweise zu verwenden. In Abstimmung mit den Sparten Unfall und Haftpflicht wird den Unternehmen ein angepasster Vorschlag zur Verfügung gestellt.

⁵ Verweis auf die Folgen der Verweigerung der Einwilligung gemäß § 4a Abs. 1 Satz 2 BDSG

⁶ Werden bei einem Versicherungsprodukt generell keine Kinder und / oder gesetzlich vertretende Personen mitversichert, ist der Absatz bzw. der entsprechende Satz zu streichen. Werden Kinder oder andere gesetzlich vertretene Personen mitversichert, unterschreiben diese ab dem 16. Lebensjahr eine eigene Erklärung, wenn davon auszugehen ist, dass diese einsichtsfähig sind. Diese Erklärung ist aus zivilrechtlichen Gründen auch vom gesetzlichen Vertreter (in der Regel dem Versicherungsnehmer) zu unterzeichnen (siehe unten, Unterschriftenfelder). Damit verbleibt die Entscheidung über das tatsächliche Bestehen der Einsichtsfähigkeit bei dem gesetzlichen Vertreter.

2. Abfrage von Gesundheitsdaten bei Dritten

2.1. Abfrage von Gesundheitsdaten bei Dritten zur Risikobeurteilung und zur Prüfung der Leistungspflicht⁷

Für die Beurteilung der zu versichernden Risiken kann es notwendig sein, Informationen von Stellen abzufragen, die über Ihre Gesundheitsdaten verfügen. Außerdem kann es zur Prüfung der Leistungspflicht erforderlich sein, dass die Versicherung XY die Angaben über Ihre gesundheitlichen Verhältnisse prüfen muss, die Sie zur Begründung von Ansprüchen gemacht haben oder die sich aus eingereichten Unterlagen (z. B. Rechnungen, Verordnungen, Gutachten) oder Mitteilungen z. B. eines Arztes oder sonstigen Angehörigen eines Heilberufs ergeben.

Diese Überprüfung erfolgt nur, soweit es erforderlich ist. Die Versicherung XY benötigt hierfür Ihre Einwilligung einschließlich einer Schweigepflichtentbindung für sich sowie für diese Stellen, falls im Rahmen dieser Abfragen Gesundheitsdaten oder weitere nach § 203 Strafgesetzbuch geschützte Informationen weitergegeben werden müssen.

Sie können diese Erklärungen bereits hier (I) oder später im Einzelfall (II) erteilen. Sie können Ihre Entscheidung jederzeit ändern. Bitte entscheiden Sie sich für eine der beiden nachfolgenden Möglichkeiten:

Möglichkeit I:

☐ Ich willige ein, dass die Versicherung XY – soweit es für die Risikobeurteilung oder für die Leistungsfallprüfung erforderlich ist – meine Gesundheitsdaten bei Ärzten, Pflegepersonen sowie bei Bediensteten von Krankenhäusern, sonstigen Krankenanstalten, Pflegeheimen, Personenversicherern, gesetzlichen Krankenkassen, Berufsgenossenschaften und Behörden⁸ erhebt und für diese Zwecke verwendet.

Ich befreie die genannten Personen und Mitarbeiter der genannten Einrichtungen von ihrer Schweigepflicht, soweit meine zulässigerweise gespeicherten Gesundheitsdaten aus Untersuchungen, Beratungen, Behandlungen

⁷ Wenn Unternehmen stets eine Einwilligung im Einzelfall einholen, wird Ziffer 2.1 gestrichen und der Erläuterungstext über dem grauen Kasten wird für die Einzelfalleinwilligung entsprechend angepasst.

⁸ Der 2008 in Kraft getretene § 213 VVG führt enumerativ die Stellen auf, bei denen der Versicherer mit Einwilligung des Betroffenen dessen Gesundheitsdaten erheben darf. Hinsichtlich der fehlenden sonstigen Heilberufe (Heilpraktiker, Physiotherapeut, Psychotherapeut) sowie der Versicherer, die keine Personenversicherer im herkömmlichen Sprachgebrauch sind, aber dennoch zur Regulierung von Personenschäden Gesundheitsdaten verarbeiten, wird § 213 VVG weit ausgelegt, vgl. auch Eberhardt in: Münchener Kommentar, § 213 VVG, Rn. 35-40.

sowie Versicherungsanträgen und -verträgen aus einem Zeitraum von bis zu zehn Jahren⁹ vor Antragstellung an die Versicherung XY übermittelt werden.

Ich bin darüber hinaus damit einverstanden, dass in diesem Zusammenhang – soweit erforderlich – meine Gesundheitsdaten durch die Versicherung XY an diese Stellen weitergegeben werden und befreie auch insoweit die für die Versicherung XY tätigen Personen von ihrer Schweigepflicht.

Ich werde vor jeder Datenerhebung nach den vorstehenden Absätzen unterrichtet, von wem und zu welchem Zweck die Daten erhoben werden sollen, und ich werde darauf hingewiesen, dass ich widersprechen und die erforderlichen Unterlagen selbst beibringen kann.¹⁰

Möglichkeit II:

☐ Ich wünsche, dass mich die Versicherung XY in jedem Einzelfall informiert, von welchen Personen oder Einrichtungen zu welchem Zweck eine Auskunft benötigt wird. Ich werde dann jeweils entscheiden, ob ich

- in die Erhebung und Verwendung meiner Gesundheitsdaten durch die Versicherung XY einwillige, die genannten Personen oder Einrichtungen sowie deren Mitarbeiter von ihrer Schweigepflicht entbinde und in die Übermittlung meiner Gesundheitsdaten an die Versicherung XY einwillige
- oder die erforderlichen Unterlagen selbst beibringe.

Mir ist bekannt, dass dies zu einer Verzögerung der Antragbearbeitung oder der Prüfung der Leistungspflicht führen kann.

Soweit sich die vorstehenden Erklärungen auf meine Angaben bei Antragstellung beziehen, gelten sie für einen Zeitraum von fünf Jahren¹¹ nach Vertragsschluss. Ergeben sich nach Vertragsschluss für die Versicherung XY konkrete Anhaltspunkte¹² dafür, dass bei der Antragstellung vorsätzlich unrichtige oder unvollständige Angaben gemacht wurden und damit die Risikobeurteilung beeinflusst wurde, gelten die Erklärungen bis zu zehn Jahre nach Vertragsschluss.

⁹ Entsprechend der Annahmepolitik der Versicherungsunternehmen kann für alle oder bestimmte Antragsfragen ein kürzerer Zeitraum zugrunde gelegt werden.

¹⁰ Umsetzung der Unterrichts- und Hinweispflicht nach § 213 Abs. 2 S. 2 i.V.m. Abs. 4 VVG

¹¹ Bei der privaten Krankenversicherung ist wegen § 194 Abs. 1 Satz 4 VVG eine Frist von drei Jahren einzusetzen. Bei vorsätzlichem Verhalten gilt auch für die PKV die Zehn-Jahresfrist.

¹² Anhaltspunkte für vorsätzlich falsche Angaben können sich etwa aus Unstimmigkeiten zwischen der Erkrankung und den Angaben im Antrag ergeben. Eine Überprüfung kann dann ergeben, dass es am Vorsatz fehlt und die Datenerhebung für den Betroffenen keine negativen Konsequenzen hat.

2.2. Erklärungen für den Fall Ihres Todes

Zur Prüfung der Leistungspflicht kann es auch nach Ihrem Tod erforderlich sein, gesundheitliche Angaben zu prüfen. Eine Prüfung kann auch erforderlich sein, wenn sich bis zu zehn Jahre nach Vertragsschluss für die Versicherung XY konkrete Anhaltspunkte dafür ergeben, dass bei der Antragstellung unrichtige oder unvollständige Angaben gemacht wurden und damit die Risikobeurteilung beeinflusst wurde. Auch dafür bedürfen wir einer Einwilligung und Schweigepflichtentbindung. Bitte entscheiden Sie sich für eine der beiden nachfolgenden Möglichkeiten:¹³

Möglichkeit I:

☐ Für den Fall meines Todes willige ich in die Erhebung meiner Gesundheitsdaten bei Dritten zur Leistungsprüfung bzw. einer erforderlichen erneuten Antragsprüfung ein wie im ersten Ankreuzfeld beschrieben (siehe oben 2.1. – Möglichkeit I)

Möglichkeit II:

☐ Soweit zur Prüfung der Leistungspflicht bzw. einer erforderlichen erneuten Antragsprüfung nach meinem Tod Gesundheitsdaten erhoben werden müssen, geht die Entscheidungsbefugnis über Einwilligungen und Schweigepflichtentbindungserklärungen auf meine Erben oder – wenn diese abweichend bestimmt sind – auf die Begünstigten des Vertrags über.

¹³ Bei Abschnitt 2.2 ist es möglich, das zweite Ankreuzfeld nicht zu nutzen, sodass keine Wahlmöglichkeit besteht und nur das erste Feld angekreuzt werden kann. Der letzte erläuternde Satz vor dem grau unterlegten Feld entfällt dann. Wird das erste (einzige) Ankreuzfeld dann nicht angekreuzt, würde bei einer gerichtlichen Prüfung entweder eine andere Willenserklärung herangezogen (z. B. Testament) oder bei Fehlen einer solchen auf den mutmaßlichen Willen des Betroffenen abgestellt. Ein automatischer Übergang der höchstpersönlichen Verfügungsbefugnis auf Erben oder Bezugsberechtigte des Vertrags erfolgt regelmäßig nicht. Bei Anbieten einer echten Wahlmöglichkeit und einem vorliegenden Kreuz erscheint der Bestand der Erklärungen vor Gericht als wahrscheinlicher, sodass die Bezugnahme auf den mutmaßlichen Willen in einem möglichen Zivilprozess nicht nötig erscheint.

3. Weitergabe Ihrer Gesundheitsdaten und weiterer nach § 203 StGB geschützter Daten an Stellen außerhalb der Versicherung XY

Die Versicherung XY verpflichtet die nachfolgenden Stellen vertraglich auf die Einhaltung der Vorschriften über den Datenschutz und die Datensicherheit.¹⁴

3.1. Datenweitergabe zur medizinischen Begutachtung

Für die Beurteilung der zu versichernden Risiken und zur Prüfung der Leistungspflicht kann es notwendig sein, medizinische Gutachter einzuschalten. Die Versicherung XY benötigt Ihre Einwilligung und Schweigepflichtentbindung, wenn in diesem Zusammenhang Ihre Gesundheitsdaten und weitere nach § 203 StGB geschützte Daten übermittelt werden. Sie werden über die jeweilige Datenübermittlung unterrichtet.¹⁵

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten an medizinische Gutachter übermittelt, soweit dies im Rahmen der Risikoprüfung oder der Prüfung der Leistungspflicht erforderlich ist und meine Gesundheitsdaten dort zweckentsprechend verwendet und die Ergebnisse an die Versicherung XY zurück übermittelt werden. Im Hinblick auf meine Gesundheitsdaten und weitere nach § 203 StGB geschützte Daten entbinde ich die für die Versicherung XY tätigen Personen und die Gutachter von ihrer Schweigepflicht.

3.2. Übertragung von Aufgaben auf andere Stellen (Unternehmen oder Personen)

Die Versicherung XY führt bestimmte Aufgaben, wie zum Beispiel die Risikoprüfung, die Leistungsfallbearbeitung oder die telefonische Kundenbetreuung, bei denen es zu einer Erhebung, Verarbeitung oder Nutzung Ihrer Gesundheitsdaten kommen kann, nicht selbst durch, sondern überträgt die Erledigung einer anderen Gesellschaft der XY-Gruppe oder einer anderen Stelle. Werden hierbei Ihre nach § 203 StGB geschützten Daten weitergege-

¹⁴ Die vertragliche Verpflichtung auf Einhaltung von Datenschutz und Datensicherheit auch für Stellen, die eigenverantwortlich Aufgaben übernehmen, ergibt sich aus dem künftigen Art. 21 Abs. 4 Code of Conduct (CoC). Diese Verpflichtung wurde dort für die Funktionsübertragung an Dienstleister als datenschutzrechtlicher Mehrwert für die Betroffenen vereinbart. Rückversicherer werden nicht als Dienstleister des Erstversicherers im Sinne von Art. 21 angesehen, wenn sie den Erstversicherer im Rahmen von Rückversicherungsverträgen bei der Risiko- und Leistungsprüfung unterstützen. Sofern der Erstversicherer Rückversicherer außerhalb von Rückversicherungsverträgen als Dienstleister einsetzt und diese noch nicht vertraglich auf die Einhaltung von Datenschutz und Datensicherheit verpflichtet hat, ist dies nachzuholen (vgl. auch Hinweis 18).

¹⁵ Die Unterrichtungspflicht wurde aufgenommen, um mehr Transparenz zu schaffen. Hierfür ist mitzuteilen, welche konkreten Daten, für welchen Zweck, an welche Stelle übermittelt werden sollen.

ben, benötigt die Versicherung XY Ihre Schweigepflichtentbindung für sich und¹⁶ soweit erforderlich für die anderen Stellen.¹⁷

Die Versicherung XY führt eine fortlaufend aktualisierte Liste¹⁸ über die Stellen¹⁹ und Kategorien von Stellen²⁰, die vereinbarungsgemäß Gesundheitsdaten für die Versicherung XY erheben, verarbeiten oder nutzen unter Angabe der übertragenen Aufgaben. Die zurzeit gültige Liste ist als Anlage der Einwilligungserklärung angefügt.²¹ Eine aktuelle Liste kann auch im Internet unter (Internetadresse) eingesehen oder bei (Ansprechpartner nebst Anschrift, Telefonnummer, ggf. E-Mailadresse) angefordert werden. Für die Weitergabe Ihrer Gesundheitsdaten an und die Verwendung durch die in der Liste genannten Stellen benötigt die Versicherung XY Ihre Einwilligung.

Ich willige ein,²² dass die Versicherung XY meine Gesundheitsdaten an die in der oben erwähnten Liste genannten Stellen übermittelt und dass die Ge-

¹⁶ Der Satzteil „für sich und“ ist nur für die Kranken, Leben- und Unfallversicherung zu verwenden.

¹⁷ Die Mitarbeiter anderer Stellen werden von ihrer Schweigepflicht entbunden, wenn sie ihrerseits im Rahmen der von ihnen zu erledigenden Aufgaben nach § 203 StGB geschützte Daten an den Versicherer oder an andere Stellen, wie z. B. mit der IT-Wartung beauftragte Subunternehmen weitergeben.

¹⁸ In der Liste werden die Stellen und Kategorien von Stellen aufgezählt, die Gesundheitsdaten erheben, verarbeiten oder nutzen. Ebenfalls gemeint sind Stellen und Kategorien von Stellen, die einfache personenbezogene Daten, die nach § 203 StGB geschützt sind, wie z. B. die Information, dass ein Lebensversicherungsvertrag besteht, verwenden. Nicht gemeint sind Stellen, die im Rahmen der ihnen zugewiesenen Aufgaben keine Gesundheitsdaten verarbeiten, diese aber theoretisch einsehen können (Bsp. Personen oder Unternehmen, die mit der IT-Wartung betraut sind). In die Liste werden sowohl Dritte im datenschutzrechtlichen Sinn als auch Auftragsdatenverarbeiter, bei denen Abgrenzungsschwierigkeiten zur Funktionsübertragung bestehen (siehe Fußnote 23), aufgenommen. Rückversicherer werden als Dienstleister des Erstversicherers angesehen, wenn sie ohne einen Rückversicherungsvertrag nur als Dienstleister des Erstversicherers tätig werden.

¹⁹ Werden Aufgaben im Wesentlichen von einem Unternehmen an ein anderes Unternehmen der XY-Versicherungsgruppe oder an eine externe Stelle abgegeben, ist die andere Stelle namentlich anzugeben unter Bezeichnung der Aufgabe. Hierunter fallen z. B. Stellen, die die Aufgaben Risikoprüfung, Leistungsfallbearbeitung oder Serviceleistung für das Unternehmen übernehmen.

²⁰ Fehlt es an einer systematischen automatisierten Datenverarbeitung, können die Stellen, an die Gesundheitsdaten weitergegeben werden bzw. die zur Erfüllung ihrer Aufgabe selbst Gesundheitsdaten erheben, in Kategorien zusammengefasst werden unter Bezeichnung der Aufgabe. Dies gilt auch für Stellen, die nur einmalig tätig werden, wie z. B. Krankentransporte.

²¹ Die Liste der Dienstleister soll in der Form, in der die Einwilligungs- und Schweigepflichtentbindungserklärung erteilt wird, als Anlage mitgegeben werden.

²² Die Einwilligung gilt in jedem Fall für die Datenübermittlung an eigenverantwortliche Dienstleister. Sie ist außerdem bei Abgrenzungsschwierigkeiten zwischen Auftragsdatenverarbeitung und Funktionsübertragung einzuholen. Das Einwilligungserfordernis gilt nicht, wenn es sich in Übereinstimmung mit der zuständigen Datenschutzaufsichtsbehörde um eine eindeutige Auftragsdatenverarbeitung handelt. In diesen Fällen sollte dennoch eine Schweigepflichtentbindung eingeholt werden.

sundheitsdaten dort für die angeführten Zwecke im gleichen Umfang erhoben, verarbeitet und genutzt werden, wie die Versicherung XY dies tun dürfte. Soweit erforderlich, entbinde ich die Mitarbeiter der XY Unternehmensgruppe und sonstiger Stellen²³ im Hinblick auf die Weitergabe von Gesundheitsdaten und anderer nach § 203 StGB geschützter Daten von ihrer Schweigepflicht.

3.3. Datenweitergabe an Rückversicherungen

Um die Erfüllung Ihrer Ansprüche abzusichern, kann die Versicherung XY Rückversicherungen einschalten, die das Risiko ganz oder teilweise übernehmen. In einigen Fällen bedienen sich die Rückversicherungen dafür weiterer Rückversicherungen, denen sie ebenfalls Ihre Daten²⁴ übergeben. Damit sich die Rückversicherung ein eigenes Bild über das Risiko oder den Versicherungsfall machen kann, ist es möglich, dass die Versicherung XY Ihren Versicherungsantrag oder Leistungsantrag der Rückversicherung vorlegt. Das ist insbesondere dann der Fall, wenn die Versicherungssumme besonders hoch ist oder es sich um ein schwierig einzustufendes Risiko handelt.

Darüber hinaus ist es möglich, dass die Rückversicherung die Versicherung XY aufgrund ihrer besonderen Sachkunde bei der Risiko- oder Leistungsprüfung sowie bei der Bewertung von Verfahrensabläufen unterstützt.

Haben Rückversicherungen die Absicherung des Risikos übernommen, können sie kontrollieren, ob die Versicherung XY das Risiko bzw. einen Leistungsfall richtig eingeschätzt hat.

Außerdem werden Daten über Ihre bestehenden Verträge und Anträge im erforderlichen Umfang an Rückversicherungen weitergegeben, damit diese überprüfen können, ob und in welcher Höhe sie sich an dem Risiko beteiligen können.²⁵ Zur Abrechnung von Prämienzahlungen und Leistungsfällen können Daten über Ihre bestehenden Verträge an Rückversicherungen weitergegeben werden.

Zu den oben genannten Zwecken werden möglichst anonymisierte bzw. pseudonymisierte Daten, jedoch auch personenbezogene Gesundheitsangaben verwendet. Ihre personenbezogenen Daten werden von den Rückversicherungen nur zu den vorgenannten Zwecken verwendet. Über die Übermitt-

²³ „und sonstige Stellen“ – Dieser Passus wird gestrichen, wenn keine schweigepflichtgebundenen Dienstleister und Auftragnehmer eingeschaltet sind.

²⁴ Sollen Gesundheitsdaten an den Rückversicherer des Rückversicherers übermittelt werden, ist eine spezielle Einwilligung zu prüfen.

²⁵ Für die Kumulkontrolle ist eine Schweigepflichtentbindung erforderlich, da nach § 203 StGB geschützte Daten weitergegeben werden, jedoch keine Gesundheitsdaten.

lung Ihrer Gesundheitsdaten an Rückversicherungen werden Sie durch die Versicherung XY unterrichtet²⁶.

Ich willige ein, dass meine Gesundheitsdaten – soweit erforderlich – an Rückversicherungen übermittelt und dort zu den genannten Zwecken verwendet werden. Soweit erforderlich, entbinde ich die für die Versicherung XY tätigen Personen im Hinblick auf die Gesundheitsdaten und weiteren nach § 203 StGB geschützter Daten von ihrer Schweigepflicht.

3.4. Datenaustausch mit dem Hinweis- und Informationssystem (HIS)²⁷

Die Versicherungswirtschaft nutzt zur genaueren Risiko- und Leistungsfall einschätzung das Hinweis- und Informationssystem HIS, das derzeit die informa Insurance Risk and Fraud Prevention GmbH (informa IRFP GmbH, Rheinstraße 99, 76532 Baden-Baden, www.informa-irfp.de) betreibt. Auffälligkeiten, die auf Versicherungsbetrug hindeuten könnten, und erhöhte Risiken kann die Versicherung XY an das HIS melden. Die Versicherung XY und andere Versicherungen fragen Daten im Rahmen der Risiko- oder Leistungsprüfung aus dem HIS ab, wenn ein berechtigtes Interesse besteht.²⁸ Zwar werden dabei keine Gesundheitsdaten weitergegeben, aber für eine Weitergabe Ihrer nach § 203 StGB geschützten Daten benötigt die Versicherung XY Ihre Schweigepflichtentbindung. Dies gilt unabhängig davon, ob der Vertrag mit Ihnen zustande gekommen ist oder nicht.

Ich entbinde die für Versicherung XY tätigen Personen von ihrer Schweigepflicht, soweit sie Daten aus der Antrags- oder Leistungsprüfung an den jeweiligen Betreiber des Hinweis- und Informationssystems (HIS)²⁹ melden.

²⁶ Die Unterrichtungspflicht des Erstversicherers ersetzt die anderenfalls von den Datenschutzbehörden geforderte ausführliche Erklärung entsprechend dem Baustein 2.1. zur Erhebung von Gesundheitsdaten bei Dritten. Zu unterrichten ist über die konkret übermittelten Daten, den Zweck der Übermittlung und den Empfänger der Daten.

²⁷ Da keine einwilligungsbedürftigen besonderen Arten personenbezogener Daten nach § 3 Abs. 9 BDSG (Gesundheitsdaten) an das HIS gemeldet werden, betrifft die Schweigepflichtentbindung nur die nach § 203 StGB geschützten Daten, hier etwa die Tatsache, dass ein Versicherungsvertrag besteht. Da nur die Sparten Unfall und Leben von § 203 Abs. 1 Nr. 6 StGB erfasst werden und mit dem HIS arbeiten, ist der Passus für die anderen Sparten zu streichen. Im Fall der Nutzung ist die Information des Versicherungsnehmers über das Hinweis- und Informationssystem dann in anderer Weise sicherzustellen. Soweit Gesundheitsdaten im Leistungsfall im Rahmen der Detailanfrage ausgetauscht werden, gelten die Einwilligungserklärungen unter 2.1.

²⁸ Ein berechtigtes Interesse für die Abfrage zum Zweck der Risiko- und Leistungsprüfung ist stets gegeben mit Ausnahme des Erlebensfalls in der Lebensversicherung.

²⁹ Durch die Formulierung „an den jeweiligen Betreiber“ sowie die Aufnahme von „derzeit“ im ersten Satz des erläuternden Textes wird deutlich gemacht, dass sich der Betreiber des HIS ändern kann. Die Schweigepflichtentbindungserklärung soll auch künftige Betreiber erfassen.

Sofern es zur Prüfung der Leistungspflicht erforderlich ist, können über das HIS Versicherungen ermittelt werden, mit denen Sie in der Vergangenheit in Kontakt gestanden haben, und die über sachdienliche Informationen verfügen könnten. Bei diesen können die zur weiteren Leistungsprüfung erforderlichen Daten erhoben werden (siehe unter Ziff. 2.1).

3.5. Datenweitergabe an selbstständige Vermittler

Die Versicherung XY gibt grundsätzlich keine Angaben zu Ihrer Gesundheit an selbstständige Vermittler weiter. Es kann aber in den folgenden Fällen dazu kommen, dass Daten, die Rückschlüsse auf Ihre Gesundheit zulassen, oder gemäß § 203 StGB geschützte Informationen über Ihren Vertrag Versicherungsvermittlern zur Kenntnis gegeben werden.

Soweit es zu vertragsbezogenen Beratungszwecken erforderlich ist, kann der Sie betreuende Vermittler Informationen darüber erhalten, ob und ggf. unter welchen Voraussetzungen (z. B. Annahme mit Risikozuschlag, Ausschlüsse bestimmter Risiken) Ihr Vertrag angenommen werden kann.

Der Vermittler, der Ihren Vertrag vermittelt hat, erfährt, dass und mit welchem Inhalt der Vertrag abgeschlossen wurde. Dabei erfährt er auch, ob Risikozuschläge oder Ausschlüsse bestimmter Risiken vereinbart wurden.

Bei einem Wechsel des Sie betreuenden Vermittlers auf einen anderen Vermittler kann es zur Übermittlung der Vertragsdaten mit den Informationen über bestehende Risikozuschläge und Ausschlüsse bestimmter Risiken an den neuen Vermittler kommen. Sie werden bei einem Wechsel des Sie betreuenden Vermittlers auf einen anderen Vermittler vor der Weitergabe von Gesundheitsdaten informiert sowie auf Ihre Widerspruchsmöglichkeit hingewiesen.

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten und sonstigen nach § 203 StGB geschützten Daten in den oben genannten Fällen – soweit erforderlich – an den für mich zuständigen selbstständigen Versicherungsvermittler übermittelt und diese dort erhoben, gespeichert und zu Beratungszwecken genutzt werden dürfen.

4. Speicherung und Verwendung Ihrer Gesundheitsdaten wenn der Vertrag nicht zustande kommt³⁰

Kommt der Vertrag mit Ihnen nicht zustande, speichert die Versicherung XY Ihre im Rahmen der Risikoprüfung erhobenen Gesundheitsdaten für den Fall, dass Sie erneut Versicherungsschutz beantragen. Außerdem ist es möglich, dass die Versicherung XY zu Ihrem Antrag einen Vermerk an das Hinweis- und Informationssystem meldet, der an anfragende Versicherungen für deren Risiko- und Leistungsprüfung übermittelt wird (siehe Ziffer 3.4.). Die Versicherung XY speichert Ihre Daten auch, um mögliche Anfragen weiterer Versicherungen beantworten zu können. Ihre Daten werden bei der Versicherung XY und im Hinweis- und Informationssystem bis zum Ende des dritten Kalenderjahres nach dem Jahr der Antragstellung³¹ gespeichert.

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten – wenn der Vertrag nicht zustande kommt – für einen Zeitraum von drei Jahren ab dem Ende des Kalenderjahres der Antragstellung zu den oben genannten Zwecken speichert und nutzt.³²

Ort, Datum

Unterschrift Antragsteller/in oder mitzuversichernde Person

Ort, Datum

Unterschrift gesetzlich vertretene Person (bei Vorliegen der erforderlichen Einsichtsfähigkeit, frühestens ab Vollendung des 16. Lebensjahres)

Ort, Datum

Unterschrift des gesetzlichen Vertreters

³⁰ Der Passus ist zu streichen, wenn eine Speicherung von Antragsdaten bei Nichtzustandekommen des Vertrags nicht erfolgt. Daten über nicht zustande gekommene Verträge sind bei dem Versicherungsunternehmen spätestens drei Jahre gerechnet vom Ende des Kalenderjahres nach Antragstellung zu löschen. Auch im Hinweis- und Informationssystem werden diese Daten entsprechend gelöscht. Gesetzliche Aufbewahrungspflichten oder -befugnisse bleiben hiervon unberührt. Werden Schadensersatzansprüche gegen das Unternehmen geltend gemacht oder bei Prüfungen durch Behörden kann sich eine längere Aufbewahrung auch aus § 28 Abs. 6 Nr. 3 BDSG rechtfertigen.

³¹ Es zählt das Datum der Unterschrift im Antrag.

³² Die Nutzung ist nur zu eigenen Zwecken des Versicherers zulässig. Die Übermittlung an ein anderes Unternehmen ist nur auf der Basis einer von diesem einzuholenden Einwilligung/Schweigepflichtentbindung nach Ziffer 2.1. zulässig.

Hinweise zur Anwendung der Einwilligungs- und Schweigepflichtentbindungserklärung für die Erhebung und Verwendung von Gesundheitsdaten und sonstiger nach § 203 StGB geschützter Daten

Der vorliegende Text einer Einwilligungs- und Schweigepflichtentbindungsklausel ist vom GDV mit den Datenschutzaufsichtsbehörden abgestimmt worden. Der Verbraucherzentrale Bundesverband war ebenfalls an den Gesprächen beteiligt. Die Klausel wird flankiert durch Verhaltensregeln für den Umgang mit personenbezogenen Daten in der Versicherungswirtschaft (Code of Conduct). Zweck ist, lediglich für die tatsächlich einwilligungsbedürftigen Datenerhebungs- und -verwendungsprozesse eine Einwilligungs- und Schweigepflichtentbindungserklärung einzuholen. Andere Datenverarbeitungen werden in einem Code of Conduct konkretisiert. Sowohl die Klausel als auch der Code of Conduct werden in regelmäßigen Abständen gemeinsam überarbeitet, um aktuelle Entwicklungen der Datenverarbeitung und gesetzliche Änderungen zu berücksichtigen.

Hinweise zur Klausel – BAUSTEINSYSTEM

Die Texte stellen einen maximalen Rahmen für Einwilligungs- und Schweigepflichtentbindungserklärungen dar. Wegen des im BDSG verankerten Prinzips der Datensparsamkeit sind nur die Textpassagen zu verwenden, die benötigt werden. Soweit im Rahmen einer Versicherungssparte oder eines Versicherungsprodukts bestimmte Datenverarbeitungen nicht erfolgen, wie etwa die Erhebung von Gesundheitsdaten bei Dritten zur Risikoprüfung, ist der Text entsprechend zu kürzen. Werden Datenverarbeitungen beschrieben, die das Unternehmen nicht durchführt oder nicht plant, wie zum Beispiel die Datenweitergabe zur medizinischen Begutachtung oder die Datenweitergabe an Rückversicherer, ist der entsprechende Absatz / Satz nicht zu verwenden.

Zu beachten ist dabei jedoch, dass die in Abschnitt 2.1. angebotenen Wahlmöglichkeiten bestehen bleiben müssen. Das heißt, wenn für die Datenerhebung bei Dritten mit dem Antrag eine Einwilligung eingeholt werden soll, müssen auch beide Alternativen (Pauschaleinwilligung / Einzelfalleinwilligung) angeboten werden. Erfolgt keine Wahl, muss spätestens unmittelbar vor der Datenerhebung eine Einwilligung eingeholt werden. Die dafür zu gestaltenden Erklärungen sollten sich an den hier vorliegenden orientieren.

Die vorliegende Einwilligungs- und Schweigepflichtentbindungsklausel bezieht sich auf Gesundheitsdaten und darüber hinaus auf weitere nach § 203 Abs. 1 StGB geschützte Daten, wie die Tatsache des Bestehens eines Versicherungsvertrags. Gesundheitsdaten können in allen Versicherungssparten anfallen, auch dort, wo dies nicht sofort vermutet wird, z. B. in der Reisegepäckversicherung (Verletzungen durch Raub) und in der Kfz-Versicherung

(Verletzungen durch Unfall). Die Einwilligungs- und Schweigepflichtentbindungserklärungen müssen vor der jeweils ersten Verarbeitung von Gesundheitsdaten im Unternehmen dem Antragsteller bzw. Versicherungsnehmer vorgelegt werden, soweit sie für bevorstehende Datenerhebungen, -verarbeitungen oder -nutzungen benötigt werden.

Sollen andere besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG erhoben, verarbeitet oder genutzt werden, wie bspw. die Information über eine Gewerkschaftszugehörigkeit zur Prämienberechnung in speziellen Tarifen gewerkschaftsnaher Unternehmen, ist mit dem betreffenden Antrag eine entsprechende Einwilligungserklärung vom Antragsteller ein-zuholen. Diese kann z. B. wie folgt formuliert und gestaltet werden:

Ich willige in die Erhebung, Verarbeitung und Nutzung meiner Angaben zur Gewerkschaftszugehörigkeit ein, soweit dies zur Antragsprüfung sowie zur Begründung, Durchführung oder Beendigung dieses Vertrages, insbesondere zur Berechnung meiner Versicherungsprämie, erforderlich ist.

3 Entschließungen der Konferenz der Informationsfreiheitsbeauftragten in Deutschland

3.1 27. Konferenz am 28. November 2013 in Erfurt

Forderungen für die neue Legislaturperiode: Informationsrechte der Bürgerinnen und Bürger stärken!

Der freie Zugang der Bürgerinnen und Bürger der Bundesrepublik Deutschland zu den Informationen der öffentlichen Stellen muss auch in Deutschland ein fester Bestandteil der verfassungsrechtlich garantierten Rechte werden. Transparenz ist eine wesentliche Grundlage für eine funktionierende freiheitlich demokratische Gesellschaft. Sie ist der Nährboden für gegenseitiges Vertrauen zwischen staatlichen Stellen und den Bürgerinnen und Bürgern.

Es reicht nicht aus, dass Informationen nur auf konkreten Antrag hin herauszugeben sind. In Zukunft sollten öffentliche und private Stellen, die öffentliche Aufgaben wahrnehmen, verpflichtet sein, Informationen von sich aus zur Verfügung zu stellen. Auf diese Weise wird der Zugang zu Informationen für alle erleichtert und der Aufwand der Informationserteilung reduziert.

Die Bundesrepublik Deutschland muss jetzt die nötigen gesetzlichen Regelungen für ein modernes Transparenzrecht schaffen, um mit den internationalen Entwicklungen Schritt zu halten und die Chancen der Transparenz wahrzunehmen.

Die Konferenz der Informationsfreiheitsbeauftragten des Bundes und der Länder fordert daher alle Beteiligten in Bund und in den Ländern auf, sich für die Stärkung der Transparenz auf nationaler, europäischer und internationaler Ebene einzusetzen.

Sie fordert insbesondere:

- den Anspruch auf freien Zugang zu amtlichen Informationen endlich in alle Verfassungen aufzunehmen,
- einen gesetzlich geregelten effektiven Schutz von Whistleblowern, die über Rechtsverstöße im öffentlichen und nicht-öffentlichen Bereich berichten,
- ein einheitliches Informationsrecht zu schaffen, das die Regelungen des Informationsfreiheitsgesetzes, des Umweltinformationsgesetzes und des Verbraucherinformationsgesetzes in einem Gesetz zusammenfasst,

- dass das Informationsfreiheitsrecht im Sinne eines Transparenzgesetzes mit umfassenden Veröffentlichungspflichten nach den Open-Data-Grundsätzen weiterentwickelt wird,
- aus der vom Bundestag in Auftrag gegebenen Evaluation des Bundesinformationsfreiheitsgesetzes die notwendigen Konsequenzen zu ziehen und die Ausnahmeregelungen auf das verfassungsrechtlich zwingend gebotene Maß zu beschränken,
- die Bereichsausnahme für die Nachrichtendienste abzuschaffen, die entsprechende Ausnahmeregelung auf konkrete Sicherheitsbelange zu beschränken und den Umgang mit Verschluss-Sachen gesetzlich in der Weise zu regeln, dass die Klassifizierung von Unterlagen als geheimhaltungsbedürftig regelmäßig von einer unabhängigen Instanz überprüft, beschränkt und aufgehoben werden kann,
- Transparenz der Kooperationen auch zwischen privaten und wissenschaftlichen Einrichtungen sicherzustellen, die im Rahmen der Wahrnehmung öffentlicher Aufgaben für staatliche Stellen tätig sind. Dies gilt auch und insbesondere für Sicherheitsbehörden.
- die Berliner Erklärung der 8. Internationalen Konferenz der Informationsfreiheitsbeauftragten zur Stärkung der Transparenz auf nationaler und internationaler Ebene vom 20. September 2013, insbesondere die Anerkennung eines Menschenrechts auf Informationszugang im Rahmen der Vereinten Nationen, den Beitritt der Bundesrepublik zur Open Government Partnership und zur Tromsö-Konvention des Europarats (Konvention des Europarates über den Zugang zu amtlichen Dokumenten) umzusetzen.

Die Konferenz der Informationsfreiheitsbeauftragten des Bundes und der Länder bietet ihre Unterstützung an.

3.2 26. Konferenz am 27. Juni 2013 in Erfurt

3.2.1 Open Data stärkt die Informationsfreiheit – sie ist eine Investition in die Zukunft!

Die gesellschaftlichen Erwartungen an einen transparenten Staat gehen inzwischen weit über das bisherige Recht der Bürgerinnen und Bürger, einen Antrag auf Informationszugang zu stellen, hinaus. Open Data – also die aktive Bereitstellung öffentlicher Informationen im Internet – wird auf den ersten Portalen bereits praktiziert. Zahlreiche Projekte befinden sich im Auf-

bau. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland begrüßt diese Entwicklungen ausdrücklich und formuliert in einem Positionspapier wesentliche Anforderungen an eine moderne Transparenzgesetzgebung.

Die Konferenz hält Regelungen in den Informationsfreiheits- und Transparenzgesetzen für erforderlich. Diese müssen um geeignete Instrumente zur Veröffentlichung von Informationen ergänzt werden. Datenbestände öffentlicher Stellen dürfen grundsätzlich nicht durch Urheberrecht oder Nutzungsbeschränkungen blockiert werden. Um Urheberrechten Dritter Rechnung zu tragen, sollten öffentliche Stellen mit diesen die Einräumung der Nutzungsrechte vertraglich vereinbaren.

Open Data muss als wesentlicher Bestandteil der Informationsfreiheit verstanden werden. Allerdings wird der Anspruch auf Informationszugang im herkömmlichen Antragsverfahren auch in Zukunft unverzichtbar sein. Eine Weiterentwicklung der bestehenden Informationsfreiheitsrechte um möglichst umfassende Veröffentlichungspflichten halten die Informationsfreiheitsbeauftragten für unerlässlich. Mit dem Positionspapier unterstützen sie die begonnenen Open-Data-Projekte und empfehlen den Gesetzgebern eine enge Verzahnung von Informationsfreiheit und Open Data.

3.2.2 Verbraucher durch mehr Transparenz im Lebensmittelbereich schützen – Veröffentlichungspflichten für Hygieneverstöße jetzt nachbessern!

Mit der Reform des Verbraucherinformationsrechts zum 1. September 2012 hat der Gesetzgeber als Reaktion auf die Lebensmittelskandale der letzten Jahre mit § 40 Abs. 1a Lebensmittel- und Futtermittelgesetzbuch (LFGB) eine Rechtsgrundlage für die Veröffentlichung von Hygieneverstößen durch die zuständigen Behörden geschaffen. Schon im damaligen Gesetzgebungsverfahren hatte die Konferenz der Informationsfreiheitsbeauftragten darauf hingewiesen, dass die Vorschrift zu undifferenziert sei.

Nachdem zahlreiche Bundesländer begonnen hatten, Verbraucherinnen und Verbraucher auf eigens dafür geschaffenen Internetplattformen über entsprechende Hygieneverstöße zu informieren, sind die Veröffentlichungen durch eine Reihe von verwaltungsgerichtlichen Entscheidungen in Baden-Württemberg, Bayern, Berlin, Nordrhein-Westfalen und Rheinland-Pfalz gestoppt worden. Nach Auffassung der Gerichte greift § 40 Abs. 1a LFGB unter anderem deshalb unverhältnismäßig in die Rechte der betroffenen Unternehmen ein, weil die Vorschrift schon bei geringen Verstößen eine Veröffentlichung zulasse und keine Grenzen für die Dauer der Veröffentlichung vorsehe.

Die Informationsfreiheitsbeauftragten des Bundes und der Länder appellieren daher an die Bundesregierung, dringend die lebensmittelrechtlichen Vorschriften über die Information der Öffentlichkeit zu überarbeiten und wie vom Bundesrat angeregt im Fachdialog mit den Ländern ein Transparenzsystem zu schaffen, das in eine rechtskonforme und effektive Gesamtkonzeption eingebunden wird. Nach der Rechtsprechung sind als Kriterien für eine Neuregelung der Veröffentlichungspflicht im Sinne des § 40 Abs. 1a LFGB insbesondere die Schwere des Rechtsverstoßes, eine behördliche Hinweispflicht auf die Tatsache und den Zeitpunkt der Mängelbeseitigung, Löschungspflichten sowie Ermessens- und Härtefallregelungen in Erwägung zu ziehen.

Umfassende Transparenz bei der Lebensmittelsicherheit darf nicht als Belastung für die Betriebe verstanden werden. Vielmehr ist dies der einzige Weg, das Vertrauen von Verbraucherinnen und Verbrauchern in die Qualität der Lebensmittel langfristig herzustellen und zu wahren.

3.2.3 Transparenz bei Sicherheitsbehörden

Im Zusammenhang mit den Enthüllungen der umfassenden und anlasslosen Überwachungsmaßnahmen des US-amerikanischen und des britischen Geheimdienstes wurde bekannt, dass auch ein großer Teil des Kommunikationsverhaltens der Bürgerinnen und Bürger in Deutschland ohne ihr Wissen von diesen Geheimdiensten überwacht worden ist.

Die Konferenz der Informationsfreiheitsbeauftragten fordert die Verantwortlichen in Deutschland und Europa auf, für Transparenz auf nationaler und internationaler Ebene zu sorgen. Das Vertrauen der Bevölkerung kann nur zurückgewonnen werden, wenn die Aufgaben und Befugnisse der Sicherheitsbehörden völkerrechtlich festgelegt und deren tatsächliche Arbeitsweisen nachvollziehbar sind.

Zweifellos verfügen die Nachrichtendienste über Informationen, die nicht offengelegt werden dürfen. Gleichwohl hält die Konferenz die pauschale Ausnahme der Nachrichtendienste des Bundes und der Länder vom Anwendungsbereich der Informationsfreiheits- und Transparenzgesetze für nicht hinnehmbar und erwartet von den Gesetzgebern entsprechende Verbesserungen.

Darüber hinaus bedürfen die weit gefassten Ausnahmeregelungen für Sicherheitsbelange in den Informationsfreiheits- und Transparenzgesetzen einer Überprüfung und Einschränkung.

Die Informationsfreiheitsbeauftragten unterstützen die Verbesserung der Transparenz der nachrichtendienstlichen Aktivitäten gegenüber den Parlamenten und schließlich die Stärkung der parlamentarischen Kontrollgremien.

3.2.4 Für einen effektiven presserechtlichen Auskunftsanspruch gegenüber allen Behörden – auch des Bundes

Das Bundesverwaltungsgericht hat mit Urteil vom 20. Februar 2013 entschieden, dass die Pressegesetze der Länder keine Verpflichtung von Bundesbehörden zur Auskunftserteilung an Journalistinnen und Journalisten begründen. Die Gesetzgebungskompetenz für den presserechtlichen Auskunftsanspruch gegenüber Bundesbehörden liege danach beim Bund. Eine entsprechende Auskunftsverpflichtung existiert bislang nicht. Das Bundesverwaltungsgericht sieht einen unmittelbar aus der Garantie der Pressefreiheit abgeleiteten „Minimalstandard von Auskunftspflichten“ und einen einklagbaren, ebenfalls unmittelbar aus Art. 5 Abs. 1 Satz 2 GG abgeleiteten Rechtsanspruch auf Auskunft, soweit dem nicht berechnete schutzwürdige Vertraulichkeitsinteressen von Privatpersonen oder öffentlichen Stellen entgegenstehen. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland begrüßt die Entscheidung des Bundesverwaltungsgerichtes insofern, als damit der Auskunftsanspruch von Journalistinnen und Journalisten grundrechtlich abgeleitet und abgesichert wird.

Aus Sicht der Konferenz gilt es – unabhängig von der kontrovers diskutierten Regelungszuständigkeit – die notwendigen gesetzlichen Grundlagen für eine effektive journalistische Recherche herzustellen, die eine zeitnahe, aktuelle und profunde Berichterstattung ohne abschreckende Kostenhürden möglich machen. Das Urteil, das einen unscharfen, beliebig interpretierbaren Minimalstandard mit unklaren Grenzen und Beschränkungsmöglichkeiten zugesteht, darf hier jedenfalls nicht das letzte Wort sein! Bundesbehörden müssen denselben Auskunftspflichten unterliegen wie Landesbehörden.

3.3 25. Konferenz am 27. November 2012 in Mainz

3.3.1 Mehr Transparenz bei Krankenhaushygienedaten

Das Vertrauen der Bevölkerung in das deutsche Gesundheitssystem, insbesondere in unsere Krankenhäuser, hat im Laufe der letzten Jahre abgenommen. Dies ist auch auf eine verbreitete Intransparenz zurückzuführen.

Zwar wurden in einem von einer Tageszeitung herausgegebenen Klinikführer Berlin-Brandenburg erstmals auch Hygienedaten veröffentlicht, jedoch nahmen nicht alle Krankenhäuser an der dieser Publikation zugrunde liegenden freiwilligen Datenerhebung teil. Das wurde unter anderem damit begründet,

dass die nur zu internen Zwecken erhobenen Daten falsch interpretiert werden könnten und dass Patientinnen und Patienten möglicherweise andere Krankenhäuser wählen würden, wenn sie über entsprechende Vergleichsdaten verfügten.

Die Entscheidung für oder gegen ein bestimmtes Krankenhaus können die Patientinnen und Patienten aber nur dann verantwortlich treffen, wenn ihnen alle relevanten Parameter zur Verfügung stehen; dazu gehören auch die jeweiligen Hygienedaten und ihre Umsetzung in den einzelnen Kliniken. Nur eine standardisierte Melde- und Veröffentlichungspflicht für alle Hygienedaten ermöglicht es jedem Patienten und jeder Patientin, die jeweiligen Hygienestandards der Krankenhäuser zu bewerten und zu vergleichen.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert daher alle Verantwortlichen, insbesondere den Bundes- und die Landesgesetzgeber auf, für Transparenz bei Krankenhaushygienedaten zu sorgen. Dazu gehören auch standardisierte und weit reichende Melde- und Veröffentlichungspflichten und die Erweiterung der Qualitätsberichte der Krankenhäuser. Dies wäre ein wichtiger Schritt, um durch mehr Transparenz das Vertrauen der Bevölkerung in die Gesundheitsversorgung durch Krankenhäuser zu fördern.

3.3.2 Parlamente sollen in eigener Sache für mehr Transparenz sorgen!

Die Informationsfreiheitsgesetze von Bund und Ländern nehmen die Parlamente von den für sonstige öffentliche Stellen bestehenden Transparenzpflichten aus. Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland sieht, dass der Kernbereich der Abgeordnetentätigkeit in der unabhängigen Wahrnehmung ihres Mandats nicht dem umfassenden Zugangsanspruch der Öffentlichkeit unterliegen kann. Defizite bei der Transparenz führen aber zu einem Verlust an öffentlicher Glaubwürdigkeit. Die Parlamente von Bund und Ländern sollten deshalb Vorreiter in Sachen Transparenz werden und Ausnahmen vom Informationszugang soweit wie möglich zurücknehmen.

In welchem Umfange Transparenz herzustellen ist, ist eine Frage des verfassungsrechtlich gebundenen, gesetzgeberischen Ermessens. Dieses verpflichtet die Parlamente dazu, die bereits vorhandenen Transparenzregelungen regelmäßig daraufhin zu überprüfen, ob sie sich bewährt haben oder ggf. zu konkretisieren und zu ergänzen sind.

Dabei sollten – soweit noch nicht geschehen – folgende Punkte berücksichtigt werden:

- a. ein möglichst hohes Maß an Transparenz bei den weiteren Tätigkeiten und Einkünften von Abgeordneten unter Berücksichtigung von Berufsgeheimnissen. Den möglichen Besonderheiten des Mandats, insbesondere bei „Teilzeit“-Parlamenten, sollte Rechnung getragen werden,
- b. Veröffentlichung von Tagesordnungen von Plena und Ausschüssen, ebenso Stellungnahmen, Protokolle und weitere Unterlagen, die Gegenstand der Beratungen sind,
- c. Öffentlichkeit von Sitzungen der Fachausschüsse,
- d. grundsätzliche Veröffentlichung von wissenschaftlichen Ausarbeitungen der Parlamentsdienste und sonstiger Gutachten,
- e. Zugang zu Informationen über Beschaffungen, Reisen, Sachausgaben und sonstige kostenträchtige Vorhaben der Parlamente und ihrer Ausschüsse.

3.4 24. Konferenz am 12. Juni 2012 in Mainz

3.4.1 Informationsfreiheit auf europäischer Ebene ausbauen, nicht einschränken!

Mit Besorgnis nehmen die Informationsfreiheitsbeauftragten in Deutschland zur Kenntnis, dass der freie Zugang zu Dokumenten der Europäischen Union gemäß Verordnung 1049/2001 erneut in Frage gestellt wird. Bereits im Jahre 2008 hatte die Europäische Kommission mannigfaltige Vorschläge zu einer drastischen Einschränkung des Zugangs zu europäischen Dokumenten vorgelegt, deren Folge eine massive Reduzierung der gebotenen Transparenz des Handelns europäischer Institutionen gewesen wäre (vgl. Entschließung der Informationsfreiheitsbeauftragten in Deutschland vom 30. Juni 2008). Das Europäische Parlament forderte daraufhin zwar eine Stärkung der Informationsfreiheit, doch arbeiten die Mitgliedstaaten derzeit daran, genau das zu verhindern. Ein „Kompromisspapier“ der dänischen Ratspräsidentschaft sah zuletzt vor, das Zugangsrecht zu Akten der Institutionen der Europäischen Union deutlich einzuschränken.

Während bislang alle Arten von Inhalten der Informationsfreiheit unterfallen, sollen zukünftig nur „formell übermittelte“ Dossiers öffentlich einzusehen sein. Damit würden der Öffentlichkeit sämtliche Entwürfe oder Diskussionspapiere des Rats, der Kommission und des Parlaments vorenthalten. Dies würde

auch Vertragsverletzungsverfahren, Wettbewerbs- und Kartellverfahren betreffen, die von hohem öffentlichem Interesse sind.

Die Konferenz lehnt die Ausnahme einzelner europäischer Institutionen von der Transparenzpflicht ab. Sie tritt dafür ein, dass insbesondere die Europäische Zentralbank und die Europäische Investitionsbank nicht nur hinsichtlich ihrer Verwaltungstätigkeiten auf mehr Transparenz verpflichtet werden.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland appelliert an die Bundesregierung, sich im Europäischen Rat für mehr Transparenz einzusetzen. Verwaltung und Politik auf der Ebene der Europäischen Union dürfen nicht in bürokratische Geheimniskrämerei zurückfallen. Die Forderungen des Europäischen Parlaments müssen endlich erfüllt werden. Gerade angesichts der zunehmenden Verantwortung, die den europäischen Institutionen von der gemeinsamen Außenpolitik bis zur Bewältigung der Finanzkrise zukommt, gilt es, alle Institutionen der Europäischen Union noch weiter zu öffnen. Denn: Vertrauen basiert auf Transparenz!

3.4.2 Mehr Transparenz bei der Wissenschaft – Offenlegung von Kooperationsverträgen

Die Kooperation zwischen Wissenschaft und Wirtschaft hat eine lange Tradition. Dies gilt für gemeinsame Institute ebenso wie für Stiftungsprofessuren und sonstige Formen der Zusammenarbeit.

Unternehmensfinanzierte Forschung nimmt einen immer größeren Anteil an der Wissenschaft ein. Deutschlandweit sollen inzwischen 660 Lehrstühle direkt oder indirekt von Unternehmen finanziert sein. Oft sind Motivation und Umfang der Förderung für Außenstehende nicht erkennbar. Für eine Beurteilung der Forschungsergebnisse und deren Bewertung ist die Kenntnis dieser Hintergründe jedoch Voraussetzung. Die Freiheit von Forschung und Wissenschaft lebt von einer offenen Diskussion; Geheimhaltung engt diese Freiheiten ein.

Einer verborgenen Einflussnahme auf Forschungsgegenstände, Forschungsergebnisse und auf deren Veröffentlichung kann nur durch eine konsequente Politik der Offenheit begegnet werden. Kooperationsverträge zwischen Wissenschaft und Unternehmen sind grundsätzlich offenzulegen. Eine solche Veröffentlichungspflicht sollte mindestens die Identität der Drittmittelgeber, die Laufzeit der Projekte, den Förderumfang und die Einflussmöglichkeiten der Drittmittelgeber auf Forschungsziele und -ergebnisse umfassen. Die Pflicht zur Veröffentlichung der Verträge darf nur zurücktreten, soweit und solange die Bekanntgabe gesetzlich geschützte Interessen beeinträchtigt.

Die regelmäßige Offenlegung der Finanzierung von Forschungsprojekten ist nach Auffassung der Informationsfreiheitsbeauftragten ein geeignetes Instrument, um die Freiheit der Forschung zu schützen, indem einseitige Abhängigkeiten oder auch nur deren Anschein vermieden wird. Eine reine Selbstverpflichtung der Universitäten und Forschungseinrichtungen ist hierfür nicht ausreichend. Es bedarf vielmehr konsequenter Regelungen in den Informationsfreiheitsgesetzen des Bundes und der Länder.

4 Abkürzungsverzeichnis

ABl.	=	Amtsblatt
Abs.	=	Absatz
AGB	=	allgemeine Geschäftsbedingungen
AOK	=	Allgemeine Ortskrankenkasse
Art.	=	Artikel
BbgDSG	=	Brandenburgisches Datenschutzgesetz
BbgKVerf	=	Kommunalverfassung des Landes Brandenburg
BbgMeldG	=	Brandenburgisches Meldegesetz
BDSG	=	Bundesdatenschutzgesetz
BGBI.	=	Bundesgesetzblatt
BRAVORS	=	Brandenburgisches Vorschriftensystem
BSI	=	Bundesamt für Sicherheit in der Informationstechnik
bzw.	=	beziehungsweise
BYOD	=	Bring Your Own Device
CD	=	Compact Disc
DIN	=	Deutsches Institut für Normung
DMDA	=	De-Mail-Diensteanbieter
DNSsec	=	Domain Name System Security Extensions
DV	=	Datenverarbeitung
DVD	=	Digital Versatile Disc
EFRE	=	Europäischer Fonds für regionale Entwicklung
e. G.	=	eingetragene Genossenschaft
eID	=	elektronische Identität
EnWG	=	Energiewirtschaftsgesetz
ggf.	=	gegebenenfalls
GPEN	=	Global Privacy Enforcement Network
GPS	=	Global Positioning System
GVBl.	=	Gesetz- und Verordnungsblatt
HGB	=	Handelsgesetzbuch
HRV	=	Handelsregisterverordnung
ID	=	Identifikator
IFG	=	Informationsfreiheitsgesetz des Bundes
inkl.	=	inklusive
INSPIRE	=	Infrastructure for Spatial Information in Europe
iOS	=	Internetwork Operating System
IP	=	Internet Protokoll
IPsec	=	Internet Protocol Security
IPv4	=	Internet Protokoll Version 4
IPv6	=	Internet Protokoll Version 6
IT	=	Informationstechnik
Kfz	=	Kraftfahrzeug
Kita	=	Kindertagesstätte

LVN	=	Landesverwaltungsnetz
NAT	=	Network Address Translation
Nr.	=	Nummer
ÖPNV	=	öffentlicher Personennahverkehr
PRISM	=	Überwachungsprogramm der amerikanischen National Security Agency
PC	=	Personal Computer
Quellen-TKÜ	=	Quellen-Telekommunikationsüberwachung
S.	=	Seite
SAGA	=	Standards und Architekturen für E-Government-Anwendungen
SCHUFA	=	Schutzorganisation für allgemeine Kreditsicherung
SGB VIII	=	Achtes Buch Sozialgesetzbuch
SGB X	=	Zehntes Buch Sozialgesetzbuch
SIM	=	Subscriber Identity Module
SKEiBB	=	Standardisiertes Kommunales Einsatzleitsystem
SMS	=	Short Message Service
SSL	=	Secure Socket Layer
StPO	=	Strafprozessordnung
Tempora	=	Codename für ein Überwachungsprogramm des britischen Government Communications Headquarters
u. a.	=	unter anderem
u. Ä.	=	und Ähnliche
USB	=	Universal Serial Bus
usw.	=	und so weiter
u. v. m.	=	und vieles mehr
vgl.	=	vergleiche
VoIP	=	Voice over IP
VPN	=	virtuelles privates Netzwerk
z. B.	=	zum Beispiel
z. T.	=	zum Teil
XKeyScore	=	Überwachungsprogramm der amerikanischen National Security Agency

5 Stichwortverzeichnis

Abwasserentsorgung	149, 151
AGB	24
Agnes 2	65
Akteneinsicht	62, 87
Akteneinsichts- und Informationszugangsgesetz	27
ALG-II-Leistungsbescheid	47
Amtsblatt	92
Android	20, 23
Anonymisierung	50
Anschriftendaten	65
Antragstellung per E-Mail	144, 153
App Store	23
Apple	20, 23
Apps	21, 23, 26, 112
Arbeitszeiterfassung	60
Archiv	87
Archivierung	26
Arzt	62, 67
Aufsichtsakte	150
Auskunft	53, 54, 87, 132, 133, 134
Auskunftei	54
Ausweisdaten	129
Authentifizierung	24, 153
Auto-Cockpit-Kamera	124
Backup	22
Bahn	119
Bausparkasse	54
Beanstandung	18
Beitragssatzung	151
Benutzerverhalten	22
Beschäftigtendatenschutzgesetz	55
Beschlussvorlage	89
Betriebsrat	61
Betriebsvereinbarung	122
Beweisführung	120
Bewerbungsunterlagen	132
Bewilligungsbescheid	47
Bildanalyse	123
Blackberry	20
Blackbox	121
Brandenburg Business Guide	130
Brandenburgischer IT-Dienstleister	75

Brandenburg-Tag	163
Brandschutz.....	84
Bundesmeldegesetz	81
Bundespolizei	123
Bürgerumfrage.....	97
Bus	119
Bußgeld	131
BYOD	25
Cloud-Dienst.....	20
Codeanalyse.....	24
Container-Applikation	22
Darlehen	54
Datenbank	
polizeiliche.....	131
Datenerhebung.....	65
unzulässige	53
Datenlöschung.....	62, 117
Datenschutzbeauftragter	
behördlicher	49, 70, 76, 158
betrieblicher.....	61, 118
Datenschutz-Grundverordnung.....	13, 31, 56
Datenschutztag	
Europäischer	163
Datenträger	
Entsorgung.....	79
Vernichtung.....	40
Datenübermittlung	46, 88
Datenverarbeitung im Auftrag	57
Datenweitergabe	92
De-Mail-Gesetz.....	44
Deutsche Flugsicherung	123
DIN 66399	40
Dritte.....	64
E-Government-Gesetz.....	44
Einrichtung	
optisch-elektronische.....	126
Einsatzleitsystem	84
Einwilligung.....	24, 63, 67
Endgerät	
mobiles.....	106
Erforderlichkeitsprinzip	47
Erschließungsmaßnahme	148
Europäische Kommission	13, 136
Europäischen Union	31

Facebook.....	100, 114
Fahrgastsicherheit	118
Fahrzeugregister	117
Fanpage	101
Fernlöschung.....	22, 26
Fernsperrung	22
Fernwartung	72
Fileserver.....	78
Fingerabdruck.....	59
Firewall	71, 74
Flughafen	122
Fördermittel	52, 151
Forderung.....	53
Frag den Staat.....	154
Fragebogen	64, 118
Funktionsübertragung.....	57
Gebäudesicherung	77
Gehaltsabrechnung	57
Georeferenzierung.....	99
Geräteverschlüsselung	20
Gesundheitsamt	63
Gewalt	120
Gläubiger.....	54
Google.....	20, 66
Google Analytics.....	113
Google Play Store.....	23
GovData	137
GPS-Ortung.....	59
Grobraster	19
Grundrecht	
auf Gewährleistung der Vertraulichkeit und Integrität	
informationstechnischer Systeme.....	105
Grundstücksverkauf.....	143
Gutachten.....	146, 151
Haftung.....	26
Hamburgisches Transparenzgesetz	140
Hausrecht	118
Heimerziehung in der DDR	87
Heimkinder der DDR.....	87
Identifikation	129
Identitätsprüfung.....	49, 55
I-frames	102
Informationsfreiheitssatzung	143
Informationsregister	136

Informationssicherheit.....	71
Inkasso Rechtsanwalt.....	53
Inkassowesen.....	52
Innenrevision	15
Integrität	25
Internet Sweep Day	111
Internetspeicherdienst	46
Internettelefonie.....	103
Internetwache	102
Intimsphäre.....	116
Investitionsbank.....	52
iOS	23, 107
iPad	20
iPhone	20
IPv6	36
IT-Grundschutz.....	73
IT-Grundschutzkatalog	96
IT-Planungsrat	137
IT-Sicherheitskonzept	75
IT-Sicherheitsmanagement.....	71
IT-Standard.....	73
IT-Strategie.....	68
Jailbreaking	21, 26
Jobcenter.....	88
Jugendamt.....	88
Jugendschöffen	90
Kalkulationsunterlagen	151
Kindeswohlgefährdung	88
Kita	52
Kommunalabgabengesetz	152
Kommunalaufsicht	149
Kommunalumfrage	95
Kommunikationsserver	78
Komplettüberprüfung	17
Konferenz der Informationsfreiheitsbeauftragten in Deutschland	161
Kontaktdaten	24
Kontrollabfrage	54
Kopie	48, 145
Kraftfahrt-Bundesamt.....	117
Kraftfahrzeugzulassung	117
Krankenkasse.....	67
Kreditinstitut.....	54
Kreisausschuss	89

Kreistag	89
Landesbeauftragte zur Aufarbeitung der Folgen der kommunistischen Diktatur	87
Landesmeldegesetz.....	82
Landesverwaltungsnetz	75
Landtagsgebäude	126
Laufzeitanalyse.....	24
Lebensgestaltung private	104
Live-Monitoring	119, 123
Lizenznutzung	26
Lohnabrechnung.....	57
Löschung.....	121
Mandant	34, 53
Mandantentrennung.....	35
Mehrfaktorauthentisierung	50
Melderegister.....	81, 90
Merkblatt.....	53
Microsoft.....	20
Ministerium der Finanzen.....	19
Mobile Device Management	22
Negativauskunft.....	134
Netzwerk soziales	100, 114
virtuelles privates.....	21
Novellierung.....	30, 31
Nulltreffer	132
Öffentlichkeit.....	90
Öffentlichkeitsfahndung	100
One-Stop-Shop.....	33
Open Data	136, 163
Opt-Out.....	113
Ordnungswidrigkeitenverfahren	131
Ortsdaten.....	24
Paket	129
Passwort.....	20, 72
Passwortrichtlinie.....	22
Patientendaten	62
Patientenrechte	62
Personalaktenführung.....	56
Personalausweis	129
Personennahverkehr	118
Personenstandsregister zentrales.....	82

Personenstandsverordnung	
Brandenburgische	82
Pflegekasse	64
Planungsunterlagen	145
PolBB-App	106
Postzustelldienst	129
PRISM	11
Pseudonymisierung	50, 67, 68
Qualitätssicherung	67
Quellcode	24
Quellen-Telekommunikationsüberwachung	103
Raumsicherung	77
Rechnungsbeleg	52
Recht auf Löschung	32
Recht auf Vergessen	32
Rechteverwaltung	117
Rechtsanwalt	53
Rechtsprechungsdatenbank	168
Regionalleitstelle	84
Reichweitenanalyse	102
Rettungsdienst	84
Richtlinie	117
Risikoanalyse	23, 25, 26, 117
Rooting	21, 26
Sachbeschädigung	120
SAGA	73
Sandbox	23
Satzung	149
Schadsoftware	20, 23, 26
Schöffen	90
Schriftformerfordernis	153
SCHUFA	54
Schulbehörde	
oberste	110
Schuldnerverzeichnis	93
Schuldnerverzeichnisführungsverordnung	94
Schule	110
Schüler	111
Schulträger	110
Schulverwaltungsprogramm	107
Schutzbedarf	41
Schutzklasse	41
Schweigepflicht	53, 135
anwaltliche	53

Scorewert	54
Selbstabfrage	132
Sensibilisierung	23
Sicherheitsinformationssystem	71
Sicherheitskonzept	21, 25, 74, 117
Sicherheitsrichtlinien	71
Sicherheitsstufe	41
Signatur	
digitale.....	50
SIM-Karte	26
Skype	104
Smart Meter.....	38
Smartphone.....	19, 23, 25
Snowden	32
Softwaretest.....	78
Sozialdaten.....	68, 87, 89
Sozialgeheimnis	48, 89
Sozialleistungen	89
Spähprogramm.....	103
Speicherdauer	120
Speicherdienst.....	46
Speicherfrist.....	123
Sperre	
der Adressdaten	130
SSL.....	117
Staatsanwaltschaft.....	104
Stadtschloss	
Potsdamer.....	126
Stammdatenportal	84
Standard 100-3 (BSI).....	50
Standesamt	82
Statistikstelle.....	97
Steuerdaten	15
Steuerdaten-Abrufverordnung	15
Steuergeheimnis.....	15
Steuern.....	52
Strafantrag.....	131, 134
Straßenbahn.....	119
Straßenbefahrung.....	99
Straßeninfrastruktur	100
Straßenraum	
öffentlicher.....	99
Straßenreinigungssatzung	149
Straßenzustandsbewertung	99

Symposium	
Internationales.....	163
Tablet-Computer.....	19, 23, 25, 65
Tarifbeschäftigte	57
Taxi.....	125
Telearbeit	49
Telekommunikationsanlage	80
Telekommunikationsgeheimnis.....	105
Tempora	11
Tracking Tools	113
Trojaner	103
Überwachung	58
Umgehungsstraße	146
Umweltinformationsgesetz.....	27, 142, 147
Unfallversicherungsträger	48
Update	25
Urheberrecht.....	26, 145
Verbraucherinformationsgesetz	141
Verfahren	
biometrisches	60
Verfahrensverzeichnis	76, 117
Verfügbarkeit	25
Verkehrsunternehmen	118
Verkehrswertgutachten.....	144
Vermögensverzeichnis	93
Veröffentlichungspflicht.....	136
Verschlüsselung	21, 26, 74, 117, 153
Ende-zu-Ende	45, 50
Versorgung	
integrierte	68
Vertraulichkeit.....	25, 63
Verwaltungsakt	153
Verwaltungsverfahrensgesetz.....	152
Verwarnung	131
Videokamera	118, 123
Videoüberwachung	55, 118, 123, 125, 126, 127, 133
Virenschutz.....	22, 71
Virtualisierung.....	22
Voice over IP	103
Volkszählung	85
Vollkontrolle	16
Vollstreckungsgericht	
zentrales.....	94
Vollstreckungsportal	93

Vorabkontrolle	22, 49, 70, 118
Vorschlagslisten	92
Wasserversorgung.....	149
weBBschule.....	107
Weiterverwendungsrichtlinie	136
Werbung	130
Wertgutachten	143
Whistleblower	32
Widerspruch	130
Widerspruchsverfahren.....	144
Willensbildung	147
Windows Phones.....	20
Wohngruppenzuschlag	64
XKeyScore.....	11
Zensus 2011	85
Zertifizierung.....	50
Zugriffsrecht.....	26, 123
Zustellung.....	129
Zutrittskontrolle	60
Zuwendungsempfänger	53
Zwangsvollstreckung	93
Zweckbindung	63, 122